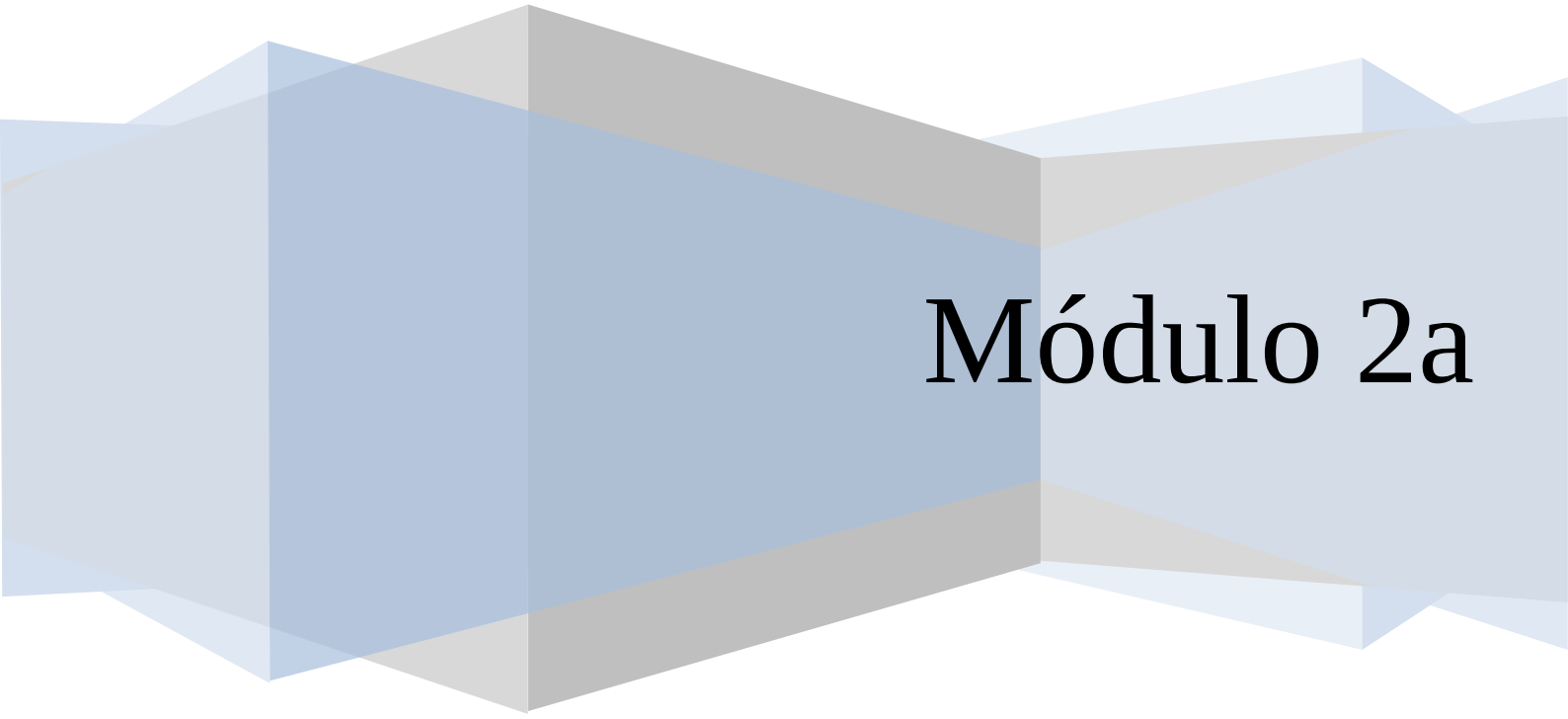
Secretaria de Assistência Social de Piúma - SEMAS
Centro de Referência de Assistência Social - CRAS
Modulo Internet e Redes Locais.
Professor: Sergio Moura

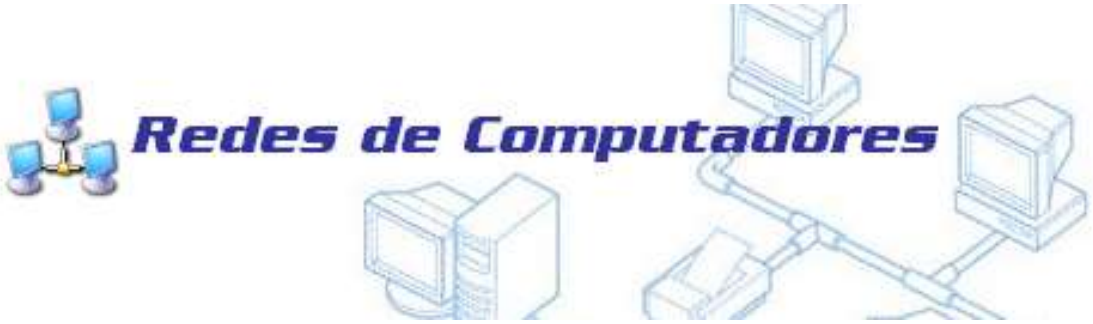
Redes – parte 01 de 02

Redes Locais e Internet

LAN, MAN e WAN



Módulo 2a



Nesta apostila você verá como nasceu a ideia da Rede entre computadores, o seu principal padrão mundialmente utilizado, as topologias, os tipos de cabos, como confeccioná-los, o cabeamento estruturado, os principais equipamentos para uma rede de computadores: Repetidores, Hub, Switch, Roteadores entre outras informações.

Introdução Básica - I

Um pouco de historia

O primeiro experimento conhecido de conexão de computadores em rede foi feito em 1965, nos estados unidos, por obra de dois cientistas: Lawrence Roberts e Thomas Merril. A experiência foi realizada por meio de uma linha telefônica discada de baixa velocidade, fazendo a conexão entre dois centros de pesquisa em Massachusetts e na Califórnia. Estava plantada ali a semente para o que hoje é a Internet – mãe de todas as redes.

O nascimento das redes de computadores, não por acaso, está associado a corrida espacial. Boa parte dos elementos e aplicações essenciais para a comunicação entre computadores, como o protocolo TCP/IP, a tecnologia de comutação de pacotes de dados e o correio eletrônico, estão relacionados ao desenvolvimento da Arpanet, a rede que deu origem a internet. Ela foi criada por um programa desenvolvido pela Advanced Research Projects Agency (ARPA) mais tarde rebatizada como DARPA.

A agencia nasceu de uma iniciativa do departamento de defesa dos estados unidos, na época preocupado em não perder terreno na corrida tecnológica deflagrada pelos russos com o lançamento do satélite Sputinik, em 1957. Roberts, acadêmico do MIT (Instituto de Tecnologia de Massachusetts), era um dos integrantes da DARPA e um dos pais da Arpanet, que começou em 1969 conectando quatro universidades: UCLA – Universidade da Califórnia em Los Angeles, Stanford, Santa Bárbara e Utah. A separação dos militares da Arpanet só ocorreu em 1983, com a criação da Milnet.

Alguns dos marcos importantes para a evolução das redes locais de computadores ocorreram nos anos 70. Até a década anterior os computadores eram maquinas gigantescas que processavam informações por meio da leitura de cartões ou fitas magnéticas. Não havia interação entre o usuário e a máquina. No final dos anos 60 ocorreram os primeiros avanços que resultaram nos sistemas multiusuários de tempo compartilhado. Por meio de terminais interativos, diferentes usuários revezavam-se na utilização do computador central. A IBM reinava praticamente sozinha nessa época.

A partir de 1970, com o desenvolvimento dos minicomputadores de 32 bits, os grandes fabricantes, como IBM, HP e Digital, já começavam a planejar soluções com o objetivo de distribuir o poder de processamento dos mainframes e assim facilitar o acesso às informações. O lançamento do VAX pela Digital, em 1977, estava calcado numa estratégia de criar uma arquitetura de rede de computadores. Com isso, a empresa esperava levar vantagem sobre a rival Big Blue.

Quando um Vax era iniciado, ele já começava a procurar por outras maquinas para se comunicar, um procedimento ousado numa época em que poucas pessoas tinham ideia do que era uma rede. A estratégia deu certo e o VAX alcançou grande popularidade, principalmente em aplicações cientificas e de engenharia. Muitos anos depois, a Digital acabaria sendo comprada pela Compaq, que por sua vez, foi incorporada a HP. Mas as inovações surgidas com o VAX e seu sistema operacional, o VMS, teriam grandes influencias nos computadores que viriam depois.

O sistema operacional Unix, desenvolvido em 1969 nos laboratórios Bell, trouxe inovações que logo o tornou popular nas universidades e nos centros de pesquisa a partir de 1974. Era um sistema portável e modular, capaz de rodar em vários computadores e evoluir junto com o hardware. Os sistemas operacionais da época eram escritos em assembly, linguagem especifica para a plataforma de hardware. O Unix foi escrito quase totalmente em C, uma linguagem de alto nível. Isso deu a ele uma inédita flexibilidade. No começo da década, ferramentas importantes foram criadas para o Unix, como o e-mail, o Telnet, que permitia o uso de terminais remotos, e o FTP, que se transformou no padrão de transferência de arquivos entre computadores em rede. Foi essa plataforma que nasceu a maior parte das tecnologias que hoje formam a Internet.

