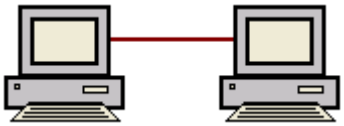
ÍNDICE – TREINAMENTO EM REDES

1 - INTRODUÇÃO

Basicamente uma rede consiste em 2 computadores interligados com o objetivo de compartilhar dados. Isso já pode ser considerado uma rede. Veja um exemplo na figura abaixo.



Este é apenas um exemplo simples, é claro que uma rede não é formada por apenas 2 computadores interligados afim de compartilhar dados e sim 2 ou mais computadores interligados. Aliás, todas as redes, não importa o quanto sejam sofisticadas, derivam desse sistema simples.

Se a idéia de dois computadores conectados por um cabo pode não parecer extraordinária, no passado representou uma grande conquista nas comunicações.

Definição: Basicamente, uma rede de trabalho é um sistema que permite a comunicação entre pontos distintos, ou seja, um sistema que permite a troca de informações. Os componentes básicos de uma rede de trabalho (ou rede de informações) são um emissor (origem da informação), o meio através da qual a informação trafega (o canal), um receptor (o destino da informação) e finalmente a mensagem, que nada mais é do que a informação em si.

Um exemplo comum seria uma pessoa falando no telefone com outra pessoa: O emissor seria quem está falando, o canal seria a linha telefônica, o receptor a pessoa que está ouvindo e a mensagem seria a própria mensagem que está sendo comunicada. Ao longo dos anos as ferramentas para a comunicação de dados foram evoluindo gradativamente, de modo a tornar a troca de informações rápida, fácil e mais eficiente.

Uma rede de computadores baseia-se nos princípios de uma rede de informações, implementando técnicas de hardware e software de modo a torná-la efetivamente mais dinâmica, para atender às necessidades que o mundo moderno impõe. Redes de computadores incluem todos os equipamentos eletrônicos necessários à interconexão de dispositivos, tais como microcomputadores e impressoras.

Esses dispositivos que se comunicam entre si são chamados de nós, estações de trabalho, pontos ou simplesmente dispositivos de rede.

Dois computadores, ou nós, seria o número mínimo de dispositivos necessários para formarmos uma rede. O número máximo não é predeterminado, teoricamente todos os computadores do mundo poderiam estar interligados.

Quanto à natureza podemos ter dois tipos de redes de computadores: cliente-servidor (client-server) e ponto-a-ponto (peer-to-peer).

Na rede cliente-servidor uma máquina, ou um pequeno grupo de máquinas, centraliza os serviços da rede oferecidos às demais estações, tais como aplicativos e filas de impressão.

As máquinas que requerem esses serviços são chamadas de clientes, e as máquinas que os fornecem são chamadas de servidores.

Na rede ponto-a-ponto não existem servidores, todas as estações compartilham seus recursos mutuamente.

A grande desvantagem que as redes ponto-a-ponto oferecem com relação às redes cliente-servidor é a dificuldade de gerenciar os seus serviços, já que não existe um sistema operacional que centralize a administração da rede.

Também não é possível estendê-las excessivamente, já que um número elevado de nós sobrecarregaria o fluxo de dados, tornando-a lenta e por conseguinte ineficaz.

Aos poucos as empresas estão substituindo suas redes ponto-a-ponto por redes cliente-servidor, e o número de redes ponto-a-ponto está diminuindo.

O principal motivo para a implementação de redes de computadores nas organizações, sejam elas simples escritórios ou empresas de âmbito internacional, resume-se em uma única palavra: dinheiro!

Os custos reduzidos com a automatização dos processos mediante a utilização de redes é realmente muito significativo.

Por exemplo, se uma empresa pudesse optar entre adquirir cem impressoras independentes ou apenas dez compartilhadas, sem dúvida alguma a segunda opção seria mais interessante.

Também é preferível adquirir o direito de compartilhar um aplicativo (chamados de pacotes para vários usuários) entre um número predeterminado de usuários, do que adquirir várias cópias unitárias.

As redes consistem em vários computadores autônomos, interligados entre si com o objetivo de se compartilhar recursos de hardware, transferência de dados e troca de mensagens entre seus usuários.

Os computadores estão ligados fisicamente através de cabos, linhas telefônicas, ondas de rádio, infravermelho.

Os tipos básicos de rede quanto à distribuição geográfica são:

LAN - Redes Locais de Computadores (Local Area Network);
MAN - Redes Metropolitanas (Metropolitan Area Network);
WAN - Redes Geograficamente Distribuídas (Wide Area Network).

LAN Redes Locais de Computadores

Este é o tipo mais comum de rede de computadores. Redes que interligam salas em um edifício comercial ou prédios de um campus universitário são exemplos de redes locais.

Até mesmo quem tem dois computadores ligados em sua própria casa possui uma rede local. No princípio a maioria das redes locais era ponto-a-ponto.

Com a expansão das redes cliente-servidor, foi viabilizado a interconexão de diferentes redes locais, dando origem às redes metropolitanas e redes remotas.

As redes locais caracterizam-se por altas taxas de transferência, baixo índice de erros e custo relativamente pequeno.

MAN Redes Metropolitanas

O conceito de rede metropolitana pode parecer um tanto quanto confuso, e algumas vezes há certa confusão no que diz respeito às diferenças existentes entre uma MAN e uma rede remota.

Na verdade, a definição para este tipo de rede de computadores surgiu depois das LANs e WANs.

Ficou estabelecido que redes metropolitanas, como o próprio nome já diz, são aquelas que estão compreendidas numa área metropolitana, como as diferentes regiões de toda uma cidade.

Normalmente redes metropolitanas são constituídas de equipamentos sofisticados, com um custo alto para a sua implementação e manutenção, que compõem a infra-estrutura necessária para o tráfego de som, vídeo e gráficos de alta resolução.

Por serem comuns nos grandes centros urbanos e econômicos, as redes metropolitanas são o primeiro passo para o desenvolvimento de redes remotas.

WAN Redes Geograficamente Distribuídas

Redes Remotas - Redes remotas são aquelas que cobrem regiões extensas. Na verdade redes remotas são um agrupamento de várias redes locais ou metropolitanas, interligando estados, países ou continentes.

Tecnologias que envolvem custos elevados são necessárias, tais como cabeamento submarino, transmissão por satélite ou sistemas terrestres de microondas.

As linhas telefônicas, uma tecnologia que não é tão sofisticada e nem possui um custo muito elevado, também são amplamente empregadas no tráfego de informações em redes remotas.

Este tipo de rede caracteriza-se por apresentar uma maior incidência de erros, e também são extremamente lentas.

Novas técnicas estão surgindo de modo a subverter esses problemas, mas a sua implementação depende de toda uma série de fatores, logo o processo é gradativo.

Um exemplo de rede remota muito popular é a *Internet*, que possibilita a comunicação entre pessoas de lugares totalmente diferentes.

Os tipos quanto aos sistemas operacionais:

- Ponto a Ponto
- Cliente-Servidor

Ponto a Ponto

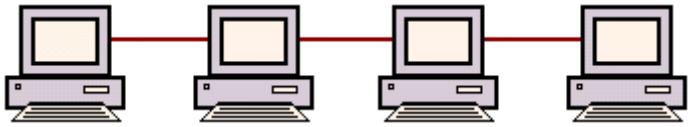
Numa rede ponto a ponto a distribuição dos dados está de forma descentralizada em todos os computadores.

Não existe uma máquina servidora de arquivos ou um gerenciamento centralizado da rede.

Todos os computadores são tratados igualmente. São redes desenhadas para pequenas ou médias redes locais.

Windows for Workgroups e a rede do Windows 95 são alguns dos exemplos de rede ponto a ponto.

A desvantagem está na falta de segurança para a arquitetura cliente/servidor.

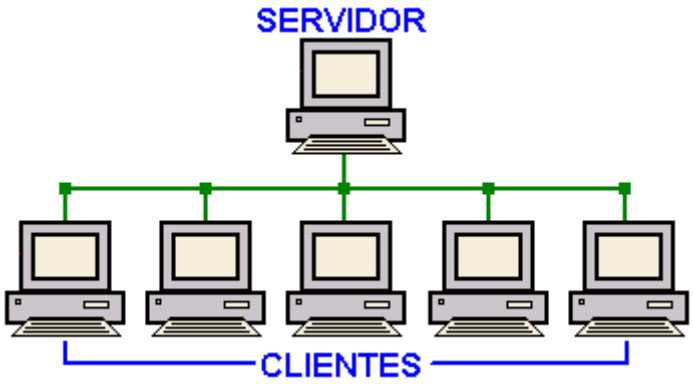


Rede ponto a ponto

Cliente-Servidor

São todos os tipos de rede que centralizam suas funções como servidor de arquivos, impressão, contas de usuários, entre outros num equipamento diferenciado tratado como servidor da rede.

As estações de trabalho acessam o servidor e os recursos que estão disponíveis neste. Dentre alguns exemplos desta arquitetura podemos citar o Novell Netware o Windows NT Server o Windows 2000 Server e o Windows 2003 Server.



Rede cliente/servidor

As vantagens desta arquitetura são:

1) Centralização dos recursos e segurança do sistema;

2) Flexibilidade: novas tecnologias podem ser facilmente integradas ao sistema;

3) Acessibilidade: diversas plataformas podem acessar remotamente o servidor.

2 - REDE DE COMPUTADORES UM POUCO DE SUA HISTÓRIA

Há tempos que o homem vem tentando fazer com que a informação circule por longas distâncias e, desta necessidade surgiram várias invenções no decorrer da história, tais como relacionadas a seguir:

- Cabo Submarino (1866)
- Telégrafo sem fio (1894)
- Corrida espacial (1957)
- Satélites artificiais a partir de1960

- Arpanet (Advanced Research Projects Agency Network) estabelecida em 1968 com a finalidade de interligar universidades visando pesquisas avançadas. É a predecessora da Internet
- E-mail (1972)
- TCP/IP (1982)
- Telenet primeira rede remota comercial (1974). Não confundir com Telnet, que é um protocolo de simulação.
- BBS (Bulletin Board System), especialmente para serviços, em 1978
- DNS (Domain Name Service), um serviço da Internet que converte nomes em números de endereçamento (1984)

ENIAC – O INÍCIO DA COMPUTAÇÃO MODERNA

Em 1946 John Mauchly e J. Presper Eckert desenvolveram o ENIAC I (**E**lectrical **N**umerical **I**ntegrator **A**nd **C**alculator).

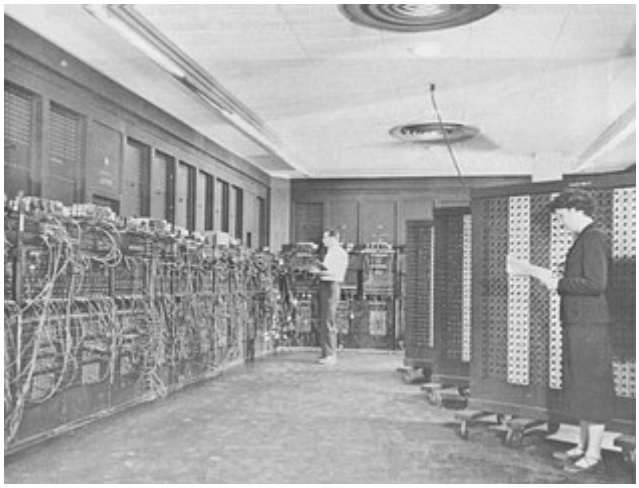
O exército dos Estados Unidos patrocinou essa pesquisa e o seu desenvolvimento, em 31 de maio de 1.943 pois necessitava na época de cálculos exatos dos processos de desempempenho do seu arsenal militar.

O projeto custou quinhentos mil dólares e ficou pronto somente dezoito meses depois, quando a guerra já tinha acabado.

Mesmo assim, o ENIAC foi utilizado para fazer os cálculos da bomba de hidrogênio.

Era composto de 17.468 válvulas, 70.000 resistores, 10.000 capacitores, 1.500 relês, 6.000 chaves manuais e 5 milhões de pontos de solda.

Ocupava uma área de 167 metros quadrados, pesava 30 toneladas e consumia 160 quilowatts e no momento em que era ligado, provocava na cidade de Filadélfia oscilações de energia.

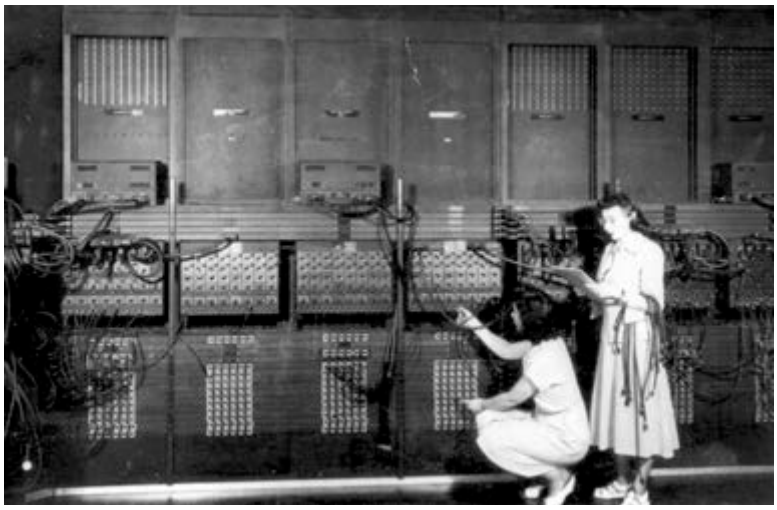


A patente do ENIAC foi concedida em 26 de junho de 1.947, com a seguinte justificativa:

"Com a necessidade nos dias de hoje de se elaborar cálculos, a velocidade tornou-se imprescindível, não havendo no mercado métodos computacionais capazes de satisfazer tal demanda".

Em um segundo, o ENIAC (que era mil vezes mais veloz do que qualquer máquina de calcular da época) podia executar 5.000 operações de soma, 357 operações de multiplicação ou 38 divisões.

Levando-se em conta que os relês e as chaves mecânicas ou manuais foram substituídas por válvulas, isto levou a um aumento da performance, no entanto, a manutenção era demorada e sua reprogramação exigia técnicos altamente competentes, tal a sua complexidade.



O lado positivo disso tudo, é que o ENIAC proporcionou um desenvolvimento tecnológico avançado para as válvulas, que na época eram os dispositivos eletrônicos mais utilizados.

Em 1948 foram feitas diversas modificações no ENIAC de tal forma a otimizar operações aritméticas e transferir essas operações simultaneamente, causando uma série de dificuldades na sua programação. Foi então introduzido o primeiro código de programação.

Com base nas experiências desenvolvidas no ENIAC foi fundada em 1.949 pelos criadores no ENIAC a Eckert-Mauchly Computer, que lançou o BINAC (BINary Automatic Computer) que usou pela primeira vez a fita magnética para armazenamento de dados.

Em 1.950 a Eckert-Mauchly Computer foi comprada pela Remington Rand Corporation, que trocou o nome para *Univac* que nada mais era do que uma divisão da Remington Rand. Isto resultou no lançamento do UNIVAC (UNIversal Automatic Computer, um importante precursor dos computadores atuais.

Em 1.955 a Remington Rand fundiu-se com a Sperry Corporation que resultou na Sperry-Rand, que mais tarde fundiu-se com a Burroughs Corporation, de onde surgiu a Unisys.

Às 23:45h do dia 2 de outubro de 1.955, o ENIAC foi definitivamente desligado.

Em 1980 J. Presper Eckert and John Mauchly receberam da IEEE (Institute of Electrical and Electronics Engineers) um prêmio pelo seu pioneirismo.

Avanços na década de 1960 possibilitaram o desenvolvimento dos primeiros terminais interativos, permitindo aos usuários acesso ao computador central através de linhas de comunicação.

Usuários passavam a ter então um mecanismo que possibilitava a interação direta com o computador, ao mesmo tempo em que avanços nas técnicas de processamento

davam origem a sistemas de tempo compartilhado (time-sharing), permitindo que várias tarefas dos diferentes usuários ocupassem simultaneamente o computador central, através de uma espécie de revezamento no tempo de ocupação do processador.

Mudanças na caracterização dos sistemas de computação ocorreram durante a década de 1970.

O desenvolvimento de minis e microcomputadores de bom desempenho, com requisitos menos rígidos de temperatura e umidade, permitiu a instalação de considerável poder computacional em várias localizações de uma organização, ao invés da anterior concentração deste poder em uma determinada área.

Embora o custo de hardware de processamento estivesse caindo, o preço dos equipamentos eletromecânicos continuava alto.

Mesmo no caso de dados que podiam ser associados a um único sistema de pequeno porte, a economia de escala exigia que grande parte dos dados estivessem associados a um sistema de grande capacidade centralizado.

Assim a interconexão entre os vários sistemas para o uso compartilhado de dispositivos periféricos tornou-se importante.

A capacidade de troca de informações também foi uma razão importante para a interconexão. Usuários individuais de sistemas de computação não trabalham isolados e necessitam de alguns dos benefícios oferecidos por um sistema centralizado.

Entre esses a capacidade de troca de mensagens entre os diversos usuários e a facilidade de acesso a dados e programas de várias fontes quando da preparação de um documento.

Ambientes de trabalho cooperativos se tornaram uma realidade tanto nas empresas como nas universidades, exigindo a interconexão dos equipamentos nessas organizações.

Para tais problemas de performance os pesquisadores a criaram novas arquiteturas que propunham a distribuição e o paralelismo como forma de melhorar desempenho, confiabilidade e modularidade dos sistemas computacionais.

3 - Topologia das Redes

Topologia de rede é a forma através da qual ela se apresenta fisicamente, ou seja, com os nós estão dispostos.

A topologia de uma rede descreve como o é o "layout" do meio através do qual há o tráfego de informações, e também como os dispositivos estão conectados a ele. São várias as topologias existentes, podemos citar:

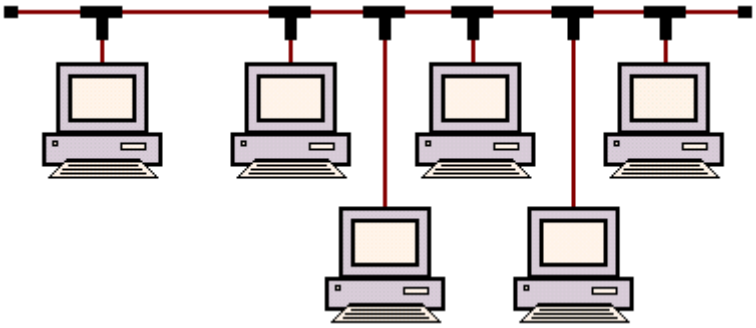
Barramento
Estrela
Anel
Malha
Híbridas

3.1 – Barramento

Esta topologia é caracterizada por uma linha única de dados (o fluxo é serial), finalizada por dois terminadores (casamento de impedância), na qual atrelamos cada nó de tal forma que toda mensagem enviada passa por todas as estações, sendo reconhecida somente por aquela que está cumprindo o papel de destinatário (estação endereçada).

Nas redes baseadas nesta topologia não existe um elemento central, todos os pontos atuam de maneira igual, algumas vezes assumindo um papel ativo outras vezes assumindo um papel passivo.

As redes locais Ethernet ponto-a-ponto usam essa topologia.



Topologia barramento

DESVANTAGENS:

1. Como todas as estações estão atreladas a uma linha única (normalmente um cabo coaxial), o número de conexões é muito grande, proporcional ao número de nós.

Logo, se a rede estiver apresentando um problema físico, são grandes as chances deste problema ser proveniente de uma dessas conexões (conectores e placas de rede) ou até mesmo de um segmento de cabo.

2. A maior dificuldade está em localizar o defeito, por conta dos vários segmentos de rede.

3. Como a troca de informações dá-se linear e serialmente, quando ocorrem tais defeitos toda a rede fica comprometida, e ela pára de funcionar.

VANTAGENS:

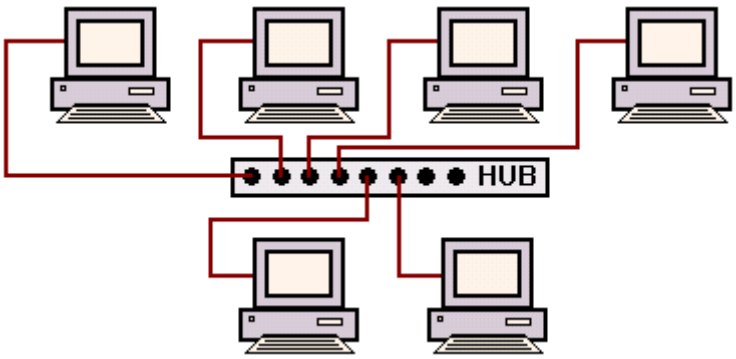
A única vantagem que este tipo de rede pode oferecer é o baixo custo, sendo ideal quando implementada em lugares pequenos.

3.2 – Estrela

A topologia estrela é caracterizada por um elemento central que "gerencia" o fluxo de dados da rede, estando diretamente conectado (ponto-a-ponto) a cada nó, daí surgiu a designação "Estrela".

Toda informação enviada de um nó para outro deverá obrigatoriamente passar pelo ponto central, ou concentrador, tornando o processo muito mais eficaz, já que os dados não irão passar por todas as estações.

O concentrador encarrega-se de rotear o sinal para as estações solicitadas, economizando tempo.



Topologia estrela

VANTAGENS:

1. Uma vez que o sinal sempre será conduzido para um elemento central, e a partir deste para o seu destino, as informações trafegam bem mais rápido do que numa rede barramento.

Essa é a melhor vantagem oferecida por uma rede estrela, sendo a mesma ideal para redes em que imperam o uso de informações "pesadas", como a troca de registros de uma grande base de dados compartilhada, som, gráficos de alta resolução e vídeo.

2. A instalação de novos segmentos não requer muito trabalho.

3. A manutenção é menos complicada, pois na rede estrela é mais fácil de visualizar os defeitos fisicamente, uma vez que se ocorrer algum problema num dos segmentos, os demais permanecerão em atividade.

4. A rede pode ser deslocada para outro ambiente sem grandes dificuldades de adaptação.

5. Oferece taxas de transmissão mais elevadas.

DESVANTAGEM:

A única desvantagem é que o custo de instalação de uma rede estrela é mais elevado.

Quanto maior for a distância entre um nó e o concentrador maior será o investimento, já que cada "braço" é representado por um segmento de cabo coaxial, par trançado ou fibra óptica, além do concentrador (Hub ou Switch) de tráfego de dados da rede.

Uma rede cliente-servidor, segue a topologia estrela.

3.3 – Anel

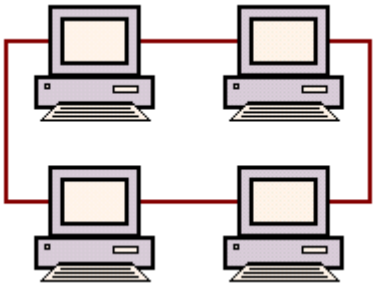
Como o nome indica, uma rede anel é constituída de um circuito fechado, tal como a rede elétrica.

A maior vantagem: não há atenuação do sinal transmitido, já que ele é regenerado cada vez que passa por uma estação (a atenuação é diretamente proporcional à distância entre um nó e outro).

A maior desvantagem: todas as estações devem estar ativas e funcionando corretamente.

A implementação mais comum da topologia estrela são as redes Token-Ring, de propriedade da IBM.

Esta topologia oferece uma taxa de transmissão maior da que é oferecida nas redes de topologia barramento, veremos melhor o seu funcionamento mais adiante.



Topologia em anel

3.4 – Híbrida

Redes híbridas são aquelas que utilizam mais de uma das topologias citadas acima, e normalmente surgem da fusão de duas ou mais LANs entre si ou com MANs.

Os serviços comerciais "on-line" e as redes públicas são exemplos de redes híbridas, como a Internet e até mesmo redes fechadas que estão sob o controle de organizações empresariais.

4 - REDES LOCAIS ETHERNET

A rede Ethernet[1] foi a primeira aplicação comercial de rede local a utilizar a topologia de barramento (bus topology).

A Ethernet é a tecnologia de rede local mais usada em todo o mundo.

Apesar do aparecimento de novas tecnologias de redes locais de alta velocidade, como ATM, FDDI, ARCnet a 20Mbps, Token Ring a 16Mbps, entre outras, a Ethernet é ainda campeã em popularidade e crescimento, agora também em duas novas versões:

Fast Ethernet
Switched Ethernet

Vários fatores pesaram no sucesso da rede Ethernet:

1. Seu custo baixo de implementação, manutenção e gerenciamento.

2. Integração de ambientes de rede Ethernet com Mainframes, com o uso de várias interfaces e programas emuladores de terminais disponíveis no mercado.

3. Disponibiliza uma taxa de transmissão de dados em redes, suficiente para a maioria das aplicações em uso atualmente.

[1] ETHERNET, padrão de rede de comunicação local, originalmente desenvolvida pela Xerox Corporation, Inc.

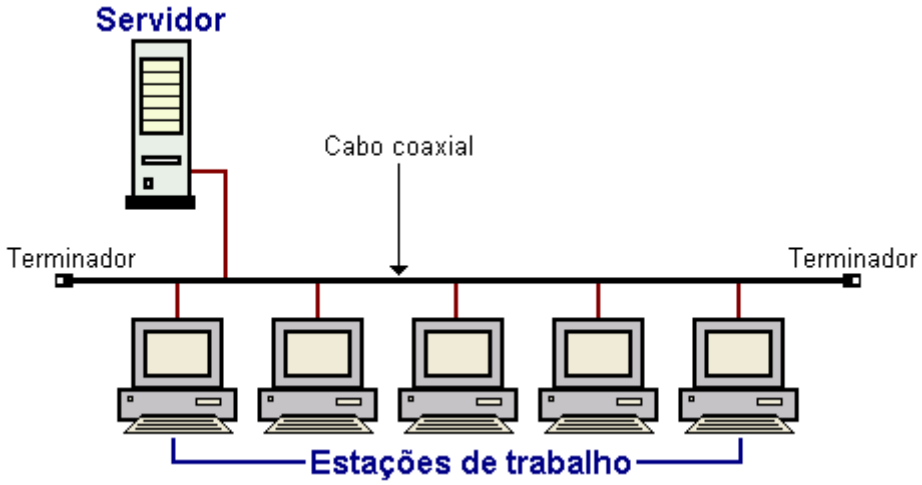
O padrão Ethernet define um método para a implementação de rede local baseado na topologia barramento.

Neste tipo de topologia o meio físico (ou cabo) está constantemente presente para todos os usuários, porém, apenas um usuário o utiliza para uma transmissão, em um dado momento.

O protocolo definido como protocolo Ethernet é definido pelo IEEE (Institute of Electrical and Electronics Engineers) como o padrão IEEE 802.3 embora não seja o proposto inicialmente pelas companhias que desenvolveram a Ethernet.

4.1 - TOPOLOGIA BARRAMENTO OU BUS:

A figura a seguir mostra a implementação de uma rede Ethernet com a topologia barramento ou bus.



Topologia em barramento

CABO COAXIAL: As redes Ethernet foram desenvolvidas para "rodar" em um tipo específico de cabo coaxial grosso (thick wire) sob uma divisão do padrão Ethernet denominado 10 BASE-5.

Este subpadrão, dividido em três partes tem o seguinte significado:

10 – refere-se à velocidade de transmissão (10Mbps)
BASE – indica que a rede é do tipo banda base
5 – especificação do meio físico (cabo coaxial grosso) com comprimento máximo de 500 metros

O 10 BASE-5 ficou conhecido como tecnologia Yellow Cable, devido a cor do cabo coaxial grosso empregado nessas redes.

Conexão: Como em qualquer rede local a conexão de cada dispositivo ou equipamento é obtida por meio de uma interface de rede denominada NIC (Network Interface Card) ou simplesmente placa de rede.

No caso do 10 BASE-5, devido as dimensões e rigidez do cabo coaxial esta conexão era feita por meio de um transceiver e uma interface AUI (Attachment Unit Interface), uma interface de conexão entre o computador e o sistema de cabeação.

O cabo AUI ou "drop cable" era um cabo fino e flexível terminado com conectores DB-15, utilizando-se nove pinos, muito semelhante aos cabos seriais RS 232C, a podia ter

um comprimento máximo de 50 metros, muito embora, raramente, essas distâncias fossem atingidas.

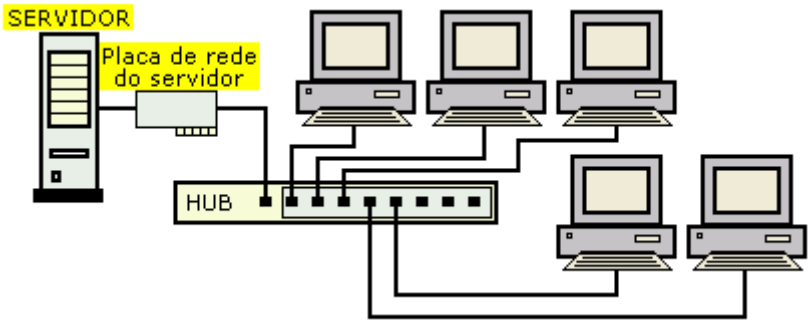
Como evolução do 10 BASE-5 foi desenvolvido o subpadrão 10 BASE-2, que representa uma rede Ethernet de banda base operando a 10Mbps, em cabo coaxial fino e comprimento máximo de 200 metros.

Assim, o 10 BASE-2 tornou a rede Ethernet em topologia de barramento de menor custo e de maior popularidade do mundo.

Devido aos problemas citados anteriormente, principalmente a dificuldade de manutenção, uma vez que um problema de conexão faz a rede toda cair, este tipo de Ethernet vem caindo em desuso há algum tempo.

4.2 - TOPOLOGIA ESTRELA:

A figura a seguir mostra uma rede Ethernet com topologia estrela, com um servidor de arquivos.



Topologia estrela

Para esta topologia o subpadrão é o 10 BASE-T (rede em banda base Ethernet a 10Mbps, que opera em cabos de pares trançados como meio físico).

Apesar de não especificado no nome do subpadrão, o comprimento máximo de cabo permitido entre as estações de trabalho nesta topologia é de 100 metros.

Observa-se na figura mostrada (topologia estrela) a presença de um elemento distribuidor do cabeamento para as estações de trabalho, denominado HUB, onde cada porta desse HUB corresponde a uma estação de trabalho.

Como a maioria dos HUBs possuem em cada porta um led indicador de atividade, isto facilita em muito a manutenção da rede. Ainda, se uma das estações parar, as demais continuam em atividade.

Os cabos originalmente utilizados para a implementação da topologia estrela foram os cabos de pares trançados de dois pares, categoria 3 (10Mbps).

Estes condutores foram largamente empregados em redes Ethernet 10 BASE-T até o advento das redes Ethernet a 100Mbps e dos cabos UTP (Unshielded Twisted Pair), categoria 5, com capacidade para suportar altas velocidades.

