

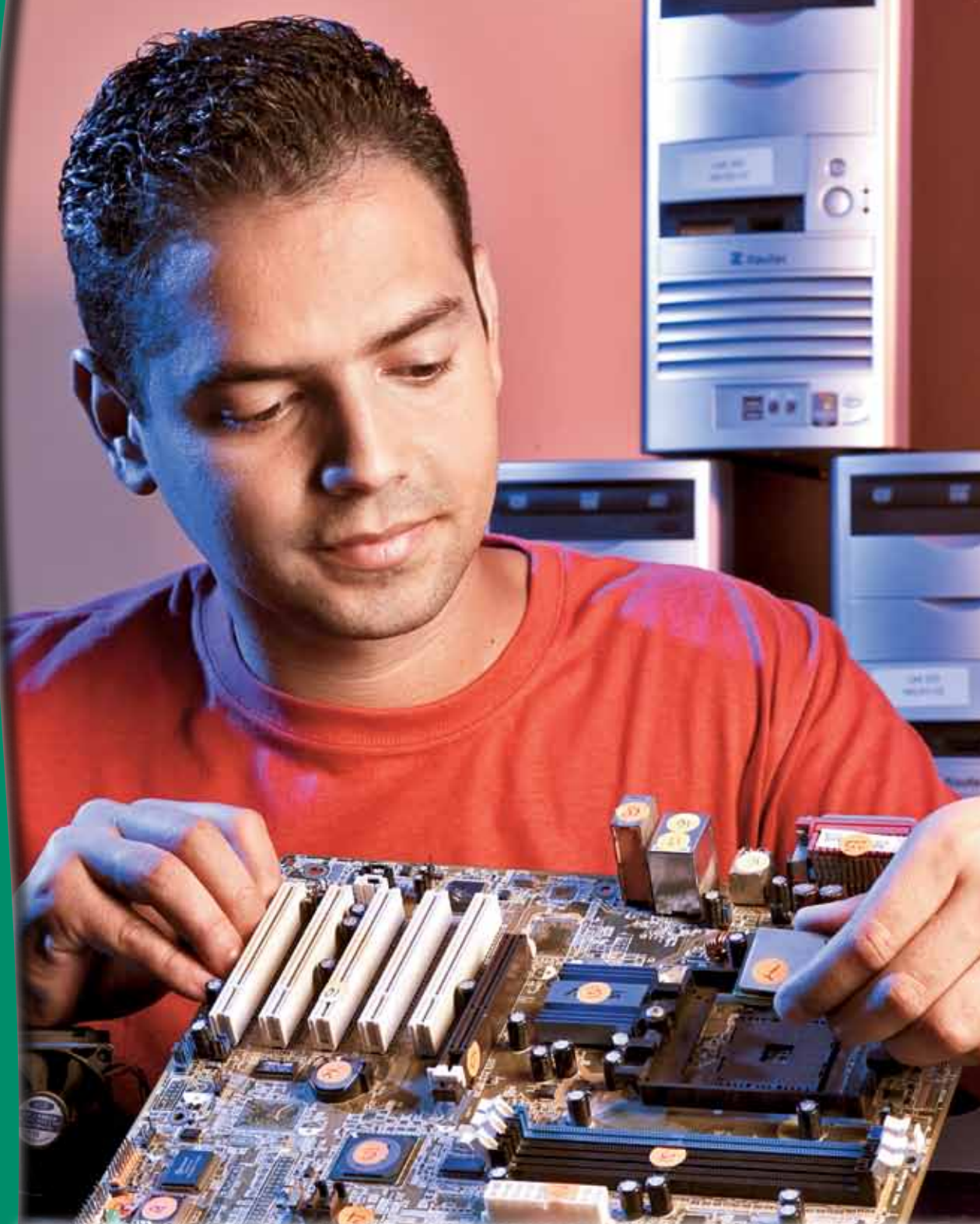
# Informática

Habilitação técnica em

# 2



GOVERNO DO ESTADO  
**SÃO PAULO**  
CADA VEZ MELHOR



## Redes e Manutenção de Computadores

CENTRO PAULA SOUZA



**CENTRO PAULA SOUZA DO GOVERNO DE SÃO PAULO**





CENTRO PAULA SOUZA

# Informática

## Volume 2





CENTRO PAULA SOUZA

# Informática

**Redes e manutenção  
de computadores**

Evaldo Fernandes Réu Júnior





FUNDAÇÃO  
PADRE ANCHIETA

**Presidente**

Paulo Markun

**Vice-Presidente**

Fernando José de Almeida

**Núcleo Cultura Educação**

**Coordenador:** Fernando José de Almeida

**Gerente:** Monica Gardelli Franco

**Equipe de autoria Centro Paula Souza**

**Coordenação geral:** Ivone Marchi Lainetti Ramos

**Coordenação da série Informática:** Luis Eduardo  
Fernandes Gonzalez

**Autores:** Carlos Eduardo Ribeiro, Evaldo Fernandes  
Réu Júnior, Gustavo Dibbern Piva, João Paulo Lemos  
Escola, Luciene Cavalcanti Rodrigues, Ralfe Della  
Croce Filho, Wilson José de Oliveira

**Revisão técnica:** Anderson Wilker Sanfins, Luis  
Claudinei de Moraes, Humberto Celeste Innarelli,  
Sérgio Furgeri

**Equipe de Edição**

**Coordenação geral**

Alfredo Nastari

**Coordenação editorial**

Mirian Ibañez

**Consultor técnico**

Victor Emmanuel J. S. Vicente

**Edição de texto:** Marlene Jaggi

**Editores assistentes:** Celia Demarchi  
e Wagner Donizeti Roque

**Secretário editorial:** Antonio Mello

**Revisores:** Antonio Carlos Marques, Fabiana Lopes  
Bernardino, José Batista de Carvalho, Lieka Felso  
e Miguel Facchini

**Direção de arte:** Deise Bitinas

**Edição de arte:** Ana Onofri

**Editoras assistentes:** Nane Carvalho, Nicéia Cecília  
Lombardi e Roberta Moreira

**Assistentes:** Ana Silvia Carvalho, Claudia Camargo  
e Felipe Lamas

**Ilustrações:** Carlos Grillo

**Pesquisa iconográfica:** Completo Iconografia,  
Maria Magalhães e Priscila Garofalo

**Fotografia:** Carlos Piratininga, Eduardo Pozella  
(fotógrafos) e Daniela Müller (produtora)

**Tratamento de imagens:** Sidnei Testa

Impresso em Vitopaper 76g, papel  
sintético de plástico reciclado, da Vitopel,  
pela Gráfica Ideal.



**GOVERNADOR**

José Serra

**VICE-GOVERNADOR**

Alberto Goldman

**SECRETÁRIO DE DESENVOLVIMENTO**

Geraldo Alckmin

**CENTRO PAULA SOUZA**

**Presidente do Conselho Deliberativo**

Yolanda Silvestre

**Diretora Superintendente**

Laura Laganá

**Vice-Diretor Superintendente**

César Silva

**Chefe de Gabinete da Superintendência**

Elenice Belmonte R. de Castro

**Coordenadora da Pós-Graduação,  
Extensão e Pesquisa**

Helena Gemignani Peterossi

**Coordenador do Ensino Superior de  
Graduação**

Angelo Luiz Cortelazzo

**Coordenador de Ensino Médio e  
Técnico**

Almério Melquíades de Araújo

**Coordenador de Formação Inicial e  
Educação Continuada**

Celso Antonio Gaiote

**Coordenador de Infraestrutura**

Rubens Goldman

**Coordenador de Gestão Administrativa  
e Financeira**

Armando Natal Maurício

**Coordenador de Recursos Humanos**

Elio Lourenço Bolzani

**Assessora de Avaliação Institucional**

Roberta Froncillo

**Assessora de Comunicação**

Gleise Santa Clara

**Procurador Jurídico Chefe**

Benedito Libério Bergamo

**Dados Internacionais de Catalogação na Publicação (CIP)  
(Bibliotecária Silvia Marques CRB 8/7377)**

R442

Réu Junior, Evaldo Fernandes  
Informática, redes e manutenção de computadores /  
Evaldo Fernandes Réu Junior; revisor Anderson Wilker Sanfins ;  
coordenador Luis Eduardo Fernandes Gonzalez. -- São Paulo :  
Fundação Padre Anchieta, 2010

(Manual de Informática Centro Paula Souza, v. 2)

ISBN 978-85-61143-49-7

I. Sistemas operacionais (Computadores) 2. Softwares de aplicação  
I. Sanfins, Anderson Wilker, revisor II. Gonzalez, Luis Eduardo  
Fernandes, coord. III. Título

CDD 005.43



# Sumário

**21 Capítulo 1**  
**O computador**

1.1. Hardware e software .....	22
1.2. Partes do Computador – hardware .....	23
1.3. Componentes externos da unidade de sistema .....	24
1.4. Pannel frontal.....	24
1.5. Parte de trás da unidade de sistema.....	26
1.6. Periféricos .....	26

**29 Capítulo 2**  
**Instalação elétrica**

2.1. Tomada .....	30
2.2. Energia eletroestática .....	31
2.3. Aterramento .....	32
2.4. Dispositivos de proteção.....	33
2.4.1. Filtros de linha .....	33
2.4.2. Estabilizador .....	33
2.4.3. No-break .....	34

**37 Capítulo 3**  
**Normas de laboratório**

**41 Capítulo 4**  
**Unidades de medida**

4.1. Binários .....	42
4.1.1. Hexadecimais .....	45

**49 Capítulo 5**  
**Gabinetes**

5.1. Padrões .....	50
5.2. Formatos .....	51
5.3. Abertura do gabinete .....	51

**55 Capítulo 6**  
**Fonte de alimentação**

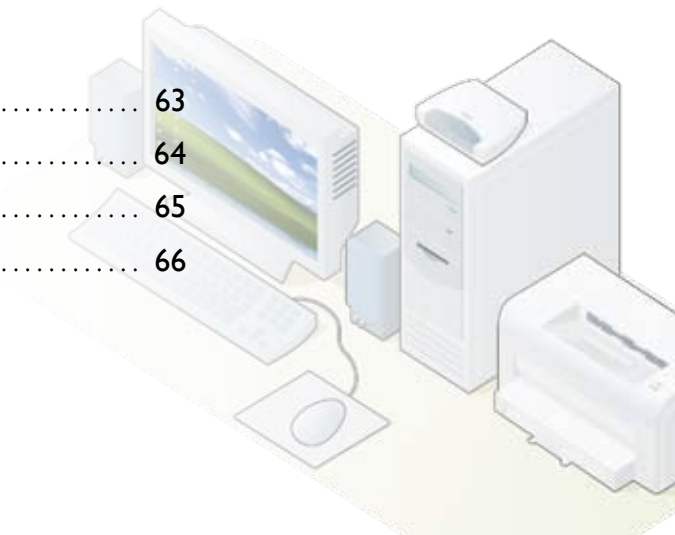
6.1. Instalação .....	58
-----------------------	----

**61 Capítulo 7**  
**Placa-mãe**

7.1. Conectores .....	63
7.1.1. Conector de áudio .....	64
7.1.2. Conector do fax-modem on-board .....	65
7.1.3. Conector de rede on-board.....	66

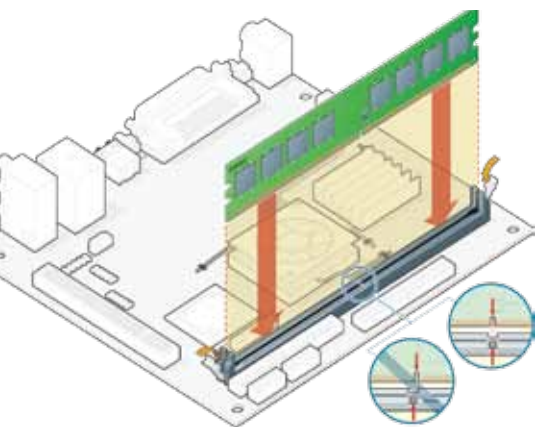


Capa: Eduardo Rodrigues Gomes, aluno de uma Etec do Centro Paula Souza.  
Foto: Eduardo Pozella  
Edição: Deise Bitinas





# Sumário



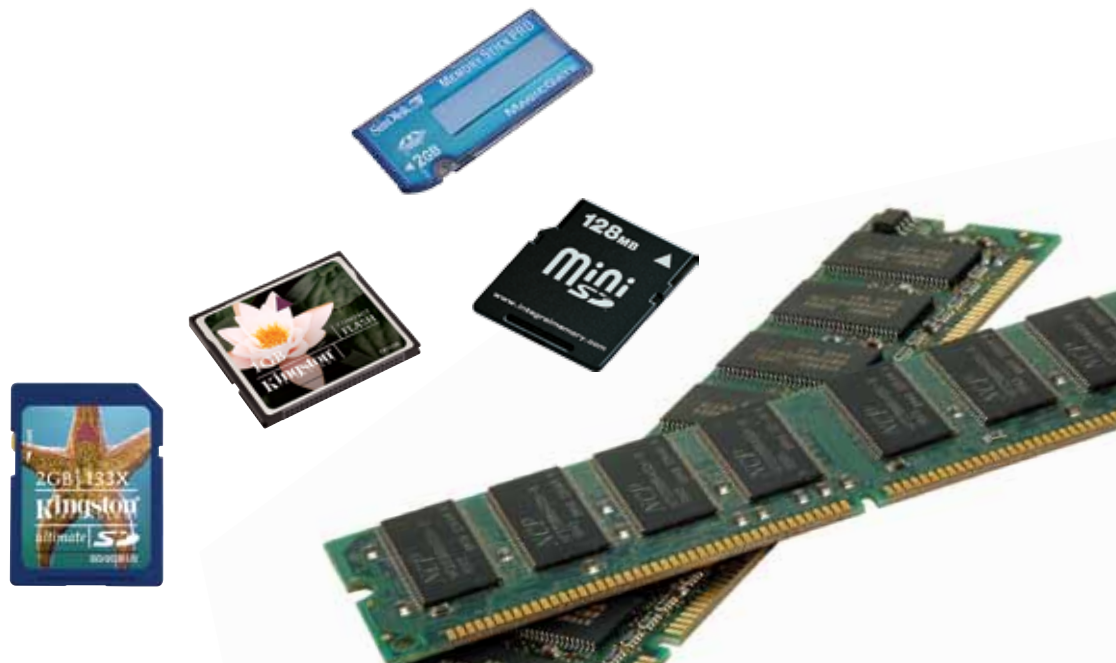
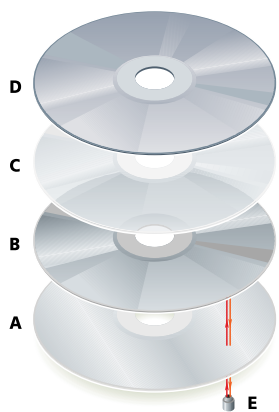
7.1.4. Conector de vídeo on-board.....	66
7.1.5. Conector do processador.....	66
7.1.6. Conector de memória.....	70
7.1.7. Conector porta serial.....	72
7.1.8. Conectores IDE ou PATA.....	72
7.1.9. Conectores SATA.....	73
7.1.10 Conector floppy disk (disquete).....	74
7.1.11. Conector de alimentação.....	74
7.1.12. Conector de teclado.....	75
7.1.13. Conector de impressora.....	75
7.1.14. Conector de mouse.....	76
7.1.15. Conector USB.....	76
7.1.16. Conector Firewire.....	77
7.1.17. Conectores de expansão.....	77
7.1.17.1 ISA.....	77
7.1.17.2. PCI.....	78
7.1.17.3. AGP.....	80
7.1.17.4. CNR e AMR.....	80
7.1.17.5. PCI-Express.....	81
7.2. Dispositivos da placa-mãe.....	82
7.2.1. BIOS BASIC INPUT OUTPUT SYSTEM - Sistema Básico de Entrada/Saída.....	82
7.2.2. Bateria.....	83
7.2.3. Chipsets.....	83



7.2.4. Sensores.....	85
7.2.5. Dispositivos on-board.....	85
7.3. Conceito de barramentos (BUS).....	85

## 87 Capítulo 8 Armazenamento

8.1. Disco rígido.....	88
8.1.1. IDE, ATA ou PATA.....	91
8.1.2. SATA.....	92
8.1.3. Funcionamento.....	92
8.1.3.1 Setor de boot.....	93
8.1.3.2 Endereçamento LBA.....	94
8.1.4. Reconhecimento de discos rígidos.....	94
8.1.4.1. Disco IDE.....	94
8.1.4.2. Disco SATA.....	95





# Sumário

8.1.5. Montagem e configuração de HD.....	95
8.1.6. Particionamento .....	95
8.1.7. Sistemas de arquivos.....	97
8.1.8. Formatação lógica e física .....	97
8.1.9. O sistema de arquivos .....	97
8.1.9.1 FAT.....	98
8.1.9.2 NTFS.....	98
8.1.9.3 Formatos para Linux .....	99
8.1.10. Identificação e correção de falhas.....	100
8.2. Disco flexível .....	101
8.3. Discos ópticos.....	102
8.3.1. CD .....	102
8.3.2. DVD .....	104
8.3.3. Blu-Ray.....	104

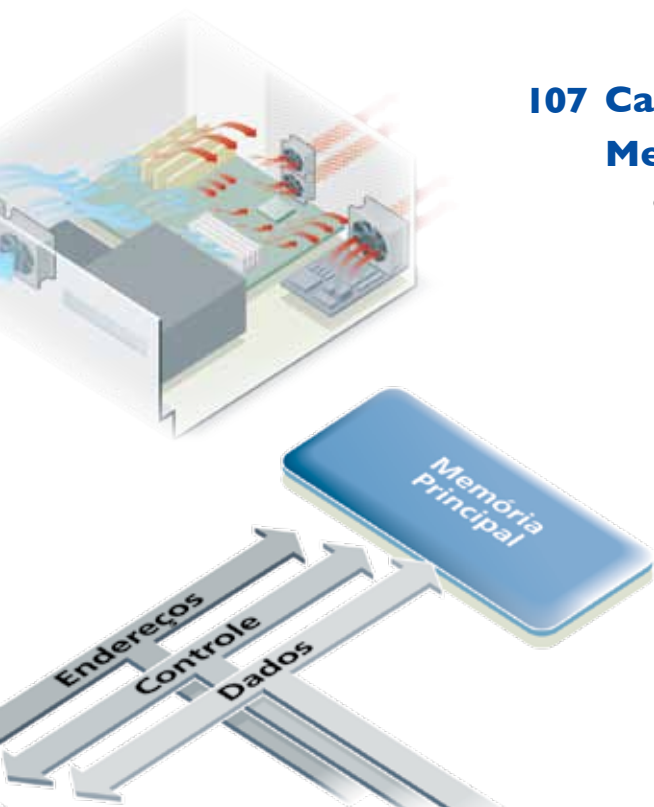
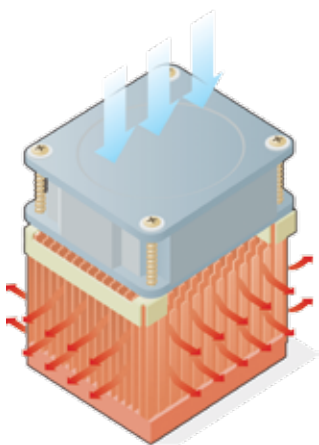
## 107 Capítulo 9 Memória

9.1. ROM .....	109
9.1.1. PROM .....	109
9.1.2. EPROM .....	110
9.1.3. EEPROM .....	111
9.1.4. Memórias flash .....	111

9.2. RAM .....	112
9.2.1. Módulos de memória DIMM .....	113
9.2.2. DRAM .....	113
9.2.3. SDRAM.....	114
9.2.4. SDR e DDR.....	114
9.2.5. Dual channel .....	115
9.3. Cache .....	115

## 117 Capítulo 10 Processador

10.1. Organização do processador .....	119
10.2. Fabricantes e tecnologias .....	120
10.3. Procedimento de instalação de um processador .....	122
10.4. Refrigeração .....	123

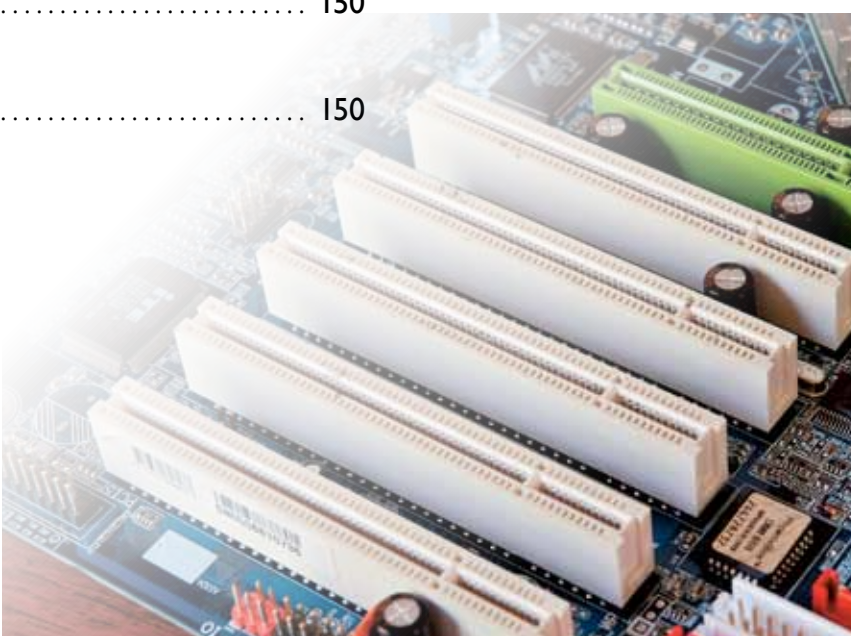
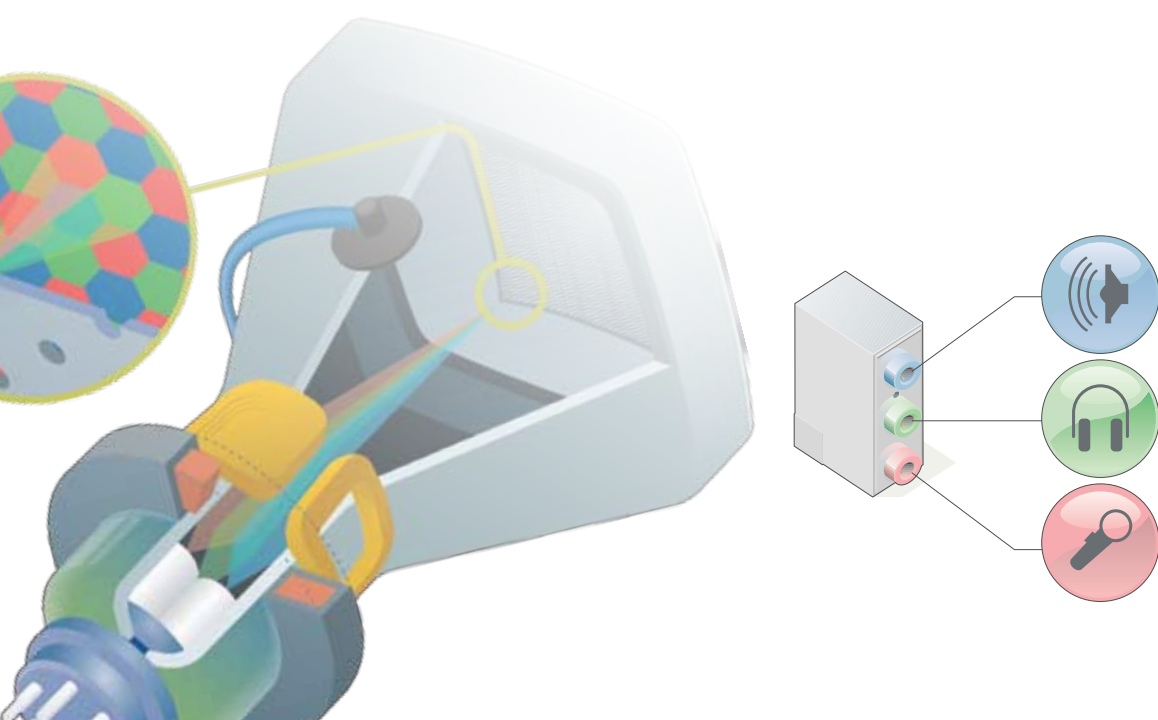


# Sumário



<b>125</b>	<b>Capítulo 11</b>	
	<b>Áudio, vídeo e jogos</b>	
	11.1. Vídeo .....	126
	11.2. Áudio .....	129
<b>131</b>	<b>Capítulo 12</b>	
	<b>Monitores</b>	
	12.1. Resolução.....	133
	12.2. Monitores CRT .....	133
	12.3. LCD .....	135
	12.4. OLED.....	136

<b>139</b>	<b>Capítulo 13</b>	
	<b>Setup</b>	
	13.1. Main (Principal) .....	142
	13.2. Advanced (Avançado) .....	141
	13.3. Power (Energia) .....	142
	13.4. Boot .....	143
	13.5. Security (Segurança) .....	144
	13.6. Exit (Saída).....	145
<b>147</b>	<b>Capítulo 14</b>	
	<b>Instalação de dispositivos</b>	
	14.1. Manual .....	148
	14.2. Softwares controladores (drivers).....	148
	14.3. Métodos de instalação no sistema	
	operacional .....	149
	14.3.1. Windows .....	149
	14.3.2. Linux.....	150
	14.3.3. Descobrir a marca e o	
	modelo de dispositivos.....	150





# Sumário

14.4. Instalação de outros periféricos .....	150
15.4.1. Teclado.....	150
14.4.2. Mouse.....	152

**155 Capítulo 15**  
**Redes de computadores**

15.1. O que são redes.....	156
15.2. Questões sociais .....	156
15.3. Segurança.....	157

**159 Capítulo 16**  
**Tipos de redes**

16.1. Topologia de redes .....	161
--------------------------------	-----

**165 Capítulo 17**  
**Software de rede**

**169 Capítulo 18**  
**Modelos de referência**

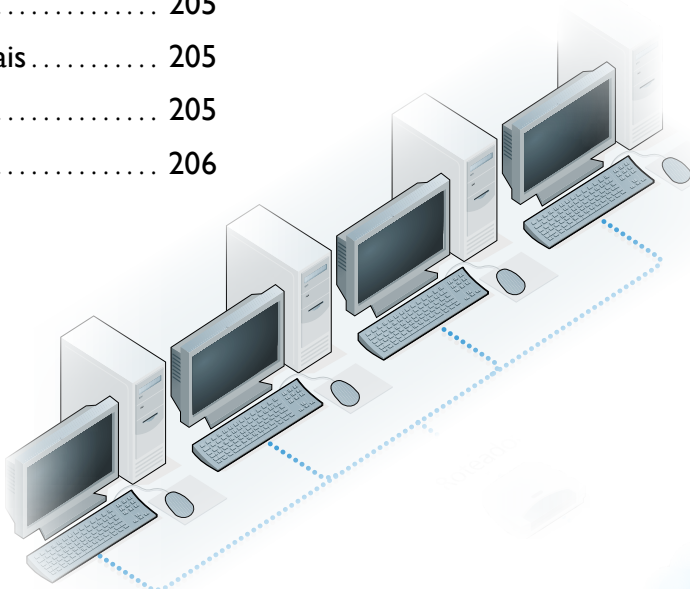
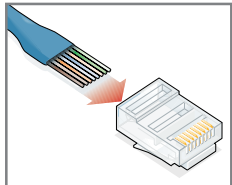
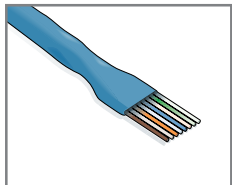
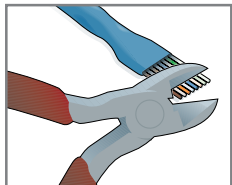
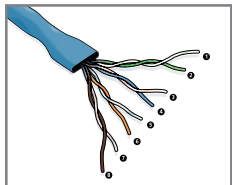
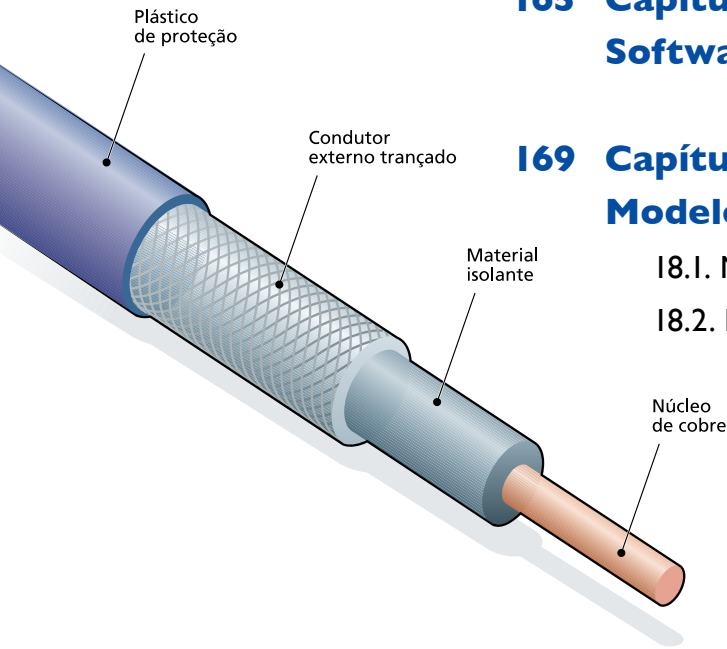
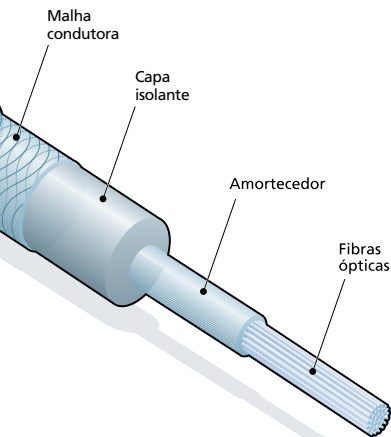
18.1. Modelo de referência ISO OSI.....	170
18.2. Modelo de referência TCP/IP.....	172

**175 Capítulo 19**  
**Internet**

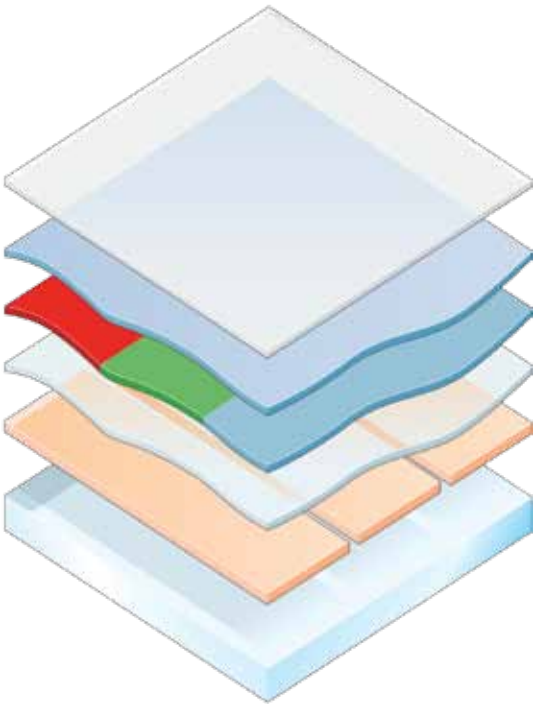
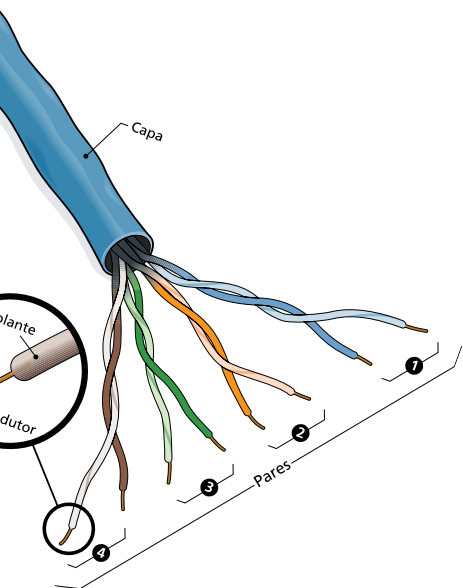
19.1. Arquitetura da internet .....	177
-------------------------------------	-----

**181 Capítulo 20**  
**Arquitetura de rede**

20.1. Camada de aplicação .....	182
20.1.1. DNS .....	182
20.1.2. Correio eletrônico .....	184
20.1.3. WWW.....	189
20.1.4. Transmissão de streaming .....	191
20.1.5. Áudio e vídeo.....	191
20.1.6. VoIP .....	193
20.1.7. P2P .....	194
20.2. Camada de transporte.....	195
20.3. Camada de rede .....	203
20.3.1. Serviços oferecidos pela camada de rede ...	203
20.3.2. Modelo de serviços .....	205
20.3.2.1. Rede de circuitos virtuais .....	205
20.3.2.2. Rede de datagramas .....	205
20.3.3. Roteamento .....	206



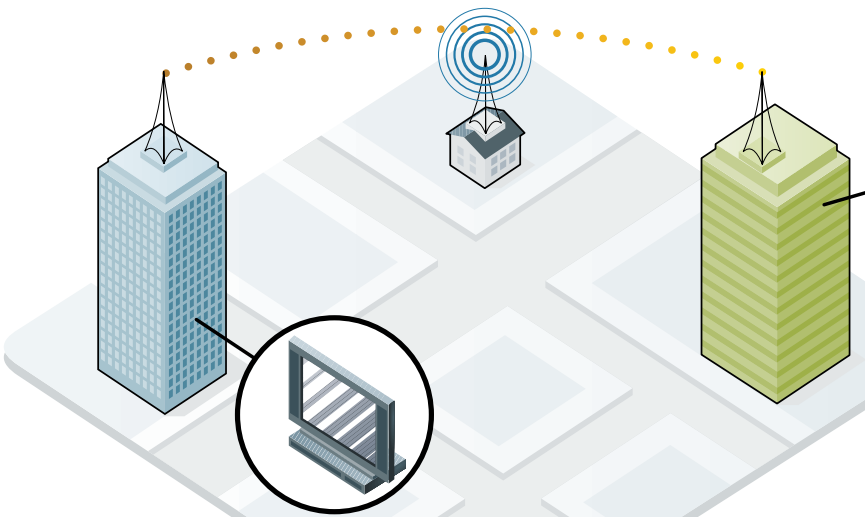
# Sumário



- 20.3.3.1. Descoberta de rotas ..... 207
- 20.3.3.2. Manutenção ..... 208
- 20.3.3.3. Algoritmos de roteamento ..... 209
- 20.3.3.4. Roteamento na internet ..... 210
- 20.3.3.5. Protocolo IGP (Internal Gateway  
Protocols) ..... 210
- 20.3.3.6. Protocolo EGP (External Gateway  
Protocols) ..... 210
- 20.3.3.7. Interligação de redes ..... 211
- 20.3.3.8. Camada de rede na internet ..... 212
- 20.3.3.9. Protocolo IP ..... 213
- 20.3.3.10. Endereços IP ..... 214
- 20.3.3.11. Sub-redes ..... 215
- 20.3.3.12. CIDR ..... 218
- 20.3.3.13. DHCP ..... 219
- 20.3.3.14. NAT ..... 220
- 20.3.3.15. ICMP ..... 221
- 20.3.3.16. Multidifusão na internet ..... 223
- 20.3.3.17. IPv6 ..... 223
  - 20.3.3.17.1. Datagrama IPv6 ..... 224
  - 20.3.3.17.2 Implantação IPv6 ..... 224

- 20.3.3.18. Camada de enlace ..... 225
  - 20.3.3.18.1. Serviços oferecidos pela  
camada de enlace ..... 225
  - 20.3.3.18.2. Subcamadas ..... 227
    - 20.3.3.18.2.1. LLC ..... 227
    - 20.3.3.18.2.2. MAC ..... 233
- 20.3.3.19. Camada física ..... 238
  - 20.3.3.19.1. Serviços oferecidos  
pela camada física ..... 238
  - 20.3.3.19.2. Meio de transmissão ..... 239
    - 20.3.3.19.3. Meio magnético ..... 239
      - 20.3.3.19.3.1. Par trançado ..... 239
        - 20.3.3.19.3.1.1. Normas de montagem ..... 240
        - 20.3.3.19.3.1.2. Ferramentas ..... 241
        - 20.3.3.19.3.1.2.1. Procedimento  
de montagem ..... 242
      - 20.3.3.19.3.2. Cabo Coaxial ..... 244
      - 20.3.3.19.3.3. Fibra óptica ..... 245
      - 20.3.3.19.3.4 Transmissão sem fio ..... 245

- 249 Considerações finais
- 251 Referências bibliográficas





# Capítulo I

## O computador

---

- Hardware e software
- Partes do computador – hardware
- Componentes externos da unidade de sistema
- Painel frontal
- Parte de trás da unidade de sistema
- Periféricos



PHOTOS 12/ALAMY/OTHER IMAGES

O filme *2001 – Uma Odisseia no Espaço*, do cineasta Stanley Kubrick, lançado em 1968, é um exemplo clássico desse temor: a máquina que gerencia a nave espacial pensa sozinha e vai exterminando os astronautas.

**D**urante toda sua história, desde os primórdios, o ser humano procurou dominar o meio ambiente e manipulá-lo de modo a criar melhores condições de sobrevivência. E para isso não usou a força, mas seu poder intelectual, até porque nunca foi fisicamente tão forte quanto grande parte dos animais. O ser humano sempre concebeu mentalmente as estratégias para alcançar seus objetivos. Quando precisou produzir mais quantidade de alimentos, recorreu aos animais, domesticando-os. Quando estes já não davam conta das demandas, cada vez maiores, começou a construir máquinas, que ao longo dos séculos foram se sofisticando para atender suas necessidades nos campos mais variados. Ou seja, ao longo de sua história, o ser humano foi construindo meios de ultrapassar os limites de seu corpo.

Com o pensamento aconteceu exatamente o mesmo: expandimos nossa capacidade de raciocínio por meio de uma máquina, o computador. Durante nossa jornada, desenvolvemos a capacidade de fazer cálculos, analisar, compreender e explorar a natureza, por meio da observação e da inteligência. Porém, nossa capacidade se tornou insuficiente à medida que nosso modo de vida foi ficando mais complexo. Por exemplo, conseguimos calcular o saldo de nossa conta corrente, mas se precisássemos saber o saldo da conta corrente de todos os clientes de uma única agência bancária, ficaríamos um dia inteiro fazendo cálculos e não conseguiríamos concluir o trabalho.

O computador veio para acelerar o processamento das informações, fazer cálculos, analisar sequências e manipular dados em velocidades muito além da capacidade do ser humano. Mas essas máquinas não têm o poder de criar, pois até agora não nos foi possível desenvolver sistemas que façam as máquinas pensar e criar por si próprias – ainda bem, não? Portanto, ninguém precisa se preocupar com a possibilidade de as máquinas virem a dominar o homem. Por enquanto, isso é apenas tema de **filmes de ficção científica**.

I.1. Hardware e software

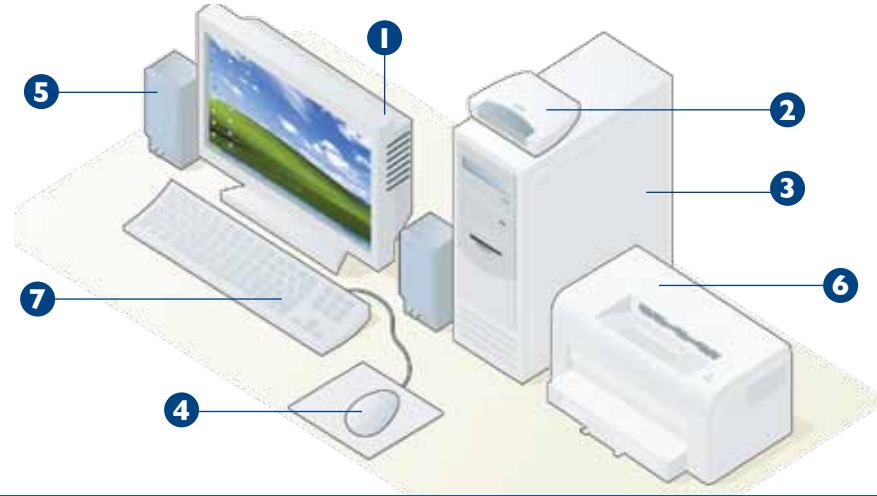
Para um computador funcionar, é necessário haver hardware e software. O hardware é a parte física do computador, seus circuitos eletrônicos, cabos, placas, dispositivos periféricos conectados etc. O software é a parte não física: programas, instruções e procedimentos escritos por programadores para controlar o hardware de modo que este possa executar as tarefas de que precisamos. Uma parte não funciona sem a outra. Se ligarmos um computador sem nenhum software gerenciador instalado, seus leds se acenderão, mas não poderemos usá-lo para absolutamente nada.

I.2. Partes do computador – hardware

O PC (computador pessoal), também conhecido como desktop, é a forma mais conhecida de computador, embora muitos outros formatos estejam presentes em nosso cotidiano, como notebooks, caixas-eletrônicos, telefones celulares, câmeras digitais, palmtops e robôs. Vamos abordar neste livro o desktop.

Componentes do computador pessoal (desktop)

- 1. Monitor** – Exibe visualmente as informações ao usuário.
- 2. Modem** – Conecta o computador à internet.
- 3. Unidade do sistema** – É o cérebro do computador. Abriga a placa-mãe, que interliga todos os componentes; o processador, que executa as informações e os comandos dos programas; as memórias, que armazenam os programas executados enquanto o equipamento estiver ligado; a unidade de disco rígido (HD ou hard disk); o drive de CD/DVD; o drive de disquete e a fonte de alimentação. Na unidade do sistema também são conectados outros dispositivos por meio de cabos que se pode ligar às portas encontradas na frente, atrás e, eventualmente, em alguma das laterais do gabinete.
- 4. Mouse** – Usuário do desktop pode indicar ao computador com qual elemento da tela pretende interagir. O mouse é usado para controlar o cursor na tela, selecionar opções em menus e acionar outros dispositivos exibidos.
- 5. Alto-falante** – Caixa de som, com amplificador, que possibilita ao usuário ouvir os sons, como músicas, áudio de filmes e de avisos enviados pelos programas.
- 6. Impressora** – Usada para imprimir documentos, fotos, trabalhos, relatórios, planilhas, gráficos.
- 7. Teclado** – Dispositivo no qual digitamos textos, confirmamos comandos, passamos as informações solicitadas pelos programas, entre outras ações.



**Figura I**  
Componentes do computador pessoal.



O conjunto dos dispositivos conectados para constituir um computador depende do uso que se fará do equipamento. Para uso pessoal, comercial ou em consultórios, por exemplo, a configuração é a da figura 1.

I.3. Componentes externos da unidade de sistema

A unidade de sistema é o centro do computador. Constitui-se de componentes e conectores de dispositivos que se conectam por cabos e que ficam à vista, e de componentes internos, não acessíveis. Estudaremos estes últimos (placa-mãe, fonte de alimentação, sistema de ventilação, discos rígidos e drives de CD/DVD e disquete) em detalhes mais adiante. Antes, identificaremos as peças visíveis da unidade de sistema.

I.4. Painel frontal

Na parte frontal de uma unidade de sistema (o gabinete), há sempre dois botões, alguns leds (diodo emissor de luz), entradas USB para conexão de pen-drive, cabo de câmera, celular e/ou outros dispositivos. Há ainda drive para inserir disco flexível (disquete), CD-ROM e/ou DVD e leitoras de cartões Flash.

**Botão interruptor Liga/Desliga ou Power** – Nos computadores nos quais se instalou o sistema operacional Windows ou Linux, esse botão é controlado pelo próprio sistema e pode ter mais algumas funcionalidades. Nesses casos, desligar o equipamento por meio do botão, sem que o sistema tenha solicitado a finalização do processo, é prejudicial a sua vida útil. O desligamento brusco pode danificar arquivos ou até mesmo o próprio disco rígido, onde são armazenados os arquivos, comprometendo o funcionamento posterior da máquina. Se o computador estiver desligado, um toque rápido no botão o aciona novamente. Se estiver ligado, um toque rápido pede ao sistema operacional para iniciar o processo de desligar. E, caso o computador pare repentinamente de responder e for preciso desligá-lo de modo forçado, deve-se apertar o botão e mantê-lo pressionado por 5 segundos.

A opção que inicia o desligamento por parte do sistema operacional precisa estar configurada no Windows. A figura 2 mostra como se faz essa configuração no Windows XP.

**Botão de Reset** – Reinicia o computador, como se desligasse e ligasse o micro novamente. Recorremos ao reset quando o computador trava.

Cada dispositivo possui um número de IRQ. Quanto menor for o número, maior será sua importância. Assim, caso duas interrupções ocorram ao mesmo tempo, o processador priorizará a de número de IRQ com menor valor. Se estiver processando uma interrupção e for novamente interrompido por um IRQ de mais prioridade, suspenderá o processamento da interrupção em andamento para tratar da nova, voltando em seguida a processar a interrupção anterior. É como um funcionário que recebe uma ordem do gerente e começa a cumpri-la, mas chega o dono da empresa e lhe pede para fazer alguma outra coisa. O funcionário resolverá antes o problema do patrão, deixando a tarefa do gerente de lado, mas voltará a esse trabalho assim que tiver terminado a tarefa prioritária.

**Figura 2**  
Sequência de telas para configurar o botão desligar da unidade de sistema.

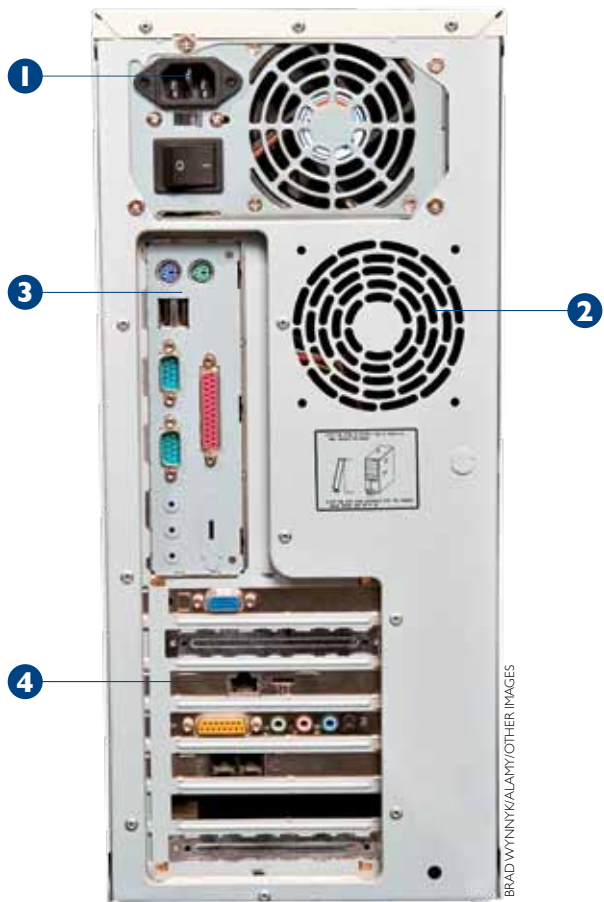


**DICA**  
A forma mais eficaz para saber se o computador está travado ou não é verificar se a luz do teclado que indica se o CapsLock está ativo ou não acende ou apaga ao pressionarmos a tecla CapsLock. Este é um bom teste, pois o teclado tem a máxima prioridade na lista de IRQs (veja no quadro da pág. 27 as prioridades do processador) e deve ser atendido pelo processador antes de qualquer outro dispositivo. Ou seja, se o micro não consegue atender o teclado, com certeza não conseguirá fazer mais nada. A solução, nesse caso, é pressionar o botão reset.

- LED de alimentação** – Indica se o computador está ligado.
- LED de atividade do HD** – Aponta se algum programa está lendo ou escrevendo no disco rígido.
- Leitora de cartões** – Muito comum em micros novos, no lugar do compartimento do antigo disquete.
- Entradas USB** – Para conexão de dispositivos como webcam, câmeras fotográficas e celulares.
- Entrada e saída de áudio** – Para conectar fone de ouvido, caixas de som e microfone.

Figura 3

Vista da parte de trás de uma unidade de sistema.



IMPORTANTE

Pode acontecer de o conector USB frontal ser ligado invertido na placa-mãe durante a montagem do computador. Isso pode danificar ou queimar os dispositivos que forem conectados nessas portas. Por isso recomenda-se testar o conector USB frontal antes de utilizá-lo, e, de preferência, usar as portas USB do painel traseiro do gabinete, pois estas vêm fixadas de fábrica na placa-mãe. Se você for montar o computador, tenha cuidado para não incorrer nesse erro. Você poderia ter de comprar câmera, impressora ou celular novos para seu cliente, Por isso, leia sempre o manual de instruções da placa-mãe.

**Periféricos de saída** – Transmitem informação para o usuário. Por exemplo: monitor, alto-falantes, impressoras.

**Periféricos mistos** – Como você já deve ter imaginado, são aqueles que permitem enviar e receber informações. Exemplo: telas sensíveis ao toque, CDs, DVDs, pen-drives, cartões de memória.

IRQ e as prioridades do processador

IRQ é a sigla para Interrupt Request Line ou linha de requisição de interrupção. Todo dispositivo no computador tem um canal de comunicação com o processador cuja função é chamar sua atenção para alguma ocorrência de que deva ser informado. Com isso o processador interrompe (daí o termo interrupção) o processo que está em execução e prioriza a ocorrência, executando a tarefa necessária para solucioná-la, para só depois prosseguir com a tarefa interrompida. Isso acontece quando uma tecla é pressionada no teclado ou quando a placa de rede recebe dados para serem encaminhados ou quando movemos o mouse. Por ser muito rápido, o processador executa várias tarefas alternadamente, sem que consigamos perceber a alternância: para nós tudo acontece ao mesmo tempo.

I.5. Parte de trás da unidade de sistema

Acompanhe na figura 3 os componentes do lado posterior do gabinete.

- 1. **Fonte de alimentação** – É onde se conecta o cabo de energia que alimenta o computador.
- 2. **Entradas de ar** – Para refrigeração interna.
- 3. **Painel traseiro** – Onde se agregam os conectores da placa-mãe.
- 4. **Baixas de placas adicionais** – Onde ficam os conectores de dispositivos instalados em slots de expansão na placa-mãe.

I.6. Periféricos

São todos os dispositivos que se conectam à unidade de sistema para obter respostas ou para passar informações ao computador. Esses dispositivos são geralmente divididos em três grupos: periféricos de entrada, de saída e mistos.

**Periféricos de entrada** – São aqueles que possibilitam ao usuário passar alguma informação para o computador. Por exemplo: teclado, mouse, microfone, webcam, joystick.



# Capítulo 2

## Instalação elétrica

- Tomada
- Energia eletroestática
- Aterramento
- Dispositivos de proteção

Para funcionar adequadamente, todo aparelho eletrônico precisa de uma alimentação elétrica de qualidade. Sem os devidos cuidados em relação a esse quesito, um computador em perfeito estado pode apresentar defeitos e até queimar.

2.1. Tomada

O computador utiliza plug tripolar (3 polos) e deve ser ligado a uma tomada corretamente polarizada. A ligação correta é: terra abaixo, fase à direita e neutro à esquerda (figura 4). A fase é o polo energizado e, para descobrir se o plug está na posição correta, podemos fazer um teste. O tipo mais comum e barato de teste disponível no mercado é a chave de fenda com neon. Uma tomada com os polos invertidos pode prejudicar o funcionamento do computador e dos dispositivos e provocar até um choque elétrico. No Brasil utilizam-se mais de 10 tipos diferentes desse dispositivo. Com a adoção do modelo padrão (com 3 polos e fio terra), espera-se garantir mais segurança aos usuários (figura 5).

Figura 4

Esquema de polarização.

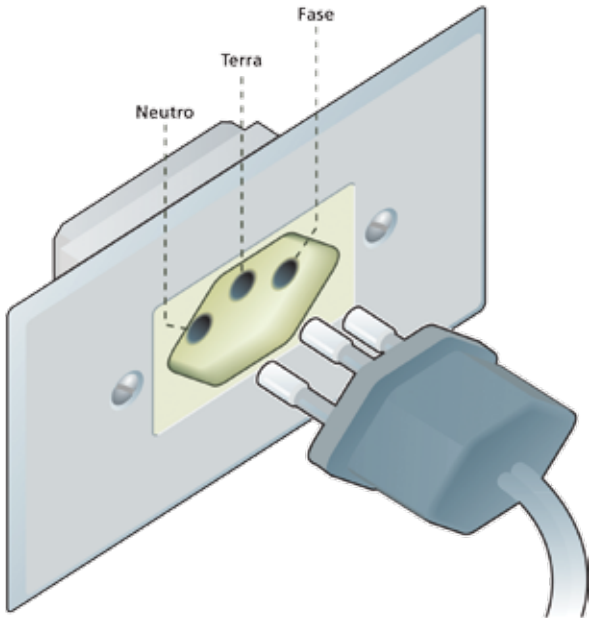


Figura 5

O modelo padrão para tomadas tem 3 polos.

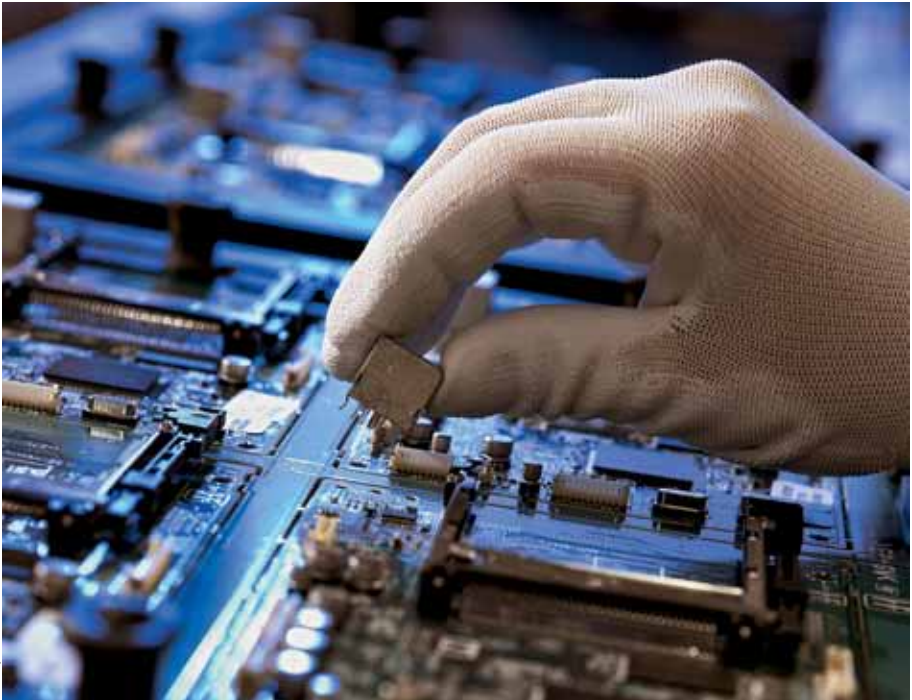
2.2. Energia eletroestática

Muitas vezes a corrente elétrica precisa escapar do aparelho elétrico quando surge algum defeito, ou também para liberar a **energia estática** captada do ambiente. Essa carga de energia vai procurar no solo o ponto de descarga mais próximo possível. Nos dispositivos que têm fio-terra, ou uma tomada com esse polo, a descarga utiliza-o como caminho. Mas se esses fios não estiverem ligados a um aterramento bem feito ou a nenhum aterramento haverá uma

Para prevenir que a energia estática acumulada pelo nosso corpo danifique o equipamento quando nós o manuseamos durante a manutenção, deve-se usar luvas ou pulseiras antiestáticas (figura 6), normalmente conhecidas dos técnicos de informática.

Figura 6

Luva antiestática.





grande chance de a energia utilizar o corpo da pessoa que toca no aparelho como veículo para chegar à terra.

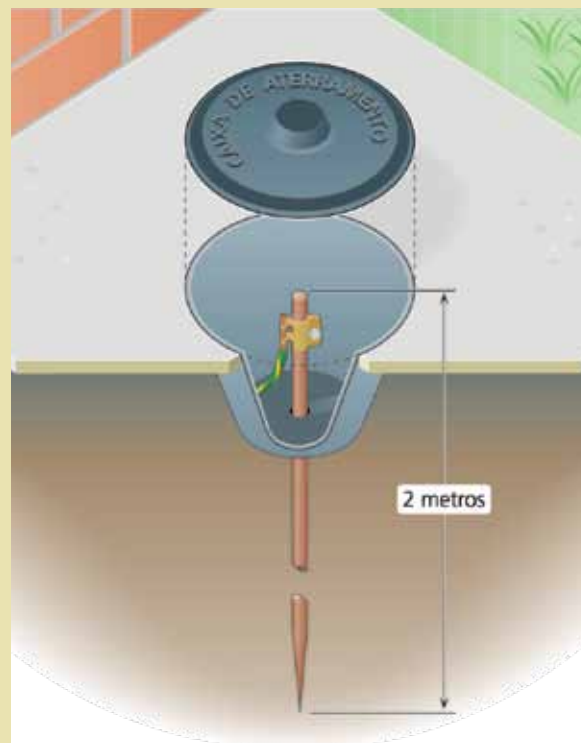
Quem nunca tomou um choque ao descer do carro? Isso decorre da energia estática produzida pela fricção do ar com o automóvel. Quando você toca o chão, essa energia é descarregada para o meio ambiente através do seu corpo. Mas, se para o corpo humano tal descarga não é tão forte, no computador pode causar danos, até mesmo a queima de componentes. O ar também possui energia estática, pois as partículas de poeira em suspensão podem acumular energia. O gabinete do computador serve como captador dessa energia e a descarrega no fio-terra da tomada, evitando que chegue até os dispositivos internos. Portanto, não se deve operar computador com a tampa do gabinete aberta, nem conectado a tomadas sem fio-terra.

### 2.3. Aterramento

No Brasil as residências não costumam ter tomadas com aterramento, embora a Lei Federal 11.337, de 26 de julho de 2006, determine que todas as novas edificações tenham o aterramento da rede elétrica. O aterramento é necessário para que a rede elétrica da construção tenha onde descarregar os surtos de cargas altas de energia, de modo que os aparelhos eletrônicos instalados nessa rede fi-

## Como fazer um aterramento

Segundo o INPE (Instituto Nacional de Pesquisas Espaciais) ocorrem mais de 100 milhões de descargas elétricas atmosféricas no Brasil. Por isso, é bom se prevenir, usando sempre o aterramento nas instalações. Você pode fazer um aterramento eficiente enterrando no solo uma haste de cobre, de mais ou menos 1,5 m, presa a um fio rígido com boa espessura, de preferência por conector, o qual será ligado ao aterramento da rede elétrica (figura 7). Para medir a diferença de potencial entre o neutro e a fase, que não pode ser muito diferente de 1 volt, use um aparelho chamado multímetro. Outro método, artesanal porém eficiente, consiste em ligar uma lâmpada incandescente na fase e outro no terra que você acabou de fazer e verificar a luminosidade produzida, que deve ser igual à da fase com o neutro. O Brasil tem normas definidas sobre proteção da rede elétrica, de acordo com a ABNT: a NBR 5419, que trata de Proteção de Edificações Contra Descargas Atmosféricas e a NB – 3, que aborda Instalações Elétricas de Baixa Tensão.



**Figura 7**

Aterramento com barra de cobre.



**Figura 8**

Filtro de linha.

quem protegidos. Esses surtos podem ocorrer por falha em algum equipamento e, principalmente, por descargas de raios.

Para aprender mais sobre os principais conceitos de energia elétrica acesse o site da Universidade Federal Rural do Rio de Janeiro (<http://www.ufrrj.br/institutos/it/de/acidentes/concp.htm>). Para ver o ranking da incidência de raios no Brasil, acesse o site do INPE: <http://www.inpe.br/ranking/>.

### 2.4. Dispositivos de proteção

Equipamentos ligados à rede elétrica e telefônica, serviços fornecidos por cabo coaxial, como TV e internet, e redes de computadores costumam ser vítimas de descargas eletrostáticas (raios). A descarga elétrica pode invadir a rede e ser transmitida até o seu computador.

Há vários equipamentos no mercado usados para bloquear o fluxo de energia caso a tensão aumente mais que o normal. Entre estes podemos citar os filtros de linha.

#### 2.4.1. Filtros de linha

Esse dispositivo (figura 8) tem um mecanismo de funcionamento muito simples, pois é constituído de fusível ligado entre as tomadas e a fonte de energia. Quando a corrente aumenta, ultrapassando sua capacidade, o fusível queima, cortando a corrente elétrica e impedindo-a de prosseguir até o equipamento. Para a corrente voltar a fluir, basta trocar o fusível. Existem modelos com conectores para cabo telefônico e coaxial.

#### 2.4.2. Estabilizador

As variações na voltagem que ocorrem normalmente no fornecimento de energia elétrica também podem causar falhas nos equipamentos ou diminuir sua vida útil. Quando dizemos que nossa tomada é de 110v, estamos nos referindo à média de energia que esse dispositivo fornece. A tensão na realidade pode ficar variando entre 108, 111 a 120, 127 volts. Para normalizar a tensão utilizamos um estabilizador (figura 9).

**Figura 9**

Estabilizador.



Existem vários modelos e marcas de estabilizador, com potências de 300VA, 400VA, 700VA, 1000VA, 2000VA.

Para saber quantos dispositivos podem ser alimentados por um estabilizador, precisamos descobrir sua capacidade em Watts. Para isso devemos multiplicar a potência em VA do estabilizador pelo Fator de Potência.

$$W = VA \times FP$$

Cada aparelho tem seu fator de potência, portanto devemos procurar esse dado no seu manual. Normalmente esse fator fica em 0.66 (2/3). Assim, uma fonte de 300VA conseguiria suportar aparelhos cujo consumo somado não ultrapassasse 198 Watts ( $W = 300 \times 0.66 = 198$ ).

### 2.4.3. No-break

A falta da energia também é um problema. Caso o computador desligue abruptamente, pode haver perda de dados (um documento que estava sendo digitado, um download que estava sendo feito) ou a corrupção de arquivos e até mesmo do sistema operacional, além de problemas físicos, como falha no disco rígido. O funcionamento de computadores que fazem o papel de servidores e por isso ficam ligados o tempo todo, por exemplo, não pode ser interrompido por falta de energia, pois serviços essenciais seriam afetados. Por isso existem os no-breaks.

Quando o sistema de fornecimento de energia elétrica falha, o no-break (figura 10) mantém o abastecimento por meio de sua bateria até que a energia volte ou o computador seja desligado. Quando o fornecimento é restabelecido o no-break se autorrecarrega.

Em caso de falta de energia prolongada, não é recomendável usar toda a carga da bateria, pois isso provocaria a perda da mesma. A quantidade de tempo que os no-breaks suportam varia de cinco minutos a três horas, dependendo do modelo e do conjunto de baterias utilizadas.

**Figura 10**

O no-break mantém a energia.



Os chamados no-breaks inteligentes possuem interface que se comunica com um software no computador, o qual pode definir uma estratégia de desligamento automático a partir de solicitação do sistema operacional. Assim, esses equipamentos ajudam a evitar falhas no computador e em sua própria **bateria**.

Em grandes empresas, com muitos servidores, utilizam-se também geradores movidos a diesel para manter os equipamentos ligados em caso de falta de energia.



# Capítulo 3

## Normas de laboratório

- Segurança de arquivos
- Vida útil dos equipamentos
- Ambiente de trabalho

**C**omputadores não são baratos, principalmente os mais bem equipados. Apesar dos avanços tecnológicos, que trazem novas versões de computadores em intervalos de tempo cada vez menores, quando alguém adquire um, espera que tenha uma vida relativamente longa, útil e produza o suficiente para compensar o investimento. É claro que, se tais expectativas não são alcançadas, haverá prejuízos, até porque projetos importantes podem se tornar inviáveis. O funcionamento do computador pode ser prejudicado por causa de má instalação, uso inadequado ou mesmo porque o equipamento é de baixa qualidade.

Num ambiente empresarial ou acadêmico o montante de lucro ou prejuízo que os computadores podem trazer é muito alto. Por isso, geralmente, boa parcela do investimento é voltada à proteção e manutenção do parque tecnológico. As instalações elétricas são bem preparadas, os ambientes são climatizados com ar-condicionado, mantidos limpos e sem umidade. Também são contratados técnicos para fazer a manutenção preventiva e corretiva.

Todos esses cuidados, porém, ainda não são suficientes para garantir o bom desempenho dos computadores. Também os usuários devem saber usar adequadamente suas máquinas e para isso devem receber instruções, de acordo com as normas desenvolvidas pela empresa ou instituição para uso de laboratórios de informática. Quando uma norma estabelecida é apresentada a todos os usuários dos computadores, estes devem entender que tal norma foi criada para ser cumprida, e que, caso isso não aconteça, haverá insatisfação e eventual repreensão.

Até o fim do ano de 2009, não havia norma padrão, nacional ou internacional, à qual pudéssemos nos referir neste livro. Cada instituição desenvolve a sua, com base no grau de instrução e na idade dos usuários dos equipamentos, na finalidade dos laboratórios e no registro do histórico dos problemas ocorridos.

As normas e regulamentos geralmente são relacionados aos seguintes assuntos:

**Segurança de arquivos** – Senhas, áreas de trabalho, forma correta de desligar o equipamento, instalação de softwares com vírus ou pirateados, utilização de pen-drives, mp3 e celulares, uso de CDs e DVDs, que também podem trazer vírus ou levar informações importantes da empresa para terceiros.



Alimentos e líquidos não devem ficar próximos ao computador.

**Vida útil dos equipamentos** – Comer e beber no ambiente (isso não deve ser permitido para evitar insetos, fungos e umidade); quebra de equipamentos por descuido, impaciência ou brincadeiras inconvenientes; troca ou reparo de periféricos defeituosos (devem ser solicitados ao pessoal responsável pela manutenção e jamais serem feitos pelos usuários do laboratório de informática).

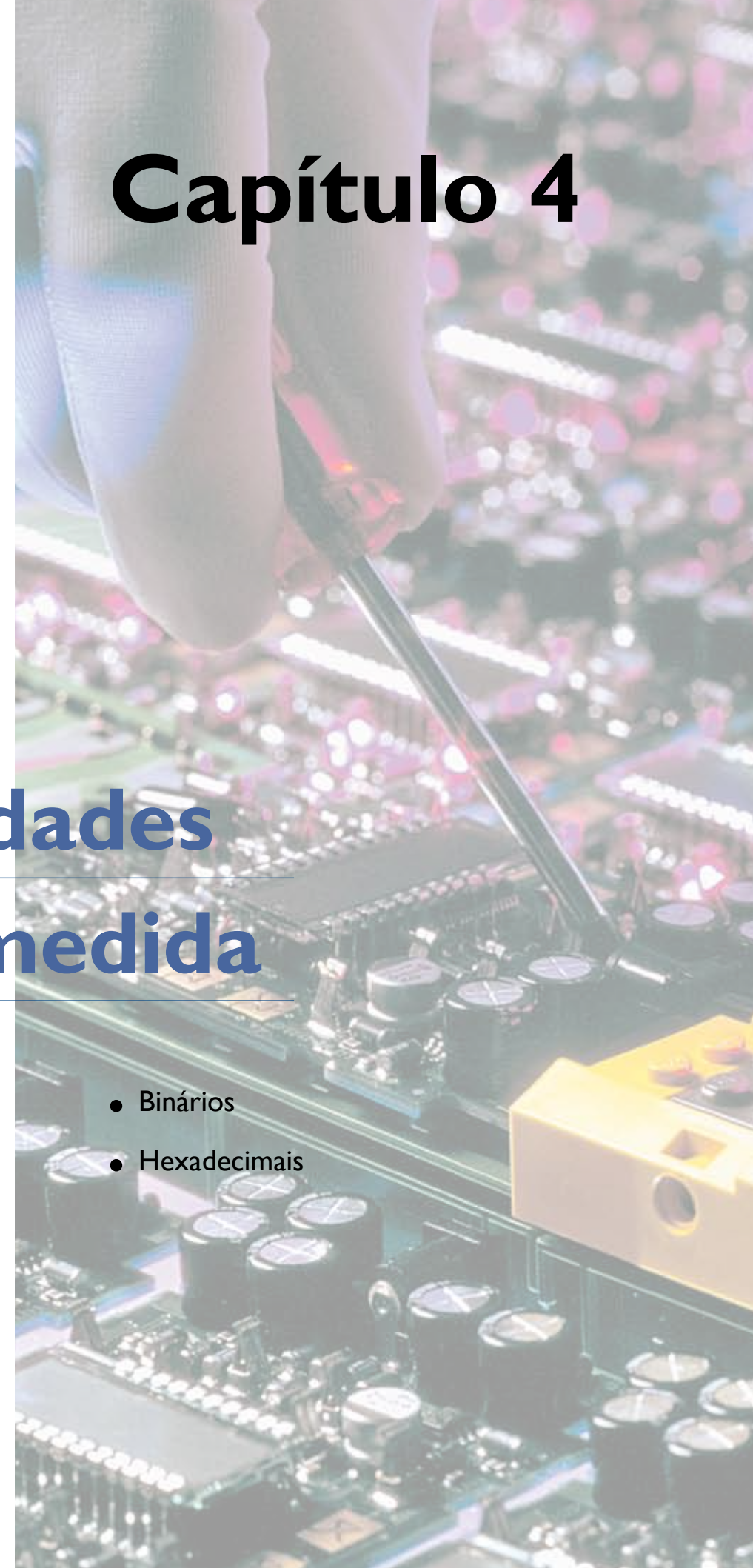
**Ambiente de trabalho** – Som alto e não autorizado, uso da internet para acesso a conteúdo ilícito, antiético e antiestético, que pode causar situações constrangedoras aos demais usuários.