Ethernet

Um dos principais saltos tecnológicos que permitiram a popularização das redes foi o desenvolvimento da tecnologia ethernet. Para se ter uma idéia do avanço que essa invenção representou, basta lembrar que, até aquela época, os computadores não compartilhavam um cabo comum de conexão. Cada estação era ligada a outra numa distância não superior a 2 metros. O pai da Ethernet é Robert Metcalfe, um dos gênios produzidos pelo MIT e por Harvard e fundador da 3Com.

Metcalfe era um dos pesquisadores do laboratório Parc, que a Xerox mantém até hoje em Palo Alto, na Califórnia. Em 1972, ele recebeu a missão de criar um sistema que permitisse a conexão das estações Xerox Alto entre si e com os servidores. A idéia era que todos os pesquisadores do Parc pudessem compartilhar as recém-desenvolvidas impressoras a laser.

Uma das lendas a respeito da criação da Ethernet é que Metcalfe e sua equipe tomaram por base um sistema desenvolvido por um casal de estudantes da universidade de Aloha, no Havaí. Utilizando um cabo coaxial, eles interligaram computadores em duas ilhas para poder conversar. O fato é que, antes de chamar-se Ethernet, a partir de 1973, o sistema de Metcalfe tinha o nome de Alto Aloha Network. Ele mudou a denominação, primeiramente para deixar claro que a Ethernet poderia funcionar em qualquer computador e não apenas nas estações Xerox. E também para reforçar a diferença em relação ao método de acesso CSMA (Carrier Sense Multiple Access) do sistema Aloha. A palavra ether foi uma referência à propagação de ondas pelo espaço.

O sistema de Metcalfe acrescentou duas letras, CD (de Collision Detection) à sigla CSMA. Um detalhe importante, porque o recurso de detecção de colisão impede que dois dispositivos acessem o mesmo nó de forma simultânea. Assim, o sistema Ethernet verifica se a rede está livre para enviar a mensagem. Se não estiver a mensagem fica numa fila de espera para ser transmitida. A ethernet começou com uma banda de 2Mbps que permitia conectar 100 estações em até 1 quilometro de cabo.

No início, usava-se um cabo coaxial chamado yellow cable, de diâmetro avantajado. A topologia era um desenho de barramento (algo parecido com um varal) no qual o computador ia sendo pendurado. O conector desse sistema foi apelidado de vampiro, porque "mordia" o cabo em pontos determinados. Dali saia um cabo serial que se ligava à placa de rede. O yellow cable podia ser instalado no teto ou no chão, conectado ao cabo menor.

O Mercado da Informação

A Ethernet não foi a única tecnologia de acesso para redes locais criadas nessa época, mas certamente se tornou o padrão mais difundido, por sua simplicidade e eficiência, chegando a mais de 100 milhões de nós no mundo todo. As tecnologias Token Ring, da IBM, e a Arcnet, da Datapoint, chegaram a ter seus dias de gloria (esta última ainda é largamente empregada no Japão para processos de automação industrial), mas perderam terreno para a poderosa concorrente. O primeiro impulso para difusão do padrão Ethernet ocorreu quando a Digital, a Intel e a Xerox, em 1980 formaram um consorcio (DIX) para desenvolver e disseminar o padrão que rapidamente evoluiu de 2Mbps para 10Mbps.

O sistema Ethernet foi padronizado pelas especificações do IEEE (Instituto dos Engenheiros de Eletricidade e Eletrônica), órgão que, entre outras funções, elabora normas técnicas de engenharia eletrônica. O protocolo Ethernet corresponde à especificação 802.3 do IEEE, publicada pela primeira vez em 1985. A conexão Ethernet utilizava, inicialmente, dois tipos de cabos coaxiais, um mais grosso (10 Base5) e outro mais fino (10 Base2). A partir de 1990, com o aumento da velocidade para 100Mbps, passou-se a usar o cabo de par trançado (10Base-T e 100Base-T), que tem a vantagem de ser mais flexível e de baixo custo. Com o advento da fibra ótica, o padrão Ethernet já está em sua terceira geração. A Gigabit Ethernet, com velocidade de até 1Gbps.

Na década de 80, com a chegada dos computadores pessoais, as redes locais começaram a ganhar impulso. O mercado corporativo demandava soluções para compartilhar os elementos mais caros da infraestrutura de TI (impressoras e discos rígidos). A Novell, uma empresa fundada por mórmons em Salt Lake City, no estado americano de Utah, desenvolveu em 1983, o sistema operacional NetWare para servidores, que usava o protocolo de comunicação IPX, mais simples que o TCP/IP. O protocolo rapidamente ganhou força e chegou a dominar 70% do mercado mundial até meados de 1993. A década de 80 foi marcada pela dificuldade de comunicação entres redes locais que e formavam e que eram vistas pelo mercado como ilhas de computadores com soluções proprietárias, como SNA, da IBM, DECnet, da Digital, NetWare, da Novell, e NetBIOS da Microsoft.

A verdade é que eles não inventaram, mas aperfeiçoaram e muito o projeto inical de um engenheiro chamado Bill Yeager. O produto foi lançado comercialmente em 1987. A Cisco hoje vale Bilhões e o resto é História. O quebra-cabeça das redes começa a se fechar a partir do momento que a Arpanet, em 1983, passa a ser de fato a Internet, adotando definitivamente a família de protocolos TCP/IP. No ano seguinte, surge outra grande inovaçã o DNS (Domain Name System), mecanismo para resolver o problema de nome e endereços de servidores na rede. Com a criação da World Wide Web, em 1991, e o desenvolvimento do browser pelo fundador da Netscape, Marc Andreesen, a Internet deslanchou para se tornar a grande rede mundial de computadores.

A difusão do protocolo TCP/IP no mundo corporativo que passou a ser a linguagem universal dos computadores se deu a partir das plataformas Unix da Sun e da HP. Nos anos 90, as empresas já estavam empenhadas em usar a informática para melhorar o processo produtivo. O mercado começou a migrar de plataformas proprietárias para sistemas abertos. A questão não era tecnologia, mas economia. O sistema Unix tinha vários fornecedores, uma plataforma de desenvolvimento mais simples e mais versátil que os tradicionais mainframes. A pluralidade de plataformas passou a ser a regra nas empresas. Isso só foi possível porque os obstáculos à interligação de sistemas de diferentes fabricantes já haviam sido superados.

A Evolução

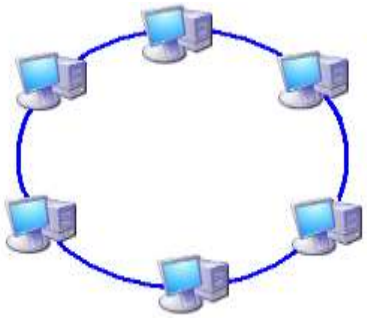
Em 1988, Dave Cutler, líder da equipe da Digital que havia criado o VMS, o arrojado sistema operacional do VAX, foi contratado pela Microsoft. A empresa já havia fracassado em uma tentativa anterior de competir com a Novell. Seu primeiro sistema operacional de rede, o LAN Manager, desenvolvido em conjunto com a IBM, não era páreo para o NetWare. Culter levou para lá boa parte da sua antiga equipe de programadores e também a filosofia que havia norteado a criação do VAX, de que a comunicação em rede deve ser um atributo básico do sistema operacional. Ele liderou o desenvolvimento do Windows NT, lançado em 1993. Com ele, a Microsoft finalmente conseguiu conquistar algum espaço nos servidores. O NT também foi base para o desenvolvimento do Windows 2000 e do Windows XP. De certa forma o XP é neto do velho VMS.

Se, há 40 anos, a ideia de uma rede de computadores era a de vários aparelhos conectados, hoje a rede transformou-se numa dos principais meios de interação entre pessoas, de disseminação da informação e da realização de negócios. O rádio levou 38 anos até formar um público de 50 milhões de pessoas. A TV levou 13 anos. A Internet precisou apenas quatro anos para alcançar essa marca. É um salto e tanto para toda a humanidade.

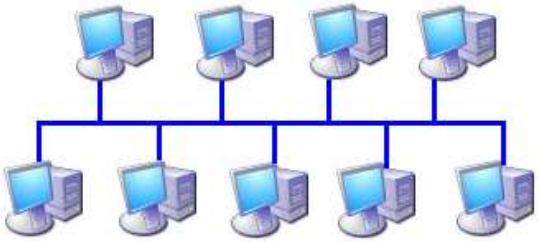
Topologias das Redes de Computadores

Ao longo da história das redes, várias topologias foram experimentadas, com maior ou menor sucesso. Os três tipos abaixo são esquemas básicos empregados na conexão dos computadores. Os outros são variantes deles:

Estrela - Todas as conexões partem de um ponto central (concentrador), normalmente um hub ou switch. É o modelo mais utilizado atualmente.



