Colégio Salesiano de Lins

"Dom Henrique Mourão"

Técnico em Desenvolvimento de Sistemas para WEB

www.projetoderedes.kit.net

Prof.: Alexandre Ponce de Oliveira

Redes de Computadores

2002

Sumário

REDES DE COMPUTADORES

1. TCP/IP

O protocolo TCP/IP é o protocolo mais usado atualmente nas redes locais, isso graças a Internet, pois ela utiliza esse tipo de protocolo, praticamente obrigando todos os fabricantes de sistemas operacionais de redes a suportarem esse protocolo.

Uma das grandes vantagens desse protocolo é a possibilidade de ele ser roteável, ou seja ele foi desenvolvido para redes de grande tamanho, permitindo que os dados possam seguir vários caminhos distintos até o seu destinatário.

Na verdade o TCP/IP é um conjunto de protocolos no qual os mais conhecidos dão o nome a esse conjunto: TCP (Transport Control Protocol) e o IP (Internet Protocol).

1.1. O modelo TCP/IP

A arquitetura do TCP/IP é desenvolvida em 4 camadas que são: Aplicação, Transporte, Internet, Interface de rede.

1.1.1. Camada de Aplicação

Corresponde as camadas 5, 6 e 7 do modelo OSI e faz a comunicação entre os aplicativos e o protocolo de transporte. Entre os principais protocolos que operam nesta camada destacam-se o HTTP (Hyper Text Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol) e o Telnet.

A camada de aplicação comunica-se com a camada de transporte através de uma porta. As portas são numeradas e as aplicações padrão usam sempre uma mesma porta. Por exemplo, o protocolo SMTP utiliza sempre a porta 25, o HTTP a porta 80 e o FTP as portas 20 (para transmissão de dados) e 21 (para transmissão de informações de controle). Através das portas é possível saber para qual protocolo vai estar sendo enviados os dados para uma determinada aplicação. Vale saber que é possível configurar cada porta de cada aplicação.

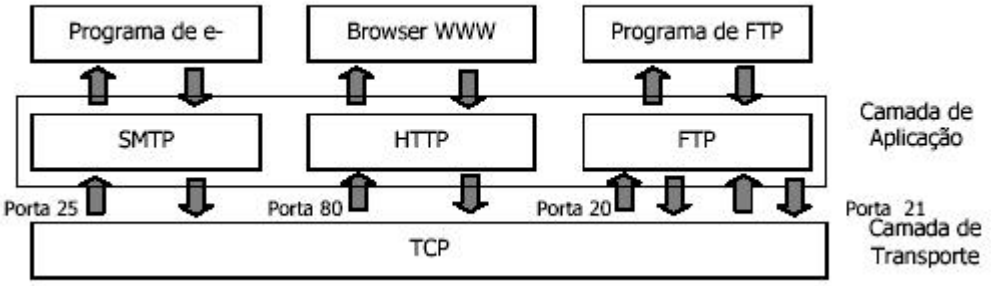


Figura 1.1 - **Funcionamento da camada de aplicação**

1.1.2. Camada de Transporte

É a camada que eqüivale a camada de transporte do modelo OSI. Esta camada é responsável por pegar os dados enviados pela camada de aplicação e transformá-los em pacotes, a serem repassados para a camada de Internet. Ela utiliza uma forma de multiplexação, onde é possível transmitir simultaneamente dados de diferentes aplicações.

Nesta camada operam dois protocolos: o TCP (Transport Control Protocol) e o UDP (User Datagrama Protocol). Ao contrário do TCP, este segundo protocolo não verifica se o dado chegou ao seu destino, já o TCP para todo pacote enviado sempre há uma confirmação se este chegou ou não.

1.1.3. Camada de Internet

É a camada correspondente no modelo OSI a camada de redes. Existem vários protocolos que podem operar nesta camada: IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol).

Na transmissão de um dado de programa, o pacote de dados recebido da camada TCP é dividido em pacotes chamados *datagramas,* que são enviados para a camada de interface com a rede, onde são transmitidos pelo cabeanento da rede através de quadros.

Essa camada é responsável pelo roteamento de pacotes, isto é, adiciona ao datagrama informações sobre o caminho que ele deverá percorrer.

1.1.4. Camada de Rede

Corresponde as camadas 1 e 2 do modelo 051, é responsável por enviar o datagrama recebido pela camada de Internet em forma de quadro através da rede.

1.2. O Protocolo IP (Endereçamento IP)

O protocolo TCP/IP foi desenvolvido com a intenção de permitir o roteamento de pacotes, e graças a essa característica é possível fazer a interligação de diversas redes (como é o caso da Internet). Para permitir o roteamento ele utiliza um esquema de endereçamento lógico denominado IP (para redes de computadores existem dois tipos de endereçamento: ***físico,*** que vem impresso nas placas de rede e o ***lógico*** que é configurado pelo usuário com um endereço IP).

Em uma rede TCP/IP cada dispositivo conectado a rede deve ter pelo menos um endereço IP, isso permite identificar o dispositivo na rede a qual ele pertence. Observe a figura 1.2 abaixo

Figura 1.2 — Esquema entre redes e roteadores.

Neste exemplo existem três redes distintas (Rede A, B, C) onde cada uma tem seu próprio fluxo de comunicação interno. As redes são interligadas através de um dispositivo chamado *roteador.* O Roteador isola o fluxo das redes só permitindo que dados atravessem por ele se esses dados se destinarem a uma rede externa.

Supondo que um computador da rede A queira enviar pacotes de dados a um computador da rede B, este envia os dados ao Roteador 1 e o Roteador 1 encaminha os dados ao seu destinatário na rede B. No caso de um computador da rede 1 querer enviar os dados para um computador da rede 3, ele envia o pacote ao Roteador 1, que então repassará esse pacote diretamente para o Roteador 2, que se encarregará de entregar esse pacote ao computador de destino.

Esse tipo de entrega de pacotes é feito facilmente pelo roteador porque o pacote de dados tem o endereço (IP) da máquina de destino. Quando um roteador recebe um pacote que não pertence a rede interna ele redireciona este pacote para uma outra rede que possa estar interligada a ele. E assim que as redes baseadas no protocolo TCP/IP funcionam. Elas têm um ponto de saida da rede *(gateway)* onde todos os pacotes que não pertencem aquela rede são encaminhados, as redes subsequentes vão enviando os pacotes aos seus *gateways* até que o pacote atinja a rede de destino.

Um endereço IP é constituído de 4 bytes (32 bits) representados na forma decimal, e separados por ponto, no formato X.Y.Z.W. Assim o menor número do endereço IP possível é 0.0.0.0 e o maior é 255.255.255.255.

Como cada dispositivo de uma rede TCP/IP precisa ter um endereço IP único, para que o pacote de dados consiga ser entregue corretamente, você terá que usar um endereço que não esteja sendo utilizado por nenhum outro computador da rede. Para facilitar a distribuição dos endereços IP, foram especificadas cinco classes de endereços IP, como mostra a tabela:

Classe	Bit de identificação	Endereço mais baixo (decimal)	Endereço mais Alto (decimal)
A	0xxxxxxx.xxxxxxx.xxxxxxxx	1.0.0.0	126.0.0.0
B	10xxxxxx.xxxxxxx.xxxxxxxx	128.1.0.0	191.255.0.0
C	110xxxxx.xxxxxxx.xxxxxxxx	192.0.1.0	223.255.255.0
D	1110xxxx.xxxxxxx.xxxxxxxx	224.0.0.0	239.255.255.255
E	1111xxxx.xxxxxxx.xxxxxxxx	240.0.0.0	255.255.255.254

Em redes usamos somente os endereços IP das classes A, B e C, com as seguintes características de cada uma delas:

- **Classe A:** O primeiro número identifica a rede, os demais três números indicam a máquina. Cada endereço classe A consegue endereçar até 16.777.216 máquinas.
- **Classe B:** Os dois primeiros números identificam a rede, os dois demais identificam a máquina. Esse tipo de endereço consegue endereçar até 65.536 maquinas em uma rede.
- **Classe C:** Os três primeiros números identificam a rede, o último indica a máquina. Com isso consegue-se endereçar até 256 máquinas.

Para entendermos melhor, vejamos um exemplo de rede classe C. Nesse tipo de rede, onde os três primeiros dígitos identificam a rede, você poderá conectar até 256 máquinas na mesma rede (0 a 255), na verdade serão 254 pois os endereços O (identifica a rede) e 255 (identifica os computadores) são endereços especiais que serão discutidos posteriormente. A realidade é que o tipo da classe de rede a ser usada vai depender da quantidade de máquinas que serão conectadas a sua rede.

O sistema de redes que forma a estrutura da Internet é chamado *backbone.* Para que sua rede possa se conectar a Internet, ela deverá estar conectada ao backbone e alguma forma, seja diretamente ou indiretamente, através de uma rede que esteja conectada ao backbone. No Brasil, um dos backbones existentes é o da Embratel. Dessa forma, se você quiser que sua rede esteja conectada à Internet, ela deverá estar conectada de alguma forma ao backbone da Embratel.

Na Internet o responsável pelo fornecimento dos endereços IPs são os backbones. Eles é quem distribuem os números IPs válidos para a Internet. Essa estrutura de distribuição funciona de uma forma hierárquica.

Em princípio, se a sua rede não for estar conectada a Internet, você pode definir qualquer endereço IP para os dispositivos que estiverem conectados a ela. O Problema é que mais cedo ou mais tarde surgirá a necessidade de se conectar a Internet e o conflito com endereços IP reais será inevitável, caso você tenha montado uma rede com endereços IPs já existentes. Para evitar tal aborrecimento, existem endereços especiais que servem para a configuração de uma rede local, sem a necessidade de se utilizar endereços IPs reais. Esses endereços são reservados para redes privadas e são os seguintes:

- **Classe A:** 10.0.0.0 a 10.255.255.255
- **Classe B:** 172.16.0.0 a 172.31.255.255
- **Classe C:** 192.168.0.0 a 192.168.255.255.

Para se criar uma rede privada é aconselhado o uso de tais endereços, a não ser que haja uma certeza de que tal rede nunca será conectada a Internet. Na figura abaixo tem-se uma rede IP configurada com o endereço reservado 192.168.100.0.

O endereço “0” indica rede. Assim o endereço de rede 192.168.100.0 indica a rede que usa

endereços que comecem por 192.168.100, e que o último byte é usado para identificar as máquinas na rede. Já o endereço 10.0.0.0 indica que os três últimos bytes identificam o computador na rede.

Já o endereço “255” é reservado para *broadcast,* o ato de enviar um mesmo pacote de dados para mais de uma máquina ao mesmo tempo. Neste caso, a rede envia o mesmo pacote de dados para todos os computadores da rede.

