Redes – Infra
- estrutura

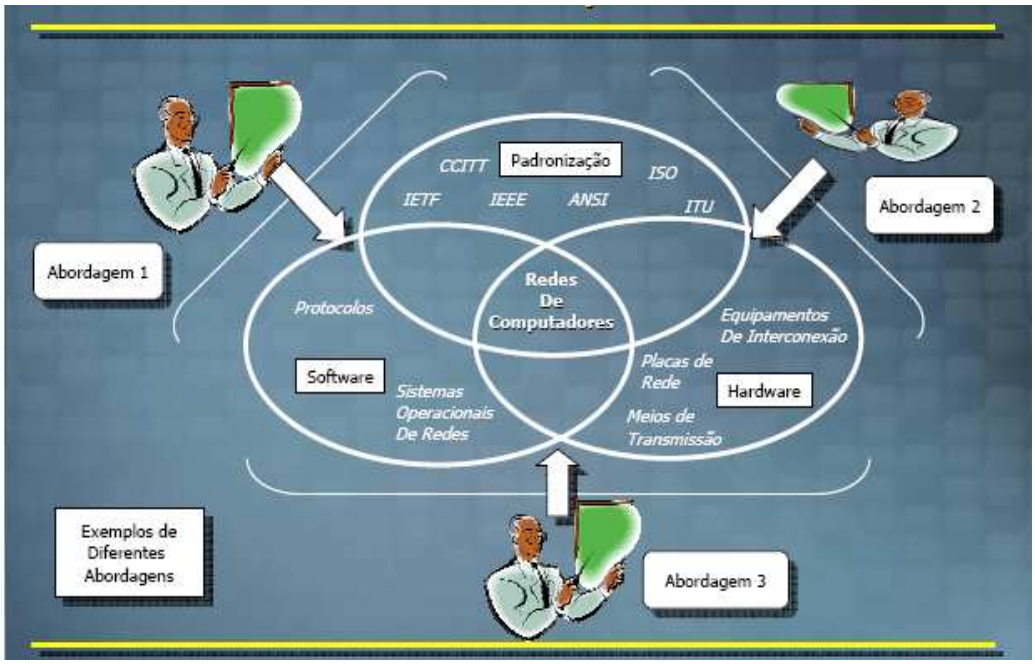
SENAC – Serviço Nacional de Aprendizagem Comercial