Anel - Todos os computadores são conectados em um anel. É a topologia das redes Token Ring, popularizadas pela IBM nos anos 80. Hoje, esse modelo é mais utilizado em sistemas de automação industrial.



Barramento - Os computadores são conectados num sistema linear de cabeamento em sequência. Esse arranjo era usado nas primeiras gerações de redes Ethernet. Está sendo lentamente abandonado.

Cabos

O projeto de cabeamento de uma rede, que faz parte do meio físico usado para interligar computadores, é um fator de extrema importância para o bom desempenho de uma rede. Esse projeto envolve aspectos sobre a taxa de transmissão, largura de banda, facilidade de instalação, imunidade a ruídos, confiabilidade, custos de interface, exigências geográficas, conformidade com padrões internacionais e disponibilidades de componentes.

O sistema de cabeamento determina a estabilidade de uma rede. Pesquisas revelam que cerca de 80% dos problemas físicos ocorridos atualmente em uma rede tem origem no cabeamento, afetando de forma considerável a confiabilidade da mesma. O custo para a implantação do cabeamento corresponde a aproximadamente 6% do custo total de uma rede, mais 70% da manutenção de uma rede é direcionada aos problemas oriundos do cabeamento.

Cabo Par trançado e Coaxial.

Em matéria de cabos, os mais utilizados são os cabos de par trançado, os cabos coaxiais e cabos de fibra óptica. Cada categoria tem suas próprias vantagens e limitações, sendo mais adequado para um tipo específico de rede.

- **Os cabos de par trançado** são os mais usados pois tem um melhor custo benefício, ele pode ser comprado pronto em lojas de informática, ou feito sob medida, ou ainda produzido pelo próprio usuário, e ainda são 10 vezes mais rápidos que os cabos coaxiais.

- **Os cabos coaxiais** permitem que os dados sejam transmitidos através de uma distância maior que a permitida pelos cabos de par trançado sem blindagem (UTP), mas por outro, lado não são tão flexíveis e são mais caros que eles. Outra desvantagem é que a maioria delas requerem o barramento ISA, não encontradas nas Placas mães novas.

- **Os cabos de fibra óptica** permitem transmissões de dados a velocidades muito maiores e são completamente imunes a qualquer tipo de interferência eletromagnética, porém, são muito mais caros e difíceis de instalar, demandando equipamentos mais caros e mão de obra mais especializada. Apesar da alta velocidade de transferência, as fibras ainda não são uma boa opção para pequenas redes devido ao custo.

Cabos de Fibra Óptica

Sem as fibras ópticas, a Internet e até o sistema telefônico que temos hoje seriam inviáveis. Com a migração das tecnologias de rede para padrões de maiores velocidades como ATM, Gigabit Ethernet e 10 Gigabit Ethernet, o uso de fibras ópticas vem ganhando força também nas redes locais.

O produto começou a ser fabricado em 1978 e passou a substituir os cabos coaxiais nos Estados Unidos na segunda metade dos anos 80. Em 1988, o primeiro cabo submarino de fibras ópticas mergulhou no oceano, dando início a superestrada da informação.

O físico indiano Narinder Singh Kanpany é o inventor da fibra óptica, que passou a ter aplicações práticas na década de 60 com o advento da criação de fontes de luz de estado sólido, como o raio laser e o LED, diodo emissor de luz. Sua origem, porém, data do século 19, com os primeiros estudos sobre os efeitos da luz.

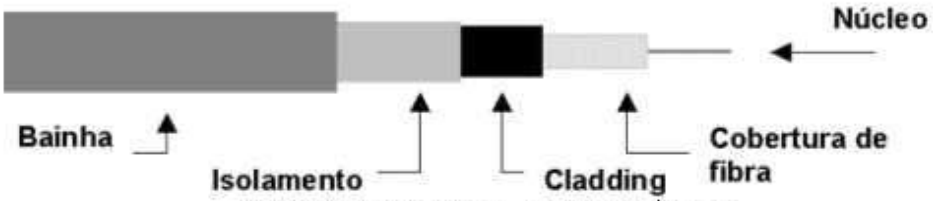
Existem dois tipos de fibras ópticas: As fibras multímodo e as monomodo. A escolha de um desses tipos dependera da aplicação da fibra. As fibras multímodo são mais utilizadas em aplicações de rede locais (LAN), enquanto as monomodo são mais utilizadas para aplicações de rede de longa distância (WAN). São mais caras, mas também mais eficientes que as multímodo.

Aqui no Brasil, a utilização mais ampla da fibra óptica teve início na segunda metade dos anos 90, impulsionada pela implementação dos backbones das operadoras de redes metropolitanas.

Em 1966, num comunicado dirigido à Bristish Association for the Advancement of Science, os pesquisadores K.C.Kao e G.A.Hockham da Inglaterra propuseram o uso de fibras de vidro, e luz, em lugar de eletricidade e condutores de cobre na transmissão de mensagens telefônicas.

Ao contrário dos cabos coaxiais e de par trançado, que nada mais são do que fios de cobre que transportam sinais elétricos, a fibra óptica transmite luz e por isso é totalmente imune a qualquer tipo de interferência eletromagnética. Além disso, como os cabos são feitos de plástico e fibra de vidro (ao invés de metal), são resistentes à corrosão.

O cabo de fibra óptica é formado por um núcleo extremamente fino de vidro, ou mesmo de um tipo especial de plástico. Uma nova cobertura de fibra de vidro, bem mais grossa envolve e protege o núcleo. Em seguida temos uma camada de plástico protetora chamada de cladding, uma nova camada de isolamento e finalmente uma capa externa chamada bainha.



Estrutura do Cabo de Fibra Óptica

A transmissão de dados por fibra óptica é realizada pelo envio de um sinal de luz codificado, dentro do domínio de frequência do infravermelho a uma velocidade de 10 a 15 MHz. As fontes de transmissão de luz podem ser diodos emissores de luz (LED) ou lasers semicondutores. O cabo óptico com transmissão de raio laser é o mais eficiente em potência devido a sua espessura reduzida. Já os cabos com diodos emissores de luz são muito baratos, além de serem mais adaptáveis à temperatura ambiente e de terem um ciclo de vida maior que o do laser.

O cabo de fibra óptica pode ser utilizado tanto em ligações ponto a ponto quanto em ligações multímodo. A fibra óptica permite a transmissão de muitos canais de informação de forma simultânea pelo mesmo cabo. Utiliza, por isso, a técnica conhecida como multiplexação onde cada sinal é transmitido numa frequência ou num intervalo de tempo diferente.

Placa de Rede com Conectores para Fibra Ótica.

A fibra óptica tem inúmeras vantagens sobre os condutores de cobre, sendo as principais:

- Maior alcance
- Maior velocidade
- Imunidade a interferências eletromagnéticas

O custo do metro de cabo de fibra óptica não é elevado em comparação com os cabos convencionais. Entretanto seus conectores são bastante caros, assim como a mão de obra necessária para a sua montagem. A montagem desses conectores, além de um curso de especialização, requer instrumentos especiais, como microscópios, ferramentas especiais para corte e polimento, medidores e outros aparelhos sofisticados.

Figura de Cabo de Fibra Óptica.

Devido ao seu elevado custo, os cabos de fibras ópticas são usados apenas quando é necessário atingir grandes distâncias em redes que permitem segmentos de até 1 KM, enquanto alguns tipos de cabos especiais podem conservar o sinal por até 5 KM (distâncias maiores são obtidas usando repetidores).

Mesmo permitindo distâncias tão grandes, os cabos de fibra óptica permitem taxas de transferências de até 155 mbps, sendo especialmente úteis em ambientes que demandam uma grande transferência de dados. Como não soltam faíscas, os cabos de fibra óptica são mais seguros em ambientes onde existe perigo de incêndio ou explosões. E para completar, o sinal transmitido através dos cabos de fibra é mais difícil de interceptar, sendo os cabos mais seguros para transmissões sigilosas. A seguir veremos os padrões mais comuns de redes usando fibra ótica:

- FDDI (Fiber Distributed Data Interface)
- FOIRL (Fiber- Optic InterRepeater Link)
- 10BaseFL
- 100BaseFX
- 1000BaseSX
- 1000BaseLX

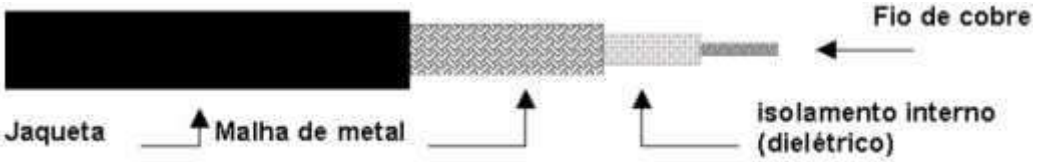
Cabo Coaxial

O cabo coaxial foi o primeiro cabo disponível no mercado, e era até a alguns anos atrás o meio de transmissão mais moderno que existia em termos de transporte de dados, existem 4 tipos diferentes de cabos coaxiais, chamados de 10Base5, 10Base2, RG-59/U e RG-62/U.