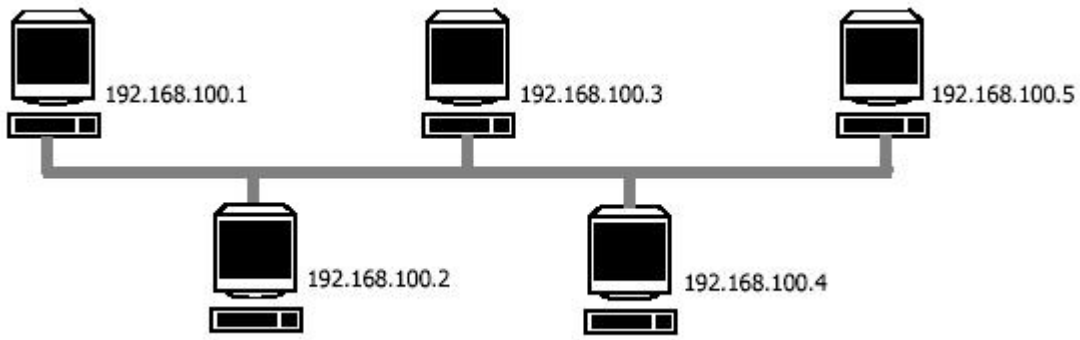


Figura 1.3 — Endereçamento IP em uma rede proprietária.

Para podermos conectarmos na Internet com a rede acima, duas ações podem ser tomadas. Uma seria conseguir uma faixa de IP de uma classe C e reconfigurar todos os endereços IPs das máquinas. Como essa situação é pouco provável, pois esses endereços são geralmente disponibilizados para provedores de Internet, uma outra solução seria obter apenas um endereço de IP real e usar um gateway (roteador) para disponibilizar o acesso a rede externa (Internet). Com o gateway é possível fazer a comunicação com a Internet sem a necessidade de alterar toda a configuração da rede. Observe a figura 1.4:

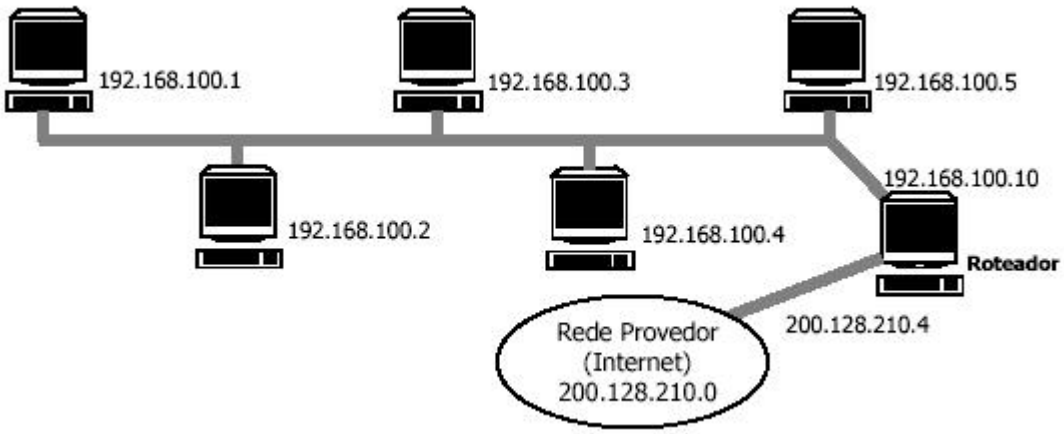


Figura 1.4 — Endereçamento IP em uma rede proprietária com conexão a Internet.

Na figura 4.4 fica clara a presença do roteador. Ele atua entre as duas redes permitindo que o trafego da rede local (192.168.100.0) não interfira no trafego da Internet. O roteador possui duas

interfaces de rede uma para a rede local e outra para a Internet, e cada uma dessas interfaces deve ser configurada para que ambas as redes possam acessá-las. A interface para a rede local é o IP 192.168.100.100, que é configurado pelo administrador da rede. Já a interface 200.128.210.4 é um endereço IP disponibilizado pelo provedor de Internet que a rede esta ligada.

A comunicação da rede local com a Internet acontece da seguinte forma. O computador 192.168.100.3 solicita uma página na www (www.salesianolins.br). Essa solicitação percorre toda a rede chegando ao roteador, que percebe que essa solicitação não pertence a essa rede. Isso é possível graças a tabela de endereços existente no roteador. Toda página www tem um endereço IP que é traduzido para um nome (veremos isso mais a frente ao falarmos sobre DNS). Como o roteador percebe que aquele endereço não pertence aquela rede, ele encaminha solicitação para a próxima rede, e assim sucessivamente até que se encontre o seu destino (ou não).

A solicitação feita pelo computador 192.168.100.3 fica guardada no roteador até se obter uma resposta de confirmação (positiva ou negativa). Quando essa resposta chega ela é encaminhada para o seu solicitante (no caso o IP 192.168.100.3).

Existem duas formas do roteador armazenar a tabela, uma estática e outra dinâmica. Na estática o roteador tem todos os endereçamentos IPs da rede já determinados, na dinâmica os endereços IPs são determinados conforme se necessita de um.

No caso do endereçamento dinâmico, utiliza-se um protocolo chamado DHCP (Dynamic Host Configuration Protocol - Protocolo de Configuração Dinâmica de Máquina), dessa forma, toda vez que um cliente solicitar um endereço IP, o servidor DHCP disponibilizará para ele um endereço válido que não esteja sendo utilizado naquele momento, e assim que o cliente finalizar o seu uso ele libera o endereço IP

1.2.1. Máscara de Rede

Um termo que você encontrará com bastante freqüência ao configurar uma rede. A mascara de rede é um endereço de 4 bytes (32 bits), no mesmo padrão do IP, onde cada bit 1 representa a parte do endereço IP que identificará a rede e o bit 0 informa a parte do endereço IP que será usado para configurar o endereçamento da máquina. As mascaras de rede padrão são:

- Classe A: 255.0.0.0
- Classe B: 255.255.0.0
- Classe C: 255.255.255.0.

Quando desejamos fragmentar uma rede em mais segmentos usamos a mascara fora do padrão, conforme a necessidade. Por exemplo temos um endereço de rede classe C (200.123.147.0), podemos fragmentá-los em 4 subredes distintas, veja as especificações:

- Rede 1: 31 endereços IP variando de 200.123.147.1 até 200.123.147.31, utilizamos uma mascara igual a 255.255.255.224 (se subtrairmos 224 de 255 temos 31 endereços válidos);
- Rede 2: 31 endereços IP variando de 200.123.147.32 até 200.123.147.63, utilizamos uma mascara igual a 255.255.255.224;

- Rede 3: 64 endereços IP variando de 200.123.147.64 ate 200.123.147.127, utilizamos uma mascara igual a 255.255.255.192;
- Rede 4: 127 endereços IP variando de 200.123.147.128 ate 200.123.147.254, utilizamos uma mascara igual a 255.255.255.128;

O valor da mascara é a diferença entre 256 e o número disponível na sub-rede em questão. Quando criamos uma subrede podemos isolar o fluxo de comunicação entre as redes através dos roteadores.

1.3. Reconhecendo um endereço IP

Como foi visto, redes TCP/IP utilizam-se de endereços virtuais. Cada placa de rede tem um endereço físico único gravado na própria placa. Para enviarmos uma mensagem pela rede precisamos conhecer o endereço virtual (IP) da máquina destinatária. Como fazer para associar um endereço físico a um endereço virtual ?

Para fazer essa associação existe o protocolo ARP (Adress Resolution Protocol). Ele funciona mandando uma mensagem broadcast para a rede perguntando, a todas as máquinas, qual responde pelo endereço IP do destinatário. Então a máquina destinatária responde e informa o seu endereço de placa de rede (MAC) permitindo a transmissão de dados entre as duas máquinas. Para não ter que ficar enviando toda vez uma mensagem broadcast pela rede, o dispositivo transmissor armazena o ultimo endereço IP recentemente acessado e o endereço MAC correspondente a cada IP. Podemos fazer um teste no DOS, para isso basta usar o comando *arp -a* e ele te relacionará o ultimo endereço IP e o respectivo endereço MAC daquele IP.

Existe um protocolo que permite descobrir um endereço IP através de um endereço físico, é o protocolo RARP (Reverse Address Resolution Protocol). Esse protocolo faz o processo inverso ao ARP.

1.4. O Protocolo TCP (Transmissão de dados)

O Protocolo TCP (Transport Control Protocol) é o responsável pelo controle do fluxo de dados na rede, já que “faz” o transporte dos dados. Ele recebe os dados vindos da camada de rede (IP) e os coloca em ordem, verificando se todos chegaram corretamente. Como já foi falado as aplicações enviam dados a serem transmitidos pela rede ao protocolo TCP, através de canais virtuais de comunicação, chamados de *portas.* As portas mais usadas (e mais conhecidas) estão listadas na tabela abaixo:

Porta	Aplicação
15	Netstat
20	FTP (Dados)
21	FTP (Controle)
23	Telnet

25	SMTP
43	Whois
80	HTTP

O protocolo TCP é endereçado pelo número de IP e o número da porta, dessa forma é que as aplicações podem conversar de forma simultânea (na camada de transporte) sem que os dados sejam trocados entre as aplicações.

Ao receber um pacote de dados, o protocolo TCP envia uma mensagem de confirmação de recebimento à máquina transmissora, chamada *acknowledge* ou simplesmente ack. Caso essa confirmação não chegue ao transmissor após um intervalo de tempo, determinado, esses dados serão retransmitidos pelo protocolo TCP.

1.4.1. Conexão

A comunicação entre duas diferentes máquinas é chamada de conexão. O protocolo TCP é responsável por abrir, manter e fechar as conexões entre as máquinas.

Para estabelecer uma conexão, o transmissor envia um pacote de dados avisando que ele quer estabelecer uma conexão. O receptor pega esses dados e confirma a conexão com um outro pacote de dados, que ao chegar ao transmissor estabelece a conexão confirmando o recebimento do pacote.

A conexão é mantida através do envio de dados do transmissor ao receptor. A finalização da conexão ocorre da mesma forma que o seu estabelecimento.

1.4.2. Socket

A transmissão de dados no protocolo TCP acontece usando o conceito de portas. Assim quando o TCP recebe um pacote destinado a porta 80, ele sabe que deve entregar aqueles dados ao protocolo HTTP (que por sua vez os entregará ao browser Internet do usuário). Ou seja, a porta serve para identificar o tipo de aplicação que gerou o pacote e para qual tipo de aplicação os pacotes de dados devem ser entregues.

Pense no seguinte problema. Você está trabalhando com um browser e resolve abrir uma nova janela (algo muito comum por sinal), como o protocolo TCP saberá a qual das janelas ele deve entregar um pacote de dados solicitado por uma das janelas do browser, já que as duas janelas usam a mesma porta 80 para a mesma aplicação HTTP?

Para resolver esse tipo de problema, o TCP faz o uso do *socket.* O socket define uma conexão dentro de uma porta. Com o uso deste conceito, pode-se ter várias conexões diferentes em uma mesma porta, permitindo o uso da mesma porta por várias janelas da mesma aplicação.