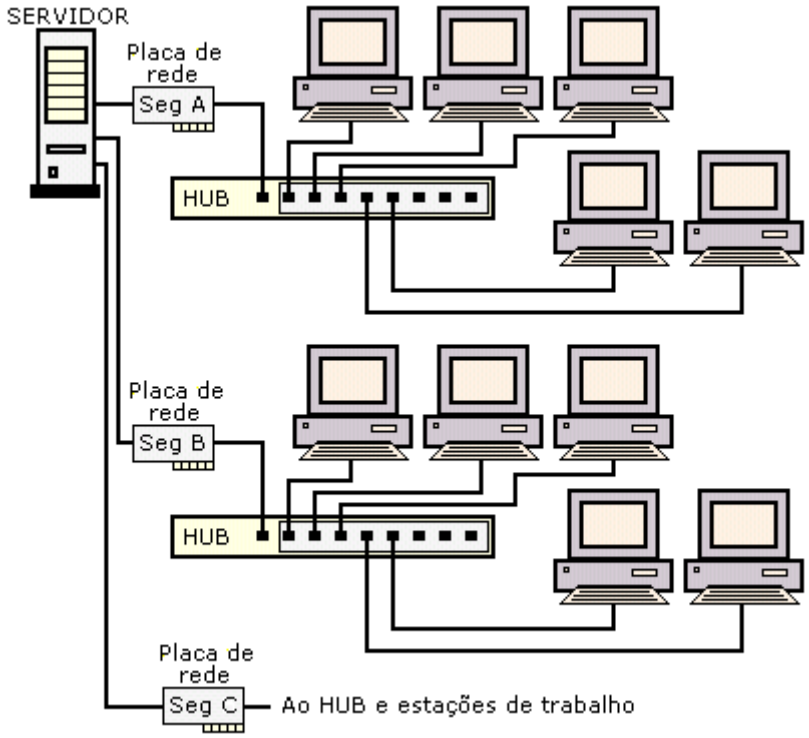
Na topologia estrela, apesar de cada estação de trabalho utilizar um segmento de cabo único com o concentrador (hub), este é conectado ao servidor por meio de um cabo, o que confere a esta configuração características de topologia de barramento.

No entanto, existem várias vantagens na implementação, como vistas anteriormente:

- Facilidade de identificação de problemas físicos no cabeamento
- Facilidade de manutenção nas estações de trabalho
- Possibilidade de gerenciamento por meio de ferramentas específicas
- Melhor organização do ambiente de rede
- Redução do downtime[2] da rede, devido a problemas físicos

Uma vez que o método de acesso ao servidor é o mesmo para ambas as topologias (barramento e estrela), um gargalo na rede será verificado com o aumento do número de estações de trabalho.

Para minimizar ou mesmo sanar esse problema, utiliza-se a técnica de segmentação, que consiste de implantação de novos barramentos, dividindo as estações de trabalho, conforme sugere a figura a seguir.



Técnicas de segmentação em redes

Observa-se que o servidor possui três placas de rede, cada uma delas representando um segmento. Com isto, obtém-se um melhor desempenho.

5 - TRÁFEGO DE DADOS NAS REDES LOCAIS ETHERNET

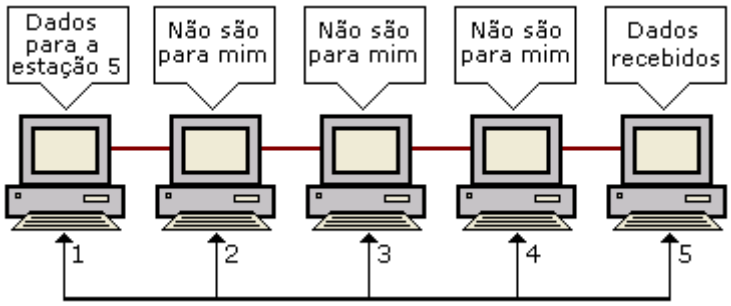
As placas de rede Ethernet são de longe as mais utilizadas atualmente, sobretudo em redes pequenas e médias.

[2] Downtime – tempo ocioso em que uma estação de trabalho pára, por motivo de manutenção

Numa rede Ethernet, temos uma topologia lógica de barramento. Isto significa que quando uma estação precisar transmitir dados, ela irradiará o sinal para toda a rede.

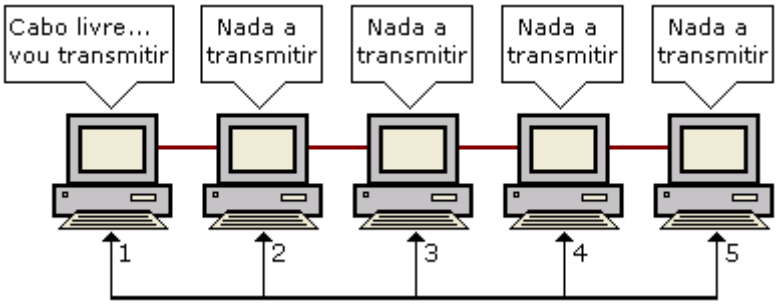
Todas as demais estações ouvirão a transmissão, mas apenas a placa de rede que tiver o endereço indicado no pacote de dados receberá os dados. As demais estações simplesmente ignorarão a transmissão.

Mais uma vez vale lembrar que apesar de utilizar uma topologia lógica de barramento, as redes Ethernet podem utilizar topologias físicas de estrela ou de barramento.



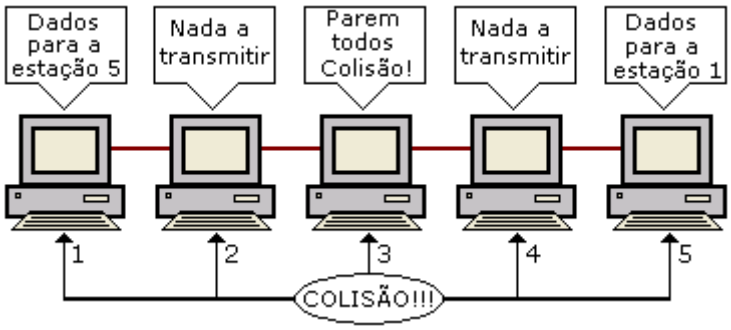
Transmissão de dados para a estação 5

Como apenas uma estação pode falar de cada vez, antes de transmitir dados a estação irá "ouvir" o cabo. Se perceber que nenhuma estação está transmitindo, enviará seu pacote, caso contrário, esperará até que o cabo esteja livre. Este processo é chamado de "Carrier Sense" ou sensor mensageiro.



Enviando o pacote Carrier Sense

Mas, caso duas estações ouçam o cabo ao mesmo tempo, ambas perceberão que o cabo está livre e acabarão enviando seus pacotes ao mesmo tempo. Teremos então uma colisão de dados.



Colisão de dados

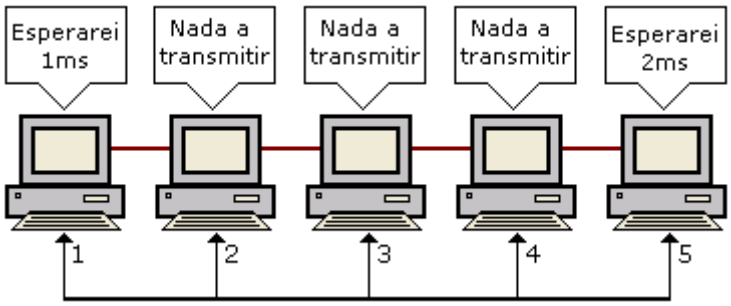
Dois pacotes sendo enviados ao mesmo tempo geram um sinal elétrico mais forte, que pode ser facilmente percebido pelas placas de rede.

A primeira estação que perceber esta colisão irradiará para toda a rede um sinal especial de alta frequência que cancelará todos os outros sinais que estejam trafegando através do cabo e alertará as demais placas que ocorreu uma colisão.

Sendo avisadas de que a colisão ocorreu, as duas placas "faladoras" (as que estão transmitindo os dados) esperarão um número aleatório de milissegundos antes de tentarem transmitir novamente.

Este processo é chamado de TBEB "Truncated Binary Exponencial Back-off". Inicialmente as placas escolherão entre 1 ou 2, se houver outra colisão escolherão entre 1 e 4, em seguida entre 1 e 8 milissegundos (ms), sempre dobrando os números possíveis até que consigam transmitir os dados.

Apesar de as placas poderem fazer até 16 tentativas antes de desistirem, normalmente os dados são transmitidos no máximo na terceira tentativa.



TBEB – Truncated Binary Exponencial Back-off

Apesar de não causarem perda ou corrupção de dados, as colisões causam uma grande perda de tempo, resultando na diminuição do desempenho da rede.

Quanto maior for o número de estações, maior será a quantidade de colisões e menor será o desempenho da rede.

Por isso existe o limite de 30 micros por segmento numa rede de cabo coaxial, e é recomendável usar bridges para diminuir o tráfego na rede caso estejamos usando topologia em estrela, com vários hubs interligados (e muitas estações).

Outro fator que contribui para as colisões é o comprimento do cabo. Quanto maior for o cabo (isso tanto para cabos de par trançado quanto coaxial) mais fraco chegará o sinal e será mais difícil para a placa de rede escutar o cabo antes de enviar seus pacotes, sendo maior a possibilidade de erro.

Usar poucas estações por segmento e usar cabos mais curtos do que a distância máxima permitida, reduzem o número de colisões e aumentam o desempenho da rede.

O ideal no caso de uma rede com mais de 20 ou 30 micros, é dividir a rede em dois ou mais segmentos, pois como vimos anteriormente, isto servirá para dividir o tráfego na rede.

É bom salientar que todo este controle é feito pelas placas de rede Ethernet. Não tem nada a ver com o sistema operacional de rede ou com os protocolos de rede usados.

6 – O MODELO "OSI"

Quando as redes de computadores surgiram, as soluções eram, na maioria das vezes, proprietárias, isto é uma determinada tecnologia só era suportada por seu fabricante.

Não havia a possibilidade de se misturar soluções de fabricantes diferentes. Dessa forma um mesmo fabricante era responsável por construir praticamente tudo na rede.

Para facilitar a interconexão de sistemas de computadores a ISO (International Standards Organization) desenvolveu um modelo de referência chamado OSI (Open Systems Interconnection), para que os fabricantes pudessem criar protocolos a partir desse modelo.

Nos Estados Unidos o representante da ISO é o ANSI (American National Standards Institute)

Interessante notar que a maioria dos protocolos existentes (como o TCP/IP o IPX/SPX e o NetBeui) tomam o modelo OSI como referência, mas não o segue ao pé da letra (como veremos esses protocolos só correspondem a partes do padrão OSI).

Todavia, o estudo deste modelo é extremamente didático, pois através dele há como entender como deveria ser um protocolo ideal, bem como facilita enormemente a comparação do funcionamento de protocolos criados por diferentes fabricantes.

O modelo de protocolos OSI é um modelo de sete camadas, apresentadas na figura a seguir. Inicia-se com a camada 1 (Física).

Modelo OSI de protocolos

Tanto o ANSI quanto o IEEE vem utilizando o modelo OSI de camadas há muito tempo, por uma boa razão: a divisão da tecnologia em diferentes camadas, permite que uma camada sofra algumas alterações sem causar problemas ao restante do modelo.

Por exemplo, o IEEE pôde acrescentar ao padrão Ethernet o uso de cabos UTP como meio físico, sem alterar o padrão.

Da mesma forma, protocolos diferentes como IPX/SPX, TCP/IP, NetBeui podem ser utilizados com o mesmo hardware, devido a cada componente formar uma camada independente, melhorando a interoperabilidade da rede.

6.1 - Camada 1 – Camada física (PHY – Physical Layer)

A camada física é representada pelas conexões e pela sinalização. O protocolo dessa camada define a sinalização elétrica, símbolos, estados de linha, requisitos de

temporização, codificação de dados e conectores para transmissão de dados e suas configurações (pinagem).

Como exemplo da camada física, podemos citar o padrão 10 BASE-T. Os hubs são dispositivos da primeira camada, pois transmitem os sinais de dados sem decodificá-los.

Todas as camadas superiores se comunicam com a camada física por meio de uma interface específica. Para o Ethernet 10 BASE-5, a interface utlizada é a AUI e um conector DB-15 pode ser usado para conectar as camadas 1 e 2.

Para a Ethernet 100Mbps, esta interface é denominada “Interface Independente do Meio” (MII – Medium Independent Interface).

A camada 1 é interfaceada com o meio pela “Interface Dependente do Meio” (MDI – Medium Interface Dependent).

Por exemplo, para Ethernet 10 BASE-T a MDI é o conector RJ-45.

6.2 - Camada 2 – Camada de link de dados (Data Link Layer)

A camada de link de dados consiste no controle de acesso à mídia (MAC – Media Access Control) e do controle do link lógico (LLC – Logical Link Control).
Como as funções do LLC ocorrem em nível superior, interessa-nos então apenas o MAC.

O controle de acesso à mídia pode ser descrito como uma estação organizada que transmite e recebe dados em um ambiente de meio físico compartilhado.

O MAC é responsável pela transferência de informações ao longo de um link, sincronizando a transmissão de dados, detecção de erros e controle de fluxo de dados.

Exemplos de MACs definidos pelo IEEE: Ethernet 802.3, Token Ring 802.5, etc.

De uma forma geral os MACs em ambiente físico compartilhado, permitem que múltiplos “nós” (workstation) podem se conectar ao mesmo canal de transmissão.

As “ bridges” (pontes) são usadas para conectar diferentes locais de mesmo tipo de MAC.

Por exemplo, um segmento Ethernet 10 BASE-2 pode ser conectado a um segmento Ethernet 10 BASE-T por meio desse dispositivo. Estes tipos de transferências de dados ocorrem em nível MAC e são denominadas funções de camada 2.

6.3 - Camada 3 – Camada de Rede (Network Layer)

A camada de rede é responsável pela conexão entre a fonte de informação e o destinatário. Redes grandes normalmente consistem de diferentes tipos de padrões MAC.

Por exemplo, uma organização pode ter uma rede Ethernet no Departamento Administrativo e uma rede Token Ring no Departamento Técnico.

O software de camada de rede deve estar apto a executar a conexão entre diferentes tipos de redes de forma otimizada. Dizemos então que, a função da camada 3 é de roteamento.

6.4 - Camada 4 – Camada de Transporte (Transport Layer)

Esta camada executa muitas tarefas em comum com a de rede, porém, em âmbito local.

Os drivers do software da rede executam tarefas da camada de transporte uma vez que, se houver uma interrupção na rede por qualquer motivo, o software da camada de transporte procurará rotas alternativas, ou irá gravar os dados transmitidos em local seguro, até que ocorra o restabelecimento.

Essa camada é responsável pelo controle de qualidade da comunicação, cuidando para que os dados recebidos estejam no formato correto.

Os recursos de formatação e ordenação são importantes quando os programas da camada de transporte estabelecem conexões em computadores de concepções diferentes.

A camada link de dados poderá contar as mensagens para verificar se estão todas lá. A camada de transporte abre as mensagens e verifica se há falhas.

As redes com computadores de concepções diferentes podem utilizar muitos protocolos de camada de transporte e um dos mais utilizados é o TCP (Transmission Control Protocol), o qual é adotado por muitas empresas como parte do protocolo TCP/IP.

Os componentes de software que operam na camada de transporte estão contidos nas estações de rede e estabelecem a chamada entre os programas aplicativos da rede. As principais aplicações que estabelecem comunicações pela camada de transporte são os programas de gateway de rede.

Exemplos de produtos usados em redes de PCs com funções da camada 4:

NetBIOS
Named Pipes
IPX (Internetwork Protocol Exchange)

6.5 - Camada 5 – Camada de sessão (Session Layer)

A camada de sessão é muito importante em redes locais com computadores pessoais, pois cabe a ela funções que permitem a comunicação entre duas aplicações (ou dois componentes da mesma aplicação) pela rede, dentre as quais: de segurança, de reconhecimento de nome, de conexão, de administração, etc.

Programas como o NetBIOS e o Named Pipes ignoram muitas vezes o padrão ISO e executam as funções da camada de transporte e da camada de sessão.

Em vista disso, torna-se difícil citar o nome de um software específico para a camada 5, porém, existe um protocolo desenvolvido pela ISO, que é o ISO 8327, denominado *Connection – Oriented Session Protocol Specification* para tal fim. O que não se sabe ao certo, é se esse protocolo está sendo utilizado pelos softwares de rede disponíveis no mercado.

6.6 - Camada 6 – Camada de apresentação (Presentation Layer)

Esta camada é responsável pela forma que as informações são entregues aos usuários, podendo também tratar da criptografia e de alguns formatos especiais de arquivos.

É responsável também pela formatação de tela e de arquivos de modo que, o produto final tenha a apresentação que o programados deseja.

Na camada de apresentação estão os códigos de controle, os gráficos especiais e o conjunto de caracteres.

6.7 - Camada 7 – Camada de aplicação (Application Layer)

A camada superior serve ao usuário, e nela estão contidos o sistema operacional da rede e os programas aplicativos.

Em suma, está contido os programas aplicativos que o usuário pode controlar: compartilhamento de arquivos, criação de spools de impressão, correio eletrônico e até a criação e o gerenciamento de banco de dados.

6.8 - NDIS e ODI

Criado pela Microsoft e pela 3Com, o **NDIS** (Network Driver Interface Specification) é um driver instalado no sistema operacional que permite que uma única placa de rede possa utilizar mais de um protocolo de rede ao mesmo tempo.

O driver **NDIS** possui duas partes. A primeira é chamada driver MAC **NDIS**, que é o driver da placa de rede (que deve ser escrito usando o padrão **NDIS**). A segunda parte é chamada vector.

Essa camada é que permite que uma mesma placa de rede possa usar mais de um protocolo, já que o driver da placa de rede (driver MAC **NDIS**) só permite uma única conexão. Quando um quadro é recebido pelo driver da placa de rede, ele o passa para a camada vector, que o envia para o primeiro protocolo, que poderá aceitar ou rejeitar o pacote.

Caso primeiro protocolo rejeite o quadro, a camada vector entrega o quadro ao segundo protocolo. Esse processo continua até que um dos protocolos instalados aceite o quadro ou então todos o tenha rejeitado.

Outra finalidade da especificação **NDIS** é possibilitar a existência de mais de uma placa de rede em um mesmo micro. Muitas vezes esse procedimento é necessário para ligar um mesmo micro a dois segmentos de rede diferentes.

Em princípio, sem o **NDIS**, com duas placas de rede em um mesmo micro seriam necessárias duas pilhas de protocolos completas, uma para cada placa de rede (isto é, seguindo o modelo OSI seriam necessários protocolos completos com sete camadas para cada placa de rede instalada).

Com o **NDIS**, um única pilha de protocolos é compartilhada (isto é, as camadas 4, 5, 6 e 7 do modelo OSI) com todas as placas de rede instaladas, já que o que existir acima da camada vector poderá ser compartilhado por todas as placas de rede.

O **ODI** (Open Datalink Interface) é um driver com o mesmo objetivo que o **NDIS**, criado pela Novell e pela Apple para os seus sistemas operacionais, só que com um funcionamento um pouco mais complexo e mais completo.

A grande diferença entre o **NDIS** e o **ODI** é o uso da camada Controle de Link Lógico (LLC) que não é usada no **NDIS**. No **NDIS** há a camada vector, que possui

funcionamento similar, porém funciona de maneira diferente. No modelo **ODI** essa camada é chamada Camada de Suporte ao Link (Link Support Layer).

Neste modelo são adicionadas duas interfaces, uma chamada interface para Múltiplos Protocolos (MPI - Multi Protocol Interface), que faz a interface entre a Camada de Suporte ao Link e os drivers das placas de rede instaladas. Os drivers da placa de rede compatíveis com o padrão **ODI** são chamados MLID ou Multiple Link Interface Driver.

A principal diferença entre o **NDIS** e o **ODI** é que, como a camada de Controle do Link Lógico ou Camada de Suporte ao Link, como chamada no **ODI**, possui um campo de endereçamento de protocolos, tanto o transmissor quanto o receptor sabem qual é o protocolo que está sendo usado no dado que foi encapsulado dentro do quadro.
Com isso, ao receber um quadro, a interface de múltiplos protocolos (MPI) entrega diretamente os dados para o protocolo responsável.

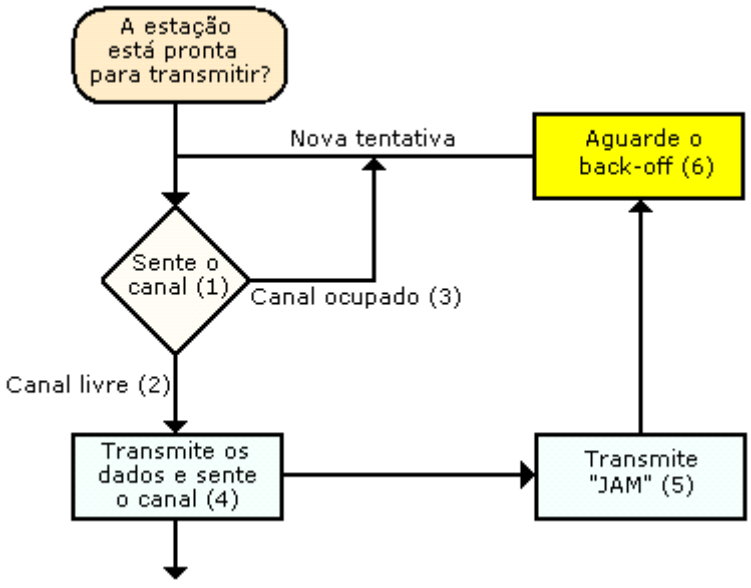
No **NDIS**, quando um quadro chega, a camada vector tenta encaminhar o quadro para cada um dos protocolos instalados, até um deles aceitar (ou todos rejeitarem), já que não há o campo do endereçamento.

A existência da Interface para Múltiplos Links (MLI) permite a instalação de mais de uma placa de rede na máquina, tendo as vantagens que já foram explicadas no **NDIS**, isto é, as duas placas de rede podem compartilhar os protocolos existentes acima desta camada.

7 – CONTROLE DE ACESSO À MÍDIA (MAC) E CSMA/CD

A Ethernet é baseada no modelo OSI e em vista disso o mecanismo de controle de acesso à mídia – MAC (Media Access Control) pode ser facilmente combinado com diferentes meios físicos. Os padrões de MAC mais importantes para a Ethernet são o 10 BASE-2 e o 10 BASE-T.

A tecnologia MAC Ethernet denominada Carrier Sense Multiple Access with Collision Detection ou CSMA/CD trabalha de forma muito similar a conversação humana. O fluxograma do CSMA/CD é mostrado na figura a seguir:



Fluxograma do CSMA/CD

1. **Carrier-sense:** a estação que precisa transmitir um pacote de informação tem que se assegurar de que não há outros nós ou estações utilizando o meio físico compartilhado. Assim, primeiramente a estação "ouve" ou "sente" o canal antes da transmissão.
2. Se o canal estiver livre por um certo período de tempo denominado IFG (Interframe Gap), a estação pode iniciar a transmissão.
3. Se o canal estiver ocupado, ele será monitorado continuamente até se tornar livre por um período de tempo mínimo de IFG. Então a transmissão será iniciada (nova tentativa).
4. **Collision detection:** uma colisão pode ocorrer se duas ou mais estações iniciam a transmissão ao mesmo tempo. Esta colisão destrói os pacotes de dados destas estações. A Ethernet monitora continuamente o canal durante uma transmissão para detectar colisões.
5. Se uma estação detecta uma colisão durante a transmissão, esta é imediatamente interrompida. Um sinal de congestionamento (JAM)[3] é enviado ao canal para garantir que todas as estações detectem a colisão e rejeitem qualquer pacote de dados que possam estar recebendo, pois pode haver erros no mesmo.
6. **Multiple access:** após um período de espera (back-off), uma nova tentativa de transmissão é feita pelas estações que precisam transmitir. Um algoritmo de back-off determina um atraso de modo que, diferentes estações tenham que esperar tempos diferentes antes que uma nova tentativa de transmissão seja feita novamente.

7.1 - Pacotes de dados nas redes Ethernet

Todos os dados transmitidos através da rede, são divididos em pacotes.

A estação emissora escuta o cabo, transmite um pacote, escuta o cabo novamente, transmite outro pacote e assim por diante. A estação receptora por sua vez, vai juntando os pacotes até ter o arquivo completo.

O uso de pacotes evita que uma única estação monopolize a rede por muito tempo, e torna mais fácil a correção de erros.

Se por acaso um pacote chegar corrompido, devido a interferências no cabo, ou qualquer outro motivo, será solicitada uma retransmissão do pacote, assim, quanto pior for a qualidade do cabo e maior for o nível de interferências, mais pacotes chegarão corrompidos e terão que ser retransmitidos e, consequentemente, pior será o desempenho da rede.

Os pacotes Ethernet 802.3 são divididos em 7 campos:

Preâmbulo	SFD	Endereço Destino	Endereço Fonte	Gênero e tamanho do campo	DADOS	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 - 1500 bytes	4 bytes

Estrutura de frame (campos) Ethernet 802.3

- **PREÂMBULO (Preamble):**

O preâmbulo é composto de 7 bytes[4] e serve para sincronizar a transmissão dos dados entre transmissor e receptor.

[3] congestionamento; processo ou mecanismo que foi interrompido devido a uma falha;
[4] 1 byte é uma unidade de informação básica composta de 8 bits

- **SFD (Start of Frame Delimiter):**
  Composto por 1 byte, indica que um frame de MAC está prestes a iniciar.

- **ENDEREÇO DE DESTINO (Destination Address):**
  Especifica para onde o frame está sendo enviado

- **ENDEREÇO FONTE (Source Address):**
  Denota o equipamento que inicia a transmissão. Cada nó ou estação tem um endereço único.

Os três primeiros do endereço são chamados de Bloco ID e identificam o fabricante do equipamento, sendo estes determinados pelo IEEE. Os outros três são chamados de Device ID e são determinados pelo fabricante.

Estes são sempre únicos, ou seja não existem por exemplo, teoricamente, placas de rede com endereços MAC iguais.

- **GÊNERO E TAMANHO DO CAMPO (Type/Lenght Field):**
  Especifica o tipo de campo ou frame.

Se for menor ou igual a 1500 decimal (0x5DC), trata-se de um pacote 802.3 e se for maior do que 1500 trata-se de um pacote DIX (DEC/Intel/Xerox) Ethernet V2.

Por exemplo, 0x0800 indica que o campo Ethernet contém um pacote IP (Internet Protocol)

- **DADOS (Data Field):**
  Varia de 46 a 1500 bytes, onde 46 bytes é a mínima condição para o CSMA/CD.

- **CRC (Cyclic Redundancy Check) ou Checksum:**
  Verifica frames ou campos inválidos, de modo a assegurar a confiabilidade da transmissão.

8 – PROTOCOLOS DE REDE E DE COMUNICAÇÃO

Os protocolos consistem num conjunto de regras que determinam como se procede a comunicação entre computadores na rede.

Estas regras definem as características da rede, tais como: tipos de cabos, velocidade de transferência, métodos de acesso ao meio, distribuição das topologias físicas permitidas na rede.

Os protocolos mais comuns são:

- **Ethernet**
- **Fast Ethernet**
- **LocalTalk**
- **Token Ring**
- **FDDI**

8.1 - Ethernet

É o protocolo de rede mais usado. Utiliza um método de acesso chamado CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Este é um sistema onde cada computador "escuta" o cabo antes de enviar algum dado pela rede, se a rede estiver livre então o computador poderá transmitir.

Caso algum outro computador queira transmitir e o cabo já esteja sendo utilizado, então este comutador irá esperar até que o cabo fique desocupado e tentar novamente quando a linha estiver livre.

Se ocorrer o fato em que dois computadores tentem transmitir no mesmo instante então ocorrerá uma colisão e a rede ficará for por um curtíssimo tempo até que seja liberado o tráfego para então poder transmitir.

Entretanto o atraso causado pelas colisões e retransmissões é muito curto e normalmente não faz efeito na velocidade de transmissão na rede. As topologias usadas para este protocolo são do tipo barramento ou estrela. O tipo de cabeamento é de par trançado, coaxial ou fibra ótica e a velocidade de transmissão é de 10 Mbps.

8.2 - Fast-Ethernet

É um novo conceito do padrão Ethernet, diferenciando-se pela velocidade de tráfego na rede que é de 100Mbps. São necessários cabos de fibra ótica ou par trançado categoria 5.

Não há possibilidade de se usar o cabo coaxial devido à sua velocidade de transmissão que é de no máximo 10Mbps.

Além disto a rede precisa de hubs, placas de rede que suportem a velocidade de 100Mbps.

8.3 - Local Talk

É uma rede desenvolvida pela Apple Computers para computadores Macintosh. O método de acesso é o CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

Semelhante ao CSMA/CD com exceção que o sinal está preparado para transmitir antes mesmo que seja feita a transmissão, ou seja, a rede é inicialmente pré-alocada em intervalos de tempo para a transmissão, ao terminar o tempo pré alocado para cada estação, então outra estação poderá transmitir sem probabilidade de colisão.

Adaptadores de rede e cabos par trançado especiais são usados para conectar uma série de computadores de um extremo a outro numa porta serial.

O Sistema Operacional Macintosh permite o estabelecimento de uma rede ponto-a-ponto sem a necessidade de software adicional.

Com a versão Server da AppleShare, uma rede cliente/servidor pode ser feita.

A topologia de rede aplicável a este protocolo pode ser barramento ou estrela utilizando par trançado. A grande desvantagem deste protocolo é a sua velocidade que é de somente 230 Kbps.

8.4 - Token Ring

Desenvolvido pela IBM em meados de 1980, utiliza-se do método de acesso de passagem de símbolo ou anel lógico.

Os computadores somente são conectados após o sinal ter passado por todos os computadores da rede; esta "volta" do sinal forma um anel lógico.

Um sinal elétrico dá as características do anel de um computador para o outro, se um computador não tem nada a transmitir ele então simplesmente passa o sinal para a próxima estação.

Quando um computador deseja transmitir uma determinada informação a uma outra estação qualquer ele então anexa os dados ao sinal juntamente com o endereço da estação a ser enviada e então a estação que recebeu os dados, absorve-os e envia um sinal de resposta de recebimento dos dados à estação que o enviou inicialmente, sendo assim, após a estação ter recebido o sinal de resposta ela reenvia um sinal "limpo" em que outras estações poderão transmitir normalmente.

Utiliza topologia anel com par trançado ou fibra ótica. Devido à crescente popularidade do padrão Ethernet, o uso do Token Ring tem diminuído.

8.5 - FDDI

FDDI (Fiber Distributed Data Interface), interconecta duas ou mais redes locais, frequentemente cobrindo longas distâncias.

O método de acesso envolve a passagem de sinal, usa topologia física de duplo anel.

A transmissão ocorre em um dos anéis, entretanto caso uma parada ou quebra ocorra, o sistema mantém a informação automaticamente usando porções do segundo anel para, então criar um anel completo.

A maior vantagem no FDDI está na velocidade. Usa somente fibra ótica com velocidade de 100Mbps.