O cabo 10Base5 é o mais antigo, usado geralmente em redes baseadas em mainframes. Este cabo é muito grosso, tem cerca de 0.4 polegadas, ou quase 1 cm de diâmetro e por isso é muito caro e difícil de instalar devido à baixa flexibilidade. Outro tipo de cabo coaxial é o RG62/U, usado em redes Arcnet. Temos também o cabo RG-59/U, usado na fiação de antenas de TV.

Os cabos 10Base2, também chamados de cabos coaxiais finos, ou cabos Thinnet, são os cabos coaxiais usados atualmente em redes Ethernet, e por isso, são os cabos que você receberá quando pedir por "cabos coaxiais de rede". Seu diâmetro é de apenas 0.18 polegadas, cerca de 4.7 milímetros, o que os torna razoavelmente flexíveis.

Os cabos coaxiais são cabos constituídos de 4 camadas: um condutor interno, o fio de cobre que transmite os dados; uma camada isolante de plástico, chamada de dielétrico que envolve o cabo interno; uma malha de metal que protege as duas camadas internas e, finalmente, uma nova camada de revestimento, chamada de jaqueta.



Estrutura do Cabo Coaxial

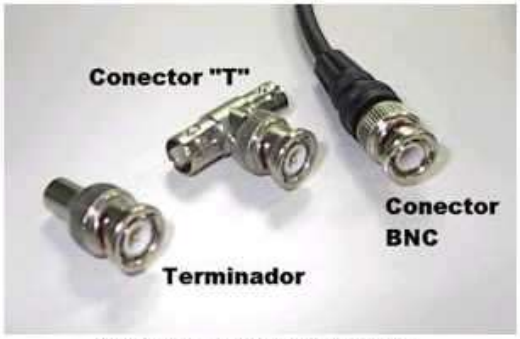
O cabo Thin Ethernet deve formar uma linha que vai do primeiro ao último PC da rede, sem formar desvios. Não é possível portanto formar configurações nas quais o cabo forma um "Y", ou que usem qualquer tipo de derivação. Apenas o primeiro e o último micro do cabo devem utilizar o terminador BNC.


Placa de rede para rede com Cabo Coaxial

O Cabo 10base2 tem a vantagem de dispensar hubs, pois a ligação entre os micros é feita através do conector "T", mesmo assim o cabo coaxial caiu em desuso devido às suas desvantagens:

- Custo elevado,
- Instalação mais difícil e mais fragilidade,
- Se o terminador for retirado do cabo, toda a rede sai do ar.

Redes formadas por cabos Thin Ethernet são de implementação um pouco complicada. É preciso adquirir ou construir cabos com medidas de acordo com a localização física dos PCs. Se um dos PCs for reinstalado em outro local é preciso utilizar novos cabos, de acordo com as novas distâncias entre os PCs. Pode ser preciso alterar duas ou mais seções de cabo de acordo com a nova localização dos computadores. Além disso, os cabos coaxiais são mais caros que os do tipo par trançado.



Conectores e Terminador

O "10" na sigla 10Base2, significa que os cabos podem transmitir dados a uma velocidade de até 10 megabits por segundo, "Base" significa "banda base" e se refere à distância máxima para que o sinal pode percorrer através do cabo, no caso o "2" que teoricamente significaria 200 metros, mas que na prática é apenas um arredondamento, pois nos cabos 10Base2 a distância máxima utilizável é de 185 metros.


Cabo de rede coaxial

Usando cabos 10Base2, o comprimento do cabo que liga um micro ao outro deve ser de no mínimo 50 centímetros, e o comprimento total do cabo (do primeiro ao último micro) não pode superar os 185 metros. É permitido ligar até 30 micros no mesmo cabo, pois acima disso, o grande número de colisões de pacotes irá prejudicar o desempenho da rede, chegando a ponto de praticamente impedir a comunicação entre os micros em casos extremos.

Cabo Par Trançado

O cabo par trançado surgiu com a necessidade de se ter cabos mais flexíveis e com maior velocidade de transmissão, ele vem substituindo os cabos coaxiais desde o início da década de 90. Hoje em dia é muito raro alguém ainda utilizar cabos coaxiais em novas instalações de rede, apesar do custo adicional decorrente da utilização de hubs e outros concentradores. O custo do cabo é mais baixo, e a instalação é mais simples.

O nome "par trançado" é muito conveniente, pois estes cabos são constituídos justamente por 4 pares de cabos entrelaçados. Os cabos coaxiais usam uma malha de metal que protege o cabo de dados contra interferências externas; os cabos de par trançado por sua vez, usam um tipo de proteção mais sutil: o entrelaçamento dos cabos cria um campo eletromagnético que oferece uma razoável proteção contra interferências externas.


Veja como os pares são entrelaçados

Existem basicamente dois tipos de cabo par trançad Os Cabos sem blindagem chamados de UTP (Unshielded Twisted Pair) e os blindados conhecidos como STP (Shielded Twisted Pair). A única diferença entre eles é que os cabos blindados além de contarem com a proteção do entrelaçamento dos fios, possuem uma blindagem externa (assim como os cabos coaxiais), sendo mais adequados a ambientes com fortes fontes de interferências, como grandes motores elétricos e estações de rádio que estejam muito próximas. Outras fontes menores de interferências são as lâmpadas fluorescentes (principalmente lâmpadas cansadas que ficam piscando), cabos elétricos quando colocados lado a lado com os cabos de rede e mesmo telefones celulares muito próximos dos cabos.

Cabo de par trançado

Na realidade o par trançado sem blindagem possui uma ótima proteção contra ruídos, só que usando uma técnica de *cancelamento* e não através de uma blindagem. Através dessa técnica, as informações circulam repetidas em dois fios, sendo que no segundo fio a informação possui a polaridade invertida. Todo fio produz um campo eletromagnético ao seu redor quando um dado é transmitido. Se esse campo for forte o suficiente, ele irá corromper os dados que estejam circulando no fio ao lado (isto é, gera Ruído). Em inglês esse problema é conhecido como cross-talk.

A direção desse campo eletromagnético depende do sentido da corrente que está circulando no fio, isto é, se é positiva ou então negativa. No esquema usado pelo par trançado, como cada par transmite a mesma informação só que com a polaridade invertida, cada fio gera um campo eletromagnético de mesma intensidade mas em sentido contrário. Com isso, o campo eletromagnético gerado por um dos fios é anulado pelo campo eletromagnético gerado pelo outro fio.

Placa de rede para cabo par trançado

Além disso, como a informação é transmitida duplicada, o receptor pode facilmente verificar se ela chegou ou não corrompida. Tudo o que circula em um dos fios deve existir no outro fio com intensidade igual, só que com a polaridade invertida. Com isso, aquilo que for diferente nos dois sinais é ruído e o receptor tem como facilmente identificá-lo e eliminá-lo.

Quanto maior for o nível de interferência, menor será o desempenho da rede, menor será a distância que poderá ser usada entre os micros e mais vantajosa será a instalação de cabos blindados. Em ambientes normais, porém os cabos sem blindagem costumam funcionar bem.

Existem no total, 5 categorias de cabos de par trançado. Em todas as categorias a distância máxima permitida é de 100 metros. O que muda é a taxa máxima de transferência de dados e o nível de imunidade a interferências. Os cabos de categoria 5 que tem a grande vantagem sobre os outros 4 que é a taxa de transferência que pode chegar até 100 mbps, e são praticamente os únicos que ainda podem ser encontrados à venda, mas em caso de dúvida basta checas as inscrições no cabo, entre elas está a categoria do cabo, como na foto abaixo

Cabo com categoria 5e

A utilização do cabo de par trançado tem suas vantagens e desvantagens, vejamos as principais:

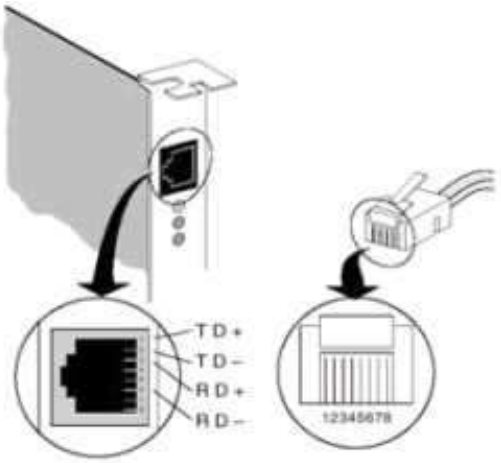
Vantagens

- **Preço**. Mesma com a obrigação da utilização de outros equipamentos na rede, a relação custo beneficia se torna positiva.
- **Flexibilidade**. Como ele é bastante flexível, ele pode ser facilmente passado por dentro de conduítes embutidos em paredes.
- **Facilidade**. A facilidade com que se pode adquirir os cabos, pois em qualquer loja de informática existe esse cabo para venda, ou até mesmo para o próprio usuário confeccionar os cabos.
- **Velocidade**. Atualmente esse cabo trabalha com uma taxa de transferência de 100 Mbps.

