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.

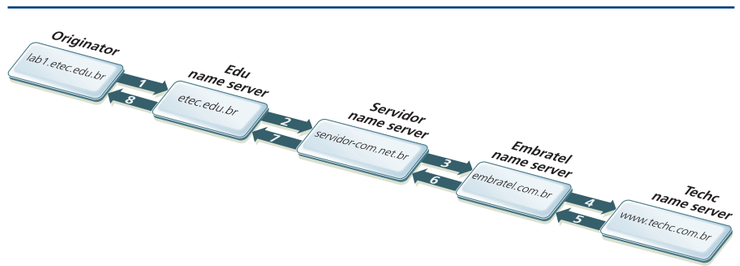


Figura 123
Processo de tradução de domínio.

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.

```
C:\>ping registro.br

Disparando registro.br [200.160.2.3] com 32 bytes de dados:
Resposta de 200.160.2.3: bytes=32 tempo=284ms TTL=58
Resposta de 200.160.2.3: bytes=32 tempo=20ms TTL=58
Resposta de 200.160.2.3: bytes=32 tempo=61ms TTL=58
Resposta de 200.160.2.3: bytes=32 tempo=25ms TTL=58

Estatísticas do Ping para 200.160.2.3:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 20ms, Máximo = 284ms, Média = 97ms

C:\>
```

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.

```
C:\>nslookup www.ipv6.com
Servidor:  dns-primario.ctbctelecom.com.br
Address:  200.225.197.34

Não é resposta de autorização:
Nome:    www.ipv6.com
Addresses:  2001:418:8c01:22::171
          204.101.17.100

C:\>
```

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

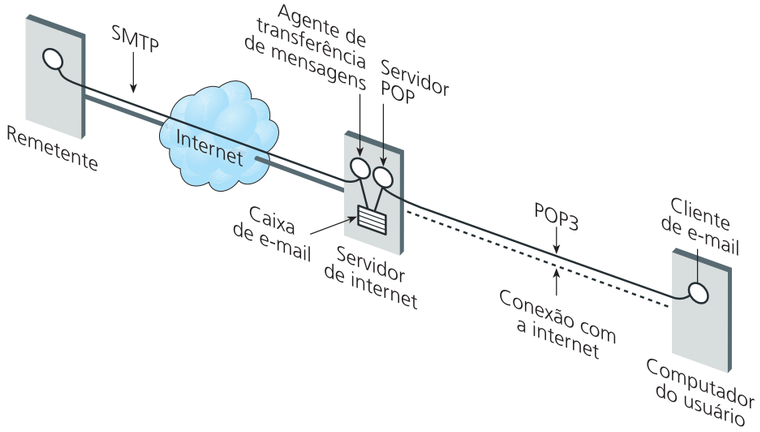


Figura 126 Protocolos de transmissão de e-mails: SMTP e POP.

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.

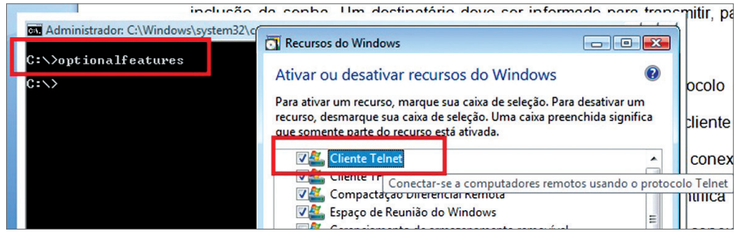
RFC é o acrônimo para Request for Comments, especificação técnica desenvolvida sobre determinado assunto por solicitação da IETF (Internet Engineering Task Force), comunidade internacional cuja meta é a evolução contínua da internet.

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).

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.

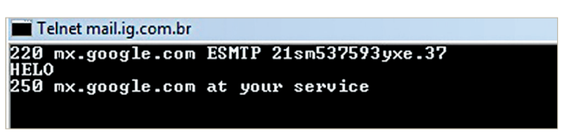
Se o servidor SMTP estiver ativo, o telnet irá se conectar na porta 25 da máquina portadora do domínio mail.ig.com.br. O servidor então enviará para o telnet cliente uma mensagem de boas vindas:

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.

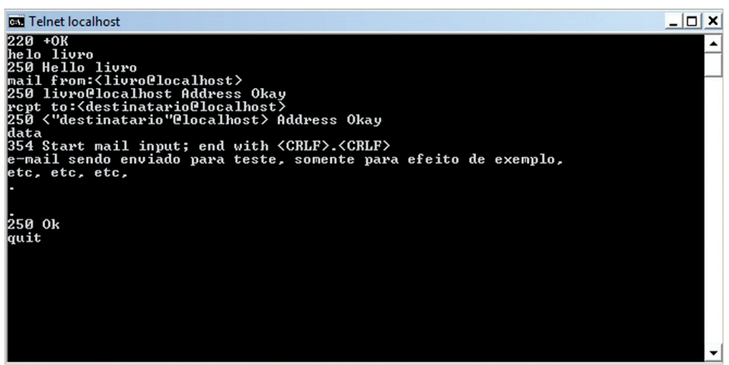


Figura 130
Diálogo entre o servidor e o cliente de telnet.

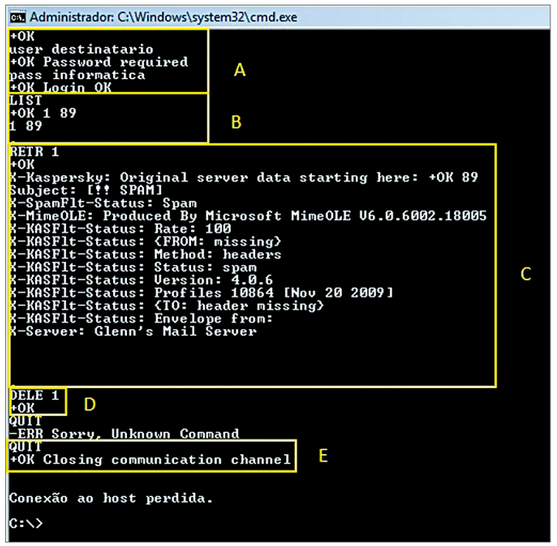
POP3 – Empregado para receber as mensagens, o protocolo Post Office Protocol versão 3 (ou Protocolo de Correio) está especificado na RFC 1939. Seu processo de recepção tem três fases: autenticação (figura 131), transação e atualização.

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, Mozzila 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:

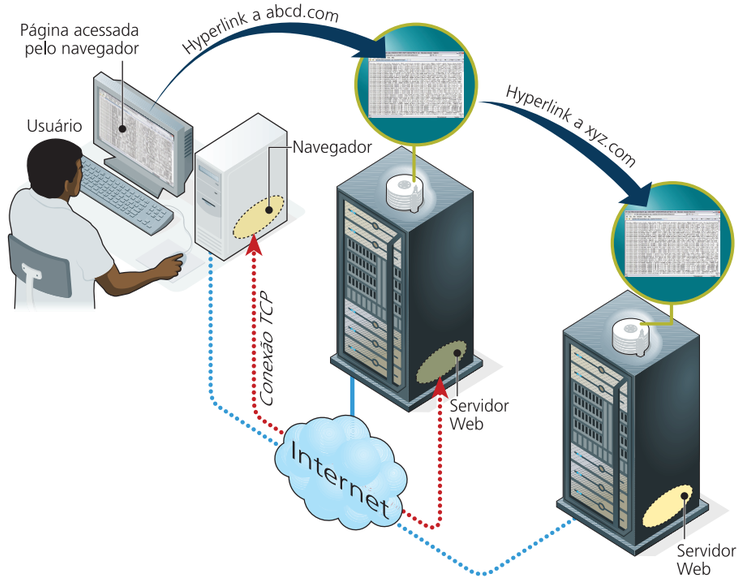
```
http://www.tvcultura.com.br/educacao.
```

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 segurança, 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.