# Capítulo 4

## Unidades de medida

- Binários
- Hexadecimais



Para representar o mundo real utilizamos unidades de medida. Para medir o tempo empregamos horas. Para medir pequenas distâncias, metros, e mais longas, quilômetros. Para medir volume de líquidos, recorreremos a litros, etc. Em computadores utilizamos bits para medir o tamanho das informações. Isso é importante, por exemplo, quando precisamos saber quantas músicas caberão no CD, qual é o espaço livre no HD ou ainda se a foto é muito grande para ser enviada por e-mail.

O bit é a menor porção de informação possível em informática. Um único bit representa somente duas informações, 0 ou 1, parecendo pouco em relação a outros formatos como o decimal, em que 1 dígito pode representar 10 valores diferentes, de 0 a 9. Mas essa representação é inerente à maneira como as informações podem ser escritas e lidas pelo computador. No início, utilizavam-se cartões de papel para armazenar informações (veja figura 11 e o quadro *Informática do século 19*). Um furo em determinada posição do papel representava a informação 1. Ausência de furos significava 0. Essa mesma lógica pode ser utilizada depois nos computadores digitais, que utilizam sinais elétricos de tensões diferentes, baixa e alta, para identificar o valor 0 e 1. Mídias magnéticas podem armazenar essas informações substituindo o furo do cartão por um ponto que pode ser ou não magnetizado.

4.1. Binários

Aprendemos a enxergar o mundo em forma decimal, e portanto temos dificuldade para compreender e nos comunicar utilizando a forma binária. Já imaginou alguém dizendo que sua idade é 1111? É o mesmo que 15, em formato decimal. Portanto, precisamos compreender como ler um número binário e transformá-lo em decimal para conhecer o valor da informação.

Quando aparece sozinho, o número 0 vale 0 em decimal e também em binário, assim como o número 1, que vale 1 em ambos os sistemas. Mas o binário 10 não vale 10 em decimal, e sim 2. O número vai aumentando à medida que se coloca mais dígitos à esquerda, como no formato decimal, em que, conforme aumentamos uma casa, o número cresce na base de 10. Por exemplo: o número 1 na primeira casa mais à direita vale 1 mesmo, mas se estiver na segunda casa, vale 10, na terceira, 100 e assim por diante. O sistema binário funciona na base 2 – o dígito mais à direita vale no máximo 1,

da segunda vale 2 (10), da terceira vale 4 (100). Ou seja: para converter um binário em decimal, multiplicamos dígito a dígito pela base 2 elevando-o à potência de sua posição. Exemplo:

CÁLCULO DE BINÁRIOS		
Binario	Cálculo	Decimal
0	$0 \times 2^0$	0
1	$1 \times 2^0$	1
10	$1 \times 2^1 + 0 \times 2^0$	2
11	$1 \times 2^1 + 1 \times 2^0$	3
100	$1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$	4
101	$1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$	5
110	$1 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$	6
111	$1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$	7

Se para converter binário em decimal utilizamos a multiplicação, para decompor decimais em binários recorreremos à divisão, que é a função inversa. E como inverso da potência é raiz quadrada, chegamos ao valor binário agregando os dígitos obtidos nos restos de divisões sucessivas pelo número 2 (base binária), a partir do último resultado até o da primeira divisão. Acompanhe na figura 12.

Informática no século 19

A origem dos cartões perfurados remonta aos Estados Unidos do final do século 19 e à criação da gigante da informática IBM. A técnica foi concebida por Herman Hollerith, nascido em 1860, que partiu do princípio de comando de teares automáticos. Em 1880, Hollerith trabalhava no National Census Office, que fazia pesquisas demográficas e levava 10 anos para tabular as informações. Naquele ano ele inventou uma máquina leitora de cartões perfurados em código binário. No início, Hollerith usou fitas de papel perfuradas divididas em campos para cada grupo da população. Depois adotou cartões para cada indivíduo. Hollerith conseguiu suas primeiras patentes em 1884 e continuou aperfeiçoando o sistema. Começou processando dados estatísticos de saúde pública e fazendo levantamentos para a administração do exército. A consolidação do empreendimento viria em 1889, quando sua empresa venceu a concorrência do United States Census Bureau para fornecer o sistema processador do censo do ano seguinte. Em 1911, a empresa de Hollerith juntou-se a outras três corporações para formar a Computing Tabulating Recording Corporation, que depois passou a se chamar IBM.

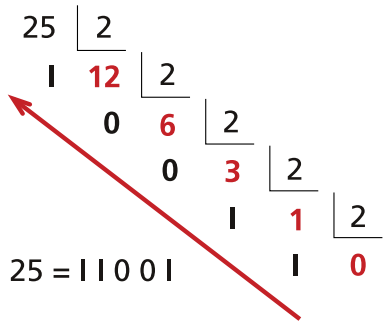


Figura 11  
Imagem de um cartão perfurado.



Figura 12

Cálculo do valor binário.



Capacidade

Não é comum usar bits para representar a capacidade de módulos de memória ou de um disco rígido: o padrão é o **byte**, também chamado de octeto. O byte é formado por 8 bits, que representam um único caractere na tabela ASCII (American Standard Code for Information Interchange – código padrão americano para troca de informações). Por isso passou a ser empregado – sabia-se que um arquivo de 50 bytes continha um texto de aproximadamente 50 letras. A ASCII é uma tabela de códigos de 8 bits que representam 128 caracteres com base no alfabeto da língua inglesa.

Múltiplos

Sempre que precisamos representar números muito grandes ou muito pequenos, costumamos utilizar múltiplos para simplificar. Por exemplo, quando queremos falar de 1000 metros, dizemos simplesmente 1 quilômetro. Essas grandezas são baseadas em uma potência. Metro é 10<sup>3</sup> de quilômetro. Ou seja, a cada número de potência temos um prefixo para identificar seu grau de simplificação.

Os números decimais levam prefixos baseados em letras gregas, chamados de greco-latinos. Veja a tabela de relacionamento abaixo:

SIMBOLOGIA DOS NÚMEROS DECIMAIS		
Prefixo	Símbolo	Fator
Exa	E	10 <sup>18</sup>
peta	P	10 <sup>15</sup>
tera	T	10 <sup>12</sup>
giga	G	10 <sup>9</sup>
mega	M	10 <sup>6</sup>
quilo	k	10 <sup>3</sup>
hecto	h	10 <sup>2</sup>
deca	da	10
deci	d	10 <sup>-1</sup>
centi	c	10 <sup>-2</sup>

Apesar de essa notação ser baseada em números decimais (note que a base é 10<sup>x</sup>), ela costuma ser utilizada também para reproduzir grandezas binárias que são baseadas em 2. Isso para que se possa compreender melhor as quantidades que estão sendo expressas.

Existe uma notação baseada em 2 (binária), desenvolvida pela IEC (International Electrotechnical Commission ou Comissão Eletrotécnica Internacional), uma empresa Suíça, que desenvolve padrões elétricos e eletrônicos.

MÚLTIPLOS DE BYTES					
Prefixo binário (IEC)			Prefixo do SI		
Nome	Símbolo	Múltiplo	Nome	Símbolo	Múltiplo
byte	B	2 <sup>0</sup>	byte	B	10 <sup>0</sup>
kibibyte(quilobyte)	KiB	2 <sup>10</sup>	kilobyte	kB	10 <sup>3</sup>
mebibyte(megabyte)	MiB	2 <sup>20</sup>	megabyte	MB	10 <sup>6</sup>
gibibyte (gigabyte)	GiB	2 <sup>30</sup>	gigabyte	GB	10 <sup>9</sup>
tebibyte(terabyte)	TiB	2 <sup>40</sup>	terabyte	TB	10 <sup>12</sup>
pebibyte(petabyte)	PiB	2 <sup>50</sup>	petabyte	PB	10 <sup>15</sup>
exbibyte(exabyte)	EiB	2 <sup>60</sup>	exabyte	EB	10 <sup>18</sup>
zebibyte(zettabyte)	EiB	2 <sup>70</sup>	zettabyte	ZB	10 <sup>21</sup>
yobibyte(yottabyte)	YiB	2 <sup>80</sup>	yottabyte	YB	10 <sup>24</sup>

4.1.1. Hexadecimais

A base hexadecimal foi adotada para facilitar a representação de números binários. Os dígitos hexadecimais vão de 0 a F (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D e F) e podem representar os números por meio de menor quantidade de dígitos.

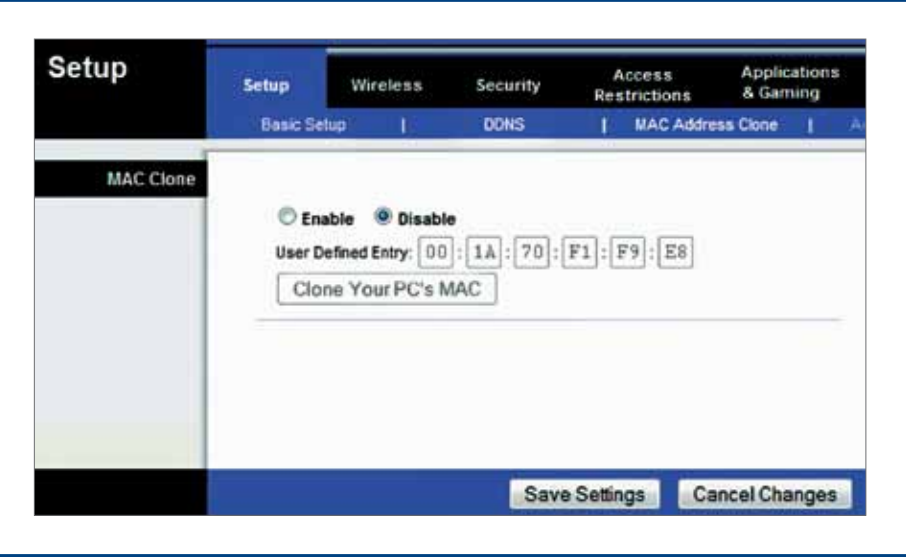
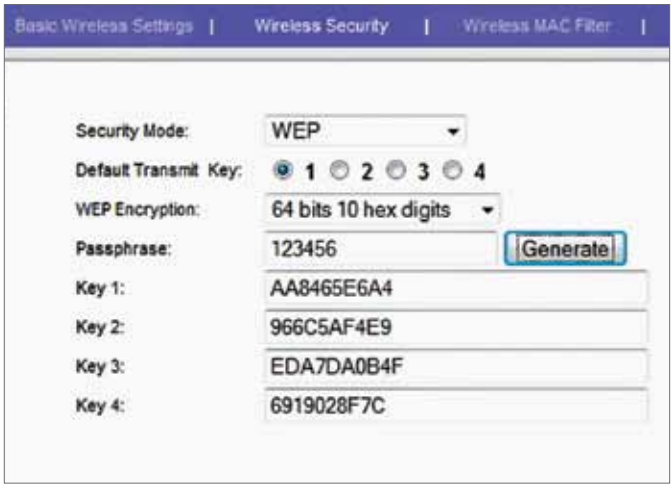


Figura 13

Tela administrativa de um roteador – Endereços MAC.

Figura 14

Definição de senhas de rede sem fio.



Por exemplo: o número binário 111110101000 em hexadecimal é representado por FA8, e equivale a 4008 em decimal. Cada dígito hexadecimal sempre representa 4 bits. Para diferenciar a representação de um número decimal de um binário, e evitar confusão, foi convencionado que os números da base 16 (hexadecimais) teriam um \$ na frente e os binários um b. Assim, podemos diferenciar, b10, \$10 e 10, que valem 2, 16 e 10, consecutivamente.

No dia a dia o técnico em informática encontrará números hexadecimais em endereços MAC de equipamentos de rede, senhas de redes sem fio (figuras 13 e 14), números de série, assinatura digital, para definir cores para componentes em vários tipos de linguagens de programação, números de IPv6 etc.

A forma de conversão de números decimais em hexadecimais é idêntica à de binários. Do mesmo modo que dividimos o número decimal por 2, em hexadecimal dividimos por 16. E vamos fazendo divisões consecutivas até que o resultado inteiro seja 0. O número hexadecimal será igual ao formado pela agregação dos restos das divisões, a partir da última para a primeira.

TABELA DE CONVERSÃO DE NÚMEROS			
Decimal	Binário	Octal	Hexadecimal
0	0	0	0
1	1	1	1
2	10	2	2
3	11	3	3
4	100	4	4
5	101	5	5
6	110	6	6
7	111	7	7

TABELA DE CONVERSÃO DE NÚMEROS			
Decimal	Binário	Octal	Hexadecimal
8	1000	10	8
9	1001	11	9
10	1010	12	A
11	1011	13	B
12	1100	14	C
13	1101	15	D
14	1110	16	E
15	1111	17	F

# Capítulo 5

## Gabinetes

- Padrões
- Formatos
- Abertura do gabinete





Apesar de não ter uma função fundamental para o computador, ou seja, sem ele o computador pode funcionar normalmente, o gabinete é de grande importância, pois organiza e fixa os seus vários componentes, como HD, CD/DVD-ROM, placa-mãe, placas de expansão com conectores externos (USB, Serial, vídeo, som, etc.), sustenta a placa-mãe e protege as placas do contato direto com pessoas, umidade, energia estática e poeira.

Além de utilidade, o gabinete tem função estética, pois muitos consumidores escolhem o computador apenas pela aparência. Geralmente, o gabinete é formado por um corpo metálico, pintado externamente com tinta eletrostática e às vezes também internamente. Tem um painel frontal para embutir leitores de mídia (DVD, CD, Floppy, cartões, fita etc.) com espaços para instalar conectores diversos (áudio, USB etc.) e entrada de ar. E um painel traseiro para placas de expansão, fonte alimentação e saída de ar.

O gabinete possui duas tampas – do lado esquerdo e do lado direito. A tampa do lado direito somente é removida se for necessário substituir a placa-mãe, pois dá acesso à chapa de suporte da placa-mãe, onde ficam os parafusos e fixadores plásticos. E, ainda no caso de ser preciso apertar ou remover os parafusos de fixação do HD ou dos leitores que ficam dos dois lados das baias. A tampa do lado esquerdo dá acesso à parte superior da placa-mãe, ao encaixe da fonte de alimentação, às baias de fixação do HD, aos drives de leitura e ventoinhas.

5.1. Padrões

Existem vários padrões no mercado. Os mais conhecidos são o AT e o ATX (o primeiro já se tornou obsoleto).

O AT (Advanced Technology) foi o padrão de gabinete utilizado nos primeiros PCs da IBM, e que, por vários problemas, foi sendo substituído pelo ATX (Advanced Technology Extended, ou seja, Tecnologia Avançada Estendida). Esse padrão, desenvolvido pela Intel em 1995, continuou sendo muito utilizado, apesar do lançamento, em 2003, pela Intel, do padrão BTX (Balanced Technology Extended, Tecnologia Balanceada Estendida). As melhorias trazidas pelo BTX em relação ao ATX estão na tentativa de padronizar placas-mãe de menor tamanho e também aumentar a refrigeração, facilitando a passagem do ar. A tendência é que este formato substitua o ATX.



Figuras 15  
Gabinetes horizontal, vertical e formato pequeno.

5.2. Formatos

Existem gabinetes em vários formatos (figura 15). São estes os mais comuns:

**Gabinetes horizontais** – São colocados sobre a mesa, com o monitor por cima. Menores que os verticais (torre), são indicados para quem tem pouco espaço. Porém, por serem menores, trazem dificuldade para os técnicos instalarem novas placas.

**Gabinetes verticais** – Mais conhecidos como torres, são encontrados em duas versões, diferenciadas pelo tamanho: torre e minitorre. Por serem pequenas, as minitorres também trazem problemas para expansão. Grandes montadoras como Dell, Positivo e IBM costumam empregar configurações padronizadas e comumente utilizam gabinetes minitorre. Já empresas que montam computadores customizados para cada cliente preferem os gabinetes maiores.

**Gabinetes SFF (Small Form Factory, ou Fabricado em Formato Pequeno)** – Modelo extremamente compacto, aceita somente componentes de notebook em seu interior e não permite expansão interna de placas, a não ser pelas portas de conexão externas, na maioria somente USB. Recomendado para quem não tem muito espaço, mas prefere usar tela, teclado e mouse de desktop, em vez de ter um notebook.

5.3. Abertura do gabinete

Antes de começarmos o processo de abertura do gabinete, é bom lembrar que os equipamentos possuem garantia. Assim, caso você não seja autorizado pelo fabricante ou revendedor a abrir o gabinete, o que implica em romper seu lacre, seu cliente pode perder o direito a reposição de peças por defeito de fabricação. Lembre também que as chapas do gabinete são bem finas e tenha cuidado para não se machucar ao manipulá-las.

DICA  
Além dos formatos mais conhecidos, em alguns modelos novos de computador a CPU é integrada ao monitor, formando uma peça única.

Figura 16

Abertura de gabinete:  
parafusos na porta trazeira.



EDUARDO POZELLA

DICA

Em alguns modelos  
novos, é possível abrir  
o gabinete apenas  
desencaixando as partes.

Para abrir o gabinete, primeiramente localize, na parte traseira, os parafusos que prendem a tampa. Geralmente são dois ou três. Remova-os com uma chave Philips (figura 16).

Procure por algum botão ou chave para desprender a tampa (não são comuns mas existem). Em seguida, force a tampa fazendo-a deslizar para trás, de modo que os encaixes se desprendam do gabinete.

Agora você já tem acesso à placa-mãe e a todos os outros componentes internos.

No processo contrário, de fechar a tampa, primeiro posicione-a de forma que os encaixes fiquem dentro de seus respectivos sulcos. Quando a tampa estiver encaixada, force-a para frente, fechando o gabinete por completo. Os parafusos servirão apenas para garantir que a tampa não se soltará posteriormente (figura 17).

Figura 17

Parafusos que  
acompanham gabinete  
ou placa-mãe.



EDUARDO POZELLA

Figura 18

Exemplo de placa  
de fixação de placa-mãe.



EDUARDO POZELLA

No caso de instalação ou remoção de uma placa-mãe, saiba que este componente é fixado em uma chapa que se solta totalmente do gabinete. Para retirá-la, force-a de maneira que deslize em seu suporte. Pode ser que haja também algum parafuso prendendo-a – neste caso, remova-o.

Coloque a placa-mãe sobre a chapa de fixação, localize seus furos que coincidem com a chapa e parafuse, usando chave de fenda Philips – os parafusos, sextavados, macho e fêmea (figura 18), são fornecidos com os dispositivos. Utilizam-se arruelas para ajudar na fixação e também para evitar o contato dos parafusos com trilhas de circuito impressas na superfície da placa, bem como danos a essa superfície pelo atrito com o parafuso ao ser girado.

Os espaçadores são mais comuns em placas mais novas. A fixação deles deve ser primeiro nos furos coincidentes da chapa de suporte da placa-mãe, e por fim a placa-mãe pode ser fixada na extremidade desses espaçadores que ficarão aparentes na superfície da chapa de fixação. Para identificar se uma chapa necessita de espaçador ou parafusos, verificamos se a chapa é lisa, sem regiões abauladas (“estufadas”). Quando a placa é lisa no lugar dos encaixes, utilizamos espaçadores plásticos e do contrário serão parafusos sextavados, parafusos de fixação, porcas e arruelas

Sobrarão vários furos da chapa sem correspondência na placa-mãe: não tem problema, servem para compatibilizar o gabinete com outros tipos de placa-mãe.



# Capítulo 6

## Fonte de alimentação

- Instalação



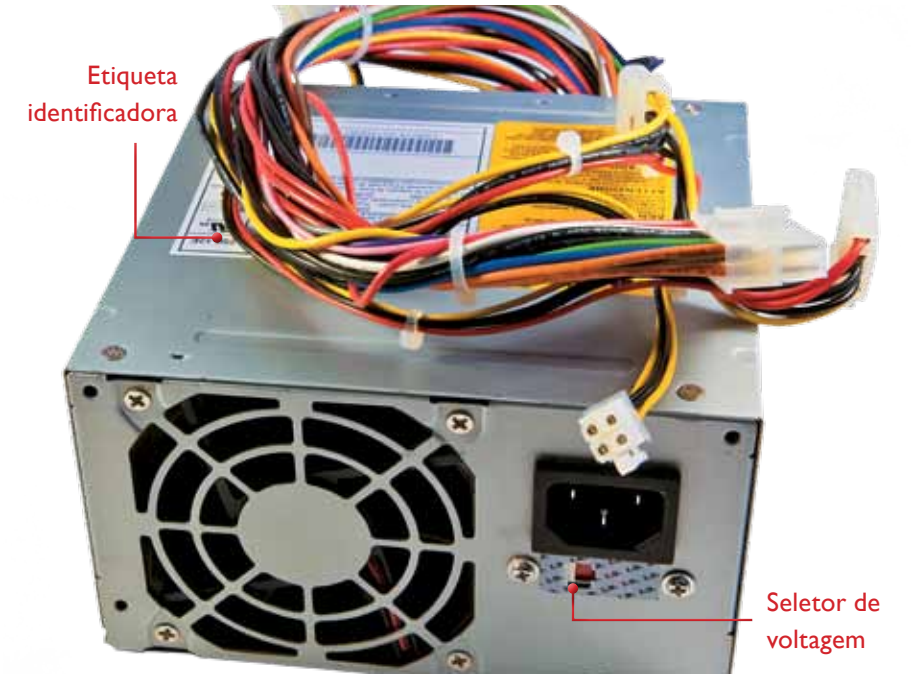
A função da fonte de alimentação é transformar a energia elétrica que vem da rede através do cabo de força, preparando-a para que chegue aos componentes do computador de forma adequada. A fonte de alimentação converte a energia elétrica de Corrente Alternada (CA) para Corrente Contínua (CC) e transforma a tensão de 110 a 240v para 12v, 3,3v, 4,5v e 5v.

Antes de ligar uma fonte na tomada devemos verificar o seletor de voltagem, que se encontra próximo ao conector do cabo de força. Algumas fontes não têm chave seletora de voltagem. Isso pode indicar que são automáticas, bivolt ou autorange e se adequarão sozinhas à voltagem conectada.

Porém, nem sempre uma fonte sem chave seletora de tensão é automática. Pode ser que trabalhe somente em uma tensão. Para ter certeza, verifique a etiqueta do dispositivo, como a da figura 19.

Figura 19

Fonte de alimentação:  
antes de ligar a máquina,  
verifique a voltagem.



Veja, na tabela a seguir, em que dispositivos se ligam os cabos da fonte.

Formato do conector	Quantidade de pinos	Dispositivo
	20 ou 24 pinos	Placa-mãe: conector principal.
	4 pinos – ATX12v	Processador: o conector fica na placa-mãe, bem próximo ao processador.
	8 pinos – EPS12v	Processador: esse modelo pode ser encontrado em substituição ao de 4 pinos. Caso a fonte não tenha esse plug, você poderá juntar 2 conectores de 4 pinos.
	6/8 pinos – PEG	Conector de expansão da placa de vídeo.
	15 pinos	HDs e Discos Ópticos Serial ATA (SATA). Caso não tenha pinos deste tipo suficientes para ligar todos os seus dispositivos SATA, você pode usar adaptadores para converter outros cabos.
	4 pinos	Conectada a periféricos como: HD IDE, discos ópticos IDE, iluminação entre outros.
	4 pinos	Liga o drive de disquete.



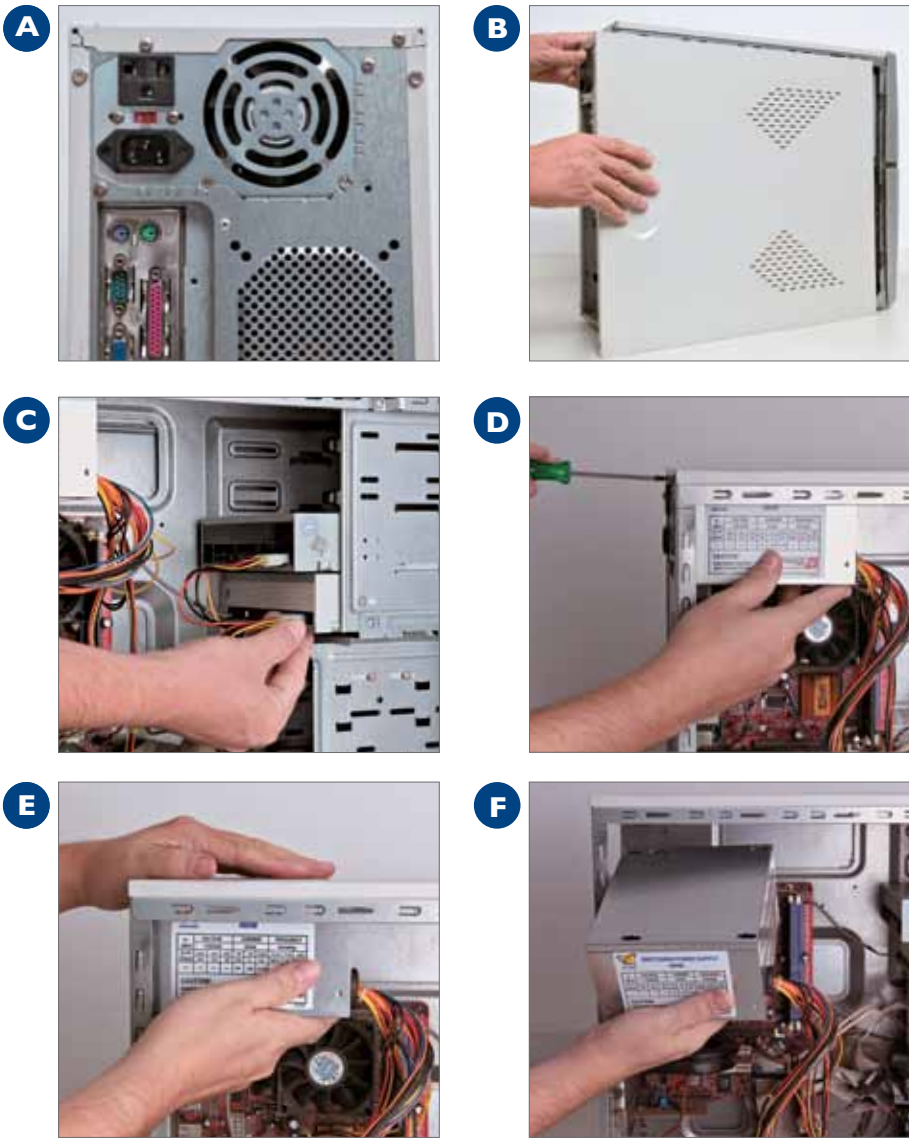
6.1. Instalação

Caso tenha de substituir uma fonte de alimentação elétrica antiga, primeiro remova-a seguindo os passos da figura 20.

Removendo a fonte antiga:

- A. Desligue o cabo de energia.
- B. Remova a tampa que dá acesso ao interior do micro.
- C. Desconecte todos os conectores fixados na placa-mãe, no HD, nos drives, na placa de vídeo etc.
- D. Posicione o micro com a parte de trás voltada para você e retire os 6 parafusos de fixação da fonte com uma chave Philips.
- E. Empurre a fonte para a frente, soltando-a dos encaixes de pressão.
- F. Retire a fonte de dentro do gabinete.

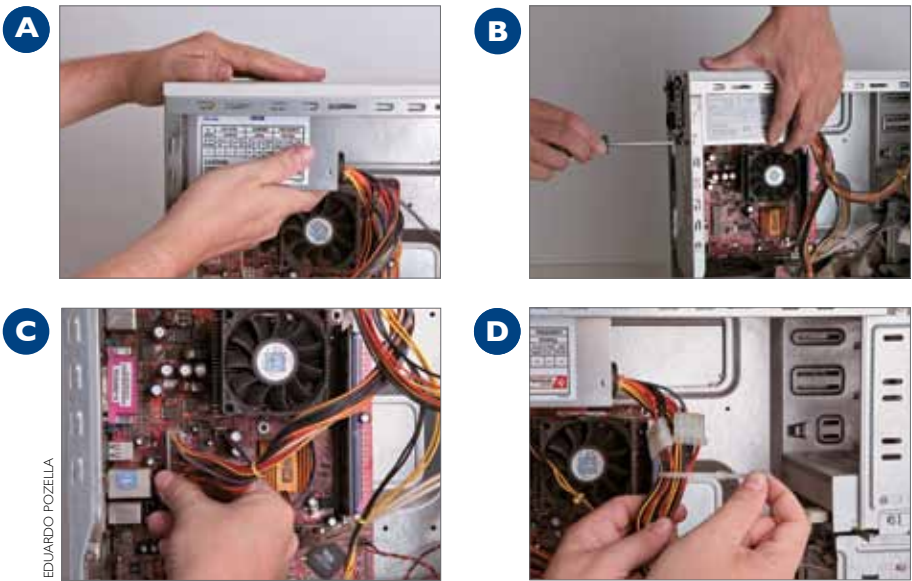
**Figura 20**  
Passo a passo da remoção da fonte.



Instalando a nova fonte:

Siga os passos da figura 21.

- A. Introduza a nova fonte no gabinete procurando pelos lugares dos encaixes. Verifique se estão todos bem encaixados.
- B. Fixe os 4 parafusos da fonte atrás do gabinete. Observe que eles não fixam as tampas laterais.
- C. Encaixe os conectores de alimentação nos devidos dispositivos e na placa-mãe (procure deixar os cabos o menos esticados possível, e sem contato com nenhuma ventoinha). Se for o caso, utilize fita adesiva para juntar os cabos.
- D. Procure juntar os cabos que sobram por meio de fita adesiva, lacres, fios encapados, de preferência fixadores, que podem vir com a fonte. Você pode enfiá-los em alguma baia que tenha sobrado no gabinete. O importante é deixar o interior do gabinete o mais arejado possível.



**Figura 21**  
Passo a passo da instalação da fonte.

Energia na medida certa

Na hora da compra de um computador novo, é muito importante calcular a potência de que precisaremos. Um computador com alimentação insuficiente pode travar, reiniciar subitamente, causar badblocks em discos rígidos, ou nem mesmo ligar. Já uma fonte com potência muito acima do necessário irá consumir mais energia. Existem fontes de potências variadas, de 350w a 1200 watts, programas que medem o uso de energia pelo computador e outros que ajudam a dimensionar a fonte necessária. O site <http://extreme.outervision.com/psucalculator.jsp> fornece uma calculadora de suprimento de energia. Outra opção é pesquisar em sites de busca o termo Power Supply Calculator.

# Capítulo 7

## Placa-mãe

---

- Conectores
- Dispositivos da placa-mãe
- Conceito de barramentos (BUS)



Todos os componentes do computador são ligados ou integrados a uma placa de circuito impresso, que pode ser encontrada ainda em outros tipos de sistemas eletrônicos complexos. Essa é denominada placa-mãe, conhecida também como motherboard, mainboard ou, nos computadores da Apple, como logic board (placa lógica). Em sites e fóruns da internet, você pode encontrar ainda a abreviação “mobo” para designá-las. Os grandes computadores de antigamente utilizavam fios para conectar as placas umas às outras. Com o passar do tempo os fios e pinos foram substituídos por placas de circuito impresso. Durante as décadas de 1980 e 1990, para baratear o preço do computador, incluiu-se dentro do circuito das placas-mãe o suporte para dispositivos de baixa velocidade, como teclado, mouse, drive de disquete, portas seriais e paralelas. E no final dos anos 1990 já estavam agregadas funcionalidades como áudio, vídeo, armazenamento e rede, sem necessidade de placas de expansão. Ainda se utilizam placas adicionais ligadas à placa-mãe, apenas quando há necessidade de aumentar o desempenho. Exemplos são as placas de vídeo para estação de jogos ou funcionalidades específicas, como áudio profissional, recepção de TV, PABX entre várias outras possibilidades.

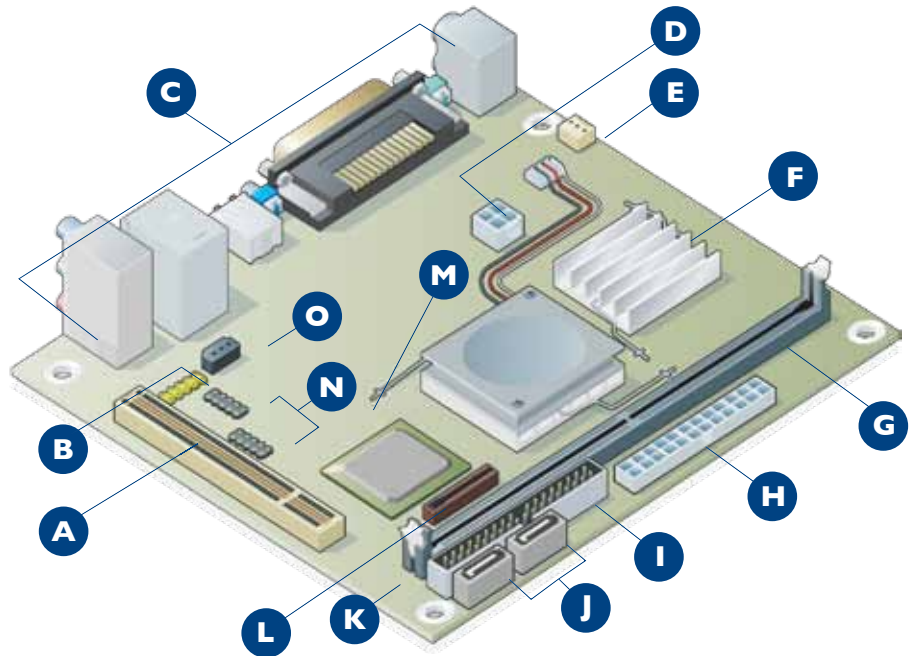
**Figura 22**  
Placa-mãe MSI-P55  
GD65 para  
os processadores  
Intel Lynnfield.



7.1. Conectores

Nas placas-mãe dos computadores há conectores para encaixe dos dispositivos, cabos e placas que irão constituir a máquina como um todo. Esses conectores seguem padrões, de modo que os fornecedores de dispositivos e de placas-mãe podem fabricar produtos compatíveis, permitindo, assim, que se montem máquinas nas mais variadas configurações. Veremos a seguir (figura 23) uma análise do funcionamento das tecnologias desses conectores e aprenderemos a fazer o encaixe correto de cada um dos diversos tipos.

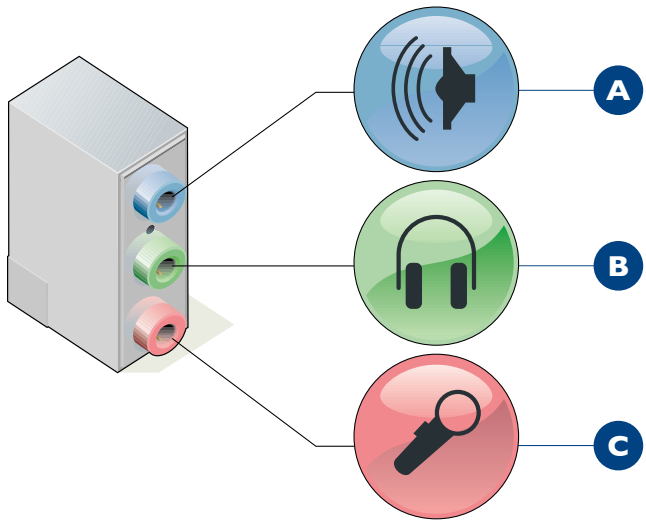
**Figura 23**  
Esquema de  
uma placa-mãe.



- A PCI-Bus: slot de expansão
- B Conectores para ligar o áudio frontal do gabinete
- C Conectores do painel traseiro
- D Conector de energia do processador (12v)
- E Conector da ventoinha traseira
- F Processador
- G Conector das memórias
- H Conector de energia principal
- I Conector de disco rígido IDE
- J Conector de disco rígido serial ATA
- K Conector do painel frontal
- L Bateria
- M Jumper de configuração da BIOS
- N Conector de interfaces USB
- O Conector S/PDIF

As placas atuais trazem os controladores de vários dispositivos, como teclado, mouse, portas de comunicação paralela e serial, vídeo e áudio. Assim, não é preciso adquirir placas adicionais para incluir essas funcionalidades. Os conectores desses dispositivos ficam aparentes no painel traseiro do gabinete.

**Figura 24**  
Conectores  
de áudio.



7.1.1. Conector de áudio

O áudio utiliza conectores do tipo P2 Stereo. A saída de áudio indicada na figura 24 pela letra B, de cor verde, é para fone de ouvido e não tem amplificação. Para ouvir o áudio em alto-falantes, será necessário usar amplificadores, como caixas de som amplificadas, potências ou aparelhos de som.

O conector A na figura, de cor azul, é para entrada de áudio (Line-in). Nessa entrada é possível ligar outros equipamentos sonoros, como telefones celulares, mp3, mp4, aparelhos de som convencionais etc.; e ouvir o som pelo computador.

O conector C, de cor rosa, é a entrada para o microfone. Ao contrário do conector de entrada de linha (Line-in Azul, letra A na figura 24), este não suporta

pré-amplificação e pode queimar se for conectado a um mp3, por exemplo, com volume médio para alto. Já se o microfone for ligado na entrada de linha, o máximo que pode acontecer é o som ficar muito baixo.

Alguns gabinetes têm conectores de áudio também no painel frontal. Nesse caso os conectores P2 já vêm acoplados ao painel frontal do gabinete, e são ligados à placa-mãe por um cabo com um conector. O encaixe na placa-mãe é indicado na figura 23 pela letra B.

Os conectores das placas-mãe mais novas utilizam o padrão Intel® HD Audio e os das mais antigas, o “Audio Codec ’97” (AC’97). Se o padrão do gabinete for diferente do padrão da placa, é possível ligar cabos de Áudio frontais do tipo AC97 em placas compatíveis com HD Áudio.

7.1.2. Conector do fax-modem on-board

As placas mais novas não vêm com esse conector porque o uso de internet discada se tornou praticamente obsoleto. Nas placas mais antigas é possível encontrar esse conector próximo ao conector de rede. Caso seja preciso utilizar um modem discado, pode-se conectar uma placa específica em um dos slots de expansão (figura 25).

**Figura 25**  
Placa de expansão  
fax-modem.



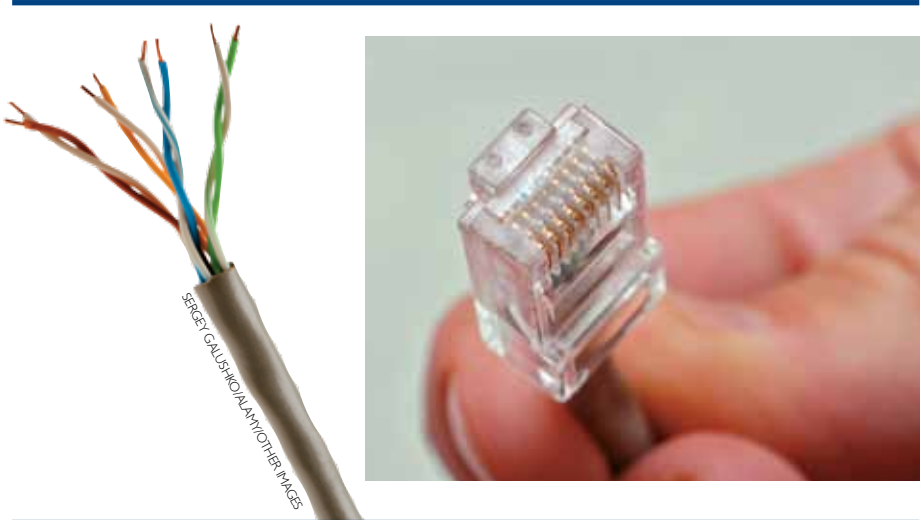
TABELA DE PINAGEM HD ÁUDIO

Pino	Sinal	Descrição
1	PORT 1L	Porta analógica 1 – canal esquerdo (microfone)
2	GND	Terra
3	PORT 1R	Porta analógica 1 – canal direito (microfone)
4	PRESENCE	Sinaliza à BIOS que um dispositivo HD Audio está conectado
5	PORT 2R	Porta analógica 2 – canal direito (fone de ouvido)
6	SENSE1_RETURN	Retorno do detector de plug no painel frontal (conector 1)
7	SENSE_SEND	Detector de inserção de plug no painel frontal
8	KEY	No pin
9	PORT 2L	Porta analógica 2 (fone de ouvido)
10	SENSE2_RETURN	Detector de inserção de plug no painel frontal (conector 2)



**Figura 26**

Cabo de rede par trançado com conector RJ45.



7.1.3. Conector de rede on-board

O conector de rede serve para conectar o cabo de rede, que geralmente se liga a uma rede pessoal ou corporativa, ou a um aparelho modem de banda-larga. O tipo é o RJ45, muito parecido com o conector de tomadas telefônicas, porém, é bem maior (figura 26).

7.1.4. Conector de vídeo on-board

Esse conector serve para ligar o cabo de sinal de vídeo do monitor. O padrão da maioria das placas é o VGA (Video Graphic Array, ou Vídeo de Gráficos Vetorizados), e os conectores são do tipo D-Sub, que é composto por três fileiras de pinos que perfazem o total de 15. Esses pinos enviam informações sobre as cores vermelha, verde e azul e também sobre a posição vertical e horizontal do ponto na tela.

7.1.5. Conector do processador

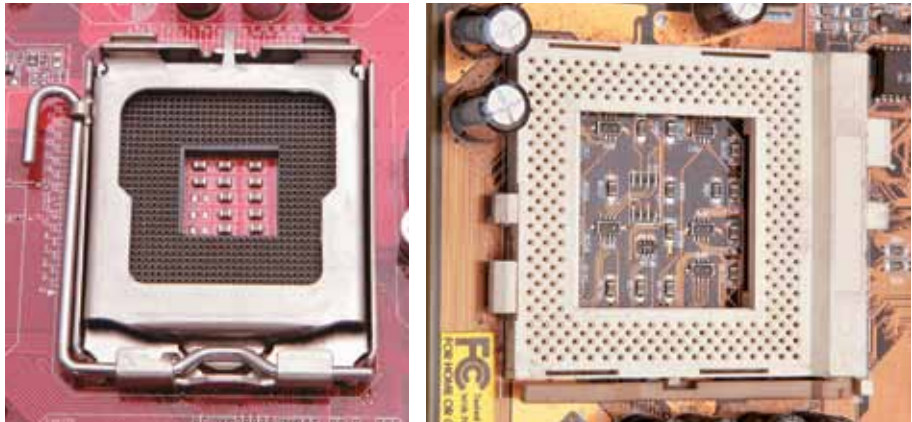
Antes de montar um processador na placa-mãe é importante verificar se os dois são compatíveis. Existem vários padrões de conectores, como soquete 478, soquete T (LGA 775), soquete B (LGA 1366) para Intel 939, 462, 754,

**Figura 27**

Soquete para processadores PPGA.

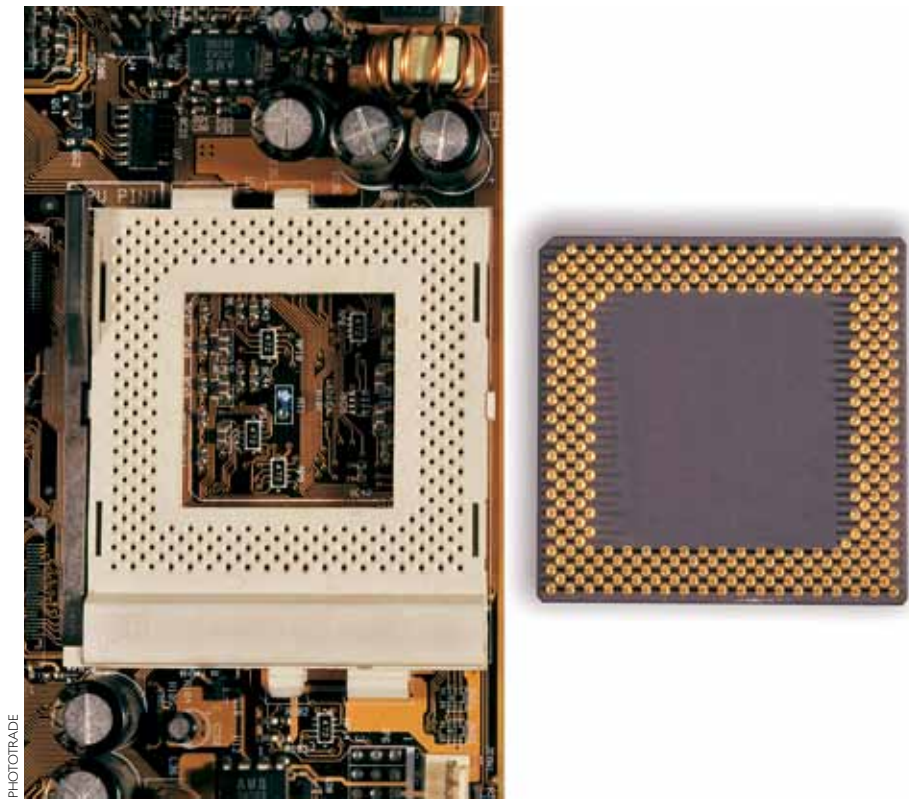
**Figura 28**

Soquete ZIF.



**Figura 29**

Placa-mãe com dois tipos de encaixe para processador; socket 370 tipo PGA-ZIF e slot (SEPP).



AM, AM2+, AM3 para AMD. Cada fabricante de processador escolhe o seu. O manual da placa-mãe informa quais processadores são compatíveis.

É possível encontrar dois tipos de encaixe para o processador: o soquete (série PGA e ZIF) (figuras 27, 28 e 29) e o slot para SEPP, SECC e SECC2.

Vamos ver agora como montar um processador de soquete. O primeiro passo é liberar a trava, uma haste que fica ao lado do conector. Pressione-a com cuidado, de modo que não desça tanto a ponto de encostar nos circuitos da placa, mas sinta que a destravou. Levante a trava e a movimente até o fim, sem forçar.

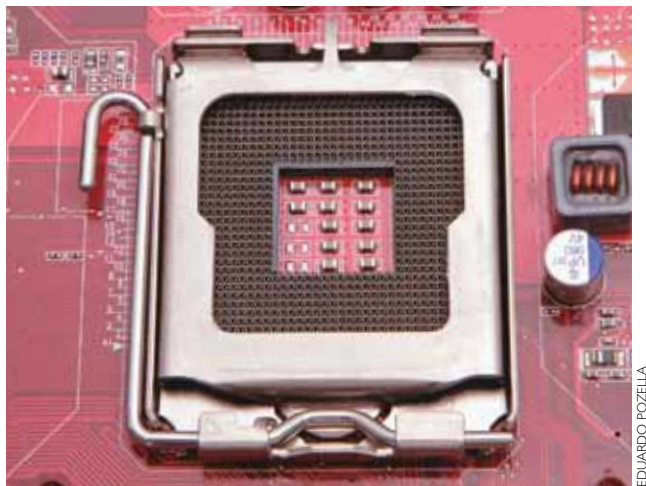
Alguns modelos de placas, como os das figuras 30 e 31, também possuem tampa, mas o procedimento para iniciar a montagem é o mesmo, ou seja, é preciso apertar, destravar e movimentar a placa até o final.

Se houver ainda uma tampa PnP sobre o soquete, retire-a com cuidado, para não tocar na placa-mãe. Os pinos do processador têm lugar certo para serem conectados. É preciso prestar atenção no processador e na placa para identificar o lado correto de encaixar o processador. Alguns processadores têm um dos lados marcados com uma seta ou uma ranhura de encaixe e/ou um lado com pinos a menos na extremidade.

Veja que no processador existe um lado marcado, que deve ser posicionado na hora de encaixar, devendo ficar na mesma posição da marca do soquete da placa (figuras 32 e 33 a e b).



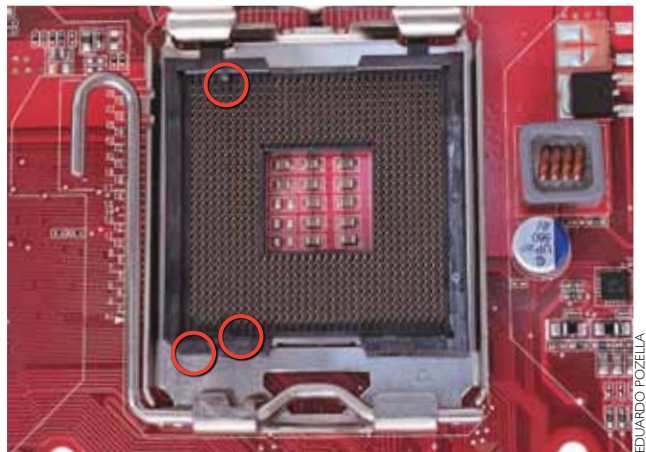
**Figura 30**  
Modelo de soquete.



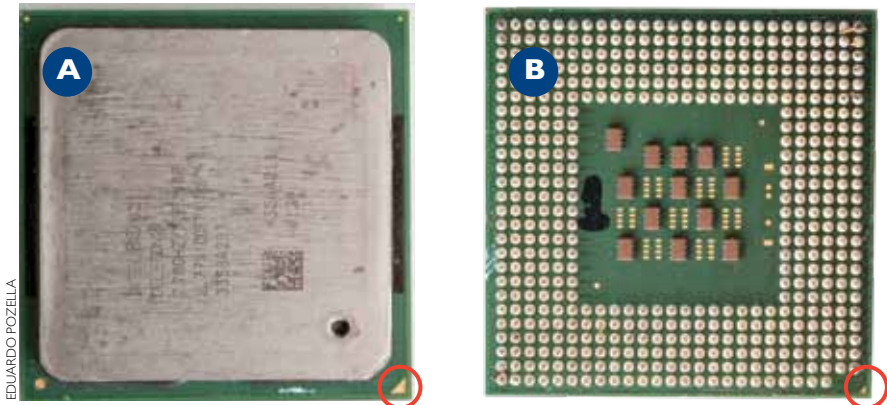
**Figura 31**  
Modelo de soquete com seta para encaixe do processador.



**Figura 32**  
Soquete com marcação de posicionamento para encaixe do processador.



**Figura 33 a e b**  
Processador com marcação de posicionamento para encaixe no soquete.



Veja também que na outra parte de um processador existem vários pinos dourados, que fazem a comunicação com a placa-mãe. É preciso, portanto, ter o máximo cuidado com esses pinos: não devemos tocá-los e precisamos de muita cautela ao conectá-los para não correremos o risco de entortar nenhum. Isso prejudicaria o encaixe, ou até poderia danificar o processador. Note que faltam alguns pinos no processador. Essa posição deverá casar com a posição onde faltam os encaixes na placa-mãe (figura 34).

Posicione o processador com cuidado sobre o soquete e verifique se o encaixe está correto. Se estiver tudo certo, pressione o processador para baixo, forçando o encaixe. Fique atento: caso o processador não desça para o encaixe sob uma leve pressão, pode ser que ainda não esteja bem posicionado. Não force. Retire, verifique a posição dos pinos e tente novamente.

Com o processador totalmente encaixado, feche a tampa do soquete e pressione levemente para travar. Da mesma forma, volte a alavanca de trava para a posição original e pressione com cuidado para travar (figura 35).

**Figura 34**  
O encaixe requer muito cuidado.





**Figura 35**  
Processador encaixado.

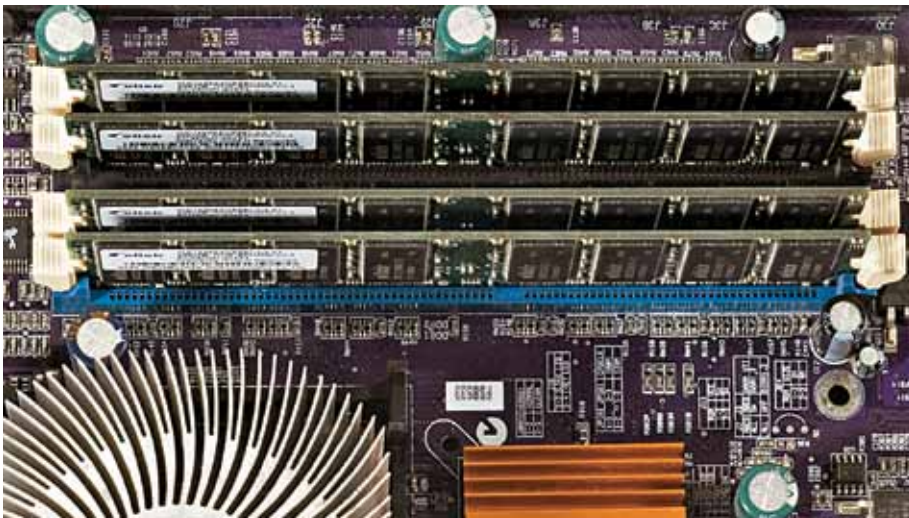


7.1.6. Conector de memória

Esse conector é ligado à memória RAM, tema que abordaremos mais adiante. Seu formato de encaixe muda conforme a tecnologia com a qual a placa-mãe é compatível. No esquema da placa exibida no início deste capítulo, o slot de memória está representado pela letra G (figura 23, na pág. 63).

Instalar uma placa de memória em um computador é uma tarefa simples, pois é praticamente impossível conectar memórias incompatíveis com a placa-mãe, já que cada tecnologia sugere um formato diferente de conectores. Elas podem diferir em tamanho, na quantidade de vias (figuras 36 e 37) ou até mesmo em sutis deslocamentos na posição do entalhe que fica entre os contatos (figura 38). Porém sempre requerem cuidados, como não colocar a mão nos conectores para evitar oxidação, o que resultaria em mau contato, e ter atenção para não forçar mais do que o necessário, evitando, assim, risco de danos ao conector e mesmo à própria placa-mãe.

**Figura 36**  
Slots de memórias de uma placa de servidor.

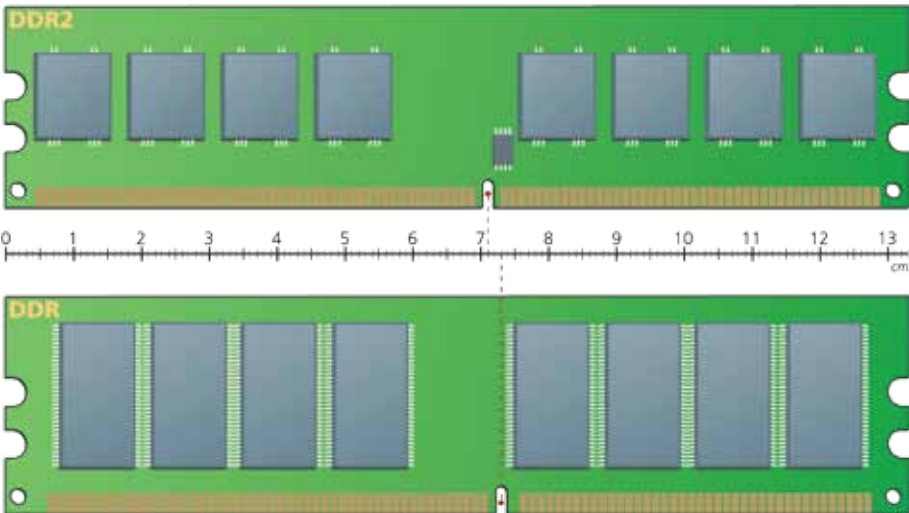


**Figura 37**  
Slot de memória de uma placa-mãe de laptop.

Para que a memória fique bem firme, esse conector é dotado de travas que se prendem nas extremidades da placa de memória. Os passos para instalar ou desinstalar uma placa são os seguintes:

- 1. Retire a placa de memória da embalagem, evitando tocar nos contatos ou em qualquer outra parte metálica.
- 2. Com o computador totalmente desligado e o gabinete aberto, de forma que se tenha acesso à parte superior da placa-mãe, localize o conector da memória e afaste as travas, deixando o caminho livre para você descer com a memória através do guia, como na figura 39.

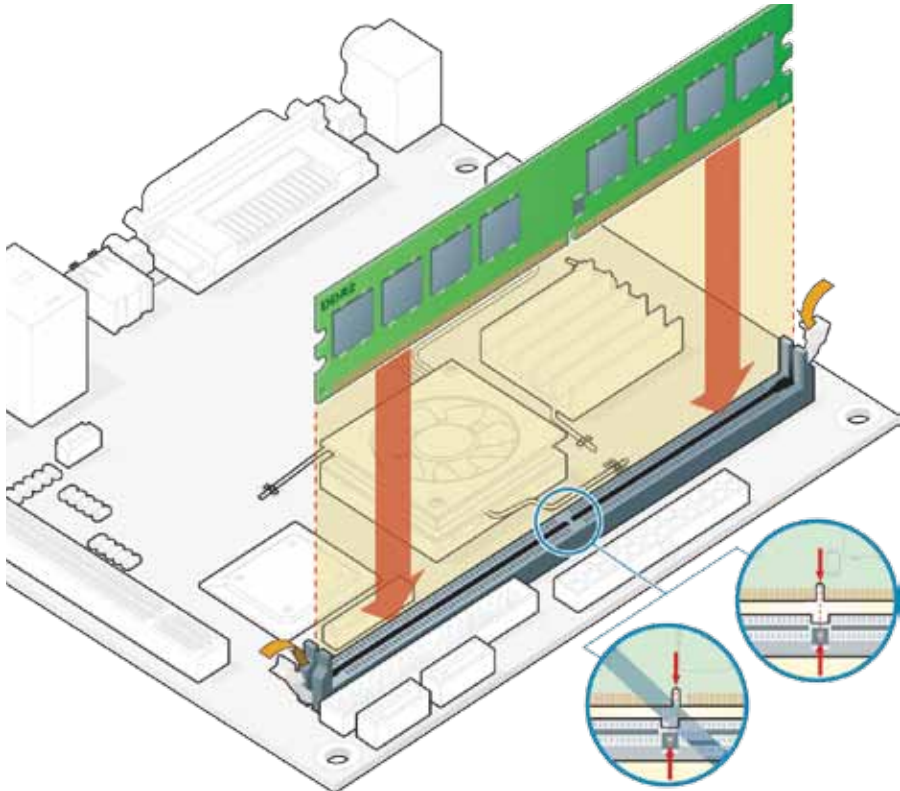
**Figura 38**  
Comparação do formato da placa de memória DDR e DDR2.





**Figura 39**

Montagem de uma placa de memória.



- 3. Em um primeiro momento, encaixe levemente a memória sem forçar. Verifique se está bem posicionada, bem encaixada nas guias do conector e com o entalhe posicionado corretamente.
- 4. Agora aperte com firmeza, mas com força moderada, para que o pente de memória encaixe no conector até o fim, de modo que as travas se fechem totalmente. Confira-as e as aperte, para que fiquem ajustadas por completo.

7.1.7. Conector porta serial

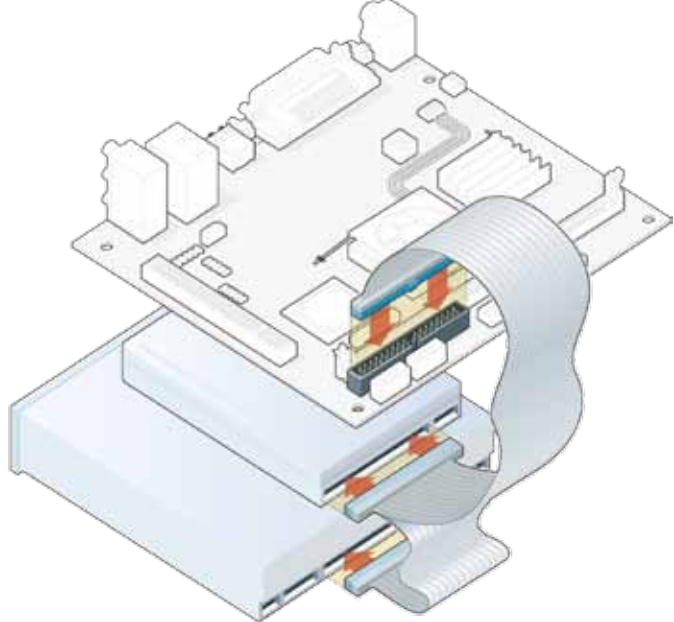
A porta serial foi muito utilizada no passado para conectar mouse, impressora, leitores de código de barras e outros dispositivos de automação, comercial e industrial. Da mesma forma que todas as outras tecnologias de transmissão por cabo, esse dispositivo tem dado lugar às conexões USB e está se tornando obsoleto. Sua velocidade máxima, de 115 kbps, é definida pela especificação RS-232 e pode se comunicar com cabos de até 8 metros.

7.1.8. Conectores IDE ou PATA

Nas placas-mãe encontramos dois conectores do tipo IDE, ou PATA, como é chamado atualmente, depois da popularização do formato Serial ATA. Neles podemos ligar até quatro discos rígidos por meio de cabos tipo fitas flat (figura 40). Cada flat possui dois conectores que se ligam aos drives de disco rígido e ópticos. Verifique, quando for instalar, que o conector do cabo flat tem uma ranhura em um dos lados e por isso só se encaixa da forma correta; ou seja, se não encaixar, não force, você poderá estar montando do lado errado.

**Figura 40**

Conexão de discos rígidos e ópticos IDE (PATA).



7.1.9. Conectores SATA

Cada conector Serial ATA tem capacidade de ligar somente um disco rígido. A conexão é simples: um lado do cabo é ligado em qualquer conector SATA da placa (A) e outro no conector do disco rígido (B), como na figura 41. A quantidade de portas SATA varia de uma placa-mãe para outra. O exemplo da figura é de placa com dois conectores.

**Figura 41**

Conexão do HD Serial ATA na placa-mãe.

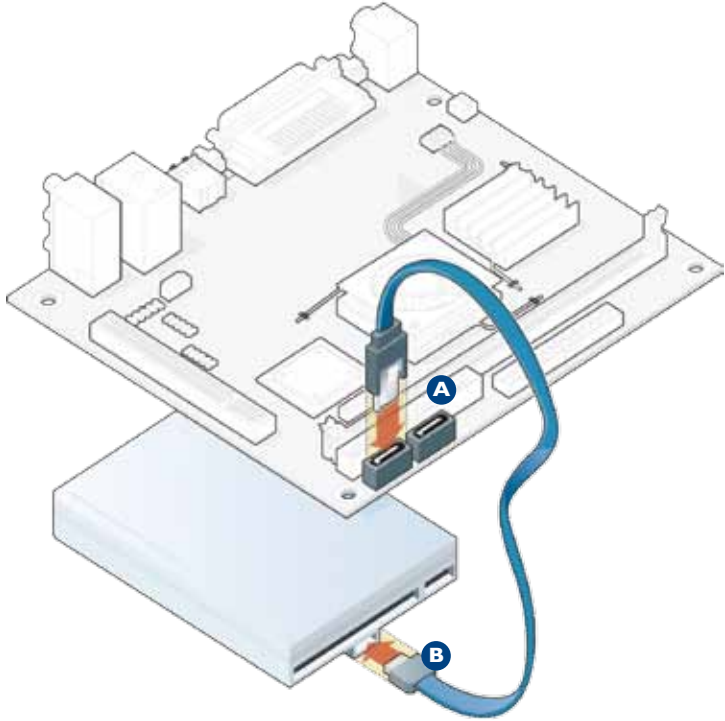
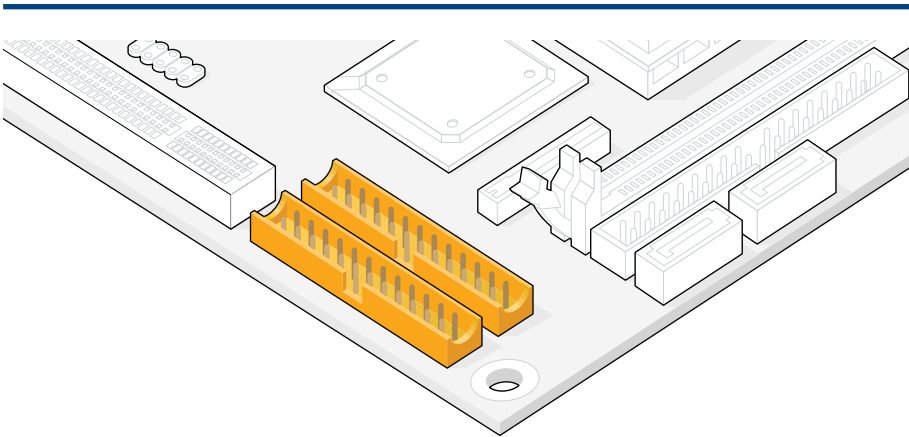




Figura 42

Conector de cabo flat do drive de disquete.



7.1.10. Conector floppy-disk (disquete)

O conector de disquete, ou floppy-disk, é bem parecido com o conector IDE do disco rígido. A diferença é o tamanho, menor, pois seu flat-cable é de 24 pinos apenas. Veja isso pela imagem do seu conector na figura 42. O drive de disquete está aos poucos sendo substituído por outras mídias, como CDs e DVDs regraváveis e cartões flash ou pen-drives.

7.1.11. Conector de alimentação

A fonte de energia alimenta a placa-mãe com uma tensão de 12v, por meio de um conector grande, o conector de energia principal, que geralmente tem 20 ou 24 pinos. Mesmo com dois tamanhos diferentes, os conectores são compatíveis. Ou seja, cabos de fontes de 24 pinos podem ser conectados em placas-mãe de 20 pinos, ou vice-versa. As placas com 24 pinos são do tipo ATX12v 2.x, e as com 20 pinos podem ser do tipo ATX12V 1.0 ou ATX (figura 43).

Figura 43

Conectores de energia da placa-mãe.

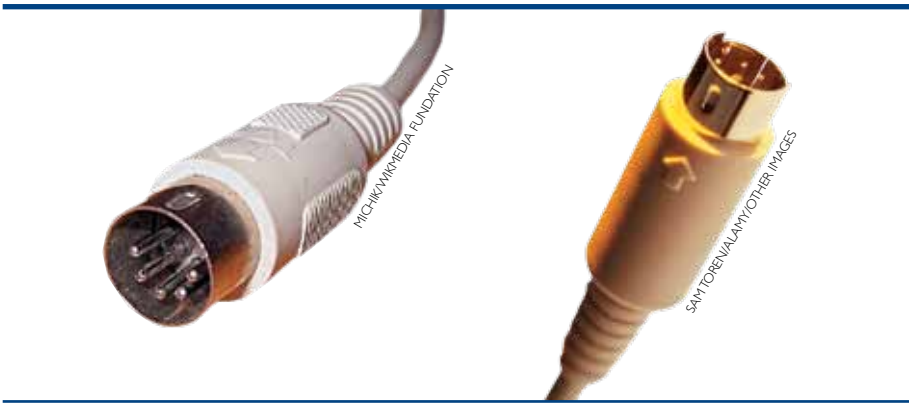
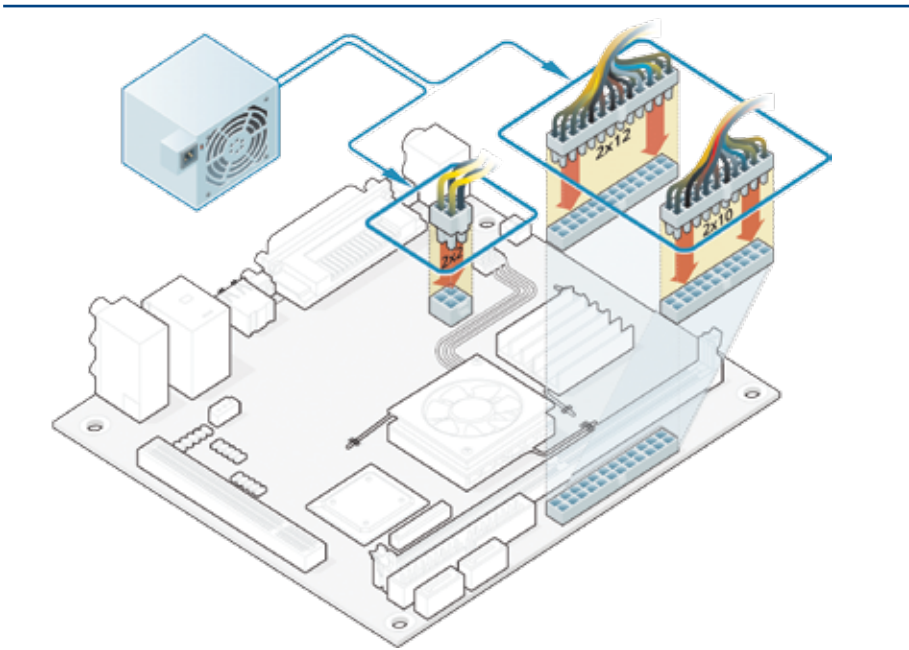


Figura 44

Conectores DIN e PS/2.

IMPORTANTE

Ainda existem máquinas antigas ou teclados e leitores de código de barras com conectores DIN. Assim, pode ser que em alguma ocasião você tenha de ligar teclado com placa-mãe de conectores diferentes. Para isso existem adaptadores que podem fazer a interconexão dos dispositivos, de DIN para PS/2 e vice-versa.

Em algumas placas é possível encontrar um conector adicional de quatro pinos que, segundo manuais de algumas placas-mãe de fabricantes, como a Intel, serve para alimentar diretamente o processador. Com isso, a CPU tem um canal de energia dedicado somente a ela, portanto estável. Sem ter que compartilhar essa energia com nenhuma outro dispositivo da placa-mãe, seu desempenho não ficará comprometido por alimentação insuficiente.

7.1.12. Conector de teclado

O conector rosa, encontrado no painel traseiro da unidade de processamento, é o conector do teclado. O teclado é um periférico utilizado para usuário se comunicar com o computador; é um dispositivo de entrada de dados. Ele possui teclas que representam cada uma das letras do alfabeto, números, símbolos e ainda botões especiais que têm funções específicas para determinados programas e sistemas operacionais. Como exemplo de teclas especiais temos o conjunto de teclas de funções F1 a F12, que estão na primeira fileira de teclas do dispositivo. Quando pressionadas, as teclas emitem um sinal elétrico que é enviado a um chip que controla o teclado. O chip identifica qual tecla foi pressionada e envia, por meio do cabo, ou por sinal de rádio (sem fio, wireless), o código da tecla pressionada. Essa operação irá causar uma interrupção no processador, avisando que uma tecla foi pressionada.