1.5. Protocolos de Aplicação

Existem vários tipos de protocolos de aplicação, mas os mais utilizados e mais comuns são:

- DNS (Domain Name System): Usado para identificar máquinas através de nomes em vez

de IP.

- Telnet: Usado para comunicar-se remotamente com uma máquina.
- FTP (File Transport Protocol): Usado na transferência de arquivos.
- SMTP (Simple Mail Transfer Protocol): Usado no envio e recebimento de e-mails.
- HTTP (Hyper Text Transfer Protocol): Usado na transferência de documentos hipermídia (WWW).

1.5.1. DNS (Domain Name System)

As máquinas na rede TCP/IP são identificadas por meio de um endereço numérico, que não são tão fáceis de serem guardados, por isso foi criado um sistema que permite relacionar endereços IPs a nomes dados as máquinas, esse sistema é chamado de DNS.

Endereços como www.globo.com, na verdade, são uma conversão para a forma nominal de um endereço IP como por exemplo 200.208.9.77. E muito mais fácil guardar um nome como www.globo.com, do que guardar o seu endereço IP.

Quando você entra com um endereço no browser de Internet, o browser se comunica com o servidor DNS que é responsável por descobrir o endereço IP do nome digitado, permitindo que a conexão seja efetuada. O DNS funciona através de uma estrutura hierárquica, como mostra a figura 1.5.

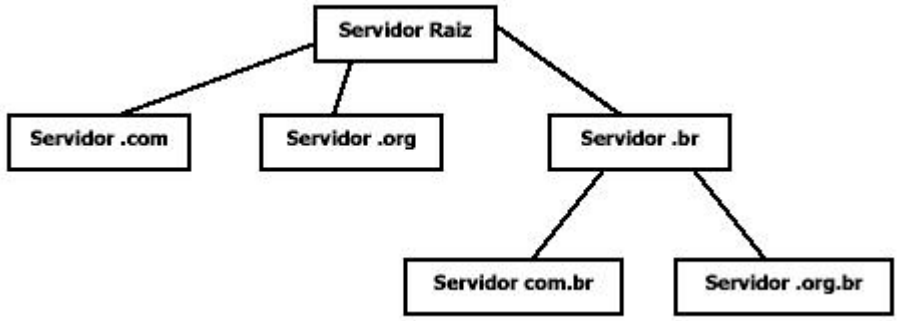


Figura 1.5 — Hierarquia de um sistema DNS

Cada rede local TCP/IP precisa ter ao menos um servidor DNS. Todos os pedidos de conversão de nomes em endereços IP são enviados a este servidor, caso ele não consiga efetuar essa conversão, ele responde o pedido enviando o endereço de um servidor que seja hierarquicamente superior a ele e, com isso, a maior probabilidade de conhecer o endereço solicitado. Uma outra vantagem desse sistema, é que cada vez que um endereço solicitado não pertencente aquele DNS é respondido, o servidor de DNS aprende aquele endereço, tornando o resposta aquela solicitação mais rápida.

1.5.2. Telnet

É um terminal remoto, onde o micro cliente pode fazer um login em um servidor qualquer que esteja conectado à rede (ou a Internet, se a rede estiver conectada a ela). Através do Telnet o usuário

pode manipular o servidor como se ele estivesse sentado em frente a ele, localmente. Tudo aquilo que o usuário fizer no terminal remoto, na verdade ele estará fazendo no servidor, e não no seu computador local.

O seu uso é extremamente simples, basta digitar (no prompt do MS-DOS ou na barra de endereços o número do IP ou o nome do servidor) como mostra a figura 1.6 e 1.7.

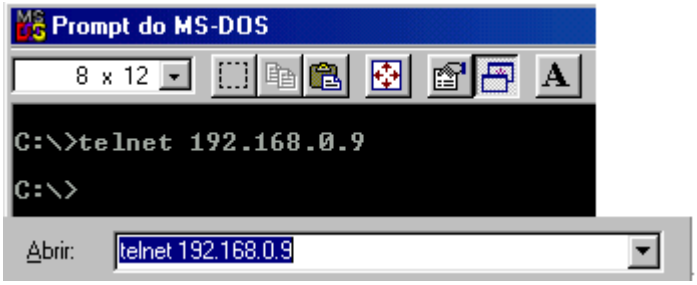


Figura 1.6 — Fazendo a chamada ao Telnet pelo MS-DOS / Executar do Windows

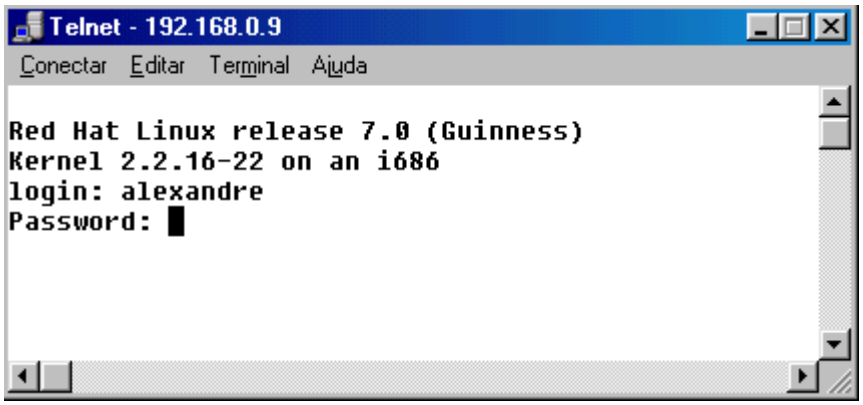


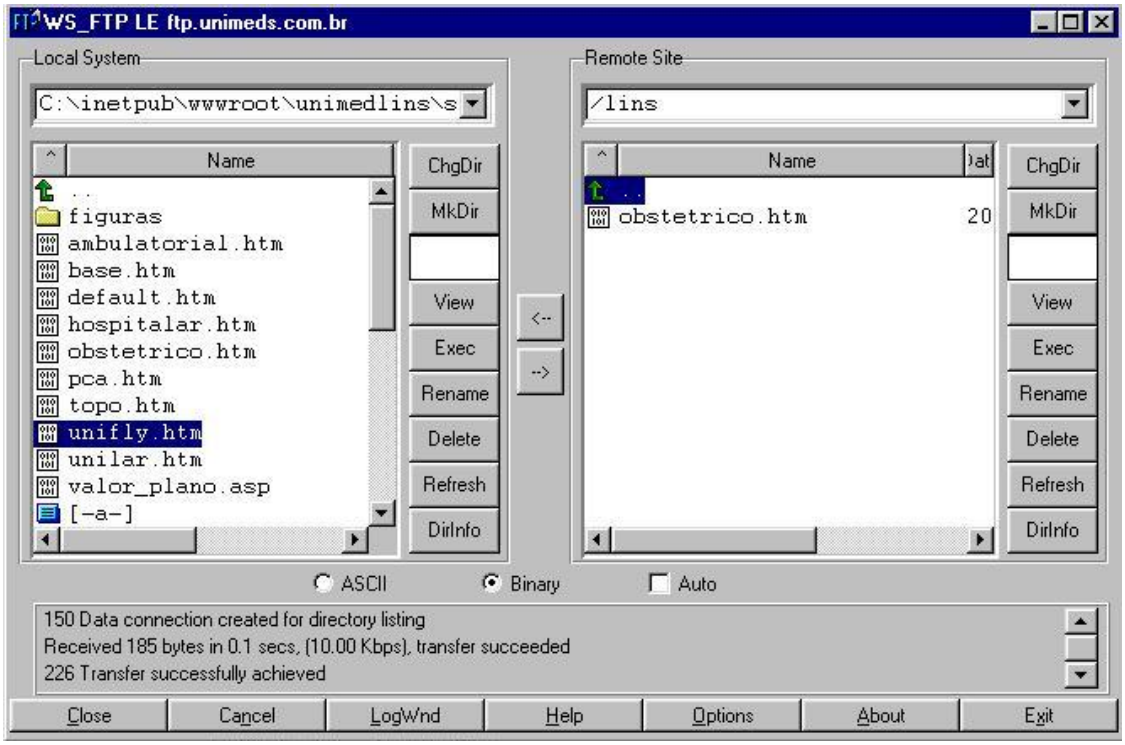
Figura 1.7 — Emulador de Telnet básico do windows.

O Telnet utiliza a porta 23 no protocolo TCP. Existem vários programas que funcionam como emulador do Telnet.

1.5.3. FTP (File Transport Protocol)

É um protocolo usado para a transferência de arquivos. Esse protocolo utiliza duas portas para se comunicar com o TCP: 21, por onde circulam informações de controle (por exemplo, o nome do arquivo a ser transferido) e 20, por onde circulam os dados.

Os micros clientes necessitam de um programa cliente FTP para terem acesso a um servidor FTP. Na conexão é pedido um login e senha. O servidor pode ser configurado para receber conexões anônimas, sem a necessidade de senha, para arquivos que deseje tornar públicos. A figura 1.8 mostra um programa de FTP.



1.5.4. SMTP (Simple Mail Transfer Protocol)

Os e-mails que usualmente trocamos para nos comunicarmos utiliza-se de um protocolo chamado SMTP. A mensagem é enviada pelo usuário para o seu servidor de e-mail, que por sua vez, trata de entregar a mensagem até o destino (muitas vezes utilizando o sistema DNS para descobrir o IP da máquina de destino). Caso o destino não seja alcançado por algum motivo, o servidor armazena a mensagem e tenta uma nova transmissão mais tarde. Se o servidor permanecer inalcançável por muito tempo, o servidor remove a mensagem de sua lista e envia uma mensagem de erro ao remetente.

Além desse existem outros dois protocolos que são muito usados que são o POP3 (Post Office Protocol 3) e o IMAP4 (Internet Message Access Protocol 4) que servem para guardar a mensagem até que o usuário a retire de sua caixa postal e a carregue em seu micro. A figura 1.9 mostra um sistema de comunicação e armazenamento de mensagens usando o SMTP e o POP3 ou IMAP4

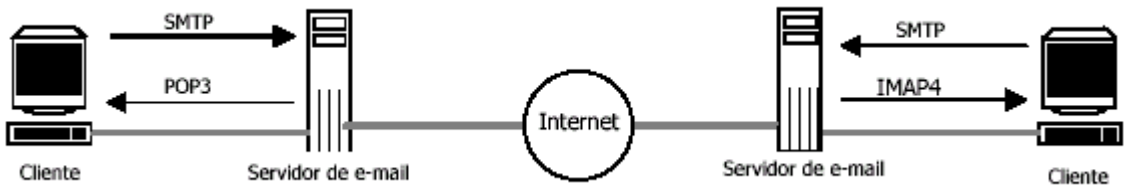


Figura 1.9 — Funcionamento do e-mail.