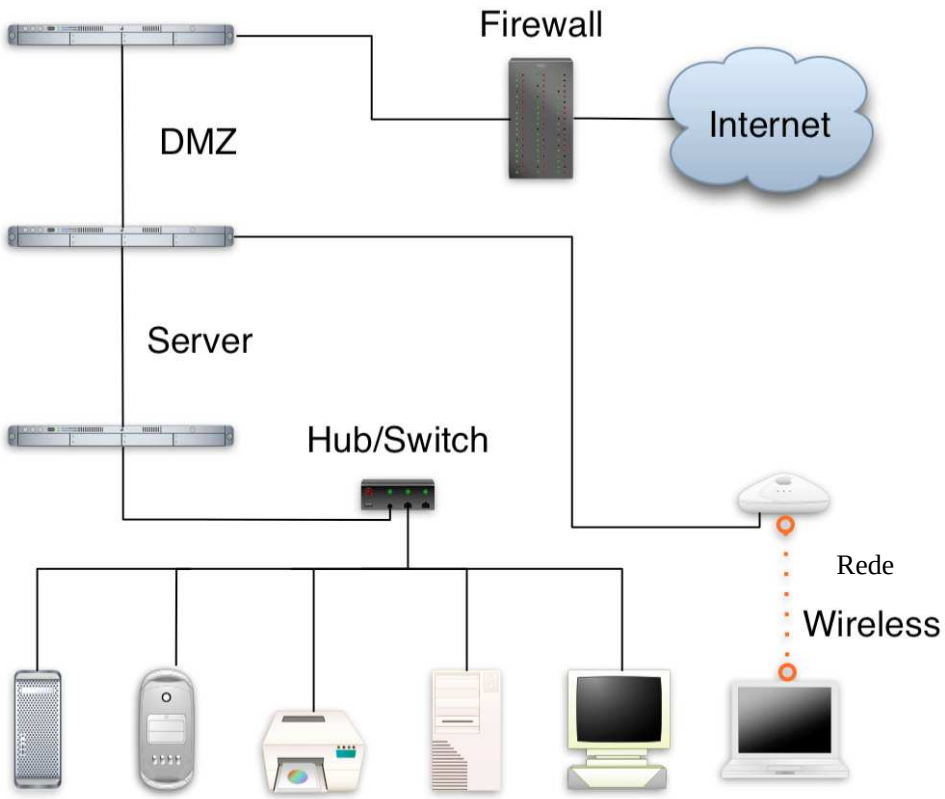
Redes
Infra-estrutura

Professora: Dárley Lima dos Santos

Governador Valadares – 2º semestre de 2007

Estudo de Rede de Computadores





Redes de Computadores

Interligação de dois ou mais computadores através de cabos (utp, fibra óptica), ondas de rádio, sinal infra-vermelho, etc., compartilhando dados e recursos.

Uma estrutura de rede, incorretamente instalada, é responsável por até 60% dos problemas apresentados na rede local.

A resolução destes problemas consome até 50% do tempo do pessoal de suporte da área de TI (tecnologia da informação).

Para seu funcionamento são necessários:

- Equipamentos e dispositivos de rede (hub, bridges, switches, roteadores);
- Meios de transmissão (cabos utp, fibra óptica, link internet);
- Protocolos de comunicação (tcp-ip).

Roteador

Uma maquina que esta em uma classe de rede não pode se comunicar com outra fora da classe, ai é que entra o **roteador.** Veja que temos três roteadores cada um ligando uma rede para outra.

Ai você pergunta. Mas como eu tenho um computador em casa e lá eu só tenho o modem e consigo entra na internet? Simplesmente porque o seu provedor faz o roteamento pra você, no caso de uma rede local você vai ter que por um roteador para ele poder fazer o papel do provedor e dar acesso a todas maquinas.

Bridges

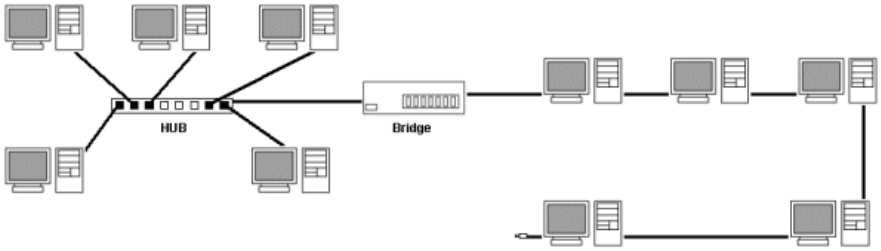
Imagine que em sua empresa existam duas redes; uma rede Ethernet, e outra rede Token Ring. Veja que apesar das duas redes possuírem arquiteturas diferentes e incompatíveis entre si, é possível instalar nos PCs de ambas um protocolo comum, como o TCP/IP por exemplo. Com todos os micros de ambas as redes 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, 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, que estudaremos à fundo mais adiante.

Imagine que você tenha 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.

Caso você tenha uma rede muito grande, que esteja tornando-se lenta devido ao tráfego intenso, você também pode utilizar 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 são chamados de bridges de encaminhamento, servem para conectar redes diferentes, mas não para diminuir o tráfego de dados.



Protocolo

Conjunto estabelecido ou aceito de procedimentos, regras ou especificações formais que governam a comunicação entre os nós de uma rede.

Protocolos Humanos
- Que horas são?
- Eu tenho uma pergunta
- Apresentações
- Regras de comportamento
- Etc.

Protocolos de Redes
- Máquinas ao invés de humanos
- Toda atividade de comunicação internet é governada por protocolos.

Protocolos definem os formatos, a ordem das msgs enviadas e recebidas pelas entidades de rede e as ações que devem ser tomadas na transmissão e recepção destas mensagens. (estudaremos mais adiante os tipos de protocolos).

Padrões de Rede

Formatado: Português Brasil

ETHERNET

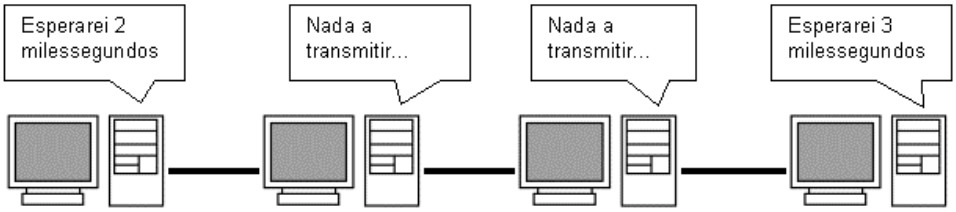
As placas de rede Ethernet são as mais utilizadas atualmente, sobretudo em redes pequenas e médias e provavelmente a única arquitetura de rede com a qual você irá trabalhar. Numa rede Ethernet quando uma estação precisar transmitir dados, ela irradiará o sinal para toda a rede. Todas as demais estações 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.