Desvantagens

- **Comprimento.** Sua principal desvantagem é o limite de comprimento do cabo que é de aproximadamente 100 por trecho.
- **Interferência.** A sua baixa imunidade à interferência eletromagnética, sendo fator preocupante em ambientes industriais.

No cabo de par trançado tradicional existem quatro pares de fio. Dois deles não são utilizados pois os outros dois pares, um é utilizado para a transmissão de dados (TD) e outro para a recepção de dados (RD). Entre os fios de números 1 e 2 (chamados de TD+ e TD–) a placa envia o sinal de transmissão de dados, e entre os fios de números 3 e 6 (chamados de RD+ e RD–) a placa recebe os dados. Nos hubs e switches, os papéis desses pinos são invertidos. A transmissão é feita pelos pinos 3 e 6, e a recepção é feita pelos pinos 1 e 2. Em outras palavras, o transmissor da placa de rede é ligado no receptor do hub ou switch, e vice-versa.



Pares de Fios de TD e RD

(obs.) Um cuidado importante a ser tomado é que sistemas de telefonia utilizam cabos do tipo par trançado, só que este tipo de cabo não serve para redes locais.

Como confeccionar os Cabos

A montagem do cabo par trançado é relativamente simples. Além do cabo, você precisará de um conector RJ-45 de pressão para cada extremidade do cabo e de um alicate de pressão para conectores RJ-45 também chamado de Alicate crimpador. Tome cuidado, pois existe um modelo que é usado para conectores RJ-11, que têm 4 contatos e são usados para conexões telefônicas

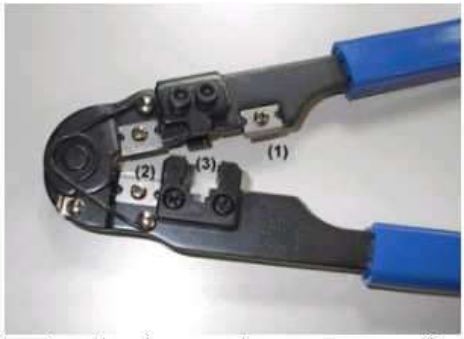
Alicate Crimpador

Assim como ocorre com o cabo coaxial, fica muito difícil passar o cabo por conduítes e por estruturas usadas para ocultar o cabo depois que os plugues RJ-45 estão instalados. Por isso, passe o cabo primeiro antes de instalar os plugues. Corte o cabo no comprimento desejado.

Lembre-se de deixar uma folga de alguns centímetros, já que o micro poderá posteriormente precisar mudar de lugar além disso você poderá errar na hora de instalar o plugue RJ-45, fazendo com que você precise cortar alguns poucos centímetros do cabo para instalar novamente outro plugue.

Para quem vai utilizar apenas alguns poucos cabos, vale a pena comprá-los prontos. Para quem vai precisar de muitos cabos, ou para quem vai trabalhar com instalação e manutenção de redes, vale a pena ter os recursos necessários para construir cabos. Devem ser comprados os conectores RJ-45, algumas um rolo de cabo, um alicate para fixação do conector e um testador de cabos. Não vale a pena economizar comprando conectores e cabos baratos, comprometendo a confiabilidade.

O alicate possui duas lâminas e uma fenda para o conector. A lâmina indicada com (1) é usada para cortar o fio. A lâmina (2) serve para desencapar a extremidade do cabo, deixando os quatro pares expostos. A fenda central serve para prender o cabo no conector.



Indicações das áreas cada uma com sua função.

- (1): Lâmina para corte do fio
- (2): Lâmina para desencapar o fio
- (3): Fenda para crimpar o conector

Corte a ponta do cabo com a parte (2) do alicate do tamanho que você vai precisar, desencape (A lâmina deve cortar superficialmente a capa plástica, porém sem atingir os fios) utilizando a parte (1) do alicate aproximadamente 2 cm do cabo. Pois o que protege os cabos contra as interferências externas são justamente as tranças. À parte destrançada que entra no conector é o ponto fraco do cabo, onde ele é mais vulnerável a todo tipo de interferência.

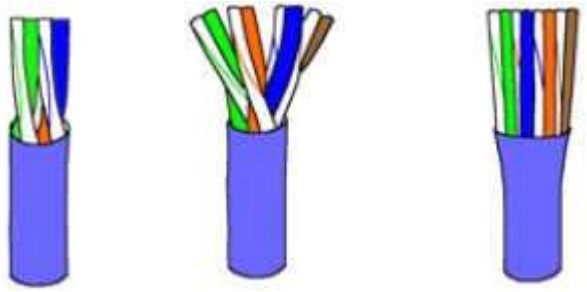
Remova somente a proteção externa do cabo, ***não desencape os fios individuais.***

Cabo desencapado

Identifique os fios do cabo com as seguintes cores:

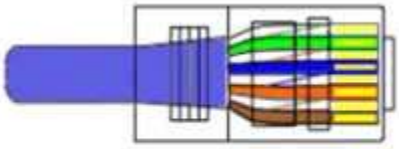
- Branco com Verde
- Verde
- Branco com Laranja
- Laranja
- Branco com Azul
- Azul
- Branco com Marrom
- Marrom

Desenrole os fios que ficaram para fora do cabo, ou seja, deixe-os "retos" e não trançados na ordem acima citada, como mostra a figura abaixo



Fios na posição certa para se colocar o conector RJ-45

Corte os fios com a parte (1) do alicate em aproximadamente 1,5cm do invólucro do cabo.Observe que no conector RJ-45 que para cada pino existe um pequeno "tubo" onde o fio deve ser inserido. Insira cada fio em seu "tubo", até que atinja o final do conector. Lembrando que não é necessário desencapar o fio, pois isto ao invés de ajudar, serviria apenas para causar mau contato, deixado o encaixe com os pinos do conector "folgado".



Fios encaixados no conector

Ao terminar de inserir os fios no conector RJ-45, basta inserir o conector na parte (3) do alicate e pressioná-lo. A função do alicate neste momento é fornecer pressão suficiente para que os pinos do conector RJ-45, que internamente possuem a forma de lâminas, esmaguem os fios do cabo, alcançando o fio de cobre e criando o contato, ao mesmo tempo, uma parte do conector irá prender com força a parte do cabo que está com a capa plástica externa. O cabo ficará definitivamente fixo no conector.

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

Uma dica que ajuda bastante e a utilização das borrachas protetoras dos conectores RJ-45 pois o uso desses traz vários benefícios com facilita a identificação do cabo com o uso de cores diferentes, mantém o conector mais limpo, aumenta a durabilidade do conector nas operações de encaixe e desencaixe, dá ao cabo um acabamento profissional.

Protetores Para os Conectores RJ-45 e um cabo com os protetores

Montar um cabo de rede com esses protetores é fácil. Cada protetor deve ser instalado no cabo antes do respectivo conector RJ-45. Depois que o conector é instalado, ajuste o protetor ao conector.

Testar o Cabo

Para testar o cabo é muito fácil utilizando os testadores de cabos disponíveis no mercado. Normalmente esses testadores são compostos de duas unidades independentes. A vantagem disso é que o cabo pode ser testado no próprio local onde fica instalado, muitas vezes com as extremidades localizadas em recintos diferentes. Chamaremos os dois componentes do testador: um de testador e o outro de terminador. Uma das extremidades do cabo deve ser ligada ao testador, no qual pressionamos o botão ON/OFF. O terminador deve ser levado até o local onde está a outra extremidade do cabo, e nele encaixamos o outro conector RJ-45.

Testador de Cabos de par trançado

Uma vez estando pressionado o botão ON/OFF no testador, um LED irá piscar. No terminador, quatro LEDs piscarão em sequência, indicando que cada um dos quatro pares está corretamente ligado. Observe que este testador não é capaz de distinguir ligações erradas quando são feitas de forma idêntica nas duas extremidades. Por exemplo, se os fios azul e verde forem ligados em posições invertidas em ambas as extremidades do cabo, o terminador apresentará os LEDs piscando na sequência normal. Cabe ao usuário ou técnico que monta o cabo, conferir se os fios em cada conector estão ligados nas posições corretas.