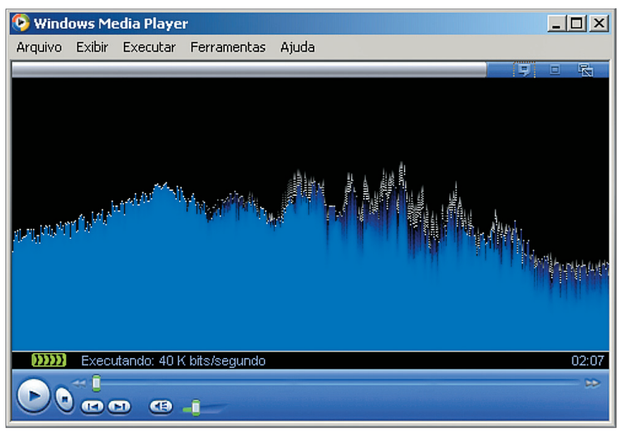
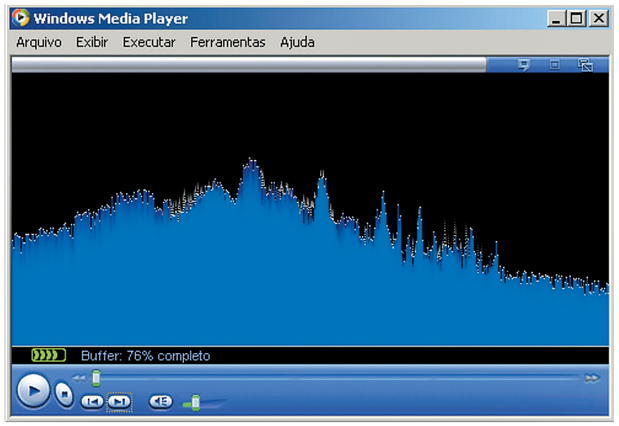


Figura 134
Formato para transmissão streaming.

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).

O Terminal Service permite contato com outro computador. Quando, por exemplo, você clica em opção inválida em um programa ou quando uma operação não pode ser concluída, o windows da máquina remota emite um som de alerta. Esse som será transmitido para quem está controlando remotamente o computador através do protocolo RDP.

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 reprodutor 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).

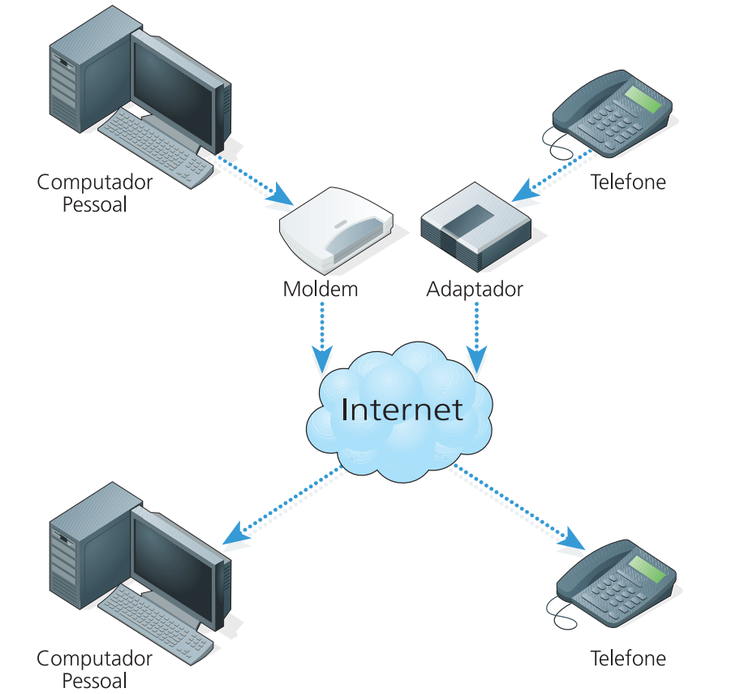


Figura 136
Esquema da tecnologia VoIP.

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

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.

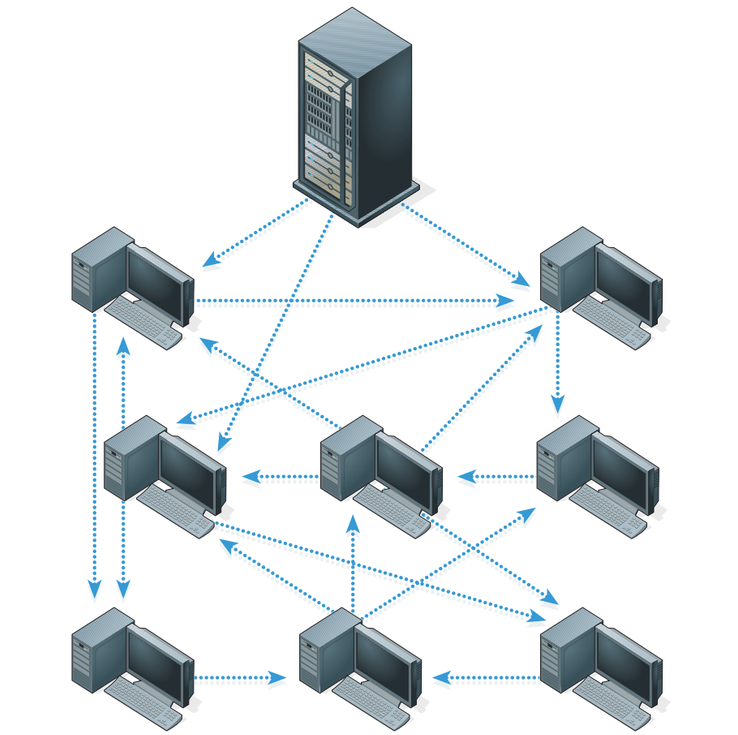


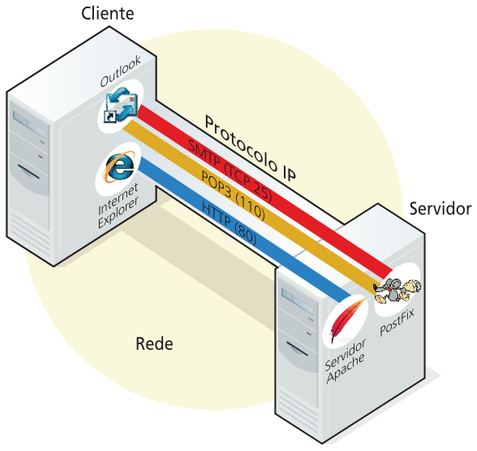
Figura 137
Compartilhando conteúdo.

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 softwarte 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

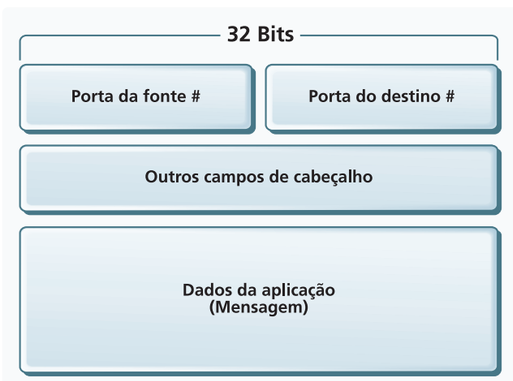


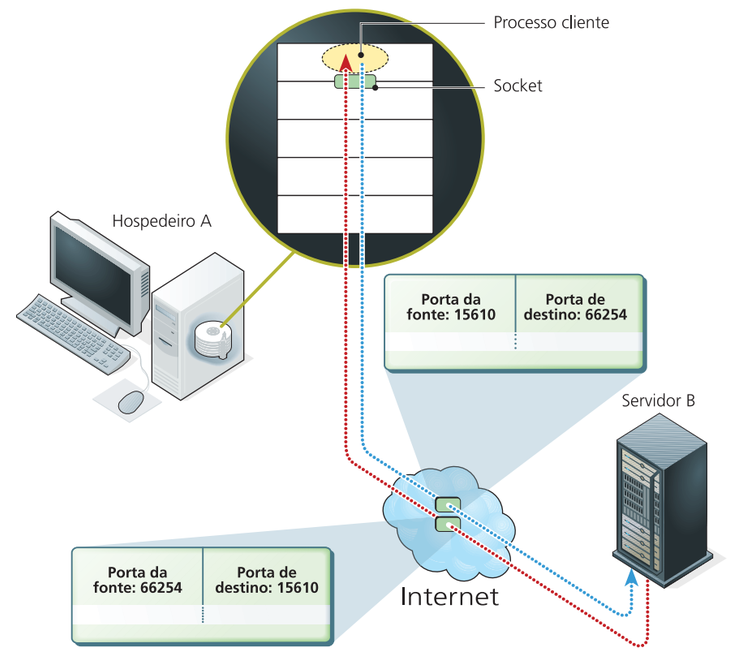
Figura 139
Formato de um segmento TPC com os campos da porta de origem e destino.