O padrão mais comum em computadores hoje em dia é o PS/2, mas também podem ser encontrados teclados USB e o modelo DIN, já ultrapassado (figura 44).

7.1.13. Conector de impressora

A **porta paralela** foi largamente utilizada para ligar dispositivos a computadores, principalmente impressoras. O modelo foi empregado nos primeiros PCs da IBM como o padrão de conexão de impressoras, mas com o tempo vem sendo substituído por portas USB. A porta paralela também é muito utilizada para a

A transmissão em paralelo de bits é feita simultaneamente por meio de várias vias. Assim, a tecnologia elevou a velocidade de transmissão de dados em relação à comunicação serial, que era de apenas 115 Kbits, para, inicialmente, 1.2 Megabytes por segundo. Mas perde de longe para a velocidade atingida pelas portas USB, que trabalham na faixa de 12 Megabytes por segundo.

ART DIRECTORS TRIP/ALAMY/OTHER IMAGES



Figura 45

Conector fêmea no padrão DB25 para transmissão em paralelo.

Figura 46

Cabo DB25 de impressora.



TONGRO IMAGE STOCK/ALAMY/OTHER IMAGES

A sigla USB significa Universal Serial Bus e se refere a uma tecnologia que veio para facilitar a ligação de maior número de aparelhos ao PC, como câmeras, joysticks, mp3 players, leitores de cartões (inclusive simultaneamente), bem como para acelerar ainda mais a velocidade da transmissão de dados.

comunicação entre dispositivos específicos, como scanners e unidades de discos externos, e ainda para coleta de dados e controle de equipamentos de automação industrial e comercial (figura 45). Os cabos utilizados para ligar impressoras na porta paralela são do tipo DB25 (figura 46).

7.1.14. Conector de mouse

Do lado do conector do teclado, e no mesmo formato, com o mesmo padrão PS/2, encontramos o conector do mouse, na cor verde. Quanto aos mouses, estão disponíveis nos dois formatos de conectores, PS/2 e USB. Normalmente os mouses com interface PS/2 são mais baratos, embora os dois tenham a mesma qualidade. A única vantagem dos mouses com barramento USB é que podem ser ligados em aparelhos sem porta PS/2, como laptops por exemplo, ou no caso de queima da porta de mouse do microcomputador.

7.1.15. Conector USB

No painel traseiro as placas-mãe costumam trazer várias portas USB. Podemos encontrar outras portas desse tipo no painel frontal e às vezes até em outras partes do gabinete, ao lado e em cima. E a tendência é que sejam incluídas cada vez mais portas USB, porque esse tipo de conexão, amplamente utilizado, tornou-se padrão para todos os novos periféricos. Dispositivos que antes tinham o próprio padrão de conector, como teclado, mouse, impressoras etc., migraram para o formato USB (simbolizado na figura 47).

Figura 47

Porta USB e símbolo do padrão USB.



EDITORIAL IMAGE, LLC/ALAMY/OTHER IMAGES

Figura 48

Conectores firewire.



BUSSE YANKUSHEV/LATINSTOCK

LATINSTOCK

A tecnologia firewire foi concebida pela Apple Computer em meados dos anos 1990. Utilizada por algum tempo pelo iPod, permitia carregar uma música para o aparelho em segundos. O formato não é aberto, e a Apple cobra royalties dos fabricantes que a empregam em seus aparelhos. Por isso a conexão só é encontrada em dispositivos com real necessidade de transmissão de dados em alta velocidade.

7.1.16. Conector Firewire

A porta Firewire (figura 48) é a principal concorrente da USB na padronização de dispositivos. Pode-se perceber que nessa briga a USB vem ganhando de longe, mas alguns dispositivos, como câmeras digitais, sistemas de áudio profissional ou outros que necessitam de transmissão de dados em alta velocidade, já utilizam o barramento **firewire**, cuja velocidade chega a ser até quase 30 vezes superior à alcançada pelo padrão USB.

7.1.17. Conectores de expansão

Uma das características das placas-mãe é a capacidade de permitir a expansão das funcionalidades do computador, ou até a implantação de funcionalidades mais eficientes em relação às que já integra.

Desde os primeiros modelos, os PCs da IBM traziam placas-mãe com vários slots de expansão, pois a empresa já supunha que outros fabricantes desenvolveriam mais equipamentos que pudessem se integrar ao computador. Para tornar viável a integração, a especificação desses barramentos foi compartilhada e vários fabricantes puderam criar placas compatíveis com os computadores da IBM.

7.1.17.1. ISA

O Industry Standard Architecture (ou Arquitetura Padrão da Indústria), mais conhecido como ISA, foi o padrão para conector de expansão utilizado pela IBM em seus primeiros computadores que possibilitou a vários fabricantes de componentes eletrônicos participarem do bom momento de entrar no mercado de computadores pessoais e desenvolverem outros tipos de equipamentos, como fax-modens, placas de vídeo entre muitos outros. Foi substituído pelo padrão PCI (Peripheral Component Interconnect – Componente de Interconexão de Periféricos). Este, inicialmente, tinha capacidade de apenas 8 bits de dados por clock, em ciclos de no máximo 8.33 MHz, e na prática dificilmente ultrapassava os 5 Mhz. Pouco tempo depois o padrão foi reformulado e ganhou mais 8 bits, passando assim a ter capacidade de 16 bits. Mas manteve, ao mesmo tempo, a possibilidade de conectar placas no padrão de 8 bits na parte maior do slot, que tem uma divisão para indicar onde se pode encaixá-las.

Nas figuras 49 e 50 podemos comparar os slots ISA e PCI e notar como a diferença de tamanho entre os dois é saliente.



Figura 49

Placa-mãe com slots ISA (preto).



7.1.17.2. PCI

A especificação PCI (figura 50) foi desenvolvida pela Intel em 1990 para substituir os barramentos ISA e VESA Local Bus, e continua sendo utilizada em placas de vídeo, rede, áudio e fax-modems, por exemplo.

O PCI Local Bus trouxe várias melhorias. A velocidade de transferência, que na versão inicial era de 32 bits a uma frequência de 33 Mhz, chegou a 66 Mhz a partir da versão 2.1. A arquitetura também possibilitou a conexão de dispositivos menores, pois seu conector era bem menor em comparação aos do ISA e do VESA. E, ainda, proporcionou independência da velocidade do barramento local, já que o barramento PCI trabalha com a própria frequência: nos padrões anteriores, sempre que surgiam novos processadores com novas velocidades, a arquitetura do barramento tinha de ser alterada. Além disso, os periféricos antigos não funcionavam com processadores mais novos. Outra vantagem do padrão PCI é a autoconfiguração: o sistema operacional passou a reconhecer se o dispositivo está ou não presente, e a alocar os recursos necessários para o aparelho conectado.

Figura 50

Slots PCI.



Vantagens da tecnologia USB

Padronização de conexão de dispositivos – Não é necessário usar vários tipos de conectores. O dispositivo pode ser conectado a qualquer porta USB disponível.

Plug and play – O sistema operacional pode reconhecer automaticamente o dispositivo, mesmo que este demande algum driver específico. Os dispositivos mais comuns, como pen-drives, mouses e impressoras, podem ser utilizados assim que são conectados.

Alimentação elétrica – Antes, os equipamentos que se conectavam no micro necessitavam de fonte de energia própria. Na tecnologia USB, o dispositivo pode receber energia por meio do cabo de comunicação, o que permite reduzir a quantidade de cabos.

Conexão de vários dispositivos ao mesmo tempo – Cada porta USB pode conectar até 127 aparelhos diferentes ao mesmo tempo. Isso se for ligada a ela um hub USB (figura 51). Temos de lembrar, porém, que a capacidade de transferência de dados nesse caso será compartilhada entre todos os dispositivos conectados e, assim, se tornará mais lenta.

Ampla compatibilidade – O padrão USB é compatível com todos os sistemas operacionais. No Windows é compatível desde a versão 98. E vários outros aparelhos eletrônicos já possuem interface USB, entre os quais os de som automotivos e convencionais, celulares, DVDs etc.

Hot-swappable – Dispositivos USB podem ser conectados e utilizados sem que se precise reiniciar o computador. Também não é necessário desinstalar, mas apenas desconectar o dispositivo.

Cabos de até 5 metros – Os cabos de conexão USB podem ter até 5 metros, o que proporciona grande liberdade na disposição dos aparelhos. Com o aumento da quantidade dos dispositivos conectados, pode ser que falte espaço e seja necessário distribuí-los por locais mais distantes do PC. Com a utilização de dispositivos repetidores, como hubs USB, pode-se utilizar outro cabo de 5 metros, aumentando assim ainda mais a potencial distância entre o micro e o dispositivo.



Figura 51 - Hub USB.



Figura 52 - Modelo de conector A.



Algumas variações foram desenvolvidas a partir deste padrão, como o Mini PCI, utilizado em notebooks, e o PCI-X (X de eXtended), que possibilita aos dispositivos transferirem dados a 64bits e é utilizado em placas de rede Gigabit, conectores de clusters, canais de fibra óptica e conectores de discos rígidos SCSI. (Atenção: não confunda PCI-X com PCI Express).

7.1.17.3. AGP

O AGP (Accelerated Graphic Port, ou Porta Gráfica Acelerada) para as placas-mãe baseadas no Pentium II foi desenvolvido pela Intel, no início de 1997. O objetivo foi oferecer suporte para melhorias de vídeo. O AGP utiliza um barramento dedicado, impedindo a concorrência de outros dispositivos no acesso ao processador. Para propiciar o barateamento das placas 3D, o AGP recebeu capacidade de acessar diretamente a memória RAM do computador para realizar tarefas complexas com texturas, necessitando trazer menos memória de vídeo na aceleradora 3D. Essa tecnologia é chamada de DIME (Direct Memory Execute – Execução de Memória Direta). O AGP trabalhava com 32bits a 66 Mhz, mas tem capacidade de transmitir duas ou mais palavras de 32 bits a cada ciclo de clock.

Não é possível identificar em qual modo trabalha a AGP de determinada placa, pois isso depende do chipset da motherboard. A forma mais simples de descobrir é consultar o manual da placa-mãe ou o site do fabricante.

7.1.17.4 CNR e AMR

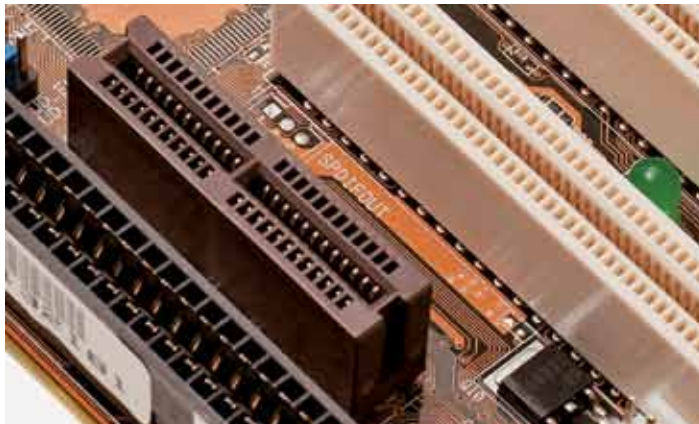
Esses dois tipos de **slots** foram desenvolvidos por fabricantes de placas-mãe que traziam áudio e modem on-board, mas optaram por deixar de embuti-los.

Isso porque esses componentes trabalham com sinais analógicos e podem causar interferência nos demais circuitos da placa, ou mesmo por questão de espaço, no caso de acomodar os conectores de placas de som de seis canais.

O AMR é um padrão aberto, desenvolvido por um consórcio de fabricantes de placas como AMD, Lucent, Motorola, 3Com, Nvidia, Texas Instruments e Via, similar ao CNR. Porém foi utilizado durante pouco tempo, em meados de 2002 e 2003.

Figura 53

Modelo de slot CNR.



MODO x TAXA DE TRANSFERÊNCIA	
Modo (Quantidade de dados por vez)	Taxa de transferência
1x	266 MBps
2x	532 MBps
4x	1 GBps
8x	2 GBps

7.1.17.5. PCI-Express

O desenvolvimento cada vez mais veloz das tecnologias 3D forçou a indústria de informática a criar barramentos também sempre mais rápidos. Para suprir essa necessidade foi criado o slot AGP que transmitia dados a 2.128 MB por segundo no padrão AGP 8x. Mas com o passar do tempo se descobriu que a tecnologia não conseguia acompanhar a evolução das aplicações, que necessitavam de cada vez mais banda, além de serem totalmente voltadas para vídeo. No início de 2001 a Intel apresentou a necessidade de se criar um novo padrão para substituir o PCI, e um consórcio entre AMD, Microsoft e IBM desenvolveu o 3GIO (3ª geração de I/O), que logo seria chamado de PCI-Express (figura 54).

A tecnologia se baseia em ler e escrever 8 bits de dados por vez, através de canais seriais que utilizam um meio de comunicação direta com o chipset, eliminando gargalos. O **PCI-Express** consegue trabalhar com taxas que chegam a 250 MB por segundo no padrão 1.0, bem maiores que os 132 do padrão PCI. No padrão 2.0 alcança até 532 MB por segundo.

Os slots podem ser encontrados normalmente nos tamanhos 1x, 4x, 8x e 16x, números que significam a quantidade de canais implementados no slot. O slot 16X da PCI-Express transmite o equivalente a 4.000 MB por segundo.

O nome PCI Express Bus sugere que o padrão seria um barramento, o que é considerado incorreto por vários especialistas, considerando-se a definição de que um barramento deve compartilhar o canal de comunicação.

Figura 54

Slots PCI Express.

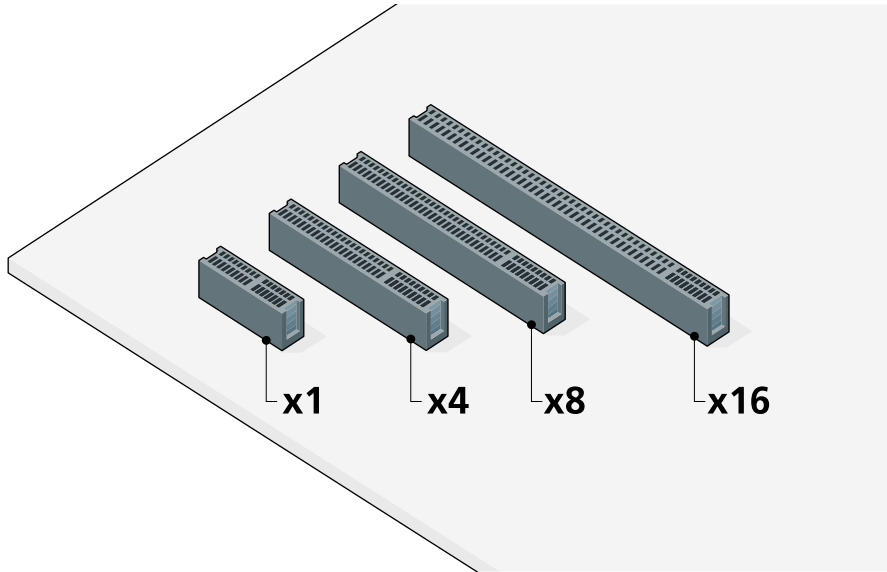


Figura 55

Chip que armazena o BIOS.



## 7.2. Dispositivos da placa-mãe

Alguns componentes da placa-mãe respondem por tarefas fundamentais para a própria placa-mãe, pois têm de integrar, controlar e configurar todos os outros componentes e periféricos.

### 7.2.1. BIOS BASIC INPUT OUTPUT SYSTEM Sistema Básico de Entrada/Saída

O BIOS é um software armazenado em um chip de memória do tipo Flash-Rom fixado na placa-mãe, do mesmo tipo encontrado em pen-drives (figura 55). Tem a função de reconhecer, configurar e iniciar os dispositivos do computador, e ainda iniciar o sistema operacional. Ao ligar o computador, os primeiros sinais que você vê na tela são da interface do BIOS.

O software firmware (programa implantado em um chip) do BIOS pode ser atualizado quando precisamos instalar um sistema operacional ou dispositivo incom-

# Tarefas do BIOS

Assim que o computador é ligado, o BIOS segue esta sequência:

- 1º Verifica a CMOS. A CMOS é outro chip responsável por armazenar configurações sobre os HDs instalados e seus tamanhos, data e hora, e várias outras informações.
- 2º Carrega os controladores de interrupção. Os controladores de interrupção, fazem a interface do sistema operacional com eventos dos dispositivos. Quando uma tecla do teclado é pressionada, por exemplo, o BIOS avisa o processador sobre qual interrupção foi acionada e este transmite a informação para o sistema operacional.
- 3º Inicializa os registradores e o controle de energia.
- 4º Testa todos os dispositivos para descobrir se estão funcionando corretamente. Essa tarefa leva o nome de POST (Power-On Self-Test ou Autotestes de Funcionamento). Quando algum dispositivo falha, impossibilitando a inicialização do sistema, o BIOS pode emitir beeps (sinais sonoros) através do alto-falante da placa. Cada fabricante pode ter um conjunto diferente de sinais para representar vários problemas.
- 5º Exibe as informações do sistema no vídeo. É a primeira informação que aparece quando o computador é ligado.
- 6º Determina os discos que podem ter sistema operacional para serem inicializados.
- 7º Inicia a sequência de Boot que irá começar o carregamento do sistema operacional. Caso o disco selecionado para boot no CMOS não contenha sistema operacional, uma mensagem será exibida na tela: Disco sem Sistema.

Figura 56

Bateria.



patível com a versão atual do BIOS. Isso pode ser necessário em máquinas antigas, mas nem sempre em placas-mãe recentes. De todo modo, deve ser feito somente em último caso, pois a falha no processo de instalação ou a implantação de uma versão incorreta pode comprometer o funcionamento da placa-mãe. O processo de upgrade do BIOS é feito por meio de um software que pode ser baixado do site do fabricante para um disquete, CD/DVD ou pen-drive inicializável. Ao ser reiniciada a máquina com a mídia utilizada selecionada para boot no CMOS Setup, o programa de atualização é carregado, apaga a versão antiga do BIOS e a substitui pela nova.

Caso o processo de instalação falhe, ou seja instalado um BIOS incorreto ou ainda este tenha sido apagado por um vírus, o chip do BIOS deverá ser substituído. Isso porque, sem um BIOS funcionando no computador, não haverá como dar boot, nem instalar um novo BIOS por meio de um programa.

### 7.2.2. Bateria

As placas trazem uma bateria, parecida com a de relógios, porém bem maior, para manter a CMOS energizada enquanto o computador estiver desligado (figura 56). Isso impede a perda de dados das configurações relativas a data e hora, configurações realizadas no setup, como configuração de dispositivos, além de informações sobre velocidade do processador, voltagem da placa, dados dos discos rígidos, entre outros. Quando recebemos a mensagem de falha de CMOS durante o boot, como "CMOS setting error", ou quando simplesmente percebemos que a data e a hora do computador se desatualizam e voltam a se referir à fabricação do BIOS, pode ser que a carga da bateria terminou. Nesse caso, deve ser substituída.

### 7.2.3. Chipsets

Placas-mãe funcionam por meio de um conjunto (set) de circuitos integrados (chips), daí o nome de chipset. Cada um desses chips tem tarefa específica, cuida de determinado tipo de função da placa, como controlar interrupções, memória e barramentos, gerar clock etc. Nos computadores antigos os circuitos integrados ficavam separados uns dos outros, cada um com a própria funcionalidade. Mas nos computadores modernos os chips foram embutidos, geralmente dentro de apenas dois chipsets, que são chamados de ponte norte e ponte sul (figura 57).

A ponte norte (northbridge) integra dispositivos de alta velocidade, como processador, memória e vídeo (AGP e PCI-Express 16x) e faz interface com o chipset da ponte sul (southbridge). Esses chips se comunicam por meio de barramento de alta velocidade. A figura 58 mostra que as ligações entre os vizinhos da northbridge são vias mais largas do que as que se ligam à southbridge, e tem transmissão mais veloz (setas em vermelho).

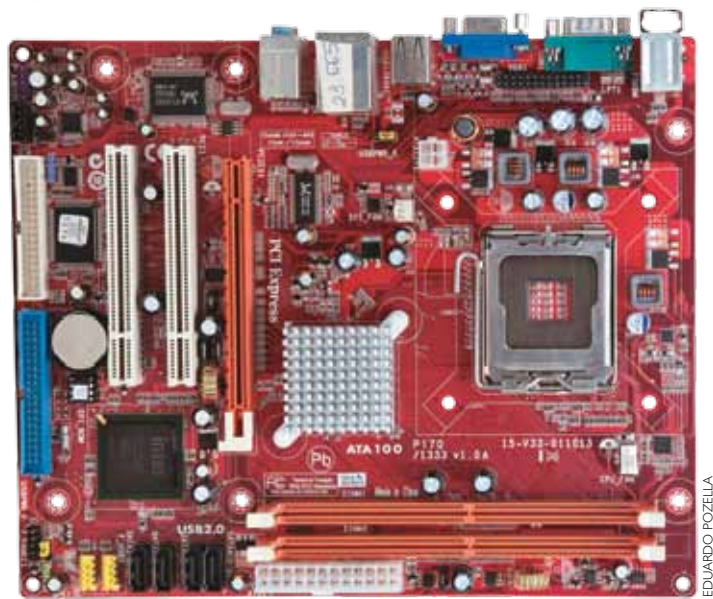
### DICA

Antes de instalar qualquer memória, é importante verificar no manual da placa-mãe detalhes de configuração e tipos permitidos.



Figura 57

Funcionalidades dos chipsets atuais em chips separados nas placas antigas.



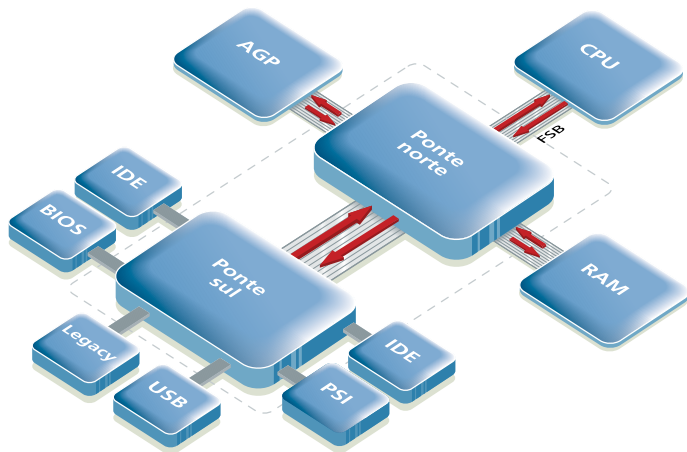
A ponte norte influencia diretamente o desempenho geral da máquina, pois contém a controladora de memória, que determina a tecnologia (DIMM, DDR ou RAMBUS), a quantidade máxima e a frequência da memória e do processador. Essa afirmação não se aplica a placas para processadores AMD K8 em diante, nos quais a controladora de memória fica no próprio processador. A estratégia da AMD permite que as placas tenham somente um chipset.

A ponte sul controla dispositivos de menor velocidade, como disco rígido, CD/DVD-ROM, USB, portas PS/2 (teclado e mouse), porta paralela e serial, barramento PCI e PCI-Express 1x. E influencia somente o desempenho desses dispositivos, até mesmo determinando a tecnologia que será possível utilizar, como USB ou USB 2.0, por exemplo, se suporta discos SATA ou PATA, quais serão suas frequências etc.

Na maioria das vezes os fabricantes de placas-mãe não são os mesmos dos chipsets. A adoção das pontes possibilitou a padronização, facilitando a criação de produtos compatíveis com os chipsets de diferentes fornecedores (figura 58).

Figura 58

Organização de chips e barramentos em placas-mãe atuais.



7.2.4. Sensores

Os sensores servem para monitorar eventuais problemas com a placa-mãe e seus dispositivos, como falhas no fornecimento de energia pela fonte e, principalmente, o superaquecimento do processador ou do HD, além da velocidade das ventoinhas. Essas informações, que podem ser visualizadas no CMOS Setup, através de softwares da placa-mãe ou de terceiros, são necessárias e podem evitar que o processador queime, desligando a máquina antes que isso aconteça.

O controle dos sensores é feito por um circuito chamado super I/O, que também controla periféricos antigos, como portas seriais e paralelas e drive de disquete.

7.2.5. Dispositivos on-board

Com a evolução das placas-mãe, os fabricantes começaram a dotá-las cada vez mais de circuitos impressos nas próprias placas, para vários tipos de aplicações. Assim, surgiram os termos on-board (na placa) e off-board (fora da placa), para descrever se um dispositivo faz parte da placa-mãe ou se será incluído à parte por meio de uma placa de expansão, específica para a tarefa.

Apesar de fazerem parte da placa-mãe, os dispositivos funcionam de modo independente para evitar que eventual defeito em um deles acarrete falhas nos demais.

Em computadores usados em escritórios, para trabalhar com planilhas, editores de texto, acesso à internet ou para ouvir música, as placas on-board são uma boa opção por serem baratas. Mas, se houver demanda por melhor desempenho de vídeo (como para jogos 3D e edição de fotos) ou áudio (como mixagem de som profissional), serão necessárias placas específicas, que trazem processadores específicos e memórias dedicadas. Os recursos on-board podem ser desligados na CMOS Setup caso sejam substituídos por equivalentes off-board.

Tenha em mente, contudo, que placa-mãe on-board indica computador de baixo custo, mas também de baixo desempenho. Dispositivos on-board, além disso, consomem processamento da CPU e espaço na memória principal do computador. Assim, máquinas com componentes off-board têm melhor desempenho de modo geral.

7.3. Conceito de barramentos (BUS)

Barramentos são circuitos integrados que fazem a transmissão física de dados de um dispositivo a outro. Esse meio de transmissão, por definição, deve ser compartilhado por vários dispositivos, como uma autoestrada que recebe veículos de várias cidades e os leva a outras, possibilitando que cada um siga a própria rota. Mas há os barramentos dedicados, concebidos para melhorar o desempenho do computador, como os que ligam a ponte sul e a ponte norte, ou o barramento FSB, que liga o processador à memória.

Os barramentos são formados por várias linhas ou canais, como se fossem fios elétricos, que transmitem sinais elétricos tratados como bits.

Há várias tecnologias padronizadas de barramentos, como ISA, MCA, VESA, PCI, VLI, AGP, DMI, HyperTransport e outros.

# Capítulo 8

## Armazenamento

- Disco rígido
- Disco flexível
- Discos ópticos



Além de processar informações, o computador é capaz também de armazená-las e recuperá-las quando for necessário. É magnífico pensar em quantas milhares de árvores foram poupadas, em todo o mundo, desde que os dados deixaram de ser armazenados em papel e passaram a ser guardados em forma de bits. Conseguimos miniaturizar a informação de qualquer tipo – visual, sonora, textual – de modo que somente a máquina pode fazer a leitura e reproduzi-la sempre que desejamos obtê-la.

Existem várias formas de armazenagem em diferentes tipos de mídia. Cada forma é otimizada em algum sentido, como custo, velocidade de leitura ou escrita, capacidade e segurança.

8.1. Disco rígido

Os discos rígidos ou HD (Hard Drive, em inglês) são dispositivos de memória não volátil (que não perdem as informações quando não estão energizados), de alta-capacidade (na verdade o de maior capacidade entre todos) e de velocidade moderada (não são tão lentos quanto unidades de fita nem tão rápidos quanto memórias RAM ou CACHE).

Apesar de as unidades externas serem comuns, o disco rígido é instalado principalmente dentro do gabinete. É utilizado em especial para armazenar arquivos do sistema operacional, programas e arquivos pessoais.

Os discos rígidos são considerados memórias secundárias, enquanto as memórias RAM e CACHE são memórias principais ou primárias, considerando-se a velocidade de acesso aos dados do processador. Quando o processador precisa de um dado ou programa, solicita-o às memórias RAM e CACHE. Caso o dado ou o programa não esteja na memória, deverá ser carregado do disco rígido para a memória, e só então o processador poderá utilizá-lo. A memória RAM fornece dados e instruções ao processador de forma muito mais rápida do que, acessando diretamente o disco rígido. Assim, pode trabalhar mais rapidamente. Certos sistemas operacionais costumam utilizar o disco rígido para armazenar o excedente quando necessitam de mais memória principal do que há, fisicamente, na máquina. No MS Windows tal possibilidade

denomina-se memória virtual. No Linux/Unix é conhecida como swap. Se isso acontece com frequência, o desempenho da máquina diminui. A solução é instalar mais memória RAM, caso isso seja possível.

O HD (figura 59) é o jeito popular de nos referirmos ao H.D.D. (Hard Disc Drive ou unidade de Disco Rígido), também conhecido como winchester, nome de uma tecnologia de fabricação antiga de discos rígidos.

Os discos rígidos são formados por uma carcaça de ferro ou alumínio hermeticamente fechada para evitar a entrada de ar, que consigo traria umidade e poeira, capazes de danificar suas partes mecânicas.

Em uma das extremidades da carcaça, encontramos os conectores de dados e controle, o jumper de configuração e os conectores de energia. Esses conectores (figura 60) são ligados à placa controladora, também chamada de placa lógica do disco (figura 61), que controla todo o funcionamento do HD.

Figura 59  
Exemplo de HD.



Figura 60  
Modelos SATA e ATA.

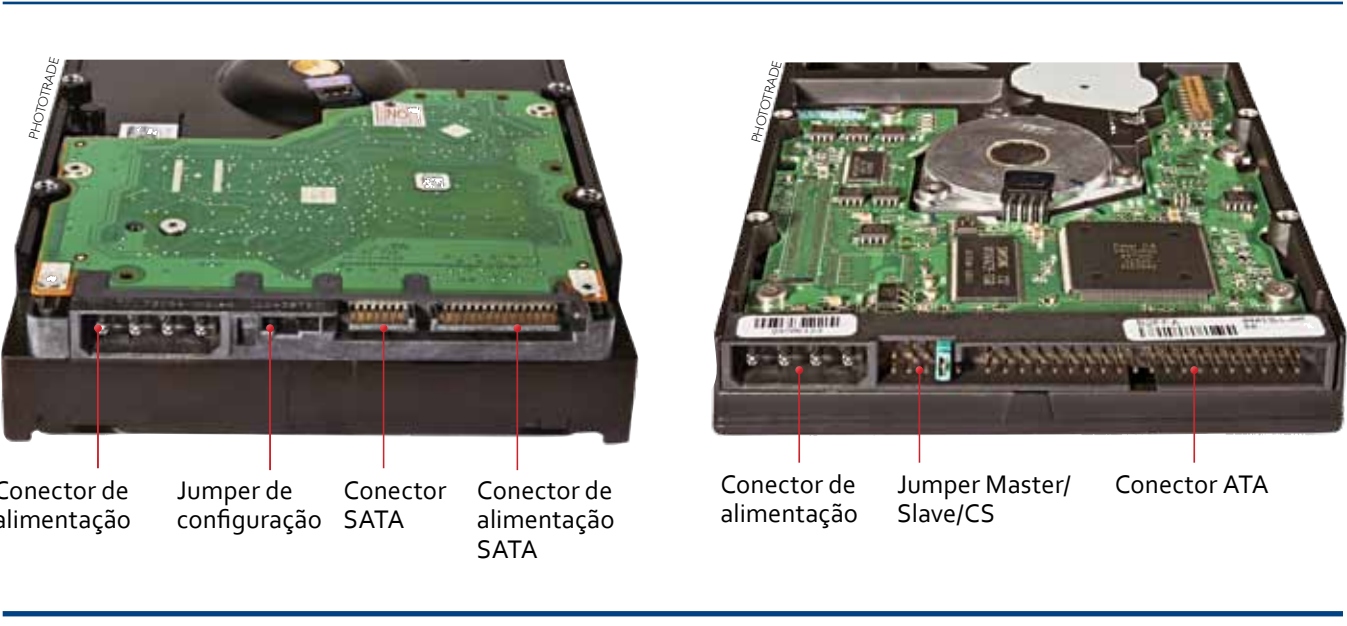
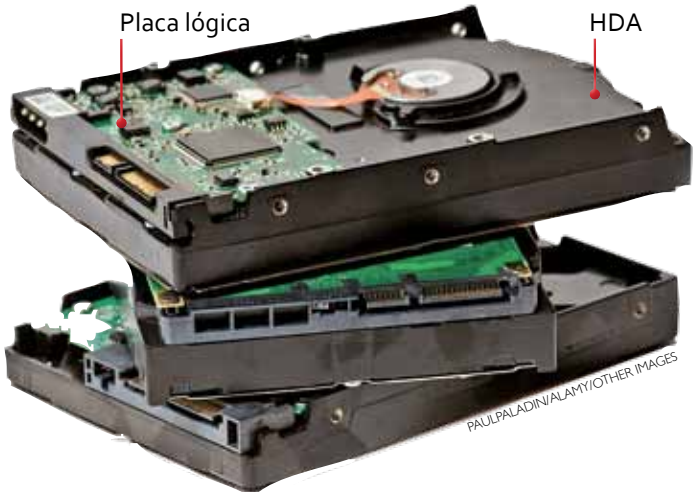


Figura 61

Placa lógica do disco.



DICA

Em situações extremas, nas quais seja necessário recuperar dados de um disco cuja placa lógica tenha sido queimada, é possível substituí-la por outra placa, de um HD idêntico, mesmo fabricante, marca, modelo e capacidade.

No interior da carcaça (figura 62) pode haver um ou mais discos metálicos sobrepostos, com superfícies cobertas por pintura magnética composta de óxido de ferro. É nesta superfície que os dados são registrados magneticamente. Esses discos giram impulsionados por um motor, a taxas que chegam hoje até 10.000 rpms (rotações por minuto).

Os dados são lidos e escritos nesses discos por meio de uma cabeça que se movimenta horizontalmente sobre a superfície, levada por um braço metálico com formato aerodinâmico. O braço metálico, movimentado pelo atuador, não toca o disco, cujo movimento produz uma bolsa de ar que o faz flutuar.

Os pontos magnéticos são organizados de forma que tenham um endereço. Assim, a placa lógica do HD consegue localizar em que disco o dado se encontra e em seguida calcular a velocidade que precisa aplicar ao disco para que sua posição esteja correta no momento em que a cabeça de leitura estiver exatamente no ponto da informação solicitada pelo processador. Um dado no disco então possui como identificação o número do disco, o setor e a trilha (figura 63).

Figura 62

Interior da carcaça.

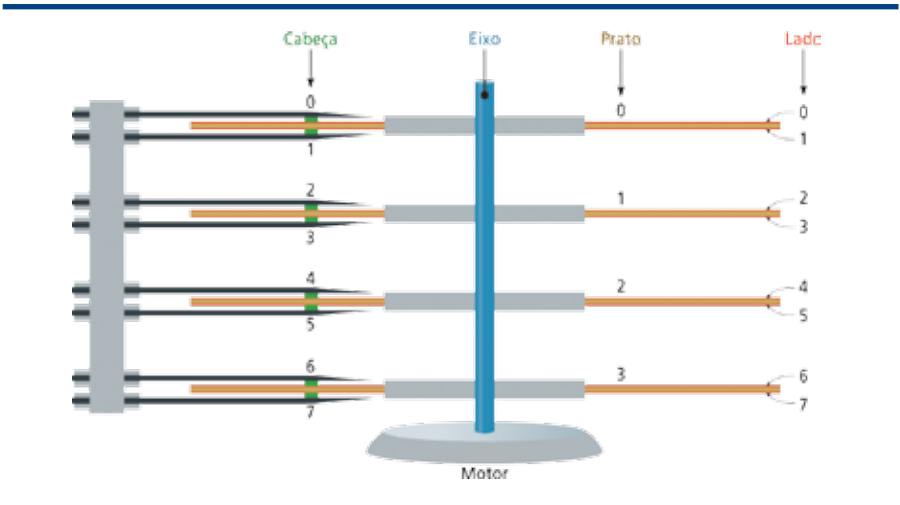
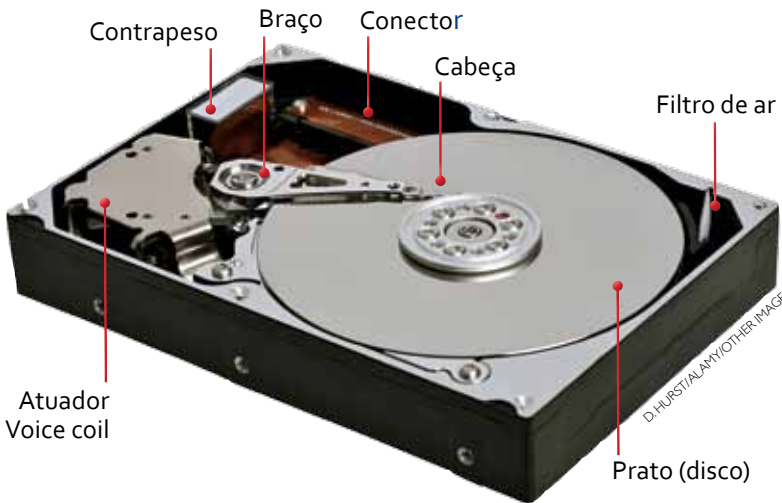


Figura 63

Os discos se movimentam todos juntos; são presos ao mesmo eixo.

As trilhas têm formato espiral e vão do centro do disco para a extremidade, fazendo um trajeto comparável ao de um disco de vinil tocado de trás para a frente. Os setores dividem as trilhas em blocos, da mesma forma como dividimos pizza (figura 64).

8.1.1. IDE, ATA ou PATA

Para serem utilizados pelo processador, os dados armazenados em discos rígidos devem ser total ou parcialmente carregados para a memória e transmitidos da memória para o disco, depois de serem alterados, ou criados. É esta a utilidade das tecnologias ATA, IDE, EIDE, FASTATA, ATAPI, Ultra-ATA, Ultra-DMA ou PATA. Passou a ser muito comum encontrar no mercado discos IDE, sendo identificados como do tipo PATA, logo que começou a popularização da tecnologia SATA (Serial ATA). PATA vem de Parallel ATA. A denominação ATA tem origem no nome do primeiro computador em que a tecnologia foi empregada, um PC/AT modelo 386, com capacidade de apenas 20 MB. Inicialmente, era chamada de PC/AT Attachmment.

O PC/AT foi lançado em 1984 pela IBM, como sucessor do modelo XT. Mas o modelo 386 só chegaria ao mercado em 1986. Criado pela Compaq, leva um chip 80386 da Intel.

Figura 64

Divisão das trilhas em bloco.

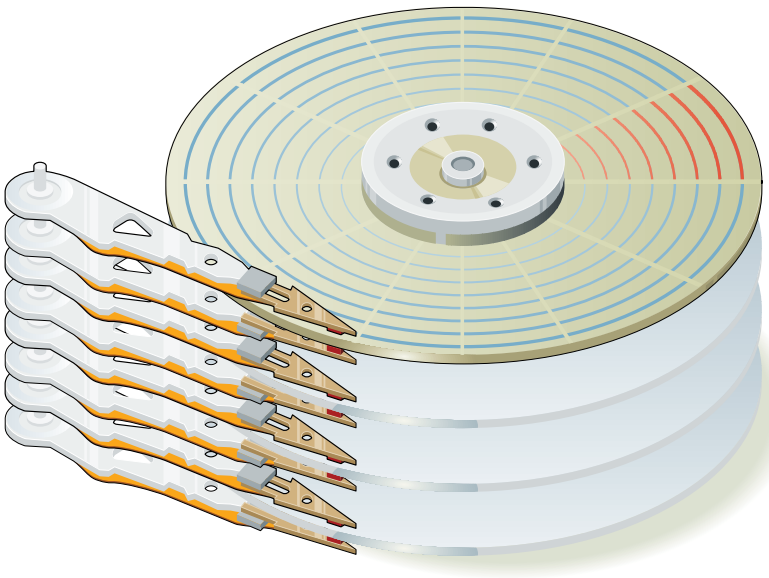
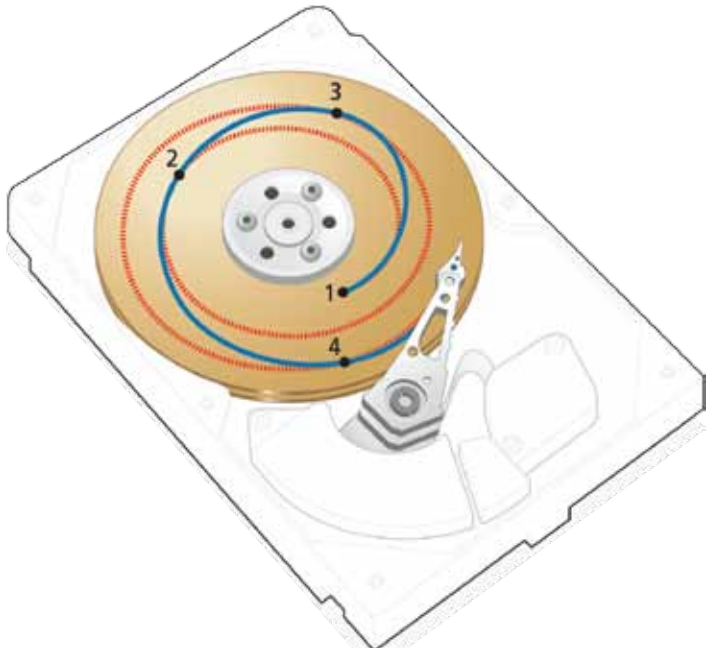




Figura 65

Sequência de leitura de dados pertencentes a dois arquivos distintos (vermelho e azul) em uma controladora SATA com NCQ.



Inicialmente, as placas que controlam o disco rígido ficavam encaixadas em slots de expansão, mas depois passaram a ser acopladas aos discos rígidos. Daí o nome IDE (Integrated Device Eletronic, que significa Eletrônica de Integração de Unidade).

A tecnologia se baseia na transmissão de dados por meio de um barramento paralelo em modo Half-duplex. Ou seja, a transmissão de leitura e escrita nesse caso é feita simultaneamente por meio de um conector (de 40 pinos). A última versão do IDE foi o ATA-7, que conseguia fazer transferências de até 133 MB/s.

8.1.2. SATA

A sucessora da tecnologia PATA é a Serial ATA, também chamada de SATA. Serial significa dizer que os bits trafegam em fila (figura 65), um após o outro, ao contrário do modo de transmissão em paralelo, que pode levar vários bits ao mesmo tempo, e nas duas direções. Durante muito tempo acreditou-se que a transmissão em paralelo fosse mais eficiente que a serial. Mas os engenheiros de computadores perceberam que era mais fácil construir circuitos mais velozes de forma serial. Isso porque o tráfego de corrente elétrica emite um campo eletromagnético que causa interferência entre as vias e corrompe os dados. Essa interferência cresce à medida que a velocidade da transmissão aumenta, o que tornou inviável a construção de discos mais velozes. Isso não acontece na transmissão serial, que tem apenas um canal de transmissão. O **SATA** pode elevar a velocidade de transmissão sem problemas e permite que se trabalhe com cabos mais compridos de até 8 metros.

8.1.3. Funcionamento

Agora que conhecemos a fisiologia de discos SATA e PATA, podemos aprender como o computador utiliza essas unidades de armazenamento, como são identificadas pelo BIOS, suas capacidades, e como os dados são organizados.

8.1.3.1. Setor de boot

O BIOS é capaz de fazer as operações iniciais no computador, identificar o hardware, contar a memória, mas não permite uma interface complexa de controle entre computador e usuário. Para isso existem os sistemas operacionais, que geralmente são gravados no disco rígido. Logo após a máquina ser ligada, o BIOS executa seus procedimentos iniciais e passa o controle do computador para o sistema operacional (Windows, Linux, Unix, MacOS, entre outros). Porém a informação de onde está o sistema operacional não fica na memória do BIOS, e sim em uma parte bem pequena do HD conhecida por setor de **boot**, MBR (Master Boot Record ou Registro Principal de Boot) ou trilha zero. O termo trilha zero vem do fato de o boot ser gravado na primeira trilha do sistema de arquivos do HD.

O setor de boot pode estar em um disco rígido como também em um disquete, um disco óptico (CD/DVD) ou até mesmo em um pen-drive ou cartão flash. Essa opção deverá ser configurada no software CMOS Setup do BIOS. Geralmente utilizamos outras mídias como boot quando algo danifica o setor de boot do HD ou quando o sistema operacional ainda não foi instalado no disco rígido. Podemos utilizar os discos de instalação do Windows ou do Linux para corrigir ou instalar o setor de boot (figura 66) pela primeira vez.

É possível instalar mais de um sistema operacional e iniciá-los a partir do mesmo setor de boot, mas neste caso é preciso utilizar um gerenciador de boot, como por exemplo o LILO ou GRUB do Linux.

Algumas falhas no sistema de arquivos ou mesmo a desinstalação de um outro sistema operacional instalado em outra partição podem remover ou danificar o setor de boot, impedindo o sistema operacional de voltar a iniciar. Nessas situações, recorreremos, no caso do Windows Vista, ao CD de instalação:

- 1. Inicializamos o computador com o CD ou DVD de instalação.
- 2. Logo abaixo do botão de instalar, que aparece em seguida, deverá haver um link para Recuperar o windows.

O termo boot (ou bota) é empregado em informática em analogia ao chute, o pontapé inicial (do sistema operacional). BOOT é ainda uma sigla para a expressão em inglês pulling himself by his own bootstraps, que significa, por-se de pé pelos cadarços de suas próprias botas. Ou conquistar algo por esforço próprio. Aplicada à computação, a expressão remete ao fato de o computador estar pronto para se inicializar sozinho.

Figura 66

Tela de seleção do sistema operacional no momento do boot.



8.1.3.2. Endereçamento LBA

Logical Block Addressing (Endereçamento Lógico de Blocos) é o método de tradução que permite ao BIOS reconhecer HDs IDE. Antes de 2001, as placas-mãe utilizavam 28 bits para endereçar 228 setores de maneira sequencial. Por exemplo: setor 1, setor 2, setor 3 e assim por diante. Isso limitava o tamanho dos discos em até 128 GB. Com a introdução da interface ATA-6 houve um extensão na quantidade de endereços disponíveis, com a utilização 48 bits, 20 bits a mais que na versão anterior, o que elevou a capacidade do BIOS de reconhecer discos de até 144 petabytes (144,000,000 gigabytes). HDs SCSI e SATA não utilizam LBR, mas suas próprias técnicas de endereçamento, e não têm limitação de tamanho.

8.1.4. Reconhecimento de discos rígidos

Existem processos diferentes para o computador conseguir acessar os dados nos discos IDE, ou para conseguir reconhecer o HD SATA. Vamos conhecê-los.

8.1.4.1. Disco IDE

Como já aprendemos, o disco IDE precisa ser reconhecido pelo BIOS para ser endereçado. Para fazer o reconhecimento, recorreremos ao CMOS Setup do BIOS. O trabalho é bem simples. Ao iniciar o micro, devemos localizar a tecla que inicia o CMOS Setup (figura 67), em geral DEL, F1 ou F2. Com o sistema em operação, localizamos a opção Standard CMOS Features ou Standard CMOS Setup. Normalmente a interface do programa tentará detectar os discos automaticamente. Saia do setup escolhendo a opção de salvar e sair (save and exit). Nesse momento, o novo disco está pronto para ser utilizado e poderá ser identificado pelo instalador do sistema operacional ou executará o boot se o sistema já estiver instalado.

**Figura 67**  
Telas do setup indicando o caminho para a tela de reconhecimento de HDs IDE.



8.1.4.2. Disco SATA

Os discos SATA não precisam ser reconhecidos pelo CMOS Setup, apesar de alguns BIOS virem com esta opção. Em SATA o controle de acesso ao disco é feito diretamente pela controladora. Para que o boot seja feito por meio de um disco SATA, o sistema operacional deve, antes, instalar os drivers corretos da controladora desse tipo de tecnologia.

Sempre que for instalar algum sistema operacional você precisará ter o driver disponível em algum tipo de mídia inicializável, em disquete, CD, DVD ou mesmo pen-drive (Windows Vista em diante). Para instalar o sistema operacional você deverá alterar a sequência de boot no Setup da CMOS para o driver onde será inserida a mídia de instalação, geralmente CD ou DVD. Assim que se iniciar o processo de instalação, o computador perguntará se há necessidade de instalar algum driver adicional. No Windows Vista a opção está na tela de gerenciamento de discos, onde você encontra o botão Load driver, que lhe possibilitará escolher a mídia que contém o arquivo de instalação. No Windows XP, logo no início da instalação aparece a mensagem “pressione a tecla F6 para fornecer drivers de terceiro”, e a mídia poderá ser acessada.

Insira a mídia com o driver e selecione-a no menu. Se o driver estiver correto, o disco será reconhecido e o processo de particionamento, formatação e instalação prosseguirá. No Linux, muitos drivers são reconhecidos automaticamente, mas há a opção selecionar. No RedHat Linux, caso não encontre o driver, você pode carregar o sistema em um disquete inicializável e executar o comando dd if= of=/dev/fd0 no prompt de comando. Em seguida dê o boot com o disco de instalação do RedHat Linux e, quando aparecer a palavra boot:, escreva na frente Linux add. Quando o programa lhe requisitar coloque o disquete no driver e siga as instruções de instalação.

8.1.5. Montagem e configuração de HD

A montagem de um HD requer cuidados especiais. Veja, nos próximos tópicos, como executar cada etapa do processo.

8.1.6. Particionamento

Para o computador encontrar o sistema operacional e criar o sistema de arquivos, o disco deve ter sido particionado anteriormente. **Particionar** é o mesmo que dividir o disco, identificando suas devidas partes e dimensões. Podemos com isso criar várias unidades lógicas do DOS, que integram o sistema operacional da Microsoft. O Windows identifica como letras (C:, D:, G:) as partes que podem ser acessadas como se fossem unidades de disco em separado. Os sistemas baseados em Unix utilizam nomes como /boot, /home etc., todas partindo da raiz (/).

A divisão do disco permite instalar mais de um sistema operacional no mesmo computador. Certas aplicações devem usar partição específica para limitar o tamanho de seus arquivos aos limites da partição separada, para não comprometer o espaço livre disponível nas outras partições. Caso contrário, podem preencher

Há dois tipos de partições: primárias e estendidas. As partições primárias servem para instalar sistemas operacionais. Pode-se criar no máximo quatro partições deste tipo por disco, que não podem ser subdivididas. As partições estendidas podem ser divididas em unidades lógicas (C:\, D:\, E:\, F:\ etc) e criadas em espaços ainda não particionados do HD. Nessas partições não se pode instalar sistemas operacionais.



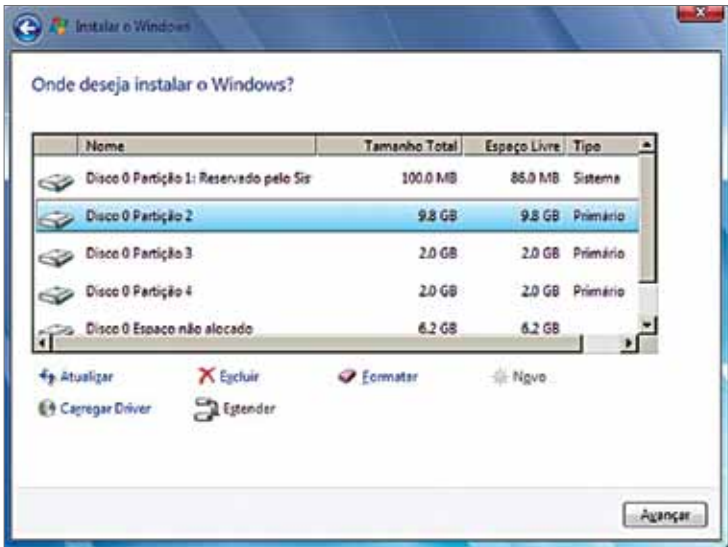
**Figura 68**  
Disco particionado.



todo o disco e paralisar o computador por falta de espaço para memória virtual. Quando o disco é particionado (figura 68), o computador cria uma tabela de alocação chamada MBR, que fica armazenada no início do disco rígido. Essa tabela informa a posição de início da partição, se está ativa e qual é o seu tipo.

A ferramenta mais utilizada para particionar o HD é o fdisk, encontrado nas distribuidoras da Microsoft desde as versões mais remotas de seus sistemas operacionais. No Linux há o QParted e o GParted, entre outros. Os instaladores dos sistemas operacionais possuem um assistente que orienta como particionar o disco (figura 69).

**Figura 69**  
Tela de particionamento de disco do instalador do Windows 7.



O padrão MBR é limitado na quantidade de partições primárias, mas possibilita a criação de partições estendidas. Cada partição ou disco pode ter no máximo 2TiB – 2 tebibytes na base 2 ( $2^{40}$ ) aproxima-se de 2 terabytes na base 10 ( $10^{12}$ ). Para resolver esse problema a Intel desenvolveu a especificação **EFI**. O objetivo é eliminar o BIOS dos computadores, introduzindo o GPT (GUID Partition Table ou tabela de partição de identificador único e global), que permitirá a criação de quantidade ilimitada de partições com tamanho de até 8 Zib (8.589.934.592 TiB), utilizando endereçamento armazenado em 64 bit ao invés de 32 bit.

8.1.7. Sistemas de arquivos

Dentro do disco rígido as informações são organizadas em arquivos e diretórios (pastas), sempre de forma hierárquica, partindo da pasta raiz. Existem vários tipos de sistemas de arquivos, todos, em geral, com a mesma lógica organizacional e várias especificidades que os diferenciam.

8.1.8. Formatação lógica e física

A formatação física do HD, feita pelo fabricante, consiste na divisão permanente dos setores e das trilhas dos discos. O conjunto de trilhas de cada disco é chamado de cilindro. Cada setor do disco tem exatamente 512 bytes.

Muitos técnicos formatam fisicamente discos que começam a apresentar falhas ao ler e escrever em determinados setores (bad sectores). Esse procedimento é feito por meio do software de formatação física fornecido pelo fabricante, geralmente em seu site da web. Tais programas são capazes de marcar os setores danificados, inutilizando-os. Há quem pense que a formatação física corrige o disco, mas isso não é verdade, pois o processo apenas isola suas partes defeituosas, que deixam de ser utilizadas. Isso funciona bem, mas o disco perde espaço útil de armazenamento.

A mais comum é a formatação lógica. Ela não marca o disco de forma permanente; apenas instala nele uma estrutura lógica para mapear todas as posições graváveis. Cada uma dessas unidades é chamada de bloco. Para a controladora do disco, os blocos são endereçados a partir do seu cilindro, trilha e setor, enquanto para o sistema operacional cada partição é identificada com uma numeração única e sequencial. É bom ressaltar que, antes de uma formatação física, é necessário particionar o disco.

8.1.9. O sistema de arquivos

A estrutura que a formatação lógica cria nas partições do HD é denominada sistema de arquivos, cuja função é proporcionar organização e agilidade ao sistema operacional para encontrar os arquivos no disco. Se, para saber o total de espaço livre que há no disco, o sistema operacional precisasse percorrê-lo inteiro, somando as áreas vazias, poderíamos ter de esperar a informação por horas. Mas este dado é obtido instantaneamente. Basta verificarmos as propriedades de uma unidade lógica na pasta Meu computador do Windows (figura 70).

A especificação EFI foi repassada ao consórcio UEFI (Unified Extensible Firmware Interface Specification, ou Especificação de Interface de Firmware Extensível e Unificada). Em 2009, o consórcio, formado por Intel, AMD, American Megatrends Inc, Apple Computer, Inc, Dell, Hewlett Packard, IBM, Insyde, Lenovo, Microsoft e Phoenix Technologies, tinha como missão avaliar a especificação e adotá-la em suas tecnologias.

Figura 70

Capacidade total e o espaço livre das unidades lógicas de um HDD.



Se procurarmos abrir determinado arquivo no editor de texto por meio da opção Localizar arquivo, no Windows, ou do comando Find, do Linux, quanto tempo teremos de esperar pela resposta? Tente e você verá que, dependendo da quantidade de arquivos do seu disco, essa tarefa será muito demorada. Mas os sistemas de arquivos embutem técnicas capazes de encontrar um arquivo cujo caminho completo conhecemos – com unidade lógica, mais o diretório e o nome – quase que de forma instantânea. Por exemplo: “c:\aula\materia.doc”.

8.1.9.1. FAT

O sistema de arquivos **FAT** (File Allocation Table ou Tabela de Alocação de Arquivos) baseia-se em uma tabela de alocação que registra os arquivos e os blocos em que estão armazenados. É como se fosse o índice de um livro indicando em que página se encontra cada capítulo.

O FAT divide os setores do disco em blocos, também chamados de clusters. A tabela do primeiro FAT podia endereçar números com até 16 bits, ou seja, 2<sup>16</sup>. Esse valor possibilita apenas 65536 endereços de clusters e, com isso, as partições poderiam chegar a no máximo 2 GB de capacidade. O FAT32 suporta até 4.294.967.296 clusters e partições de até 60 GB. Por ter pequena capacidade de endereços, os clusters eram maiores, chegando a até 64KiB. No FAT32 os clusters puderam ser reduzidos para até 4 KiB.

Clusters maiores são mais rápidos para procurar, pois têm menos endereços para administrar, enquanto clusters menores evitam desperdício de capacidade. Imagine que, no FAT32, um arquivo de 3 Kib não ocupará toda a capacidade do cluster, e o 1 Kib restante não poderá ser utilizado por outro arquivo. Numa partição FAT16 a sobra seria ainda maior, de 61 Kib.

8.1.9.2. NTFS

Desde sua primeira geração de sistemas operacionais para servidores, o Windows NT, a Microsoft utilizava o NTFS (NT em referência ao sistema operacional e FS a File System, ou seja: sistema de arquivos do Windows NT). Trata-se de um sistema de arquivos de alta-performance, que pode formatar partições de grande capacidade, até para os padrões atuais, e permite controle de acesso aos arquivos em nível de usuário, por meio das contas de usuários do próprio Windows. Isso significa que o NTFS pode prover segurança para ou-

tros usuários verem ou não seus arquivos, alterá-los ou até excluí-los. O espaço em disco de cada usuário pode ser definido por meio de quotas. O sistema ainda permite criptografar, comprimir e controlar a integridade dos dados e possibilita a recuperação de arquivos deletados, além de várias outras funções. São muitas as versões do Windows que suportam NTFS: todas as versões de servidores desde a NT e, em estações de trabalho, o Windows 2000 e todos os seus sucessores (XP, Vista e Seven). No fim de 2009, o sistema de arquivos já estava na versão NTFS v3.

No padrão, o NTFS utiliza clusters com um setor apenas (512 bytes), evitando totalmente o desperdício de capacidade, e endereçamento de 32 bits (a tecnologia prevê 64 bits, mas para as versões atuais do Windows emprega somente 32 bits). Nessa configuração uma partição pode chegar até 2 TB de capacidade. É possível configurar o tamanho dos clusters na hora de formatar uma partição – podem ser montadas partições de até 256 TB, se os clusters forem de 64 KB.

Apesar de proprietários, os sistemas de arquivos da Microsoft FAT e NTFS podem ser lidos por outros sistemas operacionais, como o Linux.

A Microsoft vinha desenvolvendo e até anunciou a implantação de um novo sistema de arquivos, o WinFS a partir do Windows Vista. Porém isso não se confirmou, nem mesmo para o Windows 7.

8.1.9.3. Formatos para Linux

No sistema operacional Linux é possível utilizar vários outros tipos de sistemas de arquivos. Os mais comuns são o Ext (nas versões 2, 3 e 4) e o ReiserFS, mas também encontramos, para aplicações mais específicas, o XFS (rápido e indicado para partições grandes), o JFS (utilizado pela IBM, permite redimensionar as partições sem precisar reiniciar o sistema), o GSF e o OCFS2 (permite utilização simultânea e compartilhada por mais de um computador), entre muitos outros.

O Ext é o padrão da maioria das distribuições, geralmente na versão Ext2 e Ext3. A partir desta última foi incluída a propriedade de journalização (do inglês journaling), que possibilita recuperar dados danificados por desligamento abrupto do computador.

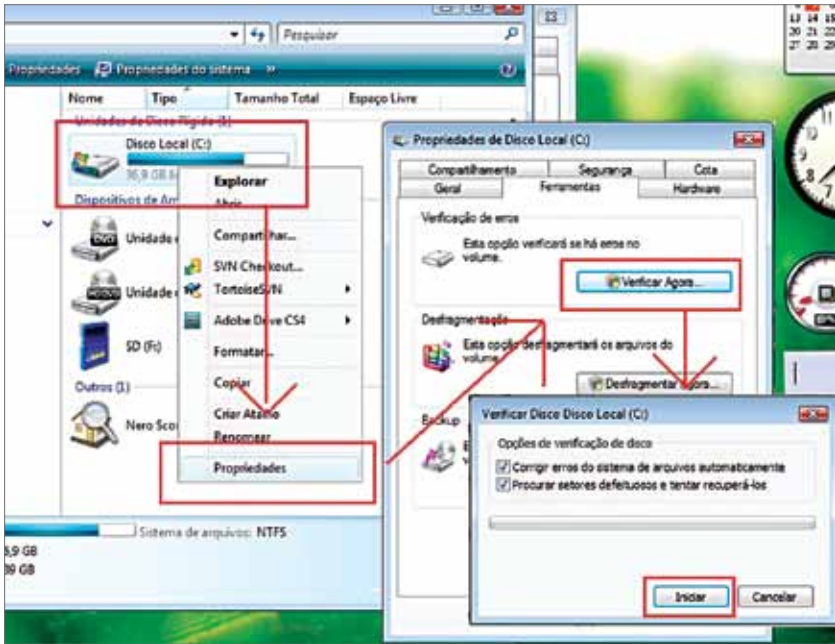
A falência do Reiser

A substituição do ReiserFs pelo Ext3 nas distribuições Linux, em que tinha se tornado padrão, não teve nada a ver com questões tecnológicas. Em 2006 o criador do sistema, Hans Reiser, nascido em 1963 e formado em programação de computadores pela Universidade de Berkley, na Califórnia, foi condenado por homicídio culposo pelo assassinato de sua esposa, Nina Reiser. Os grupos de desenvolvedores abandonaram o projeto e a empresa faliu.



Figura 71

Agendamento de verificação de disco.



O ReiserFS também foi bastante utilizado, mas vem sendo substituído pela Ext, versão padrão nas distribuições Slackware, OpenSuse, Linspire, Kurumin (veja o quadro *A falência do Reiser*). O sistema Ext permite a conversão das partições Ext2 para Ext3, e assim sucessivamente, sem demandar reformatação. O ReiserFS não converte, por exemplo, a versão ReiserFS3 para a 4.

8.1.10. Identificação e correção de falhas

O disco rígido é um dispositivo lógico, com circuito eletrônico, mecânico e magnético. Por isso, está sujeito a defeitos nessas quatro áreas. Aparelhos mecânicos podem apresentar desgaste quando sofrem atrito e perdem precisão – em casos assim, o disco tem de ser substituído. No âmbito digital, podemos ter problemas com a placa controladora que é acoplada ao disco, a qual pode queimar ou apresentar defeito em algum componente – e, também nesse caso, a solução é trocar o dispositivo. Na parte magnética do disco, podem ocorrer falhas causadas por perda do poder magnético de alguma área, a que chamamos de badblock (bloco ruim). No que diz respeito à lógica, os dados gravados podem estar inconsistentes, o que requer que sejam checados e, se possível, remapeados, reconstituídos ou mesmo removidos para que o restante dos bits ali gravados possa voltar a ser lido e apresente coerência.

Erros lógicos podem ser corrigidos, ou, no caso dos magnéticos, contornados por meio de isolamento lógico das partes defeituosas, com o uso de uma ferramenta simples, um programa que existe nos sistemas operacionais da Microsoft desde as primeiras versões do DOS. Estamos falando do CHKDSK, aplicativo de console sem janelas, que executamos no MSDOS escrevendo esse comando no prompt e no Windows, através do prompt de comando ou da opção Verificação de erros na aba Ferramentas das propriedades do disco local.

Figura 72

Comando CMD utilizado para acessar o prompt de comando.



Se você quiser executar o CHKDSK no prompt de comando, clique em iniciar, executar e escreva CMD (figura 72). Depois execute o comando CHKDSK informando a unidade de disco que quer verificar. Caso deseje corrigir o sistema de arquivos e ainda procurar e corrigir setores defeituosos, acrescente a opção R (abaixo).

>CHKDSK C: /R

Se o programa perguntar se você quer agendar a verificação é porque precisa de exclusividade no acesso ao disco e fará a verificação na vez seguinte que você reiniciar o computador, antes de começar a carregar o Windows. Problemas frequentes no disco podem indicar defeito no dispositivo ou até mesmo alguma falha na fonte de energia.

8.2. Disco flexível

O Floppy Disk (ou disquete, como ficou conhecido - figura 73) é um tipo de mídia que foi largamente utilizado no início da evolução dos computadores e ainda está presente em algumas máquinas. No começo alguns computadores não tinham HD e o sistema operacional era carregado diretamente do disquete. Depois vieram os HDs e os sistemas operacionais foram ficando maiores. Como até então as redes Lan eram pouco utilizadas e não existia internet, o floppy era

Figura 73

Floppy Disk (disquete).



o meio mais comum de transmissão de dados de um computador para outro. E mesmo após o advento do CD e DVD, Lans e internet, ainda há usuários que salvam seus arquivos em disquetes, ainda encontrados em livrarias e papelarias.

O nome disco flexível refere-se ao fato de o dispositivo ser de plástico, podendo ser magnetizado. Com 3½ polegadas, o disquete tem pouca capacidade de armazenamento, somente 1.44 MB, insuficiente para uma única música no formato MP3. Para ler o Floppy Disk, o motor da leitora o faz girar por meio de uma peça metálica afixada em seu centro.

As máquinas evoluíram e começaram a trazer leitores de cartões flash no lugar dos leitores de disquetes. Além dos discos flexíveis foram criadas outras mídias magnéticas de maior capacidade, como o Zip Drive e o Jazz Drive, mas logo foram substituídas por mídias ópticas.

8.3. Discos ópticos

Os discos ópticos vieram substituir as formas removíveis de mídia magnética. A transmissão de dados por meio da luz é mais barata, a capacidade de armazenamento dos dispositivos com essa tecnologia é maior e, além disso, eles não sofrem danos por contato com fontes magnéticas, como, por exemplo, a luz solar. Inicialmente, a intenção era criar um meio para transmissão de áudio e a primeira especificação dos discos ópticos foi Laserdisc. Tratava-se de dispositivo em formato analógico, que posteriormente se tornou digital. Os CDs têm no máximo 800 MB de capacidade e podem armazenar até 80 minutos de música. Depois vieram os DVDs (Digital Vídeo Disc, ou Disco Digital de Vídeo) com capacidade para armazenar vídeos de boa qualidade e capacidades que variam de 4.7 GB em uma camada, e com duas camadas até 8.5 GB. A leitura se dá por meio da recepção de um feixe de raio laser emitido pelo canhão, o qual é refletido na superfície da camada refletora. Esta camada possui ondulações e espaços impressos em espiral que se estendem do centro até a extremidade. Tais variações na superfície do disco modificam o feixe de luz refletido, cujos sinais o sensor então interpreta como zeros e uns.

8.3.1. CD

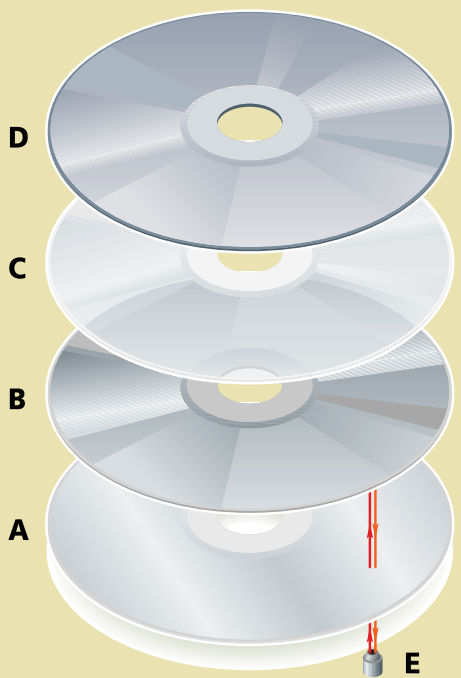
A sigla significa Compact Disc ou Disco Compacto, e foi introduzida no mercado em 1985 pela Sony e pela Philips. Tem formato de disco de duas faces com um orifício no centro. Somente é possível gravar e, portanto, ler, em uma das faces, a limpa, com superfície transparente ao laser. A outra geralmente é pintada e pode ser usada para imprimir o rótulo ou o título do conteúdo.

Usamos CDs de três tecnologias diferentes: o CD-ROM, o CD-R e o CD-RW. O primeiro leva a sigla ROM para indicar que é somente para leitura (Read-Only Memory ou Memória Apenas de Leitura) e seu conteúdo já vem impresso de fábrica. O CD-R pode ser gravado, como indica o sufixo R (de Recordable, ou Gravável), porém aceita somente uma gravação. O formato CD-RW (RW remete a Rewritable, ou Regravável) permite gravar, apagar e gravar novamente várias vezes. Para que possa ser reutilizado, este último formato tem camada de gravação composta por um material que modifica suas propriedades quando recebe calor. E para eliminar esse calor após a gravação, as camadas de materiais são diferentes das do CD-ROM (leia quadro *Por dentro do CD-ROM*):

- 1ª **Camada de proteção:** policarbonato transparente.
- 2ª **Camada de laqueamento:** igual à do CD-ROM, também serve para proteger os dados.
- 3ª **Camada dielética:** serve para proteger a camada de gravação, ajudando a eliminar o calor durante a gravação.
- 4ª **Camada de gravação:** onde fica um material composto por prata, antimônio e telúrio, capaz de alterar a sua opacidade em função do calor.
- 5ª **Camada dielética:** fica por cima da camada de gravação e também serve para proteger e retirar o calor.
- 6ª **Camada de rótulo:** mais grossa, dá sustentação às demais. É utilizada para imprimir o rótulo do CD.

Os gravadores de CD possuem um dispositivo que emite o raio laser, chamado de canhão de laser, que é capaz de emitir laser em três potências:

- Baixa:** para fazer a leitura – não modifica a estrutura da matéria de gravação.
- Média:** para limpar a unidade, pois funde o material levando-o para o estado cristalino e homogêneo.
- Alta:** para modificar o material de transparente para opaco e assim produzir as depressões que representam os dados.