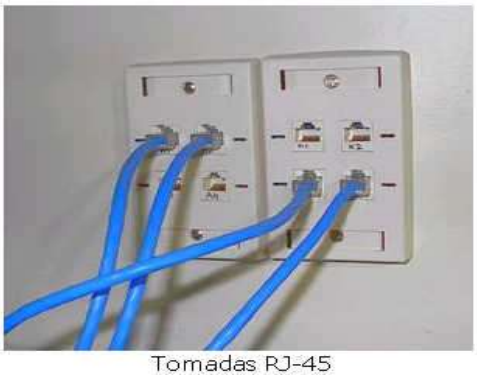
Para quem faz instalações de redes com frequências, é conveniente adquirir testadores de cabos, lojas especializadas em equipamentos para redes fornecem cabos, conectores, o alicate e os testadores de cabos, além de vários outros equipamentos. Mais se você quer apenas fazer um cabo para sua rede, existe um teste simples para saber se o cabo foi crimpado corretamente: basta conectar o cabo à placa de rede do micro e ao hub. Tanto o LED da placa quanto o do hub deverão acender. Naturalmente, tanto o micro quanto o hub deverão estar ligados.

Cabeamento Estruturado

As redes mais populares utilizam a arquitetura Ethernet usando cabo par trançado sem blindagem (UTP). Nessa arquitetura, há a necessidade de um dispositivo concentrador, tipicamente um hub, para fazer a conexão entre os computadores.

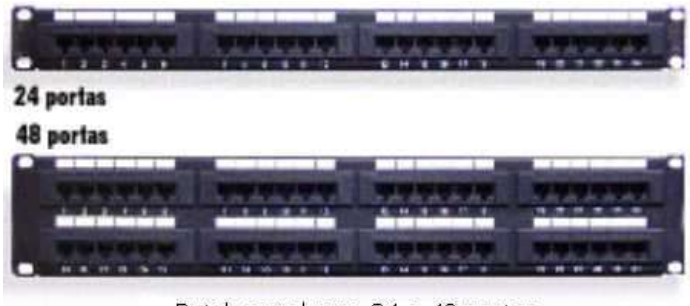
Em redes pequenas, o cabeamento não é um ponto que atrapalhe o dia-a-dia da empresa, já que apenas um ou dois hubs são necessários para interligar todos os micros. Entretanto, em redes médias e grandes a quantidade de cabos e o gerenciamento dessas conexões pode atrapalhar o dia-a-dia da empresa. A simples conexão de um novo micro na rede pode significar horas e horas de trabalho (passando cabos e tentando achar uma porta livre em um hub).

É aí que entra o Cabeamento Estruturado. A ideia básica do cabeamento estruturado fornece ao ambiente de trabalho um sistema de cabeamento que facilite a instalação e remoção de equipamentos, sem muita perda de tempo. Dessa forma, o sistema mais simples de cabeamento estruturado é aquele que provê tomadas RJ-45 para os micros da rede em vez de conectarem o hub diretamente aos micros. Podendo haver vários pontos de rede já preparados para receber novas maquinas. Assim, ao trocar um micro de lugar ou na instalação de um novo micro, não haverá a necessidade de se fazer o cabeamento do micro até o hub; este cabeamento já estará feito, agilizando o dia-a-dia da empresa.



Tomadas RJ-45

A ideia do cabeamento estruturado vai muito além disso. Além do uso de tomadas, o sistema de cabeamento estruturado utiliza um concentrador de cabos chamado Patch Panel (Painel de Conexões). Em vez de os cabos que vêm das tomadas conectarem-se diretamente ao hub, eles são conectados ao patch panel. Dessa forma, o patch panel funciona como um grande concentrador de tomadas



Patch panel com 24 e 48 portas

O patch panel é um sistema passivo, ele não possui nenhum circuito eletrônico. Trata-se somente de um painel contendo conectores. Esse painel é construído com um tamanho padrão, de forma que ele possa ser instalado em um rack.

Figuras dos Racks

O uso do patch panel facilita enormemente a manutenção de redes medis e grandes. Por exemplo, se for necessário trocar dispositivos, adicionar novos dispositivos (hubs e switches, por exemplo) alterar a configuração de cabos, etc., basta trocar a conexão dos dispositivos no patch panel, sem a necessidade de alterar os cabos que vão até os micros. Em redes grandes é comum haver mais de um local contendo patch panel.
Assim, as portas dos patch panels não conectam somente os micros da rede, mas também fazem a ligação entre patch panels.
Para uma melhor organização das portas no patch panel, este possui uma pequena área para poder rotular cada porta, isto é, colocar uma etiqueta informando onde a porta está fisicamente instalada.

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

Repetidores

O repetidor é um dispositivo responsável por ampliar o tamanho máximo do cabeamento da rede. Ele funciona como um amplificador de sinais, regenerando os sinais recebidos e transmitindo esses sinais para outro segmento da rede.
Como o nome sugere, ele repete as informações recebidas em sua porta de entrada na sua porta de saída. Isso significa que os dados que ele mandar para um micro em um segmento, estes dados estarão disponíveis em todos os segmentos, pois o repetidor é um elemento que não analisa os quadros de dados para verificar para qual segmento o quadro é destinado. Assim ele realmente funciona como um "extensor" do cabeamento da rede. É como se todos os segmentos de rede estivessem fisicamente instalados no mesmo segmento.

Apesar de aumentar o comprimento da rede, o repetidor traz como desvantagem diminuir o desempenho da rede. Isso ocorre porque, como existirão mais maquinas na rede, as chances de o cabeamento estar livre para o envio de um dado serão menores. E quando o cabeamento está livre, as chances de uma colisão serão maiores, já que teremos mais maquinas na rede.

Atualmente você provavelmente não encontrara repetidores como equipamento independentes, esse equipamento está embutido dentro de outros, especialmente do hub. O hub é, na verdade, um repetidor (mas nem todo repetidor é um hub), já que ele repete os dados que chegam em uma de suas portas para todas as demais portas existentes.

Hubs

Os Hubs são dispositivos concentradores, responsáveis por centralizar a distribuição dos quadros de dados em redes fisicamente ligadas em estrelas. Funcionando assim como uma peça central, que recebe os sinais transmitidos pelas estações e os retransmite para todas as demais.

Figura do Hub

Existem vários tipos de hubs, vejamos:

- **Passivos**: O termo "Hub" é um termo muito genérico usado para definir qualquer tipo de dispositivo concentrador. Concentradores de cabos que não possuem qualquer tipo de alimentação elétrica são chamados hubs passivos funcionando como um espelho, refletindo os sinais recebidos para todas as estações a ele conectadas. Como ele apenas distribui o sinal, sem fazer qualquer tipo de amplificação, o comprimento total dos dois trechos de cabo entre um micro e outro, passando pelo hub, não pode exceder os 100 metros permitidos pelos cabos de par trançado.

- **Ativos**: São hubs que regeneram os sinais que recebem de suas portas antes de enviá-los para todas as portas. Funcionando como repetidores. Na maioria das vezes, quando falamos somente "hub" estamos nos referindo a esse tipo de hub. Enquanto usando um Hub passivo o sinal pode trafegar apenas 100 metros somados os dois trechos de cabos entre as estações, usando um hub ativo o sinal pode trafegar por 100 metros até o hub, e após ser retransmitido por ele trafegar mais 100 metros completos.

- **Inteligentes**: São hubs que permitem qualquer tipo de monitoramento. Este tipo de monitoramento, que é feito via software capaz de detectar e se preciso desconectar da rede estações com problemas que prejudiquem o tráfego ou mesmo derrube a rede inteira; detectar pontos de congestionamento na rede, fazendo o possível para normalizar o tráfego; detectar e impedir tentativas de invasão ou acesso não autorizado à rede entre outras funções, que variam de acordo com a fabricante e o modelo do Hub.

- **Empilháveis**: Também chamado xxxxxxável (stackable). Esse tipo de hub permite a ampliação do seu número de portas. Veremos esse tipo de hub mais detalhadamente adiante.

Cascateamento

Existe a possibilidade de conectar dois ou mais hubs entre si. Quase todos os hubs possuem uma porta chamada "Up Link" que se destina justamente a esta conexão. Basta ligar as portas Up Link de ambos os hubs, usando um cabo de rede normal para que os hubs passem a se enxergar.

Sendo que existem alguns hubs mais baratos não possuem a porta "Up Link", mais com um cabo cross-over pode-se conectar dois hubs. A única diferença neste caso é que ao invés de usar as portas Up Link, usará duas portas comuns.

Note que caso você esteja interligando hubs passivos, a distância total entre dois micros da rede, incluindo o trecho entre os hubs, não poderá ser maior que 100 metros, o que é bem pouco no caso de uma rede grande. Neste caso, seria mais recomendável usar hubs ativos, que amplificam o sinal.

Empilhamento

O recurso de conectar hubs usando a porta Up Link, ou usando cabos cross-over, é utilizável apenas em redes pequenas, pois qualquer sinal transmitido por um micro da rede será retransmitido para todos os outros. Quanto mais Computadores tivermos na rede, maior será o tráfego e mais lenta a rede será e apesar de existirem limites para conexão entre hubs e repetidores, não há qualquer limite para o número de portas que um hub pode ter. Assim, para resolver esses problemas os fabricantes desenvolveram o hub empilhável.