PROTOCOLO	CABEAMENTO	VELOCIDADE	TOPOLOGIA
ETHERNET	Par trançado, cabo coaxial ou fibra ótica	10Mbps	Barramento ou estrela
FAST ETHERNET	Par trançado ou fibra ótica	100Mbps	Estrela
LOCAL TALK	Par trançado	230Kbps	Barramento ou estrela
TOKEN RING	Par trançado ou fibra ótica	4 – 16Mbps	Anel
FDDI	Fibra ótica	100Mbps	Duplo anel

8.6 - Camadas da rede (Protocolos de Comunicação)

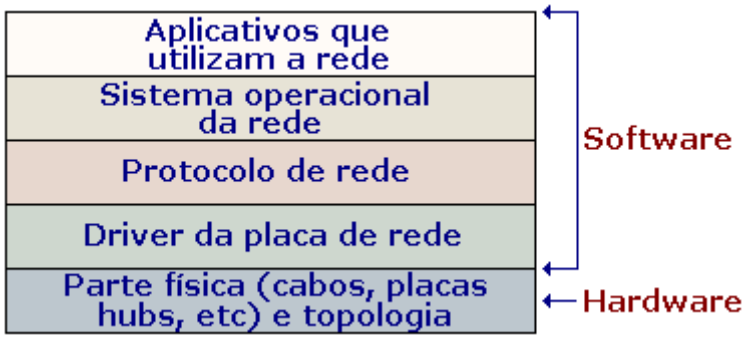
Uma rede é formada por várias camadas.

Primeiro temos toda a parte física da rede, incluindo os cabos, hubs e placas de rede.

Ainda na parte física temos a topologia lógica da rede que, como vimos, é determinada pela própria placa de rede.

Em seguida, temos o driver da placa rede que é fornecido pelo fabricante e permite que o sistema operacional possa acessar a placa de rede, atendendo às solicitações do protocolo de rede, o sistema operacional de rede e finalmente os programas.

A primeira camada é física (hardware), e as demais são lógicas (software).



Camadas de uma rede

Atualmente são usados basicamente 4 protocolos de rede, especificamente para a comunicação de dados, incluindo a transmissão e recepção: o NetBEUI, o IPX/SPX, o DLC e o TCP/IP. Cada um com suas características próprias.

Um protocolo é um conjunto de regras que definem como os dados serão transmitidos; como será feito o controle de erros e retransmissão de dados; como os computadores serão endereçados dentro da rede etc.

Um micro com o protocolo NetBEUI instalado, por exemplo, só será capaz de se comunicar através da rede com outros micros que também tenham o protocolo NetBEUI.

É possível que um mesmo micro tenha instalado vários protocolos diferentes, tornando-se assim um "poliglota".

Graças aos protocolos, também é possível que computadores rodando diferentes sistemas operacionais de rede, ou mesmo computadores de arquiteturas diferentes se comuniquem, basta apenas que todos tenham um protocolo em comum.

8.7 - NetBEUI

O NetBEUI é uma espécie de "vovô protocolo", pois foi lançado pela IBM no início da década de 80 para ser usado junto com o IBM PC Network, um micro com configuração semelhante à do PC XT, mas que podia ser ligado em rede. Naquela época, o protocolo possuía bem menos recursos e era chamado de NetBIOS.

O nome NetBEUI passou a ser usado quando a IBM estendeu os recursos do NetBIOS, formando o protocolo complexo que é usado atualmente.

No jargão técnico atual, usamos o termo "NetBEUI" quando nos referimos ao protocolo de rede em si e o termo "NetBIOS" quando queremos nos referir aos comandos deste mesmo protocolo usado pelos programas para acessar a rede.

Ao contrário do IPX/SPX e do TPC/IP, o NetBEUI foi concebido para ser usado apenas em pequenas redes, e por isso acabou tornando-se um protocolo extremamente simples.

Por um lado, isto fez que ele se tornasse bastante ágil e rápido e fosse considerado o mais rápido protocolo de rede durante muito tempo. Para você ter uma idéia, apenas as versões mais recentes do IPX/SPX e TCP/IP conseguiram superar o NetBEUI em velocidade.

Mas, esta simplicidade toda tem um custo: devido ao método simples de endereçamento usado pelo NetBEUI, podemos usa-lo em redes de no máximo 255 micros.

Além disso, o NetBEUI não suporta enumeração de redes (para ele todos os micros estão ligados na mesma rede).

Isto significa, que se você tiver uma grande Intranet, composta por várias redes interligadas por roteadores, os micros que usarem o NetBEUI simplesmente não serão capazes de enxergar micros conectados às outras redes, mas apenas os micros a que estiverem conectados diretamente. Devido a esta limitação, dizemos que o NetBEUI é um protocolo "não roteável"

Apesar de suas limitações, o NetBEUI ainda é bastante usado em redes pequenas, por ser fácil de instalar e usar, e ser razoavelmente rápido. Porém, para redes maiores e Intranets de qualquer tamanho, o uso do TCP/IP é muito mais recomendável.

8.8 - IPX/SPX

Este protocolo foi desenvolvido pela Novell, para ser usado em seu Novell Netware.

Como o Netware acabou tornando-se muito popular, outros sistemas operacionais de rede, incluindo o Windows passaram a suportar este protocolo. O IPX/SPX é tão rápido quanto o TPC/IP (apesar de não ser tão versátil) e suporta roteamento, o que permite seu uso em redes médias e grandes.

Apesar do Netware suportar o uso de outros protocolos, incluindo o TPC/IP, o IPX/SPX é seu protocolo preferido e o mais fácil de usar e configurar dentro de redes Novell.

Você já deve ter ouvido muito a respeito do Netware, que é o sistema operacional de rede cliente - servidor mais utilizado atualmente.

Além do módulo principal, que é instalado no servidor, é fornecido um módulo cliente, que deve ser instalado em todas as estações de trabalho, para que elas ganhem acesso ao servidor.

Além da versão principal do Netware, existe a versão Personal, que é um sistema de rede ponto a ponto, que novamente roda sobre o sistema operacional.

Esta versão do Netware é bem fácil de usar, porém não é muito popular, pois o Windows sozinho já permite a criação de redes ponto a ponto muito facilmente.

8.9 - DLC

O DLC é um protocolo usado por muitas instalações Token Ring para permitir a comunicação de PCs com nós de interconexão de mainframe.

Alguns modelos antigos de JetDirects da HP, assim como alguns poucos modelos de impressoras de rede também só podem ser acessados usando este protocolo.

Apesar de ser necessário instala-lo apenas nestes dois casos, o Windows oferece suporte ao DLC, bastando instala-lo junto com o protocolo principal da rede.

8.10 - TCP/IP

Uma das principais prioridades dentro de uma força militar é a comunicação.

No final da década de 60, esta era uma grande preocupação do DOD, Departamento de Defesa do Exército Americano: *como interligar computadores de arquiteturas completamente diferentes, e que ainda por cima estavam muito distantes um do outro, ou mesmo em alto mar, dentro de um porta aviões ou submarino?*

Após alguns anos de pesquisa, surgiu o TCP/IP, abreviação de "Transmission Control Protocol/Internet Protocol" ou Protocolo de Controle de Transmissão/Protocolo Internet.

O TPC/IP permitiu que as várias pequenas redes de computadores do exército americano fossem interligadas, formando uma grande rede, embrião do que hoje conhecemos como Internet.
O segredo do TCP/IP é dividir a grande rede em pequenas redes independentes, interligadas por roteadores.

Como apesar de poderem comunicar-se entre si, uma rede é independente da outra; caso uma das redes parasse, apenas aquele segmento ficaria fora do ar, não afetando a rede como um todo.

No caso do DOD, este era um recurso fundamental, pois durante uma guerra ou durante um ataque nuclear, vários dos segmentos da rede seriam destruídos, junto com suas respectivas bases, navios, submarinos, etc., e era crucial que o que sobrasse da rede continuasse no ar, permitindo ao comando coordenar um contra ataque.

Mesmo atualmente este recurso continua sendo fundamental na Internet, se por exemplo, o servidor do Yahoo cair, apenas ele ficará inacessível.

Apesar de inicialmente o uso do TPC/IP ter sido restrito a aplicações militares, com o passar do tempo acabou tornando-se de domínio público, o que permitiu aos fabricantes de software adicionar suporte ao TCP/IP aos seus sistemas operacionais de rede.

Atualmente, o TPC/IP é suportado por todos os principais sistemas operacionais, não apenas os destinados a PCs, mas a todas as arquiteturas, inclusive mainframes, minicomputadores e até mesmo celulares e handhelds.

Qualquer sistema com um mínimo de poder de processamento, pode conectar-se à Internet, desde que alguém crie para ele um protocolo compatível com o TCP/IP e aplicativos www, correio eletrônico etc.

Alguns exemplos de sistemas operacionais que suportam o TCP/IP são: o MS-DOS, Windows 3.11, Windows 95/98/NT/2000/XP, Netware, MacOS, OS/2, Linux, Solaris, a maioria das versões do Unix, BeOS e vários outros.

Voltando à história da Internet, pouco depois de conseguir interligar seus computadores com sucesso, o DOD interligou alguns de seus computadores às redes de algumas universidades e centros de pesquisa, formando uma inter-rede, ou Internet.

Logo a seguir, no início dos anos 80, a NFS (National Science Foundation) dos EUA, construiu uma rede de fibra ótica de alta velocidade, conectando centros de supercomputação localizados em pontos chave nos EUA e interligando-os também à rede do DOD.

Essa rede da NSF, teve um papel fundamental no desenvolvimento da Internet, por reduzir substancialmente o custo da comunicação de dados para as redes de computadores existentes, que foram amplamente estimuladas a conectar-se ao backbone[5] da NSF, e consequentemente, à Internet.

A partir de abril de 1995, o controle do backbone (que já havia se tornado muito maior, abrangendo quase todo o mundo através de cabos submarinos e satélites) foi passado para o controle privado.

Além do uso acadêmico, o interesse comercial pela Internet impulsionou seu crescimento, chegando ao que temos hoje.

9 – EQUIPAMENTOS PARA REDES E APLICAÇÕES

9.1 - REPETIDORES

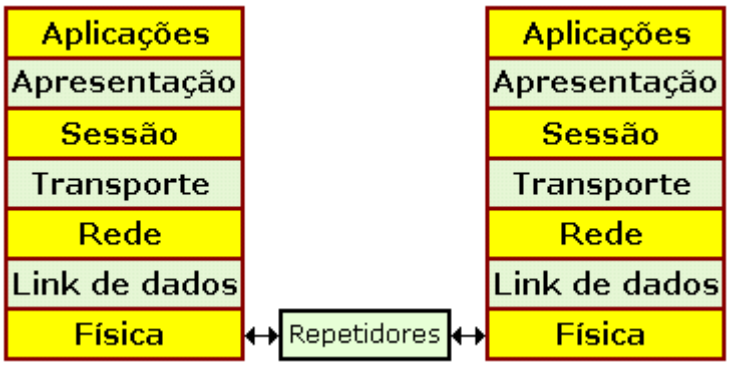
São dispositivos normalmente de baixo custo, que servem para aumentar a distância entre dois pontos, de maneira a preservar a integridade da informação que passa por eles.

Quando se deseja aumentar a distância dos segmentos de redes locais (LANs), utiliza-se repetidor regenerativo. Um repetidor regenerativo é como o próprio nome diz, um dispositivo para regenerar sinais caso estes sofram atenuações.

Os repetidores são transparentes para os demais dispositivos da rede e problemas devidos ao overhead[6] bem como o jitter[7] podem ocorrer.

Por isso, a adição de repetidores em um sistema deve obedecer critérios; os repetidores trabalham apenas na camada física do modelo OSI.

A figura a seguir representa um usuário (1) comunicando-se com outro usuário (2) por meio de um repetidor regenerativo, em relação ao modelo OSI.



Repetidores e o modelo OSI

Outros dispositivos que operam em redes na camada física do modelo OSI são os MODEMs limitados em distância – LDM (Limited Distance Modem) as Unidades de Serviço de Canal (CSU – Channel Service Unite) e as Unidades de Serviço de Dados (DSU – Data Service Unit).

Os LDMs também denominados drivers de linha são utilizados para aumentar a distância de circuitos físicos, ou seja, os LDMs são MODEMs que operam como repetidores.

[5] Backbone - infra-estrutura fisica central da Internet, redes principais que conectam redes menores à Internet
[6] Overhead - perda de dados por excesso de repetição
[7] Jitter - rápida variação de um sinal devido a perturbações elétricas

9.2 - HUBs

Os hubs ou concentradores são dispositivos que conectam vários segmentos de rede local, estações de trabalho e servidores ao meio físico.

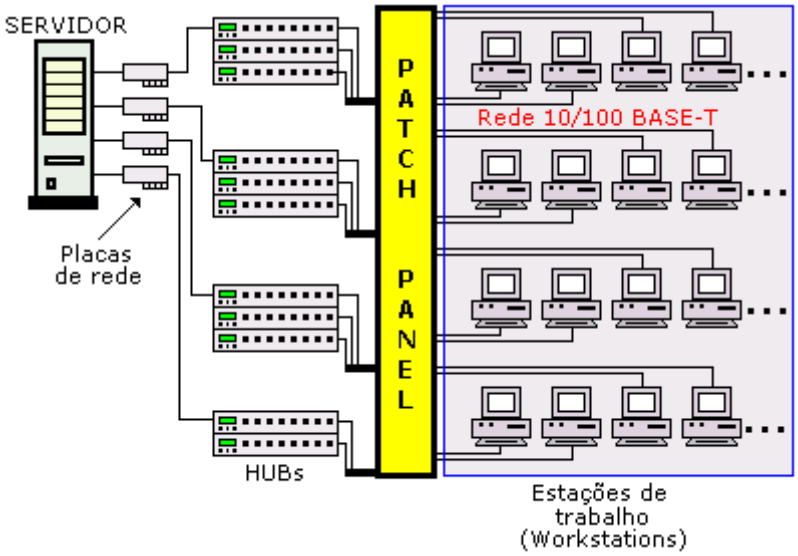
A aplicação mais simples e comum dos hubs é a conexão de várias estações de trabalho, dotadas de placas de rede compatíveis com o mesmo meio físico dos hubs.

Esse meio físico é geralmente composto de cabos de pares trançados (UTP), embora alguns tenham interfaces para outras mídias.

A quantidade de estações de trabalho que podem ser conectados ao hub depende da quantidade de portas do mesmo (em geral de 8 a 48 portas).

No entanto a conexão de muitas estações de trabalho a um hub e a conexão deste a um segmento de rede simples, pode resultar em muitas colisões com prejuízo na transmissão de dados.

A figura a seguir mostra uma aplicação típica dos hubs, com segmentação de rede, concentrada em um painel de distribuição (Patch Panel).



Aplicação típica dos HUBs

Observe na figura mostrada anteriormente (aplicação típica dos hubs) que os hubs estão empilhados.

Estes hubs são denominados hubs “stackable” (empilháveis) e são os mais utilizados em redes locais.

Desta forma, uma rede pode começar com um número pequeno de estações e, para acompanhar o crescimento da rede, coloca-se um em cima do outro, formando assim uma pilha.

Quando os hubs são empilhados eles são interligados por uma interface stack específica, de modo que todas as suas portas continuem disponíveis para os usuários da rede.

Além disso, em redes com hubs stackable gerenciáveis, apenas um hub da pilha precisa ser o agente de gerenciamento SNMP (Simple Network Management Protocol –

Protocolo de Administração Simples da Rede) que, por meio deste todos os demais hubs da pilha passam a ser gerenciáveis.

Assim, podemos dizer que uma pilha de 5 hubs com 16 portas ligados na configuração stack, com apenas um deles com o agente SNMP, se comporta como um único hub gerenciável de 80 portas.

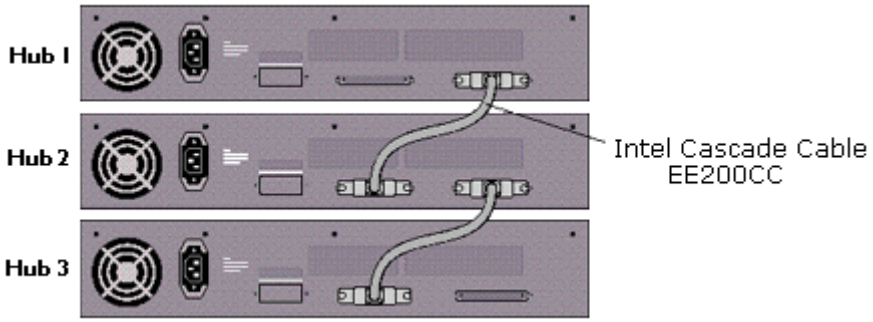
A quantidade de hubs que podem ser empilhados para formar uma única rede lógica, depende de cada fabricante.

No entanto, pilhas muito grandes de hubs em um único segmento de rede não é muito interessante, pois apenas uma estação de trabalho pode acessar o meio físico (CSMA/CD) e isto, devido ao congestionamento, pode prejudicar o funcionamento da rede.

Alguns fabricantes já estão disponibilizando hubs inteligentes, que oferecem a possibilidade de criação de multi-segmentos de rede dentro de uma única pilha de hubs, ou seja, hubs individuais podem ser agrupados em um número de segmentos em função da especificação do fabricante.

Este artifício permite a melhora do desempenho da rede, principalmente em virtude da drástica redução do congestionamento.

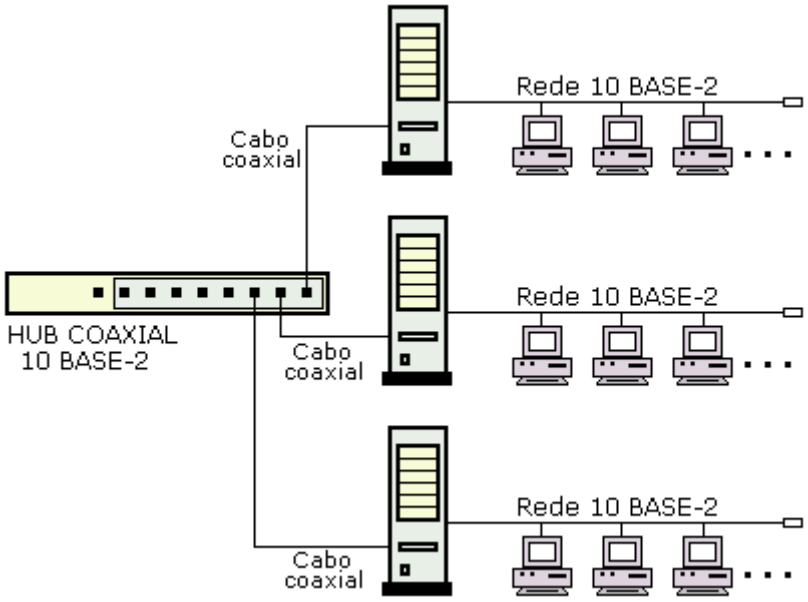
A figura a seguir, mostra 3 hubs ligados em cascata.



Hubs ligados em cascata (visto por trás)

GERAÇÕES DE HUBs:

A primeira geração de hubs Ethernet apareceu por volta de 1.984. Estes hubs eram do tipo coaxial e eram utilizados para conectar vários segmentos de rede local, conforme ilustra a figura a seguir.



Uso típico do hub coaxial 10 BASE-T

Nesta configuração, o hub está sendo utilizado simplesmente como repetidor.

Os hubs são usualmente empregados na topologia estrela, ocupando sempre o centro de uma rede local, com os dispositivos desta conectados diretamente a eles.

A segunda geração de hubs para redes locais apareceu com a mesma arquitetura da primeira, porém com algumas facilidades de gerenciamento local e remoto dos segmentos de rede a ele conectados, além de permitir a interligação de arquiteturas diferentes de redes locais, como a Ethernet e Token Ring.

A terceira geração de hubs é a dos hubs inteligentes. Estes hubs, além dos recursos dos da segunda geração, oferecem também as funções de ponte (bridge[8]). Os hubs inteligentes são gerenciáveis por meio de um agente SNMP (Simple Network Management Protocol).

A quarta geração de hubs é a dos switch-hubs.
Esses hubs são também denominados switches[9], oferecendo todas as vantagens das gerações anteriores, incluindo switching[10] em nível de MAC, funções de pontes transparentes e interfaces com a WAN.

9.3 - SWITCHES

Os switches são divididos em quatro classes:

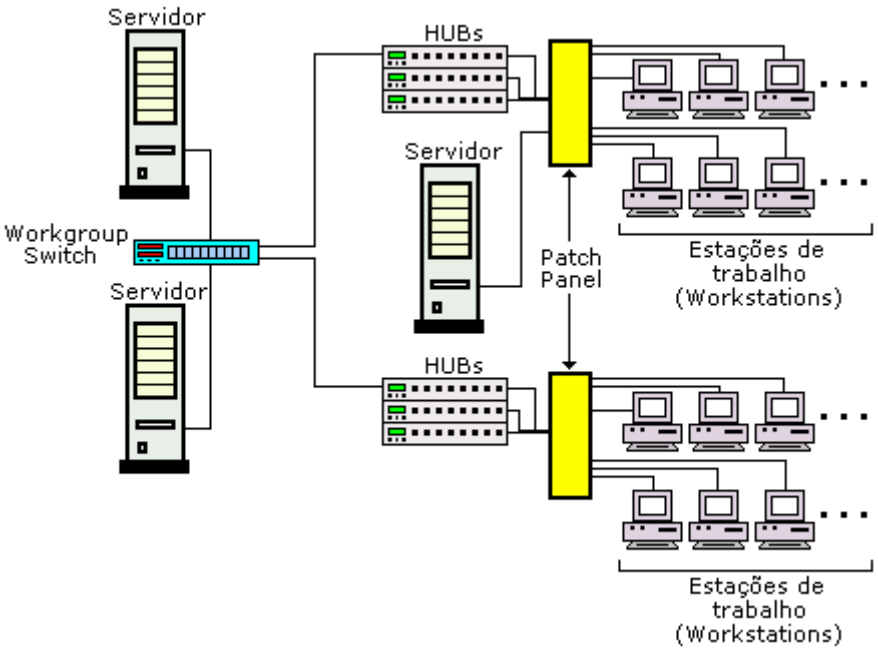
- **Workgroup switch**
- **Enterprise switch**
- **Backbone switch**
- **Edge switch**

[8] Bridge – dispositivo que coordena o tráfego de dados entre os segmentos de uma rede; estes segmentos deverão ter um endereço de rede em comum
[9] Switch – dispositivo que abre ou fecha circuitos e seleciona caminhos
[10] Switching – ação de comutação

Os workgroups switches e os enterprise switches são os mais utilizados em ambientes de redes locais.

Os workgroups switches em uma LAN isolam grupos específicos de usuários dentro de uma LAN, com um servidor próprio além daqueles que são utilizados por toda a rede.

A figura a seguir ilustra uma aplicação do workgroup switch, onde se observa que em uma das redes existe um servidor próprio.



Workgroup switch

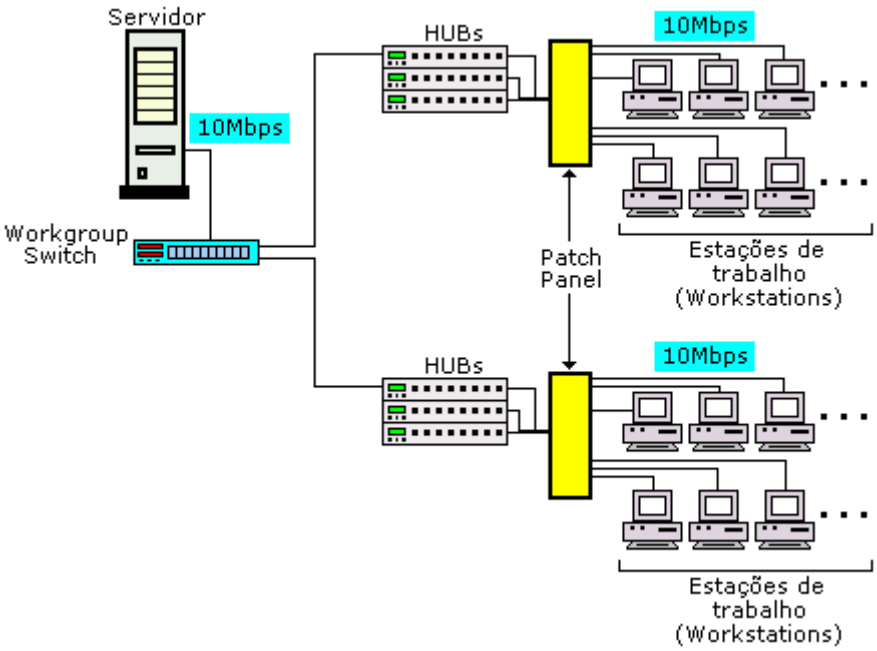
Observa-se na figura acima que o switch está sendo usado também para segmentar a rede, pois mais de um servidor está sendo utilizado pela mesma.

Não é aconselhável utilizar switches para a função exclusiva de segmentação, pois todas as estações de trabalho de todos os hubs conectados ao switch estarão concorrendo a um segmento único de rede para acessar o servidor.

A figura a seguir mostra uma forma de ligação do switch com a finalidade exclusiva de segmentação da rede.

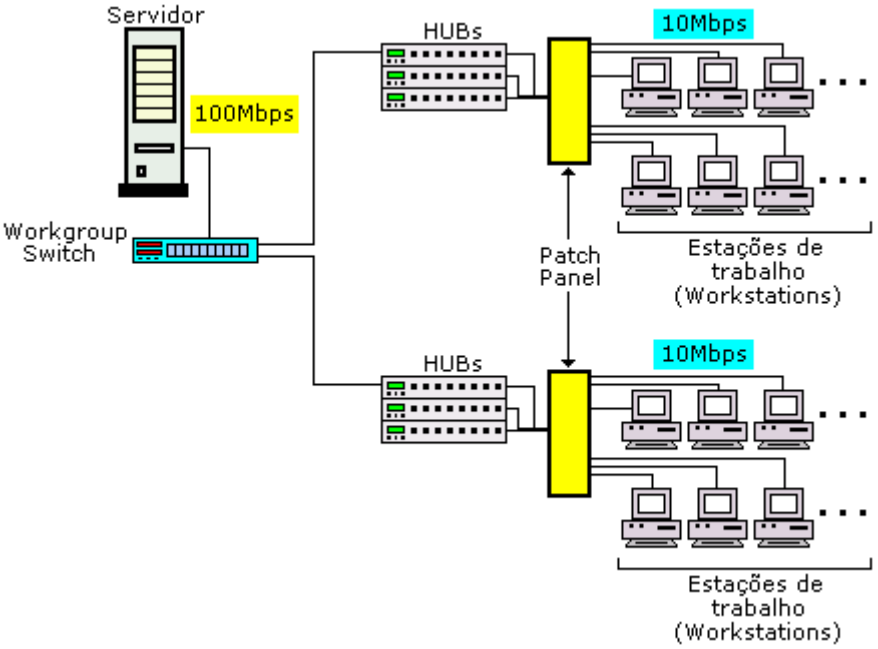
Esse arranjo não é recomendável, pois com toda a rede operando a uma velocidade única, por exemplo 10Mbps, um gargalo se formará no segmento que conecta o switch ao servidor.

O único benefício que essa configuração poderá trazer é se o segmento que interliga o servidor ao switch operar a uma velocidade maior do que a da rede, que está sendo segmentada.



Segmentação de rede com switch (1)

A arranjo mostrado na figura acima (1) não é recomendável devido ao gargalo que se formará no segmento que interliga o servidor ao switch, pois a velocidade desse segmento é igual da rede toda.

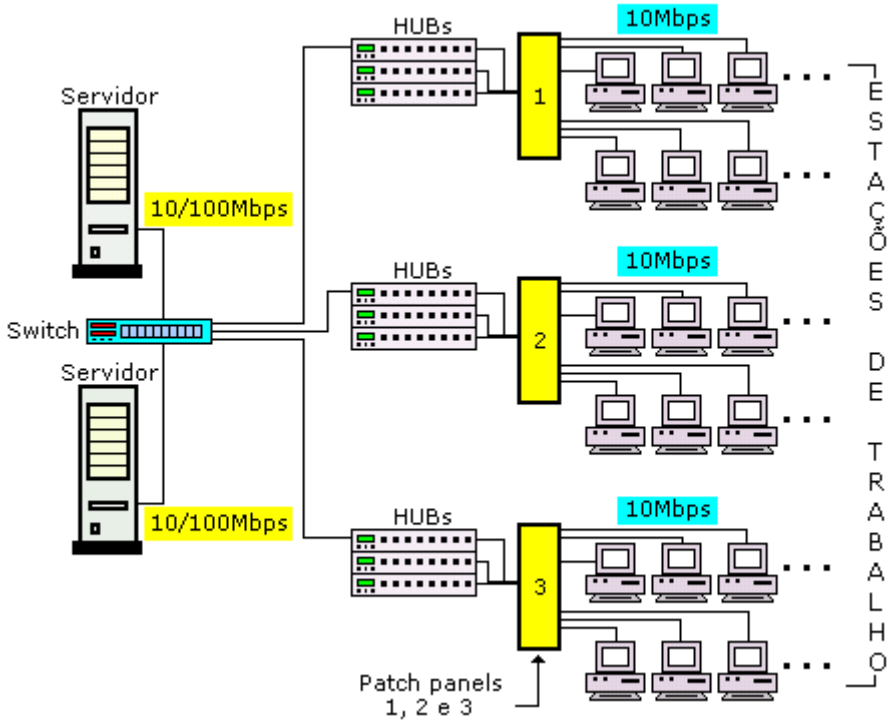


Segmentação de rede com switch (2)

O arranjo mostrado na figura anterior (segmentação de rede com switch - 2) é mais vantajoso uma vez que o link de alta velocidade entre o servidor e o switch (100Mbps) proporcionará a diminuição do gargalo entre eles.

Embora esta aplicação dos switches seja muito comum na prática, deve-se salientar que, a melhor maneira de segmentar uma rede com um único servidor é a adição de placas de rede a este.

A figura a seguir mostra uma aplicação típica de um switch em uma LAN, onde as portas do switch que conectam os servidores podem operar tanto na mesma velocidade da rede, como numa velocidade superior.



Aplicação típica do switch em uma LAN

DIFERENÇA BÁSICA ENTRE SWITCHES E HUBs:

O hub comporta-se como um repetidor, ou seja, a informação contida em uma porta qualquer do hub é repetida para todas as portas do mesmo.

O switch é um hub com endereçamento de portas.

Em cada porta do switch há um endereço único, desta forma, a informação endereçada a uma das portas do switch estará presente somente nessa porta, deixando as demais livres para tratamento dos dispositivos a ela conectados.

No caso de uma rede com mais de um servidor (conforme ilustra a figura acima), o desempenho da rede é melhorado, pois cada servidor será conectado a uma porta específica do switch, assim como os hubs, podendo ser acessados simultaneamente pelas estações de trabalho.