### Por dentro do CD-ROM

O CD-ROM é composto por quatro camadas, como você pode observar na figura 74. A letra E mostra o canhão de laser do hardware. Confira as funções de cada camada do CD-ROM:

- A. Camada de policarbonato onde os dados são impressos.
- B. Camada refletora, que reflete o raio laser para o sensor.
- C. Camada selada, para evitar danos por contato com ar, umidade e poeira.
- D. Superfície livre, utilizada para imprimir o título.
- E. Canhão de laser, que emite o feixe de luz, e leitor óptico, que identifica os sinais e os converte para bits.

**Figura 74**  
As quatro camadas do CD-ROM.



**Figura 75**

DVD.



### 8.3.2. DVD

Após dez anos do lançamento do CD, o DVD (Digital Video Disc, Disco Digital de Vídeo ou também Digital Versatil Disc, Disco Digital Versátil), com tecnologia óptica mais avançada e forma melhorada de compactar os dados melhorada, aumentou a capacidade de armazenamento (figura 75). Assim como o CD, vários formatos de DVD são comercializados. Confira:

**DVD-R:** permite uma só gravação, de até 4,7 GB.

**DVD-RW:** tem a mesma capacidade do DVD-R, mas pode ser gravado e regravado várias vezes.

**DVD+R:** idêntico ao DVD-R, porém tem formato diferente de gravação e leitura. Portanto não é lido e gravado por leitoras/gravadoras DVD-R. Essa mídia consegue desempenho maior de leitura, comparada ao DVD-R apenas para backup de dados. Para outros fins, o desempenho é o mesmo. Existem leitoras capazes de ler os dois formatos de DVD, que são chamadas de gravadores DVD±R.

**DVD+RW:** segue o mesmo formato do DVD+R, porém pode ser regravado várias vezes, assim como o DVD-RW.

### 8.3.3. Blu-Ray

Esse formato foi criado em 2008 pelas gigantes da indústria de filmes, Warner Bros., MGM, Fox e Columbia Pictures (figura 76). As empresas queriam gravar seus filmes em mídias mais seguras contra pirataria, e que pudessem armazenar imagens de alta resolução.

**Figura 76**

Blu-Ray.



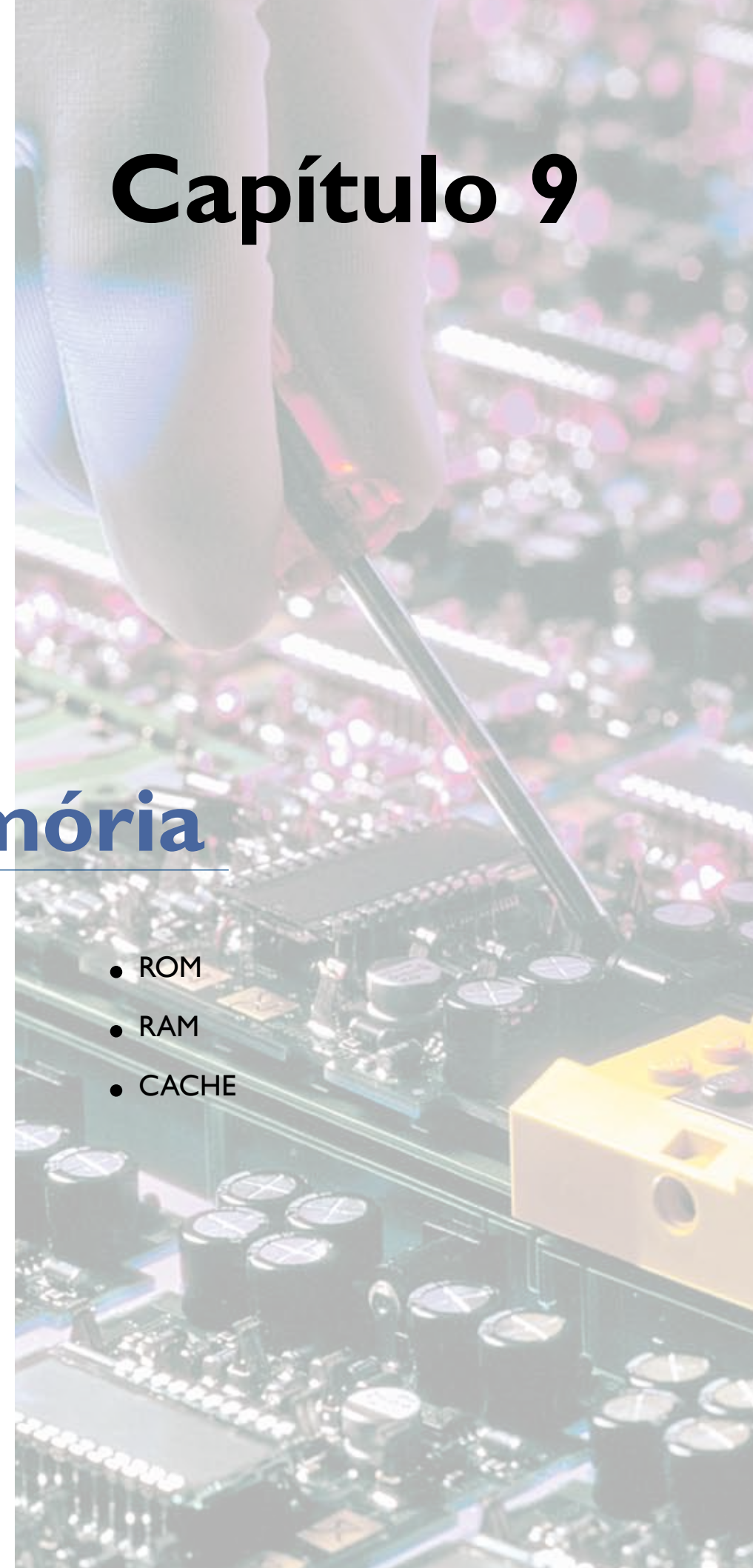
A leitura nesse caso é por meio de um feixe de raio laser de cor azul-violeta com comprimento de onda de 405 nanômetros, diferente da tecnologia do CD/DVD, cujo raio é vermelho, com comprimento de onda de 605 nm. O feixe de luz menor possibilita subdividir mais o espaço e, portanto, a tecnologia propiciou novo aumento da capacidade de armazenamento do disco, para 25 GB em unidades de camada simples e 50 GB nas de camada dupla. O **Blu-Ray** é capaz de armazenar até 4 horas de gravação em resolução 1080p em Full HD (1080p é a definição de monitores com capacidade de imprimir 1080 linhas verticais. A letra p, vem de varredura progressiva). Somente TVs e monitores de plasma e LCD de alta resolução, porém, se beneficiam desse formato.

Blu-Ray vem de raio-azul, blue ray em inglês. O nome perdeu o "e" porque alguns países não permitem o uso da palavra Blue em marcas proprietárias.

# Capítulo 9

## Memória

- ROM
- RAM
- CACHE





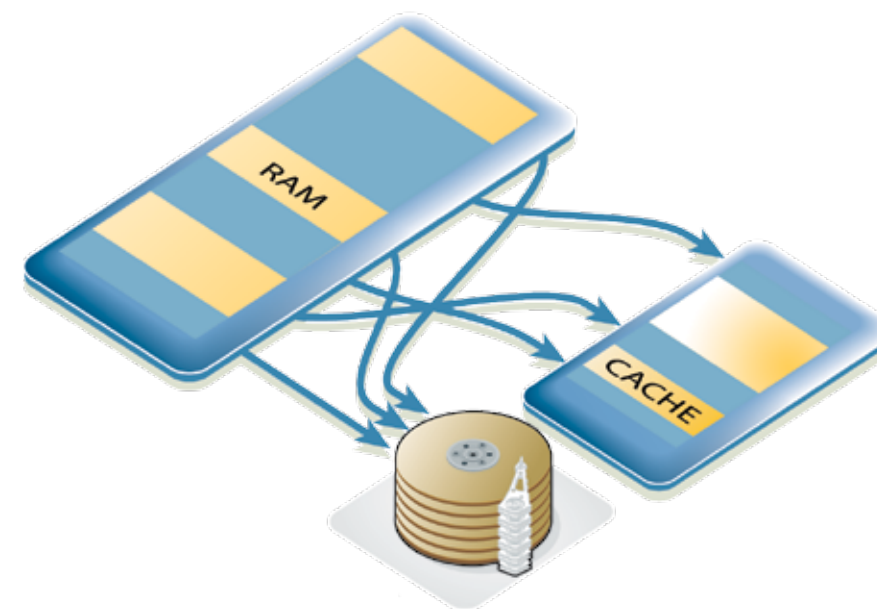
A arquitetura de von Neumann (leia o texto *Do cartão perfurado à memória*), na qual se baseiam os computadores pessoais, prevê que, entre outros componentes, um computador tem unidade central de processamento e que esta precisa de memória para possibilitar à máquina guardar e buscar dados. As memórias são classificadas em primárias e secundárias. Veja os conceitos.

**Primárias:** são as que o processador acessa diretamente. Fazem parte deste grupo os registradores e as memórias CACHE e RAM.

**Secundárias:** são as que o processador não acessa diretamente – os dados têm de ser, antes, carregados na memória principal. Estão nessa categoria o disco rígido, o disquete, as mídias removíveis como CD, DVD, cartões de memória. Ou seja, todos os outros tipos de memória.

## Do cartão perfurado à memória

Grande parte das pessoas que conhecem um pouco da história da informática só consegue associar o nome John von Neumann (1903-1957) à arquitetura von Neumann – a estrutura de armazenamento de programas na memória do computador, que se tornou clássica. Foi de fato uma contribuição decisiva, pois antes as instruções eram lidas em cartões perfurados e executadas uma a uma. Mas o matemático húngaro naturalizado americano teve participação importante também em temas como princípios de programação, análise de algoritmos, redes neurais e tolerância de falhas. Von Neumann participou da construção, entre 1944 e 1951, do EDVAC (Electronic Discrete Variable Automatic Computer), primeiro computador com programa armazenado na memória, para o U. S. Army's Ballistics Research Laboratory. O EDVAC operou até 1962.



**Figura 77**

A memória principal é formada pela RAM e pela CACHE.

As memórias também são classificadas em relação à forma de leitura: ROM e RAM.

## 9.1. ROM

A sigla ROM vem da expressão em inglês Read-Only Memory, que significa Memória Apenas de Leitura. É uma memória que não permite a alteração ou remoção dos dados nela gravados, os quais são impressos em uma única ocasião. Um DVD é um tipo ROM. Depois de queimarmos o DVD, a área utilizada pela gravação não poderá ser reutilizada. Assim, por exemplo, um DVD de um filme não pode ser reutilizado para nele se gravar outro título. Alguns tipos de ROM permitem regravação após uma intervenção específica, como o DVD-RW, que pode ser limpo e receber nova gravação. Esse tipo de memória não é volátil, ou seja, mantém os dados gravados, mesmo que o computador esteja desligado.

As memórias ROM embutem várias tecnologias relacionadas: PROM, EPROM, EEPROM, Memórias Flash, CD-ROM, DVD-ROM, BluRay-ROM.

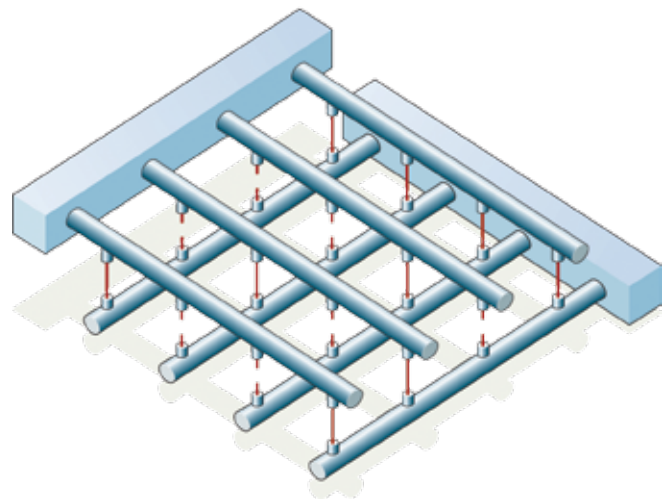
### 9.1.1. PROM

A PROM (Programable Read Only Memory, ou Memória Programável só de Leitura) foi uma das primeiras ROM da história. Foi desenvolvida nos Estados Unidos em 1956 por Wen Tsing Chow (leia na próxima página o texto *Segredo de estado*).

Aceita apenas uma única gravação, e seu funcionamento é bem simples, o que permite que seja barata e útil para vários fins – um dos quais, bastante comum, é conter brinquedos eletrônicos. Mas também encontramos PROM virgens no comércio. A PROM é um circuito eletrônico que armazena dados por meio de um conjunto de fusíveis, conforme mostra a figura 78. Cada fusível pode representar um dígito binário. Quando o fusível estiver queima-

Figura 78

A PROM é um circuito eletrônico que armazena dados por meio de um conjunto de fusíveis.



do, ele representará o valor zero. Se estiver passando corrente, o valor será 1. Para queimar uma PROM, utiliza-se um dispositivo chamado Programador.

9.1.2. EPROM

A sigla EPROM, da expressão Erasable Programmable Read Only Memory (erasable = apagável), indica que esta memória pode ser regravada (figura 79). Para gravar, aplica-se uma carga elétrica maior do que a utilizada para leitura, e depois disso os dados não poderão mais ser alterados até o dispositivo ser novamente zerado. Para limpar a memória, aplica-se um feixe de raio ultravioleta sobre a área onde o chip fica aparente, protegido por uma lente de cristal.

Uma memória EPROM pode armazenar informação por até 20 anos ou mais, desde que fique protegida da luz solar, que pode apagá-la. Antigamente chips de EPROM eram utilizados para armazenar o programa BIOS.

Segredo de Estado

A memória PROM foi inventada em 1956 por Wen Tsing Chow, quando o cientista trabalhava para a American Bosch Arma Corporation, em Nova York. A invenção foi concebida a pedido da Força Aérea dos Estados Unidos para equipar o computador digital do míssil Atlas E/F, de alcance intercontinental. Sua patente e tecnologia associada foram mantidas em segredo por vários anos enquanto o armamento foi o principal míssil operacional dos Estados Unidos. O termo burn out consta da patente original, mostrando que era preciso, literalmente, queimar as pontas de diodos internos com uma sobrecarga de corrente para produzir a descontinuidade no circuito. Os primeiros queimadores de PROM foram desenvolvidos por engenheiros da Bosch, sob a direção Chow.

Figura 79

Uma memória EPROM pode armazenar informação por 20 anos.



9.1.3. EEPROM

A EEPROM (Electrical Erasable Programmable Read Only Memory ou Memória Somente de Leitura, Programável e Limpa Eletricamente), desenvolvida pela empresa japonesa Toshiba em 1980, é também regravável. Traz um grande diferencial sobre as demais EPROM: possibilita reciclar a memória toda, em partes, ou até em uma única célula (1 bit). Ou seja: podemos apagar parte da memória e gravar novamente sem problemas. Para gravar, aplica-se uma carga elétrica no circuito da célula de memória ou em um grupo de células de memória, em vez de luz ultravioleta. Essa característica facilita seu uso, pois não demanda um aparelho programador. Além disso, as EEPROM podem ser formatadas em qualquer máquina em que estejam instaladas.

9.1.4. Memórias flash

As memórias flash baseiam-se no padrão EEPROM. O processo de gravação e leitura nesse caso é por meio da aplicação de carga elétrica – carga mais baixa para leitura e mais alta para gravação dos dados. As memórias flash se popularizaram como principal mídia para armazenamento de dados em microdispositivos,

Figura 80

Sem padrão, cartões flash são encontrados em formatos variados, cada um com o próprio tipo de leitor.





como celulares, câmeras, PDAs e notebooks, em formato de cartões de memória (figura 80) e pen-drives ou unidades internas no lugar do HD. O funcionamento desse tipo de memória é bem parecido com o da memória RAM (veja abaixo). A diferença está na capacidade de manter os dados quando falta energia elétrica em seus circuitos. A tecnologia tem baixo consumo de energia e boa durabilidade por ser um semiconductor sólido, sem partes móveis, o que evita danos por atrito. Também possui recursos de proteção, como o ECC (Error Correction Code, Código de Correção de Erros), que lhe confere bastante confiabilidade. O único problema é o preço, bem alto, o que torna viável apenas a comercialização de unidades de baixa capacidade em relação à de mídias como CD, DVD e HD.

Como não se criou nenhum consórcio de empresas para padronizar o formato de memórias em cartões, existem vários modelos no mercado, cada um com o próprio tipo de leitor (figura 80).

9.2. RAM

A memória RAM, acrônimo em inglês para Random Access Memory, ou Memória de Acesso Aleatório, traz em seu nome uma característica que leva em consideração a estratégia de recuperação dos dados. Quando precisa de um dado, o processador solicita determinado endereço e a memória vai diretamente à informação, captando-a e retornando ao processador (figura 81). O oposto dessa estratégia, só para você compreender melhor, é a utilizada pelas unidades de fita DAT. Estas têm de desenrolar um carretel do cartucho da fita para chegar à posição do dado.

O nome RAM se tornou sinônimo desse tipo de memória e não retrata corretamente a diferença que é preciso fazer entre ROM e RAM. Na prática o que diferencia os dois tipos é a capacidade para somente ler e escrever. E também a característica de ser volátil ou não. Até porque as memórias ROM também são de acesso aleatório. Se fossem classificadas ao pé da letra, todas as memórias seriam RAM.

Figura 81

A memória RAM pode obter qualquer informação diretamente.

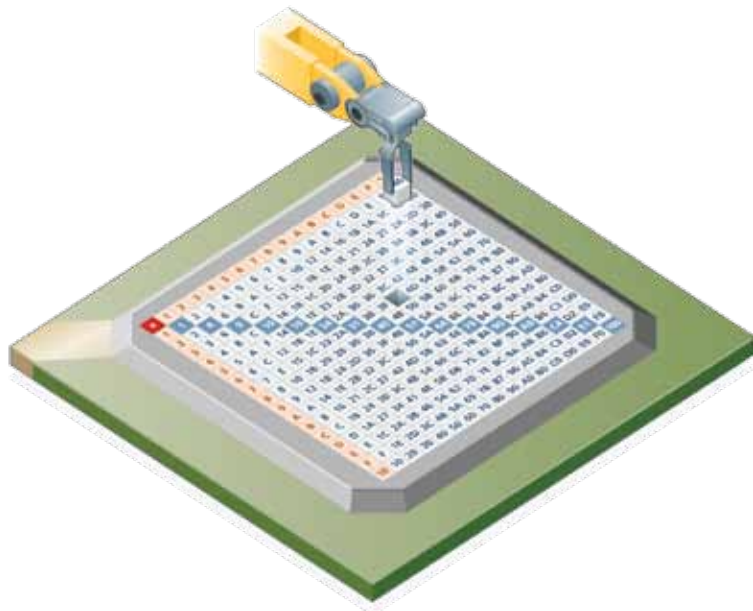


Figura 82

Imagem de módulos de memória DIMM.

A RAM, como vimos anteriormente, faz parte da memória principal do computador e é onde o processador busca dados e programas para executar. É uma memória volátil, que perde as informações nela armazenadas sempre que deixa de ser energizada.

9.2.1. Módulos de memória DIMM

Os chips de memória encapsulada são soldados um ao lado do outro sobre os dois lados de uma placa de circuito impresso, formando um módulo de memória, o que explica o significado de seu nome em inglês: Dual In-line Memory Module, ou Módulo de Memórias em Linha Dupla (figura 82).

Essa placa possui trilhas de conectores para fazerem contato com o encaixe nos slots de memória da placa-mãe. Tais módulos são conhecidos como pentes de memória, por causa de seus conectores, posicionados lado a lado na parte inferior da placa de circuitos, lembrando um pente de cabelo. O primeiro formato lançado tinha 168 vias, mas depois vieram os de 184 vias e o de 240 vias. Há também uma versão para dispositivos pequenos, como notebooks: o módulo SODIMM (Small Outline DIMM).

9.2.2. DRAM

A Dynamic RAM, ou memória RAM dinâmica (figura 83), é o tipo de memória empregada como RAM nos computadores em 2009. Trata-se de modalidade bem simples, onde cada célula de memória é composta apenas por um capacitor e um transistor por bit. Um módulo de memória possui bilhões desses minúsculos circuitos. Com processo de fabricação simplificado, o custo desse dispositivo é acessível, e podemos colocar 2 GB, 4 GB, enfim, memórias DRAM cada vez mais potentes em nossos computadores.

Os dados de uma DRAM, porém, têm de ser regravados constantemente, pois a informação não dura mais que 64 milissegundos. Isso traz inconvenientes: a tarefa consome energia e gera calor, além de atrapalhar no processo de leitura e escrita dos dados, tornando-o mais lento.

**Figura 83**  
Memória DRAM.



### 9.2.3. SDRAM

Um dos fatores que impediam o computador de alcançar o seu máximo desempenho eram as memórias, que funcionavam a frequências mais baixas que o processador. Muitas vezes, era preciso aguardar vários ciclos por informações da memória. Para solucionar esse problema foi desenvolvido o padrão Synchronous DRAM (figura 84), que segue a tecnologia DRAM, mas funciona na mesma taxa de frequência do processador, no mesmo clock.

### 9.2.4. SDR e DDR

Com o padrão DRAM foi possível desenvolver memórias que transmitem duas vezes no mesmo ciclo de clock, as DR (Double Data Rate SDRAM, ou SDRAM com Taxa Dupla de Transmissão). Com isso as primeiras memórias síncronas do tipo SDRAM que podiam transmitir somente uma vez começaram a ser chamadas de SDR SDRAM (Single Data Rate SDRAM, ou SDRAM com Taxa Simples de Transmissão). Enquanto uma memória PC-100 do tipo SDRAM podia transmitir a 800 MBps (megabytes por segundo), uma DDR SDRAM trabalhando na mesma frequência podia transmitir a 1600 MBps. Por motivos, talvez, comerciais, ou para diferenciar SDR de DDR, as memórias

DDR incluem em seus nomes a taxa de transmissão em megabytes por segundo em que operam. Por exemplo: DDR-PC1600 (de 1600 MBps). Já nas SDR o valor informado se refere à frequência (SDRAM PC-100, isto é, de 100 Mhz).

O padrão continuou evoluindo. Passou por DDR2, que transmite o dobro da DDR, ou seja, quatro operações por ciclo de clock, e leva o prefixo PC no nome (o último modelo lançado foi o PC2-10400) e, no fim de 2009 já havia sido lançado o DDR3. Este leva o prefixo PC3 (DDR PC3-14900) e transmite oito vezes por ciclo de clock, com frequência de até 1866 Mhz a taxas de 14900 MBps e 14500 MBps.

A memória DDR tem outro diferencial em relação à DIMM SDRAM: seus módulos têm somente um ranho, enquanto os das primeiras levam dois.

### 9.2.5. Dual channel

A tecnologia dual channel (canal duplo) permite que uma placa mãe tenha duas controladoras de memória, cada uma controlando um jogo de memória em separado. Esses dados são mesclados entre os módulos, de modo que possam ser acessados por meio de dois bancos de memória ao mesmo tempo. Se a tecnologia DDR3 é capaz de ler 8 bytes por vez, a dual channel consegue transferir 16. Para isso é necessário ter dois módulos de memória idênticos, um em cada banco. Geralmente esses bancos são coloridos, para identificar os slots de cada um deles.

## 9.3. Cache

As memórias cache são memórias do tipo SRAM (Static Random Access Memory, ou RAM estática). Não demandam refresh e, portanto, além de serem mais rápidas, esquentam menos e consomem menos energia. Por serem mais velozes, são colocadas junto do processador para que a resposta sobre os dados que estão sendo utilizados seja mais rápida e frequente. A cache só busca dado na RAM quando este não está na cache. Memórias dessa natureza são muito rápidas, porém caras, pois têm estrutura mais complexa que a das DRAM: levam um conjunto de quatro capacitores e mais dois resistores para cada célula de memória. Por isso não é viável ainda utilizar SRAM para construir RAMs para computador.

**Figura 84**  
Memória SDRAM.





# Capítulo 10

## Processador

- Organização do processador
- Fabricantes e tecnologias
- Procedimento de instalação de um processador

O termo Unidade Central de Processamento, ou simplesmente CPU (sigla em inglês para Central Processing Unit), refere-se ao microprocessador, e não ao gabinete como um todo, como muitas pessoas imaginam. Como o próprio nome diz, sua função é processar as instruções enviadas. O processador está para o computador assim como o cérebro está para o ser humano.

Na placa-mãe há um encaixe chamado socket, que varia de acordo com o modelo do processador, que leva em conta velocidade e capacidade de processamento, memória cache, terminais e consumo de energia.

A CPU executa uma série de rotinas. Vejamos, por exemplo, o que acontece quando você digita no teclado a palavra INFORMÁTICA e quer ver esse texto na tela.

1. Um programa constituído de uma série de instruções para o processador, armazenado no disco rígido, é transferido para a memória.
2. Por meio de um circuito chamado controlador de memória, o processador carrega as informações do programa da memória RAM.
3. As informações, agora dentro do processador, são processadas.
4. De acordo com o sistema operacional, o processador continuará a executar o programa e mostrará a informação processada imprimindo na tela do monitor a palavra INFORMÁTICA.

Com todo esse trabalho, o processador produz calor durante seu funcionamento, assim como todos os componentes eletrônicos. O excesso de calor pode queimar o processador ou fazê-lo travar.

Assim, o calor precisa ser rapidamente removido para evitar aumento de temperatura. A temperatura máxima admissível pelo processador é normalmente estampada no próprio dispositivo, em forma de código. No Data Book (documento que pode ser baixado no site do fabricante) há uma parte dedicada a explicar o código impresso sobre o invólucro do processador que inclui a tem-

peratura máxima admissível. Coolers de qualidade e o uso adequado de pasta térmica ajudarão a manter a temperatura bem abaixo da máxima admissível e, assim, a conservação do processador. Quando os padrões de temperatura estabelecidos pelo fabricante não são respeitados, o processador pode queimar e travar frequentemente, além de acontecerem resets aleatórios.

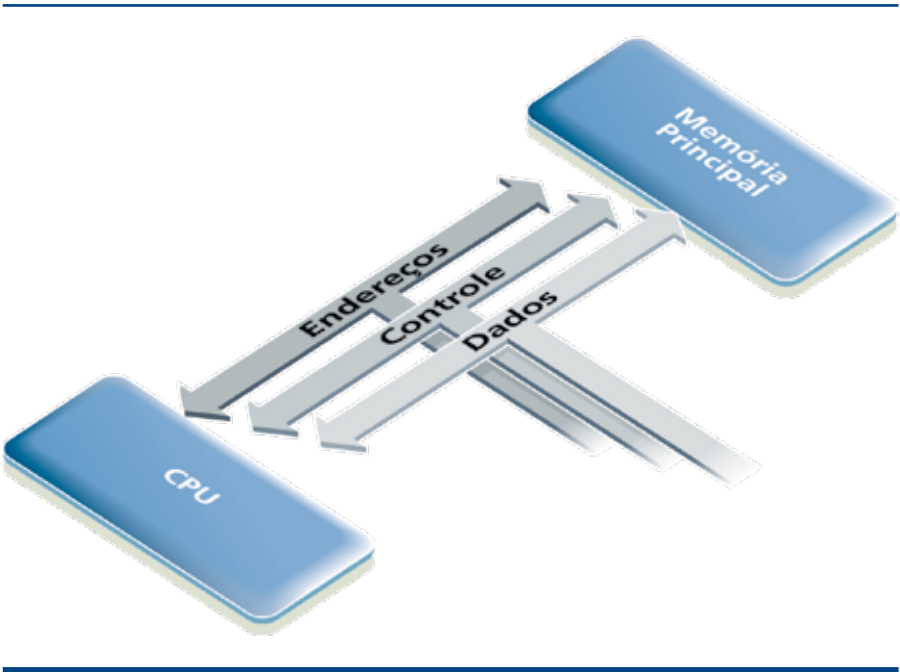
A temperatura de um processador pode ser medida por meio de um sensor existente na placa-mãe, logo abaixo do processador. Em alguns processadores mais novos como o Core 2 Duo, o sensor pode estar dentro do próprio processador. Praticamente todas as placas-mãe vêm com um programa que permite a leitura desse sensor.

### 10.1. Organização do processador

Um CI, ou Circuito Integrado, é um componente capaz de realizar somente um tipo de operação, com determinada quantidade de dados.

O microprocessador também é um circuito integrado, porém, programável, capaz de realizar várias instruções, uma de cada vez. Quem indica ao processador que comando deve executar é um programa, que foi escrito por uma pessoa, gravado em um arquivo e carregado na memória principal do computador. Uma a uma essas instruções são enviadas à CPU, por meio de um barramento específico, chamado Barramento de Controle (Control Bus), ao mesmo tempo que os dados para essa operação são solicitados à memória por meio do Barramento de Endereços (Address Bus) (figura 85). A memória, então, responde ao processador por meio do Barramento de Dados.

O processador é dividido em alguns componentes, e cada um realiza uma tarefa específica, necessária para executar todo o conjunto de instruções que é capaz de processar. Desses, o principal componente é a UC, ou Unidade de Controle, que identifica as instruções, comanda os outros componentes



**Figura 85**  
Barramentos que ligam o processador à memória.



do processador, controla a memória e todos os outros dispositivos do computador. Outro componente é a ULA (Unidade Lógica Aritmética), que funciona como calculadora: faz cálculos matemáticos, lógicos e estatísticos, e é onde realmente os dados são processados. Segundo STALLINGS, 2003, a ULA “constitui o núcleo ou a essência dos computadores”. No fim de 2009, os processadores contavam com outro componente adicional, a FPU (Float Point Unit, Unidade de Ponto Flutuante) para acelerar operações com números mais complexos, que contêm parte fracionária. Em computadores antigos essa funcionalidade era implementada em um processador à parte, fora da CPU. Um terceiro componente do processador são os registradores, unidades de memória que, por ficarem dentro da CPU, possibilitam acesso bem mais veloz aos dados do que as RAM ou cache.

Os registradores são divididos em três grupos:

- de uso geral ou de dados – têm capacidade de 32 bits cada um e são utilizados para armazenar operadores de funções matemáticas que estão sendo processados pela ULA, para fazer cálculos de endereços ou mesmo para manipular cadeias de caracteres;
- de segmento ou de endereço – possuem 16 bits e servem para identificar a localização de instruções e dados na memória;
- sinalizadores – armazenam flags, sinais que indicam o estado de algum processo que está sendo ou foi executado.

Existem também registradores ligados diretamente a processamento de números de ponto flutuante. São eles:

- numéricos – armazenam números de ponto flutuante;
- de controle – sinalizam o tipo operação de arredondamento, precisão simples ou estendida;
- de estado – sinalizam a situação no momento presente da FPU (Float Point Unit, ou Unidade de Ponto Flutuante), topo de pilhas, condições, resultados e exceções;
- condição de conteúdo – indicam o tipo de número que está sendo trabalhado.

10.2. Fabricantes e tecnologias

Durante toda a história do computador, desde o início, há mais de 30 anos, até sua popularização, a principal fabricante, e na maioria das vezes pioneira, foi a Intel. A companhia desenvolveu a maior parte das funcionalidades que conhecemos em microcomputadores, notebooks e servidores. Outra empresa que em muitos momentos surpreendeu pela capacidade de inovação é a AMD, forte concorrente da Intel. Nesse período, alguns fabricantes, como Motorola e Sun, deixaram o mercado de computadores. Mas surgiram novos players, como a Cyrix e a ARM.

A Intel foi a primeira fabricante de CIs programáveis em escala comercial. Desenvolveu, em 1970, o modelo 4004 para uma calculadora de uma marca japonesa. Mas foi somente em 1974 que o processador entrou na história da informática, com o lançamento do X86 no modelo 8086. Logo depois vieram o 80186, o 80286, 80386 e o 80486, que evoluíram até os modelos da arquitetura Pentium, que liderou o mercado por vários anos. No final de 2009, predominavam os processadores Core i7, e já se previa o lançamento do Core i9 para início de 2010. Este último embute a microarquitetura Nehallen Gulf-town, capaz de trabalhar com seis **núcleos** com clock de até 2.4 GHz cada. Outras tecnologias estão em desenvolvimento nos laboratórios da Intel, como a microarquitetura Sandy Bridge, que pode vir a ser a sucessora da Nehallen. Veja a tabela *Alguns modelos de processador Intel*.

Núcleo é a quantidade de processadores internos na mesma CPU, e FSB (Front Side Bus, ou barramento frontal) é o barramento que liga o processador até a ponte norte, chipset da placa-mãe, responsável pelo controle do acesso à memória.

ALGUNS MODELOS DE PROCESSADOR INTEL						
Microtecnologia	Marca	Núcleos (Processos)	FSB	Clock	Socket	Ano de produção
NetBurst	Pentium 4	1 (1) 32-bit	400 MHz até 1066 MHz	3.8 GHz	423,478 e LGA 775	2000 a 2008
Core	Pentium Dual-Core	2 (2) 32-bit	533 MHz até 1066 MHz	1.3 GHz até 2.93 GHz	LGA 775, M, P	2006 a 2009
Allendale	Core 2 Duo	2 (4) 32-bit	800 MHz a 1333 MHz	1.8 GHz a 3.0 GHz	LGA 771 e 775	2006 a 2009
Kentsfield e Yorkfield	Core 2 Quad	2 (8) 32-bit	2.1 GHz a 3.0 GHz	1066 Mhz a 1333 Mhz	LGA 771 e 775	2009 a 2009

ALGUNS MODELOS DE PROCESSADOR AMD						
Versão	Marca	Núcleos (Processos)	FSB	Clock	Socket	Ano de produção
K6	AMD K6	1 (1) 32-bit	66 MHz a 100 MHz	166 MHz a 500 MHz	7	1997 a 2000
K7	Athlon	1 (1) 64-bit	100 MHz até 133 MHz	500 GHz até 1.533 GHz	A	1998 a 2001
K9	Athlon II X2	2 (2) 64-bit	720 GHz a 800 MHz	1.9 GHz a 3.2 GHz	LGA 939 e AM2	2005 a 2009
K10	Phenom	3 (4)e 4 (4)	2.000 GHz (HyperTransport)	1.8 GHz a 3.4 GHz	Socket AM2+ e Socket F	a partir de 2009
K11	Phenom II Deneb e Propus	3 (4) e 4 (4)	4.000 GHz (HyperTransport 3.0)	G Nz 2.6 a 3.0 GHz	Socket AM3	a partir de 2009

Outra grande fabricante, a AMD começou a fabricar processadores em 1980, a partir de um clone do chip do 8086 da Intel. Seu primeiro processador criado com tecnologia própria, o **k5**, foi lançado em 1986.

A letra “K” do K5 da AMD vem de Kryptonite (Criptonita), numa referência ao único meio de derrotar o Superman, ou seja, a Intel, que dominava amplamente o mercado.

Logo depois vieram os K6 e os K7 ainda baseados na tecnologia X86. Em 2006 o Athlon64 trouxe um conjunto de instruções estendido utilizando codificação de 64-bit, que foi chamado de AMD64. A tecnologia trouxe alta performance de transmissão de interconexão entre processador e memória,

Como você sabe, a tecnologia de processadores avança rapidamente. Portanto é preciso atualizar-se todo o tempo. Pesquise o tema em sites de busca e visite o site da Intel Corporation, no qual você encontrará informações sobre seus processadores e tecnologias.

por meio da tecnologia Hyper Transport, como parte da arquitetura Direct Connect. A última versão, em 2009, era o K10, com os processadores Phenom, encontrados nas versões dual-core (2 núcleos), triple-core (3 núcleos) e quad-core (4 núcleos). Confira a evolução da tecnologia da empresa na tabela *Alguns modelos de processador AMD*.

10.3. Procedimento de instalação de um processador

Os processadores são comercializados em dois formatos: na versão OEM (somente o chip) e na versão BOX (figura 86), em que o processador é fornecido com dissipador, cooler e elemento térmico, em forma de pasta ou adesivo.

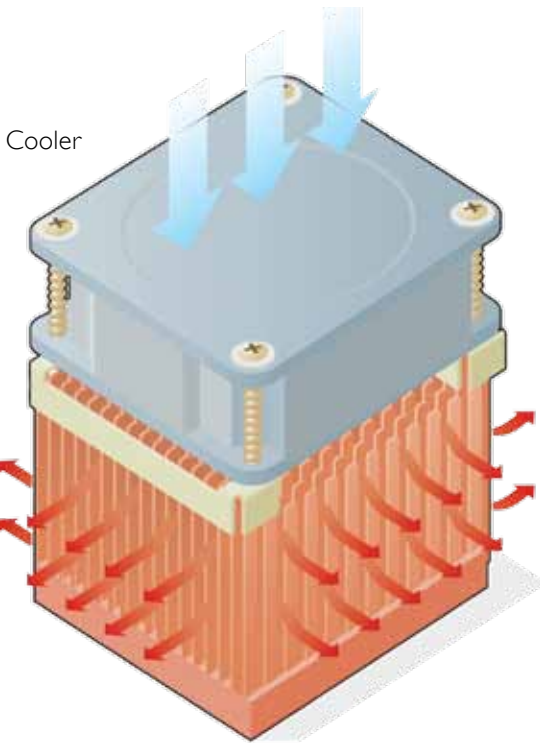
O processador emite muito calor. Nos mais antigos, como o K5 da AMD, a temperatura chegava a até 85 °C. Portanto é preciso retirar essa energia térmica o mais rápido possível para evitar o superaquecimento e eventual queima do equipamento.

O dissipador de calor é uma peça metálica, geralmente de cobre ou alumínio, metais que conduzem bem a energia térmica. Seu papel é remover o calor do processador e conduzi-lo para o ar. Esse dispositivo deve ficar em contato com a maior área possível do processador para que a transmissão de calor seja mais eficiente. Para aumentar a indução de calor, usa-se ainda pasta ou etiqueta térmica, que preenchem os mínimos espaços que possam não estar em contato com o processador.

O cooler, também chamado de fan ou ventoinha, empurra o ar e força sua passagem através do radiador do dissipador, que por sua vez transmite o calor para o ambiente.

Figura 86

Conjunto: processador, dissipador e cooler.



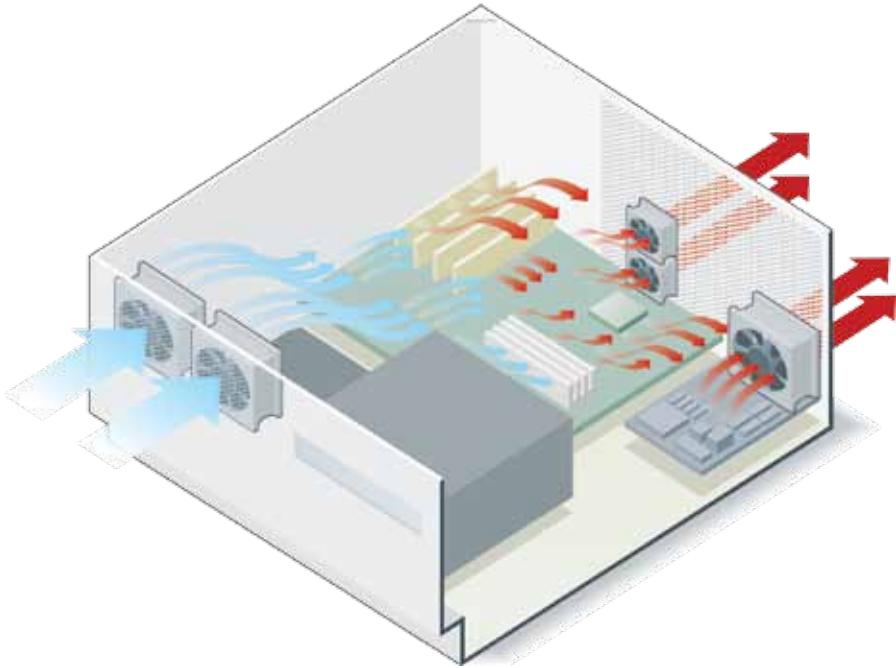
10.4. Refrigeração

Não é somente o processador que gera energia térmica dentro do computador, mas todos os demais componentes, com mais ou menos intensidade. E todo o calor precisa escapar para o ambiente para não danificar o equipamento. É necessário então utilizar um sistema de refrigeração para removê-lo.

Para que o calor saia de um corpo quente, outro corpo mais frio deve fazer contato com ele. Embora seja um isolante térmico, o ar é o elemento mais utilizado para isso, por ser mais fácil, prático e barato colocar grande quantidade de ar em contato com os dispositivos em relação a algumas outras substâncias com mais capacidade de condução de energia térmica, como a água e o nitrogênio. Assim, os gabinetes têm entradas de ar na frente e até do lado oposto à placa-mãe (na tampa). A saída é pela parte de trás. Na parte frontal, fans puxam o ar frio para dentro do gabinete e na posterior sopram o ar quente para fora. Os gabinetes com entrada de ar lateral possuem um cooler que sopra o ar frio diretamente sobre o cooler do processador. A ventoinha da fonte de energia também sopra o ar quente produzido pela própria fonte, mas ajuda a expelir o ar de dentro do gabinete (figura 87).

Figura 87

Fluxo de ar por dentro do gabinete.





# Capítulo II

## Áudio, vídeo e jogos

- Vídeo
- Áudio

Equipamento de uso geral, o computador foi evoluindo para se adequar às várias necessidades do uso. Com o passar do tempo, os preços foram baixando e o computador passou a ser empregado também fora do trabalho – para auxiliar nas tarefas domésticas e escolares e, cada vez mais, para diversão. Equipamentos profissionais específicos para mixagem de áudio e vídeo migraram para o meio digital e também começaram a ser manipulados no computador.

As estações multimídias tornaram-se comuns. Surgiram então várias tecnologias, como placas de vídeo 3D para jogos e vídeo, placas de áudio com mais canais para home-theater, placas de TV, leitores e gravadores de CD e DVD.

Também os softwares tornaram-se cada vez mais complexos e passaram a produzir efeitos cada vez mais reais. Aliás, o conceito da casa inteligente, controlada totalmente por computador (veja o quadro *Tecnologia e sofisticação*), só cresce no ambiente da arquitetura e construção civil.

Para que tudo funcione como o usuário espera, é preciso conhecer em detalhes as tecnologias que estão por trás dos equipamentos.

II.1. Vídeo

As game station, como são chamados os computadores montados para os aficionados em jogos virtuais, precisam de placa de vídeo com processador e memória dedicados e que implementem as melhores tecnologias para esse tipo de uso.

As máquinas usadas para gerar sinal para TVs LCD ou plasma, para assistir TV digital ou filmes em discos Blu-Ray, que trabalham com alta-definição de imagem, também merecem placa de vídeo especial.

Estamos falando das chamadas placas aceleradoras de vídeo (conforme é possível observar na figura 88), que são capazes de desenhar maior quantidade de telas por segundo (fps ou frames por segundo) em alta-definição e armazená-las em maior quantidade, sem que seja necessario recorrer ao processador nem à memória principal do computador.



Figura 88  
Placa de vídeo  
MSI Force 9600GT  
com 2 Gb  
de memória GDDR3.

Essas placas costumam ter saída HDMI para TVs HD (High Definition, ou Alta Definição) e conectores DVI, HDMI, Displayport e/ou Firewire, como mostra a figura 89.

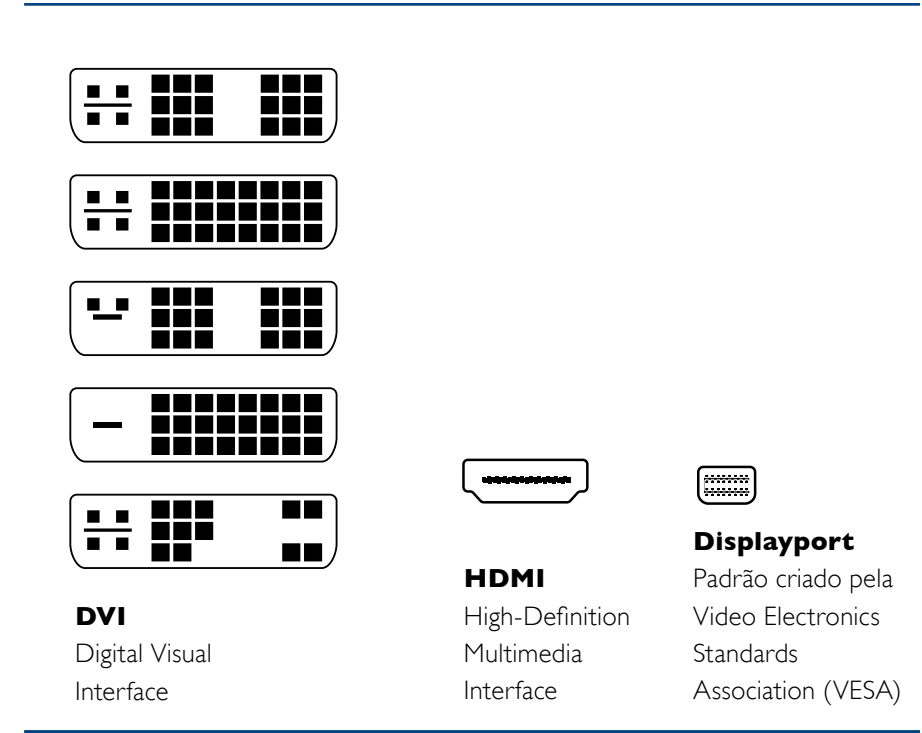


Figura 89  
Conectores  
de vídeo.



# Tecnologia e sofisticação

Já pensou nunca mais ter de pensar na chave de casa? Nem ter de se preocupar em abrir ou fechar persianas ou em acender e apagar as luzes? A cada dia, mais e mais brasileiros desfrutam dessas maravilhas tecnológicas. Isso porque boa parte das grandes construtoras e incorporadoras oferece um leque cada vez maior de casas e apartamentos automatizáveis.

Os imóveis podem ser entregues com fechaduras biométricas - aquelas que se abrem mediante a leitura das digitais dos moradores -, com sistema completo de segurança, além de infraestrutura para receber todo tipo de sistema inteligente para o controle de equipamentos eletroeletrônicos, home theater, ar condicionado. Tudo funcionando de maneira programada ou a um simples toque do proprietário.



**Figura 90**  
Controle principal de uma casa controlada por computador.



**Figura 91**  
Detalhe de  
entradas de áudio  
na placa-mãe.

## 11.2. Áudio

Processar música no computador não é algo tão complicado e nem mesmo exige instalação de placa adicional. Uma música com boa qualidade gravada em formato MP3 não consome mais do que 3 Mb e é facilmente processada por aparelhos de celulares e mp3. As placas-mãe trazem on-board tecnologias de ponta para transmitir som de ótima qualidade para aplicação em aparelhos home-theater, por exemplo. A ideia por trás das tecnologias mais modernas em desenvolvimento no fim da década de 2010, como 5.1 Surround, da empresa Dolby, e o áudio 22.2, em teste no Japão, é transmitir mais canais, que por sua vez controlem independentemente vários alto-falantes, tentando simular um ambiente real.

# Capítulo 12

## Monitores

- Resolução
- Monitores CRT
- LCD
- OLED



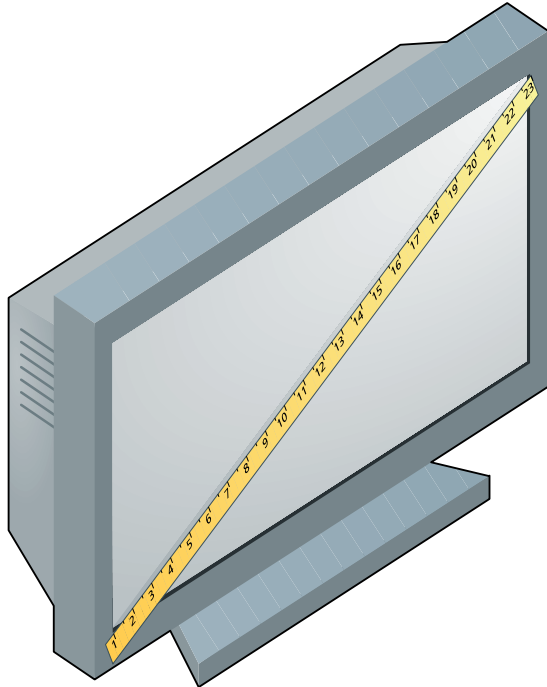


Os seres humanos são fascinados por imagens animadas. Basta lembrar o sucesso do surgimento do cinema e da televisão – que se tornou sonho de consumo em todo o mundo desde as primeiras transmissões, na década de 1930. Assim que são lançadas, as novas tecnologias de vídeo ganham mercado rapidamente, em detrimento de suas antecessoras. A TV analógica, por exemplo, está desaparecendo – no Brasil, passamos pelo processo de conversão para a TV digital e, nos Estados Unidos, o sinal analógico nem existe mais.

Com os computadores não é diferente. Os primeiros modelos vinham equipados com monitores CRT do mesmo padrão dos televisores. Hoje em dia, os monitores são cada vez mais levados em consideração pelo consumidor na hora de comprar um computador pessoal ou mesmo uma estação de trabalho.

Figura 92

As telas dos monitores são medidas em polegadas, na diagonal.



12.1. Resolução

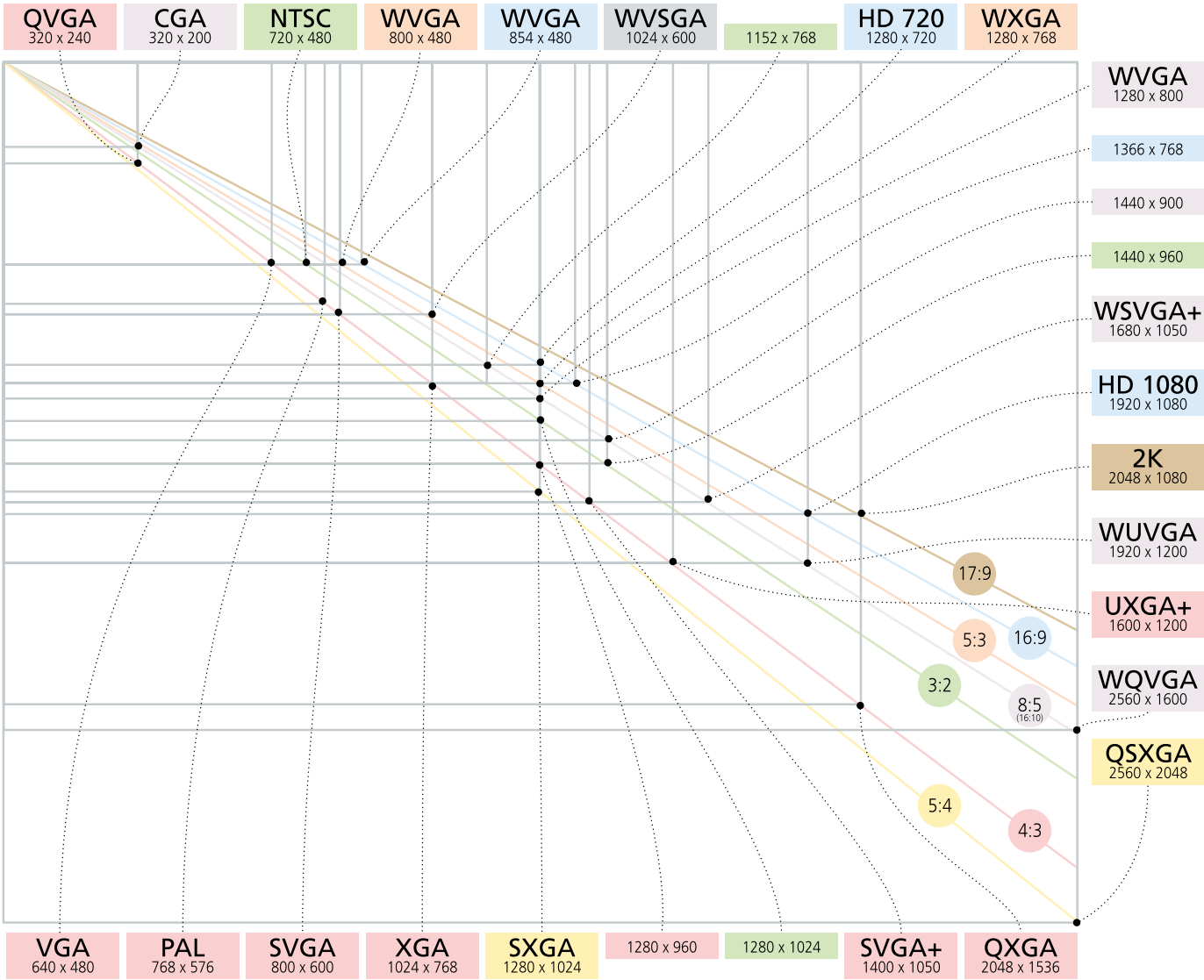
As telas dos monitores são medidas em polegadas, pela diagonal (figura 92). Os monitores CRT costumam ter telas de 14, 17 e 21 polegadas, por exemplo. Mas sua resolução é definida por pixels, que representam a quantidade de pontos, que é capaz de produzir. Expressamos uma resolução informando a quantidade de pixels na horizontal pela quantidade de pixels na vertical. O modo padrão é 800x600 – 800 pixels no eixo X (horizontal) e 600 no eixo Y (vertical). Veja outros exemplos na figura 93.

12.2. Monitores CRT

Embora seja bem antiga, a tecnologia para monitores CRT (Catodic Ray Tube, ou Tubo de Raios Catódicos) evoluiu bastante. Por muito tempo a

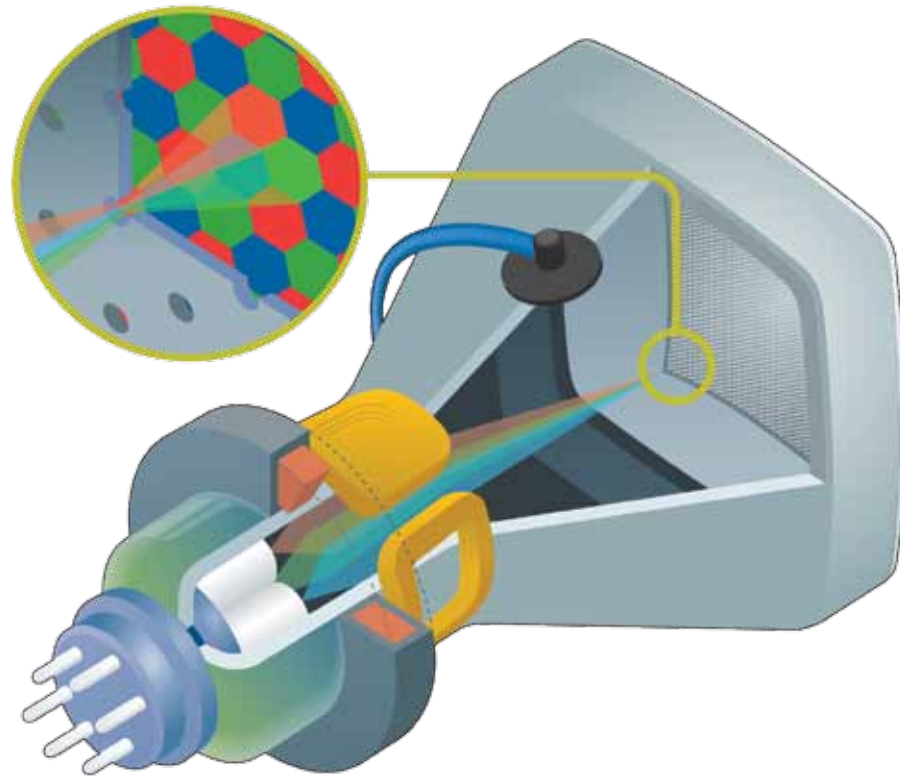
Figura 93

Resolução de monitores.



**Figura 94**

Células da tela do monitor CRT emitem luz em cores.



CRT dominou o mercado de televisores e monitores de computador, até porque, com a consolidação do processo de fabricação, seus preços caíram bastante. Porém, os produtos que utilizam essa tecnologia também devem desaparecer, dando lugar a outras mais recentes, como LCD, Plasma e OLED. Estas últimas vêm ganhando mercado a cada dia, e em consequência seus preços se tornam mais competitivos.

No monitor CRT, pequenas células da tela emitem luz, em cores (figura 94). São células de fósforo presas à superfície interna. A tela se estende para dentro da caixa do monitor, formando um tubo, em cuja extremidade oposta um canhão de elétrons dispara em direção à superfície da tela. Quando esses elétrons se encontram com as células de fósforo, há uma reação, que produz luz. As cores são obtidas a partir da variação da tensão desses elétrons.

Apenas um feixe de elétrons é necessário para pintar toda a tela. Como as células de fósforo se apagam depressa, esse feixe deve correr a tela rapidamente, linha a linha, de cima até embaixo. O tempo que o feixe leva para pintar uma tela deve ser rápido o suficiente para que os olhos humanos não consigam perceber o fenômeno. Dizer que um monitor trabalha com taxa de atualização de 75 Hz significa que ele desenha 75 telas por segundo. As taxas de atualização podem variar de 50 Hz, 60 Hz a 75 Hz, dependendo do tipo de cada monitor.

### 12.3. LCD

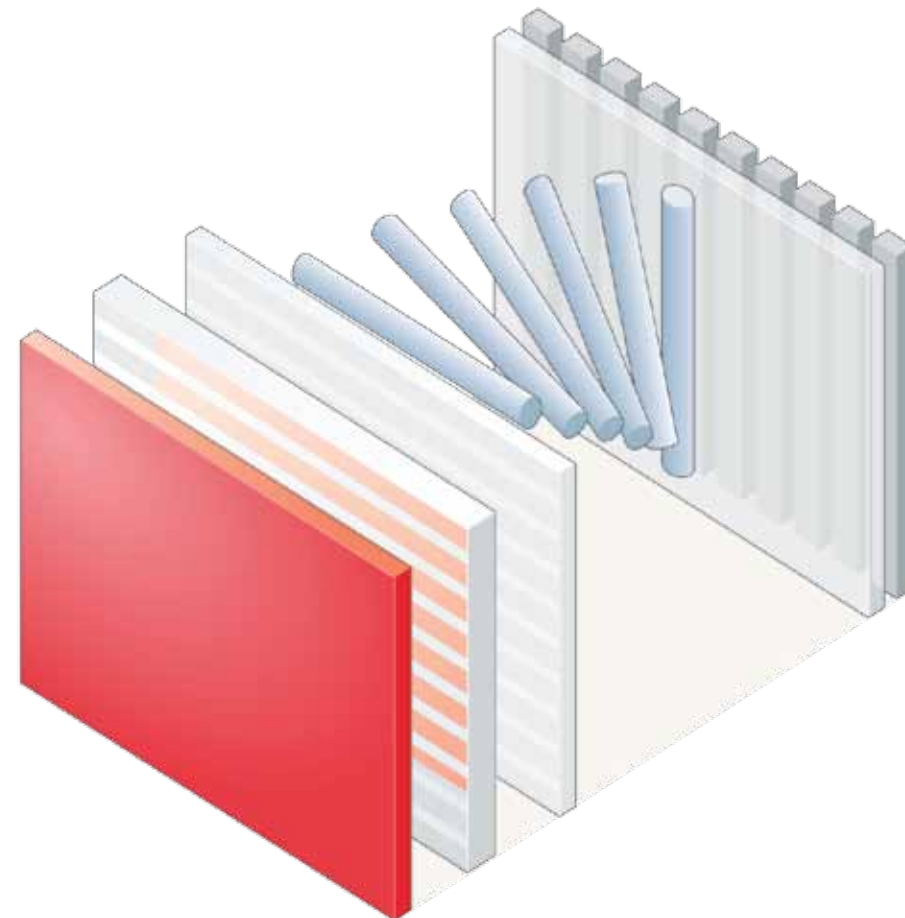
As pesquisas da tecnologia LCD (Liquid Crystal Displays, ou Tela de Cristal Líquido) começaram em 1963, nos Estados Unidos, com Richard Williams e George Heilmeyer. Em meados dos anos 1970, surgiram as telas LCD minúsculas, geralmente monocromáticas, para relógios de pulso e equipamentos eletrônicos. Na década de 1980 surgiram telas maiores, para equipar, por exemplo, notebooks de até 14 polegadas. A produção de LCD era onerosa porque a taxa de telas perdidas durante a fabricação era alta – a maioria tinha problemas com pixels defeituosos. Mas o processo de produção foi se aperfeiçoando e, a partir dos anos 1990, a tecnologia se tornou mais acessível, o que possibilitou o lançamento de telas de grandes dimensões.

A tecnologia LCD utiliza a substância chamada cristal líquido para bloquear ou dar passagem à luz. As partículas de cristal líquido têm a propriedade de se agruparem quando a substância é submetida a uma tensão elétrica, evitando a passagem de luz.

A tela LCD é formada por duas placas de vidro que possuem sulcos paralelos. Em uma das placas, os sulcos são verticais e na outra, horizontais (figura 95). Os

**Figura 95**

Tela LCD.





sulcos são preenchidos com cristal líquido e equipados com um circuito elétrico que leva corrente até cada uma das células identificadas pela intersecção das linhas com as colunas.

Em uma tela colorida são necessárias três células, uma para cada cor. A iluminação é feita por uma placa posicionada atrás da tela, que envia a luz através do vidro mais interno, o qual alinha os feixes de luz na mesma direção dos seus sulcos. Quando atravessa uma célula com cristal líquido que recebeu tensão, o feixe de luz é desviado 90°, mudando sua posição de horizontal para vertical e coincidindo com a ranhura da segunda placa de vidro, de modo a permitir a passagem da luz. Se não for aplicada nenhuma corrente, o raio de luz não será desviado e não conseguirá passar pela segunda placa de vidro.

As backlights, ou seja, as lâmpadas fluorescentes de catodo frio, que emitem luz por trás da tela LCD, não o fazem de modo uniforme e costumam variar sua luminosidade nas áreas próximas das extremidades. Além disso, não conseguem escurecer totalmente o pixel para imagens escuras porque a lâmpada está sempre acesa. Para solucionar esse problema foram criadas LCDs com iluminação por LEDs. LEDs são pequenas lâmpadas que podem ser controladas uma a uma e variar sua luminosidade até se apagarem por completo numa imagem totalmente escura. Isso eleva imensamente a qualidade de contraste em relação à da tela LCD comum.

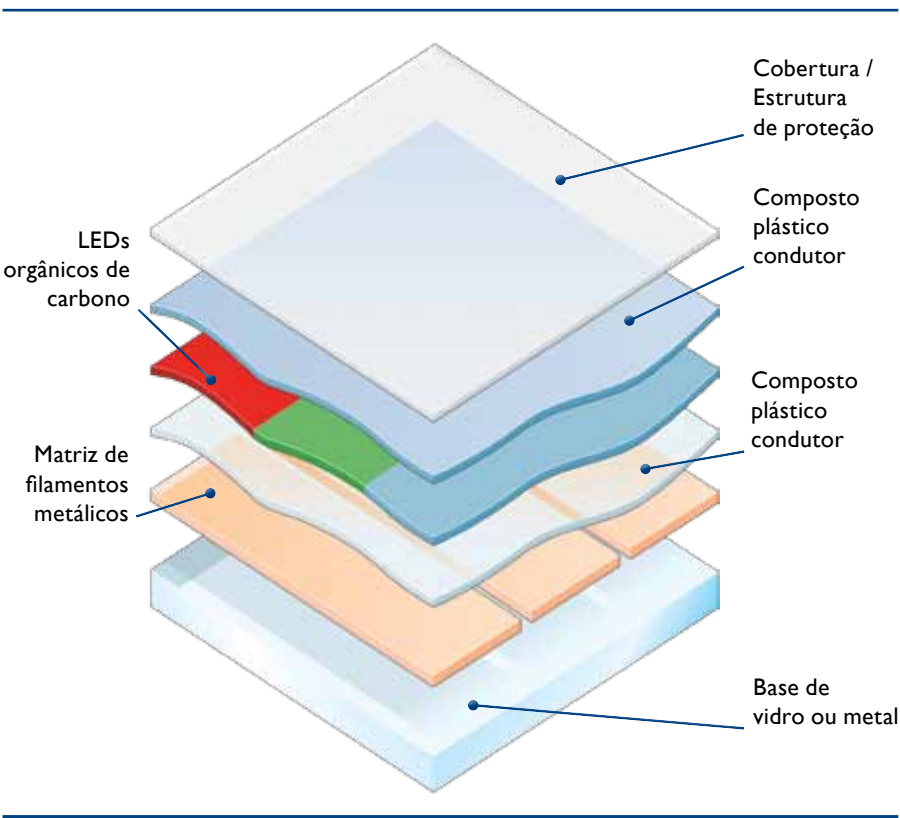
12.4. OLED

A última inovação em monitores no fim de 2009 era a tecnologia OLED. Por

permitir o uso de telas superfinas, proporcionou melhoria expressiva na qualidade de imagem (figura 96).

OLED significa Organic Lighting Emmiting Diode, ou seja, Diodo Orgânico Emissor de Luz. Diferentemente de LCD, OLED não requer lâmpada, pois os diodos que compõem as células dos pixels contêm material orgânico (à base de carbono) que emitem luz ao receberem tensão elétrica. Mas há desvantagens: o preço ainda é alto e o tempo de vida útil dos componentes orgânicos, reduzido em relação aos que integram as telas LCD, as quais podem funcionar continuamente por 60000 horas. No início as telas de OLED trabalhavam até 2000 horas apenas, mas em 2009 já duravam até 50000 horas.

Figura 96  
Camadas do monitor OLED.



# Capítulo 13

## Setup

- Main (Principal)
- Advanced (Avançado)
- Power (Energia)
- Boot
- Security (Segurança)
- Exit (Saída)





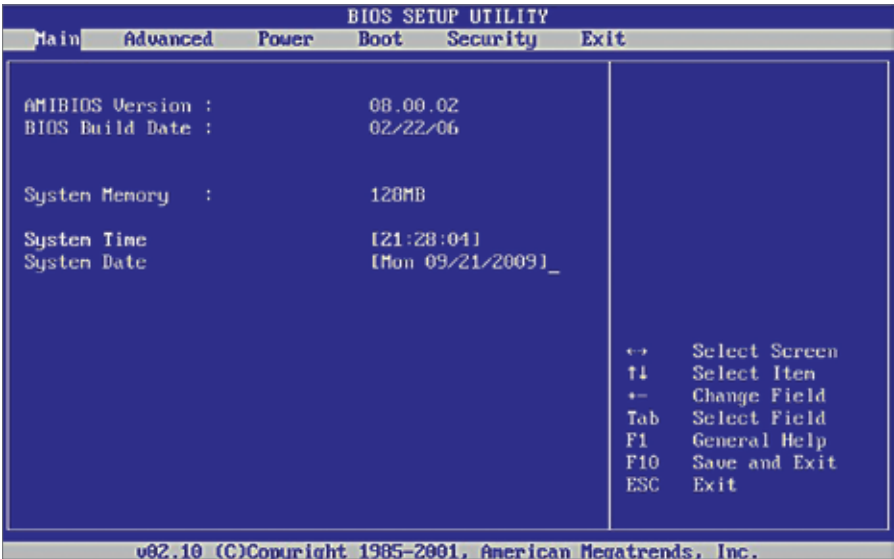
setup é um programa de configuração que todo micro tem, gravado dentro da memória ROM (que, por sua vez, fica na placa-mãe). Em geral, para acionarmos esse programa pressionamos repetidamente a tecla Del ou F2, dependendo do fabricante do BIOS, durante a contagem de memória.

As principais configurações do setup são para: reconhecimento de discos IDE, sequência de tentativas de Boot, alterar senha de acesso ao setup do computador e configurar diversas opções da placa-mãe.

Cada um dos vários fabricantes de BIOS adota seu próprio programa de configuração da CMOS. Portanto, as telas que exibiremos neste livro para exemplificar poderão ser diferentes das que você encontrará em outros computadores. Porém, as funcionalidades são basicamente as mesmas e os termos bem parecidos.

Figura 97

Tela principal do Setup do BIOS.



13.1. Main (Principal)

Geralmente é a primeira opção no setup (figura 97) e tem função de configurar a data e hora, exibir a versão do Firmware do BIOS e sua data de fabricação. Mostra também a quantidade de memória identificada pelo BIOS.

13.2. Advanced (Avançado)

Este menu nos leva até outros três sub-menus – identificação de HDs IDE, configuração das unidades de Discos Flexíveis (Floppy-Disk) e configurações de Boot.

Ao acessar o menu de configuração IDE, as versões mais recentes de Setup costumam tentar detectar automaticamente os discos e exibi-los quando são identificados na frente da descrição do canal IDE correspondente. Observe a figura 98. Ela mostra que nesse caso foi detectado somente o CDROM na IDE secundária, ou seja, que a unidade está conectada no 2º slot da placa, na posição MASTER do cabo Flat.

Quando a opção PCI IDE BusMaster ou, em outras versões de Setup, a Enable Ultra-DMA, que é a mesma, estão desabilitadas, o BIOS não carrega os drivers de 16-bits busmastering. Com isso, a controladora não é capaz de utilizar a capacidade Ultra-DMA. O DMA é uma tecnologia implementada nas placas-mãe que faz com que a transmissão de dados entre o disco rígido e outras interfaces, como memória, placa de rede, outros discos etc. seja direta, sem sobrecarregar o processador. Com essa opção desabilitada o trabalho de ler de um dispositivo e escrever em outro é todo do processador.

A configuração de Floppy (figura 99) é idêntica à das unidades IDE. O Setup vai identificar e mostrar as duas unidades, A e B, indicando qual está conectada com o hardware.