Exemplo do Funcionamento:

- Grupo de amigos que querem falar
- Enquanto um fala os outros ouvem
- Quando ninguém está a falar, outro pode começar
- Problema:
  - Quando todos estiverem calados, dois podem começar a falar ao mesmo tempo (colisão!!!)

Vantagens:

- Baixo custo
- Maior velocidade em pequenas redes



TOKEN RING

Formatado: Português Brasil

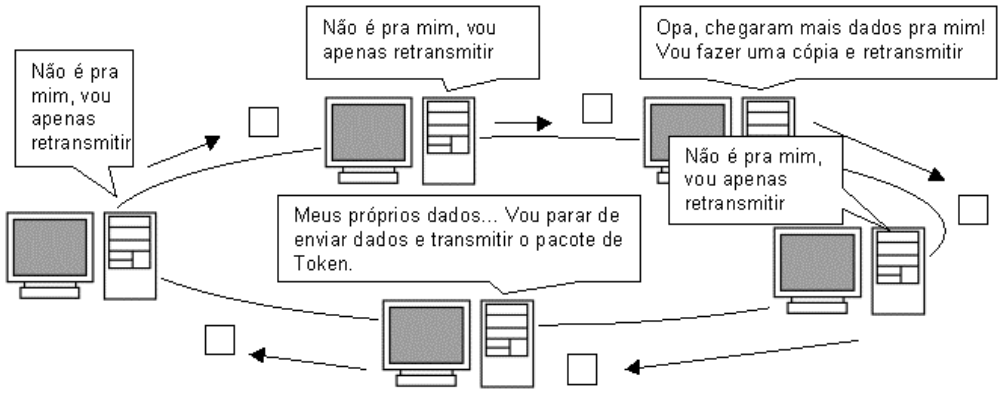
Um pacote especial, chamado pacote de Token circula pela rede, sendo transmitido de estação para estação. Quando uma estação precisa transmitir dados, ela espera até que o pacote de Token chegue e, em seguida, começa a transmitir seus dados, evitando assim a colisão.

Características:

- O custo de montagem é muito maior que o de uma rede Ethernet.
- Em pequenas redes a velocidade é limitada.
- Usa topologia lógica Anel.
- Quase imune a colisões.

Exemplo do Funcionamento:

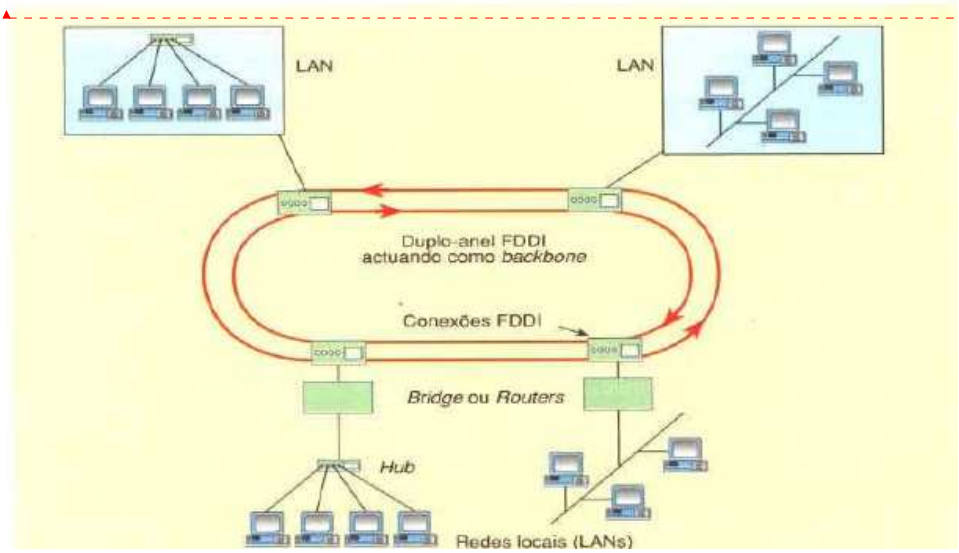
- Grupo de amigos em círculo
- Uma bola é passada de amigo para amigo
  - Quando alguém tem a bola, passa-a para o amigo à sua direita
- Cada amigo só pode falar enquanto tiver a bola
  - Isto garante que só uma pessoa fala de cada vez
- A pessoa que recebe a bola, em vez de falar, escreve a mensagem num papel
  - Incluindo o nome do destinatário
- Antes de passar a bola passa a carta à pessoa à sua direita
- Se a pessoa que receber a carta for o destinatário, lê a mensagem e assina-a
- Assim que a mensagem volta ao remetente, este verifica que a mensagem foi recebida (assinada) e de seguida destrói-a
  - Entretanto a bola continua a circular