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 empacoteamento 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 reposta 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.

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.

Segmento UDP

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

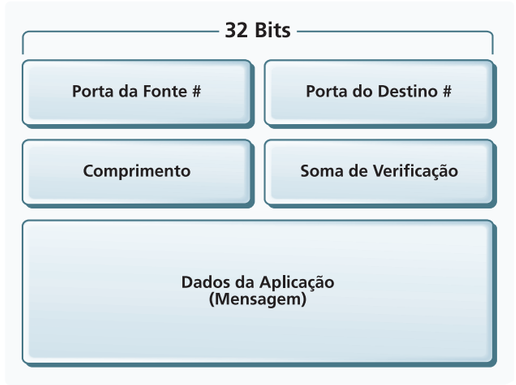
Porta da fonte – Utiliza 16 bits e indica quem enviou o segmento.

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

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.

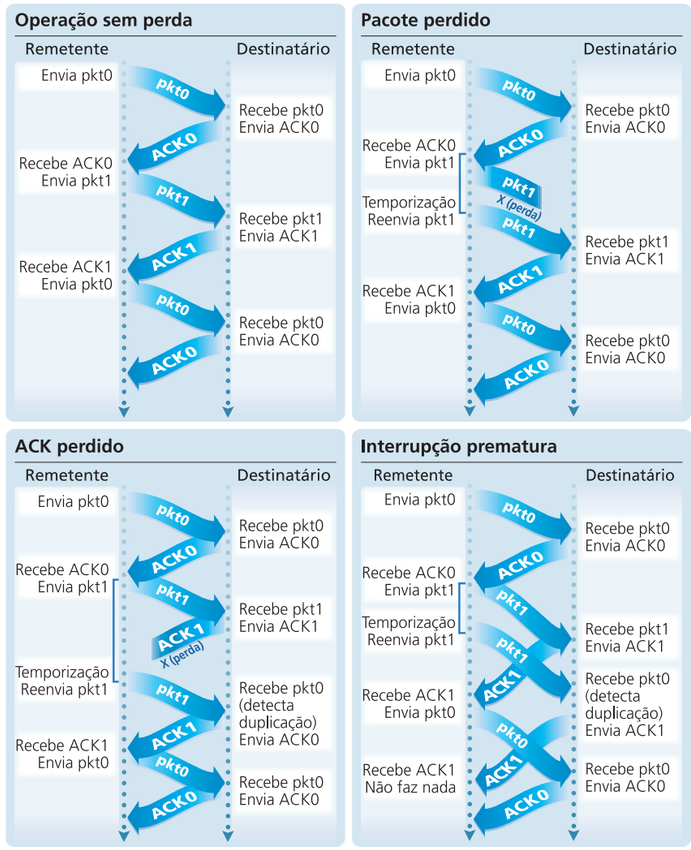
O TCP também age no controle do sequenciamento dos segmentos, identificando quando um pacote foi enviado duas vezes, ou se falta algum pacote entre os que foram recebidos. Para isso há um número sequencial em cada pacote (figura 142).

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)

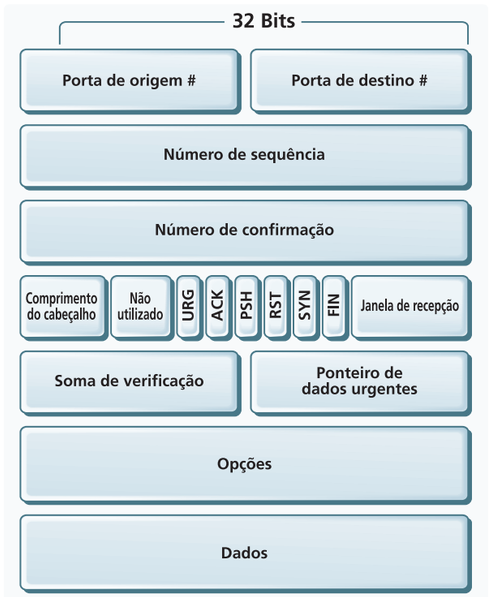
Porta da origem – 16 bits para o número do socket que envia o segmento.

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

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.

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.

Figura 144
Funcionamento do roteador.

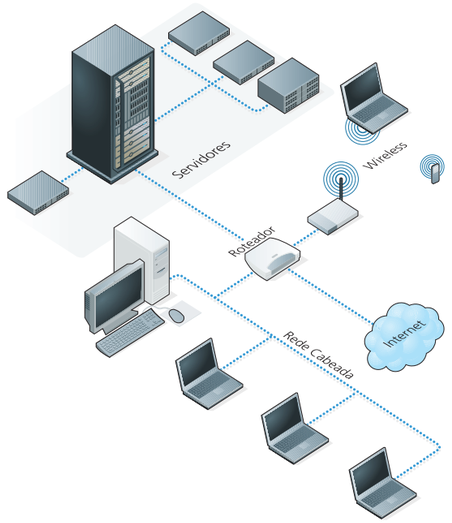
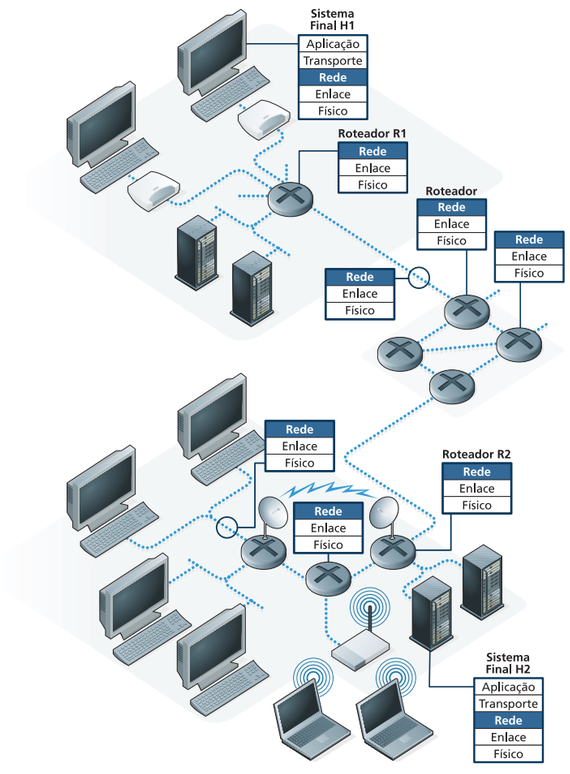


Figura 145
Ligação entre redes.



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.

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.

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.

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.

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.

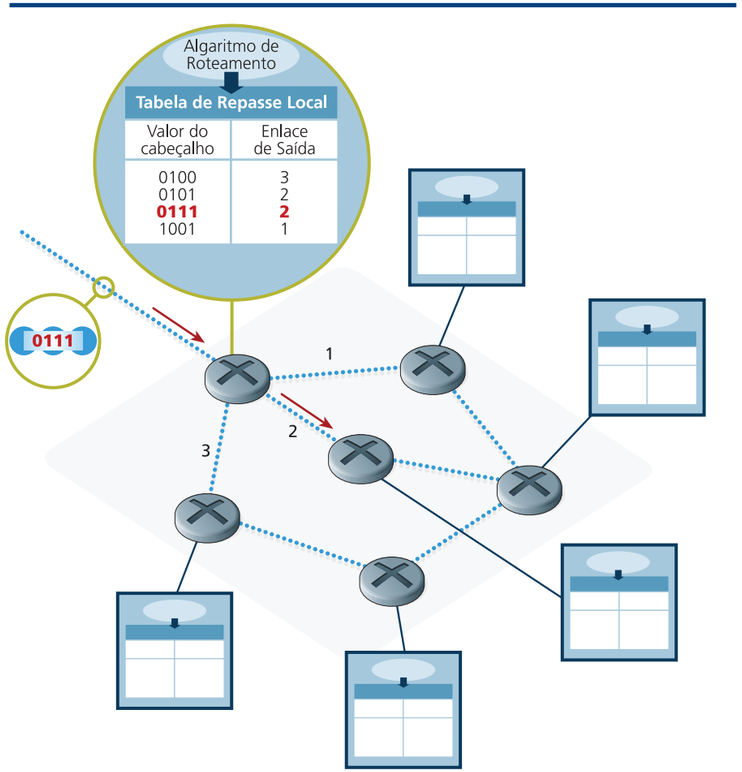
20.3.2.1. Rede de circuitos virtuais

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.