Esse hub possui uma porta especial em sua parte traseira, que permite a conexão entre dois ou mais hubs. Essa conexão especial faz com que os hubs sejam considerados pela rede um só hub e não hubs separados, eliminando estes problemas. O empilhamento só funciona com hubs da mesma marca.

A interligação através de porta especifica com o cabo de empilhamento (stack) tem velocidade de transmissão maior que a velocidade das portas.

Hubs empilháveis

Bridges (Pontes)

Como vimos anteriormente que os repetidores transmitem todos os dados que recebe para todas as suas saídas. Assim, quando uma máquina transmite dados para outra máquina presente no mesmo segmento, todas as maquinas da rede recebem esses dados, mesmo aquelas que estão em outro segmento.

A ponte é um repetidor Inteligente. Ela tem a capacidade de ler e analisar os quadros de dados que estão circulando na rede. Com isso ela consegue ler os campos de endereçamentos MAC do quadro de dados. Fazendo com que a ponte não replique para outros segmentos dados que tenham como destino o mesmo segmento de origem. Outro papel que a ponte em principio poderia ter é o de interligar redes que possuem arquiteturas diferentes.

Switches

O switch é um hub que, em vez de ser um repetidor é uma ponte. Com isso, em vez dele replicar os dados recebidos para todas as suas portas, ele envia os dados somente para o micro que requisitou os dados através da análise da Camada de link de dados onde possui o endereço MAC da placa de rede do micro, dando a ideia assim de que o switch é um hub Inteligente, além do fato dos switches trazerem micros processadores internos, que garantem ao aparelho um poder de processamento capaz de traçar os melhores caminhos para o trafego dos dados, evitando a colisão dos pacotes e ainda conseguindo tornar a rede mais confiável e estável.

Figura do Switch

De maneira geral a função do switch é muito parecida com a de um bridge, com a exceção que um switch tem mais portas e um melhor desempenho, já que manterá o cabeamento da rede livre. Outra vantagem é que mais de uma comunicação pode ser estabelecida simultaneamente, desde que as comunicações não envolvam portas de origem ou destino que já estejam sendo usadas em outras comunicações.

Existem duas arquiteturas básicas de Switches de rede: "cut-through" e "store-and-forward":

- **Cut-through**: apenas examina o endereço de destino antes de reencaminhar o pacote.
- **Store-and-forward**: aceita e analisa o pacote inteiro antes de o reencaminhar. Este método permite detectar alguns erros, evitando a sua propagação pela rede.

Hoje em dia, existem diversos tipos de Switches híbridos que misturam ambas as arquiteturas.

Diferença entre Hubs e Switches

- Um **hub** simplesmente retransmite todos os dados que chegam para todas as estações conectadas a ele, como um espelho. Causando o famoso broadcast que causa muito conflitos de pacotes e faz com que a rede fica muito lenta.

- O **switch** ao invés de simplesmente encaminhar os pacotes para todas as estações, encaminha apenas para o destinatário correto pois ele identifica as maquinas pelo o MAC addrees que é estático. Isto traz uma vantagem considerável em termos desempenho para redes congestionadas, além de permitir que, em casos de redes, onde são misturadas placas 10/10 e 10/100, as comunicações possam ser feitas na velocidade das placas envolvidas. Ou seja, quando duas placas 10/100 trocarem dados, a comunicação será feita a 100M bits. Quando uma das placas de 10M bits estiver envolvida, será feita a 10M bits.

Roteadores

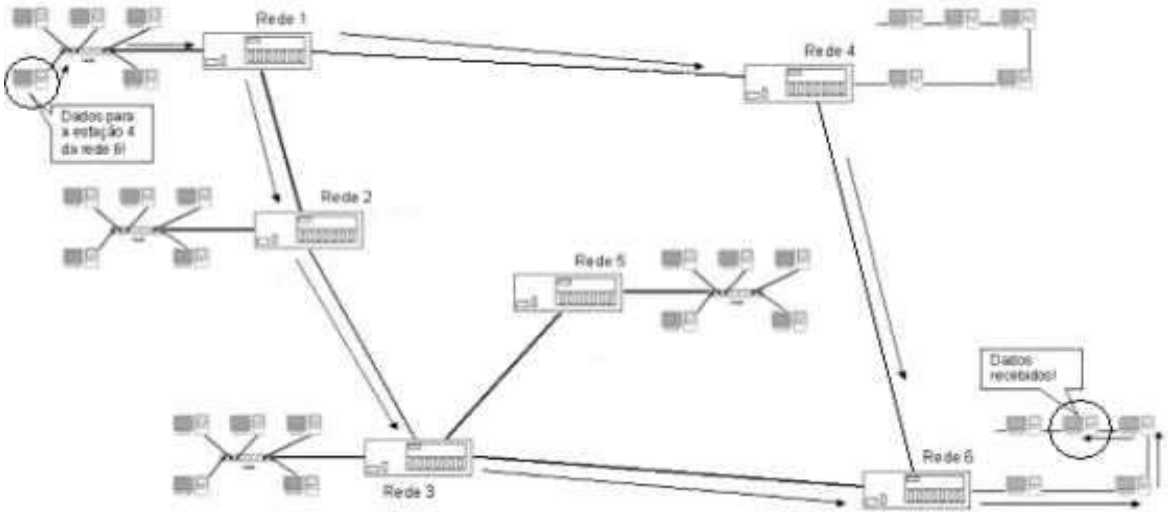
Roteadores são pontes que operam na camada de Rede do modelo OSI (camada três), essa camada é produzida não pelos componentes físicos da rede (Endereço MAC das placas de rede, que são valores físicos e fixos), mais sim pelo protocolo mais usando hoje em dia, o TCP/IP, o protocolo IP é o responsável por criar o conteúdo dessa camada.

Isso Significa que os roteadores não analisam os quadros físicos que estão sendo transmitidos, mas sim os datagramas produzidos pelo protocolo que no caso é o TCP/IP, os roteadores são capazes de ler e analisar os datagramas IP contidos nos quadros transmitidos pela rede.

O papel fundamental do roteador é poder escolher um caminho para o datagrama chegar até seu destino. Em redes grandes pode haver mais de um caminho, e o roteador é o elemento responsável por tomar a decisão de qual caminho percorrer. Em outras palavras, o roteador é um dispositivo responsável por interligar redes diferentes, inclusive podendo interligar redes que possuam arquiteturas diferentes (por exemplo, conectar uma rede Token Ring a uma rede Ethernet, uma rede Ethernet a uma rede x-25

Figura do Roteador

Na figura seguinte é mostrado um exemplo de uso de roteadores. Como você pode perceber, há dois caminhos para o micro da "rede 1" mandar dados para o micro da "rede 6", através da "rede 2" ou através da "rede 4".



Os roteadores podem decidir qual caminho tomar através de dois critérios: o caminho mais curto (que seria através da "rede 4") ou o caminho mais descongestionado (que não podemos determinar nesse exemplo; se o caminho do roteador da "rede 4" estiver congestionado, o caminho do roteador da "rede 2", apesar de mais longo, pode acabar sendo mais rápido).

A grande diferença entre uma ponte e um roteador é que o endereçamento que a ponte utiliza é o endereçamento usado na camada de Link de Dados do modelo OSI, ou seja, o endereçamento MAC das placas de rede, que é um endereçamento físico. O roteador, por operar na camada de Rede, usa o sistema de endereçamento dessa camada, que é um endereçamento lógico. No caso do TCP/IP esse endereçamento é o endereço IP.

Em redes grandes, a Internet é o melhor exemplo, é praticamente impossível para uma ponte saber os endereços MAC de todas as placas de rede existentes na rede. Quando uma ponte não sabe um endereço MAC, ela envia o pacote de dados para todas as suas portas. Agora imagine se na Internet cada roteador enviasse para todas as suas portas dados toda vez que ele não soubesse um endereço MAC, a Internet simplesmente não funcionaria, por caso do excesso de dados.

Devido a isso, os roteadores operam com os endereços lógicos, que trabalham em uma estrutura onde o endereço físico não é importante e a conversão do endereço lógico (Endereço IP) para o endereço físico (endereço MAC) é feita somente quando o datagrama chega à rede de destino.

A vantagem do uso de endereços lógicos em redes grandes é que eles são mais fáceis de serem organizados hierarquicamente, isto é, de uma forma padronizada. Mesmo que um roteador não saiba onde está fisicamente localizada uma máquina que possua um determinado endereço, ele envia o pacote de dados para um outro roteador que tenha probabilidade de saber onde esse pacote deve ser entregue (roteador hierarquicamente superior). Esse processo continua até o pacote atingir a rede de destino, onde o pacote atingira a máquina de destino. Outra vantagem é que no caso da troca do endereço físico de uma máquina em uma rede, a troca da placa de rede defeituosa não fará com que o endereço lógico dessa máquina seja alterado.