1.5.5. HTTP (Hyper Text Transfer Protocol)

Esse protocolo é o responsável pelo “boom” da Internet. Um site www consiste de uma série de documentos hipermídia, acessados através de uma URL (Uniform Resource Locator), que é o endereço do site. Quando informamos um site como www.salesianolins.br em um browser, ele irá consultar o servidor DNS para conseguir o endereço IP do servidor www, e com isso iniciar a conexão.

A transmissão dos documentos hipermídia é feita através do protocolo HTTP. Um servidor www hospeda o site, enquanto um cliente (browser) faz a requisição dos documentos lá contidos, essa transferência usa a porta 80 do TCP. Cabe ao browser interpretar o documento, geralmente escrito em HTML.

Outro recurso do HTTP chama-se CGI (Common Gateway Interface), que permite que programas sejam armazenados e executados no próprio servidor www, emitindo uma resposta no formato HTML para ser transmitida para o browser do micro cliente, dessa forma é possível que os documentos sejam criados dinamicamente.

Toda vez que um site é acessado, cópias do documento são criadas no próprio computador, isso é chamado de *cache.* Esse recurso é utilizado pois se o usuário voltar a acessar a mesma página, o browser não precisa buscar os dados diretamente do servidor www, ele busca diretamente no disco rígido do computador, diminuindo assim o tráfego da rede.

Um outro recurso possível é o chamado *proxy,* que permite que uma máquina intermediária entre o cliente e o servidor www funcione como cache. Por exemplo, é possível configurar um servidor proxy em uma rede local para ser usado como intermediário no acesso a Internet. Quando uma máquina faz acesso à Internet, os dados são copiados para o disco rígido do servidor proxy. Com isso, se alguma máquina pedir um documento que já esteja no proxy, não será necessário ir na Internet buscar os dados, basta traze-los do próprio servidor. O único detalhe é que em todos os browser da Internet deverão estar configurados para acessar o servidor proxy.

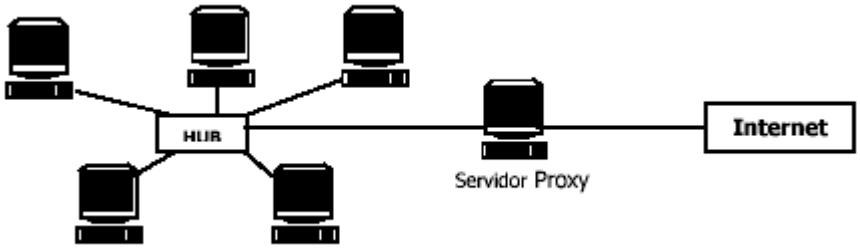


Figura 1.10 — Funcionamento de um servidor proxy

1.6. Outros Protocolos

1.6.1. IPX/SPX

O IPX/SPX é o protocolo criado pela Novell. O funcionamento deste procotolo é muito parecido com o TCP/IP. O IPX (Internet Packet Exchange) é um protocolo que opera na camada de rede, idem ao IP; o SPX (Sequenced Packet Exchange) opera na camada de transporte, equivalendo ao TCP. É um protocolo roteável, podendo operar em redes gigantescas.

O fator que contribuiu para o desaparecimento do IPX/SPX no mercado foi a popularização da Internet que utiliza o protocolo TCP/IP. A versão Netware 4 da Novell passou a permitir o TCP/IP como protocolo de rede.

Uma diferença entre os dois protocolos é o sistema de endereçamento usado pelo IPX, há dois campos : rede de 4 bytes e nó de 6 bytes. No campo nó é atribuído os 6 bytes do endereço MAC da placa de rede, com isso, não é necessário ficar criando, gerenciando e atribuindo endereços IPX para cada micro. Isso torna o protocolo IPX autoconfigurável (plug and play).

O IPX utiliza um esquema chamado número de rede interno (para resolver o problema dos servidores que possuem duas placas de rede) onde o servidor é configurado para divulgar o seu endereço como sendo o endereço de uma rede que não existe, com isso os micros pedirá a para a rede a entrega do datagrama direto ao número de rede interno do servidor, não passando pelo roteador.

O IPX baseia-se em um datagrama que não utiliza sistema para verificar se o dado chegou ou não ao destino. O protocolo de transporte (SPX) que envia pacotes contendo a confirmação de recebimento do pacote.

1.6.1.1. Estrutura do Datagrama IPX

A estrutura do cabeçalho IPX é extremamente simples, citaremos alguns campos :

- Controle de transporte : Equivale ao tempo de vida (TTL) do IP. Conta a quantidade de vezes que o datagrama passou pelos roteadores, ao chegar ao valor padrão 16 este datagrama é descartado
- Tipo do Pacote : Identifica o tipo do pacote
- Socket : Identifica o protocolo acima do IPX que o está usando, é equivalente ao conceito de portas usado no TCP/IP.

Figura 1.11 – Estrutura do datagrama IPX

1.6.1.2. Usando IPX em Redes Ethernet

Para utilizar o protocolo IPX corretamente em redes Ethernet, foi criado dois novos formatos de quadro : o quadro IEEE 802.2 e o quadro SNAP. Então, uma mesma rede pode ter máquinas operando com quadros Ethernet/IPX de padrões diferentes, isso geraria um problema. As máquinas configuradas para operar com um padrão mais antigo não conseguem entender o padrão mais novo, neste caso, a solução é utilizar um roteador que configuraria um número de rede para cada tipo de quadro.

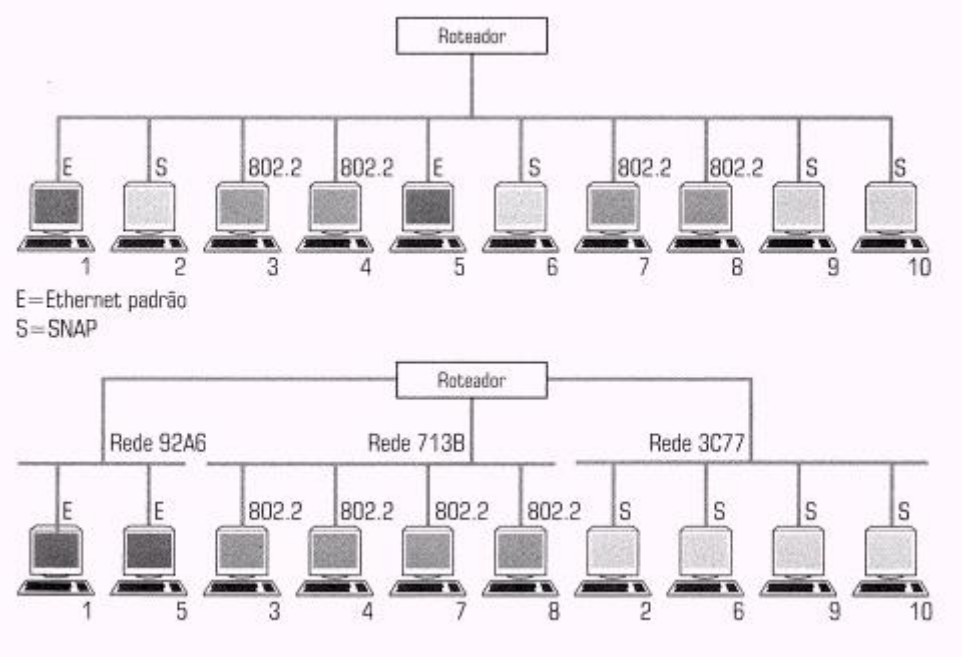


Figura 1.12 – Uso do roteador em redes Ethernet/IPX

O SPX (Sequenced Packet Exchange) parece muito com o TCP, com a diferença de não trabalhar com o conceito de janela, ou seja, o SPX espera a confirmação do último pacote enviado para poder enviar um outro pacote. Este problema foi solucionado no Netware 4 que lançou o protocolo SPX II, que trabalha com o conceito de janela e ainda permite uma quantidade maior de dados na área de dados do pacote.

1.6.1.3. Protocolo SAP (Service Advertisement Protocol)

Este protocolo é um recurso utilizado pelo Netware serve para comunicar os recursos existentes para os micros da rede. Exemplificando, quando uma impressora ou servidor torna-se disponível na rede, o SAP envia para todas as máquinas da rede a informação de que serviço pertence. Este serviço causa congestionamento na rede que pode ser detectado em redes grandes.

Um roteador que não replicasse mensagens SAP, solucionaria este problema. O SAP é uma característica do Netware e não do IPX/SPXb

1.6.2. NetBEUI (NetBIOS Enhanced User Interface)

O NetBEUI é um protocolo da Microsoft, na qual, acompanha todos os seus sistemas operacionais e produtos de redes. Foi criado originalmente pela IBM, na época em que a IBM e a Microsoft possuíam uma parceria para a produção de sistemas operacionais e softwares.

Um detalhe importante é não confundir o NetBIOS com o NetBEUI. O NetBIOS é uma API de programação do protocolo NetBEUI, que trabalha na camada 5 do modelo OSI (Camada de Sessão), fazendo o interfaceamento entre programas e o protocolo NetBEUI.

O BetBIOS é parte do NetBEUI (que trabalha nas camadas 3 e 4 do modelo OSI). O NetBIOS também pode ser utilizado em conjunto com outros protocolos operando nas camadas abaixo da camda 5 do modelo OSI (como o TCP/IP e o IPX/SPX), permitindo que os programas utilizem uma linguagem comum para acessarem a rede, independente do protocolo que está instalado na máquina.

O NetBEUI é um protocolo pequeno e rápido. Porém possui duas grandes desvantagens que tornam seu uso praticamente inviável para redes com mais de 80 máquinas.

Primeiro, ele é um protocolo não roteável, ou seja, não pode ser usado em redes que possuem outras redes interconectadas que utilizem roteadores para se comunicar.

Segundo o NetBEUI utiliza excessivamente mensagens de broadcast, congestionando a rede. Se uma máquina precisa imprimir um documento na impressora da rede, ela envia uma mensagem para todas as máquinas e não somente para a máquina onde a impressora está instalada. Com isso, a rede fica ocupada, diminuindo muito seu desempenho.

Atualmente a tendência é a interconexão de redes, especialmente por conta da Internet, podemos concluir que o uso do protocolo NetBEUI é desaconselhável.

2. Cabeamento

Este é um componente importante para uma rede, é responsável pela circulação dos dados. Neste capítulo estudaremos três tipos de cabeamento : o cabo coaxial, par trançado a fibra óptica, além das redes sem cabo, exemplificando a comunicação via rádio.

2.1. Cabo Coaxial

Um dos primeiros tipos de cabos usados em rede, utilizado mais em redes de pequeno porte. Possui uma impedância que é medida em ohms (Ω) as redes Ethernet (próximo capítulo) utilizam cabos coaxiais de 50 ohms. Apesar de parecido com o cabo coaxial utilizado em antenas de televisão possuem impedâncias diferentes. O cabo utilizado em antenas é de 75 Ω, não sendo possível utilizar um no outro.

O taxa de transferência máxima do cabo coaxial é de 10 Mbps, muito inferior em comparação com o par trançado que já operam a 100 Mbps.