UTILIZAÇÃO DOS SWITCHES:

a) *Workgroup switches*: conforme visto anteriormente esses switches são utilizados em uma LAN para isolar grupos específicos de usuários, por exemplo, usuários da rede A, rede B, etc.

b) *Enterprise switches*: interligam os workgroups switches, em outras palavras, conectam vários departamentos ou grupos de usuários.

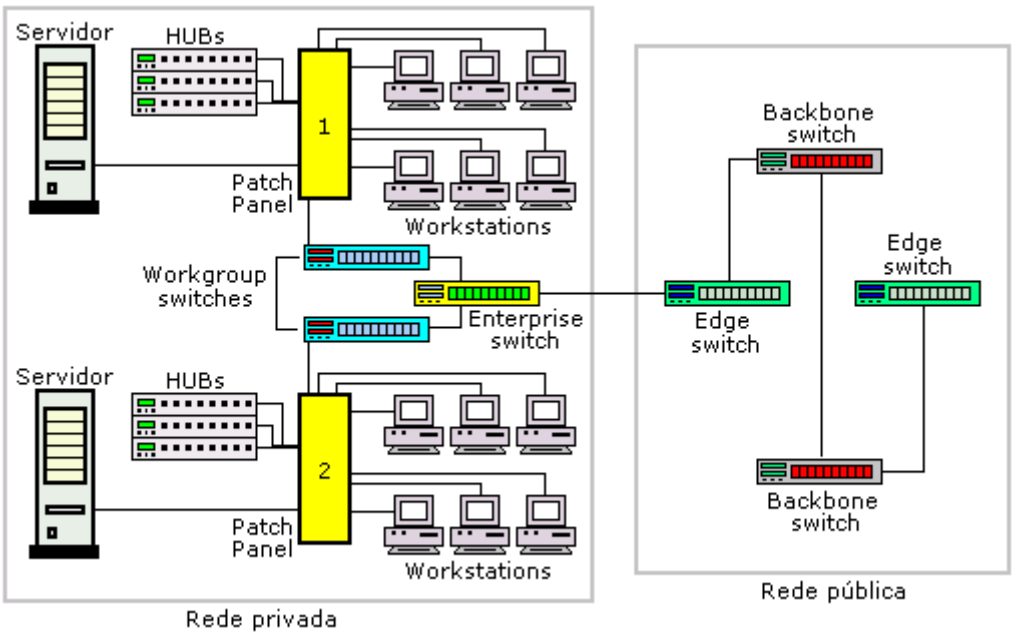
c) *Edge switches*: são utilizados como acesso a serviços públicos de dados

d) *Backbone switches*: atuam como dispositivos de interligação de alta velocidade para os edge switches.

Os switches são dispositivos orientados à conexão. As interfaces entre usuário e switch são referenciadas como UNI (User to Network Interface) e as conexões entre os switches são feitas por um protocolo “interswitch”.

As redes são interligadas entre switches por meio de uma interface denominada NNI (Network to Network Interface).

A figura a seguir mostra um diagrama das classes de switches. Observe que existe uma interligação entre uma rede privada e uma rede pública.



Classes de switches

A figura a seguir mostra um switch workgroup de 8 portas, 10/100.

A figura a seguir mostra um hub/switch de uso geral, com 24 portas.

9.4 - PONTES (BRIDGES)

Supondo que em uma empresa existam duas redes; uma rede Ethernet, e outra rede Token Ring.

Apesar das duas redes possuírem arquiteturas diferentes e incompatíveis entre si, é possível instalar nos PCs de ambas um protocolo comum, como o TCP/IP por exemplo.

Com todos os micros de ambas as redes falando a mesma língua, resta apenas quebrar a barreira física das arquiteturas de rede diferentes, para que todos possam se comunicar.

É justamente isso que um bridge faz. É possível interligar todo o tipo de redes usando bridges, mesmo que os micros sejam de arquiteturas diferentes, Macintosh de um lado e PC do outro, por exemplo, contanto que todos os micros a serem conectados utilizem um protocolo comum.

Antigamente este era um dilema difícil, mas atualmente isto pode ser resolvido usando o TCP/IP.

FUNCIONAMENTO:

Imagine duas redes, uma Ethernet e outra Token Ring, interligadas por um bridge.

O bridge ficará entre as duas, escutando qualquer transmissão de dados que seja feita em qualquer uma das duas redes.

Se um micro da rede A transmitir algo para outro micro da rede A, o bridge ao ler os endereços de fonte e destino no pacote, perceberá que o pacote se destina ao mesmo segmento da rede e simplesmente ignorará a transmissão, deixando que ela chegue ao destinatário através dos meios normais.

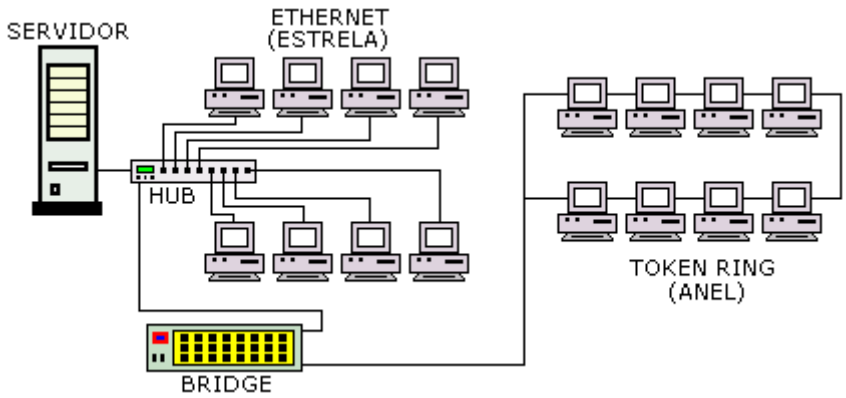
Se, porém, um micro da rede A transmitir algo para o micro da rede B, o bridge detectará ao ler o pacote que o endereço destino pertence ao outro segmento, e encaminhará o pacote.

Portanto uma característica importante de um bridge é a sua habilidade de filtrar dados.

Existem basicamente quatro tipos de bridges:

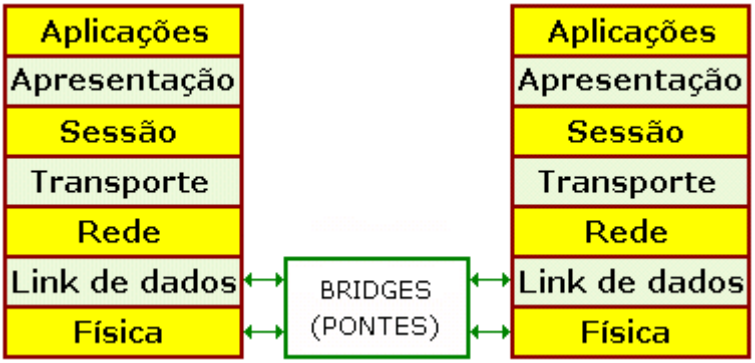
1) bridge transparente
2) bridge de translação ou conversão de mídia
3) bridge de encapsulamento
4) bridge de roteamento

A figura a seguir mostra um bridge conectando duas redes (Ethernet e Token Ring).



Interligação Ethernet/Token Ring

A figura a seguir ilustra os bridges em relação ao modelo OSI. Os bridges conectam dispositivos utilizando camadas física e de link de dados.



As pontes (bridges) em relação ao modelo OSI

No caso de uma rede muito grande, que esteja tornando-se lenta devido ao tráfego intenso, poderá ser utilizado um bridge para dividir a rede em duas, dividindo o tráfego pela metade.

Existem também alguns bridges mais simples (e mais baratos) que não são capazes de distinguir se um pacote se destina ou não ao outro lado da rede.

Eles simplesmente encaminham tudo, aumentando desnecessariamente o tráfego na rede.

Estes bridges, que são chamados de bridges de encaminhamento, servem para conectar redes diferentes, mas não para diminuir o tráfego de dados. A função de bridge também pode ser executada por um PC com duas placas de rede, corretamente configuradas.

9.5 - ROTEADORES (ROUTERS)

Os roteadores são dispositivos destinados a interconectar LANs com WANs e MANs.

São largamente utilizados quando há necessidade de interligação de redes com protocolos diferentes.

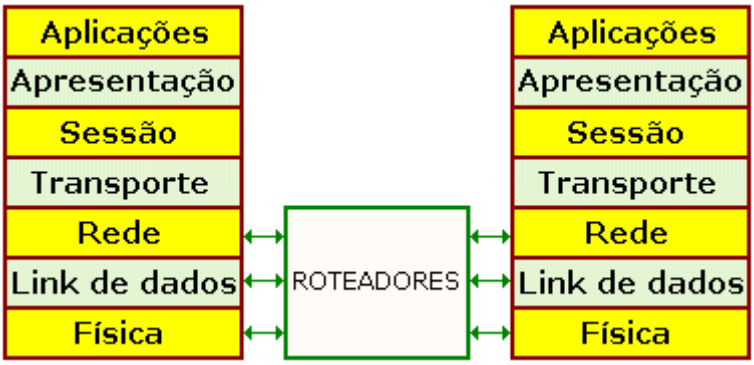
Assim, os roteadores suportam vários dispositivos de redes locais podendo empregar uma grande variedade de protocolos entre redes e esquemas de endereçamento.

Os roteadores são providos de inteligência para entender uma rede inteira, de tal forma a rotear as informações baseadas em vários fatores, proporcionando a essas informações e melhor caminho para atingir seu destino.

Por esse motivo os roteadores são largamente empregados na Internet.

Os roteadores operam nas camadas “física”, “link de dados” e “rede” do modelo OSI.

No entanto, a funcionalidade principal dos roteadores está na camada “link de dados”.



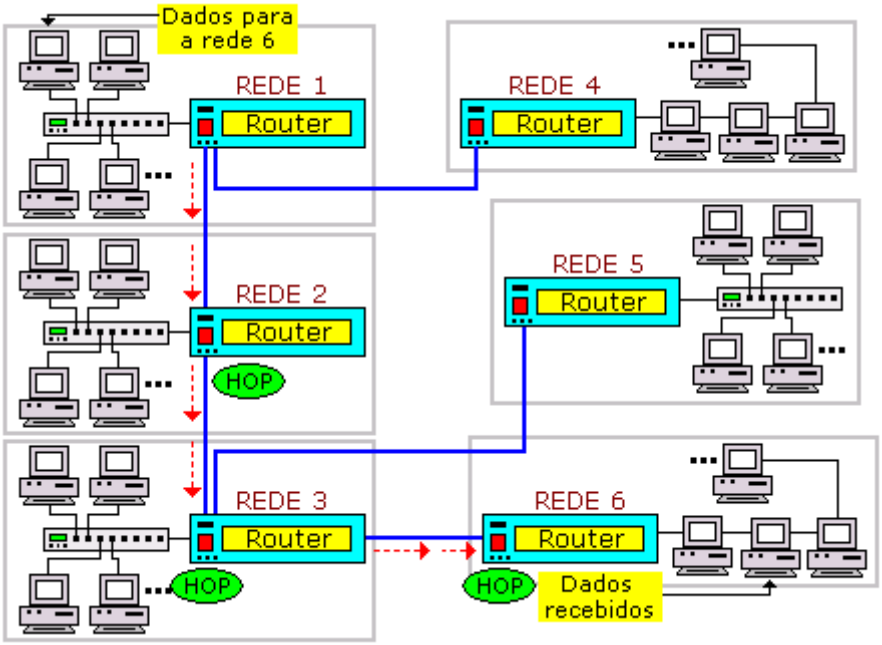
Roteadores em relação ao modelo OSI

A figura a seguir mostra um roteador sem fio.

Os roteadores não precisam suportar o mesmo protocolo de rede local ou protocolos até a camada 3, no entanto, precisam utilizar o mesmo protocolo deste a camada quatro até a camada sete do modelo OSI.

Os roteadores utilizam seus próprios protocolos entre redes, e por isso retém inteligência artificial que nada mais é do que o conhecimento dinâmico da rede inteira, podendo com isso identificar topologias.

Com isso, cria tabelas dinâmicas de modo a oferecer um roteamento que pode limitar o número de contagem de hops[11]; daí sua grande utilidade na Internet.



[11] Hops – (Internet) um dos muitos nós de uma rede de computadores nos quais uma mensagem é transferida de um ponto para outro; cada vez que um dado é transmitido de um roteador para outro forma-se um hop.

Roteadores e hops

A figura acima ilustra um processo de roteamento entre seis redes, onde se observa que os dados da estação 1 para a estação 6, passam por três roteadores, formando assim 3 hops.

A Internet é na verdade uma rede gigantesca, formada por várias sub-redes interligadas por roteadores.

Todos os usuários de um pequeno provedor, por exemplo, podem ser conectados à Internet por meio do mesmo roteador.

Para baixar uma página do Google por exemplo, o sinal deverá passar por vários roteadores, várias dezenas em alguns casos.

Se todos estiverem livres, a página será carregada rapidamente. Porém, se alguns estiverem congestionados pode ser que a página demore vários segundos, ou mesmo minutos antes de começar a carregar.

O tempo que um pedido de conexão demora para ir até o servidor destino e ser respondido é chamado de "Ping". Você pode medir os pings de vários servidores diferentes usando o prompt do MS-DOS.

Estando conectado à Internet basta digitar:

ping endereço de destino

Exemplo: **ping** www.uol.com.br ou **ping** 207.167.207.78

Outra ferramenta útil tanto para medir o tempo de resposta de um servidor qualquer, quanto para verificar por quantos e quais roteadores o sinal está passando até chegar lá é o **NeoTrace Pro 3.25.**

CONCLUSÃO:

Os bridges servem para conectar dois segmentos de rede distintos, transformando-os numa única rede.

Os roteadores por sua vez, servem para interligar duas redes separadas.

A diferença é que usando roteadores, é possível interligar um número enorme de redes diferentes, mesmo que situadas em países ou mesmo continentes diferentes.

Cada rede possui seu próprio roteador e os vários roteadores são interligados entre si.

Os roteadores são mais espertos que os bridges, pois não lêem todos os pacotes que são transmitidos através da rede, mas apenas os pacotes que precisam ser roteados, ou seja, que se destinam à outra rede.

Por este motivo, não basta que todos os micros usem o mesmo protocolo, é preciso que o protocolo seja roteável.

Apenas o TCP/IP e o IPX/SPX são roteáveis, ou seja, permitem que os pacotes sejam endereçados à outra rede. Portanto, não é possível utilizar o protocolo NetBEUI nos roteadores.

9.6 - PLACAS DE REDE (NIC – Network Interface Card)

Para que o microcomputador possa ser conectado ao meio físico, para ter acesso a todos os recursos da rede (servidor de arquivos, estações de trabalho) é necessário que o mesmo seja interfaceado com o meio.

Para isso utilizam-se placas de rede que são instaladas em um slot interno de cada micro que compõe a rede, fazendo com que ele se torne uma estação de trabalho da mesma.

Quanto à taxa de transmissão, temos placas Ethernet de 10 e 100Mbps placas Token Ring de 4 e 16Mbps.

Como vimos anteriormente, devemos utilizar cabos adequados à velocidade da placa de rede. Usando placas Ethernet de 10Mbps por exemplo, devemos utilizar cabos de par trançado de categoria 3 ou 5, ou então cabos coaxiais.

Usando uma placas de 100Mbps o requisito mínimo é a utilização de cabos de par trançado (UTP) categoria 5.

No caso de redes Token Ring, os requisitos são cabos de par trançado, por exemplo, categoria 3.

Devido às exigência de uma topologia em estrela das redes Token Ring, nenhuma placa de rede Token Ring suporta o uso de cabos coaxiais.

Cabos diferentes exigem encaixes diferentes na placa de rede. O mais comum em placas Ethernet, é a existência de dois encaixes, uma para cabos de par trançado e outro para cabos coaxiais.

Muitas placas mais antigas, também trazem encaixes para cabos coaxiais do tipo grosso (10Base5), conector com um encaixe bastante parecido com o conector para joysticks da placa de som.

Placas que trazem encaixes para mais de um tipo de cabo são chamadas placas combo. A existência de 2 ou 3 conectores serve apenas para assegurar a compatibilidade da placa com vários cabos de rede diferentes. Naturalmente, somente um conector poderá ser usado de cada vez.

As placas de rede que suportam cabos de fibra óptica, são uma exceção, pois possuem encaixes apenas para cabos de fibra. Estas placas também são bem mais caras, de 5 a 8 vezes mais do que as placas convencionais por causa do CODEC, o circuito que converte os impulsos elétricos recebidos em luz e vice-versa que ainda é extremamente caro.

Finalmente, as placas de rede diferenciam-se pelo barramento utilizado. Atualmente podem ser encontradas no mercado placas de rede ISA e PCI usadas em computadores de mesa e placas PCMCIA, usadas em notebooks e handhelds.

Existem também placas de rede USB que vem sendo cada vez mais utilizadas, apesar de ainda serem bastante raras devido ao preço salgado.

Naturalmente, caso o PC possua slots PCI, é recomendável comprar placas de rede PCI pois além de praticamente todas as placas PCI suportarem transmissão de dados a

100Mbps (todas as placas de rede ISA estão limitadas a 10Mbps devido à baixa velocidade permitida por este barramento), as mesmas poderão ser usadas muito mais tempo, já que o barramento ISA vem sendo cada vez menos usado em placas mãe mais modernas e deve gradualmente desaparecer futuramente das placas mães.

Placa de rede Ethernet PCI

Placa de rede Ethernet ISA

Placa de rede PCMCIA

O microcomputador e a placa de rede podem trocar informações pelo bus de dados deste por meio de algumas técnicas diferentes.

a) I/O[12] programada: o processador da placa de rede controla uma quantidade compartilhada de memória e se comunica com o processador do computador por meio de I/O.

Nesta técnica os dados são transferidos para o mesmo bloco de memória, gravando e lendo os dados ou informações com rapidez. Esta técnica usa menos memórias que outras técnicas.

b) DMA (Direct Access Memory) ou acesso direto à memória, para que a sinalização entre a placa e o computador fosse executada.

Esta técnica praticamente não é mais usada, levando-se em conta a evolução tecnológica dos hardwares para essa finalidade.

c) Técnica de memória compartilhada: com o objetivo de melhorar as técnicas anteriores. Uma placa de rede que opera de acordo com esta técnica possui uma área de memória que pode ser acessada pelo processador do computador diretamente, em alta velocidade e sem estados de espera (interrupção).

d) Controle de bus: uma técnica largamente utilizada em computadores com barramento EISA (Extended Industry Standard Architecture) ou ISA, em que a placa de rede envia e recebe dados para a memória do computador sem interromper a atividade do processador..

As placas de rede que operam com essa técnica assumem o bus de dados do computador e colocam as informações diretamente na região de memória RAM do computador enquanto que, o processados continua operando.

Em se falando de recursos do sistema, todas as placas de rede são parecidas: precisam de um endereço de IRQ, um canal de DMA e um endereço de I/O, que devem ser configurados corretamente.

O canal de IRQ é necessário para que a placa de rede possa chamar o processador quando tiver dados a entregar.

O canal de DMA é usado para transferir os dados diretamente à memória, diminuindo a carga sobre o processador. Finalmente, o endereço de I/O informa ao sistema onde estão as informações que devem ser movidas.

Ao contrário dos endereços de IRQ e DMA que são escassos, existem muitos endereços de I/O e por isso a possibilidade de conflitos é bem menor, especialmente no caso de placas PnP.

De qualquer forma, mudar o endereço de I/O usado pela placa de rede (isso pode ser feito através do gerenciador de dispositivos do Windows, por exemplo) é uma coisa a ser tentada caso a placa de rede misteriosamente não funcione, mesmo não havendo conflitos de IRQ e DMA.

Todas as placas de rede atuais são PnP, tendo seus endereços configurados automaticamente pelo sistema. Placas mais antigas por sua vez, trazem jumpers ou dip-switches que permitem configurar os endereços a serem usados pela placa.

Existem também casos de placas de rede que são configuráveis via software, sendo sua configuração feita através de um programa fornecido junto com a placa.

[12] I/O - input/output (dispositivo de entrada e saída num memo barramento)

Para que as placas possam “se encontrar” dentro da rede, cada placa possui também um endereço de nó.

Este endereço de 48 bits é único e estabelecido durante o processo de fabricação da placa, sendo inalterável.

O endereço físico é relacionado com o endereço lógico do micro na rede.

Se por exemplo na sua rede existe um outro micro chamado “Micro B”, e o “Micro A” precisa transmitir dados para ele, o sistema operacional de rede ordenará à placa de rede que transmita os dados ao “Micro B”, porém, a placa usará o endereço de nó e não o endereço de fantasia “Micro B” como endereço.

Os dados trafegarão através da rede e será acessível a todas as os micros, porém, apenas a placa do “Micro B” lerá os dados, pois apenas ela terá o endereço de nó indicado no pacote.

Sempre existe a possibilidade de alterar o endereço de nó de uma placa de rede, substituindo o chip onde ele é gravado.

Este recurso é usado algumas vezes para fazer espionagem, já que o endereço de nó da rede poderá ser alterado para o endereço de nó de outra placa da rede, fazendo com que a placa clonada, instalada no micro do espião também receba todos os dados endereçados ao outro micro.

10 – ENDEREÇAMENTO IP

Cada host (*qualquer dispositivo que possui placa de rede*) é identificado por um endereço IP lógico.

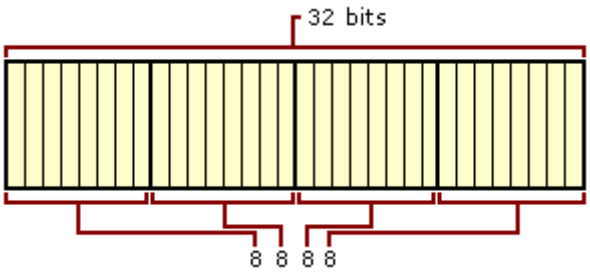
O endereço IP pertence à camada de rede no modelo OSI e não tem nenhuma dependência com a camada de enlace (*como o endereço de acesso à mídia de um adaptador, por exemplo*).

Um único endereço IP é requerido para cada host ou qualquer outro componente de rede que se comunica usando TCP/IP.

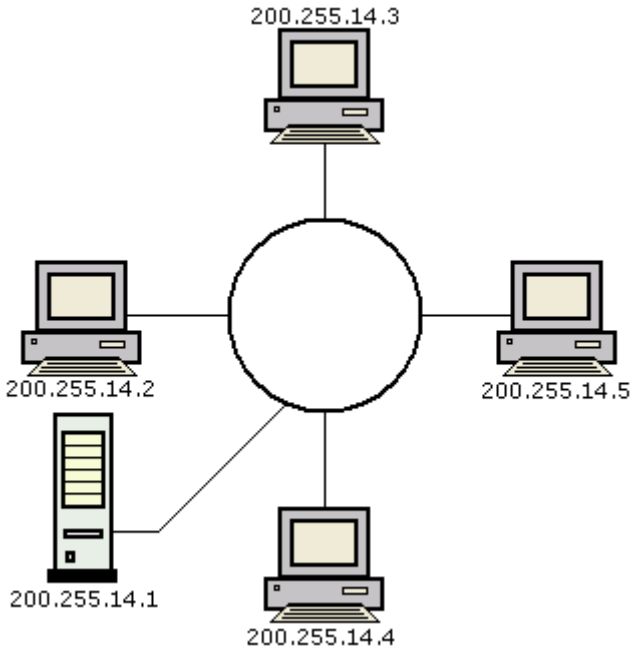
O endereço IP identifica a localização de um host na rede do mesmo modo que o endereço de uma rua identifica uma casa na cidade.

Como um endereço de uma casa deve identificar uma única residência um endereço IP deve ser globalmente único e ter um formato uniforme.

O endereço IP é composto de um número de quatro bytes, separados por três pontos como: 200.255.14.11 ou algo similar.



Composição de um endereço IP (32 bits no total)



Endereçamento IP

A figura acima representa um exemplo de endereçamento entre quatro estações de trabalho e o servidor.

Observa-se na figura acima que todos os componentes tem a mesma identificação de rede, por pertencerem ao mesmo meio físico.

A identificação de rede (*também conhecida como endereço de rede*) identifica os sistemas que estão localizados no mesmo segmento físico de rede na abrangência de roteadores IPs.

Todos os sistemas na mesma rede física devem ter a mesma identificação de rede. A identificação de rede deve ser única na rede.

A identificação de host (*também conhecido como endereço de host*) identifica uma estação de trabalho, servidor, roteador, ou outro host TCP/IP dentro de uma rede.

O endereço para cada host deve ser único para a identificação de rede.

Observações: *A identificação de rede faz referência para qualquer endereço IP na rede, seja baseada em classes, sub-redes ou uma super-rede*.
Um endereço IP consiste em 32 bits. Ao invés de trabalhar com 32 bits por vez, é comum na pratica de segmentar os 32 bits de um endereço IP em quatro campos de 8 bits chamados de octetos. Cada octeto é convertido em um número de base decimal na escala de 0-255 e separados por um ponto. Este formato é chamado notação decimal pontuada.

10.1 - CLASSES DE ENDEREÇOS

Apesar de parecer simples, a implementação do endereçamento TCP/IP é um pouco mais complicada, pois existem regras para a formação dos endereçamentos, que são divididas em classes de endereçamento: A, B, C, D e E.

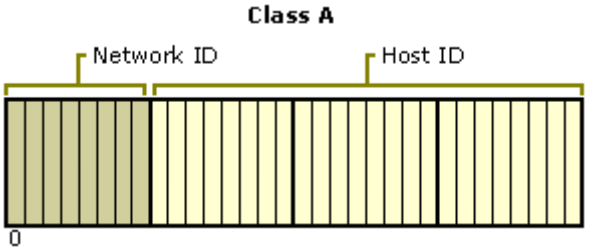
A comunidade Internet definiu originalmente nestas 5 classes de endereços para acomodar as redes de tamanhos variados.

A classe de um endereço define quantos bits estão sendo usados para identificação de rede e quantos para identificação do host, definindo também, o possível número de redes e hosts por rede.

Classe A

Endereços classe A são atribuídos a redes com um vasto número de hosts. O bit de maior grau em uma classe A é sempre zero.

Os próximos 7 bits (preenchendo o primeiro octeto) completam a identificação de rede. Os 24 bits restantes (os últimos 3 octetos) representam a identificação do host.



Endereço IP classe A

Um endereço classe A permite 128 redes e 16.777.214 hosts por rede.

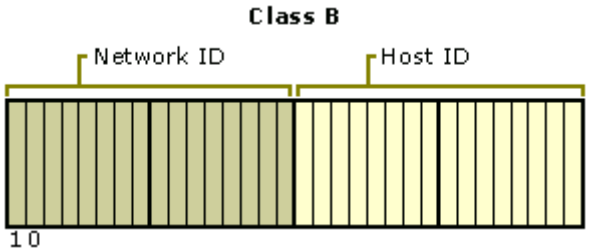
2^7 = 128 (redes)
(2^{24} – 2) = 16.777.214 (hosts)

O endereço classe A 127.x.x.x está reservado para testes de loopback e para processos de comunicação interna no computador local, portanto, a identificação da rede não pode começar com 127 pois, o número 127 em uma classe A está reservado para funções internas e loopback.

Levando-se em consideração que uma rede não pode começar também com 0 (zero), então para classe A temos valores compreendidos entre 1 e 126.

Classe B

Endereços classe B são atribuídos a redes com um número médio de hosts.
Os dois bits de maior grau em classe B são os valores binário 10.



Endereço IP classe B

Os 2 bits de maior grau em uma classe B são sempre os valores binários 10. Os próximos 14 bits (preenchendo o primeiro e o segundo octeto) completam a identificação de rede.

Os 16 bits restantes (os últimos 2 octetos) representam a identificação do host.

Assim, um endereço classe B permite 16.384 redes e 65.534 hosts por rede, que compreendem valores entre 128 e 191.

$$2^{14} = 16.384 \text{ (redes)}$$
$$(2^{16} - 2) = 65.534 \text{ (hosts)}$$

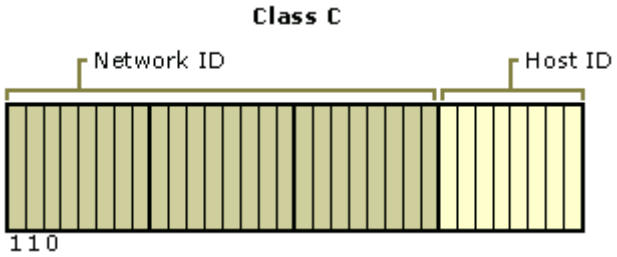
Classe C

Endereços classe C são atribuídos a pequenas redes.

Os 3 bits de maior grau em uma classe C são sempre os valores binários 110. Os próximos 21 bits (preenchendo os 3 primeiros octetos) completam a identificação de rede. Os oito bits restantes (o último octeto) representam a identificação do host.

Um endereço classe C permite 2.097.152 redes e 254 hosts por rede, que compreendem valores entre 192 e 223.

$$2^{21} = 2.097.172 \text{ (redes)}$$
$$(2^{8} - 2) = 254 \text{ (hosts)}$$



Endereço IP classe C

Observações:
➔ Não podem existir dois computadores com o mesmo endereço IP na rede, especialmente se os computadores estiverem remotamente interligados, como no caso da Internet.
➔ Um host não pode ser representado apenas por valores 0 ou 255.

Classe D

A classe D representa os endereços IP cujo primeiro número é igual ou superior a 224, e está reservado para criar agrupamentos de computadores para o uso de Multicast[13].

O sistema Multicast permite que um grupo de computadores utilize um ou mais endereços para enviar dados somente para aqueles que estejam configurados para receber por este endereço.

Não podemos utilizar esta faixa de endereços para endereçar os computadores na rede TCP/IP.

Classe E

A classe E é um endereço reservado e utilizado para testes e novas implementações e controles do TCP/IP. São endereços IP com valores iniciais acima de 240.0.0.0. Da mesma forma, não podemos utilizar esta faixa de endereços para endereçar os computadores na rede TCP/IP.

[13] Multicast - transmissão múltipla (transmissão simultânea para várias estações de trabalho); multicasting (multidifusão); transmissão para um número de receptores ou nós, com um endereço em cada mensagem para indicar o nó desejado.

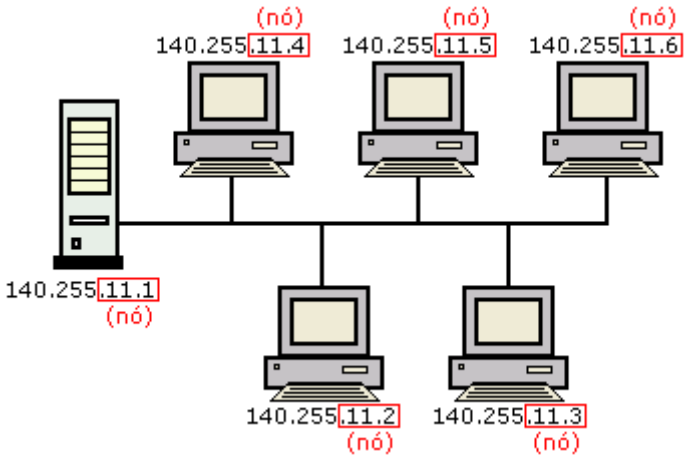
RESUMO

CLASSE	ABRANGÊNCIA	REDES DISPONÍVEIS	HOSTS DISPONÍVEIS
A	1 – 126	126	16.777.214
B	128 – 191	16.384	65.634
C	192 - 223	2.097.152	254

A figura a seguir mostra uma rede com endereçamento classe B. Observe que os "nós" estão identificados em relação aos dois últimos octetos.