Figura 146
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.

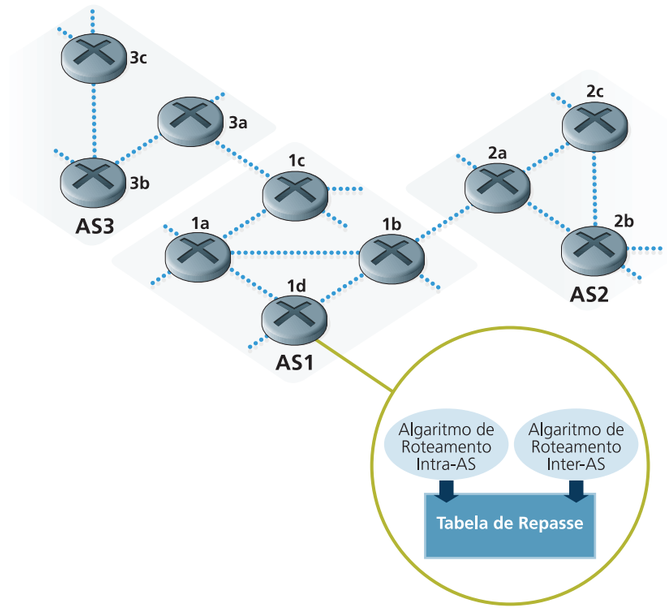


Figura 147
Sistemas autônomos podem se conectar por meio de roteadores gateway.

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 alogaritmo*. 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.

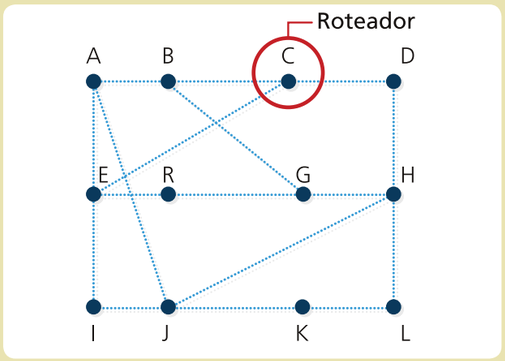
Este segundo tipo consegue se recuperar instantaneamente de alterações ocorridas nas ligações da rede, sem necessitar de qualquer intervenção.

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.

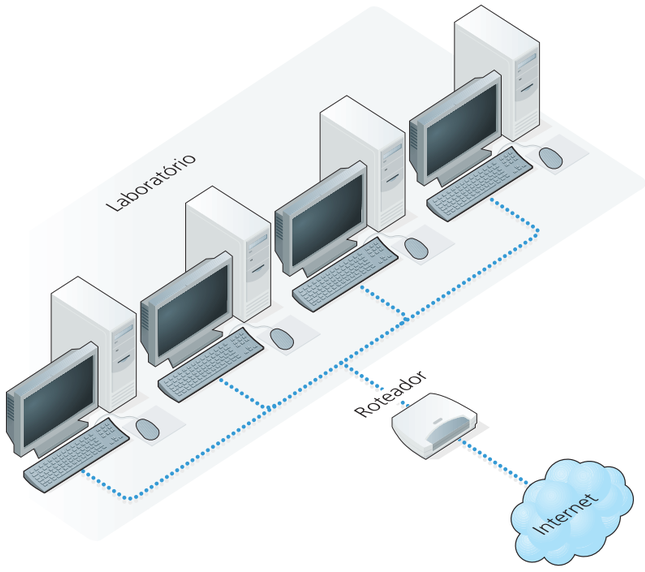
Algoritmo dinâmico com vetor de distância: nesse tipo de algoritmo, os roteadores se comunicam trocando informações sobre distância das rotas com roteadores vizinhos. A distância pode ser medida em hops (saltos), comprimento de fila ou latência das repostas. A escolha de uma ou outra depende da unidade 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	A	I	H	K	Nova estimativa de atraso a partir de J	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 atraso é **8**	JI atraso é **10**	JH atraso é **12**	JK atraso é **6**	Nova tabela de repasse para J	

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.

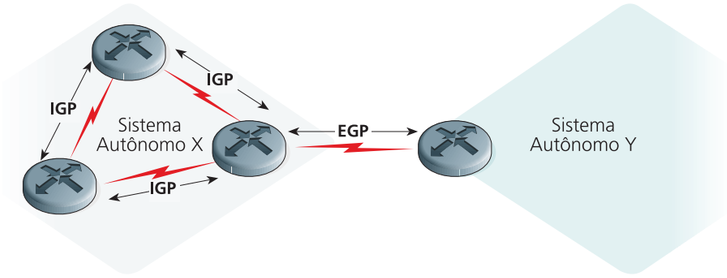


Figura 151
Protocolo EGP.

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).

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.

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.

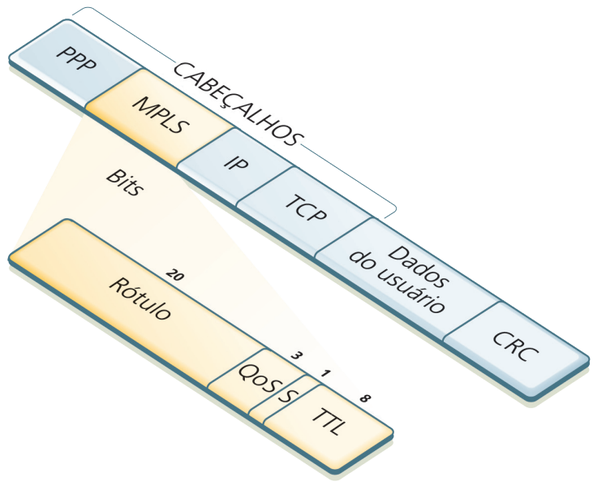
As conversões necessárias podem ser implementadas em várias camadas. Fisicamente as redes podem se conectar por switches e HUBS. Na camada de enlace, podem ser feitas com pontes e switches analisando endereços MAC e fazendo a conversão dos quadros entre, por exemplo, Ethernet e 802.11. Na camada de transporte 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

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).

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).

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

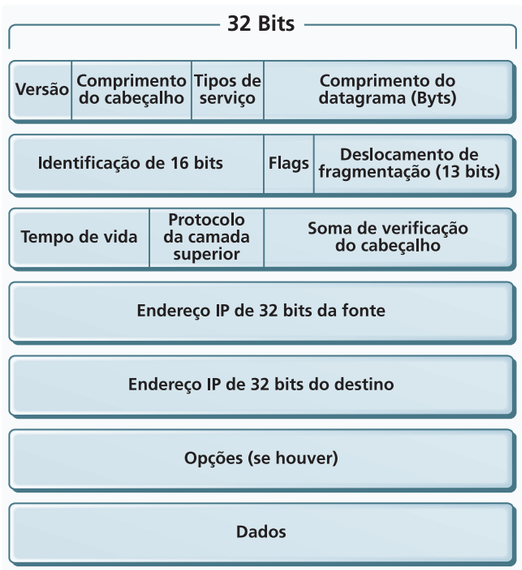
A internet é uma rede de datagramas e o centro de sua arquitetura se enquadra na camada de rede do modelo OSI (Open System Interconnection ou Sistema Aberto de Interconexão). Essa implementação utiliza o protocolo IP como forma de identificar um host e também a origem e o destino dos pacotes. Para controlar 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):** utlizado 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.

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.

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.