Vantagens do cabo coaxial :

- Sua blindagem permite que o cabo seja longo o suficiente.
- Melhor imunidade contra ruídos e contra atenuação do sinal que o par trançado sem blindagem.
- Baixo custo em relação ao par trançado.

Desvantagens do cabo coaxial :

- Por não ser flexível o suficiente, quebra e apresenta mau contato com facilidade, além de ser difícil a instalação em conduítes.
- Utilizado em topologia linear, caso o cabo quebre ou apresente mau contato, toda a rede trava.
- Em lugares com instalação elétrica precária ou mal organizada, ao fazer a instalação ou manutenção dá muito choque.
- Vedada a utilização em redes de grande porte.

2.1.1. Tipos de Transmissão

Existem dois tipos de transmissão : *baseband e broadband.*

Baseband (Banda base) é utilizado para transmitir apenas um canal (uni-canal) de dados de forma digital, é mais usados em redes locais.

Broadband (Banda larga) é usado para transmitir simultaneamente vários canais (multi-canal) de dados de forma analógica.

2.1.2. Tipos de Cabos

Existem vários tipos de cabo coaxial, uma vez, que esse tipo de cabo é utilizado também para transmissão de áudio e vídeo. Nas redes locais, são utilizados dois tipos : cabo coaxial fino ou 10Base2 e o cabo coaxial grosso ou 10Base5.

Traduzindo a nomenclatura dos cabos, teremos, 10Base2 significa que a taxa de transmissão é de 10 Mbps, a transmissão é do tipo *baseband* e o cabo é coaxial com comprimento máximo de 200 metros. Na verdade foi feito um arredondamento, pois a extensão máxima do cabo coaxial fino é de 185 metros. Já o 10Base5 indica o comprimento máximo de 500 metros.

2.1.2.1. Cabo Coaxial Fino (10Base2)

Possui o comprimento máximo de 185 metros por segmento de rede e possui um limite de 30 máquinas conectadas por segmento de rede. Utilizado em redes Ethernet com o topologia linear, ou seja, todos os computadores da rede local são conectados por um único cabo.

A conexão de cada micro com o cabo coaxial é feita através de conectores BNC em “T”. Este conector vem junto com a placa de rede adquirida. Ao final da rede e preciso instalar um terminador resistivo para dar a correta impedância do cabo.

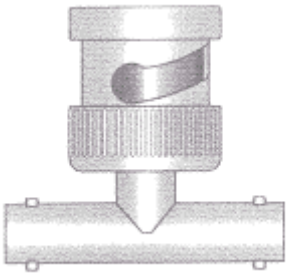


Figura 2.1 – Conector BNC em “T”.

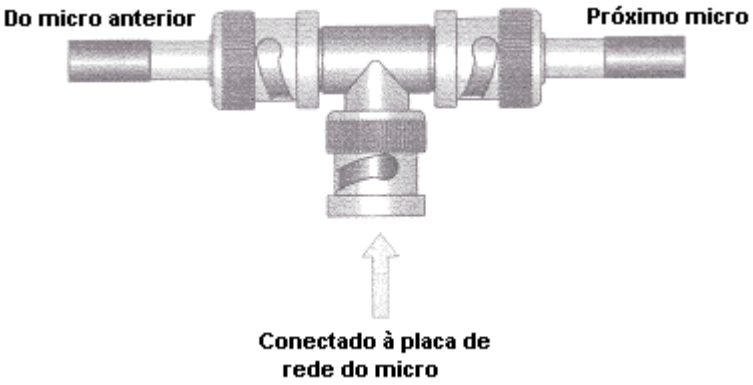


Figura 2.2 – Instalação do conector BNC em “T”.

O que fazer caso o cabo parta ou apresente mau contato ? Existem duas soluções, ou refaça o cabo problemático, ou utilize um conector BNC de emenda (barril). Entretanto, só use esse conector em último caso, porque seu uso diminui o desempenho do cabo.

2.2. Par Trançado

Existem dois tipos de cabo par trançado : sem blidagem ou UTP (Unshielded Twisted Pair) e com blindagem ou STP (Shielded Twisted Pair). Atualmente o cabo de rede mais utilizado é o par trançado sem blindagem, que utiliza o conector denominado RJ-45.

O par trançado possui uma ótima técnica contra ruído, denominada *cancelamento*. Através dessa técnica, as informações circulam repetidas em dois fios, sendo que no segundo fio a informação tem a polaridade invertida. Com isso o campo eletromagnético gerado por um dos fios é anulado pelo outro fio. O par trançado possui um limite de dois dispositivos por cabo.

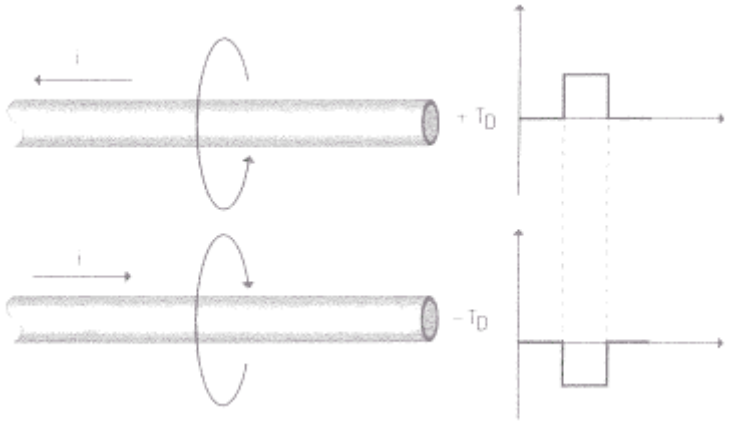


Figura 2.3 – Proteção contra ruídos do par trançado.

2.2.1. Topologia

A topologia utilizada pelo par trançado é a estrela, onde um dispositivo concentrador faz a conexão entre os computadores. Este concentrador é a mais conhecido como *hub*, com ele o problema de limite de dois dispositivos é solucionado.

Diferentemente do cabo coaxial, quando um cabo se parte, apenas a estação conectada ao respectivo cabo perde comunicação com a rede, um grande alívio. Imagine uma rede que utiliza cabo coaxial com 30 estações e de repente toda a rede trava, você terá que repassar estação por estação para identificar o cabo com defeito, quanto tempo gastaria ?

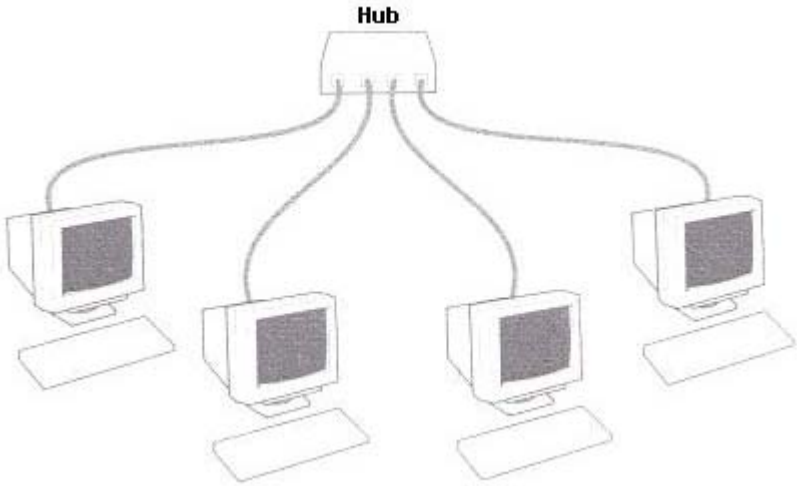


Figura 2.4 –Topologia em estrela

2.2.2. Par Trançado sem Blindagem (UTP)

Os cabos do tipo par trançado são classificados em 5 categorias. Os cabos de categoria 1 e 2 são usados por sistemas de telefonia, já cabos de categoria 3, 4 e 5 são utilizados em redes locais :

- Categoria 3 : Permite comunicações até 16 Mbps. É utilizado por redes de par trançado operando a 10 Mbps. Utilizado também em redes Token Ring.
- Categoria 4 : Permite comunicações até 20 Mbps.
- Categoria 5 : Permite comunicações até 100 Mbps, é o tipo mais utilizado hoje em dia.

Existem no cabo par trançado quatro pares de fios, sendo que, apenas dois pares são utilizados, um para a transmissão de dados e outro para a recepção de dados. Para uma melhor identificação, os quatro pares do cabo são coloridos : verde, laranja, marrom e azul. Todas as cores possuem um fio branco com uma faixa de sua própria cor.

Para um padronização na montagem do cabo, aconselha-se utilizar a mesma seqüência de cores na rede. O problema é que nem todo mundo segue a mesma seqüência, e na hora de fazer a manutenção de uma rede, fica difícil adivinhar qual a ordem dos fios que foi utilizada.

O sistema de cabeamento de 10 e 100 Mbps original utiliza um esquema de fiação derivado do padrão T568A do TIA/EIA (Telecommunications Industry Association/Electronic Industries Alliance) que é um órgão norte-americano responsável pela padronização de sistemas de telecomunicações. Esse padrão é apresentado na tabela abaixo :

Pino	Cor	Função
1	Branco Verde	+TD
2	Verde	-TD
3	Branco Laranja	+RD

4	Azul	Não usado
5	Branco Azul	Não usado
6	Laranja	-RD
7	Branco Marrom	Não usado
8	Marrom	Não usado

2.2.2.1. Cross-Over

Os cabos par trançado fazem uma ligação pino-a-pino entre os dispositivos que estejam, por exemplo, um micro a um hub. Como já é de nosso conhecimento, apenas dois pares de fios são usados sendo um para a transmissão e outro para recepção. O que acontece dentro do hub é conectar os sinais que estão das máquinas (TD) às entradas de dados das demais máquinas (RD) e vice-versa, só assim a comunicação pode ser feita. Esse processo é chamado *cross-over* (cruzamento).

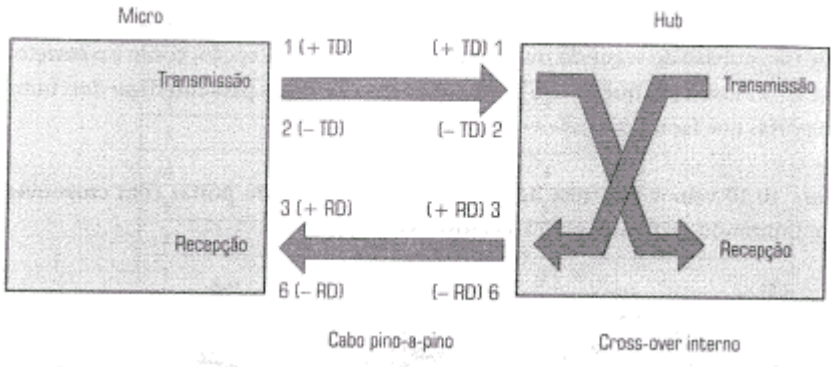


Figura 2.5 – Funcionamento do cross-over dentro do hub.