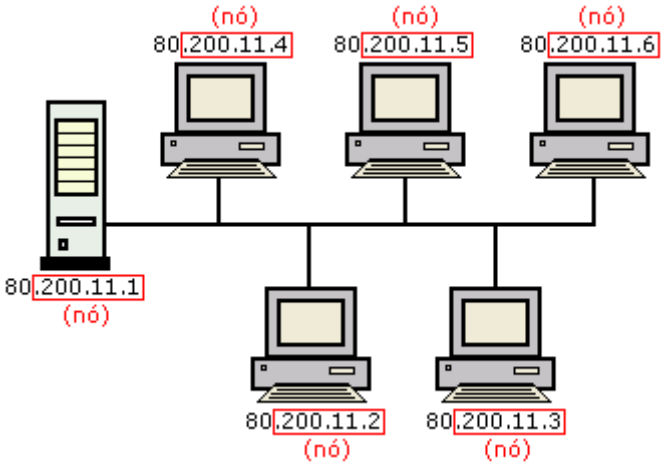
Desta forma, os hosts são identificados como 11.1, 11.2, 11.3, etc. e a rede é identificada por 140.255 (os dois primeiros octetos).

Enquanto que os dois primeiros números identificam a rede (que devem ser iguais para todos os computadores) os dois últimos números identificam os hosts ou computadores (que devem ser diferentes para cada um dos computadores).



Endereçamento IP classe B

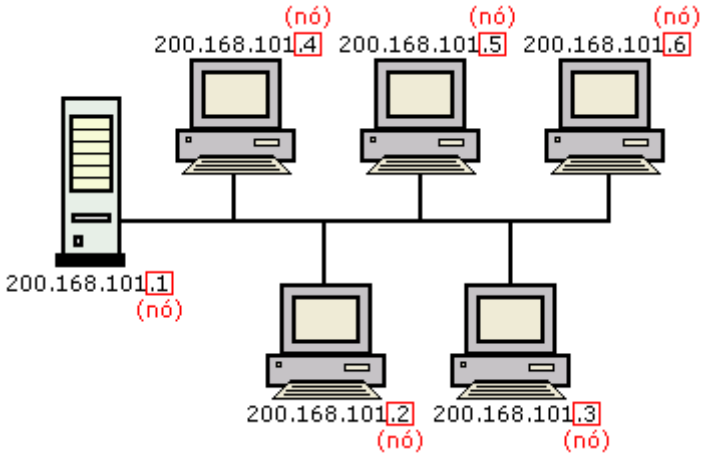
A figura a seguir mostra uma rede com endereçamento IP classe A. Atente para o detalhe da identificação da rede e dos hosts em relação ao endereçamento IP classe B mostrado na figura acima.



Endereçamento IP classe A

A rede é identificada pelo número 80, enquanto que os hosts são identificados por 200.11.1, 200.11.2, 200.11.3, etc.

A figura a seguir mostra uma rede com endereçamento classe C, onde a rede é identificada por 200.168.101 e os hosts por 1, 2, 3, etc.



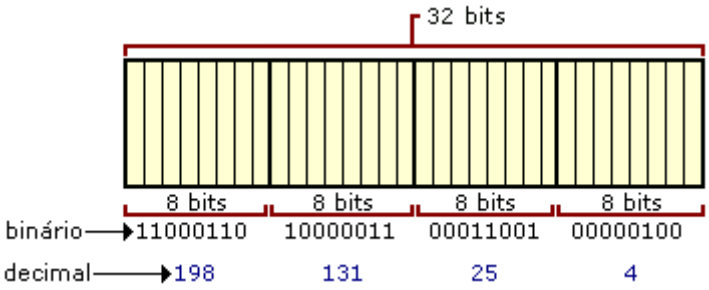
Endereçamento IP classe C

10.2 - Disposição do endereço IP – decimal e binário

Como vimos anteriormente, um endereço IP tem 4 bytes, que se denomina octeto uma vez que, cada byte de endereço abrange 8 bits.

Desta forma, um endereço IP completo tem 32 bits.

Geralmente, em termos de usuário, o endereço IP é representado na forma decimal, uma vez que é mais fácil de lembrar e portanto, de manusear.



Equivalência decimal/binário no endereço IP

11 – MÁSCARAS DE SUB-REDE

11.1 - Máscaras padrão

Ao configurar o protocolo TPC/IP, seja qual for o sistema operacional usado, além do endereço IP é preciso informar também o parâmetro da máscara de sub-rede, ou “subnet mask”.

Ao contrário do endereço IP, que é formado por valores entre 0 e 255, a máscara de sub-rede é formada por apenas dois valores: 0 e 255, como em 255.255.0.0 ou 255.0.0.0. onde um valor 255 indica a parte endereço IP referente à rede, e um valor 0 indica a parte endereço IP referente ao host.

A máscara de rede padrão acompanha a classe do endereço IP: num endereço de classe A, a máscara será 255.0.0.0, indicando que o primeiro octeto se refere à rede e os três últimos ao host.

Num endereço classe B, a máscara padrão será 255.255.0.0, onde os dois primeiros octetos referem-se à rede e os dois últimos ao host, e num endereço classe C, a máscara padrão será 255.255.255.0 onde apenas o último octeto refere-se ao host.

Exemplo de endereço IP	Classe de endereço	Rede	Host	Sub-net mask padrão
100.128.161.18	A	100	128.161.18	255.0.0.0
148.110.105.12	B	148.110	105.12	255.255.0.0
210.100.100.22	C	210.100.100	22	255.255.255.0

Para a máscara de sub-rede (sub-net mask) 255.0.0.0, teremos:
net. host.host.host

Para a máscara de sub-rede (sub-net mask) 255.255.0.0, teremos:
net. net.host.host

Para a máscara de sub-rede (sub-net mask) 255.255.255.0, teremos:
net. net.net.host

11.2 - Finalidade e utilidade das máscaras

Apesar das máscaras padrão acompanharem a classe do endereço IP, é possível "mascarar" um endereço IP, mudando as faixas do endereço que serão usadas para endereçar a rede e o host.

O termo "máscara de sub-rede" é muito apropriado neste caso, pois a "máscara" é usada apenas dentro da sub-rede.

Veja o exemplo mostrado na tabela a seguir, referente ao endereço 200.110.112.114.

Por ser um endereço de classe C, sua máscara padrão seria 255.255.255.0, indicando que o último octeto refere-se ao host, e os demais à rede.

Porém, se mantivéssemos o mesmo endereço, mas alterássemos a máscara para 255.255.0.0 apenas os dois primeiros octetos (200.110) continuariam representando a rede, enquanto o host passaria a ser representado pelos dois últimos octetos e não apenas pelo último.

Endereço IP	Sub-net mask padrão	Rede	Host
200.110.112.114	255.0.0.0	200	110.112.114
200.110.112.114	255.255.0.0	200.110	112.114
200.110.112.114	255.255.255.0	200.110.112	114

O endereço 200.110.112.114 com máscara 255.255.255.0 é diferente de 200.110.112.114 com máscara 255.255.0.0.

Enquanto no primeiro caso temos o host 114 dentro da rede 200.110.112, no segundo caso temos o host 112.114 dentro da rede 200.110.

Dentro de uma mesma sub-rede, todos os hosts deverão ser configurados com a mesma máscara de sub-rede, caso contrário poderão não conseguir comunicar-se, pois pensarão estar conectados a redes diferentes.

Se, por exemplo, houverem dois micros dentro de uma mesma sub-rede, configurados com os endereços 200.110.108.1 e 200.110.108.2 mas configurados com máscaras diferentes, 255.255.255.0 para o primeiro e 255.255.0.0 para o segundo, teremos um erro de configuração.

11.3 - Máscaras complexas

Até agora vimos apenas máscaras de sub-rede simples ou padrão.

Porém o recurso mais refinado das máscaras de sub-rede é quebrar um octeto do endereço IP em duas partes, fazendo com que dentro de um mesmo octeto, tenhamos uma parte que representa a rede e outra que representa o host.

Máscara de sub-rede (sub-net) padrão

Decimal	255	255	255	0
Binário	11111111	11111111	11111111	00000000
	rede	rede	rede	host

A figura acima representa um endereço classe C, com máscara de sub-rede padrão e respectiva equivalência decimal/binário.

Para melhor entendimento, a tabela abaixo mostra algumas equivalências decimal/binário para 8 bits.

Trata-se de uma codificação extendida do BCD8421[14], que possui peso relativo, ou seja, ao bit mais significativo (MSB – Most significant bit) associa-se:

$$2^{(n-1)}$$

Onde: *n* é o número de bits que compõe o número

Assim, para um número composto de 8 bits, teremos $2^{(8-1)} = 2^7 = 128$

Veja que na conversão decimal/binário somente são somados os valores que correspondem ao bit 1.

Valor decimal	PESO							
	128	64	32	16	8	4	2	1
135	1	0	0	0	0	1	1	1
100	0	1	1	0	0	1	0	0
254	1	1	1	1	1	1	1	0
80	0	1	0	1	0	0	0	0
11	0	0	0	0	1	0	1	1

Exemplos de conversão decimal/binário

Por exemplo, o número binário 10000111 corresponde ao 135 decimal, que é equivalente a soma dos pesos aos quais são atribuídos "1".

Desta forma teremos: 128+4+2+1 = 135

[14] BCD - Binary Coded Decimal

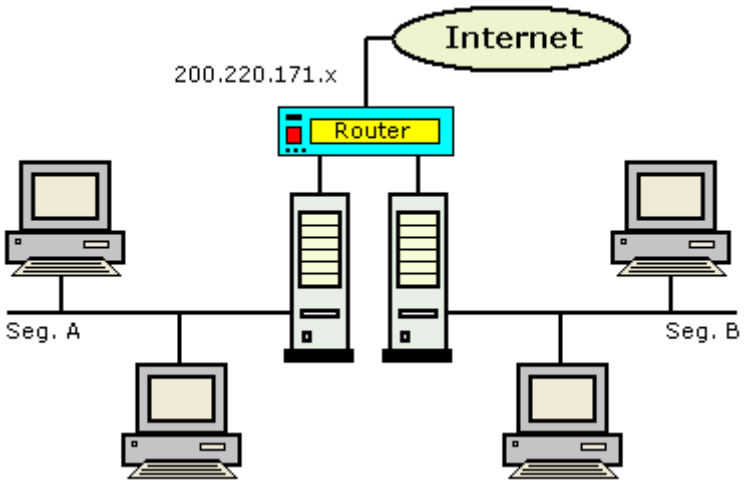
Para o número binário 01100100, que corresponde ao 100 decimal, teremos: 64+32+4, e assim por diante.

Vejamos a utilidade de quebrar um octeto, ou dividi-lo em dois, o que teoricamente seria a utilização de ½ byte para identificar a rede e ½ byte para identificar o host.

Tomemos como exemplo, uma empresa que se conecta a Internet e sua rede possui dois segmentos, interligados por um roteador.

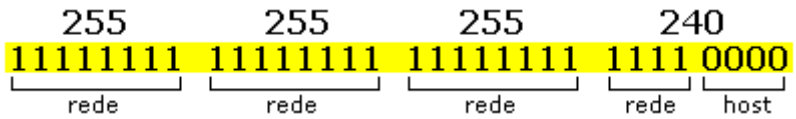
Essa empresa recebe um número IP, por exemplo: 200.220.171.x, onde 200.220.171 identifica a rede e "x" é o número de hosts (1 a 254, pois o endereço é classe C) que podem ser interligados a mesma.

Levando-se em conta um endereço classe C convencional, e supondo IP = 200.220.171.135, a sub-rede será: 255.255.255.0, restrito a 254 hosts em um único segmento.



Rede com dois segmentos interligada a Internet

O objetivo de quebrar o byte é justamente permitir que o mesmo endereço seja usado nos dois segmentos. Se utilizarmos a máscara 255.255.255.240, por exemplo, os quatro primeiros bits identificarão a rede e os quatro restantes os hosts ou "nós".



Com isto, é possível obter-se 14 redes e 16 hosts (ou 16 computadores em cada rede).

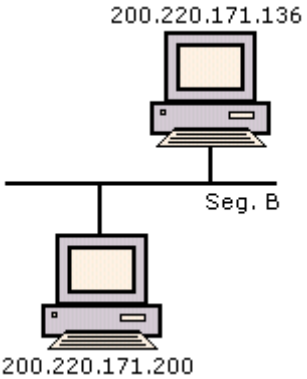
Teoricamente deveríamos ter também 16 redes, mas, como não são permitidos valores 0 e valores 1 para todos os bits da rede, então teremos apenas 14 redes.

A tabela a seguir mostra como funciona a quebra do byte, quando são escolhidos alguns parâmetros para a máscara.

Valor da máscara (último número)	Onde o byte é cortado	Número de redes possíveis	Hosts (computadores) em cada rede
128	1º	0	-
192	2º	2	64
224	3º	6	32
240	4º	14	16
248	5º	30	8
252	6º	62	4
254	7º	126	2
255	8º	254	0

Os valores 128 e 255 normalmente não são utilizados para a criação de sub-redes, uma vez que o primeiro não permitirá a criação de sub-redes e o segundo por não sobrar bits para a definição do host, principalmente em se tratando de endereçamento IP classe C.

Tomemos como exemplo dois computadores do segmento B da figura mostrada anteriormente com os endereços: 200.220.171.135 e 200.220.171.200, ambos usando a máscara (sub-net) 255.255.255.240.



Como os endereços que identificam a rede devem ser iguais no seguimento, pergunta-se: os computadores se comunicarão?

Analisemos então:

rede	nó		rede	nó
1000	1000		1100	1000
128	8		192	8
decimal: 136			decimal: 200	

Conclui-se portanto que os computadores não se comunicarão, pois a identificação da rede não é igual (1000 e 1100).

Por este motivo é muito importante ficar atento às identificações de sub-redes e explorar ao máximo os seus recursos, de acordo com as necessidades do projeto da mesma.

Obviamente, se trocarmos o endereço 200.220.171.200 para 200.220.171.135, haverá a comunicação entre os dois computadores, pois as redes terão números iguais.

rede	nó
1000	0111
128	7
decimal: 135	

Ainda com relação ao segmento B, poderão ser interligados mais 14 computadores, que abrangerão os endereços: 200.220.171.128 até 200.220.171.143, conforme ilustra a figura a seguir.

Analogamente para o segmento A, poderão ser atribuídos os endereços 200.220.171.192 até 200.220.171.207.

Podemos notar que o recurso de quebra do byte é bastante sofisticado e de grande utilidade quando se tem segmentos de rede, principalmente quando a Internet é acessada.

Resta ao administrador analisar quais as melhores condições para um determinado projeto.

Para melhor fixação deste conceito, façamos um exercício.

➔ Supondo um endereçamento: 200.220.171.x, com máscara de sub-rede 255.255.255.192. Especifique quantos hosts ou computadores poderão ser interligados a esse endereçamento e sua correlação com as redes.

Solução:

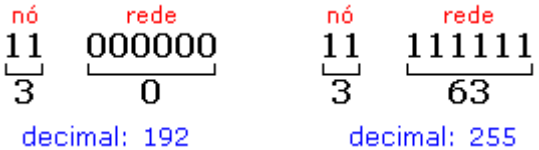
Com a máscara 255.255.255.192, podemos obter 2 redes (pois o corte ocorre no 2º bit) e 64 hosts.

Temos então:

bits da rede 11 (2 e 3 - binário)
bits de host 000000 (0 a 63 - binário)

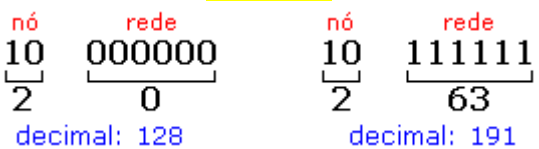
Lembrar que, numa máscara de sub-rede os números binários "1" referem-se à rede e os números binários "0" referem-se ao host.

Rede A



IP: 200.220.171.192 a 200.220.171.255

Rede B



IP: 200.220.171.128 a 200.220.171.191

CONCLUSÃO: Obteve-se um arranjo com 2 redes e com 64 hosts por rede.

12 – DHCP – GATEWAY

12.1 - DHCP

Ao invés de configurar manualmente os endereços IP em cada máquina, é possível fazer com que os hosts da rede obtenham automaticamente seus endereços IP, assim como sua configuração de máscara de sub-rede e default gateway.

Isto torna mais fácil a tarefa de manter a rede e acaba com a possibilidade de erros na configuração manual dos endereços IP.

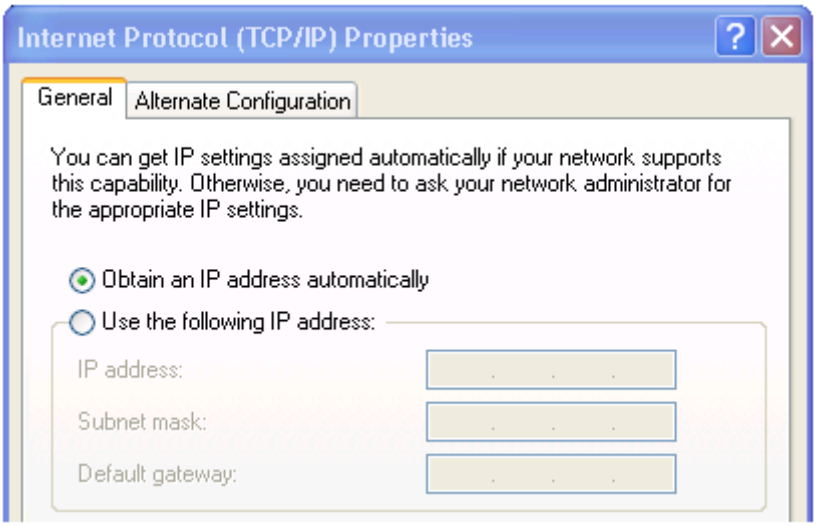
Para utilizar este recurso, é preciso implantar um servidor de DHCP[15] na rede.

Se a rede não for muito grande, não é preciso usar um servidor dedicado só para isso, pois esta tarefa poderá ser executada por um servidor de arquivos.

O serviço de servidor DHCP pode ser instalado apenas em sistemas destinados a servidores de rede, como o Windows NT Server, Windows 2000 Server, Novell Netware 4.11 (ou superior) além claro do Linux e das várias versões do Unix.

Do lado dos clientes, é preciso configurar o TCP/IP para obter seu endereço DHCP a partir do servidor.

Para fazer isso, no Windows XP por exemplo, basta abrir o ícone redes do painel de controle, acessar as propriedades do TCP/IP e na guia “General - Geral” escolher a opção “Obtain an IP address automaticaly - Obter um endereço IP automaticamente”.



Obtenção de endereço IP através do DHCP

Cada vez que o micro cliente é ligado, carrega o protocolo TCP/IP e em seguida envia um pacote de broadcast para toda a rede, perguntando quem é o servidor DHCP.

Este pacote especial é endereçado como 255.255.255.255, ou seja, para toda a rede. Junto com o pacote, o cliente enviará o endereço físico de sua placa de rede.

Ao receber o pacote, o servidor DHPC usa o endereço físico do cliente para enviar para ele um pacote especial, contendo seu endereço IP.

Este endereço é temporário, não é da estação, mas simplesmente é “emprestado” pelo servidor DHCP para que seja usado durante um certo tempo.

[15] DHCP – (Dynamic Host Configuration Protocol)

Uma configuração importante é justamente o tempo do empréstimo do endereço.

A configuração do "Lease Duration – duração do empréstimo" muda de sistema para sistema. No Windows NT Server por exemplo, pode ser configurado através do utilitário "DHCP Manager – Gerenciador do DHCP".

Depois de decorrido metade do tempo de empréstimo, a estação tentará contatar o servidor DHCP para renovar o empréstimo.

Se o servidor DHCP estiver fora do ar, ou não puder ser contatado por qualquer outro motivo, a estação esperará até que tenha se passado 87.5% do tempo total, tentando o contato por várias vezes.

Se terminado o tempo do empréstimo o servidor DHCP ainda não estiver disponível, a estação abandonará o endereço e ficará tentando contatar qualquer servidor DHCP disponível, repetindo a tentativa a cada 5 minutos.

Porém, por não ter mais um endereço IP, a estação ficará fora da rede até que o servidor DHPC volte.

Uma vez instalado, o servidor DHCP passa a ser essencial para o funcionamento da rede.

Se ele estiver travado ou desligado, as estações não terão como obter seus endereços IP e não conseguirão entrar na rede.

O tempo do empréstimo pode ser configurado como sendo de 12 ou 24 horas, ou mesmo estabelecer o tempo como ilimitado, assim a estação poderá usar o endereço até que seja desligada no final do dia, minimizando a possibilidade de problemas, caso o servidor caia durante o dia.

Todos os provedores de acesso à Internet usam servidores DHCP para fornecer dinamicamente endereços IP aos usuários. No caso deles, esta é uma necessidade, pois o provedor possui uma faixa de endereços IP, assim como um número de linhas bem menor do que a quantidade total de assinantes, pois trabalham sobre a perspectiva de que nem todos acessarão ao mesmo tempo.

Finalizando, a cada reinício da estação, um novo endereço será atribuído a esta, pelo DHCP.

12.2 - Default Gateway

Uma rede TCP/IP pode ser formada por várias redes interligadas entre si por roteadores.

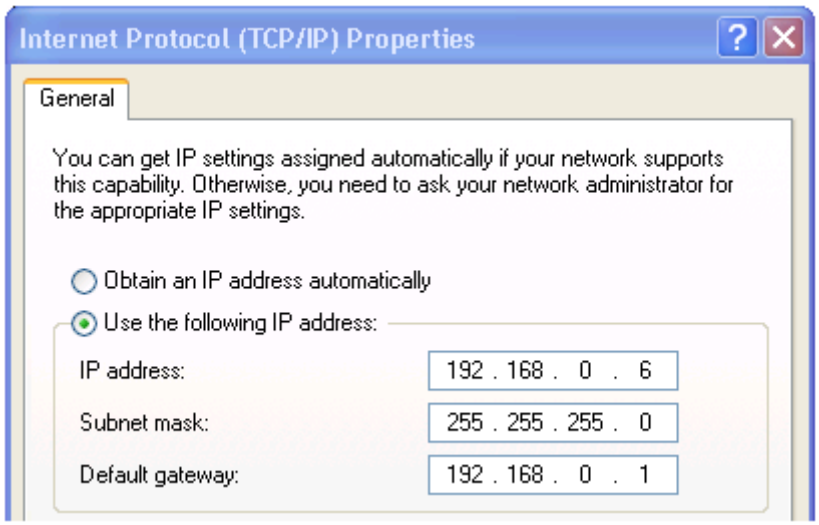
Neste caso, quando uma estação precisar transmitir algo a outra que esteja situada em uma rede diferente (isso é facilmente detectado através do endereço IP), deverá contatar o roteador de sua rede para que ele possa encaminhar os pacotes.

Como todo nó da rede, o roteador possui seu próprio endereço IP. É preciso informar o endereço do roteador nas configurações do TCP/IP de cada estação, no campo "default gateway – gateway padrão", pois sem esta informação as estações simplesmente não conseguirão acessar o roteador e como consequência, as outras redes.

Caso a rede seja suficientemente grande, provavelmente também terá um servidor DHCP.

Neste caso, o servidor DHCP poderá ser configurado para fornecer o endereço do roteador às estações junto com o endereço IP.

No caso de uma rede pequena com 6 PCs, usando os endereços IP **192.168.0.1**, **192.168.0.2**, **192.168.0.3**, **192.168.0.4**, **192.168.05** e **192.168.06** e o PC 192.168.0.1 estiver compartilhando o acesso à Web, seja através do ICS do Windows ou outro programa qualquer, as outras cinco estações deverão ser configuradas para utilizar o Default gateway: 192.168.0.1.



Configuração do default gateway

13 – DNS

Toda interface ligada a uma rede TCP/IP é identificada por um endereço IP, formado por 32 bits, conforme vimos anteriormente.

Um nome pode ser atribuído a qualquer dispositivo que possua um endereço IP. A atribuição de nomes aos endereços deve-se ao fato de que, as pessoas tem mais facilidade de memorizar nomes do que números. No entanto, o software de rede só trabalha com números.

Na maior parte dos casos, nomes e números podem ser usados indistintamente, uma vez que tanto números como nomes conduzem ao mesmo computador.

Quando nomes são utilizados, é necessário que exista um serviço que efetue a conversão deste nome em um número IP para que a conexão seja estabelecida.

A tradução entre nomes e números passou por diversos estágios durante o desenvolvimento da Internet e das redes que a precederam.

Inicialmente existia uma tabela chamada “hosts.txt”, mantida pelo DDN-NIC e que era distribuída para todos os computadores da Internet.

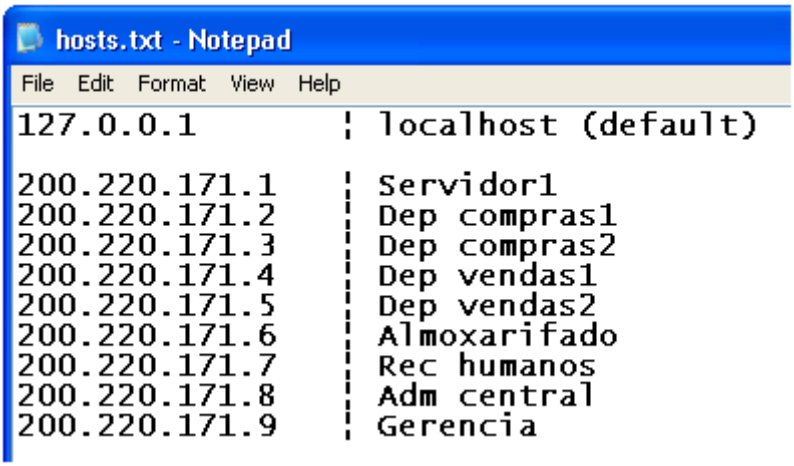
Cada rede que precisasse solucionar nomes de hosts em outras redes, carregava este arquivo.

Isto quer dizer que, quando uma nova máquina é inserida na tabela de hosts de um determinado computador, somente este computador reconhecerá a alteração na tabela.

Para que os outros computadores possam reconhecer a alteração, o administrador da rede deverá copiar este arquivo para os outros computadores, procedimento este, não recomendável para redes grandes.

No entanto, para redes locais de empresas este sistema ainda é muito utilizado. Veja a seguir um exemplo de uma tabela de hosts de uma empresa, criada dentro do diretório Windows.

Essa tabela funciona como um pequeno banco de dados que pode ser comparado a uma agenda telefônica. A mesma fica em cada computador da rede que tem o TCP/IP instalado.



Isto funciona da seguinte forma: quando o TCP/IP que está rodando em um computador não reconhece as instruções que o usuário inseriu na aplicação, ou seja, nomes no lugar do endereço IP padrão, este recorre à tabela hosts previamente criada.

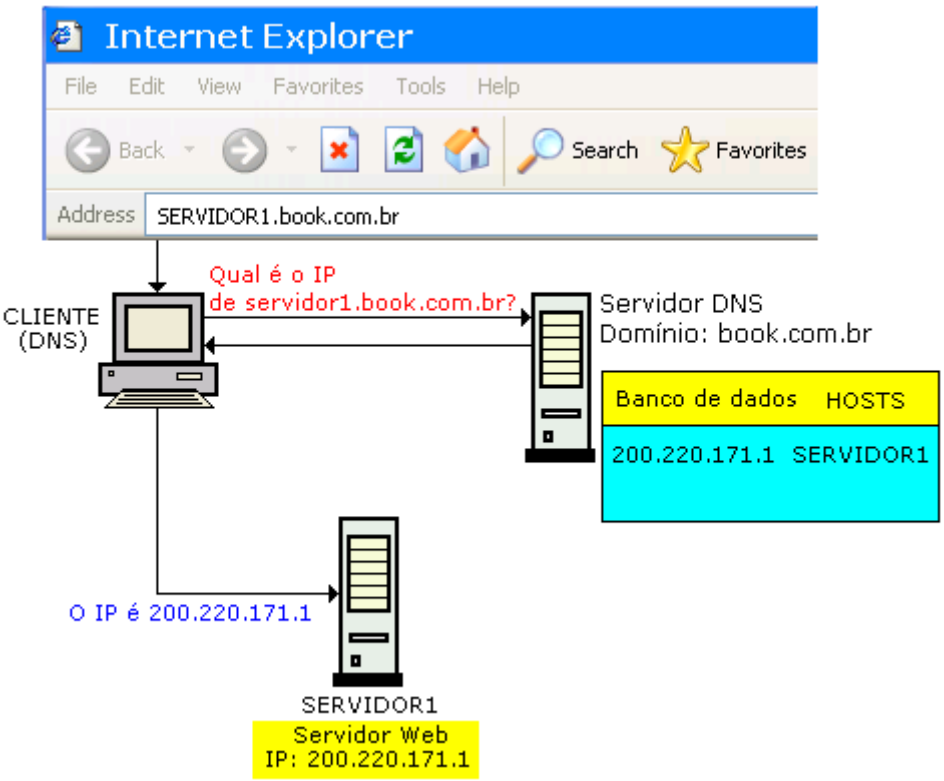
Com o crescimento da Internet essa tabela tornou-se inviável, exigindo um serviço mais eficiente para a resolução de nomes; a tabela hosts.txt, foi então substituída pelo banco de dados distribuído denominado DNS (Domain Name Service), cujas especificações encontram-se descritas na RFC 1034 e 1035[16].

O sistema de distribuição de nomes de domínio foi introduzido em 1984, e com ele, os nomes de hosts residentes em um banco de dados pode ser distribuído entre servidores múltiplos, baixando assim, a carga em qualquer servidor que provê administração no sistema de nomeação de domínios.

Ele baseia-se em nomes hierárquicos e permite a inscrição de vários dados digitados além do nome do host e seu IP.

Em virtude do banco de dados de DNS ser distribuído, seu tamanho é ilimitado e o desempenho não é comprometido quando se adiciona mais servidores nele.

[16] RFC - Request for comments



Arquitetura DNS

Dentro da arquitetura do DNS existem dois tipos de computadores: o cliente DNS (*resolver*) e o servidor DNS. O servidor DNS faz a tradução do nome para o endereço IP. A figura acima ilustra o cliente DNS solicitando do servidor DNS a resolução do endereço IP.