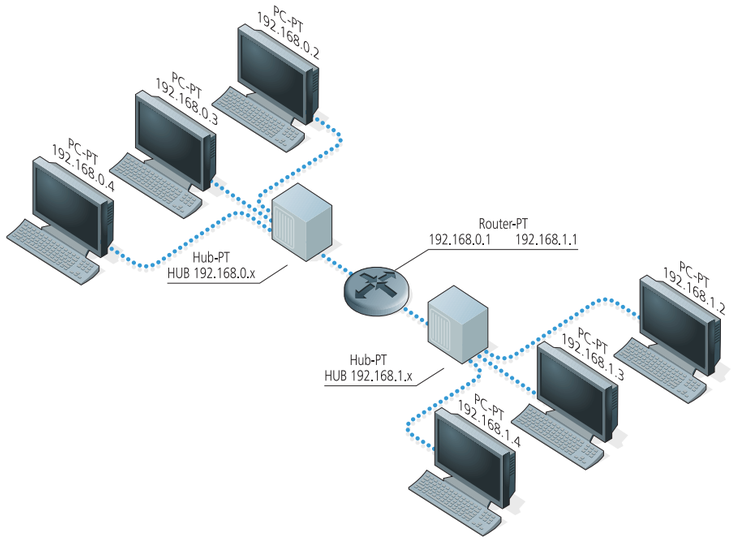
20.3.3.11. Sub-redes

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-

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 trafegarão 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:

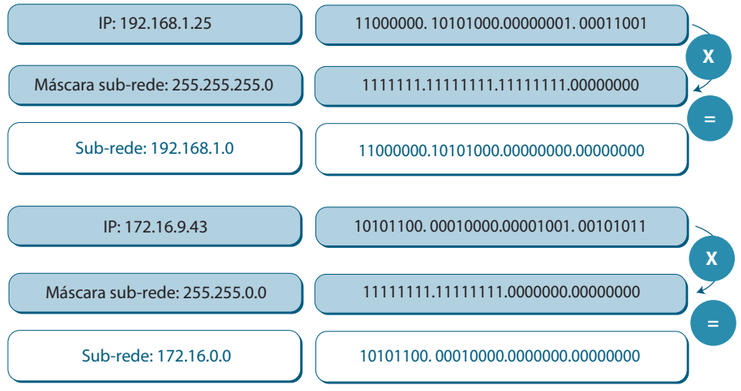


Figura 155
Para multiplicar em binário, fazemos operação bit a bit. 1 x 0 = 0 e 1 x 1 = 1.

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).

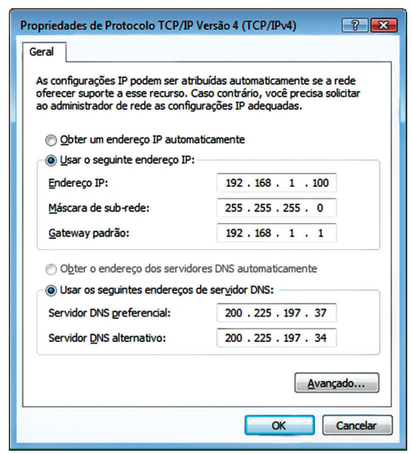
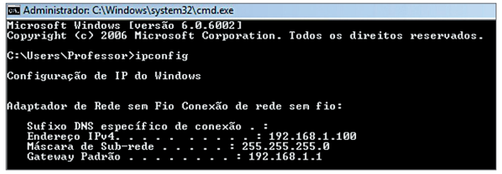


Figura 156
Configuração do protocolo IPv4 no Windows Vista.

Figura 157
No Linux, o comando equivalente é ifconfig.

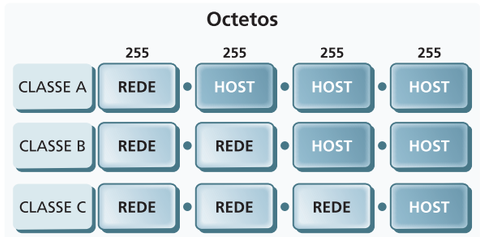


20.3.3.12. CIDR

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.

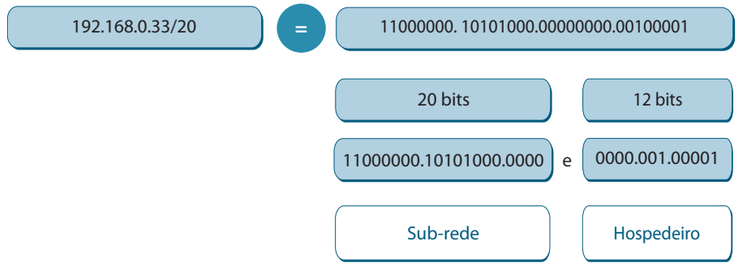


Em um número IP visto da forma decimal, podemos identificar sua classe a partir do número da primeira posição.

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 prestes 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 utililizada 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

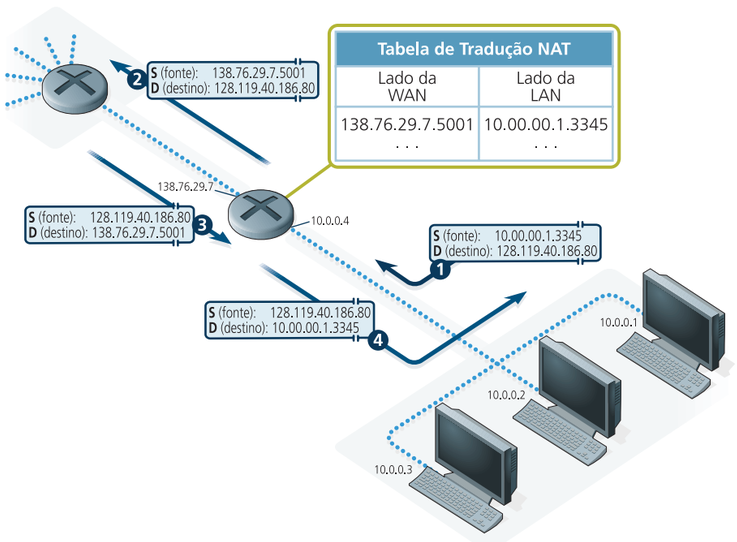
sempre mudando de redes, como notebooks e PDAs em redes sem fio. É um mecanismo adotado também em Internet Service Provider ou Provedores de Serviços de Internet (ISP), que têm uma faixa de IP para distribuir a seus clientes e precisam redistribuir endereços constantemente, já que os clientes se conectam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

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.

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

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.

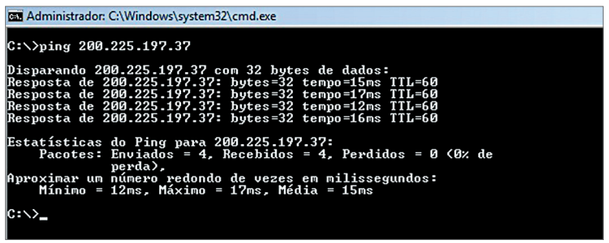


Figura 161
O comando ping utiliza icmp.

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

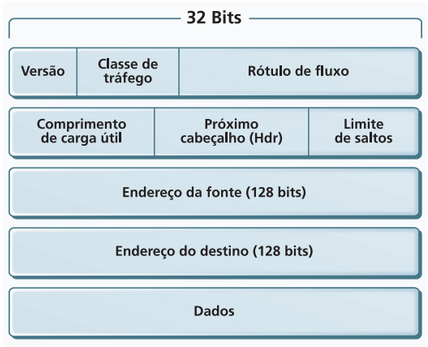
Durante muito tempo, o IPv4 mostrou-se competente na função de endereçar as redes de datagramas, sem a necessidade de uma forma mais simples de configurar o endereçamento para aparelhos móveis que estão dentro de uma rede apenas por pouco tempo. Porém, o aumento da demanda por endereços IP fez com que 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.

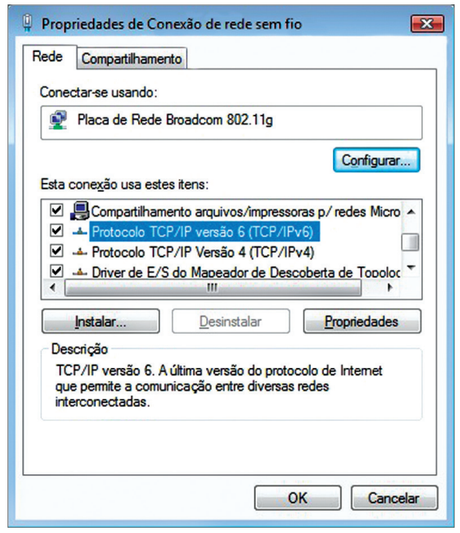


Figura 163
Tela de configuração de Redes do Windows Vista.