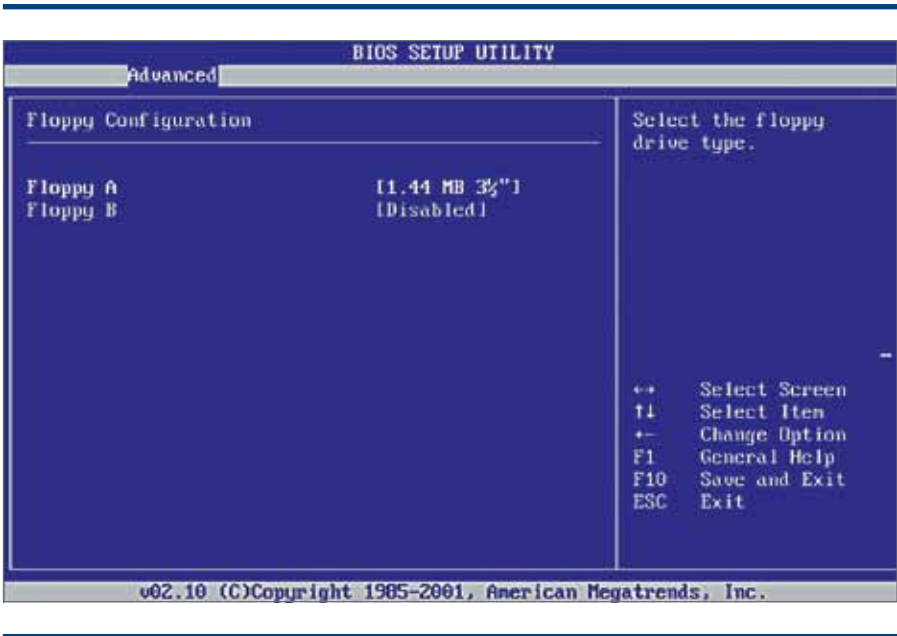
Figura 98

Menu configuração IDE.



Figura 99

Configuração das unidades de discos flexíveis.



A tela de configurações de Boot pode trazer opções como Quit Boot (figura 100), que eventualmente exibe o logo do comercial do fabricante ou da montadora, por exemplo, em vez de mostrar a sequência de POST padrão. Por meio do Bootup Num-lock, dizemos ao BIOS se o num-lock do teclado deve estar habilitado ou não quando a máquina for iniciada.

13.3. Power (Energia)

Este menu (figura 101) permite que seja habilitado o controle de energia APM (Advanced Power Management, ou Gerenciamento Avançado de Energia), que faz com que o BIOS peça à fonte para desligar o computador, após o sistema operacional ter sido descarregado.

Figura 100

Opção Quit Boot da tela de configurações de Boot.

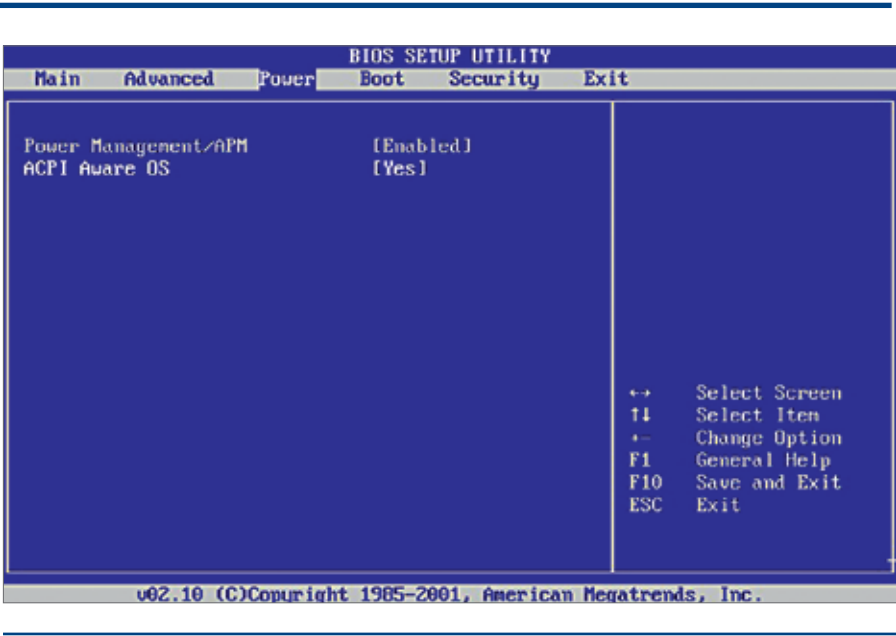


Figura 101

O menu Power facilita o controle de energia.

O ACPI Aware OS transmite informações sobre os dispositivos da placa-mãe para o sistema operacional, de modo que este possa fornecer funcionalidades de controle de energia. Essa opção é muito utilizada em notebooks.

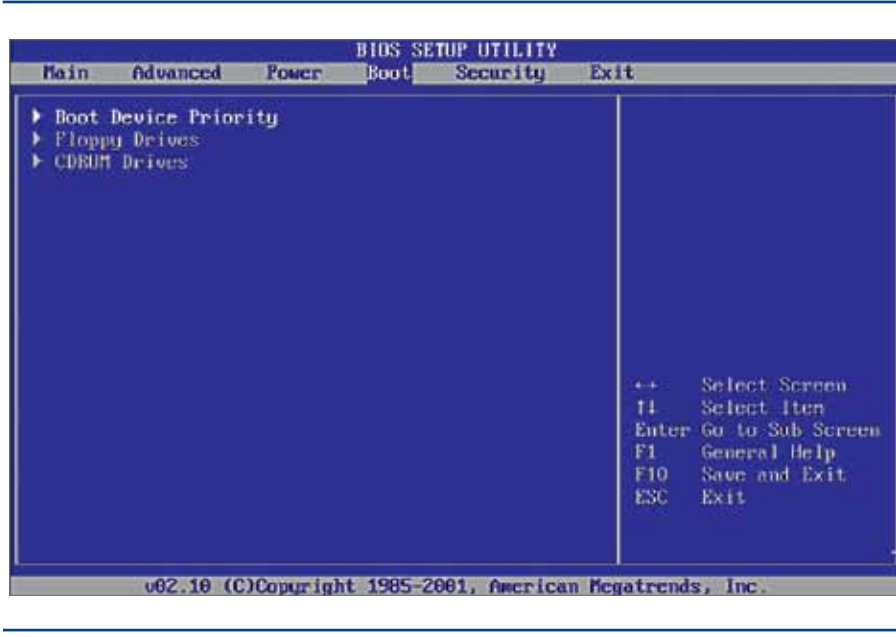
13.4. Boot

Em Boot, configuramos a prioridade de Boot (figura 102). Ou seja, determinamos em qual sequência o BIOS irá procurar por um disco com sistema operacional instalado e capaz de dar Boot.

Quando o sistema operacional já está instalado, voltamos os discos IDE para a primeira opção, para que o processo de Boot seja mais rápido e não

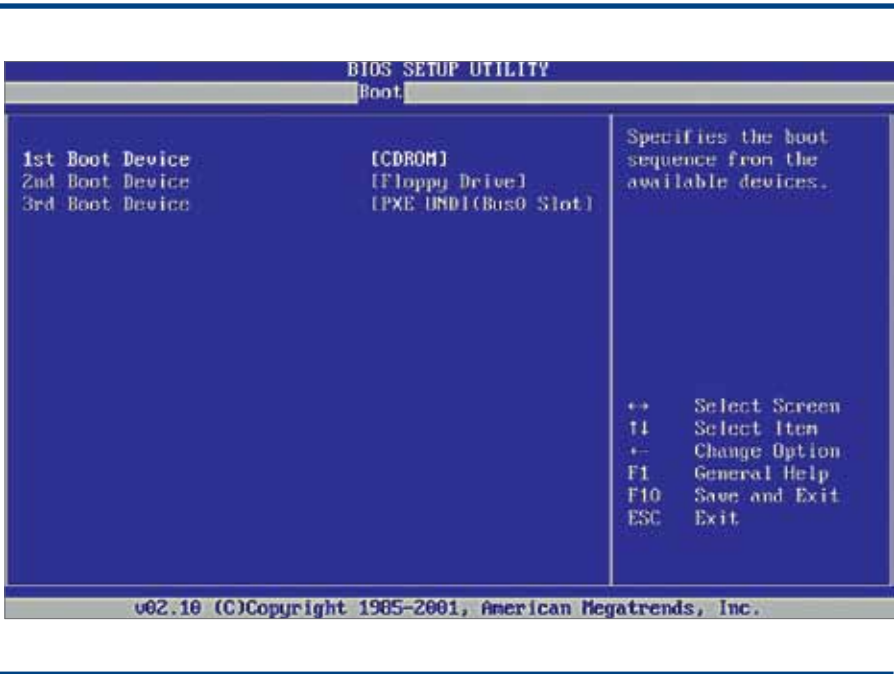
Figura 102

Configurando a prioridade Boot.





**Figura 103**  
Seleção da  
sequência de Boot.

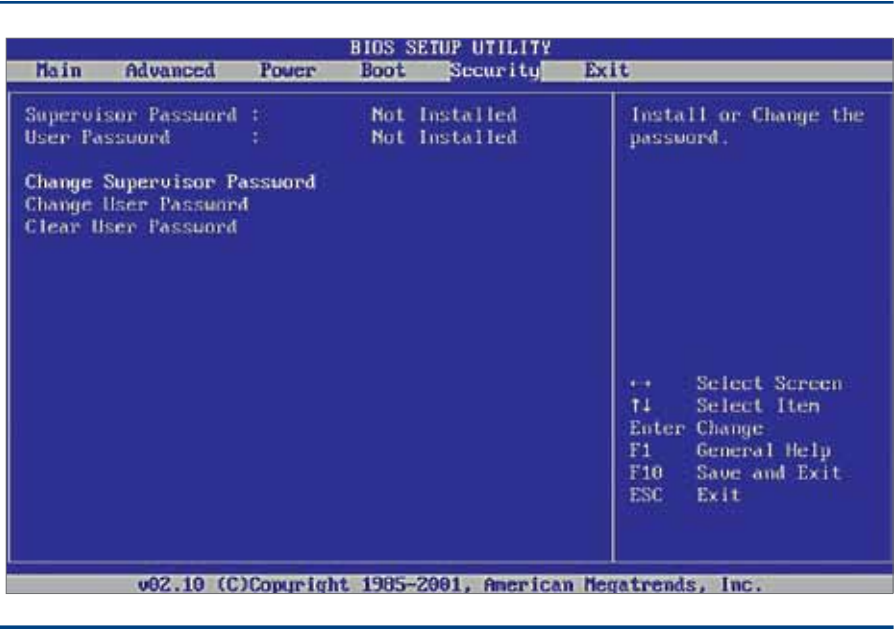


fique testando outras unidades. Porém, quando instalamos um novo sistema operacional devemos primeiramente jogar a unidade de CD, caso estejamos utilizando uma instalação gravada em um CD ou DVD. Dessa forma, podemos garantir que será carregado o conteúdo dessas mídias, e não um outro, eventualmente danificado, que possa já estar gravado no disco IDE.

13.5. Security (Segurança)

A tela Security nos permite registrar uma senha de acesso à configuração do setup para, dessa maneira, evitar que terceiros possam alterar indevidamente as configurações do BIOS (figura 104).

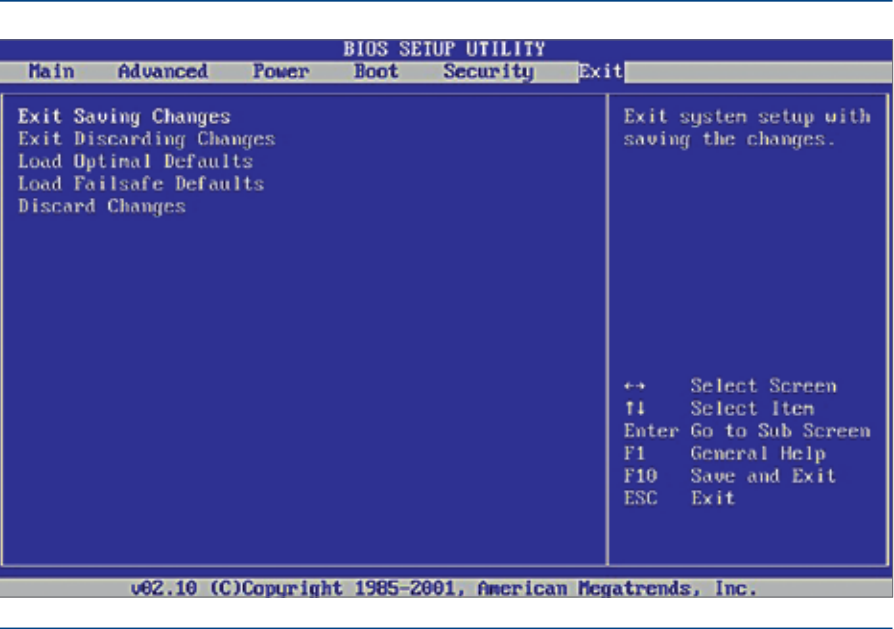
**Figura 104**  
Tela para configuração  
de segurança.



13.6 Exit (Saída)

Finalmente, no menu Setup (figura 105), temos as seguintes opções: sair e salvar as novas configurações; sair sem modificar nada; carregar as opções padrão de máxima performance; carregar as configurações padrão para evitar falhas (ou seja, funções avançadas são desabilitadas); descartar as alterações sem sair.

**Figura 105**  
Opções do  
menu Setup.



# Capítulo 14

## Instalação de dispositivos

- Manual
- Softwares controladores (drivers)
- Métodos de instalação no sistema operacional
- Instalação de outros periféricos



Novas funcionalidades podem ser adicionadas a um computador, por meio de placas de expansão, ou conectadas a portas específicas ou portas USB. O encaixe físico geralmente é fácil. Precisamos apenas verificar se o tipo de encaixe da placa é compatível com o de conexão do dispositivo, pois geralmente não é possível conectar dispositivos de conectores diferentes.

14.1. Manual

A primeira providência ao instalar um novo dispositivo é ler o manual que o acompanha. Ali, você encontra informações sobre o funcionamento do equipamento, sua compatibilidade com outros hardwares, chipsets e sistemas operacionais, configurações preliminares, bem como todos os passos para sua instalação. Por meio da leitura do manual podemos prevenir e corrigir vários problemas, evitar que a instalação fique prejudicada ou incompleta e garantir o desempenho esperado do dispositivo. No manual geralmente encontramos as soluções para problemas conhecidos, as limitações e todos os dados técnicos necessários para a configuração dos programas que utilizarão o dispositivo.

14.2. Softwares controladores (drivers)

A parte geralmente mais complexa, que toma mais do tempo empregado com a instalação de dispositivos, é a instalação dos softwares e drivers que os controlam. O sistema operacional, seja Windows, Linux ou qualquer outro, necessita de um software para intermediar a comunicação com o aparelho. Sempre que o sistema operacional precisa de uma função do hardware, solicita ao driver que a execute.

O driver é um tradutor que sabe os comandos que o sistema operacional pode enviar, interpreta-os e converte a solicitação de modo que o chip do aparelho possa reconhecê-la. Assim, componentes compatíveis podem ser desenvolvidos por vários fabricantes, que também podem funcionar em vários sistemas operacionais, alterando apenas o software controlador (driver).

Drivers (pilotos) geralmente são distribuídos em disquete que vêm junto do hardware, em CDs, DVDs ou por links na internet. Placas que vêm integradas na motherboard

são instaladas por meio dos drivers fornecidos junto com o equipamento, e podem ser diferentes dos modelos encontrados no site do fabricante. A leitura do manual é importante nesse momento, pois nos orienta quanto à sequência de instalação dos drivers e informa se estes devem ser instalados antes ou depois do hardware ser conectado. Placas de expansão costumam ser conectadas antes da instalação dos drivers, enquanto dispositivos USB devem ter seus drivers instalados previamente para que o sistema operacional possa reconhecê-los corretamente (figura 106).

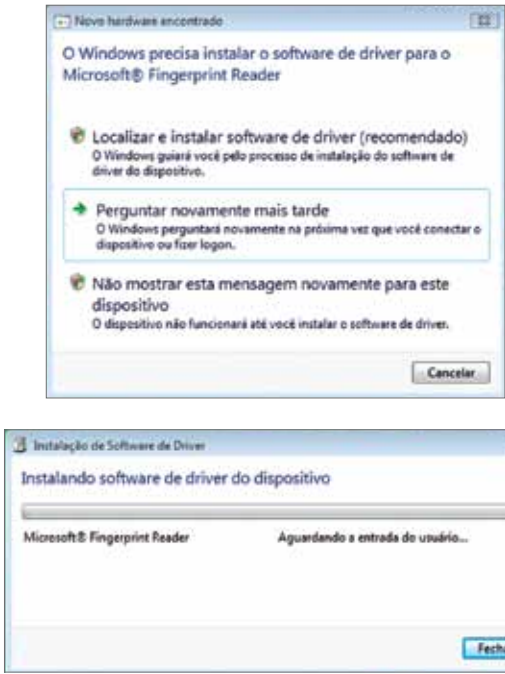
14.3. Métodos de instalação no sistema operacional

Cada sistema operacional possui técnica própria para realizar a instalação de drivers. E nem todos os dispositivos têm controladores para todos os sistemas operacionais ou tecnologias. Um bom exemplo é a compatibilidade com sistemas operacionais 64-bits, para os quais nem todos os fabricantes implementam drivers. Há dificuldades também no Linux. Muitas vezes é preciso procurar drivers de terceiros para conseguir instalar dispositivos, que podem não funcionar tão bem quanto deveriam. Também pode ocorrer falta de softwares controladores compatíveis com dispositivos mais antigos para sistemas operacionais novos.

14.3.1. Windows

Como é o sistema operacional mais popular no mundo, há uma grande quantidade de dispositivos compatíveis com o Windows. A grande maioria segue os padrões dos drivers genéricos, que já vêm na instalação do sistema operacional. Ou seja, muitos dispositivos são reconhecidos e instalados automaticamente sem necessidade de nenhuma tarefa adicional. Essa técnica, chamada plug'n play (conecte e use), é encontrada desde a versão 95 do Windows e tem seu ápice na versão XP, que é capaz de operar com quase todos os dispositivos existentes.

Figura 106  
Reconhecimento de novo dispositivo USB.



A figura 106 mostra o Windows Vista reconhecendo um dispositivo conectado via USB. Veja que o sistema solicita a localização do driver para prosseguir a instalação.

Dispositivos que são instalados por meio de placas de expansão devem ser conectados com a máquina desligada. O Windows mostrará o assistente de instalação de novos dispositivos somente no momento em que o sistema operacional reiniciar. Mas lembre que isso só vale para dispositivos plug'n play.

### 14.3.2. Linux

O Linux não tem uma tecnologia padrão para reconhecimento automático de dispositivos. Algumas distribuições mais amigáveis, como Ubuntu, trazem mais drivers e scripts prontos para fazer o reconhecimento parecer bem automático, mas, mesmo assim, algum hardware pode dar trabalho, principalmente em notebooks. Neste caso a solução é procurar ajuda em fóruns da internet para tentar encontrar a solução.

### 14.3.3. Descobrir a marca e o modelo de dispositivos

É comum que os donos de computadores não tenham o cuidado de guardar os CDs com os drivers. Também os manuais podem ser perdidos ou jogados no lixo. Em muitos casos o programa de instalação do driver pode perguntar qual o modelo do dispositivo que se quer instalar. Fabricantes costumam compilar instaladores comuns para vários dispositivos, e nesse momento precisamos saber exatamente qual o modelo certo a ser instalado. Diante dessa situação temos duas alternativas: abrir a máquina e procurar o número FCC-ID (Código de Identificação no Federal Trade Commission – Comissão Federal de Comércio dos EUA), que deve ser encontrado em alguma etiqueta ou impresso na placa, ou efetuar a pesquisa com esse número no site de busca do FCC (<http://www.fcc.gov/searchtools.html>). A alternativa mais recomendada é a utilização de softwares de reconhecimento como o Aida32, Hardware INFO, Fresh Diagnose, SISOFT Sandra, HWInfo, PCWizard, Astra 32, Belarc Advizor e, em especial, o Everest. Porém, este último não é gratuito. Uma opção grátis é o Belarc Advisor.

Depois de encontrado o fabricante e o modelo, devemos ir à página da internet do fabricante e localizar os drivers e softwares para o dispositivo que o software de reconhecimento identificou.

Abrir a máquina deve sempre ser a última opção, pois pode ser necessário remover algum lacre. Mas, para ler o FCC-ID de uma placa de expansão, esse procedimento será necessário. É importante saber que isso poderá acarretar problemas como mau contato e até perda da garantia do fabricante para outros defeitos o que o cliente eventualmente irá atribuir a você.

## 14.4. Instalação de outros periféricos

### 14.4.1. Teclado

Existem várias configurações de teclado, que variam na quantidade de teclas, no código que a tecla representa e no idioma. No Brasil temos dois padrões, o



**Figura 107**

Teclados com padrões ABNT têm teclas que representam a cedilha (ç). Nos demais, como o da figura abaixo, é possível gerar o ç com a combinação de duas teclas.

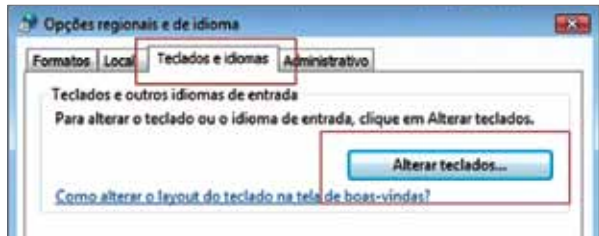
ABNT e o ABNT2, mas também encontramos teclados importados que seguem outros padrões, principalmente em notebooks. Os padrões ABNT e ABNT2 são preparados para o idioma português do Brasil e possuem teclas para representar a cedilha (ç) (figura 107). Os teclados que não têm essa tecla conseguem gerá-la através da combinação “vírgula + c”. Se o teclado conectado ao computador não estiver devidamente configurado, produzirá letras no editor de textos diferentes das que a tecla estiver indicando. Para configurar o sistema operacional Windows para esse teclado vá até a opção Painel de Controle. Comece pelo botão Iniciar e escolha o ícone Opções Regionais. Localize a aba Teclados e Idiomas, e clique no botão Alterar Teclados (figura 108).

Clique no botão adicionar e escolha o Idioma, no nosso caso Português (Brasil), e o layout do teclado que estiver utilizando. Como exemplo foi selecionado Português (Brasil – ABNT2) (figura 109 A). Teclados de notebook ou importados costumam utilizar o layout Estados Unidos (internacional). A nova configuração entrará na lista de Serviços instalados e só estará ativa depois que for selecionado Idioma de Entrada Padrão (figura 109 B).



Figura 108

Selecionando idioma do teclado.



14.4.2. Mouse

O primeiro protótipo de mouse foi criado em 1963, pelo inventor norte-americano Douglas C. Engelbart, um dos pioneiros da área de informática.

O **mouse** é um dispositivo apontador. Serve para mostrar ao sistema operacional o que se deseja fazer, indicando, através do cursor no vídeo, o elemento com o qual se quer interagir e que tipo de ação se pretende realizar. O mouse (figura 110) é composto basicamente de dois botões e uma roda. Em cada sistema operacional e em cada software pode haver um tratamento especial para cada evento nos controles do mouse. Geralmente o botão esquerdo serve para clicar e selecionar objetos, e o direito, para acessar ações que se podem executar, por meio de menus popup. A roda é usada em telas de programas cujo conteúdo ex-

cede sua capacidade, que apresentam uma barra de rolagem para movimentá-lo, assim como acontece em editores de texto e navegadores da web. A instalação do mouse não demanda maiores cuidados, pois a grande maioria dos modelos encontrados no mercado funciona com os drivers genéricos distribuídos junto com a instalação do Windows e nas distribuições Linux mais populares. As exceções são os modelos mais sofisticados, como mouses sem fio ou dotados de mais botões, que são fornecidos com alguma mídia para distribuir o instalador do driver.

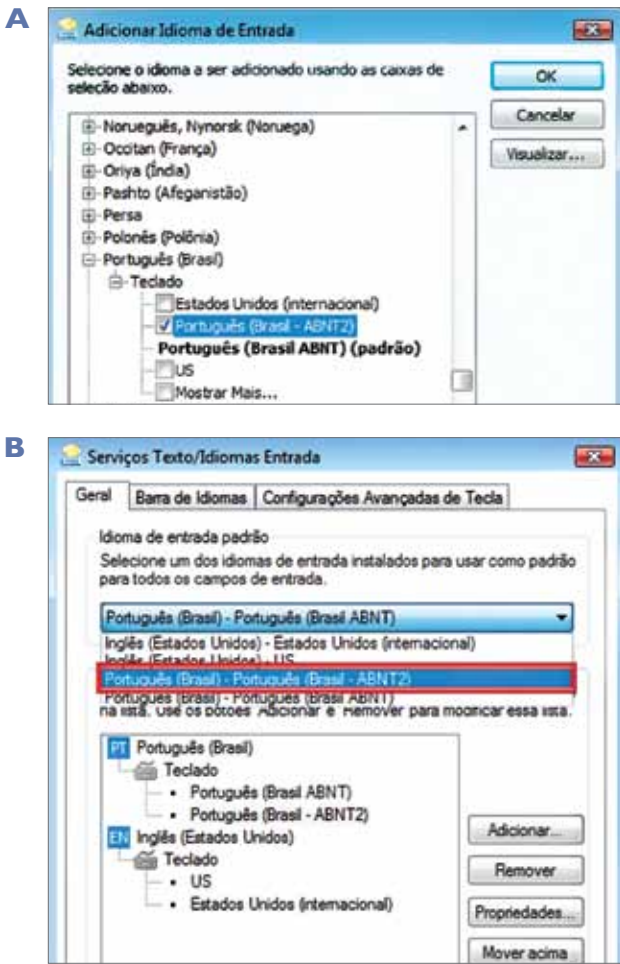
Figura 110

Mouse.



Figura 109

Opção Português do Brasil.



# Capítulo 15

## Redes de computadores

- O que são redes
- Questões sociais
- Segurança



que garante qualidade de vida à maioria dos seres humanos atualmente são as redes. Se olhar ao seu redor, você facilmente identificará várias. A água passa por redes até chegar a sua casa, assim como a energia elétrica, que é transportada, por exemplo, desde Itaipu, no Paraná, até as residências de milhões de pessoas em todo o Brasil. E há ainda as redes de transportes, de saúde pública, entre várias outras. Analisando esse cenário, podemos nos perguntar qual seria a função de uma rede, e deduzirmos que, certamente, se relaciona à oferta de serviços. Redes, enfim, são meios para disponibilizar recursos importantes para as comunidades. Sem redes, teríamos de buscar água em fontes, manter geradores domésticos de energia – e só isso já demonstra o quanto esse método facilita nossa vida.

15.1. O que são redes

Podemos definir rede como uma infraestrutura em malha que interliga vários pontos, de modo que um fornecedor de recursos possa transmiti-los até seus consumidores.

No caso das redes de computadores, o recurso é a informação. As redes possibilitam que esse recurso, disponível em uma máquina, seja distribuído a outros computadores interligados e com permissão para acessá-lo. Os serviços relacionados podem capturar um arquivo em outra máquina, solicitar impressão de um texto à impressora da mesa vizinha, enviar ou receber um e-mail e acessar páginas na internet.

15.2. Questões sociais

Muitas pessoas dizem que não saberiam mais viver sem internet por causa das facilidades e da economia de tempo que a rede proporciona. Hoje não precisamos mais ir ao banco, por exemplo. Por meio da web, podemos conferir nossos extratos bancários e quitar contas. Sequer precisamos andar com dinheiro na carteira: podemos pagar nossas compras com cartões magnéticos – a liberação do pagamento é feita pela rede da operadora de cartões, através da rede de telefonia ou da internet. Com isso as estruturas das agências bancárias puderam diminuir, assim como seu quadro de funcionários. Se nos faltassem as redes, como os bancos poderiam nos atender? Seria o caos. Já podemos até fazer cursos de todos os tipos à distância, sem precisar sair de casa. E ainda trabalhar, nos

divertir, matar a saudade de amigos e familiares ou mesmo nos relacionar com outras pessoas ao redor do mundo, utilizando e-mails, chats em tempo real e os inúmeros recursos de voz e vídeo.

Porém, do mesmo modo que nos beneficia poderosamente, a rede mundial é eficiente para os mal-intencionados e, portanto, pode também nos prejudicar. Como o acesso é livre, trafega pela internet todo tipo de informação com os mais variados fins e impactos. Por meio da rede, ladrões enviam programas espiões para roubar senhas, hackers espalham vírus que comprometem o funcionamento dos computadores, a pornografia pode invadir nossas casas sem nenhum escrúpulo e nossa privacidade se tornar pública em questão de segundos. Há ainda outro aspecto da rede que merece reflexão: o vício pelo digital. Muitas pessoas trocam o convívio social pelo virtual, o que pode acarretar problemas psicológicos tão graves que já existem centros especializados para tratá-los.

É por causa de todos esses prós e contras que o debate sobre um eventual controle do conteúdo da internet é acalorado. De modo geral, a sociedade tem se mostrado contra o controle, que limitaria o direito de expressão e ainda poderia ser utilizado para dirigir a opinião pública. No Brasil, com a liberação da internet pelo TSE (Tribunal Superior Eleitoral) para veicular propaganda política a partir de 2010, teremos uma nova experiência com a rede e poderemos tirar mais conclusões sobre seu poder.

15.3. Segurança

Ainda é grande o número de pessoas que evita fazer transações bancárias ou trocar informações sigilosas pela internet, principalmente entre as mais velhas. Elas têm razão, pois é realmente perigoso expor-se em uma rede. Mas as técnicas de proteção proporcionam nível razoável de segurança. Estamos falando de antivírus e anti-spywares para eliminar programas maliciosos, firewalls para bloquear o acesso externo ao nosso computador, métodos de criptografia para embaralhar o conteúdo da mensagem, impossibilitando sua compreensão por terceiros, e assinatura digital para assegurar a identidade de sites e pessoas (jurídicas e físicas).

A maioria dos problemas de segurança na rede tem origem em falhas humanas, e não tecnológicas. Entre essas falhas, estão atitudes como entregar a senha do computador, programa, e-mail ou site a outra pessoa, abrir e-mails suspeitos e utilizar senhas pessoais em computadores públicos.

As instituições financeiras oferecem várias ferramentas de segurança para transações pela internet.



# Capítulo 16

## Tipos de redes

---

- Topología de redes





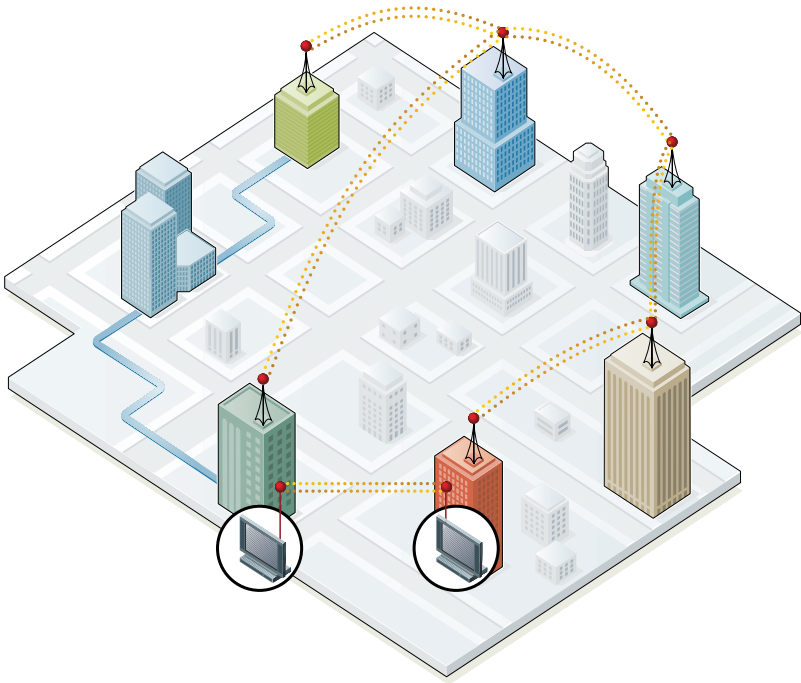
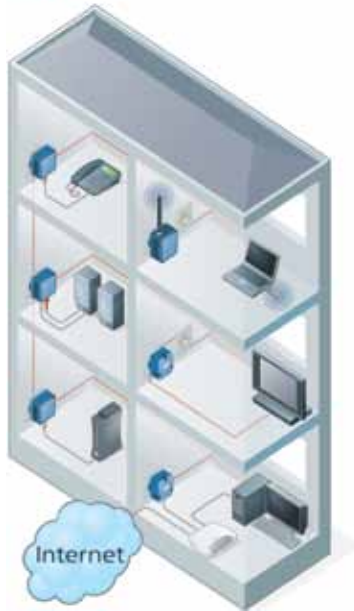
Vamos agora conhecer alguns tipos de redes. Certas denominações levam em consideração características relativas à posse da rede, que pode ser pública ou privada, além de sua abrangência territorial. Os acrônimos mais comuns são LAN, WAN e MAN.

**PAN – rede pessoal:** para rede de um único computador pessoal com outro, ou de um celular com o computador, usa-se o termo PAN (Personal Area Network, ou Rede Pessoal).

**TAN – rede pequena:** Tiny Area Network, ou Pequena Rede, como sugere a palavra tiny, define redes com apenas duas ou três máquinas.

**LAN – rede local:** para nos referir a uma rede com máquinas que se limitam a se conectar entre si num mesmo ambiente, de uma empresa, instituição ou residência, usamos a sigla LAN (Local Area Network ou Rede Local). As LAN (figura 111) podem ser de pequeno ou grande porte, dependendo da quantidade de computadores interligados.

**Figura 111**  
Exemplo de uma rede local (LAN).



**Figura 112**  
Exemplo de uma rede metropolitana (MAN).

**MAN – rede metropolitana:** Metropolitan Area Network (figura 112) quer dizer Rede Metropolitana. Assim como sugere o nome, tais redes abrangem uma cidade inteira. Pode se tratar de uma central de telefonia, transmissão de internet via rádio ou cabo, transmissão de TV analógica ou digital, seja por meio de cabos ou micro-ondas, entre outras possibilidades. As MAN podem se ligar a várias LAN que estiverem dentro do seu perímetro, e os computadores dessas redes locais podem ter acesso aos de outras redes locais que estiverem conectados à mesma MAN.

**CAN – campus area network:** as redes campus, pouco utilizadas, abrangem área maior do que as cobertas pelas LAN, mas não chegam a compreender uma cidade inteira. São exemplos de CAN as redes que interligam computadores em um condomínio, um conjunto de prédios, um campus universitário ou em uma área industrial.

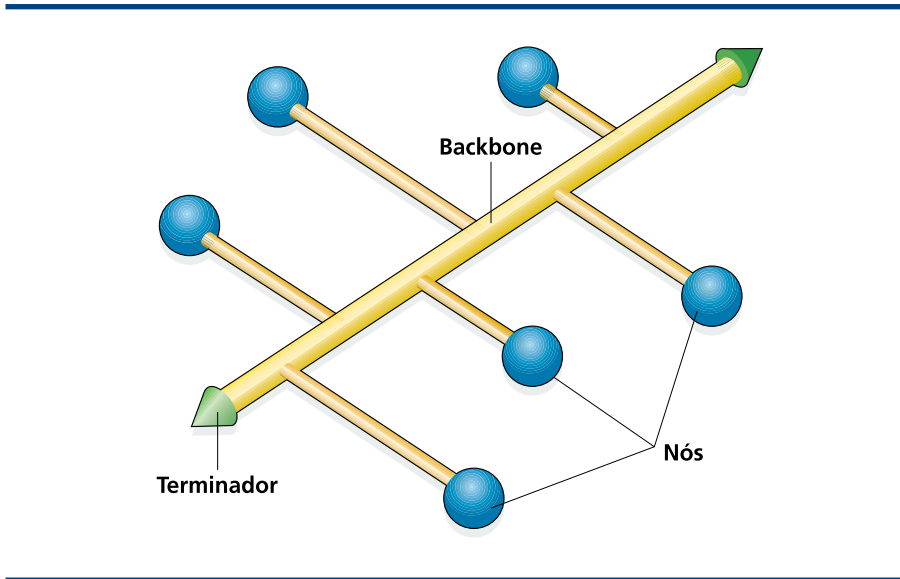
**WAN – redes geograficamente distribuídas:** as WAN se espalham por uma região de um estado, por todo o estado, um país ou o mundo todo. São, portanto, redes de longa distância. A internet, cujo acrônimo é WWW (World Wide Web ou Rede Mundial de Computadores) é a maior WAN do planeta.

As WAN podem se ligar a várias outras WAN ou LAN separadas por grandes distâncias. São geralmente implementadas e comercializadas pelas empresas de telefonia, como serviço de telefonia Voip, Banda Larga xDSL, MPLS, TVIP entre outros.

### 16.1. Topologia de redes

O modo como os computadores estão ligados entre si, os equipamentos empregados e a maneira como os dados vão trafegar dentro da rede definem uma topologia. A topologia, portanto, dá uma visão geral de como é ou será uma rede. Esse layout pode se basear nos modelos que descreveremos a seguir.

**Figura 113**  
Topologia de barramento (bus).

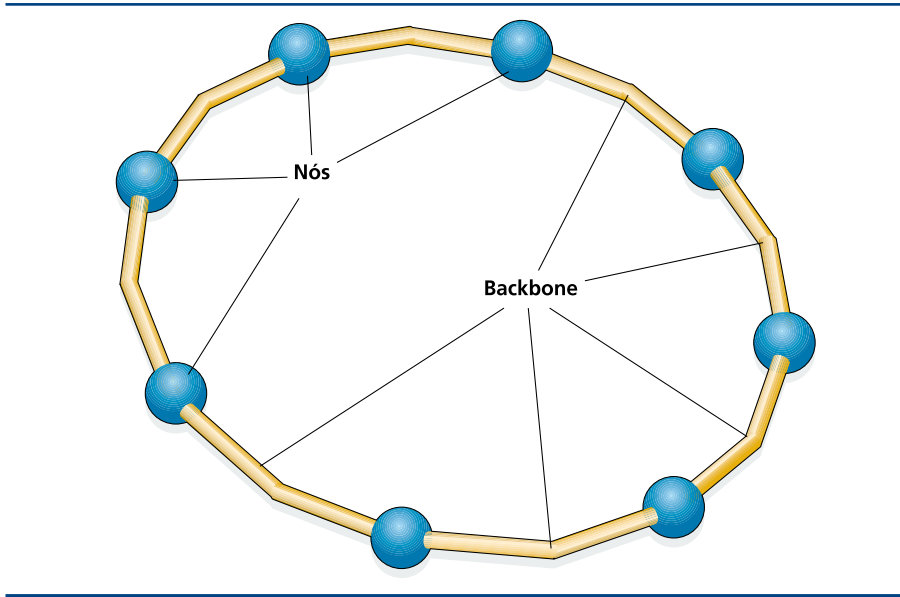


**Topologia de barramento (bus)** – nesta configuração (figura 113) todos os micros da rede se ligam uns aos outros como nós de uma corrente, ou como uma locomotiva e seus vagões. Esse tipo de ligação é feito geralmente por cabos coaxiais. Simples de implementar, essa rede é, porém, muito suscetível a problemas. Se um de seus nós apresenta defeito, a rede inteira falha.

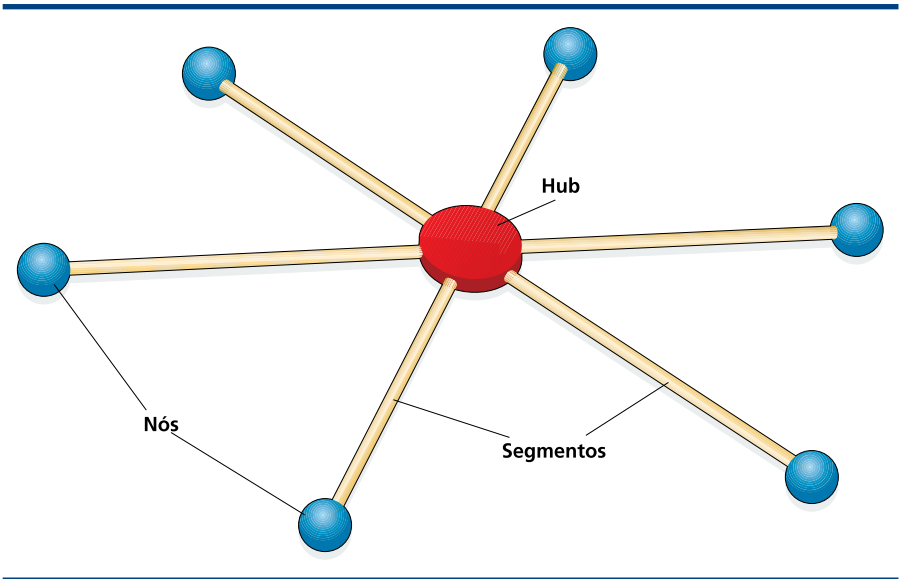
Todas as ligações são feitas por apenas um cabo. No ponto em que uma máquina será conectada, esse cabo é cortado e emendado por meio de um conector em T, que liga seus dois terminais à placa de rede do computador. Na ponta final do cabo há um resistor, o qual evita o retorno, através do cabo, do dado já analisado pelos nós da rede.

**Topologia em anel** – neste layout (figura 114) as máquinas se ligam em série, assim como na topologia de barramento. Porém, neste caso, o cabo não termina com um resistor, mas sua ponta final se liga novamente com a primeira máquina da sequência.

**Figura 114**  
Topologia em anel.



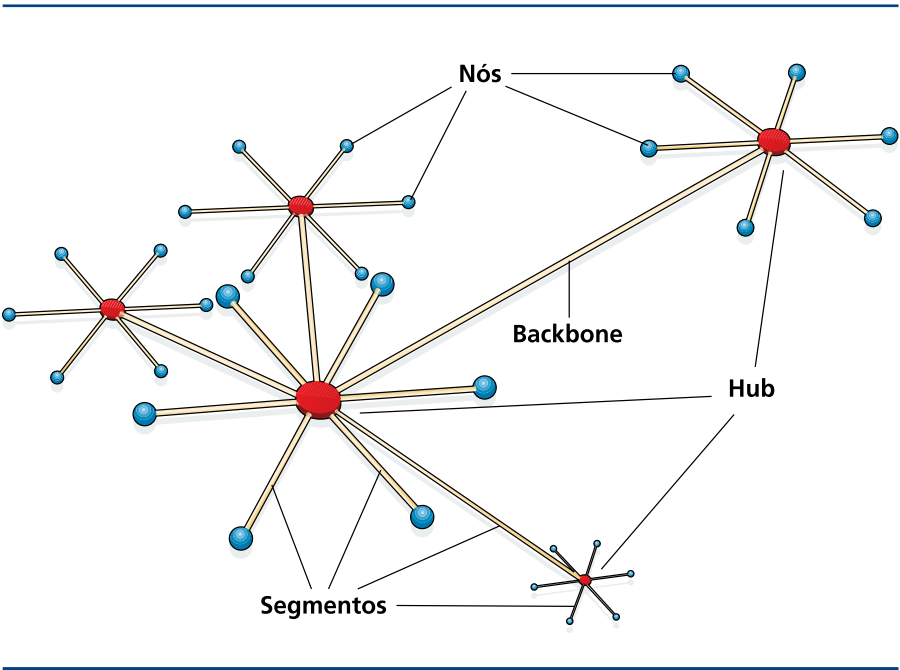
**Figura 115**  
Topologia em estrela.



**Topologia em estrela** – aqui as máquinas se ligam todas em um mesmo dispositivo central (figura 115). O equipamento utilizado geralmente é um hub ou um switch, que fecha a conexão entre todos os nós da rede. No caso dos hubs, os pacotes que chegam são retransmitidos para todos os nós, enquanto os switches podem analisar os pacotes e gerenciar sua distribuição, enviando-os somente para a máquina de destino.

**Topologia de barramento em estrela** – dois ou mais hubs que se conectam entre si por meio de uma mesma conexão, cada um com a própria rede em estrela, combinam as características das disposições em rede e em barramento. Imagine um prédio com vários andares, cada sala desses andares com um hub para fazer a ligação com os micros. Agora pense que esse hub é ligado a dois cabos que o conectam aos hubs do andar superior e do andar inferior (figura 116).

**Figura 116**  
Topologia de barramento em estrela.





# Capítulo 17

## Software de rede



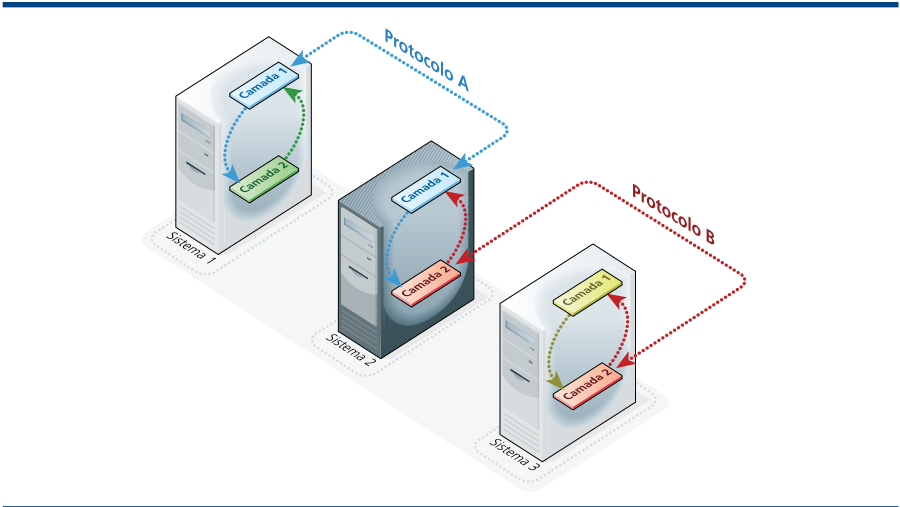
Para criar uma rede são necessários hardwares e softwares. Os hardwares são a parte física: equipamentos, cabos e computadores. E os softwares, os programas que implementam os protocolos.

Os protocolos são agrupados pelo seu tipo de serviço, em uma estrutura modular. Cada módulo (que denominamos camada) contém vários protocolos com serviços com características de mesmo nível. Os protocolos de uma mesma camada integram uma pilha de protocolos. E o conjunto de camadas e protocolos de uma rede caracteriza uma arquitetura de rede.

As camadas se ligam umas às outras consumindo serviços das camadas inferiores e os fornecendo às superiores. Dessa forma, o desenvolvedor de um protocolo da camada 4 não precisa saber como funcionam os protocolos da camada 3, mas apenas conhecer seus pontos de ligação, sua interface, sua maneira de trocar informações. Ou seja, um protocolo é um algoritmo, um software que fornece determinado serviço. Os protocolos se comunicam e as camadas oferecem serviços às camadas vizinhas.

Dentro da mesma máquina as camadas se comunicam entre si, com as camadas diretamente superiores e inferiores. De uma máquina para outra, os protocolos se comunicam apenas com uma instância do mesmo protocolo (figura 117). Imagine o seguinte cenário: um médico precisa pedir um exame de sangue para um de seus pacientes. Então, ele preenche um pedido, o entrega ao paciente e este o leva de carro ao laboratório de análises. O pedido é entregue a um atendente que o encaminha. Após fazer a análise, o biomédico preenche o resultado do hemograma. O paciente vai buscar o resultado e, de ônibus, o leva para o médico. O médico, por sua vez, o analisa e, com base na análise, faz o diagnóstico.

Podemos enxergar no relato uma rede, onde o médico e o biomédico representariam o mesmo protocolo, em uma mesma camada (figura 118). O paciente e o atendente do laboratório estariam em outra camada, e os meios de transporte, o carro e o ônibus, em uma terceira camada. Veja que no consultório o médico conversou com o paciente dentro do mesmo local. O paciente pegou um carro, que o levou até o laboratório, e foi ele quem conversou com o atendente, que está, assim, na mesma camada que a sua. O pedido e o resultado são duas mensagens trocadas pelo protocolo médico e



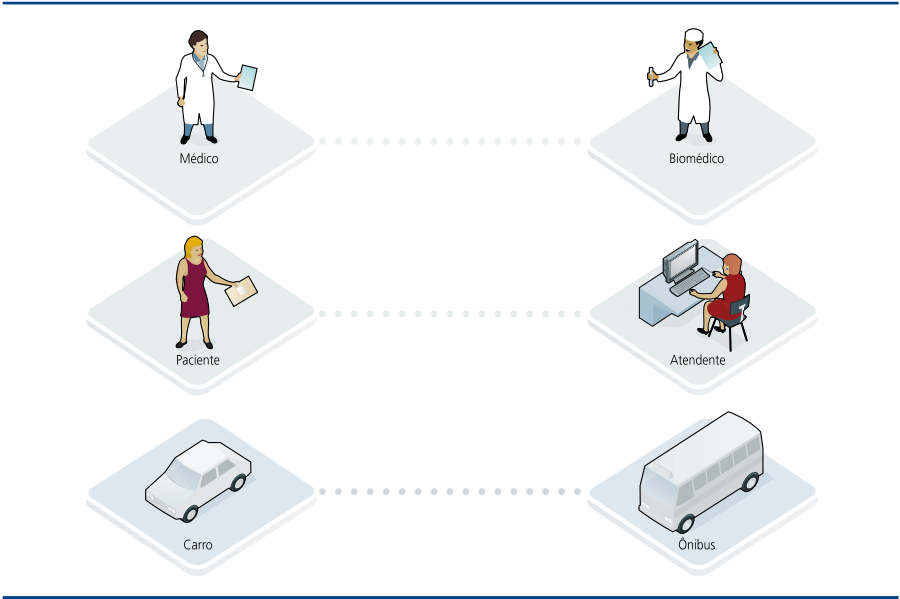
**Figura 117**  
Camadas se comunicam entre si e protocolos se comunicam com instâncias do mesmo protocolo em outra máquina.

biomédico. As informações que os dois profissionais trocaram só eram compreendidas por eles, que estavam também na mesma camada.

Os serviços que uma camada presta à camada de cima podem se dar de duas maneiras: com ou sem conexão.

Os serviços com conexão garantem que os dados chegarão intactos, e na ordem, até o destino, e que o canal de comunicação ficará aberto até que a transmissão seja encerrada. É um processo análogo ao do sistema de telefonia, no qual, depois da discagem e do atendimento pelo receptor, se estabelece uma conexão – a voz é então transmitida continuamente e a ligação só se encerra quando o telefone é colocado de volta no gancho.

Os serviços sem conexão enviam mensagens, mas não há garantia de que estas chegarão ao destino, nem sobre a ordem em que chegarão. Esse tipo de serviço se parece com o dos correios: você envia uma carta e fica esperando resposta, que pode não vir, não há garantia. E, caso você envie várias cartas, pode ser que as mais recentes cheguem antes das encaminhadas anteriormente – cada carta pode ter seguido um caminho diferente.



**Figura 118**  
Exemplo de funcionamento de uma rede em um consultório médico.



# Capítulo 18

## Modelos de referência

- Modelo de referência ISO OSI
- Modelo de referência TCP/IP

camadas: aplicação, apresentação, sessão, transporte, rede, enlace e física. O ISO não tem os protocolos definidos e, portanto, é somente um modelo, não pode ser considerado como arquitetura de rede (figura 119).

Cada camada deve realizar tarefas focadas em resolver um domínio específico de problemas. Vejamos agora um resumo das funcionalidades básicas de cada camada.

**Camada 1 – física:** relaciona-se ao hardware da rede, define questões ligadas à voltagem e à velocidade de transmissão de bits, além de tratar da construção dos equipamentos de rede.

**Camada 2 – de enlace:** implanta no meio físico um canal de comunicação. É responsável por manter a confiabilidade, garantir que os dados cheguem ao destino e correspondam ao que foi entregue na ponta de transmissão. Quebra as mensagens em quadros de dados, com centenas ou milhares de bytes. Sempre que um receptor recebe um desses quadros, emite de volta uma mensagem de confirmação e o transmissor então envia o próximo quadro. Os dados são bufferizados (armazenados), remontados e repassados para a camada de rede. Os circuitos da camada de enlace ainda enviam pacotes em um canal compartilhado por todos os computadores da rede, além de controlarem a velocidade da transmissão de dados de um dispositivo rápido para outro mais lento.

**Camada 3 – de rede:** controla o direcionamento do fluxo de dados na condução da informação pela rede. Possibilita que os dados passem por vários enlaces até serem entregues no destino. Controla rotas e escolhe os melhores caminhos. Leva em consideração a distância mais curta, congestionamentos ou falhas ocasionadas pelo desaparecimento de um ponto de passagem na rota. A camada de rede é capaz de descobrir se existe outro caminho e, se existir, encaminhar os pacotes por esta rota alternativa e fazer com que o dado chegue ao destino. Esta camada possibilita a comunicação entre sub-redes, ainda que sejam heterogêneas, e utilizem tamanhos de pacotes, velocidades ou até mesmo protocolos de comunicação diferentes.

**Camada 4 – de transporte:** tem a função de receber dados da camada de rede e fracioná-los em pedaços menores, se isso for necessário. Organiza os pacotes e os entrega na sequência correta, livres de erros, uma vez que durante a transmissão podem seguir caminhos diferentes, se perderem e ainda chegarem fora de ordem ao destino (figura 120). É um canal de comunicação fim a fim, utilizado para que um software em uma máquina consiga se comunicar com outro em outra máquina, de forma transparente, sem precisar se deter em assuntos como distância, obstáculos ou complexidades dos caminhos, que são atribuições das camadas inferiores. A camada de transporte pode controlar ou não a entrega dos dados – essa opção deve ser selecionada no início da comunicação (figura 120).

**Camada 5 – de sessão:** estabelece um “diálogo” entre duas camadas de apresentação. Administra a sessão, estabelece quando a comunicação se inicia e quando termina. Controla o “diálogo”, assegurando a lógica da comunicação, segundo a qual quando um fala, o outro escuta. Define símbolos utilizados na comunicação que evitam o conflito na execução de comandos.

Nos tempos mais remotos das redes, quando ainda se começavam a desenvolver os protocolos, não eram seguidos padrões que possibilitassem a interligação entre redes de diferentes arquiteturas. Mais tarde, esse problema foi solucionado com a criação dos modelos de referência ISO OSI e o TCP/IP.

18.1. Modelo de referência ISO OSI

O modelo ISO OSI foi apresentado pelo ISO (Internationals Standards Organization, ou Organização Internacional de Padrões), com o intuito de padronizar os protocolos em camadas, com o nome de Open System Interconnection (OSI), ou seja, Interconexão de Sistemas Abertos. O modelo divide os protocolos em sete

Figura 119  
Representação da hierarquia e comunicação entre camadas.

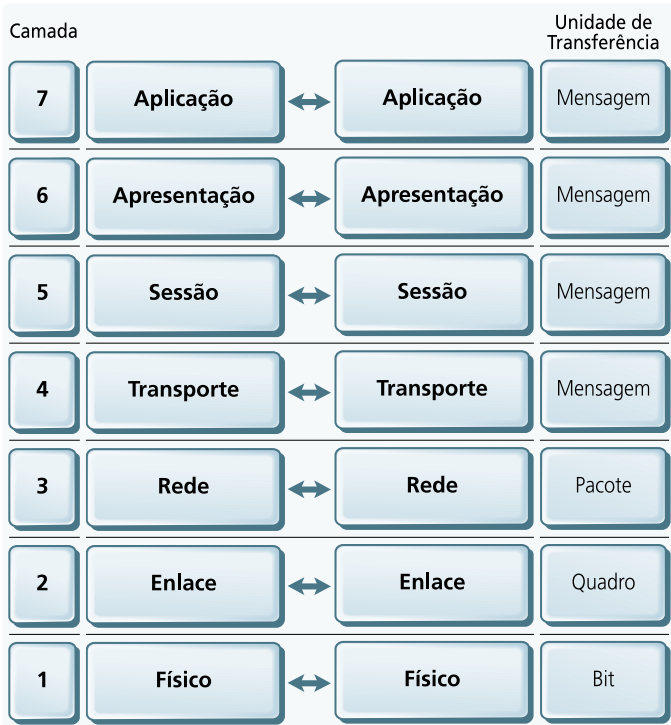
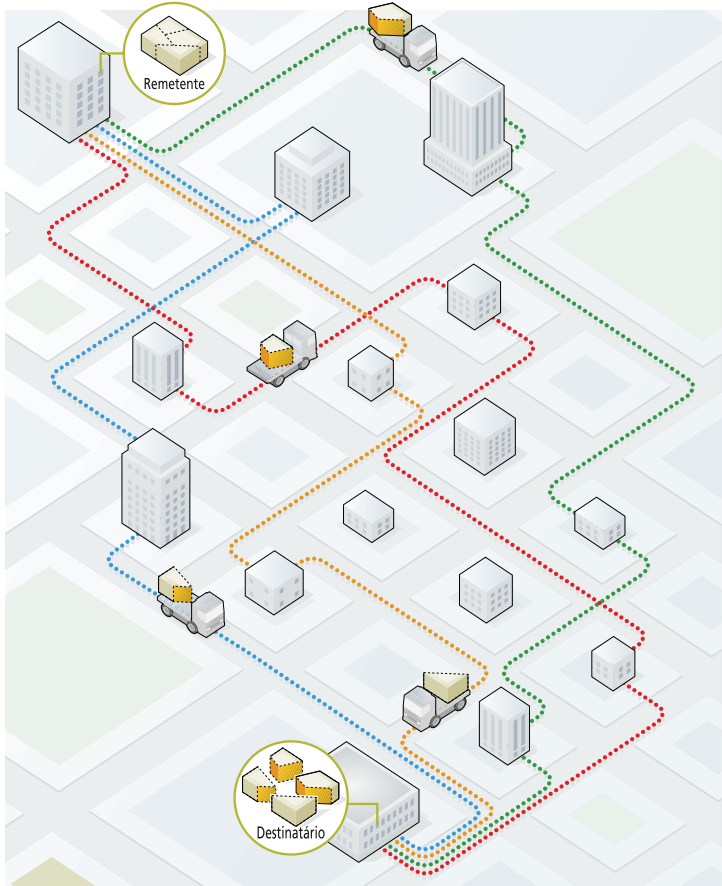




Figura 120

A camada 4 organiza os pacotes e os entrega na sequência correta.



O modelo segue a mesma lógica de camadas do padrão OSI. Neste, as camadas prestam serviços às camadas superiores, por meio de uma interface bem definida. Uma camada não interfere nas funcionalidades de outra e todas se comunicam por protocolos independentes, de forma que a eventual substituição de um protocolo em uma delas não influencia o funcionamento das demais.

Como vemos na figura 121, o modelo TCP/IP possui menos camadas que o padrão OSI. A camada de apresentação e sessão foi suprimida – a experiência com o modelo OSI demonstrou que seus protocolos eram pouco utilizados na implementação das aplicações. Quando são necessárias, as funções dessas camadas são incluídas na camada de aplicação. Já a camada de rede do padrão OSI funciona da mesma maneira que a camada Internet do modelo TCP/IP. E neste último a camada de interface de rede equivale às camadas física e de enlace do primeiro.

Os protocolos do TCP/IP são mais populares e sempre tiveram apoio no meio acadêmico, por terem sido implementados no sistema operacional Unix, que demonstrou ótimo desempenho.

Embora esteja praticamente em desuso, o modelo OSI ainda serve como referência de estudo, pois oferece uma visão hierárquica do grupo de serviços que compõem cada camada, fornecidos à camada superior, além dos protocolos e interface de comunicação entre elas.

Camada	OSI	TCP/IP
7	Aplicação	Aplicação
6	Apresentação	Não presentes no modelo
5	Sessão	Não presentes no modelo
4	Transporte	Transporte
3	Rede	Rede
2	Enlace	Enlace
1	Físico	Físico

Figura 121

Comparação das camadas no modelo OSI e TCP/IP.

HTTP para transmissão de páginas da web, FTP para transmissão de arquivos e POP e SMTP para operar e-mails são alguns exemplos de protocolo.

**Camada 6 – de apresentação:** faz a tradução de formato de dados entre máquinas que utilizam formatos diferentes. Em alguns sistemas, o byte pode ser lido da esquerda para direita ou vice-versa. Em outros, a codificação das letras pode ser diferente, ASCII, ABCDIC da IBM, e daí por diante. São realizadas e convertidas várias interpretações para que a informação recebida seja a idêntica à que foi transmitida.

**Camada 7 – de aplicação:** são **protocolos** de alto nível que possibilitam que softwares de mesmo tipo troquem informações. Este nível da rede é responsável pelo formato do conteúdo dos pacotes que estão sendo transmitidos. É constituído de softwares que interagem com o usuário, pois entrega o recurso ao cliente do serviço. Está no fim da rede.

O matemático Vint Gray Cerf (Estados Unidos, 1943) e o engenheiro Robert Elliot Kahn (Estados Unidos, 1938) são considerados os “pais da internet”. Foram eles que desenvolveram, respectivamente, os protocolos TCP e IP, na década de 1970. Em 2005, Cerf se tornou vice-presidente da Google.

18.2. Modelo de referência TCP/IP

A internet derivou da Arpanet, primeira rede geograficamente distribuída (WAN), criada nos Estados Unidos durante da Guerra Fria (contaremos essa interessante história no próximo tópico). A internet baseia-se em datagramas que, como os telegramas, são mensagens entregues à rede e direcionadas ao destino com ajuda de todos os seus nós.

Essa arquitetura precisava de um modelo para definir seus padrões. Tal modelo de referência, o TCP/IP, nome que remete aos protocolos TCP e IP, foi desenvolvido por dois norte-americanos (**CERF** e **KAHN**) em 1974.

# Capítulo 19

## Internet

---

- Arquitetura da internet



O problema das linhas telefônicas é que seguem uma estrutura hierárquica em que vários escritórios e bases se ligam a uma central de comutação, a qual se conecta a alguma outra central mais acima na hierarquia, que possibilita conexão com outras centrais e suas redes. Ou seja, a virtual destruição de algumas dessas centrais poderia isolar uma base militar ou um grupo de bases dos Estados Unidos.

**D**urante o período da Guerra Fria, que se estendeu desde o fim da segunda Guerra Mundial, em 1945, até o início dos anos 1990, após a queda do muro de Berlim, Estados Unidos e União Soviética protagonizaram uma espetacular corrida armamentista. Os dois países construíram arsenais nucleares capazes de destruir o mundo em instantes. Temerosa de um possível ataque nuclear, a potência capitalista decidiu fortalecer e tornar mais seguro o seu até então frágil modelo de transmissão de informações, que se baseava em **linhas telefônicas**.

Assim que a União Soviética saiu à frente na corrida espacial, ao lançar o primeiro satélite artificial, o Sputnik, em 1957, o presidente Dwight David Eisenhower criou a ARPA - Advanced Research Projects Agency (Agência de Projeto de Pesquisa Avançada). Ao órgão, independente das Forças Armadas, foi dada a missão de desenvolver uma arquitetura de redes para substituir a transmissão por telefonia analógica por comutação, a qual deveria ser redundante e capaz de se adaptar a falhas.

A ARPA investiu em vários projetos de universidades e, em 1967, desenvolveu a Arpanet, primeira rede WAN com pacotes comutados, a partir de um projeto desenvolvido no National Physical Laboratory, na Inglaterra, que além da proposta, já tinha protocolos funcionais desenvolvidos. Essa rede foi o tronco inicial do desenvolvimento das redes comutadas. Para que a arquitetura da rede pudesse evoluir, as universidades que tinham contratos com a ARPA começaram a se conectar à Arpanet. Um dos servidores que se interligaram foi o Unix, da Universidade de Berkeley, onde foram desenvolvidos os sockets, o TCP/IP e vários outros aplicativos para a rede. A partir de 1980 outras LANs passaram a se conectar à Arpanet.

Em 1970, porém, surgia uma rede paralela à Arpanet com a finalidade de interligar pesquisadores de várias universidades, a NSFNET. Essa rede já utilizava TCP/IP e tinha seis servidores estrategicamente distribuídos pelo território norte-americano, ligando o seu backbone a mais de 20 redes regionais. Durante o período de evolução da Arpanet e da NSFNET, outras redes de pesquisa foram sendo desenvolvidas na Europa, como a EuropaNET e a Ebone.

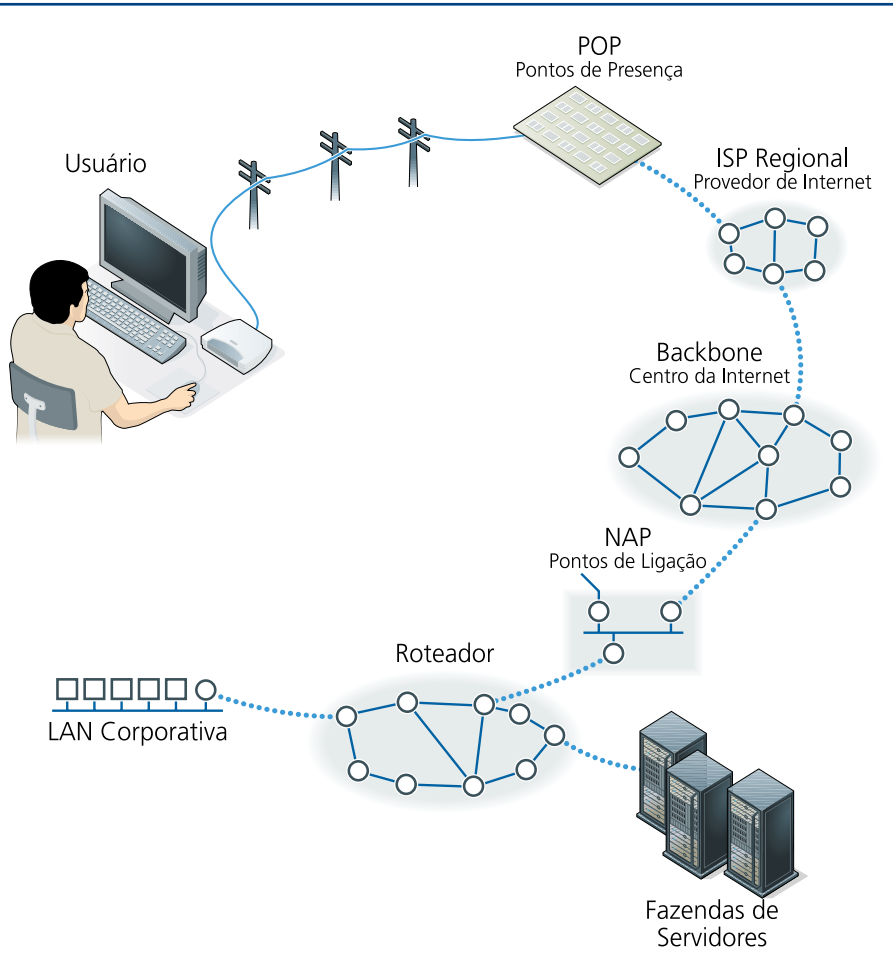
Os cientistas dessas universidades utilizavam basicamente serviços de e-mail, transferência de arquivos, newsgroups (grupos de notícias) e acesso remoto.

A partir do estabelecimento do padrão TCP/IP, as redes cresceram muito. Em 1983 a Arpanet se interconectou com a NSFNET e redes da Europa e do Canadá, entre outros países. Nascia a internet (veja o quadro *Sucesso no meio acadêmico*, na pág. 183).

19.1. Arquitetura da internet

Vamos agora estudar a organização da rede mundial, bem como os elementos que a mantêm (figura 122).

No centro da internet estão os grandes backbones (espinhas dorsais), ou linhas de transmissão tronco, conectadas a roteadores de alta capacidade, com velocidades quase inacreditáveis. Em alguns backbones da RNP (Rede Nacional de Ensino e Pesquisa), que liga universidades e instituições de ensino federal, a velocidade de conexão chega a 10 Gigabits. Mas os backbones centrais da internet têm roteadores capazes de processar até 320 Gigabits. Essas conexões são feitas por fibra óptica, rádio, micro-ondas ou satélite, por meio de redes ATM, x.25 e Frame Relay. Existem vários backbones na internet, de diferentes operadoras, que cobrem áreas diversas.



**Figura 122**  
Esquema de funcionamento da rede mundial de computadores.

Na América Latina é a empresa Hispasat que aluga satélites para conexão ao backbone da internet. No Brasil, há três conjuntos de backbones. Um deles, com seis backbones, é da RNP, voltada à educação, que interliga instituições de ensino e sites de domínio com final edu.br. Outro conjunto é o do governo, que utiliza domínios do tipo gov.br e liga prefeituras, empresas e órgãos públicos. E por fim há os backbones comerciais – o maior de todos é controlado pela Embratel/MCI.

Os backbones se conectam com outros, de outras empresas, para permitir o acesso de todos a todo o ambiente da internet. Nas conexões há centrais NAP (Network Allocation Points, ou Rede de Pontos de Distribuição), que são instalações com vários roteadores as quais ligam roteadores de uma controladora aos de outras, controlando também a largura de banda compartilhada.

Conectam-se também aos backbones centrais grandes empresas com taxas de transmissão muito altas, empresas da internet que hospedam vários serviços WWW, e-mail, FTP etc. E, ainda, provedores de internet com redes regionais distribuídas geralmente por meio de rede de telefonia, rádio ou cabo coaxial (de TV a cabo).

Os clientes comuns se conectam aos provedores e estes propiciam o acesso à rede através de pontos de acesso, chamados de POP (Point of Presence), que em geral são locais que abrigam servidores, roteadores, switches ATM de conversão analógica para digital, entre outros equipamentos. É da estrutura dos POPs que a conexão do circuito da linha de telefonia salta para a rede de dados comutada da internet e chega ao cliente final da rede.