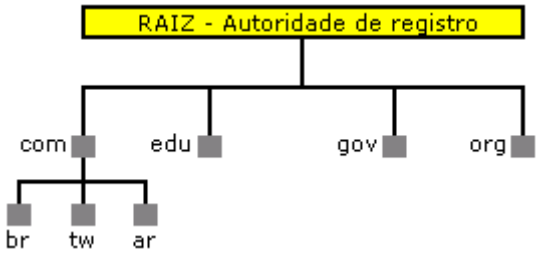
Quando o cliente DNS está configurado, este trabalha em conjunto com o protocolo IP na tradução dos nomes para os respectivos endereços IP, sempre que os nomes são fornecidos pelo usuário aos aplicativos.

Quando o usuário tenta se conectar a um computador na rede a partir do endereço IP, isto é feito diretamente, mas, quando tentar fazer uma conexão com uma máquina na rede a partir do seu nome, o protocolo IP em conjunto com o cliente DNS fará primeiro uma pesquisa no servidor DNS, que retornará o endereço IP da máquina cujo nome foi fornecido.

O DNS é administrado por uma Autoridade de Inscrição de Nome na Internet, responsável por manter domínios de topo de nível que são nomeados através de organizações e por fim, por países.

Estes nomes de domínio seguem o padrão 3166 Internacional.

A figura a seguir um exemplo que como a árvore de domínios se forma.

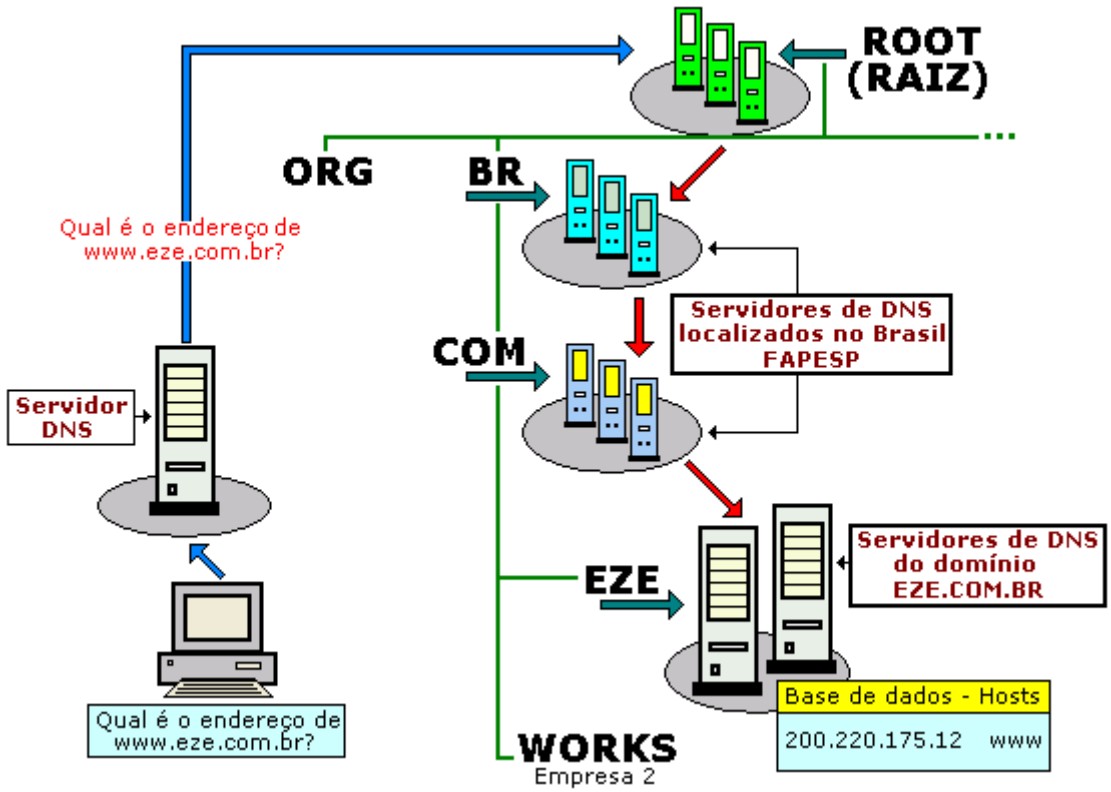


Estrutura básica de uma árvore de domínios

A árvore de domínios mostrada apresenta abreviações, que são reservadas para uso através de organizações. Veja a seguir uma tabela contendo algumas abreviações importantes e respectivos tipos.

DNS	Tipo de organizações
com	Organizações comerciais
edu	Instituições educacionais
org	Organizações filantrópitcas
net	Redes (backbone da internet)
gov	Organizações governamentais
mil	Organizações militares
num	Números de telefones
arpa	Reverso de DNS
xx	Código dos países (br, tw, etc.)

13.1 - Sistema de consulta



Sistema de consulta – I

Quando um usuário da Internet tentar se comunicar com o computador www.eze.com.br, este possivelmente estará utilizando um servidor DNS local ou do seu provedor de acesso.

O seu servidor de DNS provavelmente não tem a resposta para o cliente à pergunta: Qual é o endereço de www.eze.com.br? É a partir daí que devemos analisar o sistema de pesquisas dos servidores DNS.

O servidor DNS pode fornecer a resposta para o usuário de duas formas diferentes:

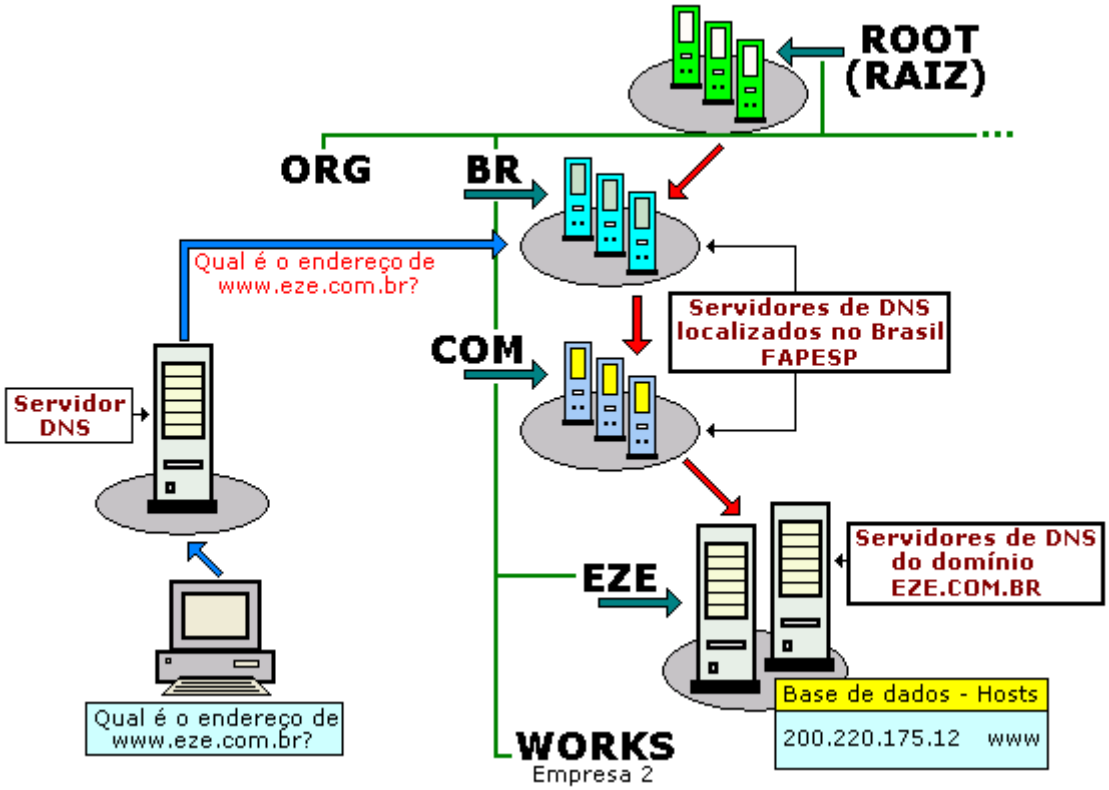
1) a partir do banco de dados que o administrador criou, contendo possivelmente apenas os computadores da rede local.

2) tentar a consulta fora do domínio.

Resumindo: quando um usuário tenta se comunicar com o computador www.eze.com.br, o TCP/IP enviará uma solicitação de tradução do nome para o endereço IP ao servidor DNS local ou do provedor de acesso.

A figura anterior mostra a pesquisa sendo feita primeiramente nos computadores que retém o domínio ROOT do DNS da Internet.

Um dos computadores que contém o domínio ROOT responde e informa ao servidor DNS, que procura descobrir qual é esse endereço IP, através de um dos servidores do domínio BR, cujo endereço IP então fornece.



Sistema de consulta – II

Na segunda tentativa o servidor DNS que procura resolver o "nome" busca agora um dos computadores do domínio BRASIL (BR).

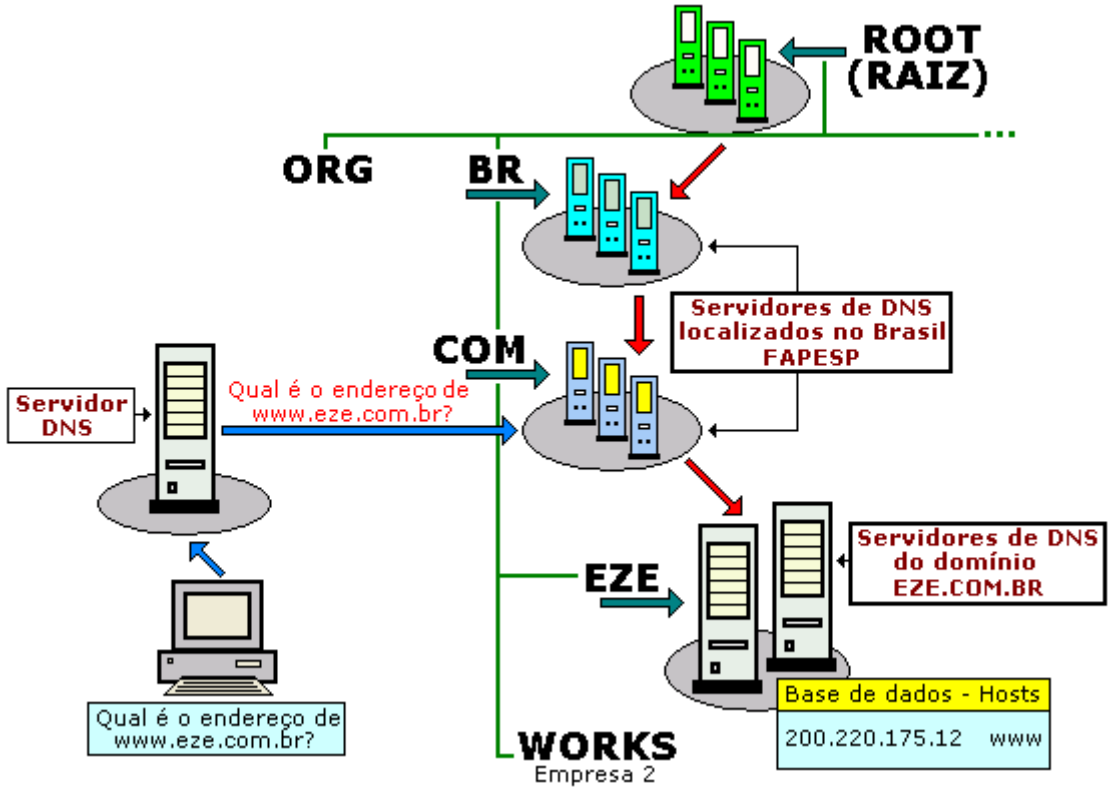
O servidor de DNS que contém o domínio BR responde ao servidor pesquisador o endereço IP dos servidores que armazenam o domínio .COM.BR e este então, entra em contato com um dos servidores do domínio COM.BR.

Os computadores do domínio COM.BR enviam, como resposta à pesquisa de endereço do servidor, os endereços IP dos servidores de DNS que respondem pelo domínio EZE.COM.BR, isto é, servidor que provavelmente contém o registro WWW em seu banco de dados.

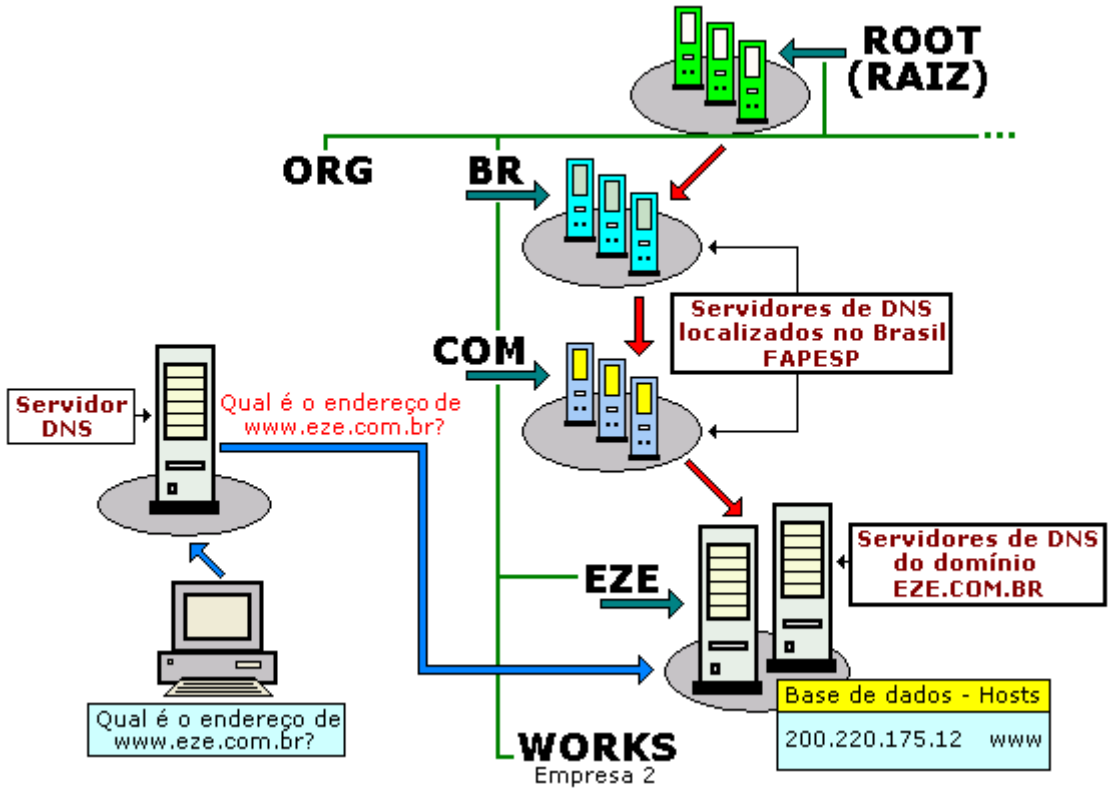
O servidor DNS entra então em contato com um dos servidores DNS do domínio EZE.COM.BR e, o servidor responsável por esse domínio procura pelo WWW. em seu banco de dados.

Caso encontre, responde ao servidor DNS que está fazendo a pesquisa e, finalmente, repassa tal informação ao cliente DNS (resolver) solicitante.

As figuras a seguir (sistema de consulta - III e sistema de consulta - IV) diagramam esse processo.



Sistema de consulta – III



Sistema de consulta – IV

14 – REDES SEM FIO (Wi-Fi)

14.1 – Antenas para transmissão de dados

Assim como em outras tecnologias de transmissão via rádio, a distância que o sinal é capaz de percorrer depende também da qualidade da antena usada.

As antenas padrão utilizadas nos pontos de acesso, geralmente de 2dBi[17] são pequenas e práticas, além de relativamente baratas, mas existe a opção de utilizar antenas mais sofisticadas para aumentar o alcance da rede.

Antena padrão típica para ambientes fechados

Embora alguns fabricantes aleguem que o alcance de suas antenas padrão possa chegar até a 300 metros, isto é um tanto quanto irreal uma vez que, na maioria das vezes essa distância é coberta em condições muito especiais, como campo aberto, por exemplo.

A medida que a distância aumenta, ocorre uma atenuação do sinal, fato esse que compromete a velocidade de transmissão. Mesmo assim, a distância máxima e a qualidade do sinal (e consequentemente a velocidade de transmissão) pode variar bastante de um modelo de ponto de acesso para outro, de acordo com a qualidade do transmissor e da antena usada.

Existem basicamente três tipos de antenas que podem ser utilizadas para aumentar o alcance da rede. As antenas Yagi, são as que oferecem um maior alcance, mas em compensação são capazes de cobrir apenas a área para onde são apontadas.

Antena Yagi

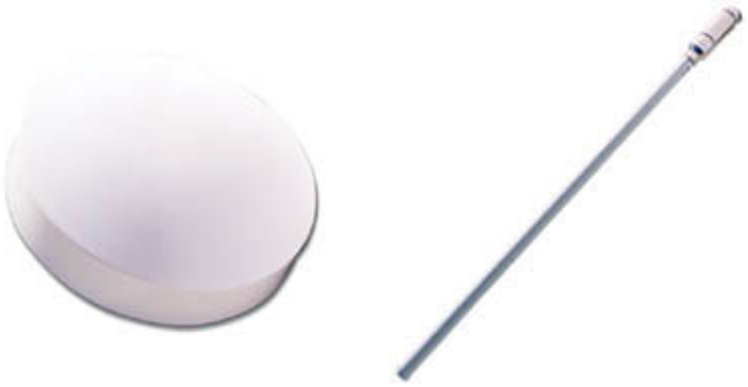
[17] dBi - é o ganho relativo em decibels de uma antena qualquer em relação a uma antena isotrópica; uma antena isotrópica é aquela que irradia igualmente em todas as direções.

Estas antenas são mais úteis para cobrir alguma área específica, longe do ponto de acesso, ou então para um usuário em trânsito, que precisa se conectar à rede. Em ambos os casos, o alcance utilizando uma antena Yagi pode passar dos 500 metros.

A segunda opção são as antenas omnidirecionais, que, assim como as antenas padrão dos pontos de acesso, cobrem uma área circular (ou esférica, caso o ponto de acesso esteja instalado acima do solo) em torno da antena.

A vantagem é a possibilidade de utilizar uma antena com uma maior potência.

Existem modelos de antenas omnidirecionais de 3dbi, 5dBi, 10dBi ou até mesmo 15dBi, um grande avanço sobre as antenas de 2dBi que acompanham a maioria dos pontos de acesso.



Antenas omnidirecionais

Assim como as Yagi, as antenas omnidirecionais podem ser usadas tanto para aumentar a área de cobertura do ponto de acesso, quanto serem instaladas numa interface de rede, em substituição à antena que a acompanha, permitindo captar o sinal do ponto de acesso de uma distância maior.

Mais uma opção de antena são as semi-parabólicas, que também captam o sinal em apenas uma direção, como as Yagi, mas em compensação podem ter uma potência ainda maior, geralmente 24dBi, dependendo do modelo usado.

Antena semi-prabólica

Estas antenas podem custar de 30 a mais de 200 dólares, dependendo da potência. As antenas Yagi estão entre as mais caras (150 dólares ou mais).

Além do problema do preço, existe um aumento no risco de uso indevido na rede, já que o sinal irá propagar-se por uma distância maior, mais uma razão para reforçar a segurança.

14.2 – Modo Ad Hoc

Assim como é possível ligar dois micros diretamente usando duas placas Ethernet e um cabo cross-over, sem usar hub, também é possível criar uma rede wireless (sem fio) entre dois PCs sem usar um ponto de acesso.

Basta configurar ambas as placas para operar em modo Ad Hoc (através do utilitário de configuração). A velocidade de transmissão é a mesma, mas o alcance do sinal é bem menor, já que os transmissores e antenas das interfaces não possuem a mesma potência do ponto de acesso.

Este modo pode servir para pequenas redes domésticas, com dois PCs próximos, embora mesmo neste caso seja mais recomendável utilizar um ponto de acesso, interligado ao primeiro PC através de uma placa Ethernet e usar uma placa wireless no segundo PC ou notebook, já que a diferenças entre o custo das placas e pontos de acesso não é muito grande.

14.3 - Bluetooth

Bluetooth é uma tecnologia de rádio de curto alcance criada pela Ericsson em meados da década de 90 e desenvolvida hoje por diversas companhias. Esta tecnologia sem fio possibilita a transmissão de dados em curtas distâncias entre telefones, computadores e outros aparelhos eletroeletrônicos.

O Bluetooth irá simplificar a comunicação e a sincronização entre estes aparelhos. A tecnologia substituirá muitos dos fios e cabos que nós usamos em nossa casa e no nosso escritório para conectar aparelhos: telefones, impressoras, PDA's, desktops e laptops, fax, teclados, joysticks - quase qualquer aparelho digital que use um chip Bluetooth será capaz de aproveitar as vantagens desta tecnologia.

Mais do que somente uma substituição de cabos, a tecnologia sem fio Bluetooth provê uma conexão universal para redes de dados existentes - possibilitando a formação de pequenos grupos privados de aparelhos conectados entre si.

A tecnologia de rádio do Bluetooth usa um sistema de frequência de sinal que provê um link seguro e robusto, mesmo em ambientes com alto ruído e de grande interferência.

A distância ideal é de no máximo 10 metros e a distância máxima é de 100 metros. Um dos trunfos dessa tecnologia é a promessa de transmissores baratos e pequenos o suficiente para serem incluídos em praticamente qualquer tipo de dispositivo, começando por notebooks, celulares e micros de mão, passando depois para micros de mesa, mouses, teclados, joysticks, fones de ouvido, etc.

Transmissor BLUETOOTH

A grande vantagem do Bluetooth é o fato de ser um padrão aberto e livre de pagamento de royalties, o que vem levando muitos fabricantes a se interessar pela tecnologia.
As especificações técnicas do padrão são as seguintes:

Alcance ideal: 10 metros
Alcance máximo: 100 metros (em condições ideais e com ambos os transmissores operado com potência máxima)
Frequência de operação: 2.4 GHz
Velocidade máxima de transmissão: 1Mbps
Potência da transmissão: 1mW a 100mW

Inicialmente imaginava-se que o Bluetooth poderia ser usado para quase tudo, desde redes sem fio até para conectar periféricos como mouses, teclados, e até mesmo eletrodomésticos entre si.

Mas, atualmente os fabricantes vem considerando seu uso para tarefas um pouco mais modestas.

A probabilidade de utilizar o Bluetooth como um padrão universal para redes sem fio caiu por terra com o IEEE 802.11b, o qual é capaz de manter taxas de transferência de 11Mbps e de cobrir distâncias maiores, sem falar nos dois sucessores, o 802.11a e o 802.11g

O 802.11b pode ser utilizado para conectar PCs, notebooks e também outros dispositivos de médio porte. O problema fica por conta dos handhelds, celulares e outros aparelhos pequenos, alimentados por baterias.

Os transmissores 802.11b trabalham com um sinal bastante intenso e por isso também consomem muita energia.

Em termos de velocidade o Bluetooth é capaz de transmitir a apenas 1 Mbps, isto em teoria, já que a velocidade prática cai para apenas 700Kbps graças aos sinais de controle e modulação. Em compensação, o Bluetooth é uma tecnologia mais barata que o 802.11b.

Atualmente os transmissores já custam, para os fabricantes, cerca de 20 dólares ou menos por unidade, um quinto do preço de uma placa de rede 802.11b.

Outra diferença é que os transmissores Bluetooth trabalham com uma potência mais baixa e são menores.

Isso permite que eles consumam menos energia, permitindo que sejam usados também em pequenos aparelhos. Os transmissores são bastante compactos, alguns um pouco maiores do que um palito de fósforo.

Devido a sua baixa velocidade de transmissão, a idéia agora é usar as redes Ethernet ou o 802.11b para ligar os PCs e notebooks em rede e o Bluetooth como um complemento para conectar periféricos menores, como Handhelds, celulares, e até mesmo periféricos de uso pessoal, como teclados, mouses, fones de ouvido, etc.

Fone de ouvido Bluetooth

O Bluetooth serviria então como uma opção às interfaces USB, seriais e paralelas para a conexão de periféricos. De fato, a velocidade permitida pelo Bluetooth é bem mais baixa que a das interfaces USB (12Mbps contra apenas 1Mbps).

14.4 - Funcionamento do Bluetooth

Numa rede Bluetooth, a transmissão de dados é feita através de pacotes, como na Internet.

Para evitar interferências e aumentar a segurança, existem 79 canais possíveis (23 em alguns países onde o governo reservou parte das frequências usadas).

Os dispositivos Bluetooth têm capacidade de localizar dispositivos próximos, formando as redes de transmissão, chamadas de “piconet”. Uma vez estabelecida a rede, os dispositivos determinam um padrão de transmissão, usando os canais possíveis.

Isto significa que os pacotes de dados serão transmitidos cada um em um canal diferente, numa ordem que apenas os dispositivos da rede conhecem.

Isto anula as possibilidades de interferência com outros dispositivos Bluetooth próximos (assim como qualquer outro aparelho que trabalhe na mesma frequência) e torna a transmissão de dados mais segura, já que um dispositivo "intruso", que estivesse próximo, mas não fizesse parte da rede simplesmente não compreenderia a transmissão.

Naturalmente existe também um sistema de verificação e correção de erros, um pacote que se perca ou chegue corrompido ao destino será retransmitido, assim como acontece em outras arquiteturas de rede.

Para tornar as transmissões ainda mais seguras, o padrão inclui também um sistema de criptografia. Existe também a possibilidade de acrescentar camadas de segurança via software, como novas camadas de criptografia, autenticação, etc.

14.5 - Consumo elétrico do Bluetooth

Os dispositivos Bluetooth possuem um sistema de uso inteligente da potência do sinal.

Se dois dispositivos estão próximos, é usado um sinal mais fraco, com o objetivo de diminuir o consumo elétrico, se por outro lado eles estão distantes, o sinal vai ficando mais forte, até atingir a potência máxima.

Dentro do limite dos 10 metros ideais, o consumo de cada transmissor fica em torno de 50 microampères, algo em torno de 3% do que um celular atual, bem menos do que outras tecnologias sem fio atuais.

O baixo consumo permite incluir os transmissores em notebooks, celulares e handhelds sem comprometer muito a autonomia das baterias.

14.6 – Padrões IEEE 802.11a, 802.11b, 802.11g

O **IEEE 802.11b** utiliza a frequência de 2.4GHz, a mesma utilizada por outros padrões de rede sem fio e pelos microondas, todos potenciais causadores de interferência.

A figura a seguir ilustra um adaptador de rede sem fio de 2.4GHz.

Adaptador de rede (wireless) padrão 2.4GHz

O **IEEE 802.11a** por sua vez utiliza a frequência de 5GHz, onde a interferência não é problema.

Graças à frequência mais alta, o padrão também é quase cinco vezes mais rápido, atingindo respeitáveis 54Mbps.

Note que esta é a velocidade de transmissão "bruta" que inclui todos os sinais de modulação, cabeçalhos de pacotes, correção de erros, etc. a velocidade real das redes 802.11a é de 24 a 27Mbps, pouco mais de 4 vezes mais rápido que no 802.11b.

Outra vantagem é que o 802.11a permite um total de 8 canais simultâneos, contra apenas 3 canais no 802.11b. Isso permite que mais pontos de acesso sejam utilizados no mesmo ambiente, sem que haja perda de desempenho.

O grande problema é que o padrão também é mais caro, por isso a primeira produção vai ser destinada ao mercado corporativo, onde existe mais dinheiro e mais necessidade de redes mais rápidas.

Além disso, por utilizarem uma frequência mais alta, os transmissores 802.11a também possuem um alcance mais curto, teoricamente metade do alcance dos transmissores 802.11b, o que torna necessário usar mais pontos de acesso para cobrir a mesma área, o que contribui para aumentar ainda mais os custos.

Ao contrário do que o nome sugere, o 802.11a é um padrão mais recente do que o 802.11b. Na verdade, os dois padrões foram propostos pelo IEEE na mesma época, mas o 802.11b foi finalizado antes e por isso chegou ao mercado com antecedência. Os primeiros periféricos 802.11a foram lançados em novembro de 2001.

O **IEEE 802.11g** é um padrão recentemente aprovado pelo IEEE, que é capaz de transmitir dados a 54Mbps, assim como o 802.11a.

A principal novidade é que este padrão utiliza a mesma faixa de frequência do 802.11b atual: 2.4GHz. Isso permite que os dois padrões sejam inter compatíveis.

A idéia é que se possa montar uma rede 802.11b agora e posteriormente adicionar placas e pontos de acesso 802.11g, mantendo os componentes antigos, assim como hoje em dia temos liberdade para adicionar placas e hubs de 100Mbps a uma rede já existente de 10Mbps.

A velocidade de transferência nas redes mistas pode, ou ser de 54Mbps ao serem feitas transferências entre pontos 802.11g ou de 11Mbps quando um dos pontos 801.11b estiver envolvido, ou então ser de 11Mbps em toda a rede, dependendo dos componentes que forem utilizados. Esta é uma grande vantagem sobre o 802.11a, que também transmite a 54Mbps, mas é incompatível com os outros dois padrões.

15 – REDES HOME

15.1 - Home PNA

Este é um padrão para transmissão de dados através de cabos telefônicos comuns a curtas distâncias.

A idéia é que os usuários interessados em montar uma rede doméstica mas que não tenham como passar cabos de rede pela casa, possam aproveitar as extensões telefônicas já existentes para ligar seus micros em rede.

Existem duas versões deste padrão: a versão 1.0, já obsoleta, transmite a apenas 1Mbps, muito pouco se comparado às redes Ethernet, enquanto a versão 2.0 já transmite a 10Mbps, uma velocidade próxima à das redes 802.11b.

Os dispositivos Home PNA utilizam uma arquitetura de rede ponto a ponto, sem a necessidade de usar nenhum tipo de hub ou concentrador e os sinais não interferem com as ligações de voz, nem com os serviços de acesso via ADSL, já que ambos utilizam frequências diferentes.

A distância máxima entre os pontos é de 330 metros e, é possível utilizar em redes de até 50 PCs. É possível conectar mais PCs caso necessário, mas quanto maior o número de PCs, maior o número de colisões de pacotes e pior o desempenho.

O uso do Home PNA só é viável caso já existam extensões telefônicas para todos os PCs, caso contrário, será mais vantajoso usar as velhas redes Ethernet, que são mais rápidas e mais baratas.

Em termos de custo, temos uma faixa intermediária entre as redes Ethernet e as redes Wireless. Nos EUA cada placa PCI custa de 40 a 60 dólares, dependendo do modelo, menos da metade do preço das placas 802.11b, mas ainda, um custo um pouco elevado.

No Brasil estes produtos ainda não são muito comuns, mas os preços não são muito mais altos que isto. Além dos PCI, existem também alguns modelos USB, que são um pouco mais caros.

Como esta é uma tecnologia destinada a usuário domésticos, o mais comum é os fabricantes oferecerem os produtos na forma de kits, com duas placas de rede, ao invés de vendê-los de forma unitária.

A figura a seguir ilustra um desses kits para uso doméstico.

Kit com placas Home PNA

Fora a praticidade de poder utilizar as extensões telefônicas, as redes Home PNA não oferecem vantagens sobre as redes Ethernet e por isso não são tão difundidas quanto as redes sem fio.