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.

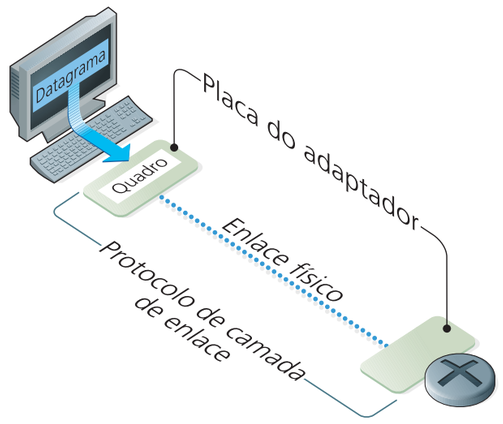
20.3.3.18.1. Serviços oferecidos pela camada de enlace

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

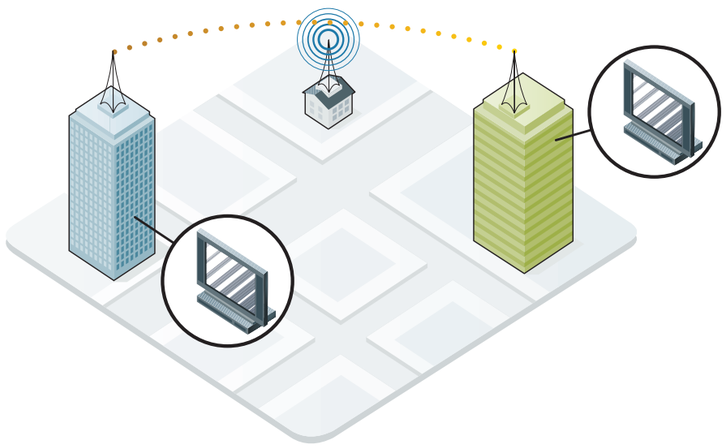


Figura 165
Interferências externas (ondas, por exemplo) podem alterar os dados.

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 Mpbs para que a comunicação seja possível.

20.3.3.18.2. Subcamadas

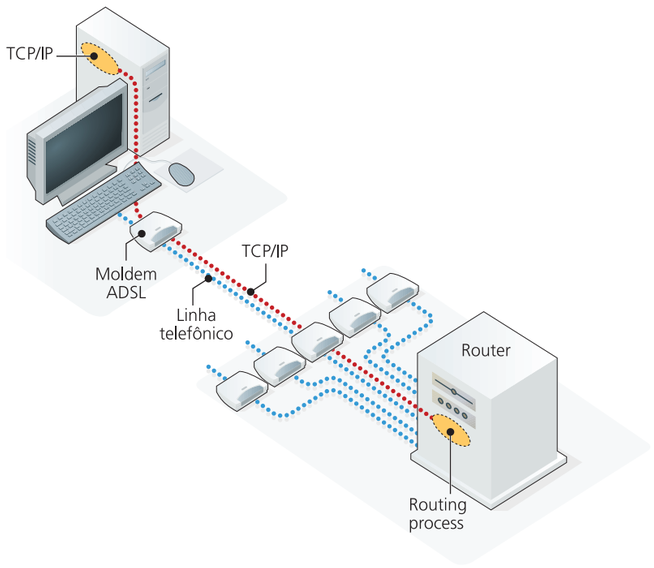
Uma das funções mais importantes da camada de enlace é fazer com que vários nós da rede sejam capazes de acessar o mesmo meio físico de transmissão, de forma compartilhada. Para fazer esse controle, a camada é dividida em dois subgrupos de protocolos ou subcamadas: o LLC (Logic Link Layer) e o MAC (Media 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.

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)

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).

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 –Assymmetric 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.

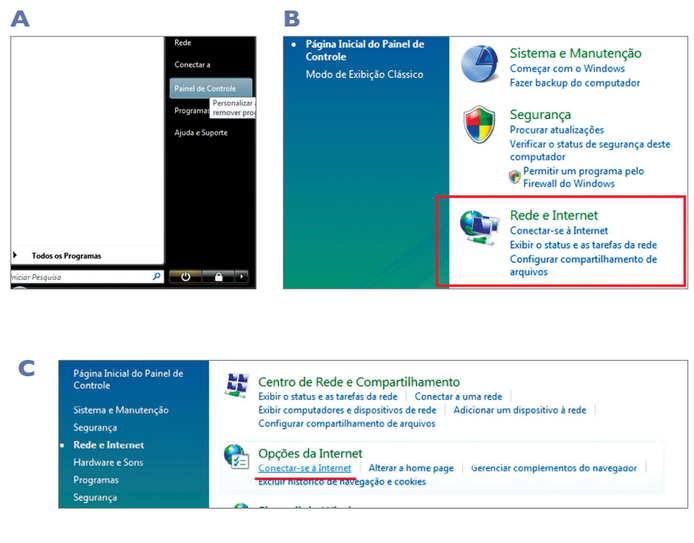
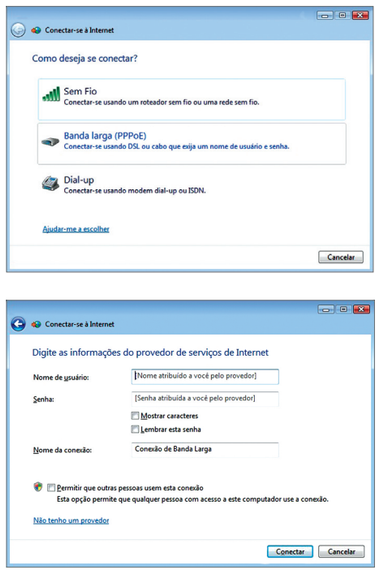


Figura 167
Configurando a ADSL de forma clássica.

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).

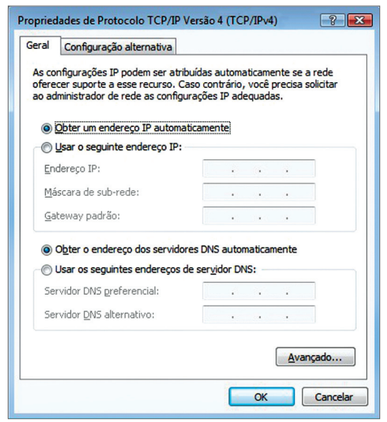


Figura 169
Configuração IP para utilizar DHCP.

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.

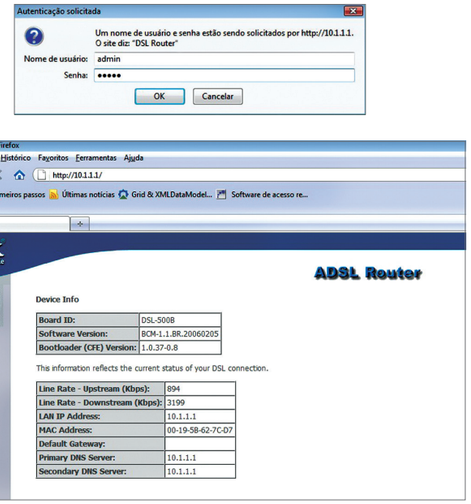
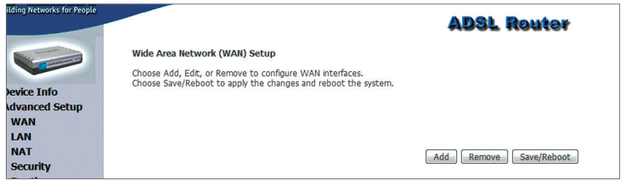


Figura 170
Autenticação no sistema de configuração do ADSL Router.

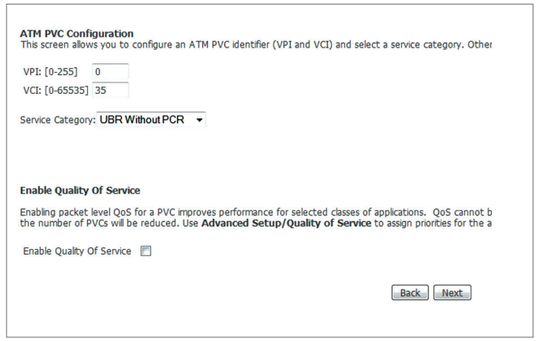
3. Nesse caso, estamos utilizando o modem ADSL Router DSL-500B da D-Link. Para acessar a configuração da conexão, devemos clicar no link "Advanced Setup" e, dentro dele, em "WAN". Depois, no botão "Add" para adicionar uma nova conexão (figura 171).