Os principais meios de conexão para acesso aos provedores são:

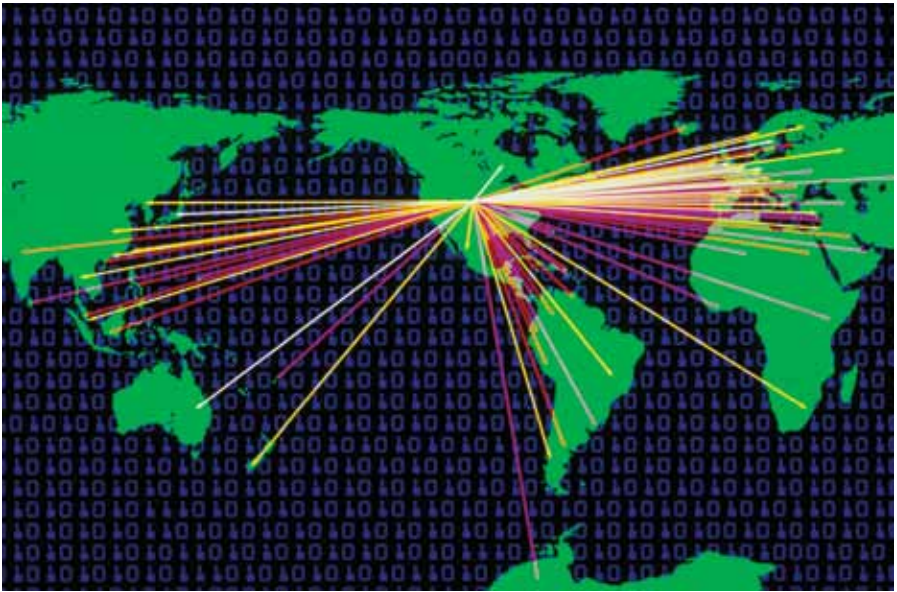
- linha telefônica, a partir de modems ADSL conectados à rede de telefonia (as conexões discadas);

- cabo coaxial, que utilizam cable modems (modem de cabo) de empresas de TV a cabo, principalmente;
- sem fio, por meio de antenas transmissoras e receptoras WiFi, WiMax, TMax e satélite;
- sem fio móvel, que utiliza telefones celulares ou modems, os quais transmitem baseados em tecnologias como CSD, GPRS EDGE, UMTS, HSDPA, EVDO, entre outras.

## Sucesso no meio acadêmico

A rede mundial começou a se popularizar fora do meio acadêmico com a criação, em 1991, da aplicação WWW (World Wide Web) pelo físico Tim Berners-Lee na CERN (European Organization for Nuclear Research), e do primeiro navegador web, por Marc Andreessen no NCSA (National Center for Supercomputing Applications). A partir daí conteúdos como texto e imagens poderiam ser visitados rápido e facilmente. Mas o que de fato impulsionou a grande adesão global à internet foram os ISPs (Internet Service Providers, ou provedores de internet), que começaram a comercializar o acesso, oferecendo serviços de e-mail, páginas web, IRC, ICQ entre muitas outras aplicações.

Os backbones utilizam fibra óptica, rádio e satélite entre outros meios de conexão.





# Capítulo 20

## Arquitetura de rede

- Camada de aplicação
- Camada de transporte
- Camada de rede
- Considerações finais
- Referências bibliográficas

Como já dissemos, a arquitetura de uma rede é seu modelo de camadas e o conjunto de protocolos desenvolvidos para cada uma das camadas. Vamos agora fazer um estudo das camadas a partir do modelo de referência TCP/IP. Começaremos com o que nos é mais familiar, as tecnologias com as quais estamos acostumados. Partiremos da visão mais superficial da rede, a do usuário comum, que abrange navegadores, e-mail, transferência de arquivos, voz e vídeo. Em seguida, aprofundaremos o estudo das camadas mais internas da rede até chegarmos à camada física, onde trataremos do hardware.

20.1. Camada de aplicação

A camada de aplicação é a camada mais acima, que não fornece serviços a nenhuma outra, mas é consumidora de serviços da camada logo abaixo, a camada de transporte.

A camada de aplicação possui protocolos conhecidos, como o DNS, correios eletrônicos (POP3 e SMTP), FTP entre outros. É nessa camada que a rede é realmente utilizada – as camadas inferiores formam a infraestrutura para que as aplicações consigam se comunicar. Assim, a função dos protocolos dessa camada é estritamente enviar mensagens diretamente para o software interlocutor e, se for o caso, aguardar uma resposta, sem levar em conta se o pacote será transmitido, se para isso recorrerá à conexão ou não, se será transmitido por rádio, por cabo ou qualquer outro meio.

20.1.1. DNS

Quando entramos no navegador para acessar uma página qualquer da web digitamos o endereço da homepage – por exemplo, `www.centropaulasouza.sp.gov.br` – na barra de endereços e, pronto, a página é carregada. Para que isso aconteça, a aplicação cliente precisa se conectar com o servidor de páginas na internet que possui o domínio `centropaulasouza.sp.gov.br` e está esperando por requisições de páginas web e solicitar sua página principal. O servidor aceita a requisição e responde pela mesma conexão com o hipertexto solicitado. Todo esse processo será possível se a requisição puder chegar até o servidor. E para isso a mensagem deve conter o endereço IP do servidor para o qual ela será transmitida, pois somente

assim os roteadores da internet poderão encontrá-la. Nesse caso, no entanto, não temos o endereço IP (leia quadro *Saiba como localizar números IP*), mas apenas um nome de domínio (`informatica.com.br`), o que tornou a busca viável. A página foi carregada normalmente devido à aplicação DNS (Domain Name System, ou sistema de nomes de domínio), um serviço de resolução de nomes de domínios. Sempre que uma conexão é solicitada por meio de um nome em vez de um número IP diretamente, o cliente DNS é acionado. Em seguida, ele se conecta ao seu servidor de nomes requisitando o IP do domínio informado. O servidor, por sua vez, acessa uma base de dados de nomes e endereços de IP correspondentes e, caso encontre o relativo à solicitação, responde ao cliente.

Como a quantidade de domínios cresceu rapidamente, tornou-se impossível a um único servidor de nomes atender a toda a internet, pois os nomes teriam de ser gerenciados por apenas uma entidade reguladora de domínios. Por isso foi definida uma hierarquia, constituída por 13 servidores de nomes raízes, cujos nomes começam com as letras A a M. O servidor “I” fica em Estocolmo, na Suécia, o “K” em Londres, Inglaterra, e o “M” em Tóquio, no Japão. Todos os demais estão nos Estados Unidos.

Esses servidores delegam o controle dos domínios de determinada região a servidores TLD, que são de Alto Nível e, em sua maioria, controlam os domínios de determinado país. Cada país tem o próprio sufixo, como `.jp` (Japão), `.uk` (inglaterra), `.fr` (França), `.br` (Brasil).

No Brasil a entidade que controla os domínios chama-se registro.br. Em seu site, no endereço `http://registro.br/info/dpn.html`, você encontra toda a lista de DPNs (Domínios de Primeiro Nível) empregados no Brasil, como por exemplo `.com.br`, `.edu.br`, `.gov.br`, `.net.br`. Alguns domínios são liberados apenas com a apresentação de documentos. Entre estes estão: `.am.br` (rádio AM), `.coop.br` (cooperativas), `.edu.br` (faculdades de nível superior), `.fm.br` (rádio FM), `.g12.br` (escolas de primeiro e segundo grau), `.gov.br` (órgãos públicos), `.mil.br` (Forças Armadas do Brasil), `.org.br` (entidades privadas sem fins lucrativos), `.psi.br` (provedores de internet) e `.tv.br` (canais de televisão).

Quando uma máquina precisa traduzir um domínio e encontrar seu IP, consulta primeiramente o arquivo “`%WINDIR%\system32\drivers\etc\hosts`” no Windows ou “`/etc/hosts`” no Linux (figura 123). Em seguida o procura no servidor de nomes configurado em sua interface de rede. Caso este não o encontre em sua lista de nomes, consulta seu servidor de nível mais alto. Se este ainda não o localizar, recorre ao servidor TLD, responsável pelo domínio solicitado. Assim que for encontrada, a informação retorna ao requisitante.

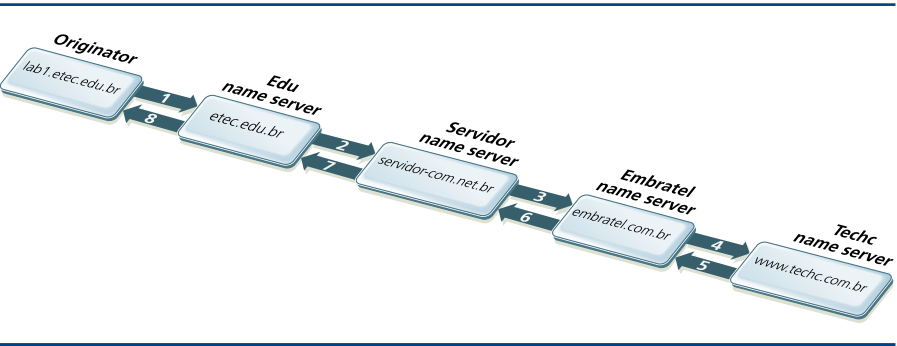


Figura 123  
Processo de tradução de domínio.



# Saiba como localizar números IP

Para fazer um breve teste com DNS, tente disparar um ping contra algum domínio da internet, como demonstra a figura 124, e você verá o nome do domínio convertido para IP.

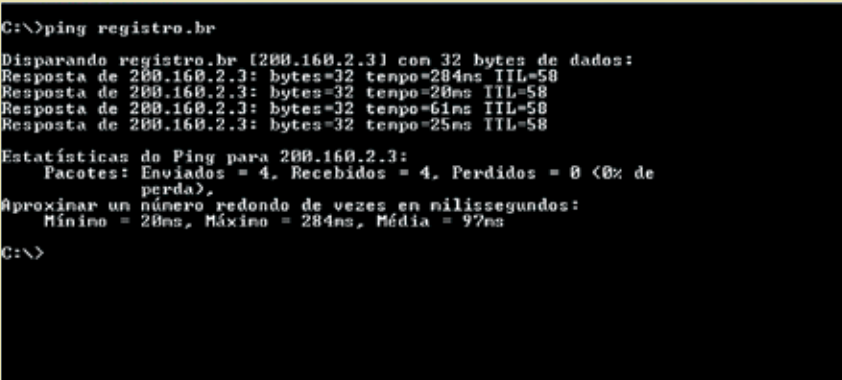


Figura 124 Disparando um ping.

No Windows é possível utilizar o comando nslookup. Esse comando é capaz de retornar informações sobre o servidor de nomes que encontrou o domínio, a partir apenas da sigla nslookup mais o nome do domínio. Por exemplo: nslookup www.ipv6.com. Veja como fazer, na figura 125.

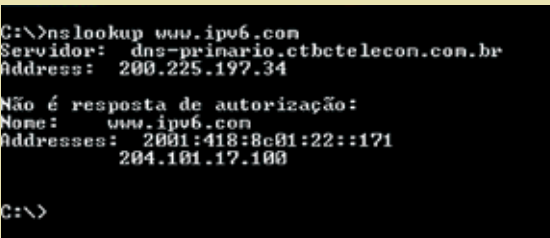


Figura 125 Utilizando o comando nslookup.

Para ver os dados de cada servidor consultado, utilize o parâmetro -d. Por exemplo: nslookup -d ipv6.com.

## 21.1.2. Correio eletrônico

O correio eletrônico, mais conhecido como e-mail, é uma das aplicações mais antigas e até hoje uma das mais utilizadas da internet. Pesquisadores de universidades dos Estados Unidos já o usavam antes de 1970. Muitas vezes quando enviamos e-mails o computador da pessoa para quem se destina a mensagem está desligado, o que inviabilizaria o recebimento. Mas o processo de enviar e receber e-mails inclui um computador intermediário, geralmente o provedor de internet, que armazena os e-mails de seus clientes enquanto estiverem off-line.

Para enviar mensagens para o servidor, o computador do cliente de e-mail utiliza o protocolo SMTP (Simple Mail Transfer Protocol, ou protocolo de

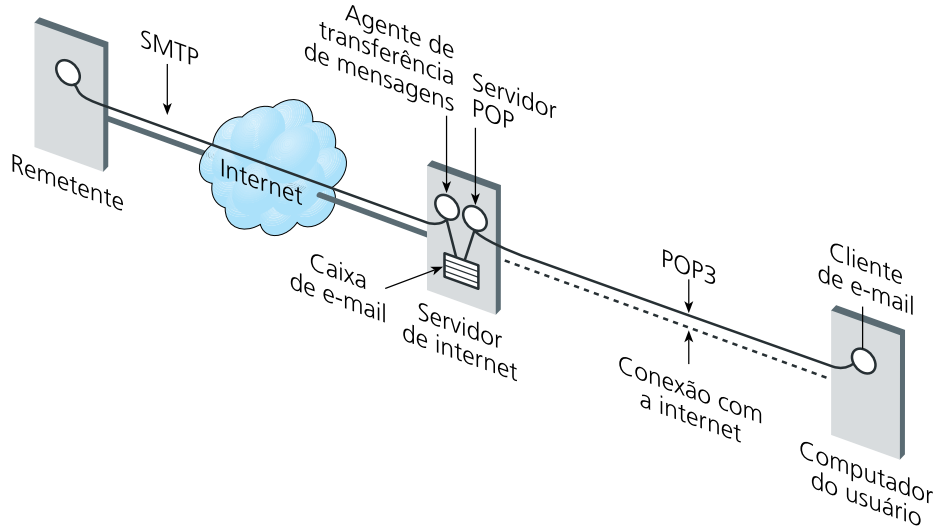


Figura 126

Protocolos de transmissão de e-mails: SMTP e POP.

transmissão de e-mail simples). E para solicitar o download dos e-mails armazenados no computador intermediário, recorre ao protocolo POP3. Os protocolos tiveram de ser separados, pois os dois processos de enviar e receber arquivos são totalmente diferentes um do outro (veja figura 126). Não têm, de fato, relação nenhuma. Por exemplo, certas configurações não requisitam nem mesmo senha para enviar e-mails. Já para baixá-los, a senha é imprescindível. Para transmitir, é preciso informar um destinatário, mas para receber e-mail tal informação é irrelevante.

**SMTP** – foi definido na RFC 821, e é utilizado quando um cliente de e-mail quer enviar uma mensagem. O software cliente tenta abrir uma conexão com o servidor SMTP, troca algumas configurações iniciais, identifica os containers de destino e transmite o conteúdo do e-mail. No final do processo a conexão deve ser encerrada. O servidor SMTP, por padrão, aguarda conexões na porta 25.

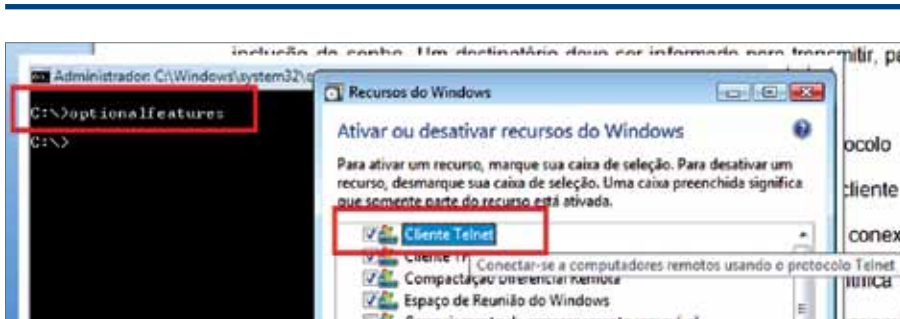
Como na maioria dos protocolos da internet, os comandos do SMTP são transmitidos em texto puro, da tabela ASCII, fáceis de compreender.

Faça uma experiência: tente se comunicar com um servidor SMTP por meio de um terminal de telnet, em modo texto. Telnet é também uma aplicação de rede da camada de aplicação: um terminal de texto que se conecta a um servidor TCP qualquer e consegue transmitir mensagens de texto por meio dessa conexão. Basta você escrever a mensagem e confirmar com enter. As mensagens que chegam pela conexão são exibidas na linha debaixo do último comando.

Observação: no Windows Vista e no Seven, o telnet tem de ser habilitado executando-se o comando Optionalfeatures no prompt de comando. Em seguida, é preciso habilitar a opção Cliente Telnet (figura 127).

RFC é o acrônimo para Request for Comments, especificação técnica desenvolvida sobre determinado assunto por solicitação da IETF (Internet Engineering Task Force), comunidade internacional cuja meta é a evolução contínua da internet.

**Figura 127**  
Habilitando o telnet.



Agora já podemos executar o comando no prompt do Ms-Dos para iniciar uma sessão telnet. Procure descobrir o endereço do servidor SMTP do seu ISP, pois alguns servidores são configurados para não aceitar mensagens oriundas de fora de sua rede. Outra ressalva: em servidores de e-mail que utilizam TLS (Transport Layer Security, ou Segurança na Camada de Transporte) a experiência não funcionará. A conexão será feita, mas nada aparecerá na tela, pois os dados são criptografados e o telnet não será capaz de exibir ou enviar as informações.

Se o servidor SMTP estiver ativo, o telnet irá se conectar na porta 25 da máquina portadora do domínio mail.ig.com.br. O servidor então enviará para o telnet cliente uma mensagem de boas vindas:

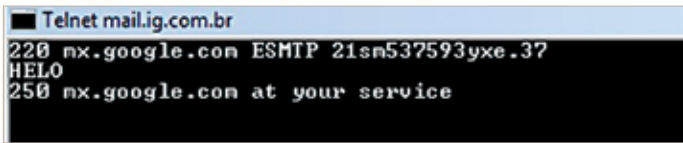
Com a mensagem de resposta de boas vindas de tipo 220 pronta na tela, como mostra a figura 128, já podemos iniciar uma conversação. Escreva a palavra HELO e pressione ENTER.

Uma resposta do tipo 250 deve ser transmitida como retorno. Neste caso surgirá uma mensagem educada do servidor: mx.google.com ao seu dispor (figura 129). Encerramos a sessão por meio do comando QUIT.

**Figura 128**  
Mensagem de resposta de boas vindas.



**Figura 129**  
Mensagem de resposta do servidor.



Os servidores de SMTP modernos utilizam o ESMTP, evolução do padrão original. O ESMTP inclui mais comandos relativos à segurança e está definido na RFC 1869. Tente se comunicar novamente, mas agora escrevendo EHLO em vez de HELO, e o servidor deverá responder algo parecido com o que mostramos no quadro a seguir:

```
220 mx.google.com ESMTP 23sm695203yxe.36
EHLO
250-mx.google.com at your service, [189.41.133.160]
250-SIZE 35651584
250-8BITMIME
250-STARTTLS
250-ENHANCEDSTATUSCODES
250 PIPELINING
```

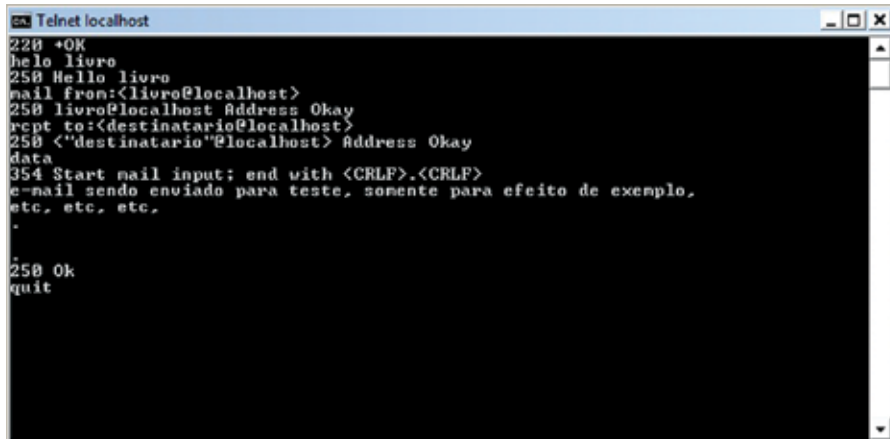
Isso significa que está ativo o protocolo ESMTP (SMTP Service Extensions), pois o SMTP não compreenderia o comando EHLO.

Poderíamos ir tentando outros comandos, como os listados abaixo, porém teríamos de passar uma senha criptografada para continuar. Para obter a lista completa dos comandos, pesquise a RFC.

```
MAIL FROM:<endereço@doemail.com.br>
(para identificar o remetente)
RCPT TO:<endereço@destinatario.com.br>
(para identificar os destinatários)
SUBJECT:<o assunto desta mensagem>
(para descrever o assunto)
DATA
(para iniciar a transmissão do conteúdo do e-mail)
```

Vamos agora compreender a figura 130, que contém o diálogo entre o servidor e o meu cliente de telnet. Veja que os comandos com números na frente foram as respostas do servidor aos meus comandos anteriores. E os comandos HELO, MAIL FROM, RCPT TO, DATA foram digitados por mim.

Nessa sequência, uma mensagem de e-mail foi enviada com sucesso para a caixa de mensagens do destinatário do e-mail através do telnet.



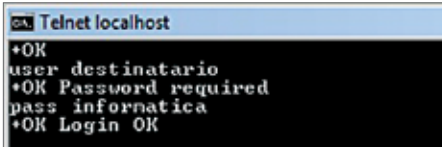
**Figura 130**  
Diálogo entre o servidor e o cliente de telnet.

**POP3** – Empregado para receber as mensagens, o protocolo Post Office Protocol versão 3 (ou Protocolo de Correio) está especificado na RFC 1939. Seu processo de recepção tem três fases: autenticação (figura 131), transação e atualização.

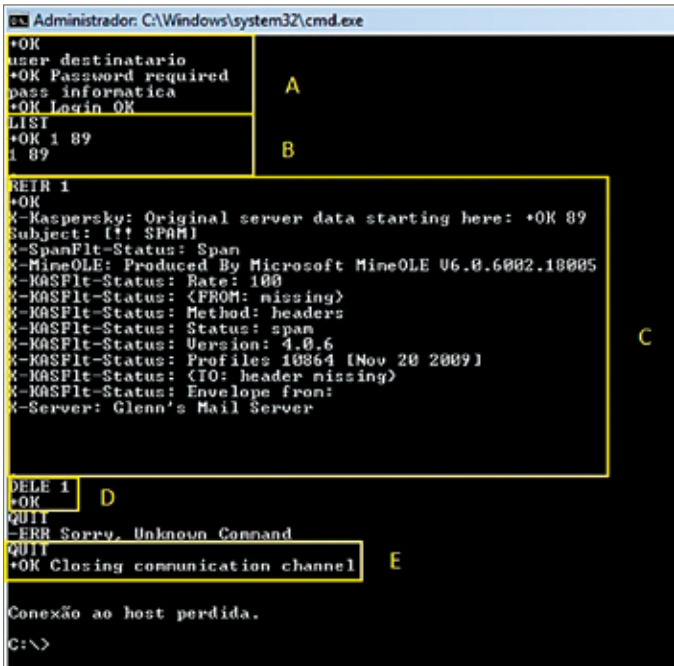
Para autenticar, utilizamos o comando USER (nome do usuário). Em seguida vamos para o PASS (senha). Vamos nos conectar agora no servidor POP3, geralmente no mesmo host do SMTP, mas ocupa a porta 110.

```
telnet localhost 110
```

**Figura 131**  
Fase de autenticação.



**Figura 132**  
Pedido do comand list ao servidor.



O comando LIST pedirá uma lista com as mensagens no servidor. Compreenda o processo por meio da figura 132 e das explicações a seguir.

- A. Identifica o usuário “destinatario” e a senha “informatica”.
- B. Pede a lista com e-mails que estão no servidor pelo comando LIST. O servidor listou somente um e-mail.
- C. Solicitando com o comando RETR a mensagem número 1. Abaixo, as linhas são as respostas do servidor com o conteúdo da mensagem.

- D. Comando DELE, para remover a mensagem número 1 do servidor.
- E. QUIT pede para encerrar a comunicação. Veja que é o servidor que encerra a conexão para o telnet (“a conexão ao host foi perdida”).

20.1.3. WWW

Uma das formas mais populares de uso da internet é a navegação em páginas. As páginas web têm formatos atraentes, coloridos, contêm informações, vídeos, músicas, fotos e são fáceis de usar. São visualizadas por meio de programas chamados navegadores, entre os quais os mais conhecidos, são Internet Explorer da Microsoft, Mozilla FireFox, Chrome da Google, Opera e Safari da Apple. Esses navegadores podem abrir páginas publicadas por uma vasta quantidade de servidores integrados à rede mundial. Quando deseja acessar uma página, o usuário precisa ter em mãos seu endereço, uma **URL** (Uniform Resource Locator, ou Localizador Padrão de Recursos). A URL tem o formato seguinte:

```
http://www.tvcultura.com.br/educacao.
```

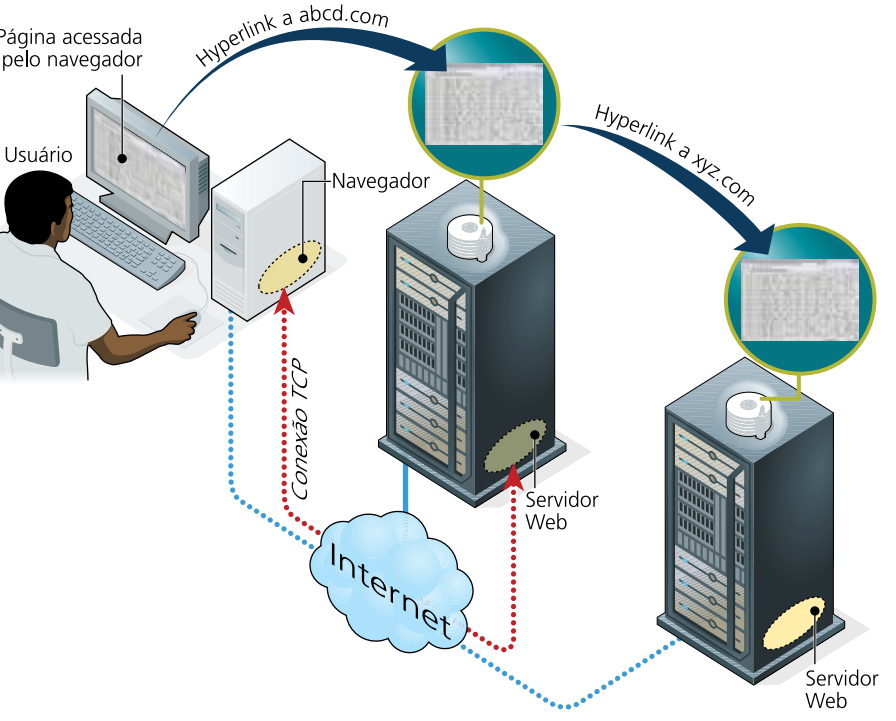
Quando o usuário já tem o nome da página e solicita que o navegador a abra, este se conecta ao servidor de páginas informado na URL. Se encontrar a página, o servidor transmite-a para o navegador por meio da mesma conexão (figura 133).

As páginas podem conter links que, clicados com o mouse, levam a outras páginas do mesmo servidor ou não. Link é um texto que geralmente aparece em azul, sublinhado, e que contém uma URL da página à qual ele se refere, que fica

Cada parte da URL traz uma informação diferente para o navegador. Veja:

- **HTTP**: indica o protocolo da camada de aplicação. Nos navegadores podem ser utilizados HTTP, HTTPS, FTP, FILE, entre outros.
- **//www.tvcultura.com.br**: indica o servidor que hospeda a página solicitada. Após o endereço pode ser encontrado o número 8080 ou outro qualquer, que identifica a porta onde o servidor web aguarda por requisições. Quando esse número não é informado, o sistema utiliza a porta 80, que é a porta padrão para o serviço HTTP.
- **/educacao**: nome da página web solicitada. Quando esta informação não aparece na URL, a página padrão será a página index.html, index.htm, index.php, index.jsp ou default.htm.

**Figura 133**  
Processo de transmissão de páginas e links.





escondida, não é visível. É possível visualizar essa página, contudo, parando o ponteiro do mouse sobre o link, mas sem clicar. No rodapé do navegador será exibida a URL correspondente ao link.

Os navegadores são programas de visualização de páginas HTML (Hyper Text Markup Language, linguagem de páginas), que têm capacidade para conteúdo multimídia. Confira este fragmento de código HTML:

```
<HTML>
<HEAD>
<TITLE>Sou o titulo da página</TITLE>
</HEAD>
<BODY>
<H1>Sou um cabeçalho</H1>
Sou um parágrafo do texto que aparece na página.<P>
E eu sou o segundo. <P>
</BODY>
</HTML>
```

O HTML possui uma nova versão, o XHTML, que estende as funcionalidades do HTML original trazendo características do XML (Extensible Markup Language). As especificações da web são definidas pelo World Wide Web Consortium (W3C).

**HTML** é uma linguagem de marcação por meio de tags que indicam o início do texto (<>) e o fim (</>). Por exemplo: <BODY></BODY>. As marcas sinalizam para o navegador como este deve tratar o texto contido entre elas. As principais tags são:

<HTML></HTML>, que indica o início e o fim da página HTML (o que estiver fora é ignorado).

<HEAD></HEAD>, indica a área para incluir configurações, importações de bibliotecas etc.

<TITLE></TITLE>, que contém o título da página.

<BODY></BODY>, que se refere ao conteúdo da página em si.

Podem ser empregadas várias outras tags. Na WEB 2.0 são comuns as tags adicionais, incluídas por meio de TagLibs (bibliotecas de Tags).

O código HTML também pode ter embutidas outras linguagens, como Scripts Java Script, JQuery, Flash, Silverlight etc.

As páginas podem ser estáticas ou dinâmicas. As páginas estáticas são arquivos HTML que o servidor entrega aos navegadores sem analisar. Ao passo que as de conteúdo dinâmico contêm código PHP, ASP, Java entre outros, que serão executados pelo servidor e irão gerar o conteúdo HTML correspondente às informações solicitadas antes de responder para o navegador. Exemplos de página dinâmica: páginas de internet banking, fóruns, blogs, lojas virtuais.

Existem ainda algumas variações do protocolo. O HTTPS, por exemplo, utiliza criptografia e é empregado em páginas que precisam de maior nível de segu-

rança, como sites de bancos, lojas virtuais etc. O protocolo WAP é aplicado a dispositivos pequenos, como telefones celulares, PDAs, Smartphones, que são mais leves e consomem menos recursos de rede e de processamento.

20.1.4. Transmissão de streaming

Com o aumento da largura de banda oferecida pelas operadoras de internet, torna-se cada vez mais viável o acesso a rádios on-line, TVs, canais de filmes, sites que fornecem vídeos on-demand (sob demanda, quer dizer, que aceitam novas conexões à medida que aumentam as solicitações dos clientes) e ainda videoconferências e serviços de telefonia pela internet (Voip, ou voz sobre IP). Esse tipo de transmissão é chamado de streaming (transmissão por fluxo de dados), termo para transmissões multimídia ininterruptas por uma fonte a vários clientes e ao mesmo tempo. A transmissão de streaming depende de uma largura de banda razoável e também de qualidade estável do serviço para evitar interrupções e processos de buffering.

As transmissões de fluxo de dados (streaming) são iniciadas pelos clientes reprodutores multimídia. Vários podem conectar-se no mesmo servidor multimídia, o que se caracteriza como um encaminhamento unicast – quando vários pacotes de origem diferente são encaminhados para um mesmo endereço.

20.1.5. Áudio e vídeo

A transmissão streaming é utilizada principalmente para áudio e vídeo. Devem exibir o conteúdo transmitido de forma linear, sem falhas e com uma resolução razoável. Para popularizar a internet como meio de difusão de conteúdo multimídia em tempo real foram desenvolvidas algumas novas tecnologias. Foi preciso reduzir o máximo possível a quantidade de bytes necessários para recriar a imagem ou o som no micro do usuário, como também controlar a frequência da transmissão de dados da rede do usuário, que pode oscilar ou ser insuficiente. Também foi preciso desenvolver formatos (codecs) compactados, com ou sem perda, como mp3Pro, MP4, QuickTime da Apple, Ogg Vorbis, Windows Media Player (figura 134), entre várias outras, além de técnicas de proteção como **Buffer Underrun Protection**.

O buffer (área usada para armazenar dados) é utilizado sempre que o computador precisa ler dados de uma fonte que não tenha velocidade de transmissão constante. Os dados são armazenados antes de o processo começar a consumi-los, de modo a garantir a fluência da transmissão. Tocadores de vídeo e áudio sob demanda, por exemplo, levam buffers: primeiro carregam parte do conteúdo e só depois começam a tocar. Ou seja, o tocador obtém as informações do buffer, e não diretamente da rede. O buffer underrun acontece quando o processo demanda dados e encontra a área de armazenamento vazia porque a velocidade de consumo de dados é maior que a de alimentação do buffer.

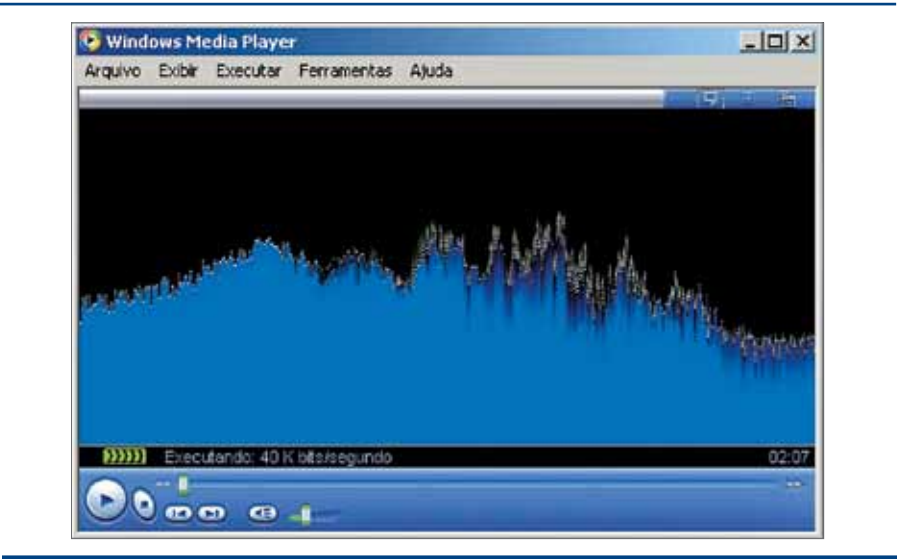
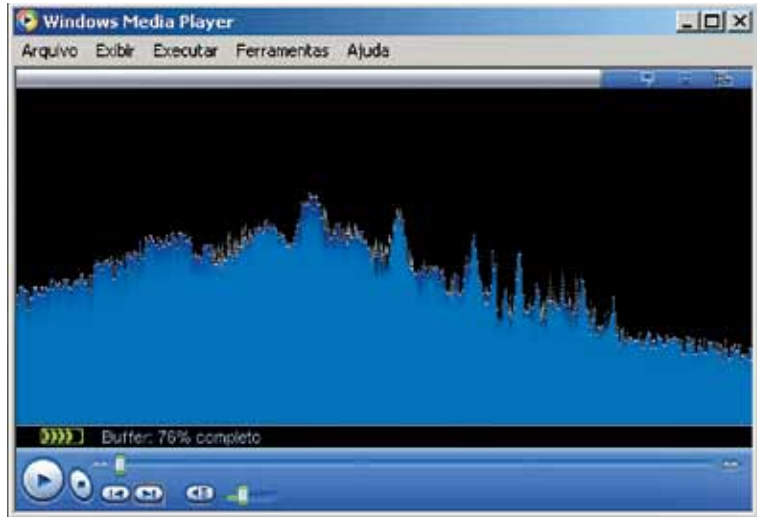


Figura 134  
Formato para transmissão streaming.

Figura 135

Tocador de multimedia recarregando o buffer, após um buffer underrun.



É comum percebermos que o som às vezes para quando escutamos uma rádio online. Se olharmos para o tocador, veremos uma mensagem de buffering, indicando algum percentual. Isso acontece porque os players multimídias utilizam a técnica Buffer Underrun Protection, que possibilita armazenar dados. A técnica é importante porque streaming demandam muitos bytes e a conexão de internet pode ser mais lenta que essa demanda ou o serviço ter baixa qualidade e declinar em alguns momentos. Para resolver tais problemas os players de vídeo de áudio armazenam alguns segundos da transmissão na memória, de modo que possa suprir a falta de dados em determinados momentos. Porém, se o buffer se esvazia por completo, é necessário recarregá-lo antes de prosseguir (figura 135).

Protocolos

**RDP (Remote Desktop Protocol):** o Protocolo de Área de Trabalho Remota é empregado para transmissão de dados da camada de aplicação. Permite transmitir áudio e vídeo em vários canais de uma transmissão da aplicação Microsoft **Terminal Service**, encontrada nas versões mais atuais do Windows por meio do atalho “Conexão de Área de Trabalho Remota do Windows”. Empresas que possuem um grande computador e vários terminais não costumam instalar os softwares proprietários em todos eles. Os usuários acessam um programa chamado Terminal Service, por meio do qual podem conectar-se ao servidor e iniciar uma sessão Windows como se estivessem trabalhando na máquina local. Podem ver o vídeo da área de trabalho e ouvir o áudio dos alertas.

**RTP/RTCP, Real Time Protocol e Real Time Control Protocol:** o Protocolo de Tempo Real e o Protocolo de Controle de Tempo Real são utilizados em conjunto e foram desenvolvidos para transmitir áudio em tempo real. O RTP pode fragmentar as mensagens enviadas, enquanto o RTCP controla a entrega das mensagens, colocando-as na ordem correta antes de chegarem ao reproduzidor de áudio. O RTCP também controla os pacotes perdidos durante a transmissão pela rede e tenta manter a qualidade do áudio em

patamar aceitável. São muito utilizados em VoIP (voz sobre IP) e são especificados na RFC3550.

**RTSP, Real Time Streaming Protocol:** o Protocolo de Transmissão de Fluxo de Dados em Tempo Real, detalhado na RFC2326, é utilizado para transmitir e controlar a transmissão tanto de áudio quanto de vídeo sob demanda em tempo real.

**MMS, Microsoft Media Service:** é o protocolo proprietário da Microsoft para transmissão de fluxo de dados em tempo real, chamado também de NetShow.

Transmissões de áudio e vídeo por meio de redes de datagramas da internet utilizam o protocolo UDP da camada de transporte, que não oferece controle de garantia de entrega dos pacotes e, assim, não gera resposta para o remetente, diminuindo a sobrecarga da rede e potencializando a velocidade de transmissão.

20.1.6. VoIP

A tecnologia de voz sobre IP foi concebida com a intenção de substituir a telefonia comum das redes de circuitos pela de redes comutadas da internet. O som das ligações telefônicas não precisa de tanta definição, nem tampouco ser stereo. Com isso os dados que o representam não são tão complexos e podem ser transmitidos com mais rapidez. Tais características tornam viável a transmissão de voz pela internet – muitas organizações já percebem no VoIP uma alternativa para diminuir os custos com telefonia (figura 136).

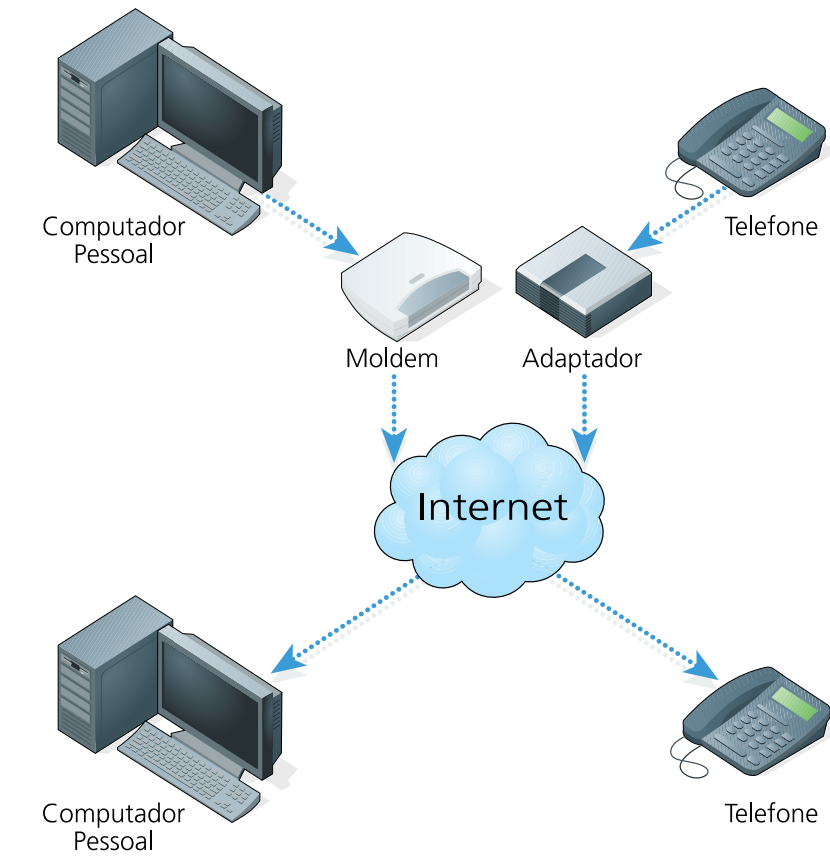


Figura 136

Esquema da tecnologia VoIP.

Uma ligação de um computador para outro, por meio de SoftPhones (softwares telefones), não tem custo algum, pois esses aparelhos não utilizam o serviço de telefonia. Quando são integrados à rede de telefone comum, por meio de um adaptador para telefones analógicos (ATA), possibilitam ligações interurbanas com preço de ligação local. É que algumas operadoras VoIP possuem linhas de telefones analógicos em várias cidades e consideram as ligações entre essas cidades como locais. Para fazer uma ligação de São Paulo para Marília, por exemplo, você discaria o número do telefone fixo que quer contatar em Marília. O servidor gateway da provedora de VoIP compreende e localiza o destino da chamada (Marília). Nesse momento o gateway VoIP fecha comunicação entre o softphone e o ATA que está em Marília e o conecta à linha telefônica analógica local. Ao iniciar a ligação o áudio é transmitido do softphone para o ATA e do ATA para a linha telefônica analógica e vice-versa.

As filiais de uma empresa podem conversar entre si como se usassem ramais telefônicos, utilizando VoIP instalado diretamente em um PABX com função ATA, conectado à internet. Por exemplo: um funcionário que trabalha na matriz de uma empresa em São Paulo deseja falar com outro, da filial de Cuiabá, em Mato Grosso. Ele disca o número da filial mais o ramal do funcionário que precisa contatar. Do aparelho telefônico até o PABX, a ligação utiliza a linha analógica interna da empresa. Depois o PABX abre uma conexão via internet com o PABX de Cuiabá, que disca o ramal desejado. Quando o telefone é tirado do gancho na filial começa a transmissão de dados por meio dos protocolos RTP/RTCP entre os dois PABX e analógica dentro da rede de telefonia interna da empresa. Sem custo nenhum, portanto.

20.1.7. P2P

P2P (Peer-to-Peer, ou de par em par) é o termo para os softwares que fazem transferência de arquivos de um computador para outro. Um dos primeiros desses programas foi o Mirc, um sistema mensageiro que permite trocar texto e transmitir arquivos. Mas o Kazaa, o Napster (veja o quadro *Conquista histórica*) e o Gnutella foram os primeiros a se massificar, por não demandarem solicitação ao dono do arquivo em mensagens de chat. O arquivo desejado pode ser localizado em listas de um servidor e baixado diretamente da máquina em que está armazenado. Com o tempo, essas tecnologias e softwares se multiplicaram, agregando, por exemplo, os softwares Torrents, e-Mule, Kad, eDonkey, entre outros. Essas redes são impulsionadas por conteúdos pirateados: músicas em

Conquista histórica

Em 2001, a indústria fonográfica dos Estados Unidos ganhou uma batalha contra o Napster. Acusado de desrespeitar direitos autorais, o servidor, de uma das redes P2P pioneiras, que se alastrou nos anos 1990 em todo o mundo, acabou banido da web em julho de 2001. O Napster foi tirado do ar após a conclusão do processo movido em 1991 contra seus desenvolvedores pela RIAA, entidade que representa a Warner Music, EMI, BMG, Universal Music e Sony Music.

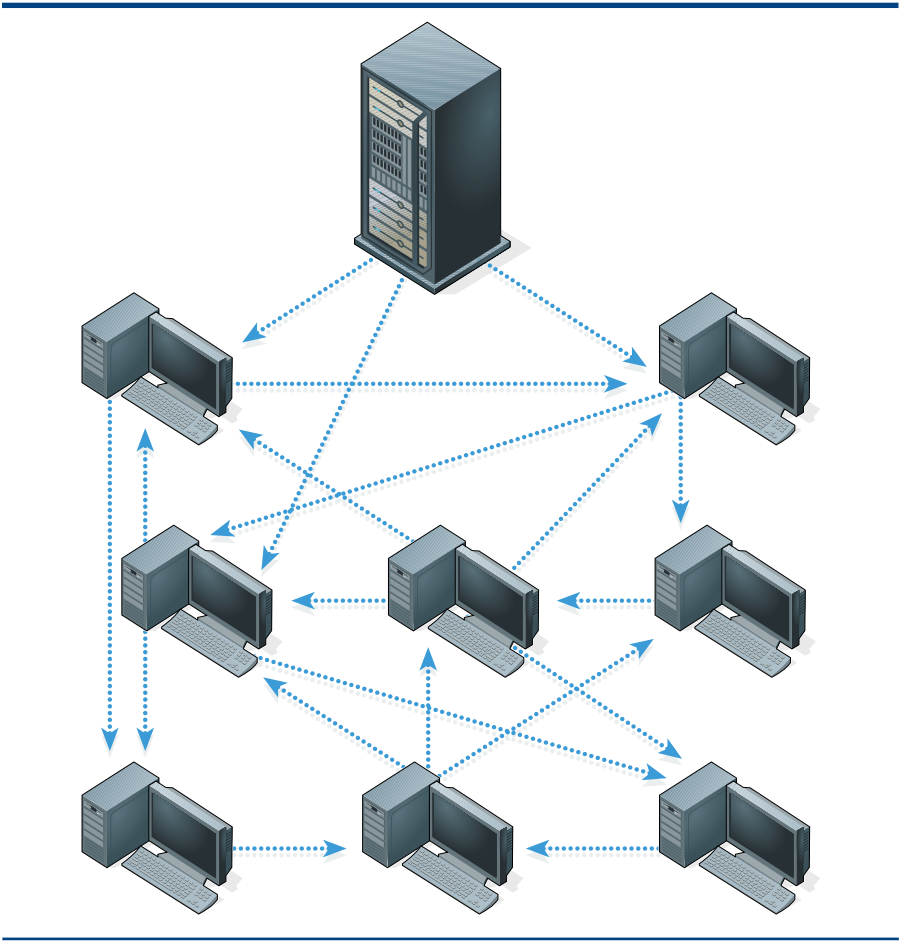


Figura 137  
Compartilhando conteúdo.

mp3, programas e até filmes inéditos em formatos de baixa qualidade filmados diretamente das telas dos cinemas ou conseguidos por meios ilícitos.

Os arquivos nessas redes não estão nos servidores, ficam nos clientes, que juntos formam um grande repositório de arquivos distribuídos (figura 137). Os clientes se conectam e enviam listas do conteúdo compartilhado em seus HDs. Quando deseja algum arquivo, o usuário acessa o site do servidor na barra de endereços ou diretamente pelo software, e solicita uma busca. Então aparece uma lista de títulos similares, que ele precisa apenas selecionar para baixar. Nesse momento o servidor pede que o transmissor abra uma porta UDP de comunicação, que irá aguardar pela solicitação do receptor. Agora só falta que o servidor avise o receptor das informações necessárias para que ele consiga se conectar no transmissor. Assim, a transferência começa. Caso o arquivo se encontre em mais de uma fonte, o cliente pode tentar se conectar para baixar partes diferentes do mesmo arquivo de locais diversos. No final, as partes são agrupadas e o arquivo, reconstituído.

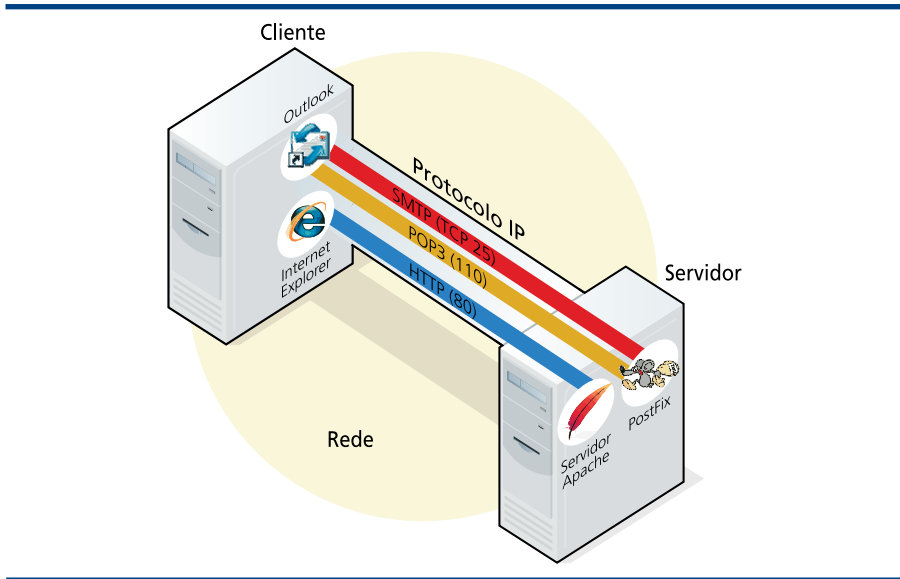
20.2. Camada de transporte

Entre a camada de aplicação e a de redes, encontra-se a camada de transporte. Sua função é dividir as mensagens vindas da camada de aplicação em pacotes menores para que a camada de rede possa repassá-los pelos roteadores da rede. Quando precisa transmitir dados pela internet, uma aplicação de rede tem de abrir uma porta de comunicação de chamada de socket – por meio de sockets podemos



Figura 138

Ligação do software de rede com outro software da rede.



escrever e ler dados como se estivéssemos lendo ou escrevendo em um arquivo (figura 138). O fluxo de bits é transmitido sem que o programador de uma aplicação de rede precise se preocupar com questões como o caminho entre os roteadores da rede, se o pacote está chegando do outro lado da conexão ou se há congestionamento. Isso porque as camadas inferiores cuidam de todos esses serviços.

Além de segmentar as mensagens, acaba sendo papel da camada de transporte assegurar que estas sejam entregues para a aplicação na ordem correta e integralmente, isto é, sem faltar nenhum pedaço. Devemos levar em consideração que a rede IP é uma rede de datagramas e que estes são enviados pela rede, chegando ao seu destino com auxílio de vários roteadores. Porém, por diversos motivos, como congestionamentos e falhas físicas, os pacotes podem se perder. A camada de rede da arquitetura TCP/IP não oferece garantia de entrega dos datagramas, e os dados podem ser duplicados, perdidos ou embaralhados. Todo o trabalho de manter a sequência dos pacotes e controlar erros é atribuição da camada de transporte.

Vejamos também que o socket da camada de transporte é aberto pelo processo da aplicação e, portanto, conecta logicamente um processo a outro de forma direta. Ou seja, a camada de transporte é capaz de ligar logicamente as aplicações e processos, enquanto a camada de rede liga logicamente hospedeiros com outros hospedeiros, host-to-host. A camada de transporte fornece um canal de transmissão de dados fim a fim. Devemos levar em consideração, também, que a conexão é feita socket a socket, pois podem existir vários sockets dentro da mesma aplicação.

A camada de aplicação baseia-se no processo de uma aplicação de rede, a camada de transporte, no processo do sistema operacional e a camada de rede, nos roteadores.

Multiplexação/demultiplexação

Para se comunicar pela rede, uma aplicação pede ao sistema operacional que crie um socket. O socket recebe um número de identificação de 16 bits que chamamos de porta. O número de cada porta pode variar de 1 a 65535. Porém, os sistemas operacionais não costumam utilizar portas de número inferior a 1023, por

serem consideradas reservadas, empregadas por processos conhecidos (a menos que o programa não tenha solicitado explicitamente uma porta específica).

Exemplo da criação de um objeto em Java, responsável por abrir uma conexão UDP na porta especificada 1010:

```
Socket socket = new DatagramSocket(1010);
```

Para transmitir com esse socket, uma aplicação deverá ter sido marcada originalmente e no cabeçalho, com o endereço da máquina de destino e o número da porta do socket. É como identificar o destinatário de uma correspondência postal, na qual informamos o nome da rua e o número da casa. A sequência é a mesma: o IP da máquina e o número da porta do socket. Esse processo leva o nome de multiplexação. Quando o segmento chegar ao hospedeiro, lerá no cabeçalho o número da porta e passará a procurar o socket aberto com a porta correspondente para entregar a este o seu segmento. O processo de abrir o cabeçalho do datagrama, ler as informações nele contidas e entregá-lo ao socket devido é chamado de demultiplexação.

A camada de transporte oferece seus serviços divididos em dois protocolos, o TCP e o UDP. Têm a mesma função básica, que é dividir as mensagens em segmentos e entregá-los na ordem, mas somente o TCP é orientado à conexão e faz o controle da confiabilidade, de erros e congestionamento. O protocolo UDP não é confiável, pois é um serviço sem conexão.

Vamos ver um exemplo de como funciona a multiplexação e a demultiplexação de uma conexão TCP.

Imagine uma aplicação A que precisa transmitir o valor “HELLO” para a aplicação B em máquinas diferentes na rede. A máquina A cria um socket, sem especificar a porta, e o sistema operacional delegará uma porta que não está em uso e é maior que 1023. Vamos utilizar como exemplo a porta 2222. A aplicação informa para o socket que a aplicação de destino está aguardando a mensagem na porta 1032. Tudo certo, agora a camada de transporte já tem as informações

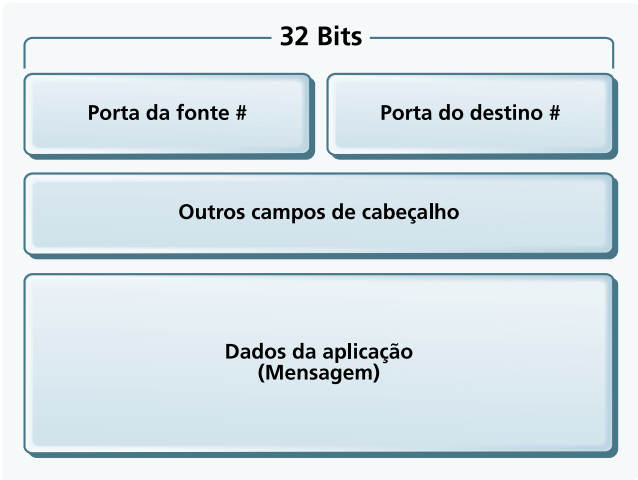


Figura 139

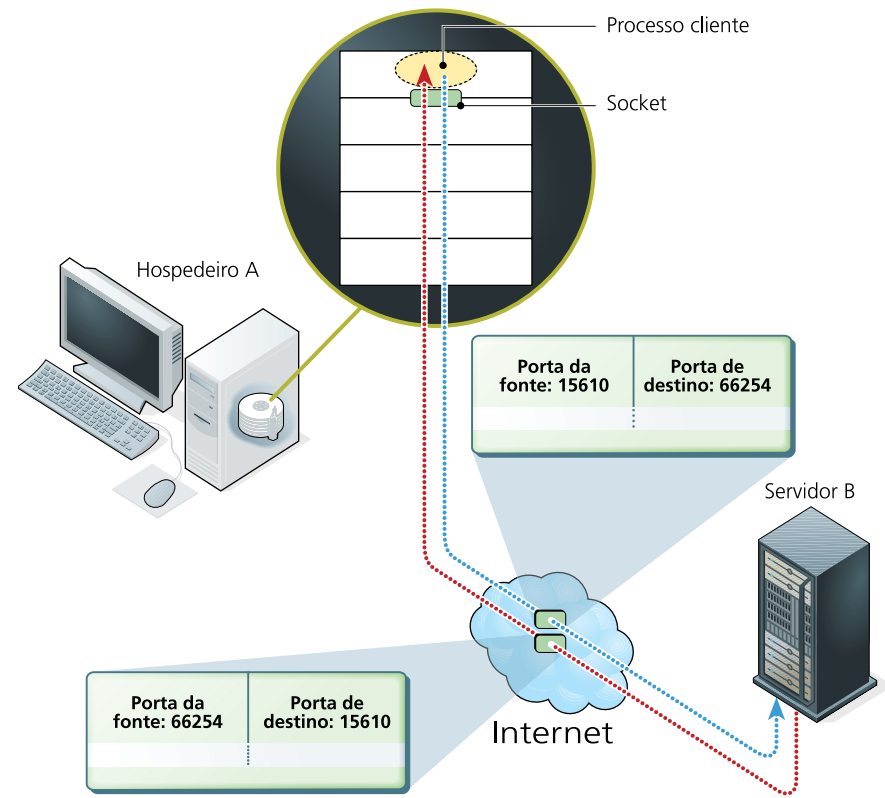
Formato de um segmento TPC com os campos da porta de origem e destino.

para criar um segmento UDP, carregar os seus campos de porta de origem e destino e o dado que será transportado. A multiplexação foi concluída:

Porta Origem: 2222	Porta Destino: 1032	Dado: "HELLO"
--------------------	---------------------	---------------

Com o segmento UDP pronto, a camada de rede necessita do endereço IP da máquina de destino para que seja encaminhado o segmento UDP pela rede até o destino. Digamos que o destino seja o IP 172.16.9.12. Mas a rede irá precisar também do endereço de origem, que será 172.16.9.15. Agora o pacote pode ser entregue à camada de rede e ser enviado. Chegando a mensagem à camada de rede da máquina B, esta repassa o pacote à camada de transporte, que fará a demultiplexação: lerá o cabeçalho do pacote, a informação do número da porta de destino (1032) e localizará, em um banco de dados de portas, o socket carregado na memória que possui tal identificador. Encontrado o socket, o segmento é entregue a ele, e a aplicação consegue ler o dado contido no segmento UDP ("HELLO"). A aplicação analisa o valor e prepara uma resposta (figura 140). Vamos supor que essa aplicação, em sua lógica própria, retorne a palavra "HELLO" para o socket da porta 2222 da máquina A. Para realizar o empacotamento da mensagem em segmentos, o software da máquina B lê o endereço de origem do pacote para obter o número da porta que vai utilizar como destino (2222) e emprega como número de porta de origem o número do seu próprio

**Figura 140**  
Ilustração do envio e resposta UDP.



socket (1032). A camada de transporte monta o segmento, atribui valor aos campos de seu cabeçalho e o entrega para a camada de rede, que anexa os endereços de origem e destino e prossegue com a transmissão.

É bom lembrar que em determinada máquina pode haver várias aplicações de rede rodando, e cada uma pode ter mais de um socket. Ou seja: a camada de transporte é capaz de multiplexar e demultiplexar várias transmissões simultâneas.

O protocolo UDP

Este protocolo não dá suporte à conexão. E por isso ele é bem mais simples que o protocolo TCP. UDP significa User Datagram Protocol, ou seja, Protocolo de Datagrama do Usuário. Esse nome talvez remeta à simplicidade de seus segmentos, que não oferece nenhuma função além das realizadas na camada de rede, onde as unidades lógicas de transmissão também têm nome de datagramas.

Quando uma aplicação precisa enviar um dado, o protocolo UDP não envia antes nenhum tipo de comunicação combinando a conexão ou avisando da transmissão. O dado é enviado simplesmente. Ou seja, antes do envio não é feita uma conexão para saber se o destino existe na rede ou se ele permite o recebimento da mensagem. O processo de origem apenas manda o dado, sem levar em conta se este será ou não recebido.

Apesar de não parecer muito útil, a característica de simplicidade do protocolo UDP se torna especial para algumas aplicações. Veja as vantagens do UDP sobre o TCP:

- A aplicação pode criar seu próprio modelo de conexão, além de evitar o atraso da transmissão do dado, que não precisa aguardar pelo estabelecimento da conexão.
- Os pacotes são mais simples e possuem menos sobrecarga de cabeçalhos. Assim, dados transmitidos por UDP consomem menos recurso de banda.
- Não existe controle do estado da conexão. Para isso o TCP precisa de buffers de envio e destino, sinalizadores de congestionamento e parâmetros de sequência dos segmentos, entre outras informações. Dessa forma, uma aplicação de UDP, como transmissão de áudio e vídeo, pode controlar mais facilmente várias conexões ao mesmo tempo.

Segmento UDP

O segmento **UDP** tem um cabeçalho simples (figura 141), contendo:

**Porta da fonte** – Utiliza 16 bits e indica quem enviou o segmento.

**Porta do destino** – Tem também 16 bits e indica o socket do host de destino.

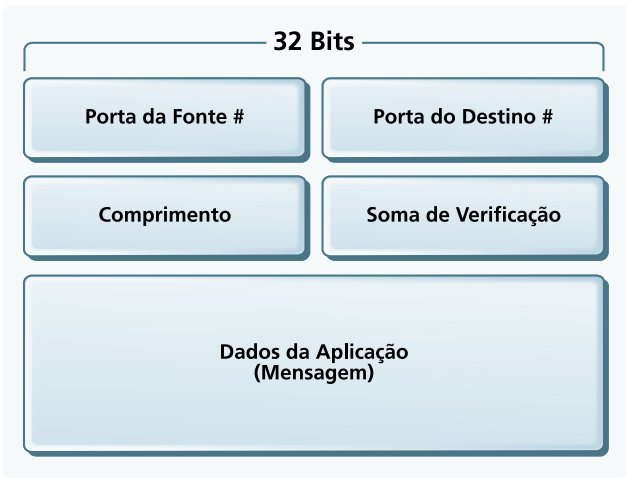
**Comprimento** – Em 16 bits, indica o segmento de dados que será encontrado após os 64 bits iniciais, que forma o cabeçalho do segmento.

**Soma de verificação** – O checksum, como é chamado, é um valor calculado na origem e armazenado neste campo para que, quando a mensagem chegar no

Por suas características, o protocolo UDP se faz especial para aplicações que não sofrem com alguma perda insignificante de dados, em transmissões multimídia, por exemplo. Se perdermos um milésimo de segundo de uma música que estamos ouvindo em uma rádio on-line, nem perceberemos a falha. Mas a falta de um pedaço da notícia em uma página web de jornalismo pode causar muita confusão. Ou seja, o UDP não é recomendado para aplicações que demandam transmissão precisa das informações. Outra vantagem do UDP é não fazer o controle de congestionamento. Assim, mesmo que uma conexão da rede esteja congestionada, o pacote será enviado e transmitido até seu destino. O protocolo DNS utiliza UDP para se comunicar, pois precisa ser enviado de qualquer forma, mesmo em ambiente congestionado. Porém, como o controle ajuda a impedir congestionamentos na rede, deve-se evitar o uso de conexões UDP em ambientes que demandam, contínua disponibilidade de banda.

Figura 141

Formato do segmento UDP.



destino, seja feito o mesmo cálculo. Se os valores resultarem iguais, indica que a mensagem chegou integralmente.

Protocolo TCP

O TCP – Transfer Control Protocol (RFC 793), ou Protocolo de Transferência com Controle, implementa uma solução confiável de envio de dados fim a fim.

Para garantir a confiabilidade, o TCP demanda uma resposta para cada segmento enviado, sinalizando que o pacote chegou ao destino. Se a resposta da entrega não chegar à origem durante determinado tempo, o segmento é considerado perdido e reenviado até que se obtenha a resposta de confirmação ou que a quantidade máxima de vezes de reenvio do pacote chegue ao limite. Isso leva à conclusão de que o processo de destino não está respondendo ou que a rede está congestionada.

A sinalização de entrega é feita por um bit denominado ACK, sigla para a palavra acknowledge, que neste contexto indica que o bit foi aceito no destino.

O TCP também age no controle do sequenciamento dos segmentos, identificando quando um pacote foi enviado duas vezes, ou se falta algum pacote entre os que foram recebidos. Para isso há um número sequencial em cada pacote (figura 142).

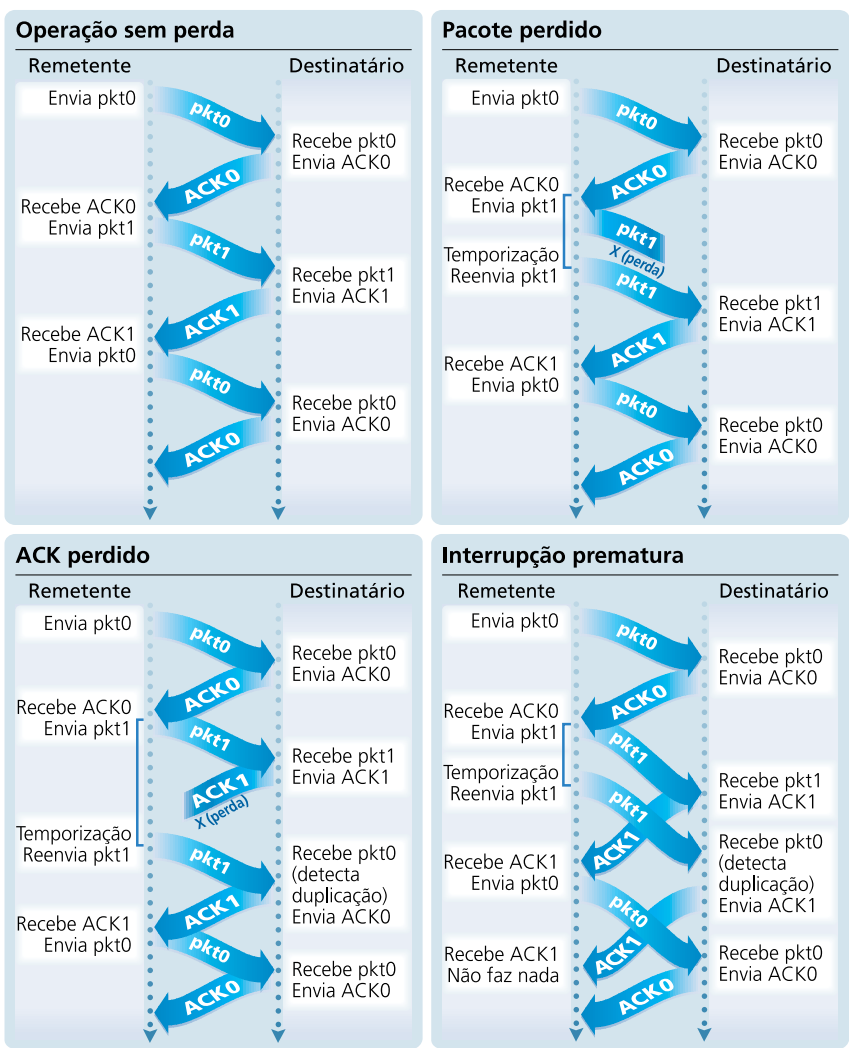
Como o nome diz, TCP é um protocolo de controle, que negocia entre as partes como se dará a conexão antes que um dado seja enviado e mantém o estado da conexão, mesmo que as camadas inferiores da rede não ofereçam controle de estado – esse controle é feito no nível da camada transporte no protocolo TCP.

O estado da conexão permite ao TCP transmitir informações de um ponto da conexão a outro nos dois sentidos, enviando ou recebendo dados, ao que chamamos de serviço full-duplex. Transmissões para vários destinatários, ou multicast, não são possíveis, pois as conexões são feitas apenas entre dois processos.

Para que uma conexão seja estabelecida, as duas partes devem se apresentar fazendo uma comunicação inicial em três passos (3-way handshake). O cliente da conexão

Figura 142

O TCP mantém o estado da conexão.



envia um segmento para o servidor (1), e este responde pedindo uma identificação (2). O cliente responde com sua identificação (3) e, então, o servidor pode aceitar a conexão e começar a transmitir dados – ou não aceitar, cancelando a conexão.

Segmento TCP (figura 143)

**Porta da origem** – 16 bits para o número do socket que envia o segmento.

**Porta de destino** – 16 bits para o número da porta do socket ao qual o segmento se destina.

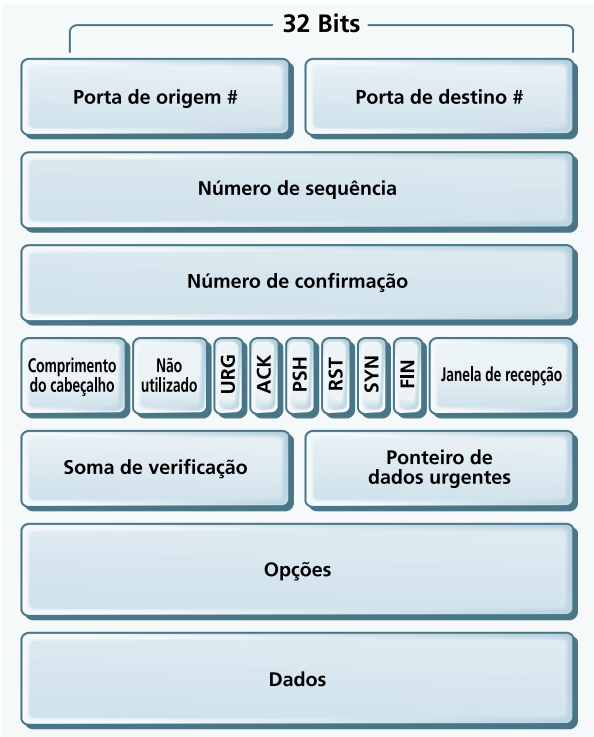
**Número de sequência** – 32 bits para identificar um a um os segmentos da transmissão para que não sejam repetidos ou apontar se faltou algum.

**Número de confirmação** – Número de sequência do segmento anterior ao atual. Faz com que o algoritmo conclua qual é o número esperado para o próximo pacote. Os campos Número de sequência e Número de confirmação trazem as informações necessárias para implantar uma conexão confiável.



Figura 143

Formato do segmento TCP.



**Flags** – Possuem 6 bits, e cada um indica uma informação booleana:

URG	Urgente : 1 – Sim / 0 – Não
ACK	Utilizado em conjunto com SYN. Se SYN = 0, e ACK = 1 “segmento recebido”
PSH	Passar dados para camada superior: 1–Sim / 0 – Não.
RST	Ressetar a transmissão, comprometida por muitas falhas: 1 – Reiniciar / 0 – Continuar transmitindo
SYN	Utilizado em conjunto com ACK. Faz parte da negociação da conexão: Com SYN = 1, então ACK = 1 “Conexão Aceita” ACK = 0 “Conexão Requisitada”
FIN	Encerra conexão: 1 – Sim / 0 – Não

**Tamanho de janela de recepção** – Serve para indicar ao transmissor o tamanho disponível de buffer no destinatário, de modo que o transmissor diminua a velocidade de transmissão e evite a perda de bits que não possam ser armazenados no destino.