Apesar disso, as placas são relativamente baratas, o que deve garantir a sobrevivência do padrão pelo menos até que as redes sem fio tornem-se mais acessíveis.

Apesar de não serem mais produzidas, ainda existe oferta de placas de 1 Mbps, que são suficientes apenas para compartilhar a conexão com a Internet e transferir pequenos arquivos.

É possível misturar placas de 1 e 10Mbps na mesma rede mas, neste caso, as placas de 10Mbps passarão a trabalhar a apenas 1Mbps para manter compatibilidade com as placas mais lentas.

15.2 - HomePlug Powerline

Esta é mais uma tecnologia que segue a idéia de utilizar os cabos que já temos em casa ao invés de instalar mais cabos para a rede.

Mas, enquanto o Home PNA permite usar as extensões telefônicas, o HomePlug permite utilizar a própria fiação elétrica da casa, algo ainda mais prático.

Apesar dos cabos elétricos não serem exatamente um meio adequado para a transmissão de dados, o HomePlug permite velocidades mais altas que o 802.11b e o HomePNA, 20Mbps no total ou 14Mbps reais, descontando o protocolo de correção de erros utilizado para garantir a confiabilidade das transmissões através de um meio tão hostil quanto os cabos elétricos.

Descontando todas as perdas com as várias camadas de modulação e protocolos, temos velocidades de transmissão de dados de 8 a 9Mbps, uma marca respeitável, que supera por uma boa margem os 7Mbps reais das redes Ethernet de 10Mbps.

O padrão HomePlug 1.0 foi estabelecido em Julho de 2001 e os primeiros produtos começaram a ser lançados em Novembro ou seja, trata-se de um padrão bastante novo.

Não existe um número máximo de dispositivos que podem ser adicionados à rede, mas a banda é compartilhada entre todos os dispositivos. Quanto mais dispositivos, pior será o desempenho.

O maior problema do HomePlug é que os sinais da rede se propagam por toda a instalação elétrica até o transformador da rua. Isto é um problema sobretudo em apartamentos e conjuntos residenciais, onde é comum cada prédio ou bloco compartilhar o mesmo transformador.

Caso um número grande de moradores resolvesse usar redes HomePlug, sem dúvida a velocidade de transmissão cairia bastante.

Para garantir pelo menos a privacidade dos usuários, o padrão utiliza o algoritmo de encriptação DES, que utiliza chaves de 56 bits, razoavelmente seguras para os padrões atuais.

Cada interface HomePlug custa em média 100 dólares, apesar de haver perspectiva de queda futuramente, já que o padrão ainda é muito novo.

A tendência é que o sistema se mantenha mais barato que o 802.11b, já que não é necessário utilizar pontos de acesso, os transmissores são mais baratos e não é necessário usar a antena que responde por boa parte dos custo das placas 802.11b

Ainda é muito cedo para dizer se o HomePlug será capaz de conquistar seu espaço competindo diretamente com as redes sem fio, mas sem dúvida o padrão tem potencial para tornar-se uma alternativa viável, principalmente considerando que já está em desenvolvimento o padrão 2.0, que aumentará a velocidade de transmissão para 100Mbps.

15.3 – Home RF

O Home RF é mais um padrão de redes sem fio que utiliza a faixa dos 2.4 GHz, mas que acabou levando a pior com o lançamento do 802.11b.

O Home RF utiliza um protocolo chamado Shared Wireless Access Protocol, onde as interfaces de rede se comunicam diretamente, sem o uso de um ponto de acesso.

Isto diminui o custo da rede, mas também compromete o alcance do sinal, que é de (em condições ideais) apenas 50 metros.

É possível criar redes HomeRF com até 127 nós, mas como o mesmo canal é compartilhado por todos, quanto mais nós mais baixa será a velocidade. O ideal seria criar redes com no máximo 10 nós, segundo o recomendado pelos próprios fabricantes.

A idéia original era que o Home RF fosse um padrão de redes sem fio de baixo custo, o que não se concretizou, já que no auge do padrão as placas não custavam menos de 100 dólares a unidade.

Até aí não temos nenhuma grande desvantagem, já que mesmo hoje em dias as interfaces 802.11b custam nesta faixa de preço (sem incluir o ponto de acesso), o grande problema é que além de tudo o padrão Home RF também é mais lento; apenas 1.6Mbps.

Na época em que foi lançado esta era uma boa marca, já que a versão original do IEEE 802.11 transmitia a apenas 1Mbps e a segunda versão, que já utilizava modo DSS (Digital Satellite System) atingia apenas 2Mbps.

Como o preço das placas 802.11 era mais alto na época, o Home RF tinha tudo para conquistar seu espaço.

Foi então que surgiu o padrão 802.11b, que além de ser mais rápido, conseguiu uma razoável aceitação, permitindo que os fabricantes produzissem os componentes em maior quantidade e baixassem os preços.

O Home RF é um padrão quase esquecido, mas que pode voltar a ser usado em aparelhos de telefone sem fio e outros dispositivos de comunicação, já que o padrão permite a transmissão de 4 chamadas de voz simultâneas.

16 – GIGABIT ETHERNET

Depois dos padrões de 10 e 100Mbps, o passo natural para as redes Ethernet seria novamente multiplicar por 10 a taxa de transmissão, atingindo 1000Mbps. E foi justamente o que aconteceu.

O padrão Gigabit Ethernet começou a ser desenvolvido pelo IEEE em 1997 e acabou se ramificando em quatro padrões diferentes.

A figura a seguir ilustra um adaptador de rede Gigabit

Adaptador Gigabit Ethernet

16.1 – 1000BaseLX

O **1000BaseLX** é o padrão mais caro, que suporta apenas cabos de fibra óptica e utiliza a tecnologia *Long Wave Laser*, com laseres de 1300 nanometros. Apesar de, em todos os quatro padrões a velocidade de transmissão ser a mesma, 1Gbps, o padrão 1000BaseLX é o que atinge distâncias maiores.

Usando cabos de fibra óptica com núcleo de 9 mícrons o sinal é capaz de percorrer distâncias de até 5km, enquanto que utilizando cabos com núcleo de 50 ou 62.5 mícrons, com frequências de respectivamente 400 e 500MHz, que são os padrões mais baratos, o sinal percorre 550 metros.

16.2 – 1000BaseSX

O segundo padrão é o **1000BaseSX** que também utiliza cabos de fibra óptica, mas utiliza uma tecnologia de transmissão mais barata, chamada *Short Wave Laser*, que é uma derivação da mesma tecnologia usada em CD-ROMs, com feixes de curta distância.

Justamente por já ser utilizada em diversos dispositivos, esta tecnologia é mais barata, mas em compensação o sinal atinge distâncias menores.

Existem quatro padrões de laseres para o 1000BaseSX. Com laseres de 50 mícrons e frequência de 500MHz, o padrão mais caro, o sinal é capaz de percorrer os mesmos 550 metros dos padrões mais baratos do 1000BaseLX.

O segundo padrão também utiliza laseres de 50 mícrons, mas a frequência cai para 400MHz e a distância para apenas 500 metros.

Os outros dois padrões utilizam laseres de 62.5 mícrons e frequências de 200 e 160MHz, por isso são capazes de atingir apenas 275 e 220 metros, respectivamente.

16.3 - 1000BaseCX

Para distâncias mais curtas existe o **1000BaseCX**, que ao invés de fibra óptica utiliza cabos twiaxiais, um tipo de cabo coaxial com dois fios, que tem a aparência de dois cabos coaxiais grudados.

Este padrão é mais barato que os dois anteriores, mas em compensação o alcance é de apenas 25 metros. A idéia é que ele servisse para interligar servidores em data centers, que estivessem no mesmo rack, ou em racks próximos.

16.4 - 1000BaseT

O padrão que está crescendo mais rapidamente, a ponto de quase condenar os demais ao desuso é o **1000BaseT**, também chamado de *Gigabit Over Copper*, por utilizar os mesmos cabos de par trançado categoria 5 que as redes de 100Mbps atuais.

Isto representa uma enorme economia, não apenas por eliminar a necessidade de trocar os cabos atuais por cabos muito mais caros, mas também nas próprias placas de rede, que passam a ser uma evolução das atuais e não uma tecnologia nova.

O alcance continua sendo de 100 metros e os switches compatíveis com o padrão são capazes de combinar nós de 10, 100 e 1000Mbps, sem que os mais lentos atrapalhem os demais.

Toda esta flexibilidade torna uma eventual migração para o 1000BaseT relativamente simples, já que você pode aproveitar o cabeamento já existente.

Na verdade, muita pouca coisa muda. Note que apesar dos cabos serem os mesmos, o 1000BaseT faz um uso muito mais intensivo da capacidade de transmissão e por isso detalhes como o comprimento da parte destrançada do cabo para o encaixe do conector, o nível de interferência no ambiente, cabos muito longos, etc. são mais críticos.

Com um cabeamento ruim, o índice de pacotes perdidos será muito maior do que numa rede de 100Mbps.

Todos estes padrões de Gigabit Ethernet são inter compatíveis a partir da camada Data Link do modelo OSI.

Abaixo da camada Data Link está apenas a camada física da rede, que inclui o tipo de cabos e o tipo de modulação usado para a transmissão de dados.

Os dados transmitidos, incluindo camadas de correção de erro, endereçamento, etc. são idênticos em qualquer um dos padrões.

Assim como muitos hubs, inclusive modelos baratos permitem juntar redes que utilizam cabos de par trançado e cabo coaxial, é muito simples construir dispositivos que permitam interligar estes diferentes padrões.

Isto permite interligar facilmente seguimentos de rede com cabeamento e cobre e de fibra óptica, que podem ser usados nos locais onde os 100 metros dos cabos categoria 5 não são suficientes.

As placas Gigabit Ethernet podem operar tanto no modo full-duplex, onde os dois lados podem transmitir dados simultaneamente, quanto no modo half-duplex.

O que determina o uso de um modo ou de outro é novamente o uso de um hub ou de um switch.

As placas anunciadas como capazes de operar a 2Gbps, nada mais são do que uma alusão ao uso do modo full-duplex.

Já que temos 1Gbps em cada sentido, naturalmente a velocidade total será de 2 Gigabits.

Mas, na prática não funciona bem assim pois raramente ambas as estações precisarão transmitir grandes quantidades de dados.

O mais comum é uma relação assimétrica, com uma falando e a outra apenas enviando os pacotes de confirmação.

Assim como as placas de 100 megabits, as placas gigabit são completamente compatíveis com os padrões anteriores.

Pode-se até mesmo ligar uma placa Gigabit Ethernet a um hub 10/100 se quiser, mas a velocidade terá de ser nivelada por baixo, respeitando a do ponto mais lento.

Considerando o custo, o mais inteligente é naturalmente usar um switch, ou um PC com várias placas de rede para que cada ponto da rede possa trabalhar na sua velocidade máxima.

16.5 – 10 Gigabit Ethernet

O primeiro padrão de redes 10 Gigabit Ethernet, novamente 10 vezes mais rápido que o anterior, está em desenvolvimento desde 1999 e chama-se 10GBaseX.

Este padrão é bastante interessante do ponto de vista técnico, pois além da velocidade, o alcance máximo é de nada menos que 40km, utilizando cabos de fibra óptica monomodo. Existe ainda uma opção de baixo custo, utilizando cabos multimodo, mas que em compensação tem um alcance de apenas 300 metros.

O 10 Gigabit Ethernet também representa o fim dos hubs. O padrão permite apenas o modo de operação full-duplex, onde ambas as estações podem enviar e receber dados simultaneamente, o que só é possível através do uso de switches.

Isto encarece mais ainda o novo padrão, mas trás ganhos de desempenho consideráveis, já que além de permitir o uso do modo full-duplex, o uso de um switch acaba com as colisões de pacotes.

Outra mudança importante é que, pelo menos por enquanto, sequer é cogitado o desenvolvimento de um padrão que utilize cabos de cobre, pois ainda não se tem idéia se isso seria possível.

Mas, isto não é conclusivo, pois os padrões iniciais do Gigabit também traziam como opções apenas os cabos de fibra óptica. O par trançado veio posteriormente ao lançamento, cerca de dois anos depois.

O 10 Gigabit não se destina a substituir os padrões anteriores, pelo menos a médio prazo.

A idéia é complementar os padrões de 10, 100 e 1000Mbps, oferecendo uma solução capaz e interligar redes distantes com uma velocidade comparável aos backbones DWDM (Dense Wavelength Division Multiplex)[18], uma tecnologia muito mais cara, utilizada atualmente nos backbones da Internet.

Suponha por exemplo que você precise interligar 5.000 PCs, divididos entre a universidade, o parque industrial e a prefeitura de uma grande cidade.

Você poderia utilizar um backbone 10 Gigabit Ethernet para os backbones principais, unindo os servidores dentro dos três blocos e os interligando à Internet, usar uma malha de switches Gigabit Ethernet para levar a rede até as salas, linhas de produção e salas de aula e usar hubs 10/100 para levar a rede até os alunos e funcionários, talvez complementando com alguns pontos de acesso 802.11b para oferecer também uma opção de rede sem fio.

Isto estabelece uma pirâmide, onde os usuários individuais possuem conexões relativamente lentas, de 10 ou 100 megabits, interligadas entre si e entre os servidores pelas conexões mais rápidas e caras, um sistema capaz de absorver várias chamadas de videoconferência simultâneas por exemplo.

Tanto o Gigabit quanto o 10 Gigabit sinalizam que as redes continuarão a ficar cada vez mais rápidas e mais acessíveis. Hoje em dia é possível comprar uma placa 10/100 por volta de 20 reais e, com o barateamento dos novos padrões, estes preços não voltarão a subir.

Com as redes tão baratas, aplicações que estavam fora de moda, como os terminais diskless, terminais gráficos, etc. voltaram a ser atrativas.

Os PCs continuam relativamente caros, mas a banda de rede está muito barata.

Com isto, começa a fazer sentido aproveitar PCs antigos, transformando-os em terminais de PCs mais rápidos.

Um único Pentium III ou Duron pode servir 5, 10 ou até mesmo 20 terminais 486 e com um desempenho muito bom, já que os aplicativos rodam no servidor, não nos terminais.

[18] DWDM - tecnologia de transmissão de dados através em ondas de luz através de fibras óticas; cada sinal tem seu próprio comprimento de onda e pode-se transmitir até 80 canais diferentes em uma única fibra ótica.

17 – PROXY E FIREWALL

17.1 – Proxy

Os servidores de proxy são usados para permitir aos micros de uma rede interna o acesso à Web, FTP e outros serviços mais, no qual ele foi previamente configurado.

O proxy é um servidor especial, que roda em uma máquina que pode agir também como se fosse um Firewall, escondendo os computadores da rede interna.

Basicamente, ele recebe requisições de máquinas que estão na rede interna, envia aos servidores que estão do lado externo da rede, lê as respostas externas e envia de volta o resultado aos clientes da rede interna.

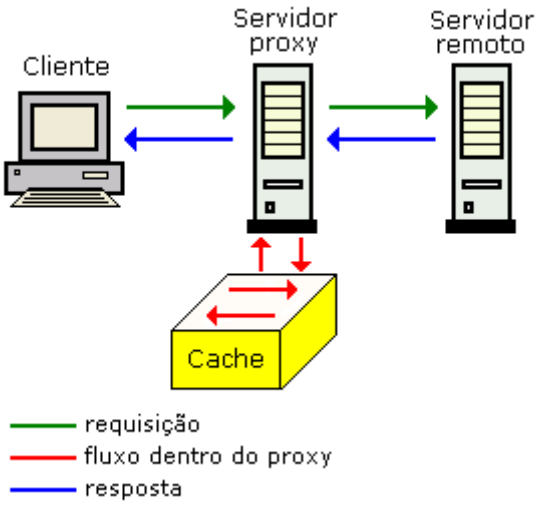
Normalmente, o mesmo servidor proxy é usado para todos os clientes em uma rede interna, que pode ou não ser constituída de sub-redes.

Os tipos de servidores Proxy mais utilizados, são:

A) Os proxies genéricos, que oferecem serviços de proxy para várias aplicações (por exemplo Web, Ftp, Gopher e Telnet) em um único servidor.

B) Os proxies específicos, que oferecem serviços de proxy para uma determinada aplicação, como é o caso do Web Proxy, que é um proxy que tem por finalidade, fazer caching de documentos Web que foram acessados, reduzindo de forma considerável, o tráfego de acesso à Internet em requisições futuras.

Nota: A habilidade de fazer cache dos documentos acessados, tornou atrativo o seu uso dentro de empresas e provedores de acesso à Internet, pois com ele, existe o ganho de "banda virtual", tendo em mente que documentos frequentemente acessados, serão retornados do cache local ao invés de um servidor remoto distante.



Fluxo de informações no proxy

Na ilustração mostrada acima, temos uma demonstração de como funciona o fluxo dentro de um Servidor Proxy (Servidor Web Proxy); ele recebe as requisições, faz uma análise no cache local, e se o documento estiver no cache, ele responde automaticamente, caso contrário, se o documento não estiver no cache, ou se ele estiver precisando de atualização, ele vai ao endereço remoto e busca o documento, ou as atualizações e guarda

no cache local, para ser usado nas requisições futuras.

Os proxies de circuitos, que oferecem conexões virtuais ponto a ponto entre o cliente e o destino final, eles normalmente fazem a autenticação antes de estabelecer a conexão final, agindo como se fosse um controlador.

Esse tipo de proxy, baseia-se livremente no conceito de proxy genérico.

17.2 – Firewall

Firewall é o mecanismo de segurança interposto entre a rede interna e a rede externa com a finalidade de liberar ou bloquear o acesso de computadores remotos aos serviços que são oferecidos em um perímetro ou dentro da rede corporativa.
Este mecanismo de segurança pode ser baseado em hardware, software ou uma mistura dos dois.

Três fatores estão em risco quando nos conectamos a Internet, são eles, a reputação, os computadores e as informações guardadas, e três fatores precisam ser resguardados, a privacidade, a integridade e a disponibilidade.

Existem situações de riscos como, roubo de conexão depois dela ter sido autenticada, espionagem de dados secretos enquanto em trânsito pela rede e um usuário não autenticado convence a rede que ele foi autenticado.

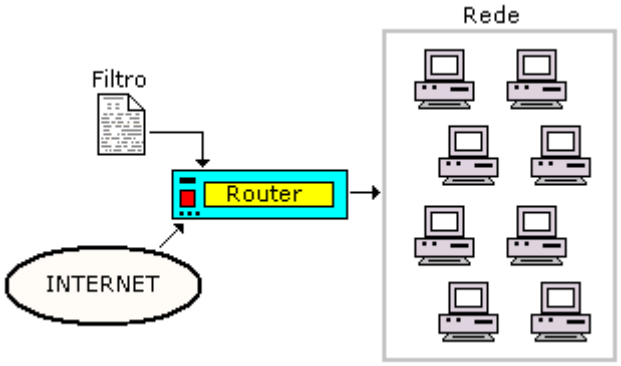
O firewall é o ponto de conexão com a Internet, tudo o que chega à rede interna deve passar pelo firewall, ele é também o responsável por aplicar as regras de segurança, autenticar usuários, logar tráfego para auditoria e deve limitar a exposição dos hosts internos aos hosts da Internet, entretanto, algumas tarefas não podem ser executadas, como, proteger a rede contra usuários internos mal intencionados, conexões que não passam por ele, ameaças novas, no qual ele não foi parametrizado para executar uma ação.

17.3 - Arquiteturas de Firewall

Normalmente, as empresas preferem implementar um firewall baseado apenas em uma máquina, seja ele um host PC ou um roteador, entretanto, os firewalls mais robustos, são compostos de várias partes. Veja algumas arquiteturas a seguir:

17.3.1 - Roteador com Triagem (Screening Router)

Essa é a maneira mais simples de se implementar um firewall, pois o filtro, apesar de ser de difícil elaboração, é rápido de se implementar e seu custo é zero, entretanto, se as regras do roteador forem quebradas, a rede da empresa ficará totalmente vulnerável.

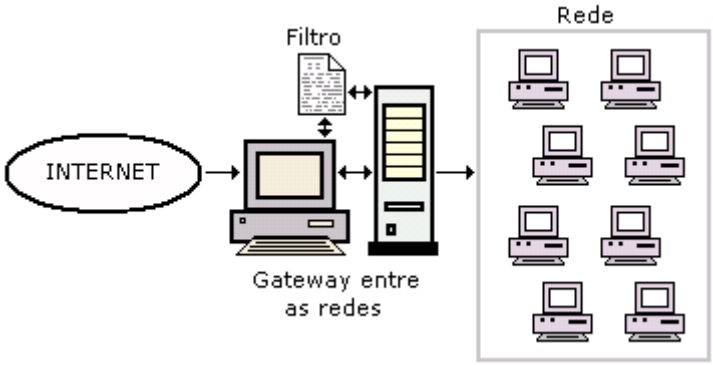


Roteador com triagem

17.3.2 - Gateway de Base Dupla (Dual Homed Gateway)

Aqui, é posto uma única máquina com duas interfaces de rede entre as duas redes (a Internet e a rede da empresa).

Quase sempre, esse Gateway, chamado de Bastion Host (host guardião) conta com um proxy de circuito para autenticar o acesso da rede da empresa para a internet e filtrar o acesso da Internet contra a rede da empresa. Como na arquitetura anterior, se o proxy for desativado, a rede da empresa ficará totalmente vulnerável.

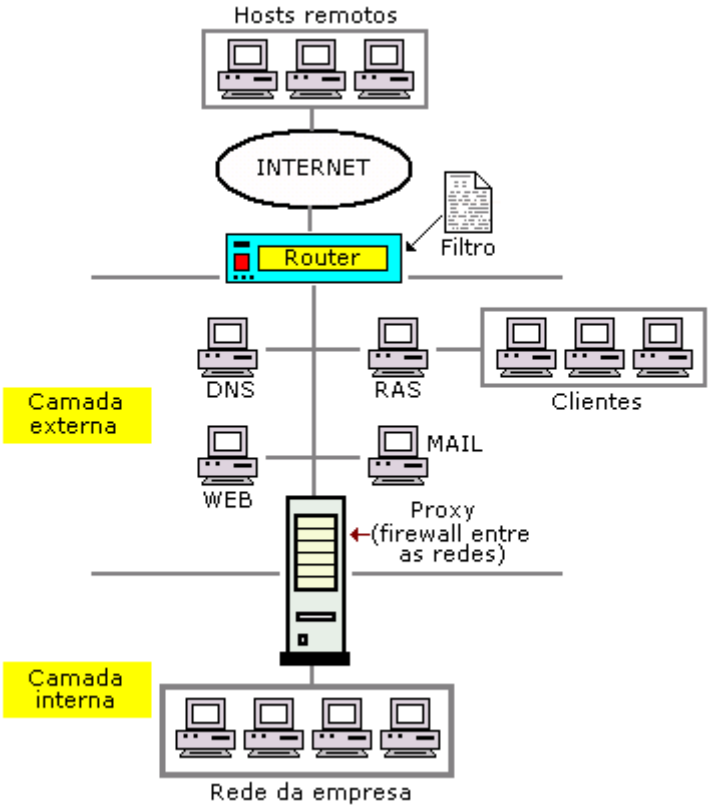


Dual Homed Gateway

Bastion Host é qualquer computador configurado para desempenhar algum papel crítico na segurança da rede interna, ele fica publicamente presente na Internet, provendo os serviços permitidos pela política de segurança da empresa.

17.3.3 - Gateway Host com Triagem (Screened Host Gateway)

Roteador e Gateway aqui, são usados conjuntamente em uma arquitetura, formando assim, duas camadas de proteção. Veja a figura a seguir.



Gateway com triagem (Screened Host Gateway)

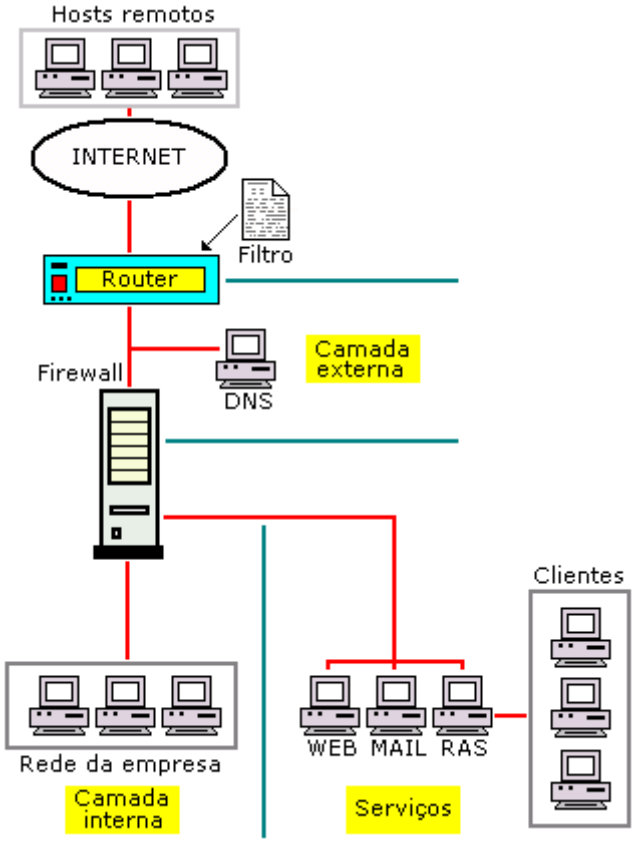
A primeira camada, é a rede externa, que está interligada com a Internet através do roteador, nesta camada a rede só conta com o "filtro de pacotes" que está implementado

no roteador e tem como finalidade aceitar ou bloquear pacotes de rede seguindo as regras definidas pela política administrativa da empresa.

A segunda camada, é a rede interna, e quem limita os acessos neste ponto é um Bastion Host com um "proxy firewall", pois nele temos um outro filtro de pacotes além de mecanismos de autenticação da própria rede interna.

17.3.4 - Sub-rede com Triagem (Screened Subnet)

Roteador e Gateway, são usados aqui também conjuntamente em uma arquitetura que é bem parecida com a arquitetura anterior, entretanto a camada de serviços nesta, fica na mesma linha da camada interna, atrás do Bastion Host Gateway, em uma das sub-redes que podem ser criadas nele, fortalecendo bem os serviços contra ataques externos. Veja a figura a seguir.



Sub-rede com triagem (Screened Subnet)

A primeira camada, é a externa, que está interligada com a Internet através do roteador, nesta camada a rede só conta com o "filtro de pacotes" que está implementado no roteador, e tem como finalidade aceitar ou bloquear pacotes de rede seguindo as regras definidas pela política administrativa da empresa.

A segunda camada, está dividida em duas partes, a de serviços prestados (Exemplo, E-mail, Web, Ftp e Ras) e a interna (rede da empresa), e elas, recebem duas filtragens, a do roteador e a do próprio programa Firewall. Esta camada utiliza também uma outra técnica chamada NAT (Network Address Translator), que tem por finalidade transcrever números de internet em números privados, fortalecendo bem a transparência da camada.

17.3.5 – Características importantes

Autenticação - Processo que verifica a identidade de um usuário para assegurar de que o mesmo que está pedindo o acesso, seja de fato, o mesmo a quem o acesso é autorizado.

Controle de Acesso - Processo que bloqueia ou permite conexões de entrada ou de saída baseado em filtros de acesso ou através de mecanismos inteligentes que detectam o uso abusivo, bloqueando o acesso temporariamente.

Compatibilidade - O firewall deve permitir o pleno funcionamento dos serviços prestados na rede, bem como, interagir ou até mesmo se integrar com as aplicações servidoras escolhidas pela corporação.

Auditoria - Processo vital na detecção de vulnerabilidades e acessos indevidos.

Flexibilidade - Facilidade no uso, ferramentas de administração de boa compreensão e suporte técnico.

Considerações finais:

Um bom programa de segurança de rede, é construído por um conjunto de programas e técnicas que tem por finalidade liberar ou bloquear serviços dentro de uma rede interligada à Internet, de forma controlada.

Embora o firewall seja a parte mais importante em um programa de segurança, não devemos nos esquecer da importância de se utilizar ferramentas que auxiliam na detecção de brechas e vulnerabilidades dos sistemas operacionais que estão em uso na rede, com a finalidade de detectar intrusos ou ataques. É importante também, saber a ação que deverá ser tomada quando uma violação ou um serviço importante parar.

17.4 – NAT (Network Address Translator)

NAT (**Network Address Translator**) é um tradutor de endereços de rede que visa otimizar a utilização dos endereços IP, uma vez que o crescimento da Internet tem sido muito grande tornando escassos tais endereços IP e como sabemos, para que uma máquina tenha acesso à rede, é preciso ter um endereço IP válido.

O NAT é uma das soluções que existem para a economia de endereços IP. Para o tradutor funcionar, é preciso usar endereços IP privados e é importante observar que tais endereços só podem ser utilizados em redes corporativas, pois, não são propagados pela Internet.

O NAT abordado neste artigo, é do tipo que é utilizado em roteadores, mas, ele também é aplicado nos firewalls e nos proxies.

Além de fazer economia de endereços IP, ele é o responsável por manter a rede interna transparente. Os endereços IP reservados estão definidos na RFC 1918, através do órgão IANA (Internet Assigned Numbers Authority) e suas faixas são:

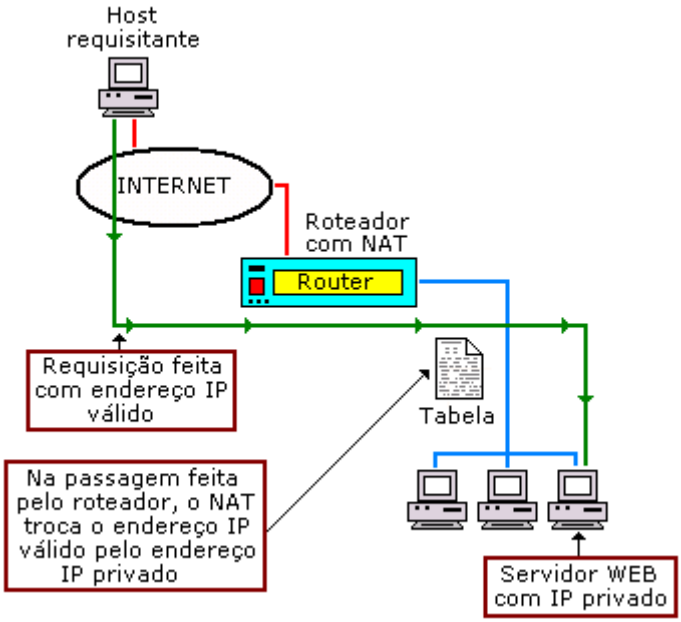
10.0.0.0 até 10.255.255.255 (10/8 prefix)
172.16.0.0 até 172.31.255.255 (172.16/12 prefix)
192.168.0.0 até 192.168.255.255 (192.168/16 prefix)

O tradutor NAT, tem três finalidades principais:

1. Cria um tipo especial de firewall, escondendo os endereços IP internos;

2. Habilita uma empresa a utilizar maior quantidade endereços IP internos. Desde que esses endereços sejam usados somente internamente, não há possibilidade de conflitos com endereços IP de outras empresas;
3. Permite a empresa combinar várias conexões ISDN dentro de uma conexão de Internet simples.