Se você quiser montar uma rede com apenas dois micros, pode fazer a ligação direta sem o uso de hub, neste caso o cabo pino-a-pino não funcionará, pois será ligado a saída de dados de um micro na saída de dados do outro, e não na entrada de dados como seria o correto. A figura abaixo mostra como fica o cruzamento externamente.

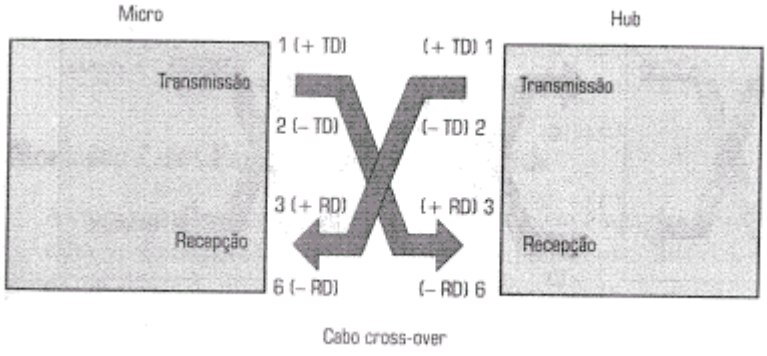


Figura 2.6 – Funcionamento do cabo cross-over

O cabo cross-over é utilizado também na interligação do dois hubs, a pinagem desse tipo de cabo é mostrado na tabela a seguir.

Pino	Conector A	Conector B
1	Branco Verde	Branco Laranja
2	Verde	Laranja
3	Branco Laranja	Branco Verde
4	Azul	Azul
5	Branco Azul	Branco Azul
6	Laranja	Verde
7	Branco Marrom	Branco Marrom
8	Marrom	Marrom

2.2.2.2. Montando Cabos Par Trançado Sem Blindagem

A montagem do cabo par trançado sem blindagem é relativamente simples. Além do cabo, você precisará de dois conectores RJ-45 de pressão e do alicate de pressão para conectores RJ-45 (também chamado de alicate de *crimp)*.

A seguir mostraremos passo-a-passo como montar um cabo par trançado. Estamos levando em conta que se trata de uma rede pequena onde não está sendo utilizado nenhum sistema de cabeamento estruturado. O cabo que montaremos será utilizado para a conexão direta entre dois micros ou cross-over.

1. O cabo par trançado é vendido em rolos de centenas de metros, por isso corte o cabo no comprimento desejado, vamos trabalhar com 1,5 metros. Lembre-se de deixar uma folga de alguns centímetros, você poderá errar na hora de instalar o plugue RJ-45, fazendo com que você precise cortar alguns poucos centímetros do cabo para instalar novamente o plugue.

2. Desencape aproximadamente 2,5 cm do cabo. Remova somente a proteção externa do cabo. Isso pode ser feito cuidadosamente com uma pequena tesoura ou com o desencapador do alicate. Alguns cabos possuem um filme plástico envolvendo os fios que também deve ser removida.

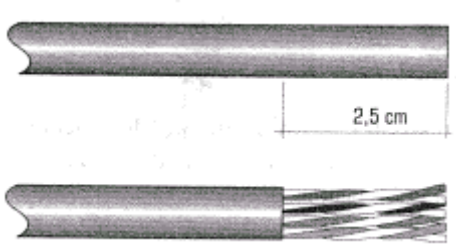


Figura 2.7 – Desencapando o cabo por trançado.

3. Desenrole os fios que ficaram para fora do cabo.

4. Coloque os fios na ordem em que eles serão instalados no conector RJ-45 (ver tabela a seguir). Os pinos do conector RJ-45 são contados da esquerda para a direita, com o clip apontado para baixo.

Pino	Conector A	Conector B
1	Branco Verde	Branco Laranja
2	Verde	Laranja
3	Branco Laranja	Branco Verde
4	Azul	Azul
5	Branco Azul	Branco Azul
6	Laranja	Verde
7	Branco Marrom	Branco Marrom
8	Marrom	Marrom

5. Corte os fios a 1,5 cm do invólucro do cabo utilizando um alicate de corte, como mostra a figura.

Figura 2.8 – Cortando os fios.

6. Insira cada fio em seu "tubo", até que atinja o final do conector.

7. Insira o conector no alicate de pressão e pressione o alicate. Antes disso, verifique atentamente se todos os fios realmente atingiram o final do conector. Os pinos do conector são pequenas lâminas que desencapam os fios e, ao mesmo tempo, fazem o contato externo.

8. Após pressionar o alicate, remova o conector do alicate e verifique se o cabo ficou bom. Para isso, puxe o cabo para ver se não há nenhum fio que ficou solto ou frouxo.

9. Repita o processo para a outra ponta do cabo.

2.2.3. Cabeamento Estruturado

No cabeamento estruturado há a necessidade de um dispositivo concentrador, tipicamente um hub, para fazer a conexão entre os micros, já que o par trançado só pode ser usado para ligar dois dispositivos.

Em redes pequenas, o cabeamento não é um ponto que atrapalhe o dia-a-dia da empresa, já que apenas um ou dois hubs são necessários para interligar todos os micros.

Entretanto, em redes médias e grandes a quantidade de cabos e o gerenciamento dessas conexões pode atrapalhar o dia-a-dia da empresa. A simples conexão de um novo micro na rede

pode significar horas e horas de trabalho (passando cabos e tentando achar uma porta livre em um hub).

A ocorrência de mudança de micros em empresas médias e grandes é freqüente. É aí que entra o cabeamento estruturado. A idéia básica é fornecer um sistema de cabeamento que facilite a remoção de equipamentos, igual ao que ocorre com o sistema elétrico do prédio: para instalar um novo equipamento elétrico, basta ter uma tomada de força disponível.

O sistema mais simples de cabeamento estruturado é aquele que as tomadas RJ-45 são as intermediárias entre o micro e o hub. Em um escritório, por exemplo, teria vários pontos de rede já preparados para receber novas máquinas, neste caso, não teria a necessidade de a cada micro novo fazer o cabeamento até o hub. Isso agiliza muito o dia-a-dia da empresa e da instalação.

Existem muitos prédios modernos que já são construídos com dutos próprios para a instalação de redes, inclusive com esse tipo de cabeamento estruturado. A tomadas que são embutidas na rede apresentam conectores de telefone também, para aproveitar como ponto de ramal telefônico.

A idéia do cabeamento estruturado vai muito além disso. Além do uso de tomadas, o sistema de cabeamento estruturado utiliza um concentrador de cabos chamado patch panel (painel de conexões). Neste sistema, os cabos que vêm das tomadas são conectados ao patch panel que depois conectam ao hub. O patch panel funciona como um grande concentrador de tomadas, como mostra a figura abaixo.

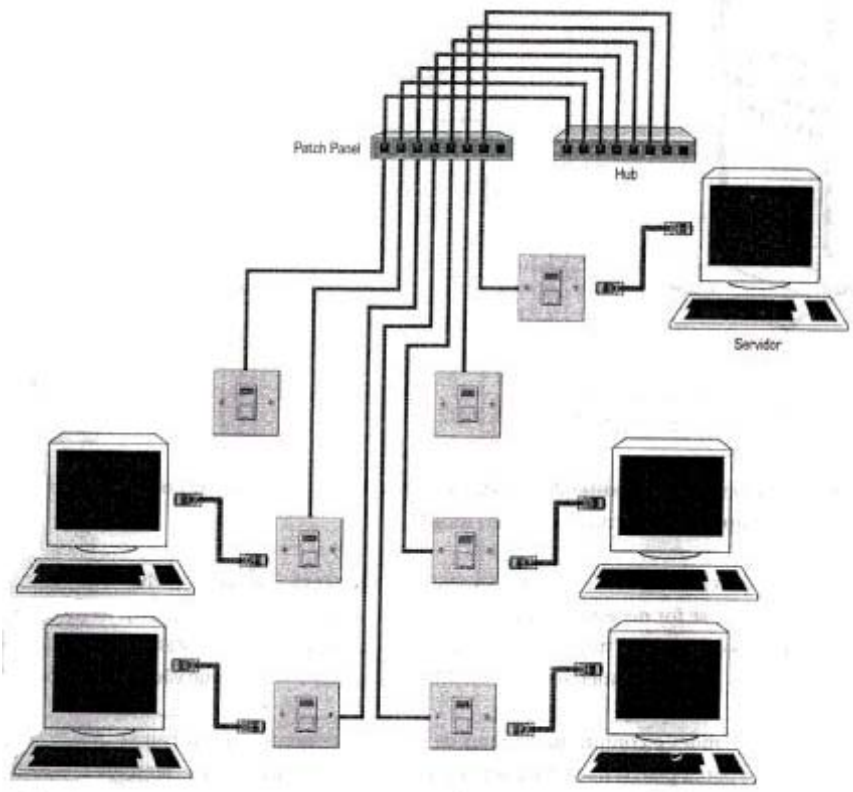


Figura 2.9 – Sistema simples de cabeamento estruturado usando um patch panel.

O patch panel é um sistema passivo, não possui circuito eletrônico. Assim como hubs, switches e roteadores, o patch panel possui tamanho padrão de rack. Podemos concentrar todos esses dispositivos em um mesmo local.

Você deve estar se perguntando por que usar patch panels, já que fica óbvio que o uso desses componentes torna a rede mais cara. O uso de patch panels facilita enormemente a manutenção de redes médias e grandes. Por exemplo, se for necessário trocar dispositivos, adicionar novos dispositivos (hubs e switches), alterar a configuração de cabos. Basta trocar a conexão dos dispositivos no patch panel, sem a necessidade de alterar os cabos que vão até os micros.

Em redes grandes é comum haver mais de um local contendo patch panels, neste caso as portas dos patch panels são conectadas também a outros patch panels. Se for necessário conectar algum dispositivo presente na rede 1 a algum dispositivo presente na rede 2 ou 3, basta fazer as conexões necessárias nos patch panels, não sendo necessário passar nenhum novo cabo na rede.

Finalizando, o cabeamento estruturado tem como essência o projeto do cabeamento da rede. O cabeamento deve ser projetado sempre pensando na futura expansão da rede e na facilidade de manutenção. Devemos lembrar sempre que, ao contrário de micros e de programas — que se tornam obsoletos com certa facilidade —, o cabeamento de rede não é algo que fica obsoleto com o passar dos anos. Com isso, na maioria das vezes vale à pena investir em montar um sistema de cabeamento estruturado.

Um detalhe importante, devido ao uso de tomadas e plugues, as redes usando cabeamento estruturado deve diminuir 10 metros na conta do comprimento máximo do cabo. O comprimento máximo do cabo passa a ser 90 metros.