**Soma de verificação** – Tem a mesma função no protocolo UDP. É um cálculo feito com o conteúdo do segmento, cujo resultado deve ser igual ao do cálculo no destino.

**Ponteiro de dados urgentes** – Indica para a camada de aplicação quando uma mensagem foi marcada como urgente na origem e a posição do último segmento dessa mensagem. Esse campo tem 16 bits.

**Opções** – Trazem informações não obrigatórias e não têm limite de tamanho. Podem então conter informações que auxiliam na transmissão desse segmento por condições especiais. Para um estudo aprofundado dessas opções, é interessante estudar as RFCs do TCP 854 e 1323.

**Dados** – São os dados enviados pela aplicação.

20.3. Camada de rede

É composta por um conjunto de protocolos que permitem que uma mensagem da camada de transporte seja repassada através da rede até chegar ao destino. Funciona como os correios: a carta é postada e levada ao destino, passando no caminho por várias centrais de distribuição. Portanto, a camada de rede define os trâmites para que as informações caminhem na rede até seu destino, de forma colaborativa. Várias redes e computadores se juntam para formar uma única malha. Se o destinatário estiver em outra filial da empresa, outra residência, cidade ou país, a camada de rede faz com que o pacote seja repassado para vários roteadores que ligam várias redes e ajudam na entrega da mensagem, de maneira tal que utilize a melhor rota, mais curta ou mais rápida.

20.3.1. Serviços oferecidos pela camada de rede

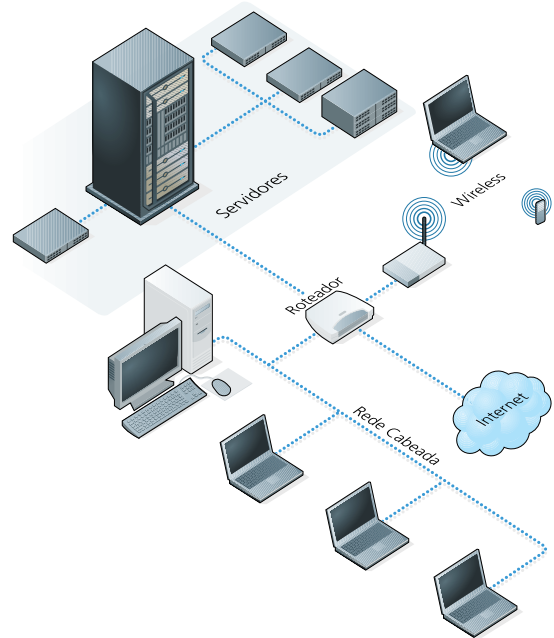
A tarefa dessa camada, então, é fazer a transmissão de pacotes de um host (hospedeiro) a outro. Se os computadores estiverem em uma rede local, a tarefa até pode ser simples, mas percebemos sua real complexidade quando o cenário muda para a internet. Desde quando sai do computador de um professor situado em Franca, por exemplo, e chega a uma escola em São Paulo, um e-mail terá caminhado por vários roteadores que se ligam a várias redes. Podemos visualizar um exemplo dessa situação quando executamos o comando tracert no prompt de comando do Windows ou tracerout no Linux.

```
C:\>tracert tvcultura.com.br
Rastreando a rota para tvcultura.com.br [200.136.27.81]
com no máximo 30 saltos:
 1  2 ms  1 ms  1 ms 192.168.1.1
 2  *    *    *  Esgotado o tempo limite do pedido.
 3 39 ms 16 ms 14 ms 200-225-219-206.static.ctbctelecom.com.br
[200.225.219.206]
 4 37 ms 28 ms 29 ms ansp.ptt.ansp.br [200.136.34.1]
 5 37 ms 23 ms 38 ms unip.ptta.ansp.br [200.136.37.16]
 6 37 ms 37 ms 43 ms 200.136.27.81
Rastreamento concluído.
```

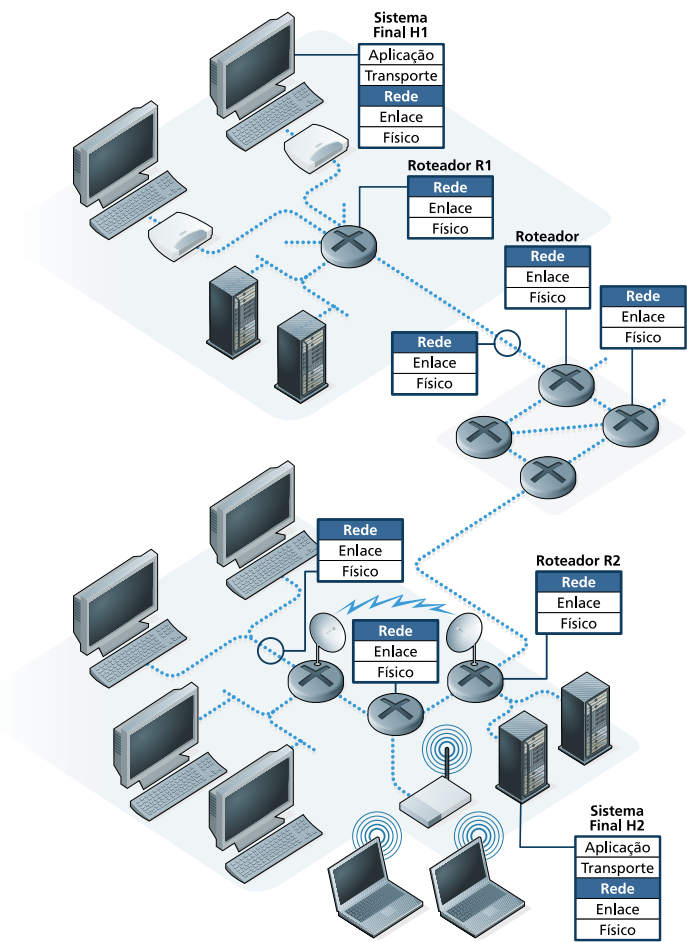
No rastreamento acima vemos que, para chegar até o host da TV Cultura, um pacote passou por 5 roteadores, perfazendo 5 passos. Saiu de uma rede local através do gateway 192.168.1.1, passou pelo roteador 200-225-219-206.static.

O cabeçalho do TCP é maior que o do UDP. Um segmento UDP tem no máximo 8 bytes enquanto o TCP chega a até 20 bytes.

**Figura 144**  
Funcionamento  
do roteador.



**Figura 145**  
Ligação entre redes.



Os equipamentos da rede responsáveis por levar pacotes de uma rede a outra devem ser capazes de realizar duas funções denominadas repasse e roteamento.

**Repasse:** é a tarefa de levar um pacote de uma interface ligada a uma rede “A” (enlace) para outra ligada a uma rede “B”.

**Roteamento:** é um algoritmo que analisa o tráfego de rede entre os pontos que estão transferindo pacotes para verificar o caminho que eles estão seguindo.

Repasse e roteamento geralmente são realizados por equipamentos chamados roteadores (figura 144). Esses equipamentos fazem interconexão com várias redes. Cada ligação com uma rede é chamada de interface, por onde os pacotes chegam ou saem (figura 145). São equipados com processadores de roteamento, que processam programas para consultar e manter as tabelas de repasse, além de rotinas de gerenciamento da rede.

Além dos serviços de repasse e roteamento, algumas redes como ATM, Frame Relay e X.25 necessitam estabelecer conexão entre os roteadores, antes que algum pacote seja transmitido. A internet não utiliza o serviço de conexão.

Os roteadores também são usados para formar redes residenciais, que se tornam mais comuns a cada dia. Nesse caso, utilizam-se roteadores sem fio para compartilhar internet entre os PCs e notebooks da família.

### 20.3.2. Modelo de serviços

Há duas maneiras de controlar a comutação dos pacotes através dos roteadores da rede: por circuitos virtuais ou por datagramas. As redes baseadas em circuitos virtuais utilizam o número do circuito para sinalizar o pacote, enquanto a rede de datagramas emprega os endereços de origem e destino. A internet utiliza comutação por datagramas, enquanto outras redes como ATM, X.25 e Frame Relay recorrem a circuitos virtuais.

#### 20.3.2.1. Rede de circuitos virtuais

Circuitos virtuais são análogos a circuitos fim a fim. É como se duas máquinas estivessem ligadas direta e exclusivamente uma à outra. Sempre que uma comunicação se inicia entre duas máquinas de uma rede de circuitos virtuais, um novo circuito é criado e um número é atribuído a ele. Esse número de circuito e a interface de enlace, de origem e destino, serão registrados na tabela de repasse de todos os roteadores que, no caminho, participam da retransmissão do pacote. Todos os pacotes da transmissão sempre usarão o mesmo caminho, eliminando a necessidade de controlar a entrega ou a ordem dos pacotes. O estado da rede é controlado e, quando uma conexão termina, o circuito é removido das tabelas de repasse, criando-se um novo sempre que uma conexão se inicia. A comutação nesse modelo de rede é bem rápida, pois os endereços de origem e destino do pacote não precisam ser analisados em uma faixa de caminhos possíveis. É necessário apenas consultar nas tabelas de repasse um índice único em uma tabela indexada.

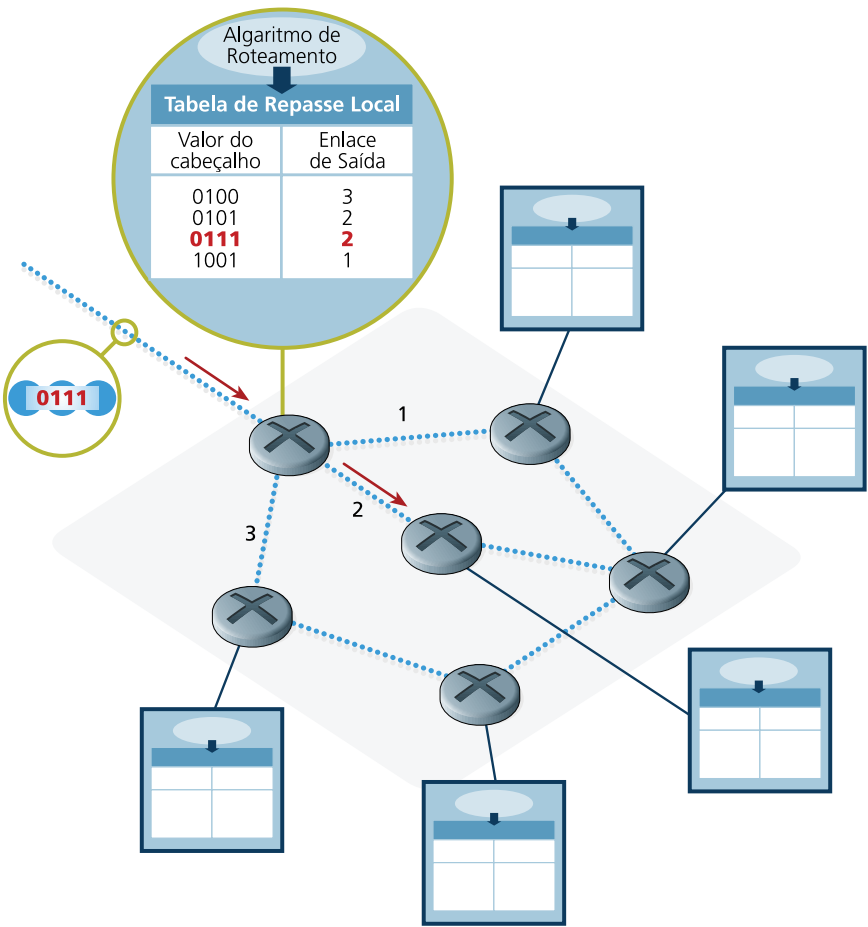
#### 20.3.2.2. Rede de datagramas

Diferentemente da rede de circuitos virtuais, a rede de datagramas, como citado anteriormente, não cria um canal de comunicação do início ao fim do trajeto. Os pacotes são entregues na rede através de uma interface e cada computador ligado ao barramento dessa interface auxilia no encaminhamento até o destino.

ctbctelecom.com.br, depois pelo ansp.ptt.ansp.br, pelo unip.ptta.ansp.br e finalmente chegou ao destino 200.136.27.81, que é o endereço do host que hospeda o site tvcultura.com.br no endereço IP 200.136.27.81.

Figura I46

Na rede de datagramas os pacotes são tratados individualmente.



Mas não há garantia de entrega. Os pacotes são tratados individualmente, e podem seguir caminhos diferentes pela rede, ficando vulneráveis a congestionamentos ou falha de alguma conexão no meio do trajeto. Os dados devem ser bufferizados (armazenados) e reorganizados no destino, como mostra a figura 146.

Um comutador sabe para qual interface de saída ele deve repassar o pacote por meio de consulta em uma tabela indexada contendo o registro de várias redes e a interface que leva até elas. Nesta rede o estado não é controlado, pois não há conexão entre os nós da rede. A descoberta das rotas é realizada por protocolos que implementam algoritmos de busca e anúncio da presença na rede.

20.3.3. Roteamento

Hosts de uma mesma rede, ou seja, conectada no mesmo barramento, conhecem e repassam as informações entre si. Mas quando um pacote é destinado a um host na internet, esse pacote é encaminhado para o gateway dessa rede. Este por sua vez retransmite o pacote a outro gateway ou a algum que o reencaminhará ao host de destino ou ainda um gateway dentro de sua hierarquia. Podemos dizer que gateway, como o próprio nome diz (gate = portão e way = caminho, caminho do portão), indica que essa máquina tem acesso à saída da sub-rede, ou seja, a que consegue levar o pacote para fora, ou vice-versa.

20.3.3.1. Descoberta de rotas

O papel do roteamento é descobrir o caminho mais curto e mais rápido para repassar o pacote, seja diretamente para o gateway da rede onde o host de destino está ou para outro roteador mais próximo do destino. Para isso, ele deve conhecer os roteadores vizinhos. E, se for um gateway, precisa também conhecer os roteadores e computadores internos da sua rede. Assim, sempre que um pacote chega até a interface de enlace desse roteador, ele consulta uma tabela na qual constam os computadores e roteadores da rede para saber qual é o melhor caminho a ser escolhido.

Antes do envio, no entanto, o pacote é armazenado. E, no caso da internet, o número IP do destino é analisado e comparado com as regras de repasse registradas. A seguir, o roteador escolhe a rota mais conveniente e encaminha o pacote para a interface onde está o próximo roteador, que, por sua vez, irá levar o pacote até o respectivo host.

Podemos comparar os roteadores a automóveis em um cruzamento de uma estrada. O veículo seria o pacote; o departamento de engenharia de tráfego, o algoritmo de roteamento, e as placas de sinalização seriam a tabela de repasse. O departamento de engenharia, no caso, prepara as placas com as rotas e suas distâncias. Quando chega ao cruzamento, o motorista pode escolher, por meio das placas, o melhor caminho a seguir para chegar mais rapidamente ao seu destino, mesmo que para isso seja necessário passar por outros cruzamentos.

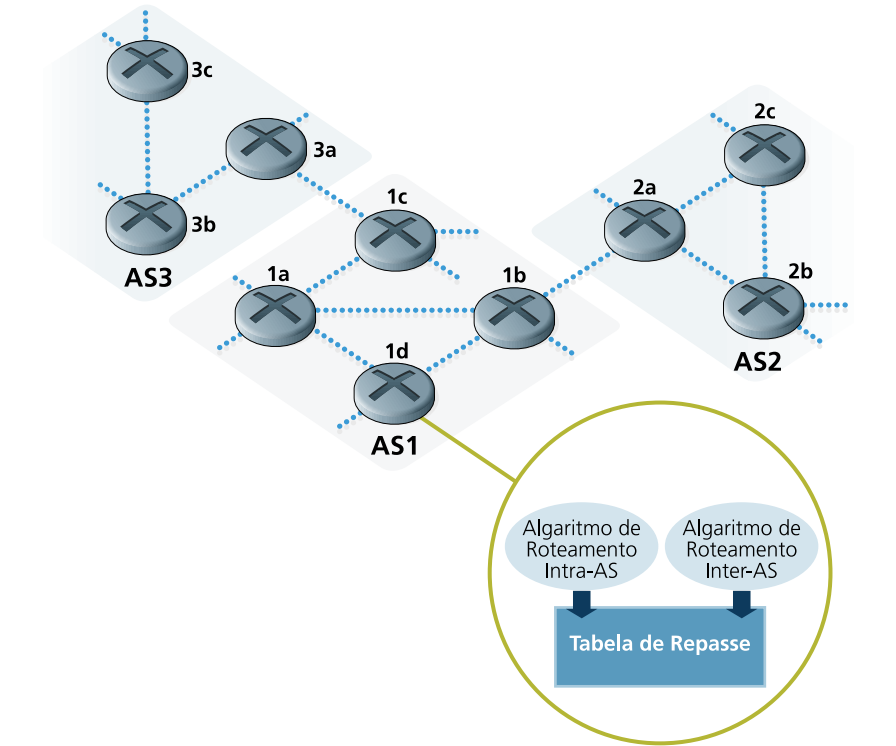


Figura I47

Sistemas autônomos podem se conectar por meio de roteadores gateway.



20.3.3.2. Manutenção

É grande a quantidade de roteadores que podem estabelecer uma comunicação entre si. Por isso, foram desenvolvidos protocolos com algoritmos de roteamento capazes de analisar as rotas possíveis e preencher, automaticamente, a tabela de repasse com as distâncias a serem percorridas (figura 147). Esses protocolos também atualizam as informações e removem rotas interrompidas ou muito distantes. Além disso, podem controlar as regiões internas e externas, denominadas AS, Autonomous Systems, ou seja, Sistemas Autônomos.

As AS podem ser os roteadores que ficam sob o controle de uma mesma estratégia de roteamento, ou seja, são controladas por um ISP (Internet Service Provider ou Provedor de Internet). Também podem ser roteadores pertencentes a uma rede privada ou pessoal. Uma AS é vista por outras ASs como um único indivíduo. Porém, só o gateway das AS é visível. A estrutura existente dentro de cada uma nunca é descoberta pelas demais. Elas podem se conectar por meio de roteadores gateway.

**Figura 148**  
Hipótese de roteadores e suas interfaces.

20.3.3.3. Algoritmos de roteamento

Quem administra as listas de roteamento e decide para qual interface de saída do roteador um pacote deve ser transmitido é um software. Esse programa utiliza diferentes tipos de algoritmos desenvolvidos para solucionar tipos específicos de problemas, como mostra o quadro *Modelos mais comuns de algoritmo*. Isso inclui fatores como a otimização da performance, a adaptabilidade das interrupções, o congestionamento e a confiabilidade dos caminhos.

Existem basicamente dois tipos de algoritmos. Os estáticos, que atualizam suas tabelas apenas quando a rede é iniciada (mas não quando ocorrem mudanças durante o tempo em que estão em funcionamento), e os dinâmicos, capazes de adaptar suas tabelas regularmente.

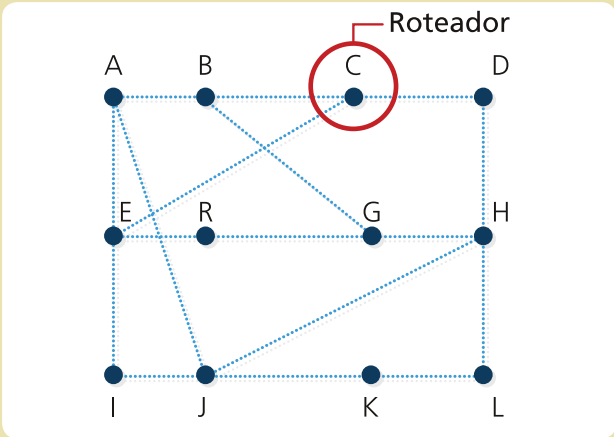
Este segundo tipo consegue se recuperar instantaneamente de alterações ocorridas nas ligações da rede, sem necessitar de qualquer intervenção.

**Figura 149**  
Hipótese de roteadores e suas interfaces.

Modelos mais comuns de algoritmo

Conheça a lógica utilizada pelos roteadores na busca pela melhor rota para encaminhar pacotes.

**Algoritmo estático de menor distância:** analisa a rede para obter a quantidade de passos necessários para chegar a todos os nós adjacentes. Quando um pacote chega ao computador, esse algoritmo escolhe o caminho que permitirá passar pelo menor número possível de roteadores até o destino.



**Algoritmo estático de roteamento por inundação:** também conhecido por “flooding”, esse algoritmo retransmite cada pacote de entrada para o maior número possível de interfaces de saída, pulverizando o pacote em

várias cópias. Porém, pode acontecer de o pacote ser retransmitido infinitamente pela rede. Essa inundação deve ser controlada com o uso de um contador atribuído ao pacote, que registra cada passagem por um roteador. Esse contador é inutilizado assim que determinada quantidade de passos for atingida.

**Algoritmo dinâmico com vetor de distância:** nesse tipo de algoritmo, os roteadores se comunicam trocando informações sobre distância das rotas com roteadores vizinhos. A distância pode ser medida em hops (saltos), comprimento de fila ou latência das repostas. A escolha de uma ou outra depende da unidade de medida usada pelos roteadores da rede. Sempre que uma nova mensagem de atualização chega, o algoritmo dinâmico com vetor de distância compara as informações de distância do roteador que enviou a mensagem (como exemplo e em referência à imagem, vamos chamá-lo de “J”) em relação a seus vizinhos. A partir daí, analisa qual é a sua própria distância até os roteadores vizinhos de “J”. Depois, a rota para os vizinhos de “J” será incluída no vetor do roteador que está recebendo a mensagem, considerando “J” como ponto de partida. Por meio da análise da mensagem que contém os

dados sobre as rotas registradas em sua tabela, esse algoritmo insere novas informações na tabela de rotas local, respeitando sempre a ordem crescente, ou seja, da mais curta para a mais longa. Toda a informação sobre uma distância é armazenada, mesmo que esse dado já exista na tabela e que a distância até determinado ponto, utilizando outros caminhos, já tenha sido incluída. Essa informação será valiosa quando uma rota preferencial se tornar indisponível. Então, surgirá a informação sobre a rota alternativa, ainda que seja mais demorada que a antiga preferencial.

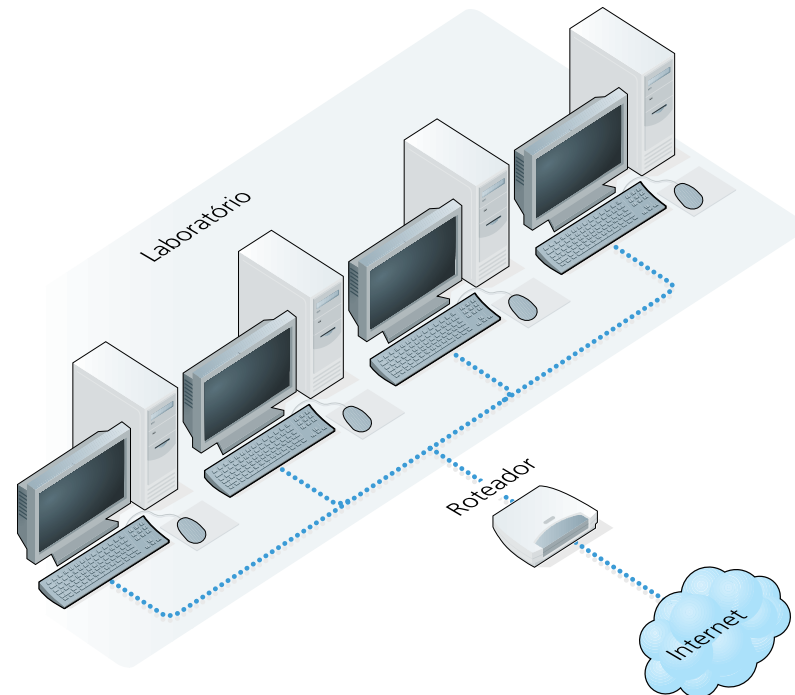
**Algoritmo dinâmico de estado de enlace:** assim como ocorre no algoritmo de vetor de distância, esse tipo se comunica com outros roteadores para alimentar suas tabelas de rotas, mas de forma diferente. No vetor distância, um roteador se comunica apenas com os roteadores vizinhos, recebendo deles informações a respeito do custo de todas as rotas sobre as quais eles têm conhecimento. Já no algoritmo de estado de enlace, o roteador envia, por difusão, para todos os roteadores da rede as informações sobre a distância apenas dos roteadores que estão diretamente ligados à outra ponta de cada uma de suas interfaces de enlace. Dessa forma, as mensagens curtas são

recebidas, porém, em maior quantidade. Isso porque cada roteador da rede recebe mensagens de todos os outros. No vetor distância, as mensagens com vetores extensos podem ser recebidas, desde que venham dos roteadores vizinhos.

Para					Nova estimativa de atraso a partir de J	
	A	I	H	K		Linha
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	-
K	24	22	22	0	6	K
L	29	33	9	9	15	K
JA		JI	JH	JK	Nova tabela de repasse para J	
atraso é 8		atraso é 10	atraso é 12	atraso é 6		
Vetores recebidos dos quatro vizinhos						

**Figura 150**

Roteamento em um laboratório de informática de uma escola.



#### 20.3.3.4. Roteamento na internet

O roteamento na internet funciona de forma hierárquica. As redes se agrupam em sub-redes, que podemos visualizar quando analisamos o que está à nossa volta. Por exemplo: uma rede de computadores de uma escola, que se liga a um roteador e que, por sua vez, se liga à internet por meio de um provedor (figura 150).

A escola é um sistema autônomo AS. A provedora de internet, com todos seus clientes, formam uma outra AS, sendo a AS da escola uma sub-rede da provedora de internet. Os protocolos da internet são divididos em dois tipos: os que controlam o repasse dentro de uma AS e suas sub-redes e os que monitoram as rotas para outras AS.

#### 20.3.3.5. Protocolo IGP (Internal Gateway Protocols)

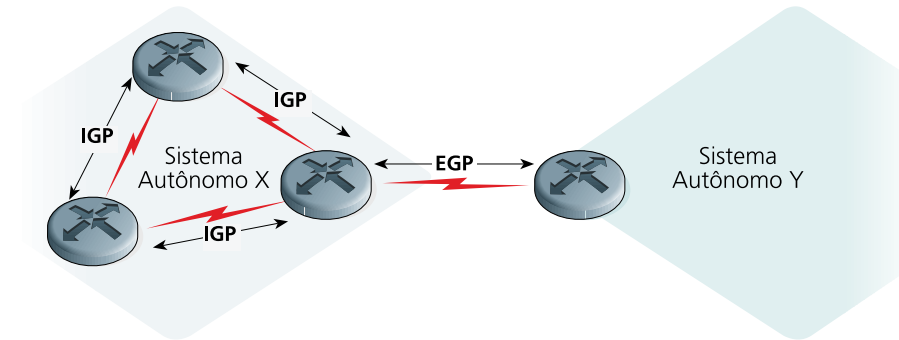
O IGP (Internal Gateway Protocols ou Protocolo de Roteamento Interno) controla as rotas dos hosts dentro de uma AS. Um desses protocolos é o Open Shortest Path First – OSPF (Protocolo Aberto Menor Caminho Primeiro), que utiliza um algoritmo de menor caminho. O OSPF registra na tabela as informações de identificação da interface, o número do enlace, a distância e a métrica. Outro protocolo IGP utilizado é o RIP (Route Information Protocol, ou seja, Protocolo de Informações de Roteamento), que é baseado no algoritmo vetor distância.

#### 20.3.3.6. Protocolo EGP (Exterior Gateway Protocol)

O protocolo do tipo EGP é útil, por exemplo, quando uma empresa tem dois ou mais links de internet e necessita fazer o balanceamento do tráfego ou manter a redundância para o caso de algum dos links falhar.

**Figura 151**

Protocolo EGP.



Os roteadores que fazem a ligação com outras AS são chamados roteadores de borda e utilizam o protocolo **BGP** (Border Gateway Protocol ou Protocolo de Roteador de Borda). O BGP faz com que todas as ASs da internet tomem conhecimento das suas sub-redes e possam receber dados vindos de outros Sistemas Autônomos (figura 151).

#### 20.3.3.7. Interligação de redes

Em sua maioria, as redes vêm convergindo para o padrão TCP/IP utilizado na internet. Porém, não é difícil encontrar redes sem fio, ATM, AppleTalk ou SNA da IBM conectadas à internet e trocando informação entre si como se estivessem trabalhando sob uma mesma tecnologia. Vamos imaginar um cenário simples: o sinal de internet que chega em nossa residência vem de uma rede telefônica (WAN), que pode utilizar ATM. Esse sinal é compartilhado com uma sub-rede de notebooks (LAN) que se interligam por meio de um roteador sem fio do tipo 802.11. Essa situação já mostra a necessidade de se implementar meios para a interconexão de redes. As diferenças entre as redes podem estar em vários aspectos: protocolos diferentes, tamanhos limites para os pacotes, tipo de serviços orientados ou não à conexão, qualidade de serviço, entre outras.

As conversões necessárias podem ser implementadas em várias camadas. Fisicamente as redes podem se conectar por switches e HUBS. Na camada de enlace, podem ser feitas com pontes e switches analisando endereços MAC e fazendo a conversão dos quadros entre, por exemplo, Ethernet e 802.11. Na camada de transporte gateways, é possível fazer a conversão mantendo uma conexão confiável TCP por meio de uma rede TCP/IP e de uma SNA, por exemplo. As conversões podem ser feitas ainda na camada onde os gateways de aplicação convertem e-mails da internet para e-mails de redes proprietárias como o x.400 utilizado pelo antigo cliente de e-mail Microsoft Exchange.

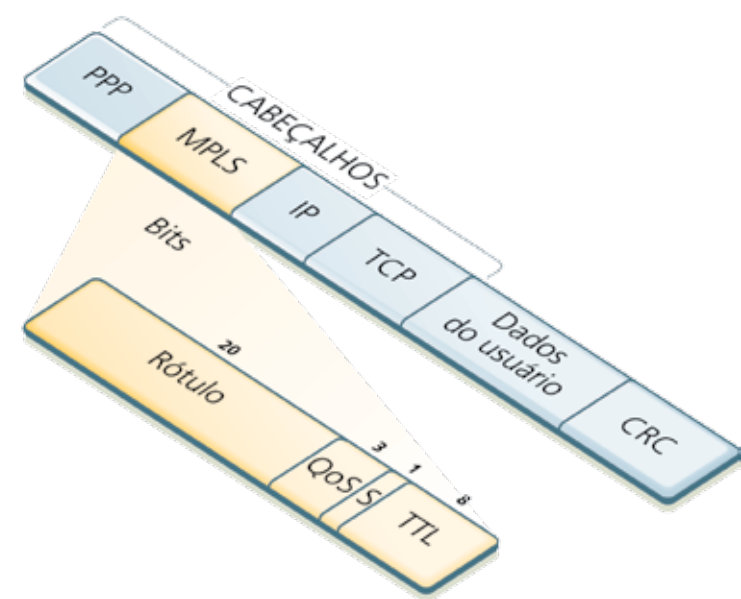
Na camada de rede, a função de interconexão também é papel de roteadores e roteadores multiprotocolo capazes de fazer roteamento entre redes de tecnologias distintas. A técnica mais utilizada é a do protocolo MPLS (MultiProtocol Label Switching ou Comutação de Rótulos Multiprotocolo) padronizada pela **Internet Engineering Task Force** (IETF) na **RFC 3031**. Essa técnica é muito parecida com a comutação em redes de circuitos virtuais, que utiliza um rótulo. Trata-se de um identificador utilizado para consultar uma tabela de repasse no

O BGP tem três funções básicas: identificar as ASs vizinhas; repassar essas informações aos outros roteadores internos da AS e definir as melhores rotas para chegar até as sub-redes da AS.

Internet Engineering Task Force (IETF) pode ser traduzida como espécie de força-tarefa criada para que a internet funcione melhor, com alta qualidade, principalmente no que diz respeito a documentos técnicos. O IETF é uma atividade desenvolvida pela Internet Society ou Associação Internet (ISOC), organização sem fins lucrativos fundada em 1992 (fonte [www.ietf.org](http://www.ietf.org)).

RFC (Request for Comments ou Requerimento para Comentários) é um conjunto de documentos que define padrões de tecnologias e protocolos para internet e redes (fonte [www.ietf.org](http://www.ietf.org)).

**Figura 152**  
Mensagem TCP sendo  
endereçada através  
de IP, MPLS e PPP.



roteador e encontrar a interface com a qual deve se conectar. A consulta é feita por meio do número IP do destino. Não existe no corpo do endereço qualquer espaço reservado para o armazenamento de um rótulo. Para rotear pacotes IP entre redes heterogêneas, normalmente adiciona-se à mensagem IP mais um cabeçalho MPLS. E para empacotar essa combinação, é necessário usar o protocolo PPP (Point-to-Point Protocol ou Protocolo Ponto a Ponto), que irá juntar os cabeçalhos do protocolo TCP, IP, MPLS e o do próprio PPP em um único quadro.

O cabeçalho MPLS é composto por: 20 bits para o Label, que é o campo principal, e 3 bits para QoS. Ele traz a taxa de qualidade da transmissão, um campo de Pilha (na figura como S), que possibilita a junção de vários rótulos. Por fim, traz o campo TTL, que serve para armazenar o tempo de vida do pacote.

Na figura 152, um pacote é enviado a partir da máquina “O” dentro de uma LAN Ethernet por meio de um roteador que identifica a rota conforme o endereço IP de destino. A mensagem é empacotada em um quadro PPP e enviada por meio de uma comunicação ponto a ponto que, por meio de uma ATM, percorre milhares de quilômetros até ser repassada para a estação “D” da LAN 2. Aí, o roteador que desempacota o PPP lê o cabeçalho IP, analisa o endereço IP de destino e transmite a mensagem para a interface que a levará até o host de destino.

20.3.3.8 Camada de rede na internet

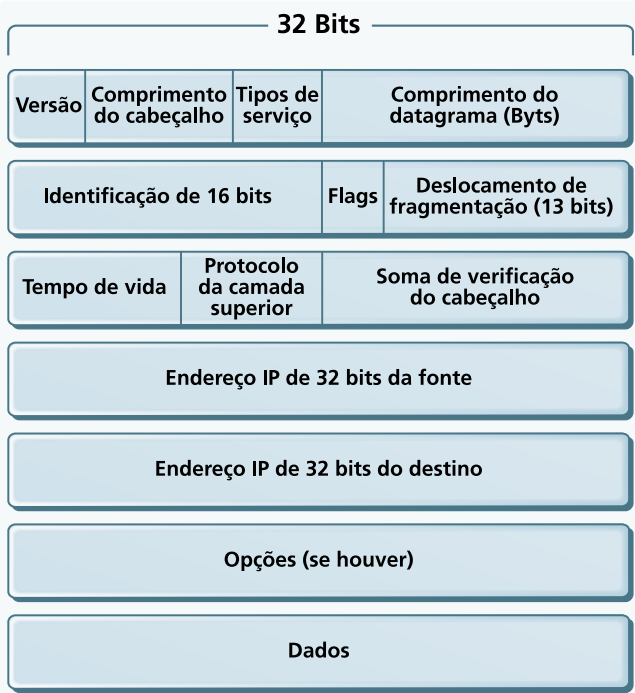
A internet é uma rede de datagramas e o centro de sua arquitetura se enquadra na camada de rede do modelo OSI (Open System Interconnection ou Sistema Aberto de Interconexão). Essa implementação utiliza o protocolo IP como forma de identificar um host e também a origem e o destino dos pacotes. Para controlar o escoamento dos dados pelos nós da rede são utilizados protocolos de roteamento, já estudados anteriormente: RIP, OSPF e BGP. Para manter a confiabilidade na entrega das mensagens por meio de uma rede é utilizado também o protocolo ICMP (Internet Control Message Protocol, Protocolo de Controle de Mensagens na Internet).

20.3.3.9. Protocolo IP

Atualmente, utilizamos a versão 4 do IP, também conhecido por IPv4, definida pela especificação RFC 791. Essa versão utiliza 32 bits para endereçar até 4.294.967.296 hosts. Por conta dessa limitação, o IP tem sofrido críticas, pois muitos acreditam que em algum momento poderemos não ter endereços suficientes. Essa preocupação tem fundamento: há muito mais dispositivos no mundo conectados à internet do que o número de endereços possíveis. Existem desde computadores pessoais de empresas, faculdades, escolas até aparelhos de celulares, PDAs, smartphones (celulares que também funcionam como computadores pessoais), entre outros. Porém, até hoje esse limite não foi alcançado. Isso porque nem todas as máquinas utilizam IP da internet, e sim IP da sua rede interna e compartilham o número IP do servidor ou do roteador. Isso é possível graças a uma técnica chamada de NAT (Natural Address Translation ou Tradução Natural de Endereços). Dessa forma, ocorrem outros problemas relacionados ao roteamento, complicando os algoritmos e provocando atraso no repasse. Além de todos esses problemas, uma máquina configurada na rede interna, como um notebook, por exemplo, ao se deslocar para fora da rede, não conseguirá acessar a internet. Portanto, deverá ser reconfigurada com os endereços da rede atual onde o equipamento está conectado. A versão 6 do IP, ou IPv6, definido na especificação RFC2373 e RFC2460 – já em produção, mas ainda pouco utilizada –, traz solução para esse tipo de problema. Essa nova geração do IP suporta cerca de 4 bilhões de endereços IP. Pela figura 158 é possível entender melhor como funciona um datagrama IP.

Cada linha da tabela da figura 153 representa 32 bits de informação. Os campos contêm informação necessária para o encaminhamento e o roteamento dos datagramas pela rede (veja quadro *Conheça as funções dos campos*).

**Figura 153**  
Formato de um  
datagrama IP.





20.3.3.10. Endereços IP

Vamos primeiro estudar endereços IPv4, por serem os mais utilizados. Essa versão é formada por quatro números de 8 bits, somando 32 bits. E o maior número que se pode escrever com 8 bits é 255 (11111111, em binário).

O endereço IP traz duas informações para o roteador: qual é a rede e qual é o hospedeiro. Na estratégia utilizada atualmente, esse número tem prefixo e sufixo flutuantes. Isso significa que a posição do bit que inicia a identificação do hospedeiro pode mudar em função da máscara de sub-redes, assunto que veremos mais adiante. O prefixo identifica a rede e o sufixo, o hospedeiro (host).

Conheça as funções dos campos

- **Versão:** utiliza 4 bits e indica ao roteador qual é o formato do cabeçalho que difere a cada versão do protocolo.
- **Comprimento do cabeçalho:** define que, por padrão, são 20 bytes. Mas é possível que haja outras opções e o tamanho pode ser maior. Isso só acontece na versão 4 do IP.
- **Tipo de Serviço ou TOS (type of service):** é utilizado por alguns fabricantes de roteadores para definir prioridades no pacote. É como se um datagrama com alta prioridade pudesse furar a fila na passagem do roteador e passar na frente dos outros que têm menos prioridade.
- **Tamanho do datagrama:** é o tamanho total da mensagem, incluindo o cabeçalho e os dados que ele carrega: não pode ser maior que 65.535 bytes.
- **Identificador, Flags e Deslocamento de fragmentação:** fornecem informações sobre a fragmentação do pacote entre roteadores. Para serem transmitidos, os datagramas IP devem caber em quadros da camada de enlace. Caso não caibam em um único quadro, é preciso repartir o quadro. Quando isso acontece, esses campos indicam em qual datagrama foi armazenado um número identificador. O campo flag informa se é o ultimo fragmento ou se existem mais. E o deslocamento informa a partir de qual byte do datagrama esse quadro carrega. No IPv6, não é permitido fragmentar.
- **Tempo de vida (TTL ou Time-to-Live):** utilizado para evitar que o pacote seja roteado infinitamente, esse dado é reduzido sempre que passa por um roteador. Ele é descartado quando seu valor chega a 0.
- **Endereços IP (fonte e destino):** incluídos na criação do pacote pelo emissor, indicam o endereço do host de origem e de destino.
- **Opções:** campo opcional, utilizado para conter informações específicas sobre a estratégia de alguma rede.
- **Dados:** trata-se da informação que está sendo transmitida. Geralmente é um segmento da camada superior (TCP ou UDP), mas pode ser também da camada de rede, um ICMP.

É importante salientar que o endereço de IP é atribuído à interface de enlace do host e não diretamente ao host. Uma máquina que se conectar a um cabo de rede ethernet e também a uma conexão de rede sem fio necessitará de um endereço de IP para cada uma das interfaces. Então, serão dois endereços de IP. A internet é uma única rede e cada interface que se conecta a ela deve possuir um único número dentro de outras redes como LANs, WANs etc. Os endereços podem ser atribuídos conforme uma faixa de endereços qualquer. Porém, essa faixa deve ser única também para cada interface. Ou seja, não é possível conectar duas interfaces com os mesmos endereços de IP dentro de uma mesma rede, pois isso geraria conflito.

Exemplo de um endereço IP:

Notação Decimal	192.168.0.1
Notação Binária	11000000. 10101000.00000000.00000001

Os endereços que começam por 192, 10, 172.16 até 172.32 são reservados somente para redes locais (LANs) e não são utilizados na internet. Os roteadores da internet são geralmente configurados para ignorar pacotes com esses endereços.

Na internet, quem controla a distribuição mundial de endereços é a Internet Assigned Numbers Authority ou Autoridade Atribuidora de Números para Internet (**IANA** – <http://www.iana.org>), que atribui e repassa o controle regional a entidades chamadas RIRs (Regional Internet Registers ou Registros Regionais de Internet). As RIRs também recebem da IANA uma faixa definida de IPs para distribuir.

Na América Latina e Caribe, quem controla a distribuição de IPs é a Latin American and Caribbean Internet Adresses Registry ou Registro de Endereços de Internet para América Latina e Caribe (LACNIC – <http://www.lacnic.net/pt/>). No Brasil as solicitações devem ser feitas diretamente ao NIC.BR, que é o registro Nacional Internet para o Brasil. As RIRs vendem faixas de IPs para as provedoras de acesso à internet, que, por sua vez, redistribuem, administram e repassam os custos aos seus clientes.

20.3.3.11. Sub-redes

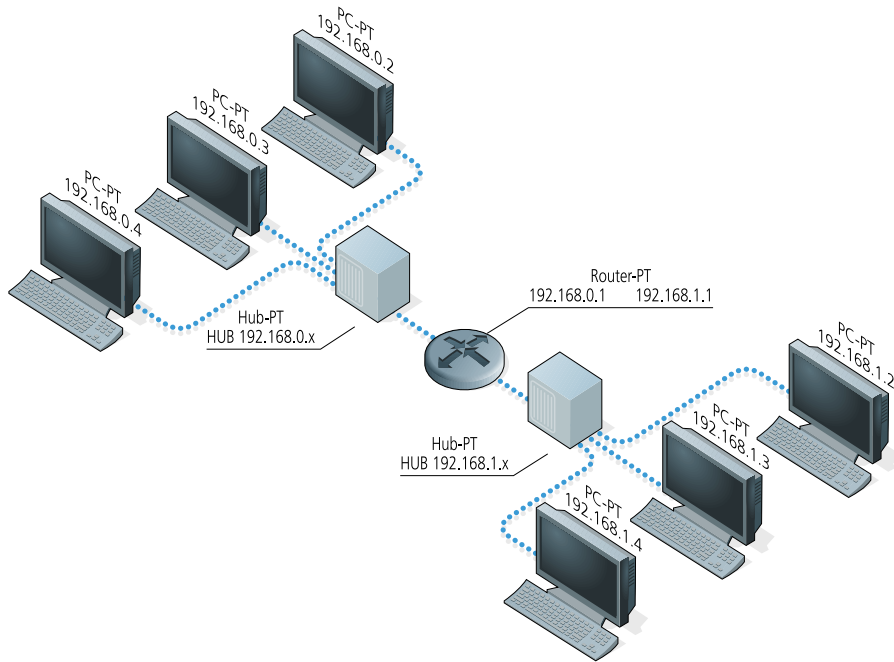
As sub-redes são grupos de hosts que têm o mesmo prefixo IP. Computadores conectados entre si dentro de uma mesma infraestrutura, ligados a hubs ethernet ou a um mesmo roteador sem fio formam uma sub-rede.

Na figura 154, vemos o exemplo de duas sub-redes. Os computadores estão ligados por um barramento ethernet, compartilhado por meio de hub. Vamos imaginar os departamentos de uma empresa, localizados em andares diferentes de um mesmo prédio. Veja que o hub não tem interface e, portanto, não tem IP. É somente um modo de ligar as interfaces da sub-rede. As máquinas dessas sub-redes têm IP no formato 192.168.0.x, ou seja, os primeiros 24 bits do número identificam a sub-rede. Portanto, temos duas sub-redes: a 192.168.0.0/24 e a 192.168.1.0/24.O roteador tem uma interface ligada a cada rede e possui endereços que participam das sub-redes em que estão conectadas.

O roteador manterá os pacotes entregues dentro de uma sub-rede e não os repassará à outra interface. Isso minimizará a sobrecarga de dados do canal de comunica-

A IANA é a entidade internacional responsável pela coordenação global dos sistemas de endereçamento de protocolo da internet e dos números do sistema autônomo utilizado para o encaminhamento de tráfego internet.

**Figura 154**  
Exemplo de duas sub-redes.



ção entre uma sala de departamento e outra, além de aumentar o desempenho da rede. Por exemplo, imagine que numa dessas salas existe apenas um computador com impressora, a qual recebe trabalhos de outras estações. Os pacotes de dados que irão para o host da impressora não tráfegarão por toda a rede da empresa. Serão analisados apenas pelos hospedeiros que estão dentro da mesma sub-rede.

## Fique atento

Regras a serem observadas ao se atribuir um endereço de IP:

- Número de IP não pode começar com zero.
- Nenhuma interface pode receber o endereço 127.XXX.XXX.XXX, reservado para a interface de loopback (canal de comunicação que tem apenas um ponto como destino), que gera uma interface para serviços a serem conectados dentro da mesma máquina.
- Nenhum endereço pode ter como hospedeiro o endereço 0: Ex: 192.168.1.0, com máscara 255.255.255.0. Ou 172.16.0.0 com máscara de sub-rede 255.255.0.0. Esses endereços são reservados para a identificação de rede.
- A parte do endereço que representa a rede não pode ser 255. Ex: 255.xxx.xxx.xxx com mascara de sub-rede 255.0.0.0. Também não pode haver endereço de hospedeiro com todos os octetos 255. Ex: xxx.255.255.255. Esses números são reservados para broadcast.

Sempre que configuramos um endereço de IP em um computador, não informamos apenas o número IP. Devemos informar também qual a máscara de sub-rede. Esse número é utilizado para definir quais bits do endereço representam a sub-rede. Quando for necessário descobrir a qual sub-rede pertence determinado IP, o protocolo de rede fará a multiplicação binária do endereço IP pela máscara de sub-rede. Exemplos:

IP: 192.168.1.25	11000000.10101000.00000001.00011001
Máscara sub-rede: 255.255.255.0	11111111.11111111.11111111.00000000
X	
=	
Sub-rede: 192.168.1.0	11000000.10101000.00000000.00000000

IP: 172.16.9.43	10101100.00010000.00001001.00101011
Máscara sub-rede: 255.255.0.0	11111111.11111111.00000000.00000000
X	
=	
Sub-rede: 172.16.0.0	10101100.00010000.00000000.00000000

**Figura 155**  
Para multiplicar em binário, fazemos operação bit a bit. 1 x 0 = 0 e 1 x 1 = 1.

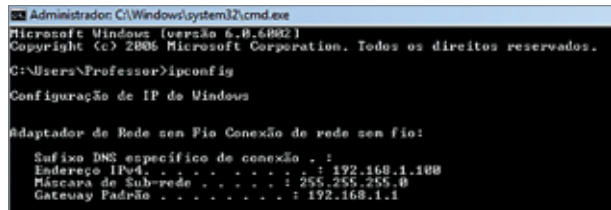
Para configurar uma estação de rede que se conecta a outras redes, como a internet, é preciso informar o endereço do gateway da rede. Na nossa imagem (figura 155), representada pelo roteador e aplicada a ambientes mais comuns, o gateway pode ser o modem de internet, o servidor proxy, o roteador sem-fio etc. Por padrão, são usados para endereçar os gateways o menor número possível dentro de uma sub-rede, geralmente o numero de host 1, ou o número máximo: 254. Isso numa rede com máscara 255.255.255.0.

Para ver a configuração das interfaces de uma estação com Windows, podemos também utilizar o comando “ipconfig” no prompt de comando (figuras 156 e 157).



**Figura 156**  
Configuração do protocolo IPv4 no Windows Vista.

**Figura 157**  
No Linux, o comando equivalente é ifconfig.

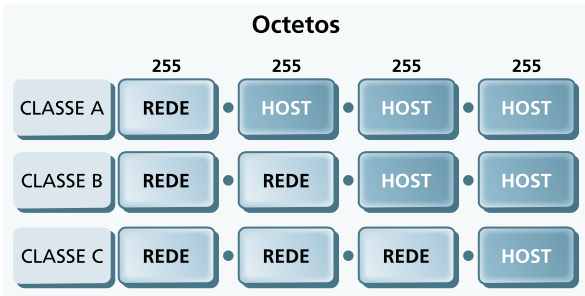


20.3.3.12. CIDR

No início da internet, os IPs eram subdivididos em classes A,B,C, D e E. Na prática, eram utilizadas apenas as faixas A, B e C. As classes D e E ficavam reservadas para experimentos e para uma possível expansão dos números, que acabou não ocorrendo e talvez nunca ocorra. Essa classificação era uma forma de determinar quantos bits eram utilizados para identificar a rede e o que ficava disponível para o host (hospedeiro). Os endereços da classe A utilizam o primeiro octeto para determinar a rede, e os outros três para determinar os hosts. Os endereços da classe B utilizam o primeiro e o segundo octetos; e o da classe C, os três primeiros octetos (figura 158).

Os endereços da classe C são utilizados para redes pequenas de até 254 máquinas, pois somente o último octeto representa os hospedeiros. A máscara de sub-rede de um endereço classe C é 255.255.255.0. Caso o conjunto de máquinas seja maior que 254, a solução seria utilizar endereços da classe B com máscara 255.255.0.0. Os dois últimos octetos seriam utilizados para representar os hosts.

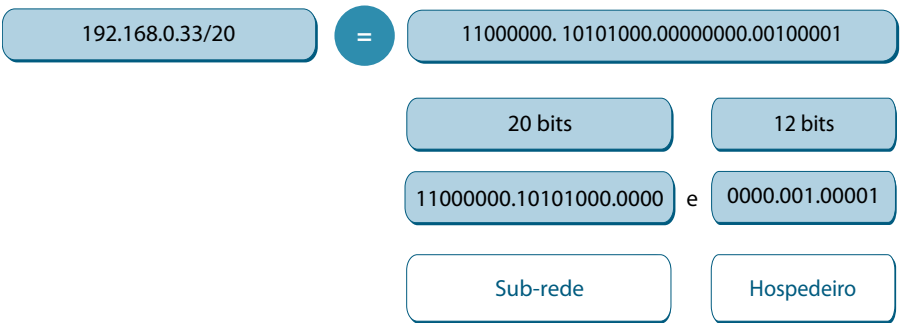
**Figura 158**  
Faixa de IPs.



Em um número IP visto da forma decimal, podemos identificar sua classe a partir do número da primeira posição.

DISTRIBUIÇÃO DE NÚMEROS IP POR CLASSES				
Classe	Máscara de sub-rede	Faixa de IPs	Quantidade de redes possíveis	Quantidade de hospedeiros possíveis
A	255.0.0.0	1.xxx.xxx.xxx a 126.xxx.xxx.xxx	254	16.777.214
B	255.255.0.0	128.xxx.xxx.xxx a 191.xxx.xxx.xxx	65.534	65.534
C	255.255.255.0	192.xxx.xxx.xxx a 223.xxx.xxx.xxx	16.777.214	254

**Figura 159**  
Subredes por CIDR.



Esse modelo não é mais utilizado por desperdiçar números de IP, que estão presentes a se esgotar. Acredita-se que isso deva acontecer entre 2012 e 2014.

Proposta na RFC 1519, a CIDR (Classless Inter Domain Routing ou Roteamento Interdomínio sem Classes) é uma estratégia usada para distribuir melhor os endereços IP e prover um mecanismo de agrupamento de informações de roteamento. Isso cria uma forma hierárquica de organizar os computadores das redes em sub-redes e super-redes. A estratégia consiste em substituir a máscara de sub-redes por um número único que indica a quantidade de bits a ser utilizada pelo roteador para identificar a rede. A diferença é que com uma máscara temos somente quatro opções 255.0.0.0, que seria compatível com o /8, 255.255.0.0; com o /16, 255.255.255.0; com o /24, 255.255.255.255 e com /32. Com a utilização do CIDR, é possível encontrar endereços com /20. Os roteadores de borda podem gerenciar melhor suas tabelas de repasse, pois utilizam somente o número da rede para identificar a rota. E com bits escolhidos de 1 em 1, e não de 8 em 8, pode-se balancear melhor o desempenho de roteadores e a quantidade de IPs disponíveis dentro da faixa de números de host. Esses números, por sua vez, podem ser mapeados a partir da quantidade de bits restantes. Observe a figura 159.

Nas configurações de rede de estações desktop, geralmente não é necessário configurar o endereço IP com CIDR, somente com máscara de sub-rede. Já nas configurações de servidores Windows, Linux e em roteadores é mais comum encontrar a definição da rede do endereço por CIDR. Essa técnica é utilizada também no IPv6.

20.3.3.13. DHCP

Uma vez definida qual faixa de IP será utilizada pela rede, os endereços nas estações e nos roteadores precisam ser configurados. É possível fazer isso manualmente, informando na conexão de rede de cada uma das máquinas o endereço de IP, a máscara de sub-rede e o gateway padrão. Ou, então, pode-se utilizar o DHCP para obter automaticamente essa configuração fornecida pelo roteador ou por um servidor.

O DHCP (Dynamic Host Configuration Protocol ou Protocolo de Configuração Dinâmica de Hospedeiros), definido na RFC 2131, possui uma das técnicas mais usadas para facilitar a configuração de hospedeiros que estão



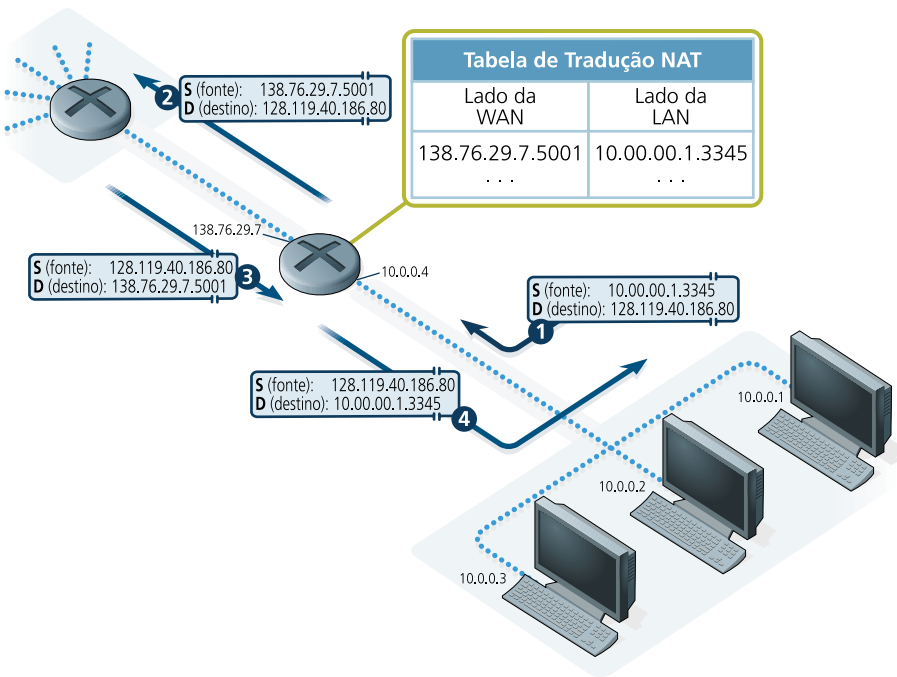
sempre mudando de redes, como notebooks e PDAs em redes sem fio. É um mecanismo adotado também em Internet Service Provider ou Provedores de Serviços de Internet (ISP), que têm uma faixa de IP para distribuir a seus clientes e precisam redistribuir endereços constantemente, já que os clientes se conectam e desconectam a todo instante, liberando um IP ou necessitando de um novo.

20.3.3.14. NAT

Como vimos, redes internas, intranets de empresas, escolas, residências, LANs e até WANs inteiras podem ter faixas de endereços próprios, formando sistemas autônomos, separados da internet. Quando uma dessas redes precisa se conectar à rede mundial de computadores ou a outra rede, são utilizados roteadores de borda ou roteadores gateway. Geralmente, roteadores têm duas interfaces ou mais, mas pelo menos uma se liga com a rede interna, e outra(s) se conecta(m) com a internet. Dessa maneira, a única máquina que se encontra na internet é o gateway e só ela é alcançável na rede mundial de computadores. As máquinas por trás dele não.

As máquinas da rede interna conseguem enviar pacotes para a internet, mas não recebem resposta. Para compartilhar a conexão, utiliza-se o Network Address Translation ou NAT definido na RFC 1631 e RFC 3022 (figura 160). O NAT é uma técnica de compartilhamento de um único endereço IP da internet com várias máquinas, que soluciona o problema da resposta das mensagens. É implementado em dispositivos como roteadores ou computadores com duas placas de rede que fazem ligação entre redes internas e a internet.

**Figura 160**  
Troca de informação  
do cabeçalho e  
tabela de tradução.



Quando o protocolo IP da interface de origem verifica que o endereço de rede da mensagem tem um destino diferente de sua própria rede, o pacote é enviado ao seu gateway, que, por sua vez, substitui o número do endereço de origem pelo seu próprio endereço de interface ligado na internet. Ou seja, para a internet, quem enviou o pacote foi o gateway e não a máquina interna que está por trás do gateway. Além disso, na camada de transporte do roteador gateway é aberta uma nova porta de saída.

Antes de repassar o pacote adiante, no entanto, o NAT registra em uma tabela de tradução o endereço e a porta de origem do pacote, além do número da porta aberta para receber a resposta. Assim, quando uma mensagem de resposta chegar ao roteador, ele irá analisar o cabeçalho do protocolo de transporte, identificar a porta de destino e cruzar as informações com sua tabela de tradução. Depois, fará o trabalho inverso em relação ao envio para a internet. O endereço de destino será obtido a partir do registro da tabela de tradução relacionado com a porta de saída do roteador. E o endereço e a porta de destino do cabeçalho do pacote serão substituídos.

É possível também configurar rotas pré-definidas para que sejam criados, dentro da rede interna, servidores que atenderão clientes na internet. Em alguns roteadores, essa função é chamada de Virtual Server (Servidores Virtuais).

20.3.3.15. ICMP

Para manter a confiabilidade da rede e fazer com que pareça que está tudo bem sempre – e que problemas não ocorrem (pois problema é o que mais acontece) –, é utilizado o protocolo **ICMP** (Internet Control Message Protocol ou Protocolo de Controle de Mensagem na Internet). Esse protocolo permite a comunicação de controle entre dispositivos da rede. Assim, os componentes da rede podem procurar soluções de problemas, que serão resolvidos pela camada sem que sejam reportados às camadas superiores.

As mensagens ICMP são as seguintes:

MENSAGEM DE DESTINO INALCANÇÁVEL, TIPO 3	
Código	Descrição
0	Rede inalcançável
1	Hospedeiro inalcançável
2	Protocolo inalcançável
3	Porta inalcançável
4	Necessidade de fragmentação.
5	Falha na rota de origem

MENSAGEM DE TEMPO PERDIDO, TIPO 11	
Código	Descrição
0	Tempo de vida excedido (TTL)
1	Tempo para remontagem do fragmento excedido

O ICMP foi especificado na RFC 792 e é utilizado por roteadores nas seguintes situações:

- quando um datagrama não pode ser entregue no destino;
- quando um gateway não tem capacidade de repassar um datagrama;
- quando um gateway identifica congestionamento e necessita utilizar outras rotas;
- quando o gateway identifica uma rota mais curta para enviar o datagrama.

MENSAGEM DE PROBLEMA COM PARÂMETROS, TIPO 12\*

Código	Descrição
0..3	Endereço IP incorreto. O código representa o octeto inválido

\*Relativa a erros com o endereço de destino.

MENSAGEM DE REDUÇÃO DA FONTE, TIPO 4

É utilizada normalmente para controlar congestionamento. Possibilita que um roteador sobrecarregado avise os hospedeiros que estão enviando datagramas a sua situação. Esses, por sua vez, podem responder com uma diminuição de velocidade de transmissão ou utilizar outra rota.

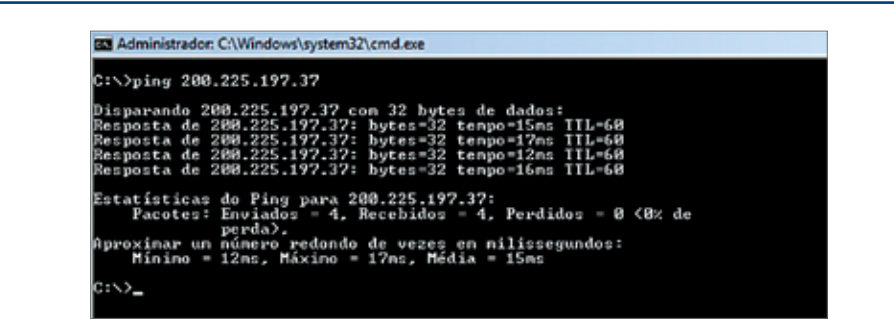
MENSAGENS DE REDIRECIONAMENTO, TIPO 5\*

Código	Descrição
0	Redirecionar os pacotes para determinada rede
1	Redirecionar os pacotes para determinado hospedeiro
2	Redirecionar os pacotes para determinado tipo de serviço e rede
3	Redirecionar os pacotes para determinado tipo de serviço e hospedeiro

\*Um roteador informa à origem que os pacotes devem ser encaminhados por outra rota.

MENSAGEM DE ECO, TIPO 8, E RESPOSTA DE ECO, TIPO 0

Utilizado pelo comando “ping” para descobrir a existência de um hospedeiro na rede e qual é o seu tempo de resposta.



MENSAGENS DE SOLICITAÇÃO DE HORÁRIO, TIPO 13, E MENSAGENS DE RESPOSTA DE HORÁRIO, TIPO 14

Pede e responde informação sobre o horário do relógio da máquina.

PEDIDO E RESPOSTA DE INFORMAÇÃO, TIPOS 15 E 16\*

Esse comando serve para descobrir a rede em que a interface está conectada. A resposta da mensagem traz o endereço terminado em zero, que representa a rede. Exemplo: 192.168.0.0, 172.16.0.0.

\*Respectivamente

20.3.3.16. Multidifusão na internet

O Internet Group Management Protocol ou Protocolo de Gerenciamento de Grupos da Internet (IGMP) foi desenvolvido para identificar os clientes de um determinado serviços multicast formando um grupo. Em vez de enviar os datagramas a todos os computadores da rede, O IGMP faz com que a transmissão chegue apenas aos hospedeiros que estiverem no grupo de clientes. Tem a vantagem de utilizar melhor os recursos da rede.

20.3.3.17. IPv6

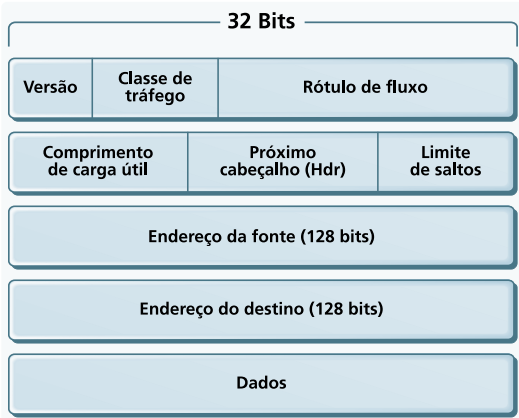
Durante muito tempo, o IPv4 mostrou-se competente na função de endereçar as redes de datagramas, sem a necessidade de uma forma mais simples de configurar o endereçamento para aparelhos móveis que estão dentro de uma rede apenas por pouco tempo. Porém, o aumento da demanda por endereços IP fez com que a Internet Engineering Task Force (IETF) desenvolvesse uma nova versão desse protocolo, a versão 6 (veja quadro *Mudanças importantes* e figura 162).

Mudanças importantes

Principais características da evolução do IPv4 para o IPv6:

- **Aumento na oferta de endereços:** o endereço IPv6 possui um protocolo de 128 bits, contra os 32 do IPv4, o que permite uma quantidade gigantesca de oferta de endereços. A ordem de grandeza é de 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços possíveis.
- **Configuração de endereços automáticos:** não é necessária nenhuma configuração manual. Se houver um servidor DHCP na rede, o IPv6 atribuirá os IPs, seguindo a regra estabelecida. Caso não exista, o hospedeiro sozinho será capaz de se autoendereçar com base nas informações obtidas por meio de mensagens IGMP.
- **Endereçamento e roteamento eficiente:** facilita o trabalho de roteamento. A hierarquia da infraestrutura de endereços públicos da internet possibilita ao roteador criar listas de repasse mais simples, como no caso de um cabeçalho de tamanho fixo de 40 bits.
- **Melhor controle de qualidade:** unifica a forma de controlar a qualidade do serviço e o faz de forma mais leve que nas soluções de QoS (quality of services ou qualidade de serviços) implementadas no IPv4.
- **Segurança:** inclui o protocolo IPSec (Segurança IP), que implementará uma criptografia nativa, sem a necessidade de configuração ou de instalação de protocolos adicionais em outras camadas.

Figura 162  
Datagrama IPv6.



20.3.3.17.1 Datagrama IPv6

Funções do protocolo V6

**Versão** – Identifica um datagrama na versão 6.

**Classe de tráfego** – Similar ao campo TOS (Type of Service ou Tipo de Serviço) do IPv4, que é tilizado por alguns fabricantes de roteadores para definir prioridades no pacote. Um datagrama com alta prioridade pode furar a fila no roteador e passar na frente dos outros com menos prioridade.

**Rótulo de fluxo** – Identifica um fluxo de datagramas.

**Comprimento da carga útil** – É o tamanho do segmento de dados fora o cabeçalho do datagrama.

**Próximo cabeçalho** – Identifica o protocolo da próxima camada que está sendo transportado pelo datagrama. Um UDP (User Datagram Protocol ou Protocolo de Datagrama de Usuário), TCP (Transmission Control Protocol ou Protocolo de Controle de Transmissão) ou um ICMP (Internet Control Message Protocol ou Protocolo de Controle de Mensagem na Internet), por exemplo.

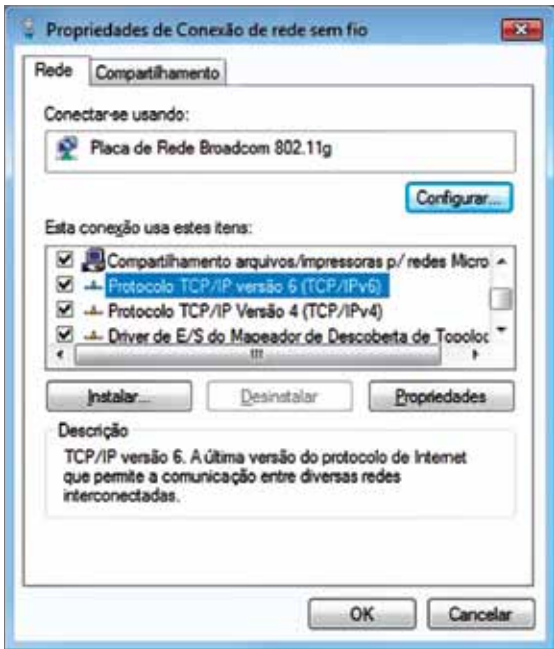
**Limite de saltos** – Tem a mesma função do TTL (Time to Life ou Tempo de Vida). Possui um contador que decrementa a cada roteador que passa.

**Dados** – É o conteúdo que está sendo transportado pelo datagrama.

20.3.3.17.2. Implantação IPv6

As técnicas como NAT e DHCP vão permitir que o IPv4 se perpetue em redes de pequeno porte por muito tempo. Mesmo a internet deve passar por um período de transição, utilizando durante um bom tempo o protocolo IPv4 junto com o IPv6. Os principais sistemas operacionais do mercado já trazem, ativadas, as duas versões do protocolo. Na figura 163 vemos as duas versões do protocolo IP ativado em uma interface com o sistema operacional Windows Vista. Espera-se que, na medida em que os equipamentos mais antigos sejam substituídos, a internet se torne puramente IPv6.

Figura 163  
Tela de configuração de Redes do Windows Vista.



20.3.3.18. Camada de enlace

A camada de enlace encontra-se entre cinco outras camadas: lógica, rede, transporte, aplicação e física, onde ficam os equipamentos da rede. Ela tem a função de transportar os pacotes da camada de rede, quebrando as mensagens em quadros lógicos compatíveis com o tipo de ligação física da rede. Além disso, essa camada é responsável pela transmissão entre as interfaces de dois ou mais dispositivos de rede, de modo a sincronizar a velocidade entre esses dispositivos, e pode tratar os erros causados por interferências inerentes ao meio físico. Em suma, a camada de enlace cria uma conexão lógica capaz de fazer a comunicação entre dispositivos que se ligam por um meio físico de transmissão. O software dessa camada geralmente fica em um chip da placa de rede.

20.3.3.18.1. Serviços oferecidos pela camada de enlace

A camada de enlace fornece três serviços básicos: faz o enquadramento dos dados, disponibiliza um canal de comunicação confiável e controla o fluxo de dados em meios compartilhados e com tratamento de erros.