Não é pra mim, vou apenas retransmitir
Não é pra mim, vou apenas retransmitir
Opa, chegaram mais dados pra mim! Vou fazer uma cópia e retransmitir
Não é pra mim, vou apenas retransmitir
Meus próprios dados... Vou parar de enviar dados e transmitir o pacote de Token.

IEEE → (Institute of Electrical and Electronis Engineers – responsável pelos padrões I3Es)
ATM → Estudo aprofundado mais adiante,

FDDI → Token Ring usando fibra óptica.

Formatado: Português Brasil



O padrão FDDI (Fiber Distributed Data Interface) foi estabelecido pelo ANSI (American National Standards Institute) em 1987. É uma rede em duplo anel usando fibra ótica como meio físico para transmissão de dados.

A expansão de redes de âmbito mais alargado, designadamente redes do tipo MAN (Metropolitan Area Network), são algumas das possibilidades do FDDI, tal como pode servir de base à interligação de redes locais, como nas redes de campus.

As redes FDDI adotam uma tecnologia de transmissão idêntica às das redes Token Ring, mas utilizando, vulgarmente, cabos de fibra óptica, o que lhes concede capacidades de transmissão muito elevadas (na casa dos 100 Mbps ou mais) e a oportunidade de se alargarem a distâncias de até 200 Km, conectando até 1000 estações de trabalho.

Estas particularidades tornam esse padrão bastante indicado para a interligação de redes através de um backbone – nesse caso, o backbone deste tipo de redes é justamente o cabo de fibra óptica duplo, com configuração em anel FDDI, ao qual se ligam as sub-redes.

O FDDI alarga a extensão de uma LAN para uma área geográfica muito maior do a habitual com Ethernet, o que pode trazer um incremento no numero de utilizadores do sistema.

Enquanto os padrões ETHERNET e TOKEN-RING têm aplicação exclusivamente em redes locais (LANs), o padrão FDDI permite o desenvolvimento de redes com um âmbito maior, nomeadamene redes do tipo MAN (Metropolitam Área Network).

Meios de transmissão

Transmissão guiada:
- Cabo coaxial
- Par trançado UTP
- Par trançado STP
- Par trançado FTP
- Fibras ópticas

Transmissão não guiada:
- Infra-vermelho
- Micro-ondas
- Rádio
- Satélite

Cabo Coaxial

É um tipo de cabo condutor usado para transmitir sinais e são bem mais protegidos contra interferências magnéticas.

A principal razão da sua utilização deve-se ao fato de poder reduzir os efeitos e sinais externos sobre os sinais a transmitir. O cabo coaxial é constituído por um fio de cobre condutor revestido por um material isolante e rodeado duma blindagem. Este meio permite transmissões até freqüências muito elevadas e isto para longas distâncias.

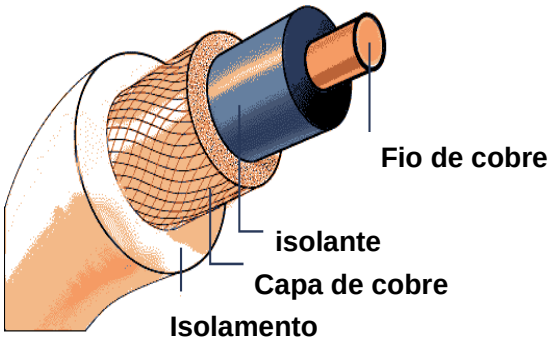
Os cabos coaxiais geralmente são usados em múltiplas aplicações desde áudio ate ás linhas de transmissão de alta freqüência. A velocidade de transmissão é bastante elevada devido à tolerância aos ruídos graças à malha de proteção desses cabos.