Figura 171
Configuração da interface WAM.



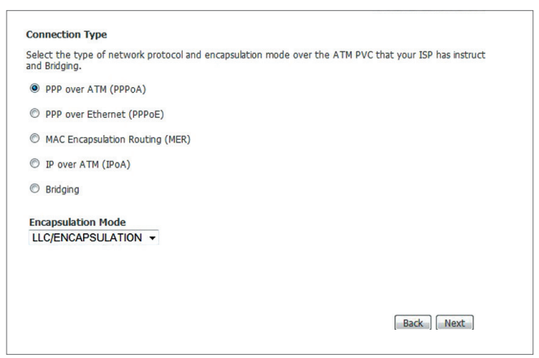
4. Configure o identificador VPI e VCI da ATM de sua operadora (figura 172). Geralmente, quando esses modems são adquiridos pela própria operadora, os valores vêm preenchidos corretamente. Quando isso não acontece, é aconselhável se informar no suporte telefônico da operadora de telefonia.

Figura 172
Configuração ATM.



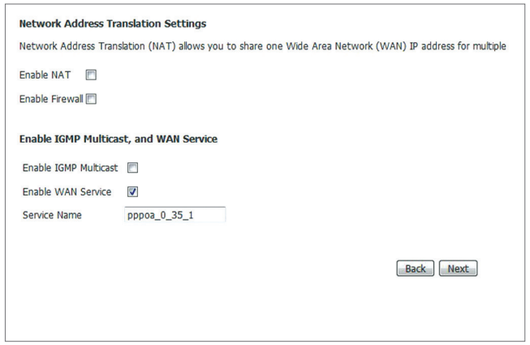
5. Escolha PPPoA e o tipo de encapsulamento utilizado por sua operadora de telefonia. Mas lembre-se de que vale a mesma regra em relação ao local de origem do modem. Para facilitar a instalação no local onde está o usuário, as empresas que fornecem serviço de banda-larga distribuem os modems com os padrões pré-configurados (figura 173).

Figura 173
Escolhendo o PPoA e o encapsulamento.



6. Entre com o usuário e a senha e clique em "Next".

Figura 174
Finalizando o processo.



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.

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.

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.

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.
- **Detecção 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 detecção por intermédio da portadora e transmitem sempre que precisar. Caso haja colisão, transmitem novamente.

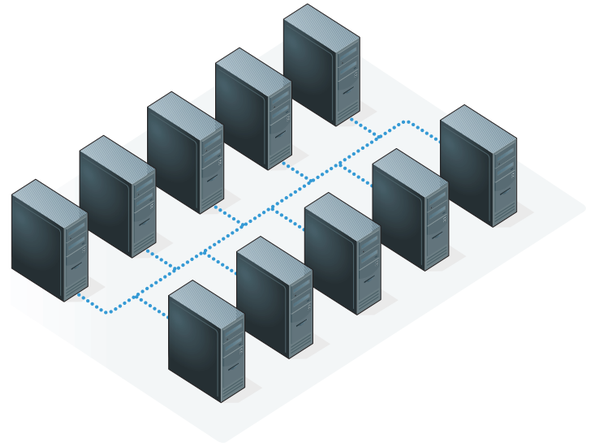


Figura 175
Meio físico compartilhado.

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).

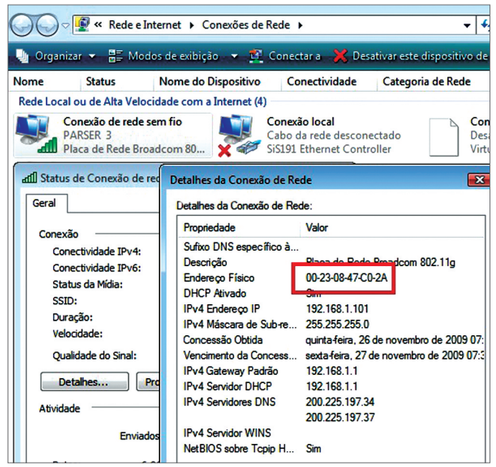
Outra técnica é FDM (Frequency Division Multiplexing ou Multiplexação Dividida por Frequência). Nesse caso, o canal é dividido em frequências diferentes, que não interferem umas nas outras e podem ser transmitidas ao mesmo tempo. É semelhante às rádios AM/FM, que transmitem pelo ar, porém, cada uma trabalha 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 Equipament 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".

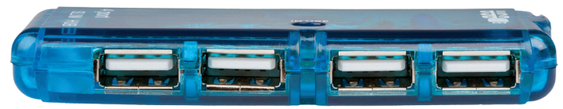
A identificação dos enlaces é feita por meio de endereços MAC, representados pelo número 48 bits escrito normalmente em notação hexadecimal. Esse número é um identificador global, ou seja, não podem existir dois adaptadores de rede com o mesmo número. O fabricante do adaptador de rede é quem atribui 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 GRIFFIN/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.

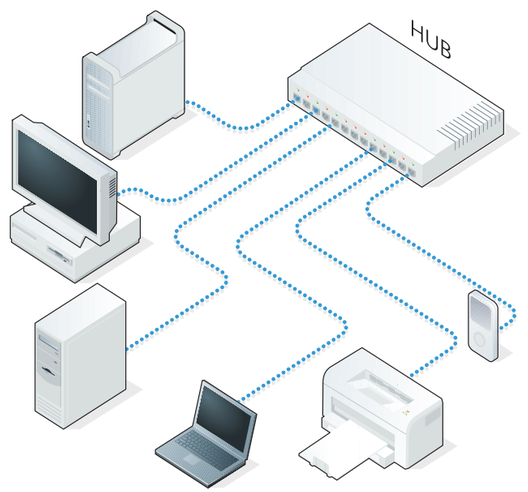


Figura 178
Esquema de interligação com HUB Ethernet.

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

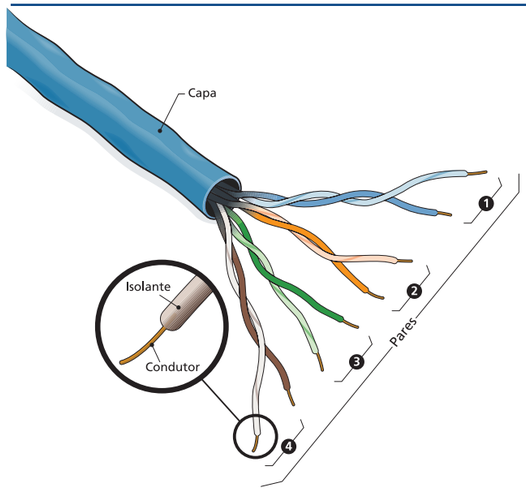


Figura 180
Visão lateral de um cabo UTP categoria 5.

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 Mpbs (FastEthernet) como para Ethernet Gigabits.

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.

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 plásticos 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.

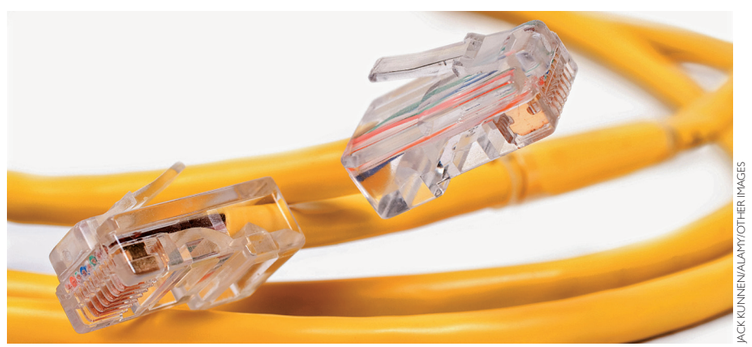
20.3.3.19.3.1.1. Normas de montagem

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.