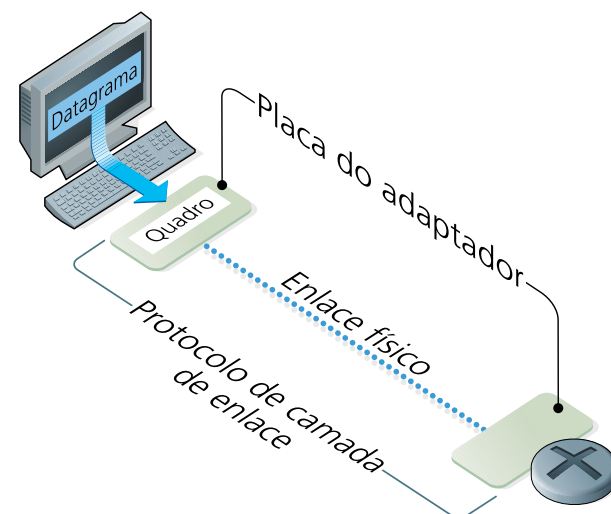
Enquadramento

Quando o software da camada de enlace recebe o datagrama da camada de rede, ele prepara um quadro, expressão usada para definir um conjunto de dados a serem transmitidos pela camada de enlace. Esse quadro contém um cabeçalho (header) e um trailer (campo no final do quadro), com informações que aparecem no fim da transmissão. Entre o cabeçalho e o trailer é embutido o datagrama recebido da camada de rede, intacto. A figura 164 representa um datagrama de rede sendo enviado entre duas placas de rede (interfaces de enlace), através de um quadro de dados da camada de enlace.



**Figura 164**

Enlace entre duas interfaces.



### Comunicação confiável

Dizer que uma camada é confiável significa afirmar que as transmissões não têm erro. É o caso da camada de enlace, que tem capacidade para assegurar a entrega dos quadros. Quando uma interface de enlace envia os quadros, a camada aguarda que o enlace de destino confirme a chegada da mensagem dentro de determinado tempo (timeout). Caso não receba a informação, o quadro é reenviado. Isso quer dizer que, além de estabelecer a conexão entre os enlaces, o protocolo da camada de enlace garante que todos os quadros do pacote sejam entregues.

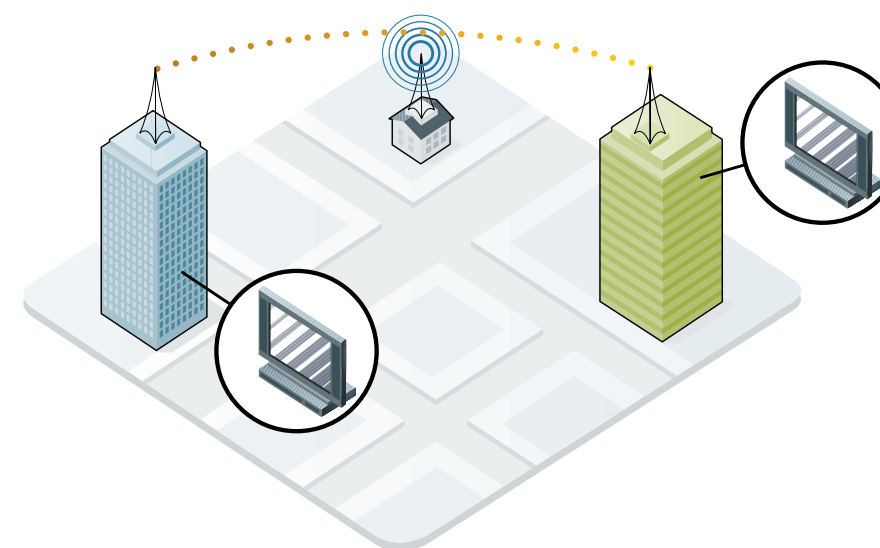
Deve-se levar em consideração, no entanto, que o controle de erros consome mais recursos e deixa a rede mais lenta. Redes mais propícias a falhas, como as sem fio, são mais sensíveis a interferências e por isso o controle de conexão e de resposta é ainda mais importante. Já as redes com fibra óptica não requerem tanto controle – o que pode ser feito em qualquer uma das camadas superiores.

### Controle de erros

Além da eventualidade de perder um quadro durante a transmissão, é possível que ocorra outro problema: a modificação do dado (figura 165) por conta de alguma interferência de ondas vindas do ambiente, por exemplo. Assim, um bit que estava em um quadro pode se tornar zero. Para contornar esse problema, vários algoritmos da camada de enlace incluem no final do quadro uma somatória de todos os bits das mensagens. Quando o enlace de destino recebe o quadro e faz o cálculo, o resultado tem de bater com o da somatória (checksum ou checagem da soma). Se o valor for diferente, pode ser solicitado o reenvio da mensagem.

### Fluxo

Em uma rede podem ser utilizados equipamentos diferentes ou com tecnologia mais antiga e de configurações distintas. Por isso, os dispositivos de enlace dispõem de protocolos capazes de enviar dados de forma que o dispositivo de destino consiga ler. São algoritmos de feedback que servem para controlar a

**Figura 165**

Interferências externas (ondas, por exemplo) podem alterar os dados.

velocidade das informações para que os adaptadores de rede mais lentos não percam dados. Sem esse dispositivo, ocorreria algo semelhante àquela situação em que, ao final de um filme, tentamos ler os créditos, mas não conseguimos fazer a leitura completa, porque o texto passa rápido demais pela tela.

Na prática, se uma rede tiver máquinas com placas ethernet de 100 Mbps e se conectar a uma máquina mais antiga, com interface de 10 Mbps, a placa de 100 Mbps terá de baixar sua velocidade de transmissão para 10 Mbps para que a comunicação seja possível.

#### 20.3.3.18.2. Subcamadas

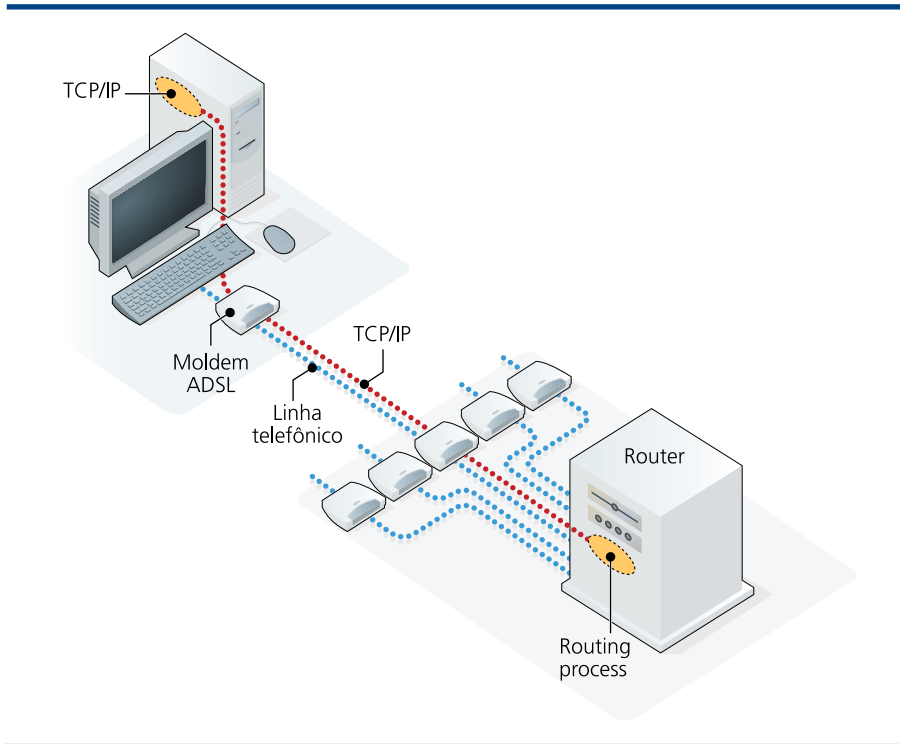
Uma das funções mais importantes da camada de enlace é fazer com que vários nós da rede sejam capazes de acessar o mesmo meio físico de transmissão, de forma compartilhada. Para fazer esse controle, a camada é dividida em dois subgrupos de protocolos ou subcamadas: o LLC (Logic Link Layer) e o MAC (Media Access Control), que conheceremos melhor adiante. A **IEEE** (Institute Electrical and Electronics Engineers) desenvolveu os padrões 802.x para definir esses protocolos e os equipamentos do meio físico.

##### 20.3.3.18.2.1. LLC

A função da subcamada LLC (Logical Link Control ou Controle do Link Lógico) é atuar em redes ponto a ponto, ou seja, naquelas em que a comunicação é feita diretamente entre duas interfaces sem compartilhamento do meio físico. Essa subcamada é capaz de garantir a entrega dos pacotes, descobrir e corrigir erros e controlar o fluxo dos quadros. Pode ainda regular a velocidade de transmissão, permitindo a entrega correta da mensagem conforme a capacidade do receptor. A LLC é definida na especificação IEEE 802.2 e é utilizada para fazer comunicação de longa distância (WAN).

O Institute Electrical and Electronics Engineers, ou Instituto de Engenharia Elétrica e Eletrônica (IEEE) é uma sociedade técnico-profissional internacional, criada em 1884 nos E.U.A. A instituição é dedicada ao avanço da teoria e prática da engenharia nas áreas de eletricidade, eletrônica e computação. Congrega mais de 312.000 associados, entre engenheiros, cientistas, pesquisadores e outros profissionais em cerca de 150 países. (<http://www.ieee.org.br>)

**Figura 166**  
Conexão ponto a ponto entre usuário doméstico e o ISP.



Os principais protocolos da LLC são o HLDC e o PPP

**HLDC (High Level Data Link Control ou Controle de Link de Dados de Alto-Nível)**

Esse protocolo é proprietário da CISCO, que é a maior e mais conceituada fabricante de equipamentos para redes. É o padrão mais antigo e é utilizado em redes de baixa e média velocidades.

**PPP (Point-to-point Protocol ou Protocolo Ponto a Ponto)**

Protocolo aberto muito utilizado na internet, principalmente para facilitar o acesso de usuários domésticos por meio de linha telefônica (discada e ADSL –Asymmetric Digital Subscriber Line ou Linha Digital Assimétrica para Assinante) com seus ISPs (Internet Service Provides ou Provedores de Serviços de Internet) (figura 166). O procolo PPP conecta roteadores por meio de canais FDDI (Fiber Distributed Data Interface – sistema de comunicação que utiliza fibra ótica), ATM (Asynchronous Transfer Modem ou Modo de Transferência Assíncrono) etc e permite fazer autenticação para estabelecer a conexão.

O PPP foi modificado para atender a duas situações: uma é quando a conexão é feita por uma ATM, chamada de PPPoA (PPP over ATM), usada para acessar a internet por meio de linha telefônica (discado ou ADSL). A outra é quando o meio utilizado é uma ethernet, que nesse caso se chama PPPoE (PPP over Ethernet).

A configuração mais comum de acesso à internet banda-larga no Brasil é feita via ADSL. Nesse caso, os enlaces costumam ocorrer entre o computador e o modem e entre o modem e a operadora de telefonia. Constatamos, então, que entre o modem e a operadora a comunicação é feita por cabo de telefone, ou

seja, sobre a ATM. Porém, entre o modem e o micro a conexão se dá por cabo de pares trançados e recebe o nome de rede ethernet. Nesse tipo de rede para acesso à internet, é permitido fazer o link PPP entre o modem e a operadora. Ou então, o que é mais comum, utilizar o modem como ponte (bridge) e ligar o computador direto ao ISP.

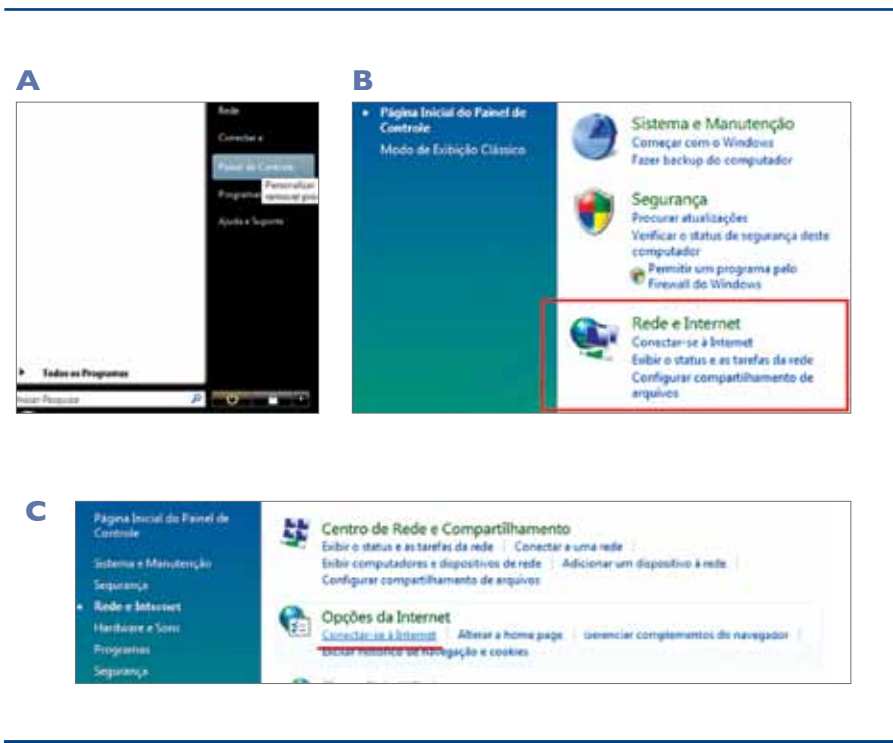
Podemos então concluir que se fizermos a configuração no computador, estaremos utilizando PPPoE. No modem, utilizaremos a PPPoA.

**Configurando a ADSL no computador (PPPoE)**

Essa configuração é simples, porém, deve levar-se em conta que quando fizer a conexão com a internet, o computador se tornará um host da internet, acessível na rede. Para um servidor, isso é o desejável. Para uma estação doméstica, significa exposição direta a ataques externos. Portanto, é preciso ter em mente que uma máquina que utiliza PPPoE deve ter segurança reforçada, com Firewall, Antivírus, Anti-Spyware sempre ativos e atualizados. Outra questão é que para compartilhar essa conexão com outras máquinas, o computador deve possuir duas placas de rede: uma para se conectar ao modem e outra para se ligar à rede e ativar o compartilhamento de “Conexão com a Internet do Windows”.

O processo de configuração é praticamente o mesmo em um computador com o Windows Vista ou Windows 7. Pode ser feito a partir da “Central de Redes e Compartilhamento”, acessada pelo “Painel de Controle” ou pelo ícone da rede na barra de tarefas do Windows. Vamos seguir a opção clássica, pelo Painel de Controle.

1. Acesse o “Painel de Controle” pelo botão “Iniciar”, depois “Redes de Internet” e, por fim, clique no link “Conectar-se à Internet”, como mostra a figura 167.



**Figura 167**  
Configurando a ADSL de forma clássica.

2. Escolha o meio de transmissão, que, no caso da conexão PPP, será a opção “Banda-Larga PPPoE”. Clique nessa opção. Aparecerá o formulário a ser preenchido com usuário e senha de acesso ao servidor de internet (ISP). Clique em “Conectar” (figura 168).

**Figura 168**  
Escolhendo o meio de transmissão.



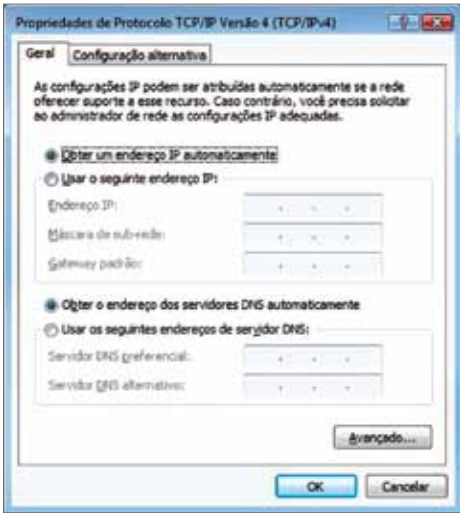
Configurando a ADSL no modem ADSL (PPPoA)

Essa configuração deve ser feita no software firmware do modem ADSL. Como cada fabricante possui o seu programa específico, a descrição se torna mais difícil. Mas, apesar de diferentes, os passos podem ser bem parecidos. Essa conexão pode ser mais segura, pois o host nesse caso é o modem ADSL e as máquinas internas não são diretamente acessíveis pelos computadores da internet. Por serem os modems ADSL também roteadores, é possível compartilhar a internet em uma LAN, fazendo a ligação física por meio da Ethernet do modem a um HUB ou a um ponto de acesso Wi-Fi (LAN sem fio).

Passos para configuração PPPoA:

1. Ligue o modem na linha telefônica e, pela interface Ethernet, conecte-se a um computador. Localize debaixo do modem uma etiqueta com o endereço IP da configuração de fábrica ou procure no manual. O IP costuma ser 10.1.1.1, ou 10.0.0.1 ou 192.168.1.1. Tente primeiro se conectar por DHCP. Se não for possível, configure a máquina conectada ao modem com um IP da mesma rede, mas com número diferente. Se for 10.0.0.1 (endereço do modem), coloque na máquina o número 10.0.0.3, por exemplo. A máscara de rede pode ser 255.255.255.0 e o gateway será o número IP do modem (figura 169).

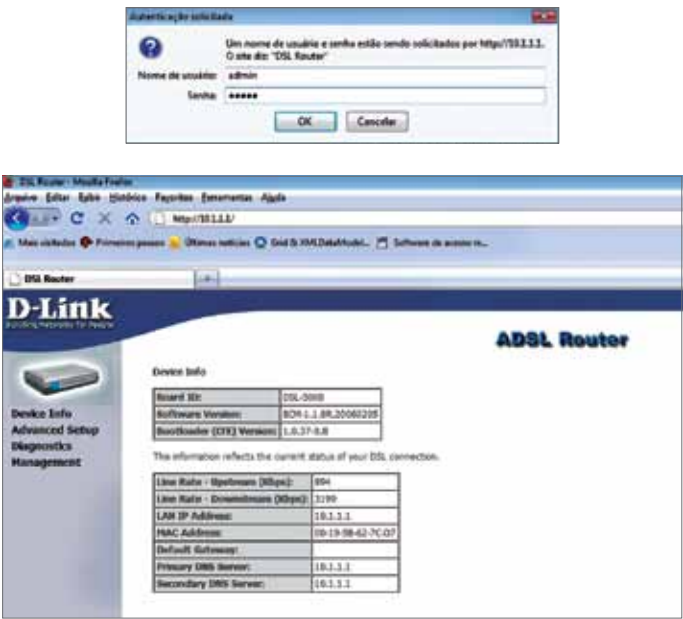
**Figura 169**  
Configuração IP para utilizar DHCP.



2. Os softwares firmware oferecem uma interface web para a configuração. Portanto, vamos abrir um navegador e acessar o **endereço do modem** por meio do serviço HTTP. Exemplo: <http://10.1.1.1>. O modem deve pedir o nome do usuário e a senha do administrador da rede. Todos os modems já vêm de fábrica com um usuário e senha, que podem ser alterados. Os mais comuns são: usuário “admin” e senha “admin”, ou usuário “root” e senha “root” (figura 170).

O endereço correto do modem pode ser encontrado na página de configuração do manual do equipamento.

**Figura 170**  
Autenticação no sistema de configuração do ADSL Router.

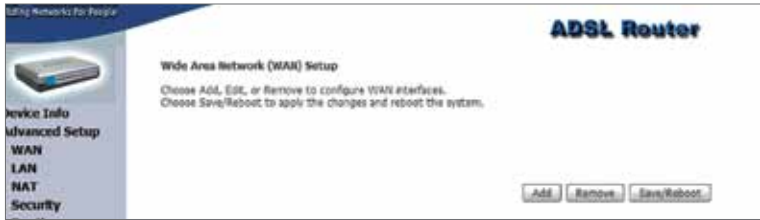


3. Nesse caso, estamos utilizando o modem ADSL Router DSL-500B da D-Link. Para acessar a configuração da conexão, devemos clicar no link “Advanced Setup” e, dentro dele, em “WAN”. Depois, no botão “Add” para adicionar uma nova conexão (figura 171).



Figura 171

Configuração da interface WAM.



4. Configure o identificador VPI e VCI da ATM de sua operadora (figura 172). Geralmente, quando esses modems são adquiridos pela própria operadora, os valores vêm preenchidos corretamente. Quando isso não acontece, é aconselhável se informar no suporte telefônico da operadora de telefonia.

Figura 172

Configuração ATM.



5. Escolha PPPoA e o tipo de encapsulamento utilizado por sua operadora de telefonia. Mas lembre-se de que vale a mesma regra em relação ao local de origem do modem. Para facilitar a instalação no local onde está o usuário, as empresas que fornecem serviço de banda-larga distribuem os modems com os padrões pré-configurados (figura 173).

Figura 173

Escolhendo o PPoA e o encapsulamento.



6. Entre com o usuário e a senha e clique em “Next”.



7. Se for compartilhar a conexão da internet com sua rede, selecione a opção NAT na tela mostrada na figura X e habilite o Firewall para dar segurança ao modem (figura 174). A partir desse ponto, a configuração deverá estar completa. Após a conclusão, salve e reinicie o modem.

20.3.3.18.2.2 MAC

Os protocolos LLC (Logical Link Control ou Controle do Link Lógico) são capazes de realizar conexões de redes ponto a ponto, sendo que o meio físico de comunicação somente transmite dados entre duas partes. Porém, em redes de difusão, nas quais o acesso é compartilhado, a camada MAC (Media Access Control – Controle de Acesso ao Meio) é que entra em ação. O ambiente, na maioria dos casos, são as LANs, já que nas WANs, por exemplo, os **backbones** da internet ou conexões ADSL fazem a comunicação ponto a ponto.

As redes de difusão são aquelas em que o canal é compartilhado por vários hospedeiros, onde um nó pode se comunicar com qualquer outro ou um com todos (broadcast). Ou ainda, todos os nós podem transmitir para um único hospedeiro alvo (unicast). A complexidade aumenta na medida em que o número de máquinas conectadas ao barramento também cresce. Cabe aos protocolos da subcamada MAC organizar esse caos e disponibilizar a utilização do meio físico da maneira eficiente.

Uma rede de difusão pode ser comparada a uma reunião em uma empresa, na qual os funcionários estão em uma mesma sala. Todos estão próximos uns aos outros de forma que cada um pode falar com os demais e ser ouvido. Mas, e se todos quiserem falar ao mesmo tempo? Com certeza será uma confusão e ficará difícil compreender o que cada um diz. Para que a pauta da reunião possa ser entendida pelos participantes, deve ser definida uma sequência para as colocações. Assim, cada um pode falar na sua vez e transmitir o seu recado. Outro problema que pode ocorrer em uma situação como essa é que existem funcionários que teriam muito para dizer e outros, quase nada. Ou seja, deve ser reservado maior tempo a quem tem mais informações para passar.

Figura 174

Finalizando o processo.

DICA

A sociedade ABUSAR (Associação Brasileira dos Usuários de Acesso Rápido) oferece manuais de configuração de modems e roteadores de diversas marcas e modelos. Entidade civil sem fins lucrativos criada em 2001, a ABUSAR tem como objetivo melhorar a qualidade dos serviços de acesso à internet por banda-larga (conexões de alta velocidade). Mais informações podem ser obtidas no site <http://www.abusar.org.br>.

**Backbone** – expressão que significa espinha dorsal ou suporte principal. Refere-se às linhas com capacidade para transmitir grandes quantidades de dados em alta velocidade na internet.

Esse cenário simula perfeitamente uma rede de difusão e os problemas que devem ser gerenciados. Nessa analogia, os participantes da reunião são comparados a computadores, comunicando-se dentro do ambiente da sala, que é o meio físico para a propagação da voz. Nesse caso, as palavras transmitidas pelos “enlaces bocas” e recebidas pelos “enlaces ouvidos” se portam como o segmento da camada de enlace. Significa que somente é possível fazer a comunicação de um transmissor para um receptor de cada vez. Caso contrário, a informação se perderá. Além disso, deve haver um controle na distribuição do tempo de uso do canal entre as estações participantes do barramento.

Distribuição do canal

Assim como na reunião da empresa em que só uma pessoa deve falar por vez, em uma rede de difusão apenas um hospedeiro pode transmitir por vez. Para saber de quem é a vez de falar, ou melhor, de transmitir, existem várias estratégias; algumas estáticas, outras dinâmicas (veja quadro *Transmissão eficiente*).

Transmissão eficiente

Para melhor aproveitar o canal de comunicação, alguns protocolos da camada MAC programam a distribuição dinâmica, conforme as seguintes premissas:

- **Modelo da estação:** se uma estação começar a receber quadros, ela não poderá transmitir ao mesmo tempo. Deverá esperar até que a mensagem toda termine. Resumindo, se um fala, o outro deve somente escutar.
- **Canal único:** todos podem transmitir, mas existe controle de prioridade para prestigiar alguma estação que tenha mais dados para enviar.
- **Colisão:** caso duas estações resolvam transmitir ao mesmo tempo, os quadros vão ser mutuamente alterados. É o que se chama de colisão. Quando isso acontece, os adaptadores de rede conseguem identificar o que houve e forçam a retransmissão dos quadros em tempos aleatórios para evitar que colidam novamente.
- **Tempo segmentado:** para transmitir o adaptador de rede, é preciso aguardar um temporizador que delimitará o tempo de transmissão. Nesse caso, diferentemente da divisão estática, o tempo que não estiver sendo utilizado será redistribuído. Algumas implementações de rede não fazem esse controle e transmitem a qualquer momento.
- **Deteção de portadora:** antes de transmitir dados, as estações podem monitorar o canal para descobrir se alguém está transmitindo. Se o canal estiver ocioso, o quadro será transmitido e os outros terão que esperar o processo terminar para fazer a sua transmissão. Algumas redes não realizam essa deteção por intermédio da portadora e transmitem sempre que precisar. Caso haja colisão, transmitem novamente.

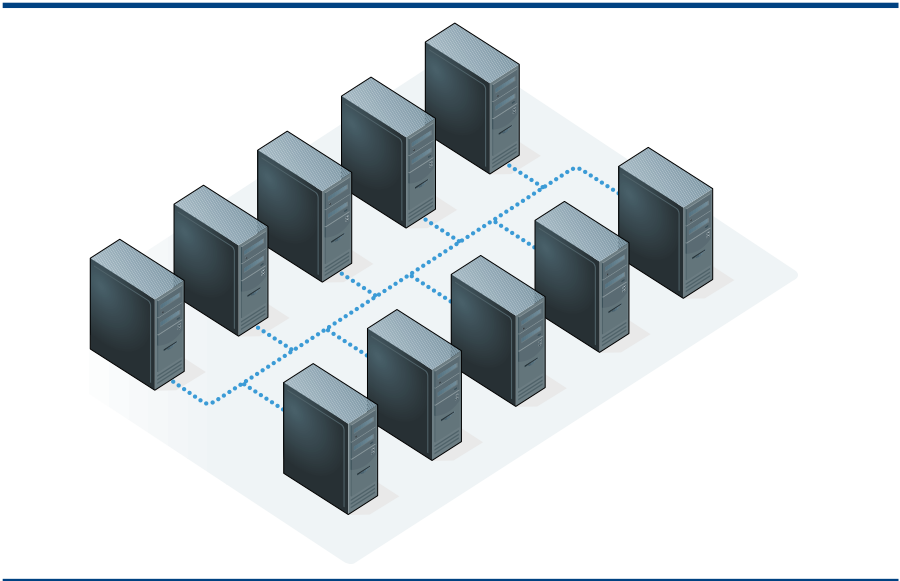


Figura 175

Meio físico compartilhado.

Em uma Distribuição Estática de canais, a porção de tempo que cada hospedeiro tem para transmitir é simétrica, ou seja, é igual para todos os hosts, mesmo que uma dessas máquinas seja um servidor e, portanto, deva transmitir mais. Pense em uma rede com dez computadores (figura 175), sendo que cada um pode transmitir por apenas 1 segundo. Chega a vez do computador 1 transmitir. Ele, então, envia o que puder em um segundo e passa a vez de usar o meio físico para o micro 2. Agora, o hospedeiro 1 deverá esperar 9 segundos até passar o tempo de todas as outras estações da rede para transmitir por mais 1 segundo. Isso vai acontecer mesmo que os computadores 3, 4, 5, 6, 7, 8, 9 e 10 nada tenham para transmitir e não utilizem o tempo reservado para eles. Essa técnica estática tem o nome de TDM (Time Division Multiplexing ou Multiplexação Dividida por Tempo).

Outra técnica é FDM (Frequency Division Multiplexing ou Multiplexação Dividida por Frequência). Nesse caso, o canal é dividido em frequências diferentes, que não interferem umas nas outras e podem ser transmitidas ao mesmo tempo. É semelhante às rádios AM/FM, que transmitem pelo ar, porém, cada uma trabalha em sua faixa de frequência sem interferir no som de outras rádios que estão em outras frequências. No entanto, a largura de banda, ou seja, a quantidade de dados que pode ser transmitida ao mesmo tempo, também acaba sendo dividida de forma simétrica. E, mesmo que uma frequência não esteja sendo utilizada por vários computadores, a largura de banda não pode ser redistribuída para quem estiver transmitindo. Isso quer dizer que tanto na TDM como na FDM ocorre ociosidade e baixo aproveitamento da capacidade de transmissão do canal.

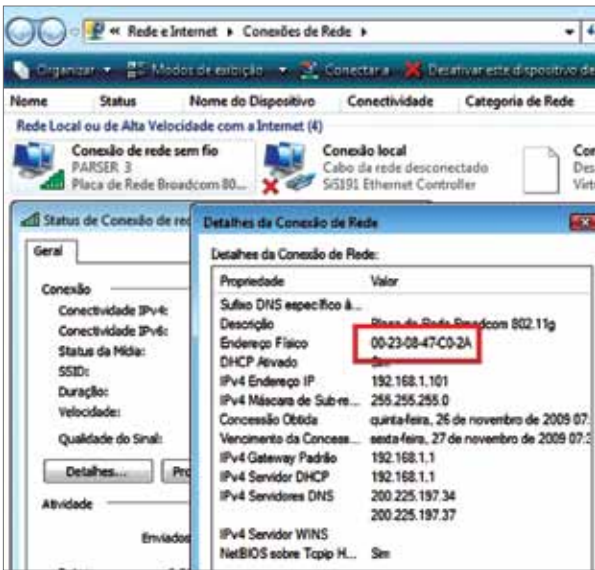
Ethernet

A Ethernet foi desenvolvida por Robert Metcalf, em 1973, quando ele trabalhava na Xerox **PARC**. E só começou a ser comercializada em 1979, ano em que o próprio Metcalf fundou a 3Com para produzir equipamentos para essa tecnologia. A empresa contou com apoio da Intel (fabricante de processadores para computador), da DEC (Digital Equipment Corporation) e também da Xerox para tornar a Ethernet um padrão para redes locais ou menores, pressionando o mercado das

PARC é a sigla para Palo Alto Research Center, o centro de pesquisas da Xerox em Palo Alto, Califórnia, Estados Unidos, fundado em 1970.

Figura 176

Endereço MAC do Adaptador sem fio.



As redes Token Ring utilizam uma topologia lógica de anel e não de barramento como acontece nas redes Ethernet. O custo de montar uma rede Token Ring é mais alto do que o de uma rede Ethernet e sua velocidade de transmissão está limitada a 16 mbps contra os 100 mbps das redes Ethernet. Porém, as redes Token Ring têm suas vantagens: a topologia lógica em anel é quase imune a colisões de pacote. E, por usarem hubs inteligentes, essas redes permitem que diagnóstico e a solução de problemas sejam mais simples. A Arcnet é uma arquitetura de rede criada nos anos 1970 e hoje considerada ultrapassada e em vias de extinção. Oferece pouca largura de banda e não é compatível com o Windows. Quem utiliza essa arquitetura ainda hoje acaba recorrendo ao DOS.

tecnologias concorrentes como **Token Ring e ARCNET**. O nome “Ether-net” remete ao material chamado “éter luminífero”, ao qual os físicos do início do século XIX atribuíam a capacidade de ser um meio de transmissão da luz.

A Ethernet utiliza o padrão CSMA/CD (Carrier Sense Multiple Access with Collision Detection ou Detecção de Portadora em Múltiplos Acessos com Detecção de Colisão) para gerenciar o acesso ao meio físico. Esse sistema utiliza “detecção de portadora”.

A identificação dos enlaces é feita por meio de endereços MAC, representados pelo número 48 bits escrito normalmente em notação hexadecimal. Esse número é um identificador global, ou seja, não podem existir dois adaptadores de rede com o mesmo número. O fabricante do adaptador de rede é quem atribui esses endereços, que estão ligados ao hardware. Por esse motivo, é comum chamar um endereço MAC de endereço físico (figura 176).

A Ethernet foi padronizada na especificação IEEE com o número 802.3. A partir daí, algumas variantes foram desenvolvidas, tanto para redes LAN quanto para WAN. Porém, muitas se tornaram obsoletas, como a 10BASE5, e outras nem chegaram a ser produzidas, como é o caso da 10BASE-FP.

VARIANTES DO PADRÃO ETHERNET		
Variação	Especificação	Taxa Transmissão
10Base-T Ethernet padrão original, já em desuso.	802.3	10 MBps
100Base-T FastEthernet Mais utilizada atualmente no Brasil	802.3u	100 MBps
1000Base-T Gigabit	802.3z	1G Bps
10000Base-T 10 Gigabit Ethernet	802.3ae	10 GBps

Figura 177

HUB de quatro portas.



MICHAEL GRIFIN/ALAMY/OTHER IMAGES

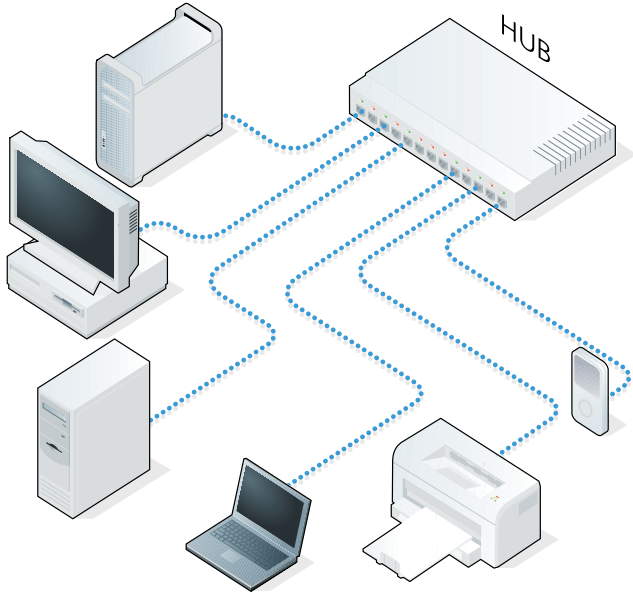
HUB – Concentrador

O cabo de par trançado é o meio físico mais utilizado em LANs. Nesse tipo de cabo, existem somente duas terminações, nas quais se podem conectar adaptadores. À primeira vista, só seria possível conectar duas estações. Porém, para ampliar essa capacidade, utiliza-se um equipamento da camada física denominado HUB (figura 177). Ele funciona como um agregador, um ponto onde os cabos podem se unir, formando um único barramento. Aparentemente é uma topologia em estrela, mas na verdade seu layout lógico é mesmo em forma de barramento. Esse tipo de conexão permite que um quadro transmitido pela rede seja visto por todas as estações conectadas ao HUB, da mesma forma que acontece quando se usa cabo coaxial (figura 178).

Os HUBs são recomendados para redes pessoais e pequenas redes locais por vários motivos. Um deles está ligado à segurança da informação: os dados podem ser facilmente lidos por pessoas maliciosas que usam sniffers (“farejadores”), que são programas capazes de analisar o tráfego da rede. Com os HUBs, porém, há perda de desempenho, pois o barramento estará sempre difundindo os pacotes que chegam para todos os nós conectados a ele, sem qualquer tipo de gerenciamento de repasse.

Figura 178

Esquema de interligação com HUB Ethernet.





**Figura 179**  
Switch de 24 portas.



**Switch – Chaveador Ethernet**

Um switch, que em português significa interruptor, é um equipamento usado para interligar cabos vindos de várias estações. É semelhante ao HUB. Porém, suas portas não se comunicam diretamente entre si, e os circuitos são controlados por um software de gerenciamento. Esse software analisa o fluxo de dados e o redireciona para as portas envolvidas apenas na transmissão. Assim, o switch (figura 179) evita que os quadros sejam retransmitidos para os outros enlaces (portas). O equipamento gera verdadeiros circuitos e o meio de comunicação física entre esses circuitos fica praticamente livre de compartilhamento com outras estações. Isso evita colisões e garante o máximo desempenho do equipamento. Além de todas essas vantagens, o switch tem se tornado cada vez mais barato. Isso quer dizer que praticamente não existem motivos para se usar os HUBs hoje em dia.

Alguns fabricantes oferecem equipamentos classificados como HUB gerenciável ou HUB switch. São peças consideradas “quase” switches, criadas para fazer o controle do tráfego da rede, porém de maneira um pouco mais barata e simples em relação ao switch. Mas, apesar de possuírem técnicas gerenciáveis, esses dois tipos de HUBs não são capazes de fechar circuitos entre portas. Continuam oferecendo barramentos compartilhados por todos a todo o momento.

**20.3.3.19. Camada física**

Agora, apresentaremos a camada mais baixa de todas: a camada física do modelo ISO/OSI (Open System Interconnection ou Sistema Aberto de Interconexão, definido pela International Organization for Standardization – ISO). Nessa camada, conheceremos os meios físicos de transmissão, procedimento de montagem de cabos e ferramentas.

**20.3.3.19.1. Serviços oferecidos pela camada física**

O meio físico tem a função de oferecer às camadas superiores o “éter”, ou seja, o meio por onde os dados serão transportados em forma de sinais elétricos, magnéticos, ópticos etc. Nessa camada, são utilizados diferentes tipos de materiais para transmitir informações de um computador para outro. Cada um deles tem qualidades específicas, como custo, largura máxima de banda, retardamento, complexidade de instalação etc.

Devemos levar em consideração que a velocidade de transmissão, ou seja, a largura de banda, depende diretamente do tipo de material utilizado, assim como do comprimento e da espessura desse material.

**20.3.3.19.2. Meio de transmissão**

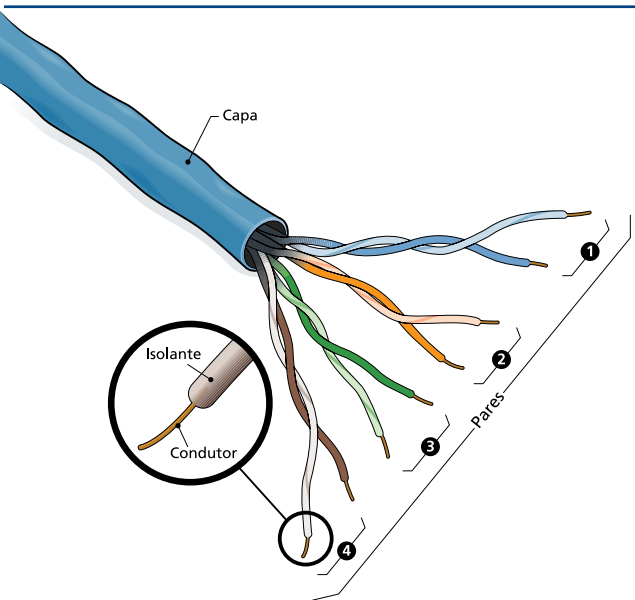
Os meios de transmissão se dividem em dois grupos: os meios guiados, como cabos de cobre ou de fibra óptica, e os não guiados, como ondas de rádio e laser, que são transmitidos pelo ambiente.

**20.3.3.19.3. Meio magnético**

É muito comum a transmissão de dados de um computador para outro por meio de memória flash (cartão, pen-drive), de disco rígido e até de unidades de fita, que são de alta capacidade. Apesar de serem considerados meios desconectados, essas unidades de armazenamento conseguem levar dados de um computador para outros com uma considerável largura de banda. Por exemplo, o tempo que você leva para tirar o pen-drive de um notebook ao lado do seu computador de mesa e inserir na USB de um notebook do seu lado pode ser de até 2 segundos, isso se você tiver prática. Ou seja, se o pen-drive tiver capacidade de 16 GB, a transmissão será de 8 GBps (16 GB / 2 segundos). É uma velocidade de transmissão fenomenal. Porém, na medida em que a distância entre esses computadores vai aumentando, a velocidade da banda cai.

**20.3.3.19.3.1. Par trançado**

Quando se trata de um projeto de rede para uma LAN que exige baixo custo e bom desempenho, uma boa opção é usar cabos de pares trançados (UTP- Unshielded Twisted Pair). Esses cabos são utilizados tanto pelas empresas de telefonia quanto por proprietários de LANs e até por usuários domésticos há mais de 10 anos. Isso faz com que a tecnologia amadureça e vários fabricantes melhorem o processo de



**Figura 180**  
Visão lateral de um cabo UTP categoria 5.

produção, principalmente por conta do aumento da concorrência. Dessa forma, o custo de implantação se torna cada vez mais baixo em relação a outros tipos de meio físico. Porém, o tamanho desses cabos não pode ultrapassar 100 metros. Na verdade, é recomendado no máximo 50 metros para evitar perda de desempenho. Tanto para redes de 100 Mbps (FastEthernet) como para Ethernet Gigabits.

O cabo de par trançado utilizado em redes FastEthernet e Gigabit é o da categoria 5. É formado por um feixe de 8 fios de cobre, com 1mm em média cada um. Esses fios são recobertos por um material plástico isolante e torcidos de dois em dois, formando 4 pares de fios (como se pode ver na figura 180). E cada par é envolvido por uma capa de PVC que ajuda a proteger e conduzir os cabos.

Os fios são torcidos por uma razão muito simples: diminuir a interferência, já que esses cabos conduzem eletricidade. E dessa corrente elétrica que trafega por eles escapam ondas que invadem a comunicação do cabo vizinho provocando interferência. Se os cabos que ficam juntos estivessem em paralelo, transmitiriam sinal como se fossem antenas, o que seria ainda pior. Mas quando os cabos estão torcidos, os sinais de onda se espalham para todos lados e vão se anulando na medida em que colidem entre si.

20.3.3.19.3.1.1. Normas de montagem

Os cabos UTP são conectados às portas dos HUBs, a adaptadores de rede, a switches etc., por meio de conectores do tipo RJ45 (figura 181). Esse conector possui oito vias que farão a ligação entre o fio e os filamentos de contato da tomada.

O processo de montagem de um cabo é chamado de crimpagem. A norma da **ABNT** NBR 14565:2000 padroniza dois tipos de disposição dos fios na crimpagem dos conectores dos cabos: a EIA/TIA T568A e a T568B. Essa norma foi atualizada na revisão de 2006, com a inclusão do padrão EIA/TIA 568-C para as redes Ethernet 10 Gigabits com cabos de pares trançados blindados (Shielded Twisted Pair – STP).

Os cabos possuem cores que identificam os pares. Cada par contém um fio com uma única cor e outro com uma faixa branca. Na figura 182 podemos ver a sequência de montagem dos fios nos dois padrões de crimpagem UDP (User

A Associação Brasileira de Normas Técnicas (ABNT) é a responsável por definir normas e padrões para produtos e serviços de vários setores da economia. A TIA (Telecommunications Industry Association ou Associação da Indústria de Telecomunicações) e a EIA (Electronic Industries Association ou Associação das Indústrias Eletrônicas) são instituições que criam padrões para a Indústria de Telecomunicações e de Eletrônicos.

Figura 181

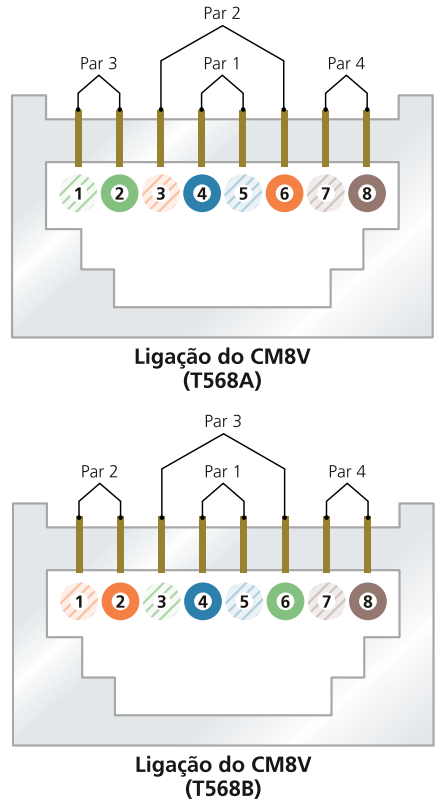
Conector RJ45.



JACK KUNNEN/ALAMY/OTHER IMAGES

Figura 182

Padrão de ligação do T568A e T568B.



Datagram Protocol ou Protocolo de Datagrama de Usuário): T568A e T568B

Vimos como são as sequências padrões de encaixe dos fios. Agora, devemos identificar quando iremos utilizá-las. Existem duas combinações possíveis:

**Cabo Direto:** nesse formato, as duas extremidades do cabo devem ter sido crimpadas da mesma maneira. Existem cabos direto montados tanto com T568A ou T568B. Esse tipo de cabo é próprio para ligar dispositivos diferentes: Computador e HUB; Computador e Switch etc.

**Cabo Crossover (Cabo Cruzado):** ao contrário do cabo direto, o crossover é montado de forma alternada, utilizando em uma extremidade o padrão T568A e na outra o T568B. Serve para conectar dois equipamentos iguais: dois computadores, fazer cascadeamento de HUB (um HUB ligado ao outro), ligar switches, roteador com roteador etc.

Existem dispositivos que são Auto-MDIX (Automatic Medium-Dependent Interface Crossover, que pode ser traduzido como detecção automática de dependência de cabo cruzado) e se adaptam ao tipo de montagem de cabos que for conectado nele.

20.3.3.19.3.1.2. Ferramentas

Para a confecção de cabos UTP e STP, devemos usar ferramentas apropriadas, como o alicate de crimpagem (figura 183) e o alicate decapador (figura 184). Para teste, utilizamos testadores de cabo.

Figura 183

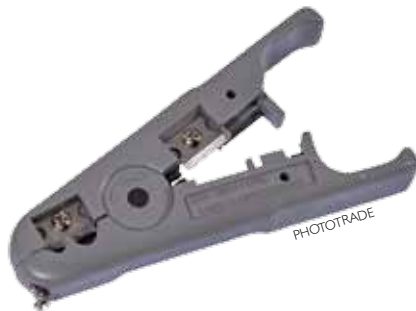
Alicate de crimpagem.



ROBERT GRUBBA/ALAMY/OTHER IMAGES

Figura 184

Alicate decapador.



Na verdade, o testador de cabos (figura 185) não é obrigatório, mas é recomendável dispor de um equipamento desse tipo. Se o cabo foi montado errado, ainda que por descuido, o problema será detectado imediatamente. Outra alternativa é conectar o cabo em dois computadores e tentar fazer uma transmissão para ver se está tudo em ordem. Em alguns casos, mesmo ligado errado, um cabo pode aparecer como conectado no computador. Porém, não será capaz de transmitir dados nem oferecerá o desempenho máximo possível.

20.3.3.19.3.1.2.1. Procedimento de montagem

Depois de medir o tamanho do cabo, podemos crimpar os conectores RJ45 nas suas extremidades. No entanto, é preciso tomar muito cuidado para não torcer o cabo durante essa etapa do trabalho, pois os filamentos são finos e podem se romper facilmente. Se isso acontecer, todo o trabalho ficará prejudicado (leia *Como montar o cabo em quatro passos*).

Figura 185

Testador de cabo UTP.



EDUARDO POZELLA

Como montar o cabo em quatro passos

1. Decapagem

Para que possamos organizar os fios dentro dos padrões vistos anteriormente, temos de remover a capa isolante de PVC e deixá-los aparentes. Utilizaremos um alicate decapador ou um alicate de crimpagem que possua as duas funções (figura A).

Posicione o cabo entre as lâminas de decapagem do alicate, de forma que a ponta fique com uma sobra de 2 a 3 cm (figura B). Aperte com cuidado para cortar somente a capa, sem atingir os fios.

2. Organização dos fios

Para facilitar o manuseio na hora de organizar os fios, segure na ponta dos fios que estão aparecendo e corra a mão sobre o cabo. Puxe a capa no sentido contrário, fazendo uma leve pressão. A capa deverá retrair e deixar um pedaço maior dos fios aparentes, sem que o material isolante seja danificado. Agora, separe os pares trançados e acerte um por um, deixando-os bem retos (figura C).

Posicione o cabo no padrão T568A ou T568B. Aperte bem com os dedos os fios já posicionados, ajeitando para que eles se acomodem um do lado do outro (figura D).

Caso haja fios mais compridos que outros, corte as sobras com as lâminas de corte do alicate de crimpagem (figura E) para que todas as pontas fiquem com o mesmo tamanho (figura F).

3. Inserção

Com o cabo já preparado, podemos inserir os fios no conector, sempre com a parte lisa para cima e a trava para baixo. Assim, é possível ver os fios entrando nos seus devidos condutores (figura G).

Empurre os fios até o final, sem deixar folga entre as suas extremidades e a parede do conector. Depois, puxe a capa para dentro do conector para que ela chegue até o seu limite. Mas tome cuidado para não retirar sem querer os fios que já foram inseridos.

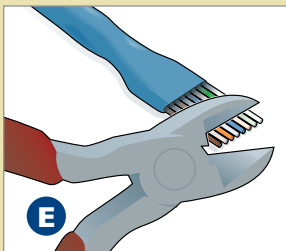
4. Crimpagem

Insira o conector na seção de crimpagem e aperte com bastante força para que os conectores “vampiros” possam descer e fincar-se nos fios. Isso permitirá o contato entre os fios e a parte de cobre. E o ressalto de fixação prenderá o cabo para que ele não se mova (figura H).

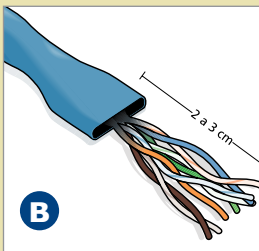
O padrão FastEthernet utiliza apenas dois pares de fios. Já o Gigabit utiliza todos os quatro pares.



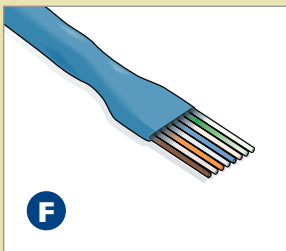
Identificando as lâminas de decapagem do cabo.



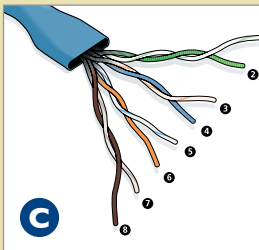
Corte de fios para alinhar o comprimento.



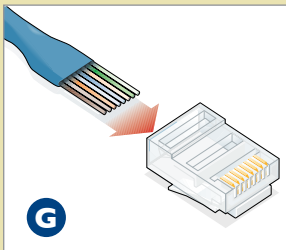
Cabo depois de decapado.



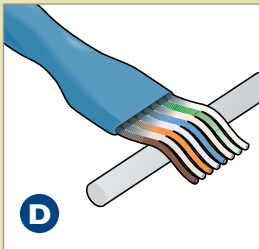
Fios prontos para crimpar.



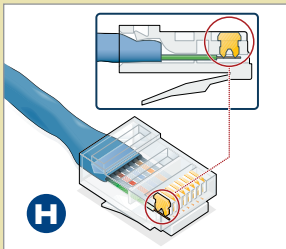
Fios bem separados e retos.



Fios sendo inseridos corretamente no conector RJ45.



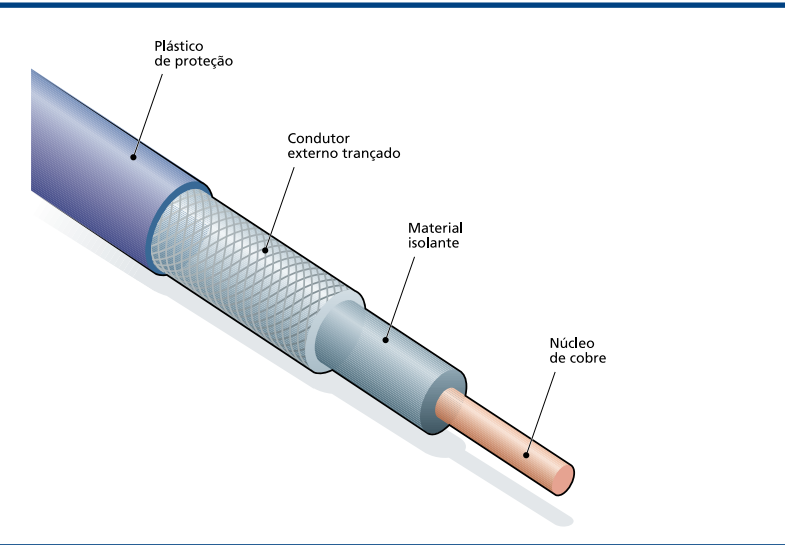
Fios sendo endireitados e posicionados um ao lado do outro.



Na crimpagem, os conectores “vampiros” se inserem nos fios e o ressalto pressiona o cabo para fixação.



**Figura 186**  
Partes de um  
cabo coaxial.



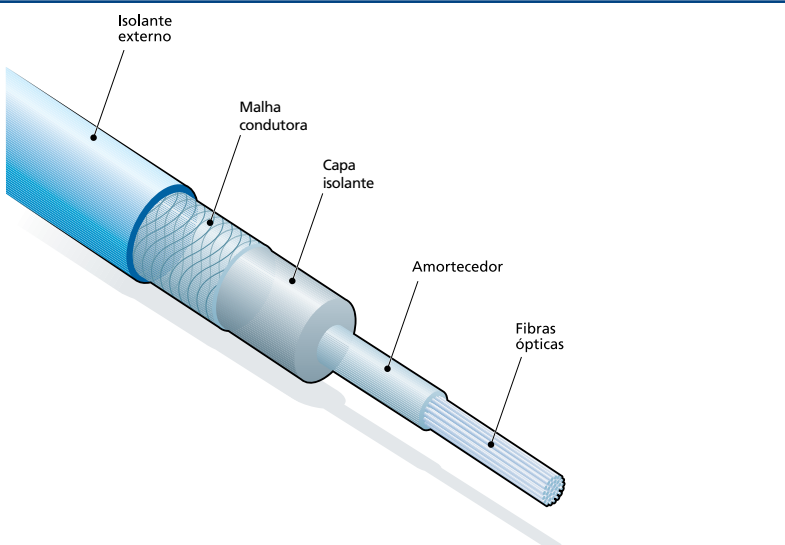
20.3.3.19.3.2 Cabo coaxial

Os cabos coaxiais já foram muito utilizados no início das redes de computadores, inclusive na montagem de LANs na primeira Ethernet de 10Base-T de 10 Mbps. Mas foram substituídos pelos cabos UTP, com as especificações FastEthernet e Gigabit.

Os cabos coaxiais permitem a transmissão de dados por vários metros, com extensa largura de banda. Por esse motivo, também foram utilizados durante muito tempo pela empresas de telefonia em redes de longa distância. No entanto, acabaram sendo substituídos pela fibra óptica e hoje são utilizados basicamente nas transmissões de TV a cabo e de internet a cabo.

A capacidade de transmissão com banda-larga e em grandes comprimentos desses cabos se deve à sua blindagem, que elimina as interferências externas (figura 186). Porém, essa mesma característica torna o custo do cabo coaxial alto em relação ao cabo de par trançado.

**Figura 187**  
Camadas de um  
cabo óptico.



No cabo coaxial, o meio de transmissão é um filamento de cobre que passa dentro de um material plástico isolante. Por fora existe uma malha condutora que absorve as interferências vindas do meio ambiente. E tudo isso é revestido com uma capa protetora de PVC. Por conter bem as interferências, a banda de transmissão desse tipo de cabo pode chegar a 1 GHz. A topologia de montagem desses cabos em uma LAN é em forma de anel, mas eles também podem ser utilizados para conexões ponto a ponto.

20.3.3.19.3.3 Fibra óptica

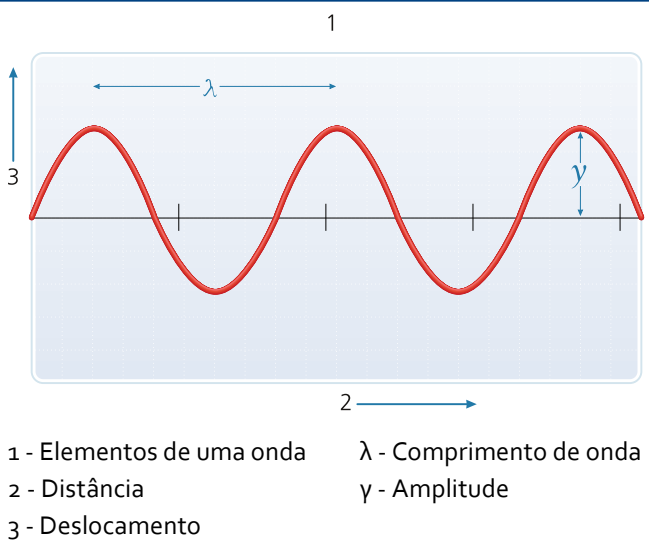
O cabo de fibra óptica é semelhante ao cabo coaxial, tanto no formato quanto na topologia. Ambos são montados em forma de anel ou ponto a ponto. Mas as semelhanças param aí. No centro do cabo de fibra óptica, vão as fibras de vidro condutoras de luz, que são as fibras ópticas propriamente ditas (figura 187). Essas fibras são capazes de direcionar a luz por vários quilômetros sem perder a intensidade.

Cada uma das fibras de vidro existentes no centro do cabo possui a espessura de um fio de cabelo. O feixe de fibras é revestido por uma “casca”, também feita de material condutor (dielétrico), que atua como se fosse um espelho, mantendo a luz presa no núcleo. Sobre essa casca há uma camada plástica protetora. Dependendo de onde o cabo será utilizado, ele poderá receber revestimentos especiais contra roedores, por exemplo. A fibra óptica é o meio de transmissão mais utilizado nos backbones de telefonia e internet e também no padrão Ethernet de 10 Gigabits.

Os cabos de fibra óptica são praticamente imunes a interferências eletromagnéticas e térmicas e oferecem uma largura de banda de até 50 Gbps em até 100 km. Necessitam de repetidores para recuperar a intensidade da luz a cada 50 km. O cabo coaxial, precisa de repetidores a cada 5 km.

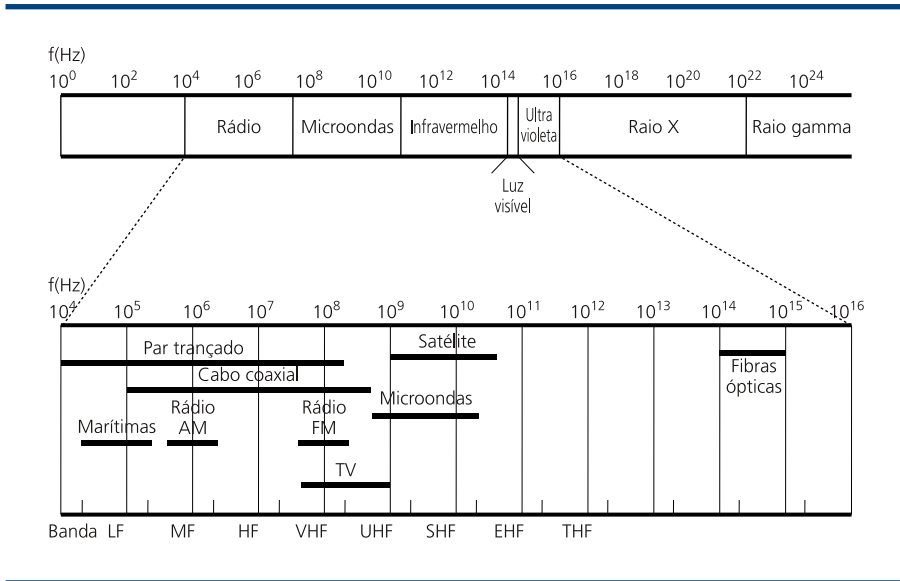
20.3.3.19.3.4 Transmissão sem fio

Quando um elétron se move, ele produz um espectro que pode ser transmitido por fios de cobre, por luz, pelo ar e até mesmo através do vácuo. Esse espectro oscila formando ondas. A distância entre as cristas dessas ondas é chamada de frequência.



**Figura 188**  
Descrição de onda.

**Figura 189**  
Espectro  
eletromagnético.



Quanto mais curta a distância entre duas cristas, maior a frequência, pois ela indica que existem mais oscilações dentro de um mesmo período de tempo (figura 188).

Da mesma forma que acontece com as cordas de um violão quando são tocadas, as ondas oscilam de cima para baixo formando uma onda sonora no ar.

Na figura 189, podemos ver que à medida que a frequência de onda do espectro aumenta, suas propriedades de transmissão se alteram. E a velocidade de transmissão de dados aumenta conforme cresce a frequência. Portanto, podemos tirar as seguintes conclusões sobre a transmissão de dados em cada uma das faixas de frequência de onda:

- A faixa de frequência de onda de até 100 Mhz, chamada de rádio, é a mais lenta para a transmissão de dados. Porém, pode se propagar por vários quilômetros e é capaz de penetrar em objetos sólidos, atravessando paredes, por exemplo. Esse tipo de transmissão sem fio é muito comum em telecomunicações. As ondas de rádio são utilizadas pelas tecnologias Bluetooth e 802.11, também conhecido como sistema Wi-Fi (figura 190).
- Acima de 100 Mhz as ondas trafegam em linha reta e conseguem transmitir mais dados. Esse meio de transmissão é usado nos celulares e nos sinais de TV. As tecnologias que adotam essa faixa de onda conseguem largura de banda cada vez maior por meio de frequências mais altas. Porém, as propriedades mudam à medida que a frequência aumenta. A partir de 4Ghz a onda é absorvida pela água, provocando aquecimento como num forno micro-ondas. Quando isso acontece, a transmissão é anulada.

- Infravermelho e milimétricas: esse tipo de onda é bastante utilizado em transmissões de curta distâncias. Exemplo: controles remotos de aparelhos eletrônicos e transmissão de dados. Antes do surgimento do Bluetooth, as transmissões sem fio entre aparelhos celulares eram feitas por meio de infravermelho.
- Luz: é bastante utilizada para transmissão entre prédios ou locais que não possuam obstáculos e não são tão distantes. Para esse tipo de transmissão é utilizado um feixe concentrado de luz chamado de laser, que emite um raio direcionado para um receptor fotodetector. Podem ocorrer problemas de interferências de objetos que atravessam o caminho da luz ou oscilações provocadas por fontes de calor.
- Raios X e raios gama: apesar de oferecem uma frequência alta e, portanto, serem capazes de transmitir em alta velocidade, esses raios não são utilizados na transmissão de dados por causarem danos à saúde.

**Figura 190**  
Símbolos comerciais  
do WiFi e Bluetooth.



## Considerações finais

Para que um técnico possa densenvolver bem seu trabalho, ele deve conhecer os equipamentos e saber como cada um funciona. É provável que quando você ler este livro, muitas das tecnologias aqui destacadas estejam obsoletas e outras talvez nem tenham sido citadas. Isso porque o universo da informática é imenso e existem várias tipos de computadores para diferentes necessidades e aplicações, como laptop, celular, PDA, GPS, que não foram abordados no livro. Para se manter atualizado, você pode visitar sites e lojas de equipamentos de informática, pesquisar e ler para saber melhor sobre as tecnologias citadas aqui. As novas gerações de dispositivos geralmente seguem uma linha de evolução e melhoram tecnologias já existentes. Portanto, não será difícil assimilar as novidades tomando por base o funcionamento de dispositivos mais antigos.

Já na área de redes observamos hoje uma evolução enorme nas últimas três décadas. Em especial, na década de 2000, quando houve uma grande expansão da internet banda-larga. A previsão é que muita coisa mude no futuro. Está prevista para 2014 a troca da versão do IPv4 pelo IPv6. Isso facilitará bastante a vida de quem utiliza a computação móvel. Várias aplicações nessa área surgirão. O IP móvel e a configuração zero do novo formato permitirão que as redes sem fio se tornem mais fáceis para o usuário leigo. Com certeza a infraestrutura dessas redes tende a crescer cada vez mais, aumentando a necessidade de profissionais especializados. As fibra ópticas devem ser mais utilizadas, como já acontece no Japão, onde a maioria das redes de fornecimento de acesso à internet já abandonou o cabo UTP (*Unshilded Twisted Rair* ou Par Trançado sem Blindagem). E a tendência é que as redes municipais tornem o serviço de acesso a altas velocidades disponível sem custos, como já vem ocorrendo em várias cidades do mundo. No Brasil, o projeto Cidades Digitais, da Universidade Estadual de Campinas (Unicamp), vem ajudando vários municípios a implantar redes que interligam a administração pública, como também as residências, com acesso gratuito à internet. As cidades de Cachoeira Paulista e Guará, ambas no estado de São Paulo, são exemplos dessa iniciativa.

Portanto, a informática tem e terá necessidade de muita mão de obra em qualquer uma de suas ramificações. E as áreas de redes de computadores, desenvolvimento web e computação móvel estão entre as mais promissoras.



## Referências bibliográficas

ABNT/CB-03 - Comitê Brasileiro de Eletricidade. (2000). *Norma brasileira para cabeamento de telecomunicações em edifícios comerciais*. 07: ABNT - Associação Brasileira de Normas Técnicas.

ABNT/CB-03 - Comitê Brasileiro de Eletricidade. *NBR 5410 - Instalações elétricas de baixa tensão*. Rio de Janeiro, RJ: ABNT, 2004.

ABNT/CB-03 - Comitê Brasileiro de Eletricidade. *NBR 5419 - Proteção de estruturas contra descargas atmosféricas*. Rio de Janeiro, RJ: Associação Brasileira de Normas Técnicas, 2001.

*CLASSLESS Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy* (01 09 1993). Disponível em <http://www.ietf.org/rfc/rfc1519.txt>. Acesso em 28, dezembro 2009

ASSIS, A. U. de e ALVES JÚNIOR, N. (19 de 09 de 2001). Protocolos de roteamento RIP e OSPF. Rede Rio de Computadores – FAPERJ, 19 set. 2001. Disponível em <http://www.rederio.br/downloads/pdf/nt01100.pdf>. Acesso em 7 out. 2009.

RED Hat, I. (2005). *Red Hat Enterprise Linux 4: Guia de Instalação para Arquitetura POWER da IBM®*. Disponível em [http://web.mit.edu/rhel-doc/OldFiles/4/RH-DOCS/rhel-ig-ppc-multi-pt\\_br-4/ap-partitions.html](http://web.mit.edu/rhel-doc/OldFiles/4/RH-DOCS/rhel-ig-ppc-multi-pt_br-4/ap-partitions.html). Acesso em 19, setembro, 2009.

IETF - Internet Engineering Task Force. (01 09 1981 r.). *INTERNET PROTOCOL*. Disponível em <http://www.ietf.org/rfc/rfc791.txt>. Acesso em 28, dezembro 2009.

IETF - Internet Engineering Task Force. (01 07 1998 r.). *IP Version 6 Addressing Architecture*. Disponível em: <[http://www.ietf.org/rfc/rfc2373.tx](http://www.ietf.org/rfc/rfc2373.txt)> Acesso em 28 dezembro 2009.

IETF - Internet Engineering Task Force. (01 01 2001 r.). *RTF 3031*. Multiprotocol Label Switching Architecture: <http://www.ietf.org/rfc/rfc3031.txt>. Acesso em 28, dezembro 2009

INTEL. Intel® Desktop Board D945GCLF Product Specification. Estados Unidos da América.

KUROSE, J. F. e ROSS, K. W. *Redes de computadores e a internet*. São Paulo: Person Addison Wesley, 2006.

STALLINGS, W. *Arquitetura e organização de computadores*. São Paulo: Prentice Hall, 2003.

TANENBAUM, A. S. *Redes de computadores*. 4ª edição. Rio de Janeiro: Campus Elsevier, 2003.

TORRES, G. *Hardware curso completo*. 4ª edição. Rio de Janeiro: Axcel Books, 2001.

Traditional IP Network Address Translator (Traditional NAT). (01 01 2001 r.). *RFC 3022 - Traditional IP Network Address Translator (Traditional NAT)*., IETF.ORG. Disponível em <http://www.apps.ietf.org/rfc/rfc3022.html>. Acesso em 28, dezembro 2009.





**CENTRO PAULA SOUZA**





## Excelência no ensino profissional

Administrador da maior rede estadual de educação profissional do país, o Centro Paula Souza tem papel de destaque entre as estratégias do Governo de São Paulo para promover o desenvolvimento econômico e a inclusão social no Estado, na medida em que capta as demandas das diferentes regiões paulistas. Suas Escolas Técnicas (Etecs) e Faculdades de Tecnologia (Fatecs) formam profissionais capacitados para atuar na gestão ou na linha de frente de operações nos diversos segmentos da economia.

Um indicador dessa competência é o índice de inserção dos profissionais no mercado de trabalho. Oito entre dez alunos formados pelas Etecs e Fatecs estão empregados um ano após concluírem o curso. Além da excelência, a instituição mantém o compromisso permanente de democratizar a educação gratuita e de qualidade. O Sistema de Pontuação Acrescida beneficia candidatos afrodescendentes e oriundos da Rede Pública. Mais de 70% dos aprovados nos processos seletivos das Etecs e Fatecs vêm do ensino público.

O Centro Paula Souza atua também na qualificação e requalificação de trabalhadores, por meio do Programa de Formação Inicial e Educação Continuada. E ainda oferece o Programa de Mestrado em Tecnologia, recomendado pela Capes e reconhecido pelo MEC, que tem como área de concentração a inovação tecnológica e o desenvolvimento sustentável.