2.3. Fibra Óptica

A fibra óptica transmite informações através de sinais luminosos, em vez de sinais elétricos. A idéia é simples: luz transmitida indica um valor “1,’ e luz não transmitida, um valor “0”. Ela apresenta duas grandes vantagens em relação aos cabos tradicionais.

- Interferências eletromagnéticas não ocorrem no tráfego da luz, ou seja, é totalmente imune a ruídos. Significando comunicações mais rápidas, já que praticamente não haverá a necessidade de retransmissões de dados.
- O sinal sofre menos do efeito da atenuação, ou seja, conseguimos ter um cabo de fibra óptica muito mais longo sem a necessidade do uso de repetidores. A distância máxima de um segmento do tipo de fibra óptica mais usado é de 2 Km (compare com o limite de 185 metros do cabo coaxial fino e com o limite de 100 metros do par trançado).

Outra vantagem é que a fibra não conduz corrente elétrica e, com isso, você nunca terá problemas com raios nem qualquer outro problema envolvendo eletricidade. Como a luz só pode ser transmitida em uma direção por vez, o cabo de fibra óptica possui duas fibras, uma para a transmissão de dados e outra para a recepção, permitindo, dessa forma, comunicações full-duplex. Interessante notar que a fibra óptica é bastante fina e flexível. Sua espessura é similar à espessura

do cabo par trançado sem blindagem, com isso dutos, racks e dispositivos similares usados no cabeamento estruturado também podem ser usados pela fibra óptica sem qualquer problema.

Se a fibra óptica é tão melhor, por que os cabos de cobre ainda existem? O preço é o fator determinante. Embora o custo da fibra óptica tenha caído muito nos últimos anos, o custo de instalação ainda é alto. A solução mais usada na maioria das vezes é uma rede mista, usando fibras ópticas nas comunicações que exijam alto desempenho, e par trançado sem blindagem (UTP) na conexão dos micros com os dispositivos concentradores. Em geral as comunicações que exigem alto desempenho são aquelas que fazem a conexão dos dispositivos concentradores das várias redes locais que compõem a rede. Essa conexão de alto desempenho é também chamada espinha dorsal ou *backbone.*

Existem dois tipos de fibras ópticas: modo múltiplo (MMF, Multiple Mode Fiber) e modo único (SMF, Single Mode Fiber). Essa classificação diz respeito a como a luz é transmitida através da fibra.

As fibras de modo múltiplo são mais grossas do que as fibras de modo único. No modo múltiplo a luz reflete mais de uma vez nas paredes da fibra e, com isso, a mesma informação chega várias vezes ao destino, de forma defasada. O receptor possui o trabalho de detectar a informação correta e eliminar os sinais de luz duplicados, quanto maior o comprimento do cabo, maior esse problema.

Já as fibras de modo único são finas e, com isso, a luz não ricocheteia nas paredes da fibra, chegando diretamente ao receptor. Esse tipo de fibra consegue ter um comprimento e um desempenho maiores que as fibras de modo múltiplo.

As fibras ópticas de modo múltiplos são as mais usadas, devido serem mais baratas e também pela espessura, existe a dificuldade em fazer o acoplamento da placa de rede com a fibra óptica de modo único, ou seja , alinhar o feixe de luz produzido pela placa de rede com a fibra de transmissão de modo que a luz possa ser transmitida.

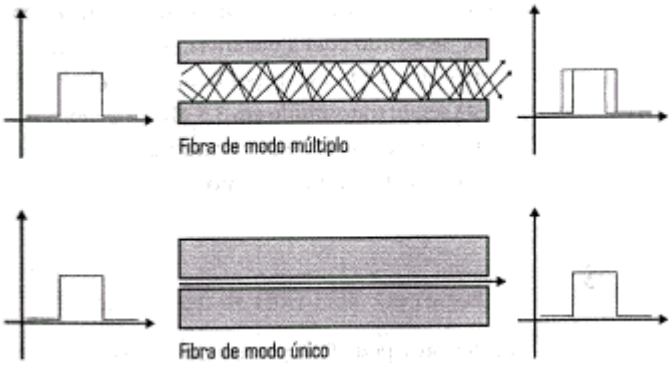


Figura 2.10 – Transmissão de luz na fibra óptica.

Os fabricantes de fibra óptica especificam a largura de banda máxima da fibra em uma unidade chamada MHz.Km. Uma fibra de 200 MHz.Km pode transmitir dados a 200 MHz a até 1 Km de distância ou então a 100 MHz a até 2 Km de distância, ou seja, quanto mais longe menor a taxa

de transmissão. A atenuação (ou perda) que a fibra sofre no sinal que está sendo transmitido, de acordo com a distância, é medida em uma unidade chamada dB/Km (decibéis por quilômetro). Uma fibra com perda de 3,5 dB/Km, diminuirá a força do sinal que está sendo transmitido em 3,5 dB por quilômetro.

Importante. Nunca olhe diretamente para uma fibra óptica (caso você faça isso, você corre o risco de ficar cego) — como a luz usada na transmissão de dados é invisível, você nunca saberá se a fibra está transmitindo ou não luz. É melhor prevenir do que remediar.

2.4. Redes sem fio

Normalmente quando falamos em redes logo pensamos em que tipo de cabo será usado. Entretanto, as informações de uma rede não necessariamente trafegam de um lado para outro através de cabos convencionais. Vários sistemas de transmissão de dados podem ser usados, dependendo da necessidade. O mais conhecido é o sistema de transmissão de dados através de ondas de rádio, ao invés dos micros da rede estarem conectados através de um cabo, eles estão conectados a um transmissor e receptor de rádio.

Essa solução pode ser mais barata do que o aluguel de linhas Ei ou Ti das operadoras de telecomunicações. Entretanto, a tecnologia de rádio não podem ser usadas para a conexão de duas (ou mais) redes, ou por conta da existência de muitos obstáculos físicos, ou por conta da distância.

É muito importante ter em mente que a idéia da comunicação sem fio não é substituir o cabo tradicional, mas sim ter mais possibilidade dentro dos sistemas de cabeamento disponíveis.

Os sistemas mais conhecidos para transmissão de dados sem fio são:

- Rádio
- Infravermelho
- Laser

2.4.1. Rádio

Existem dois modos básicos de transmitirmos dados através de ondas de rádio. O não-direcional e o direcional.

No primeiro, a transmissão dos dados não é direcional e, com isso, antenas localizadas na região de alcance das ondas de rádio da antena transmissora podem captar os dados transmitidos. Esse sistema não é seguro, já que qualquer antena na região de alcance pode captar os dados transmitidos. Embora esse sistema não transmita os dados de uma forma segura, ele é muito usado em sistemas onde os dados são públicos (por exemplo, bolsa de valores).

Esse sistema é também muito usado dentro de prédios, de forma a interligar máquinas ou redes entre si sem a utilização de cabos. Nesse caso, normalmente usa-se um sistema de baixa potência, onde antenas instaladas fora do prédio normalmente não são capazes de captar as informações que estão sendo transmitidas na rede (embora esse problema ocorra, como veremos mais adiante).

O segundo sistema de transmissão usando ondas de rádio é a transmissão direcional,

usando pequenas antenas parabólicas. Nesse caso, somente duas redes podem se comunicar. Esse sistema apresenta como grande vantagem transmitir os dados somente para o receptor.

A desvantagem é que as antenas têm de estar alinhadas, ou seja, não podendo ter obstáculos no caminho e tempestades podem desalinhar a antena, impedindo a comunicação entre as redes.

2.4.1.1. Padronização

Um dos grandes problemas das comunicações sem fio é a falta de padronização entre os fabricantes. Antigamente, um determinado equipamento para a transmissão através de ondas de rádio de um fabricante não era compatível com o equipamento produzido por outro fabricante, mesmo quando usavam a mesma faixa de freqüência para a transmissão de dados (a questão não era a faixa de freqüência usada, mas sim como os dados eram transmitidos).

Para resolver essa questão, o Instituto de Engenharia Elétrica e Eletrônica (IEEE) lançou o padrão 802.11, que define a camada de Controle de Acesso ao Meio (MAC) para transmissões sem fio.

A partir dessa padronização as redes sem fio começaram a operar via rádio facilmente. As redes podem ser constituídas usando equipamentos de diferentes fabricantes, desde que, utilizem o padrão IEEE 802.11, vão se comunicar sem qualquer problema.

O padrão IEEE 802.11 utiliza um esquema de transmissão chamado CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Na primeira transmissão o transmissor escuta o canal para verificar se ele está desocupado, se nenhuma transmissão estiver sendo efetuada, ele inicia a primeira transmissão. Após a primeira transmissão ter ocorrido, cada máquina é configurada para transmitir a um determinado período de tempo. Neste sistema não há colisões, já que cada máquina possui uma hora certa de transmitir.

Se a rede ficar ociosa, então o canal pára de ser usado e a rede volta ao estado anterior ao da primeira transmissão, isto é, a alocação de tempo de transmissão de cada máquina só é definida após a primeira transmissão ter sido efetuada.

Existe um único momento que pode haver a colisão, na primeira transmissão; quando duas ou mais máquinas verificam que o canal está livre e tentam transmitir ao mesmo tempo.

Isso não acontece no esquema CSMA/CD (Carrier Sense Multiple Access with Collision Detection) usado por redes Ethernet, onde a colisão pode ocorrer sempre que o canal estiver livre. Esse padrão define transmissões por rádio usando as técnicas FHSS ou DSSS.

2.4.1.1.1. FHSS (Frequency Hopping Spread Spectrum)

Esse método de transmissão, em vez de uma freqüência de transmissão fixa, usa uma faixa de freqüência, isto é, várias freqüências de transmissão, sendo dividida em canais.

Nesse sistema, o canal usado é alterado automaticamente por todos os dispositivos da rede, só que não de uma maneira seqüencial, mas sim de um maneira aleatória. Os dispositivos da rede necessitam saber a seqüência exata dos canais usados para poderem transmitir e receber dados.

Uma vantagem desse sistema é que várias redes operando por ondas de rádio podem co-existir usando a mesma faixa de freqüência na mesma região sem gerarem interferência de rádio entre elas.

Quando ocorrer a interferência, os sistemas irão ter problemas somente durante 100 milissegundos. Como a troca de canais é feita aleatoriamente, possivelmente o próximo canal usado pelos sistemas será diferente, eliminando o conflito. Em uma área que tenha dois sistemas FHSS operando, as chances de conflito de canal são de 1:79 (1,26%), já que existem 79 canais disponíveis.

Este tecnologia está sendo substituída pelo DSSS, que é mais rápida, devido sua freqüente alternância de canais. As taxas de transmissão utilizadas são de 1 ou 2 Mbps.

2.4.1.1.2. DSSS (Direct Sequence Spread Spectrum)

A tecnologia DSSS, que também é definida pelo padrão IEEE 802.11, funciona de maneira similar à tecnologia FHSS, só que, a troca dos canais é feita de uma forma seqüencial.

É importante notar que as tecnologias FHSS e DSSS são incompatíveis entre si. Apesar de serem especificadas pelo mesmo padrão, uma antena FHSS não consegue comunicar-se com uma antena DSSS e vice-versa.