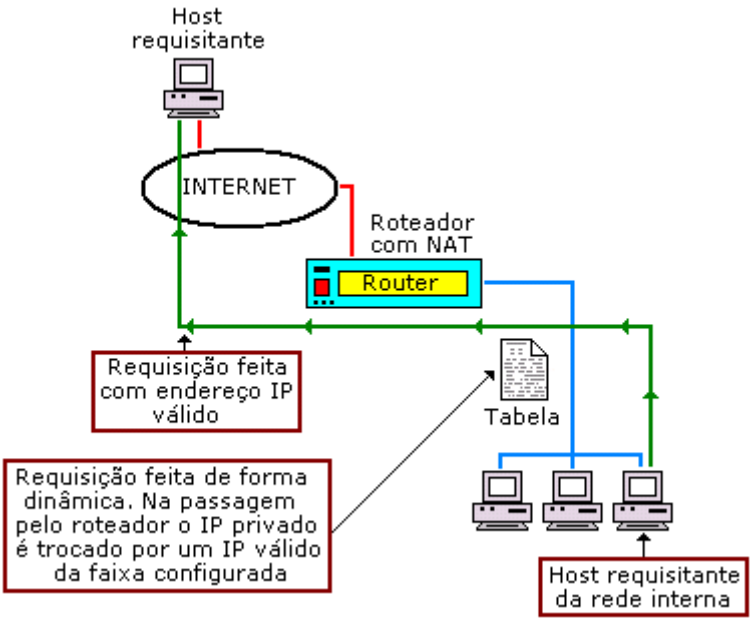
A tradução pode ocorrer de forma estática, onde se estabelece uma relação entre endereços locais e endereços da Internet, ou dinâmica, onde o mapeamento de endereços locais e endereços da Internet é feito conforme a necessidade de uso. As traduções estáticas, são úteis quando disponibilizamos serviços na rede interna, como exemplo, um site Web. A figura a seguir ilustra um processo de tradução estática.



Tradução estática

Nestas condições, quando o pedido de conexão chega ao roteador, o NAT consulta a tabela de endereços e transcreve para o IP interno correspondente, permitindo assim, que seja possível fazer uma conexão no sentido da Internet para a rede interna.

A figura a seguir ilustra um processo de tradução dinâmica.



Tradução dinâmica

As traduções dinâmicas, são úteis quando, se pretende dar acesso aos computadores no sentido da rede corporativa para Internet, e ela funciona da seguinte maneira:

O computador da rede corporativa faz uma requisição que passa pelo roteador e ele, aloca em sua tabela, o endereço da máquina interna que requisitou a informação e o endereço Internet configurado no roteador (esse endereço pode ser único ou uma faixa de endereços).

Quando os dados retornam da Internet, o NAT consulta a tabela de traduções e responde à máquina que fez a requisição.

18 – VPN

VPN (Virtual Private Network) ou Rede Privada Virtual, é uma rede privada construída sobre a infra-estrutura de uma rede pública, normalmente a Internet.

Na VPN, ao invés de se utilizar links dedicados ou redes de pacotes (como Frame Relay e X.25) para conectar redes remotas, utiliza-se a infra-estrutura da Internet.

A grande adesão às redes privadas virtuais ocorre principalmente pelo lado financeiro, pois os links dedicados são caros, e do outro lado está a Internet, que por ser uma rede de alcance mundial, tem pontos de presença espalhados pelo mundo.
Conexões com a Internet em geral tem um custo mais baixo que links dedicados, principalmente quando as distâncias são grandes, e esse tem sido o motivo pelo qual, as empresas cada vez mais utilizam a infra-estrutura da Internet para conectar a rede privada.

A utilização da Internet como infra-estrutura de conexão entre hosts da rede privada é uma ótima solução em termos de custos mas, não em termos de privacidade, pois a Internet é uma rede pública, onde os dados em trânsito podem ser lidos por qualquer equipamento.

Isto então compromete a segurança e a confidencialidade das informações da empresa. Como solucionar isso?

A adoção da criptografia é a solução mais confiável para tal. Incorporando criptografia na comunicação entre hosts da rede privada, se os dados forem capturados durante a transmissão, não poderão a princípio, serem decifrados.

Os túneis virtuais habilitam o tráfego de dados criptografados pela Internet e esses dispositivos, são capazes de entender os dados criptografados formando uma rede virtual segura sobre a rede Internet.

Os dispositivos responsáveis pelo gerenciamento da VPN devem ser capazes de garantir a privacidade, integridade, autenticidade dos dados.

18.1 – Implementação de uma VPN

Basicamente uma VPN pode ser feita de duas formas.

A primeira forma um simples host em trânsito, conecta-se em um provedor Internet e através dessa conexão, estabelece um túnel virtual com a rede remota.

Nesse túnel estão contidas as informações criptografadas.
Os protocolos utilizados no túnel virtual são:

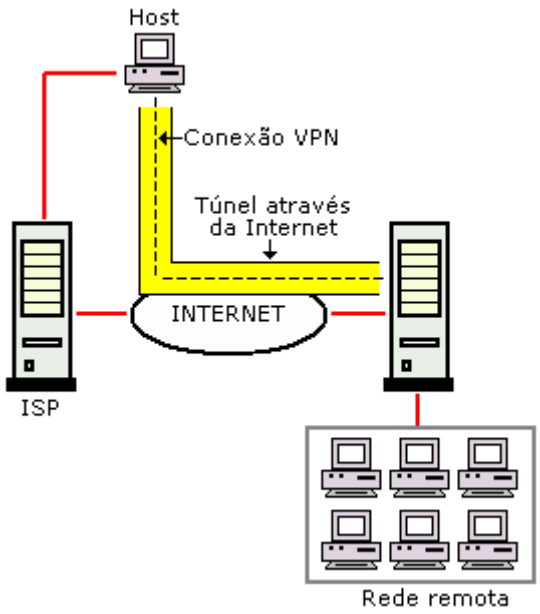
- (IPSec) Internet Protocol Security
- (L2TP) Layer 2 Tunneling Protocol
- (L2F) Layer 2 Forwarding
- (PPTP) Point-to-Point Tunneling Protocol

O protocolo escolhido, será o responsável pela conexão e a criptografia entre os hosts da rede remota.

Eles podem ser normalmente habilitados através de um servidor firewall ou RAS que esteja trabalhando com um deles agregado.

A figura a seguir demonstra ilustra uma conexão de uma VPN com um host.

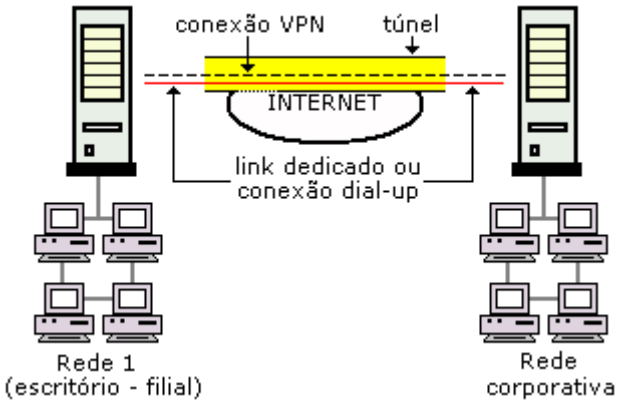
Observa-se que existe uma ligação entre o host e a rede remota através da Internet em um túnel virtual, onde estão os dados criptografados.



Conexão VPN entre um host e uma rede remota

Uma outra forma (segunda forma) é a interligação de duas redes através de hosts com link dedicado ou discado via internet, formando assim um túnel entre as duas redes.

A figura a seguir ilustra essa forma.



Conexão VPN entre duas redes interligadas

18.2 – Conexão a uma VPN

Uma VPN, ou rede privada virtual é uma rede de longa distância que usa a Internet como meio de comunicação.

Numa VPN o servidor só precisa ter um link dedicado ou dial-up para que qualquer usuário da rede possa acessá-lo de qualquer parte do mundo usando a Internet.

O Windows 98 ou ME pode atuar apenas como cliente de uma VPN, o servidor obrigatoriamente deve estar rodando Windows 2000 server ou qualquer outro tipo de sistema que opere como servidor.

Para conectar-se a uma VPN basta marcar a “Rede Particular Virtual” que aparece dentro da pasta “Comunicações” durante a instalação do Windows.

Se o Windows 98 já estiver instalado, siga os procedimentos a seguir:

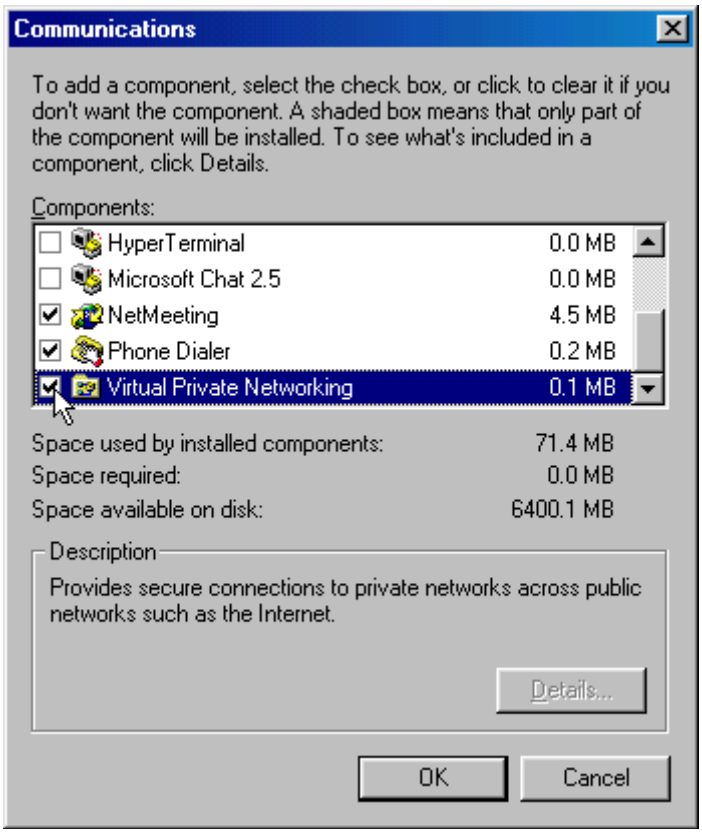
1) Abra o ícone Adicionar/remover programas (Add/Remove Programs) no Painel de controle;

2) Clique no guia Instalação do Windows (Windows Setup);

4) Clique na opção Comunicações (Communications);

5) Clique em Detalhes (Details);

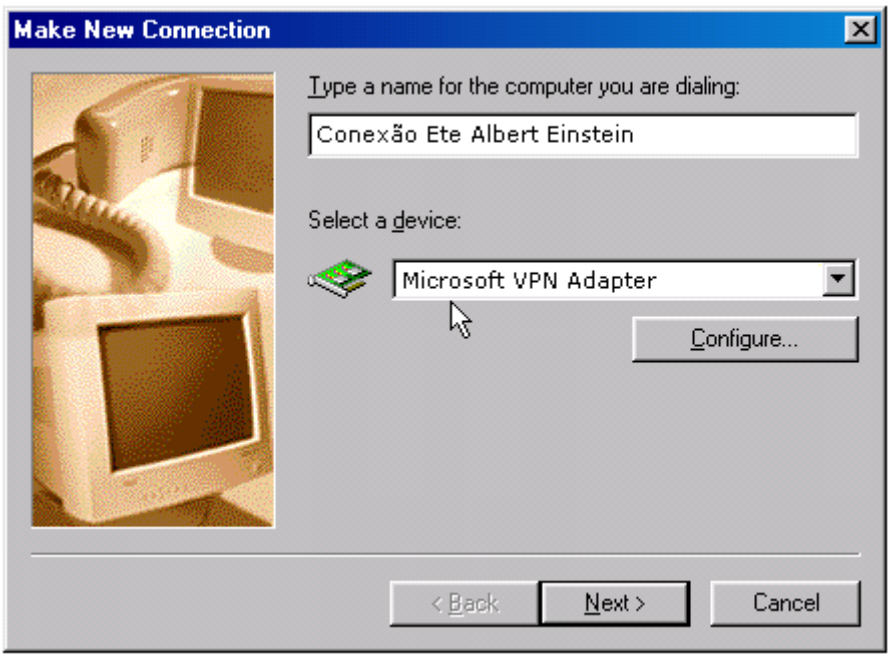
6) Clique em Rede Particular Virtual (Virtual Private Network);



Instalação da VPN no Windows 98

7) Com o programa cliente instalado, abra a janela de acesso à rede dial-up e clique em Fazer Nova Conexão (Make New Connection).

8) Digite o nome do servidor VPN e no campo Selecionar um Dispositivo (Select a Device) escolha “Microsoft VPN Adapter”, conforme ilustra a figura a seguir.

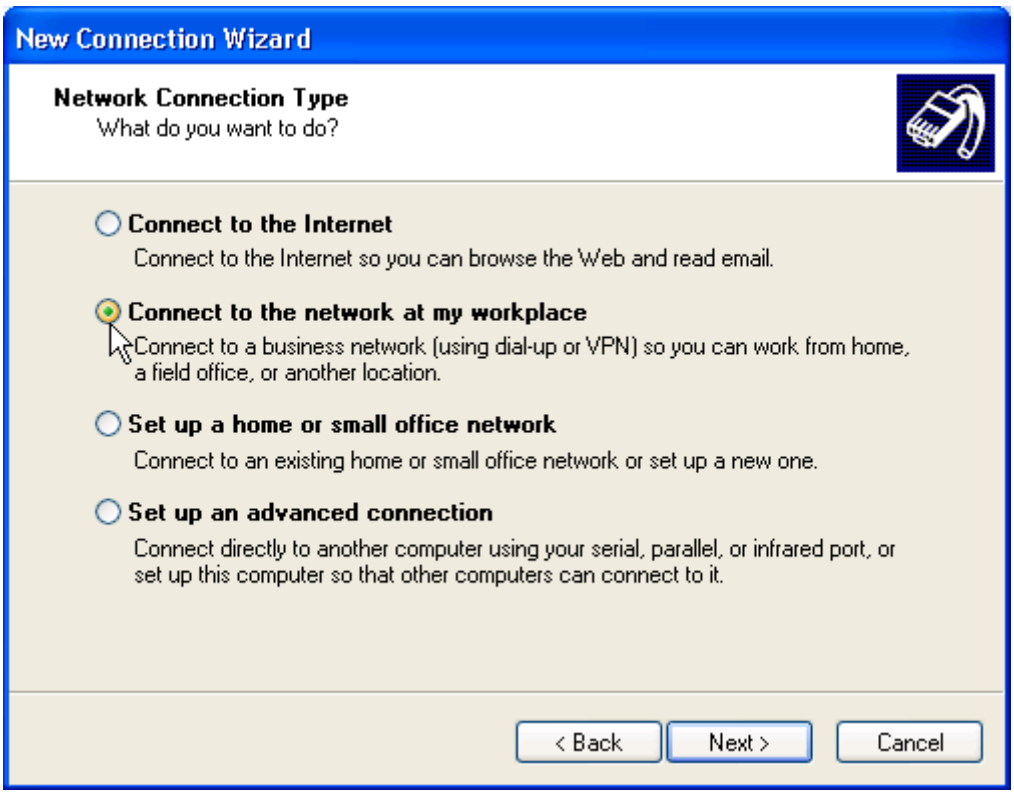


Para conectar-se à VPN através do Windows XP, proceda da seguinte forma:

1) Abra o Painel de Controle (Control Panel);

2) Clique em Network Connections (Conexões de Rede);

3) Em Tarefas de Rede (Network Tasks) selecione Criar uma nova conexão (Create a new connection);



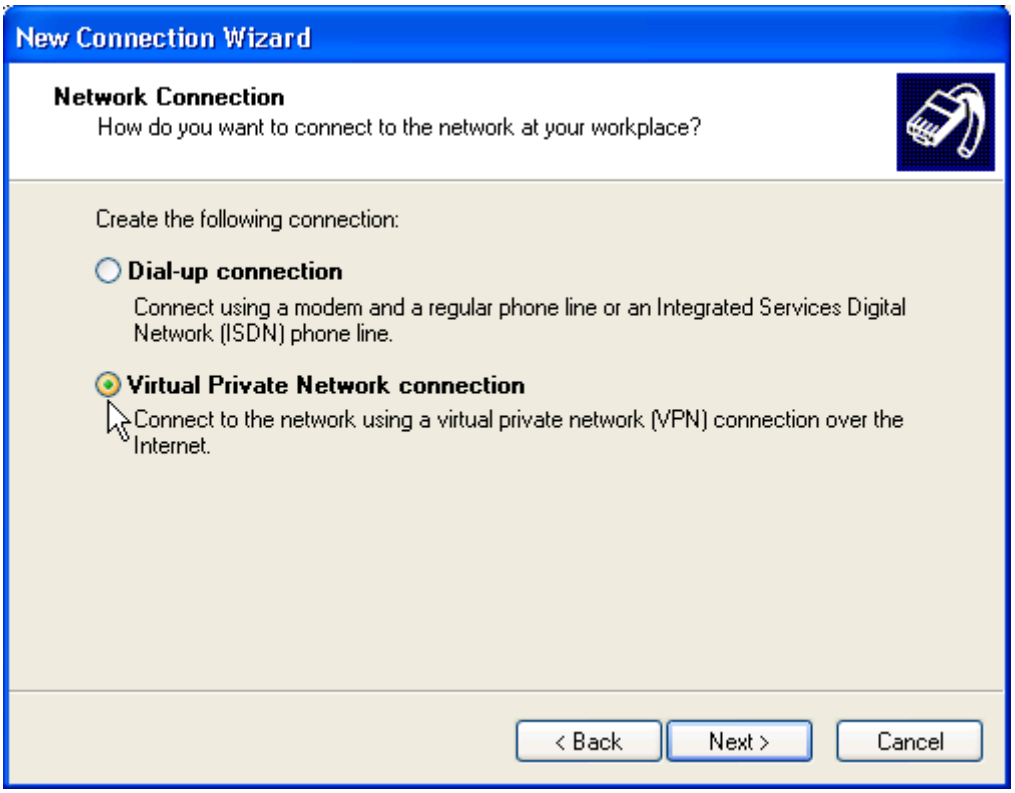
4) Ao aparecer a caixa de diálogo Assistente para Novas Conexões (New Connection Wizard) clique em Avançar (Next);

5) Oriente-se pelas caixa de diálogo a seguir, clicando em Conectar-me a uma rede em meu local de trabalho (Connect to the network at my workplace) e a seguir em Avançar (Next);

Ao conectar-se a uma rede no local de trabalho, usando VPN ou dial-up, será possível acessar todos os dados necessários da empresa de qualquer lugar do mundo, lembrando que o canal para estabelecer esse tipo de comunicação é a Internet.

6) Na próxima caixa de diálogo, selecione a opção Conexão VPN (rede virtual privada) (Virtual Private Network connection);

Observe que nessa opção a conexão VPN está vinculada à Internet, que formará então um túnel para o tráfego das informações.

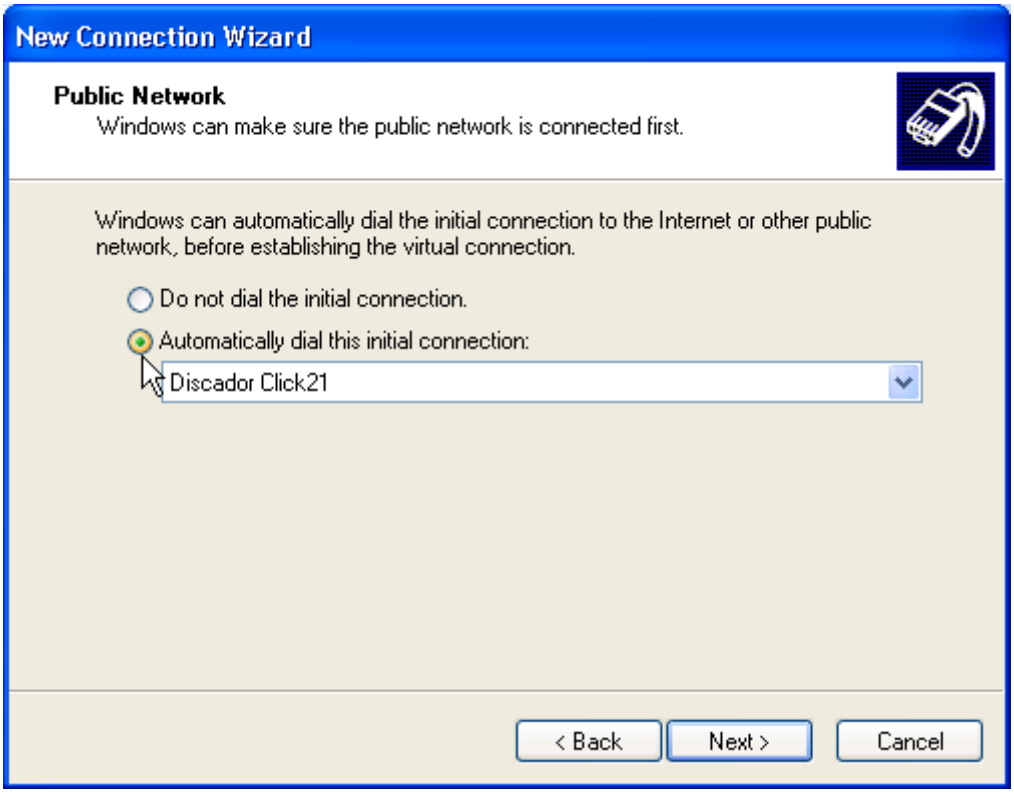


7) Digite o nome da empresa;
(por exemplo: você pode digitar o nome do seu local do trabalho ou o nome do servidor ao qual irá se conectar).

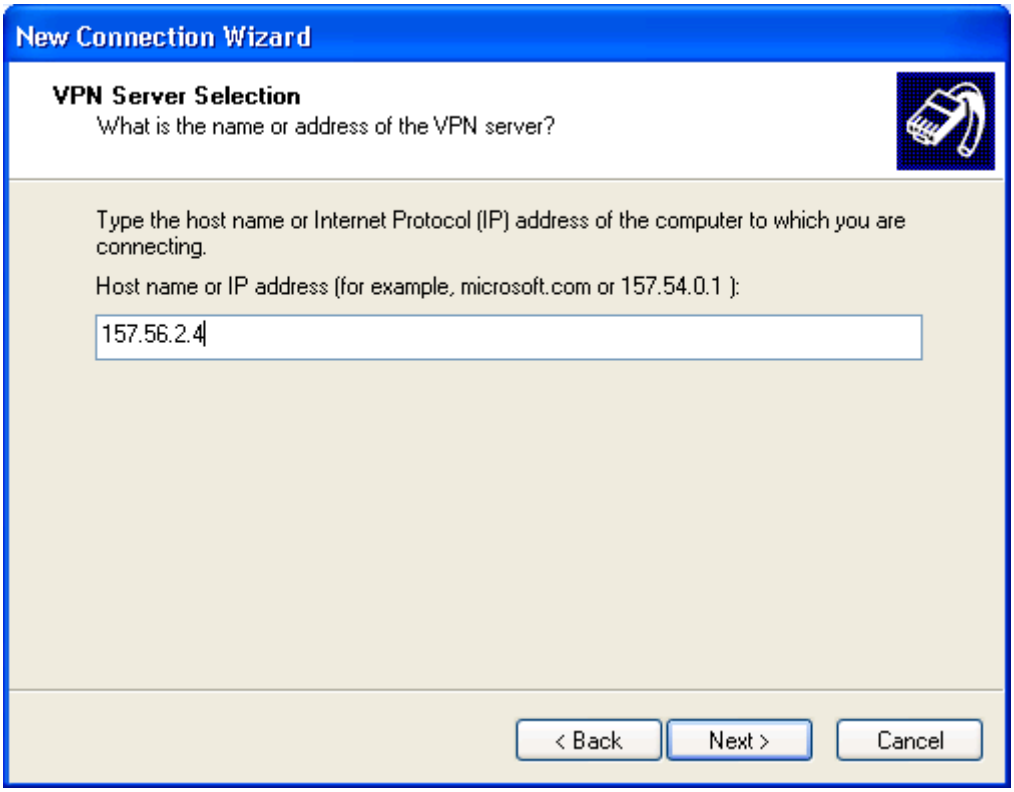
A caixa de diálogo mostrada a seguir mostra um local específico, por exemplo, o laboratório de informática ESF1.

Neste caso estará sendo conectado ao servidor do referido laboratório.

O Windows pode certificar-se de que a rede pública está conectada, e para isso, basta selecionar uma das opções na próxima caixa de diálogo, ou seja, use o discador padrão ou opte por não iniciar nenhum tipo de conexão.



8) Para concluir, digite o nome para conexão ou o endereço IP;



Ao clicar em Avançar (Next), a conexão VPN estará criada.

Aparecerá uma caixa de diálogo indicando que a conexão foi criada com sucesso após os passos sugeridos pelo Assistente de Nova Conexão.

Você poderá optar ainda, por adicionar o ícone correspondente a essa conexão na área de trabalho (Desktop).

19 – COMO FUNCIONA O PROTOCOLO FTP

O **FTP** (*File Transfer Protocol*) é uma opção comum e oferece um meio viável de transferir arquivos na Internet. Dos seus serviços, o mais comum é o FTP anônimo, pois este, permite o download de dados e arquivos contidos nos sites sem a necessidade de autenticação.

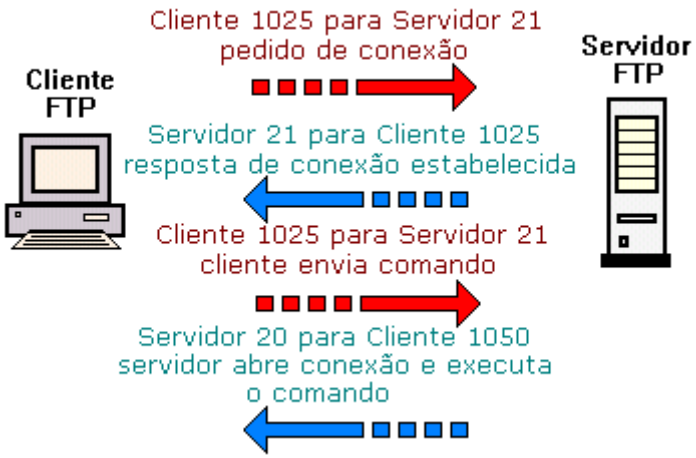
Ele é utilizado também de forma personalizada e automática em soluções que trabalham como o EDI (Eletronic Data Interchange), onde Matriz e Filial trocam arquivos de dados com a finalidade de sincronizar seus bancos de dados.

Os programas que aceleram download, também se utilizam do protocolo FTP, sendo que estes, usam tecnologia de empacotamento e quebra dos arquivos conseguindo assim, uma melhora significativa na velocidade do download.

19.1 – O FTP no modo padrão

O protocolo FTP utiliza duas conexões TCP, a primeira é conhecida como "*Ftp-controle*" que é estabelecida pelo cliente em uma porta TCP de número alto (1025 a 65535) e se comunica com o servidor de FTP em uma porta TCP padrão, número 21. Essa conexão diz ao servidor qual(is) arquivo(s) o cliente deseja e permite a passagem de outras informações de controle (comandos por exemplo).

Contudo, quando chega à hora de transferir os dados reais, uma segunda conexão, conhecida como "*Ftp-dados*" será aberta. Diferente da conexão de controle, essa conexão é aberta pelo servidor na porta TCP 20 e se comunica com o *FTP* cliente em uma porta TCP que é atribuída dinamicamente e não é privilegiada (o cliente e o servidor negociam a porta como parte da troca de controle).

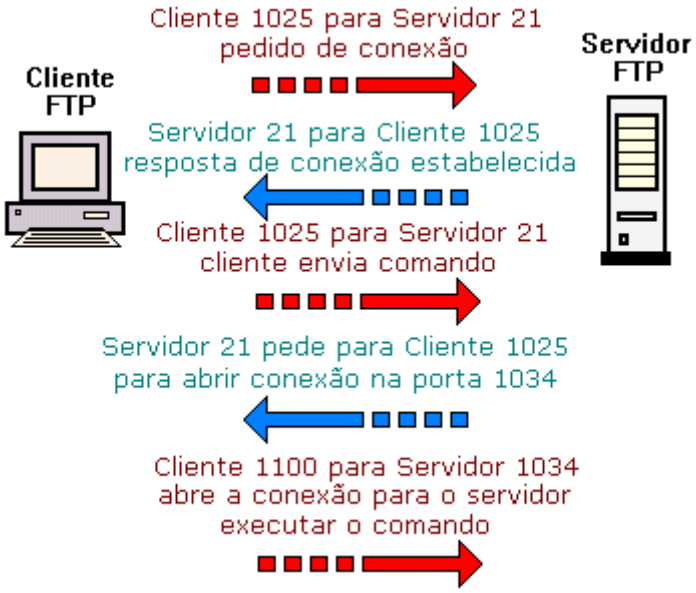


Conexão no modo padrão

Na figura acima, por exemplo, o Cliente 1025 refere-se a porta TCP 1025 e o Servidor 21 refere-se a porta TCP 21 e assim por diante.

19.2 – O FTP no modo passivo

O segundo método para a execução do protocolo é o *FTP* em modo passivo. Esse, consiste em fazer com que o cliente abra a conexão do "*Ftp-dados*" quando for preciso, e tudo é estabelecido na conexão "*Ftp-controle*" onde fica estabelecida inclusive a porta TCP que o cliente vai usar contra o servidor. Além de modificar o sentido da conexão "*Ftp-dados*", as portas nesse modo são altas tanto no cliente como no servidor, ou seja, valores que variam entre 1025 a 65535.



Conexão no modo passivo

Outro aspecto importante que deve ser mencionados aqui é o fato de que as redes, normalmente, se conectam à Internet através de um Gateway, e que esse, dependendo do tipo e concepção, pode fazer com que o FTP seja configurado de forma nada convencional.

Um exemplo é o Proxy da AnalogX, nesse, o programa FTP deve ser configurado para conectar diretamente no servidor Proxy, como se ele fosse realmente o servidor de FTP, entretanto, será passado a ele o endereço do FTP correto, de tal forma que ele fará o resto do trabalho (conexões no FTP correto e repasses para o cliente da rede interna que solicitou a conexão).

***Nota sobre segurança**: Na conexão FTP no modo padrão, a parte "Ftp-dados", traz sérios problemas para a segurança das redes, o motivo é que a conexão no sentido do servidor em uma porta abaixo de 1025 (o default é 20), contra o cliente em uma porta dinâmica, maior que 1024, sem o flag ACK acionado, é considerado pelos administradores de segurança de redes, como acesso indevido e, será simplesmente descartado. Já o modo passivo, é considerado o modo correto de se conectar com FTP.*