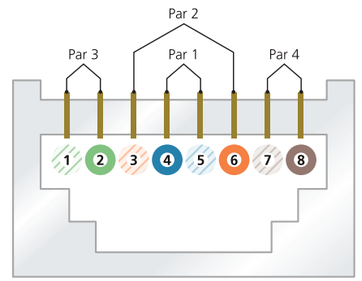
O processo de montagem de um cabo é chamado de crimpagem. A norma da **ABNT** NBR 14565:2000 padroniza dois tipos de disposição dos fios na crimpagem dos conectores dos cabos: a EIA/TIA T568A e a T568B. Essa norma foi atualizada na revisão de 2006, com a inclusão do padrão EIA/TIA 568-C para as redes 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 Datagram Protocol ou Protocolo de Datagrama de Usuário): T568A e T568B

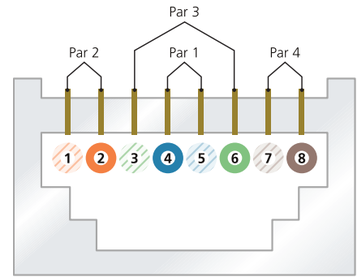
Figura 181
Conector RJ45.



JACK KUNNEN/ALAMY/OTHER IMAGES



Ligação do CM8V
(T568A)



Ligação do CM8V
(T568B)

Figura 182
Padrão de ligação do 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 cascateamento de HUB (um HUB ligado ao outro), ligar switchs, 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.

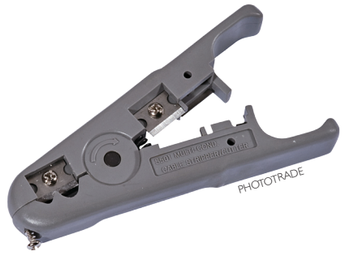
20.3.3.19.3.1.2. Ferramentas

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

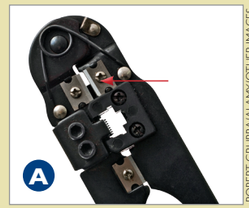
Com o cabo já preparado, podemos inserir os fios no conector, sempre com a parte lisa para cima e a trava para baixo. Assim, é possível ver os fios entrando nos seus devidos condutores (figura G).

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.

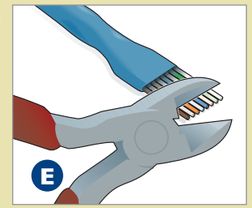
4. Crimpagem

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.

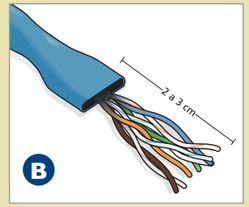


Identificando as lâminas de decapagem do cabo.

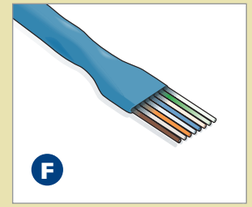


ROBERT GRUBBA/ALAMY/OTHER IMAGES

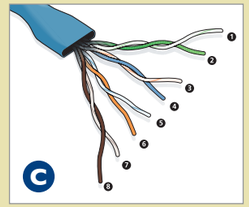
Corte de fios para alinhar o comprimento.



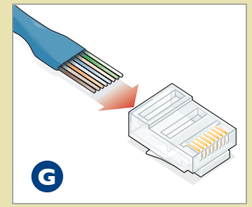
Cabo depois de decapado.



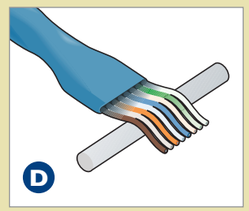
Fios prontos para crimpar.



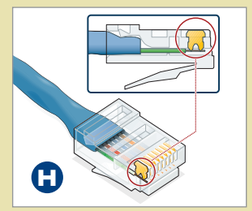
Fios bem separados e retos.



Fios sendo inseridos corretamente no conector RJ45.

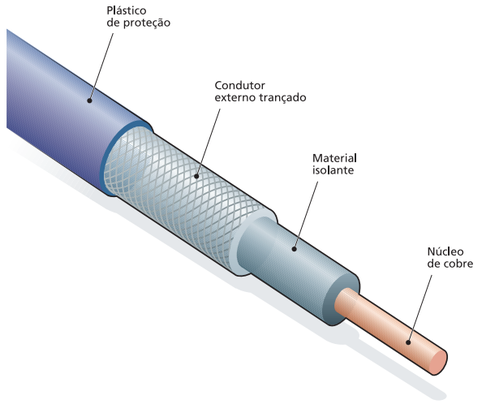


Fios sendo endireitados e posicionados um ao lado do outro.



Na crimpagem, os conectores "vampiros" se inserem nos fios e o ressalto pressiona o cabo para fixação.

Figura 186
Partes de um cabo coaxial.



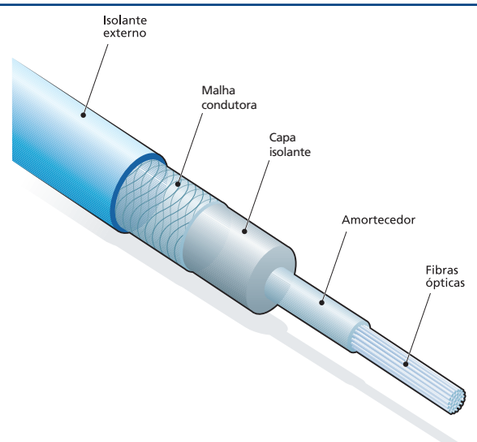
20.3.3.19.3.2 Cabo coaxial

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.

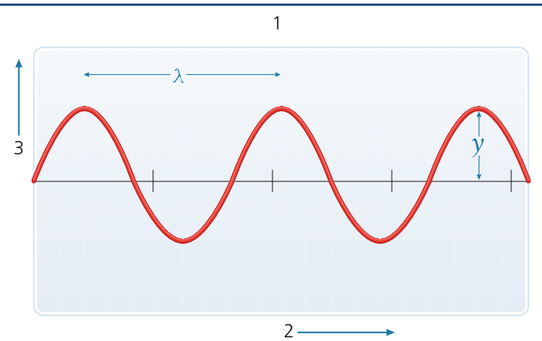
Cada uma das fibras de vidro existentes no centro do cabo possui a espessura de um fio de cabelo. O feixe de fibras é revestido por uma "casca", também feita de material condutor (dielétrico), que atua como se fosse um espelho, mantendo a luz presa no núcleo. Sobre essa casca há uma camada plástica protetora. 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

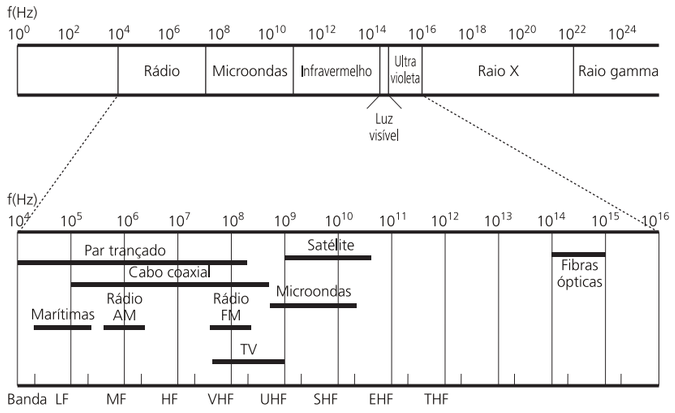
Quando um elétron se move, ele produz um espectro que pode ser transmitido por fios de cobre, por luz, pelo ar e até mesmo através do vácuo. Esse espectro oscila formando ondas. A distância entre as cristas dessas ondas é chamada de frequência.

Figura 188
Descrição de onda.



1 - Elementos de uma onda
2 - Distância
3 - Deslocamento
λ - Comprimento de onda
γ - Amplitude

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.

Figura 190
Símbolos comerciais do WiFi e Bluetooth.

- 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.

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. 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, de**zembro 2009.

IETF - Internet Engineering Task Force. (01 07 1998 r.). *IP Version 6 Addressing Architecture*. Disponível em: <http://www.ietf.org/rfc/rfc2373.tx> 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 Especification. 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 DO GOVERNO DE SÃO PAULO
GOVERNO DE SÃO PAULO
CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA 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.

Fundação
Padre Anchieta