É importante notar, que o papel do roteador é interligar redes diferentes (redes independentes), enquanto que papel dos repetidores, hub, pontes e switches são de interligar segmentos pertencentes a uma mesma rede.

Protocolos

Os roteadores possuem uma tabela interna que lista as redes que eles conhecem, chamada tabela de roteamento. Essa tabela possui ainda uma entrada informando o que fazer quando chegar um datagrama com endereço desconhecido. Essa entrada é conhecida como rota default ou default gateway.

Assim, ao receber um datagrama destinado a uma rede que ele conhece, o roteador envia esse datagrama a essa rede, através do caminho conhecido. Caso ele receba um datagrama destinado a uma rede cujo caminho ele não conhece, esse datagrama é enviado para o roteador listado como sendo o default gateway. Esse roteador irá encaminhar o datagrama usando o mesmo processo. Caso ele conheça a rede de destino, ele enviará o datagrama diretamente a ela. Caso não conheça, enviará ao roteador listado como seu default gateway. Esse processo continua até o datagrama atingir a sua rede de destino ou o tempo de vida do datagrama ter se excedido o que indica que o datagrama se perdeu no meio do caminho.

As informações de rotas para a propagação de pacotes podem ser configuradas de forma estática pelo administrador da rede ou serem coletadas através de processos dinâmicos executando na rede, chamados protocolos de roteamento. Note-se que roteamento é o ato de passar adiante pacotes baseando-se em informações da tabela de roteamento. Protocolos de roteamento são protocolos que trocam informações utilizadas para construir tabelas de roteamento.

É importante distinguir a diferença entre protocolos de roteamento (routing protocols) e protocolos roteados (routed protocols). Protocolo roteado é aquele que fornece informação adequada em seu endereçamento de rede para que seus pacotes sejam roteados, como o TCP/IP e o IPX. Um protocolo de roteamento possui mecanismos para o compartilhamento de informações de rotas entre os dispositivos de roteamento de uma rede, permitindo o roteamento dos pacotes de um protocolo roteado. Note-se que um protocolo de roteamento usa um protocolo roteado para trocar informações entre dispositivos roteadores. Exemplos de protocolos de roteamento são o RIP (com implementações para TCP/IP e IPX) e o EGRP.

Roteamento Estático e Roteamento Dinâmico

A configuração de roteamento de uma rede específica nem sempre necessita de protocolos de roteamento. Existem situações onde as informações de roteamento não sofrem alterações, por exemplo, quando só existe uma rota possível, o administrador do sistema normalmente monta uma tabela de roteamento estática manualmente. Algumas redes não têm acesso a qualquer outra rede e, portanto não necessitam de tabela de roteamento. Dessa forma, as configurações de roteamento mais comuns são:

- **Roteamento estático**: uma rede com um número limitado de roteadores para outras redes pode ser configurada com roteamento estático. Uma tabela de roteamento estático é construída manualmente pelo administrador do sistema, e pode ou não ser divulgada para outros dispositivos de roteamento na rede. Tabelas estáticas não se ajustam automaticamente a alterações na rede, portanto devem ser utilizadas somente onde as rotas não sofrem alterações. Algumas vantagens do roteamento estático são a segurança obtida pela não divulgação de rotas que devem permanecer escondidas; e a redução do overhead introduzido pela troca de mensagens de roteamento na rede.

- **Roteamento dinâmico**: redes com mais de uma rota possível para o mesmo ponto devem utilizar roteamento dinâmico. Uma tabela de roteamento dinâmico é construída a partir de informações trocadas entre protocolos de roteamento. Os protocolos são desenvolvidos para distribuir informações que ajustam rotas dinamicamente para refletir alterações nas condições da rede. Protocolos de roteamento podem resolver situações complexas de roteamento mais rápida e eficientemente que o administrador do sistema. Protocolos de roteamento são desenvolvidos para trocar para uma rota alternativa quando a rota primária se torna inoperável e para decidir qual é a rota preferida para um destino. Em redes onde existem várias alternativas de rotas para um destino devem ser utilizados protocolos de roteamento.

Protocolos de roteamento

Todos os protocolos de roteamento realizam as mesmas funções básicas. Eles determinam a rota preferida para cada destino e distribuem informações de roteamento entre os sistemas da rede. Como eles realizam estas funções, em particular eles decide qual é a melhor rota, é a principal diferença entre os protocolos de roteamento.

Tipos de Protocolos

IGP (interior gateway protocol) - Estes são utilizados para realizar o roteamento dentro de um Sistema Autônomo. Existem vários protocolos IGP, vejamos alguns:

- RIP (Routing Information Protocol)
- IGRP (Interior Gateway Routing Protocol)
- Enhanced IGRP
- OSPF (Open Shortest Path First)
- IS-IS (Intermediate System-to-Intermediate System)

EGP (exterior gateway protocol) - Estes são utilizados para realizar o roteamento entre Sistemas Autônomos diferentes. É dividido em:

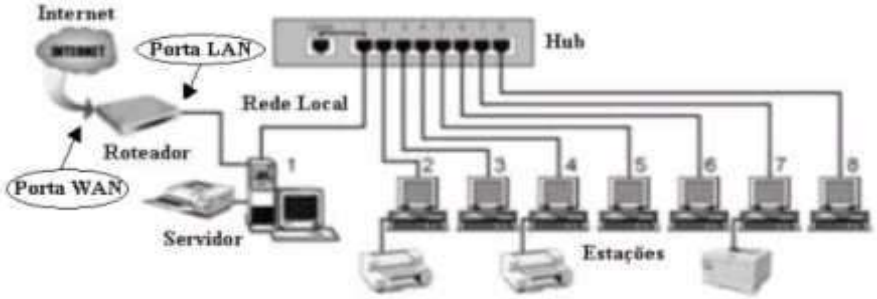
- EGP (Exterior Gateway Protocol) - protocolo tem o mesmo nome que o seu tipo.
- BGP (Border Gateway Protocol)

Características

Quando se fala em roteadores, pensamos em basicamente três usos: conexão Internet, conexão de redes locais (LAN) ou conexão de longo alcance (WAN).

Relembrando como vimos anteriormente podemos definir esse equipamento como sendo um modulo processador que interliga duas ou mais redes.

Para ficar mais claro seu uso, vamos dar o exemplo do uso de roteadores na interligação entre duas redes: a Internet e a rede local de uma empresa, veja figura:



O roteador típico para esse uso deve possuir basicamente duas portas: uma porta chamada WAN e uma porta chamada LAN. A porta WAN recebe o cabo que vem do backbone da Internet. Normalmente essa conexão na porta WAN é feita através de um conector chamado V.35 que é um conector de 34 Pinos. A porta LAN é conectada à sua rede local. Essa porta também pode ser chamada Eth0 ou saída Ethernet, já que a maioria das redes locais usa essa arquitetura. Existem outros tipos de conexões com o roteador, a ligação de duas redes locais (LAN), ligação de duas redes geograficamente separadas (WAN).

O roteador acima mostrado é apenas um exemplo ilustrativo, pois normalmente os roteadores vêm com mais de uma porta WAN e com mais de uma porta LAN, sendo que essas portas têm características de desempenho muito distintas, definidas pelo modelo e marca de cada roteador.

Cada uma das portas / interfaces do roteador deve receber um endereço lógico (no caso do TCP/IP, um número IP) que esteja em uma rede diferente do endereço colocado nas outras portas. Se você rodar um traceroute através de um roteador conhecido, verá que dois endereços IP aparecem para ele. Um refere-se à sua interface WAN e outro à sua interface LAN.

Na hora de se escolher um roteador ou desenhar um esquema de rede com roteadores, deve-se levar em consideração algumas características básicas encontradas nos roteadores:

- Número de portas WAN
- Número de portas LAN
- Velocidade das portas WAN
- Velocidade das portas LAN
- Redundância
- Tolerância a falhas
- Balanceamento de carga

Alguns roteadores possuem um recurso chamado *redundância de call-up*. Esse recurso permite ligar o roteador a um modem através de um cabo serial e, caso o link WAN principal falhar, o modem disca para um provedor e se conecta mantendo a conexão da rede local com a Internet no ar.

Modem utilizado para conexão Backup

Alguns roteadores trazem a solução para esse problema através de recursos de redundância e tolerância à falhas. Através desse recurso, o roteador continua operando mesmo quando ele se danifica. Para entender isso, basta imaginar um roteador que possua, na realidade, dois dentro roteadores dentro dele. Caso o primeiro falhe, o segundo entra em ação imediatamente. Isso permite que a rede não saia do ar no caso de uma falha em um roteador.

Existem ainda roteadores capazes de gerenciar duas ou mais conexões entre ele e outro roteador, permitindo dividir o tráfego entre esses links, otimizando as conexões. Essa característica, chamada balanceamento de carga, é utilizada, por exemplo, em conexões ter filiais de empresas.