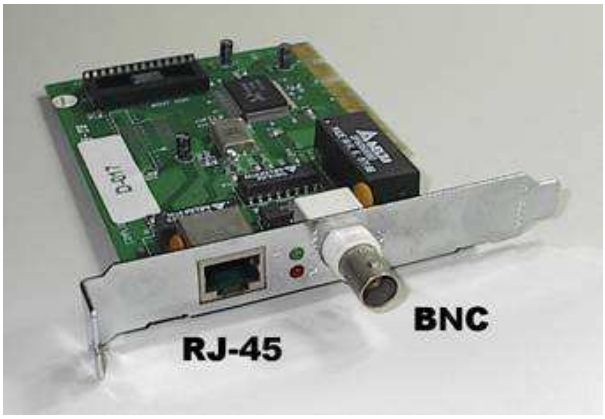
Os cabos coaxiais são usados em diferentes aplicações:
- Ligações áudio
- Ligações rede de computadores
- Normalmente utilizado em instalações que envolvem prédios nos quais *a rede se estende na vertical*.
- Usado em sistemas de distribuição de TVs e TV à cabo.

Vantagens:
O Cabo Coaxial possui vantagens em relação aos outros condutores utilizados tradicionalmente em linhas de transmissão por causa de sua blindagem adicional, que o protege contra o fenômeno da indução, causado por interferências elétricas ou magnéticas externas (imune a ruídos).

Desvantagem:
Mais caro que o par trançado.

Figuras: Cabo e conector coaxial.





Par trançado

O par trançado é o meio de transmissão mais antigo e ainda mais usado para aplicações de comunicações. O cabeamento por par trançado (Twisted pair) é um tipo de fiação na qual dois condutores são enrolados ao redor dos outros para cancelar interferências magnéticas de fontes externas e interferências mútuas (crosstalk) entre cabos vizinhos. A taxa de giro (normalmente definida em termos de giros por metro) é parte da especificação de certo tipo de cabo. Quanto maior o número de giros, mais o ruído é cancelado.

Quando se trata de um número muito grande de pontos a velocidade decresce muito.

Todo o meio físico de transmissão sofre influências do meio externo acarretando em perdas de desempenho nas taxas de transmissão. Essas perdas podem ser atenuadas limitando a distância entre os pontos a serem ligados.

A vantagem principal na utilização do par de fios é seu baixo custo de instalação e manutenção, considerando o grande número de bases instaladas.

Existem várias categorias de cabo par trançado.

Existem 5 categorias, levando em conta o nível de segurança e a bitola do fio, onde os números maiores indicam fios com diâmetros menores.

Categorias 1, 2, 3 4, 5, 5e 6 7.

Categoria do cabo 5: usado muito em redes ethernet. Pode ser usado para frequencias até 100MHz com uma taxa de 100Mbps.

Categoria do cabo 5e: é uma melhoria da categoria 5. Pode ser usado para frequencias até 125MHz .

Categoria do cabo 6: Pode ser usado em redes gigabit ethernet a velocidade de 1.000Mbps.

***OBS**.: Existe a categoria 7 que está em fase de aprovação e testes.
Esses cabos contêm 4 pares de fios, que são crimpados (ligados ao conector) com uma determinada combinação de cores.

Existem também limites de comprimentos para esse tipo de cabo. É recomendado um limite de 80 à 100 metros de comprimento para que não haja lentidão e perda de informações.
Obs: A taxa de transmissão de dados correspondente depende dos equipamentos a serem utilizados na implementação da rede.

Devido ao custo e ao desempenho obtidos, os pares trançados são usados em larga escala e é provável que assim permaneçam nos próximos anos. O conector utilizado é o RJ-45

Vantagens:
- ❖ simplicidade
- ❖ baixo custo do cabo e dos conectores
- ❖ facilidade de manutenção e de detecção de falhas
- ❖ fácil expansão

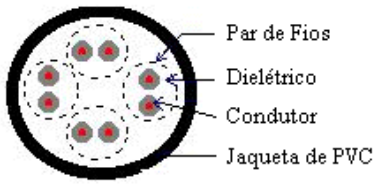
Desvantagens:
Susceptibilidade à interferência e ao ruído.

Existem três tipos de par trançado:

- ❖ Par trançado sem blindagem (UTP-Unshielded Twisted Pair)
- ❖ Par trançado blindado (STP-Shielded Twisted Pair).
- ❖ Par trançado blindado (FTP).