Tecnicamente falando, esta é uma tecnologia de transmissão menos segura do que a FHSS, basta ter uma antena DSSS para conseguir captar os dados que estão sendo transmitidos na rede. E não precisa ser um hacker muito inteligente para fazer isso: basta um computador dotado de uma antena DSSS instalado perto de sua rede.

Por isso a importância de habilitarmos a criptografia WEP, pois muitas vezes os equipamentos DSSS não vêm com essa criptografia habilitada de fábrica.

3. Arquiteturas de Redes Locais

3.1. Ethernet

A arquitetura Ethernet é a mais usada em redes locais. O Ethernet é um padrão que define como os dados serão transmitidos fisicamente através dos cabos da rede, ou seja, opera nas camas 1 e 2 do modelo OSI assim como na arquitetura Token Ring. O Ethernet define também como fisicamente esses dados serão transmitidos.

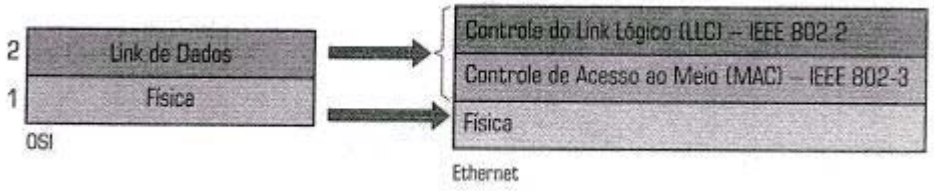


Figura 3.1 – Arquitetura Ethernet

As três camadas da arquitetura Ethernet possuem as seguintes funções:

- Controle do Link Lógico (LLC, JEEE 802.2): Inclui informações do protocolo de alto nível que entregou o pacote de dados a ser transmitido. Com isso, a máquina receptora tem como saber para qual protocolo de alto nível ela deve entregar os dados de um quadro que ela acabou de receber.
- Controle de Acesso ao Meio (MAC, JEEE 802.3): Monta o quadro de dados a ser transmitido pela camada física, incluindo cabeçalhos próprios dessa camada aos dados recebidos da camada de Controle do Link Lógico.
- Física: Transmite os quadros entregues pela camada de Controle de Acesso ao Meio usando o método CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Define como os dados são transmitidos através do cabeamento da rede e também o formato dos conectores usados na placa de rede.

3.1.1. Camada Física

A seguir veremos o funcionamento da camada física da arquitetura Ethernet: o padrão CSMA/CD, a codificação dos dados e a placa de rede.

Em redes Ethernet, todos os micros compartilham o mesmo cabo, independentemente da topologia utilizada. Isso significa que, quando o cabo está sendo utilizado nenhuma outra máquina poderá usá-lo ao mesmo tempo.

O primeiro passo na transmissão de dados em uma rede Ethernet é verificar se o cabo está livre. Isso é feito pela placa de rede e daí o nome C*arrier Sense* (detecção de portadora). Se o cabo

estiver livre, a placa de rede inicia sua transmissão. Caso ele esteja ocupado, a placa espera até que ele fique livre. A transmissão só será iniciada caso o cabo esteja livre.

Entretanto, o protocolo CSMA/CD não gera nenhum tipo de prioridade (daí o nome *Multiple Access*, acesso múltiplo). Com isso, pode ocorrer de duas ou mais placas de redes perceberem que o cabo está livre e tentarem transmitir dados ao mesmo tempo. Quando isso ocorre, há uma *colisão* e nenhuma das placas consegue transmitir dados.

Quando ocorre uma colisão, todas as placas de rede param de transmitir, esperam um período de tempo aleatório, e tentam a retransmissão. Como cada placa de rede envolvida na colisão provavelmente gerará um valor aleatório diferente, possivelmente não ocorrerá novamente outra colisão, pois uma das placas começará a sua transmissão antes das demais. E as demais verificarão que o cabo está ocupado e não tentarão transmitir.

3.1.1.1. Transmissão de Dados

Antes de serem transmitidos, os dados são codificados (modulados). Porque isto é feito ? É feito com a finalidade de fazer com que possam existir informações especiais de controle entre os dados que estão sendo transmitidos.

Para cada taxa de transferência utilizada, um padrão diferente de codificação é usado:

- 10 Mbps (Ethernet padrão): É usada a codificação Manchester.
- 100 Mbps (Fast Ethernet): É usada uma codificação chamada 4B/SB.
- 1 Gbps (Gigabite Ethernet): Usa a codificação chamada 4D-PAM5.

Na codificação Manchester, cada O e cada 1 que deve ser transmitido não é substituído diretamente por um valor de tensão (5 V para o valor 1 e o v para o valor 0), mas sim por uma transição de tensão. O valor O é substituído por uma transição de 1 para O e o valor 1 é substituído por uma transição de O para 1.

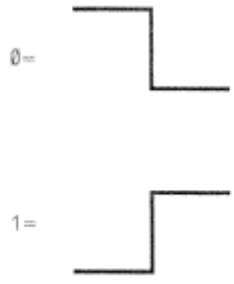


Figura 3.2 – Funcionamento da codificação Manchester.

Abaixo citarei alguns componentes que fazem parte da arquitetura Ethernet.

3.1.1.2. Placa de Rede

Tem como função, receber os quadros enviados pela camada de Controle de Acesso ao Meio e transmitir os dados através do cabeamento da rede. Nas placas de rede Ethernet você encontrará os seguintes conectores :

- BNC: Usado por cabo coaxial fino (10Base2).
- RJ-45: Usado por cabo par trançado sem blindagem (10BaseT).

3.1.1.3. Cabeamento

Os padrões de cabeamento Ethernet são expressos no seguinte formato:

[Taxa máxima de transmissão][Tipo de transmissão][Tipo do cabo]

- Taxa máxima de transmissão: é expressa em Mbps.
- Tipo de transmissão: o tipo de transmissão usado em redes Ethernet é do tipo uni-canal (baseband) e, por isso, você encontrará o termo "Base".
- Tipo do cabo: No caso do cabo coaxial, é expresso o comprimento máximo do cabo, "2" para cabo coaxial fino (arredondamento do limite máximo desse cabo, que é de 185 metros por segmento) e "5" para cabo coaxial grosso (já que esse cabo possui um limite de 500 metros por segmento). O par trançado sem blindagem é expresso com um "T" (de *Twisted pair).* E a fibra óptica é expressa com um "F".

Abaixo, temos os principais padrões de cabos em redes Ethernet:

- 10Base2: Cabo coaxial fino, comprimento até 185 metros por segmento.
- 10BaseT: Cabo par trançado sem blindagem, comprimento até 100 metros por segmento.
- 10BaseFL: Fibra óptica de modo múltiplo, comprimento de 2 Km por segmento.

3.1.1.4. Topologia

Os tipos de topologia utilizados nas redes Ethernet são :

- Linear ou Barramento: todos os micros são ligados fisicamente a um mesmo cabo. Utilizado pelo cabo coaxial fino, tem como grande desvantagem o fato de que se o cabo partir ou apresentar mau contato, toda a rede trava.
- Estrela: todos os micros são ligados a um mesmo cabo através de um dispositivo concentrador (por exemplo, hub). Utilizam cabos do tipo par trançado sem blindagem e fibra óptica. A grande vantagem é sua flexibilidade, em caso de defeito no cabo apenas o micro em questão travará.

3.2. Token Ring

Token Ring é uma arquitetura de redes locais criada pela IBM e padronizada pelo IEEE em seu padrão 802.5. Isso significa que a arquitetura do padrão Token Ring é igual à arquitetura do padrão Ethernet, com a diferença que as suas camadas Física e Controle de Acesso ao Meio funcionam diferentemente.

A diferença é que no Ethernet todas as máquinas têm a mesma prioridade e, com isso, podem ocorrer colisões. Já na rede Token Ring, cada máquina possui um tempo certo de enviar um quadro de dados, mesmo que o cabo esteja livre, cada máquina só pode enviar dados em um determinado momento.

A topologia das redes Token Ring é a de anel *(ring)*, na qual, circula um quadro dentro deste

anel (chamado token -> ficha). Cada máquina só pode enviar um quadro de dados para a rede quando a ficha passa por ela e esta estiver vazia. Assim, a rede consegue garantir que somente uma transmissão é efetuada por vez. Só pode circular uma única ficha na rede e ela sempre circula na mesma direção.

Para um melhor desempenho das redes Token Ring, é utilizado um periférico concentrador chamado MAU (Multistation Access Unit). Funciona como um hub, porém específico para redes Token Ring. O MAU implementa o anel internamente. Quando uma máquina é adicionada ao MAU ou então removida, esse dispositivo automaticamente percebe essa condição e altera o anel interno de forma a adicionar ou remover a máquina do anel, ou seja, a rede não pára quando uma máquina é adicionada ou removida.

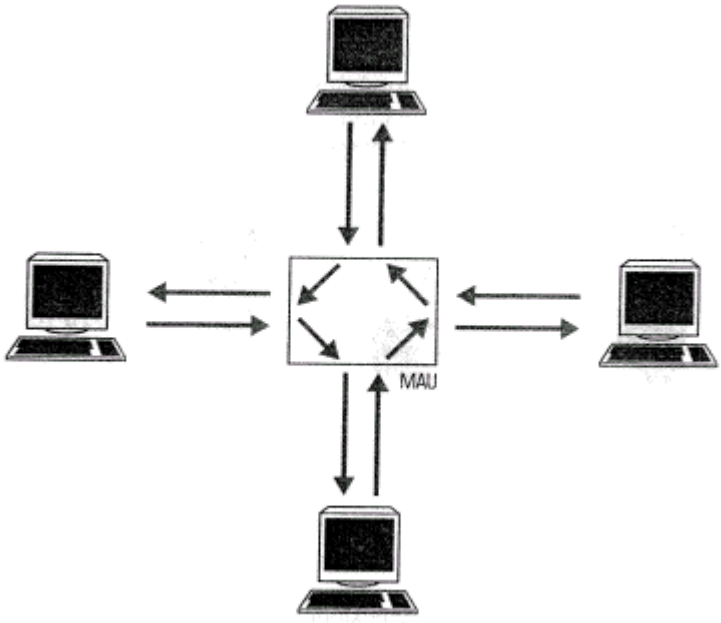


Figura 3.3 – Funcionamento interno do MAU.

4. Bibliografia

Torres, Gabriel – Redes de Computadores Curso Completo. 1ª Edição – Rio de Janeiro: Axcel Books do Brasil Editora Ltda, 2001

Arnett, Matthew Flint – Desvendando o TCP/IP. 4ª Edição – Rio de Janeiro: Editora Campus Ltda, 1997

Minasi, Mark; Anderson, Christa; Creegan, Elizabeth – Dominando o Windows NT Server 4. 1ª Edição – São Paulo: Makron Books do Brasil Editora Ltda, 1997