Par trançado sem blindagem (UTP)

É composto por pares de fios sendo que cada par é isolado um do outro e todos são trançados juntos dentro de uma cobertura externa. Não havendo blindagem física interna.

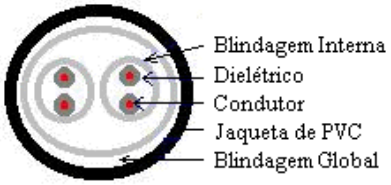


Dielétrico → Dielétrico (ou isolante): material que não conduz corrente elétrica mobilidade baixíssima dos portadores de carga.

Uma grande vantagem é a flexibilidade e espessura dos cabos. O UTP não preenche os dutos de fiação com tanta rapidez como os outros cabos. Isso aumenta o número de conexões possíveis sem diminuir seriamente o espaço útil.

Par trançado blindado (STP)

Possui uma blindagem interna envolvendo cada par trançado que compõe o cabo, cujo objetivo é reduzir a diafonia. Um cabo STP geralmente possui 2 pares trançados blindados.



Vantagens:

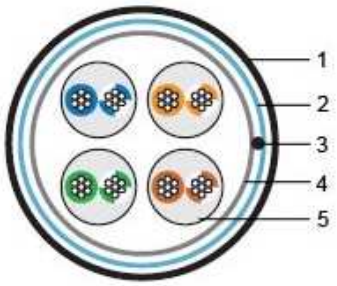
- ❖ Alta taxa de sinalização
- ❖ Pouca distorção do sinal

Desvantagens:

A blindagem causa uma perda de sinal que torna necessário um espaçamento maior entre os pares de fio e a blindagem, o que causa um maior volume de blindagem e isolamento, aumentando consideravelmente o tamanho, o peso e o custo do cabo.

Par trançado blindado (FTP):

Cabo blindado bem mais resistente que o STP, usado em redes industriais.



1 - Cobertura externa
2 - Blindagem de folha de aço
3 - Cabo de drenagem
4 - Fita de proteçã
5 - Par trançado patch

Fibras ópticas:

As fibras de óticas são muito utilizadas pelos computadores para a transmissão de dados.

Os sistemas de comunicações baseados em fibra óptica utilizam lasers ou dispositivos emissores de luz (LEDs).

Algumas das características físicas da Fibra Óptica:

Pode ser instalada verticalmente em prédios. É perfeita também para uso aéreo (externos) e subterrâneo (internos).

A prova de fogo, resistentes à umidade e fungos, alguns tipos de fibras são protegidos por uma jaqueta (revestimento).

Facilmente maleável durante a instalação

Atende às especificações FDDI.

A principal razão para a confiabilidade dos sistemas de fibras reside no fato de que elas não transportam sinais elétricos. Mesmo com proteção e um bom aterramento, os cabos de cobre se comportam como antenas e absorvem energia de motores, transmissores de rádio e outros dispositivos elétricos. Dessa forma, há o risco de ocorrerem diferenças de potencial em relação ao aterramento, podendo ser ocasionadas até mesmo fagulhas nos cabos. Essas interferências elétricas acabam por enfraquecer o sinal e distorcer os pacotes de dados. Os cabos de fibras de vidro são imunes a campos elétricos e magnéticos, sendo, portanto imunes a problemas dessa natureza.

Os dados são convertidos em luz antes de serem transmitidos.

Vantagens:

- Não sofre interferência eletromagnética
- Consegue transmitir mais longe e em maior quantidade as informações que um fio de cobre faz com um sinal elétrico.
- Não requer dois fios de fibra de vidro para transmitir dados.

Desvantagens:

- Requer equipamento especiais para polimento e instalação das extremidades do fio;
- Requer equipamentos especiais para unir um cabo partido;
- Dificuldade em descobrir onde a fibra se partiu dentro do revestimento plástico.
- Alto custo

Aplicações:

- Usados em troncos de comunicação;
- Troncos metropolitanos;
- Redes LANs

Wireless

As tecnologias de redes sem fio incluem desde redes de dados e de voz globais, que permitem que os usuários estabeleçam conexões sem fio por longas distâncias, até tecnologias de freqüência de rádio e luz infravermelha que são otimizadas para conexões sem fio de curta distância. Entre os dispositivos utilizados com freqüência nas redes sem fio estão computadores portáteis, computadores de mesa, computadores de bolso, assistentes digitais pessoais (PDAs), telefones celulares, computadores com canetas e beeps. As tecnologias sem fio atendem a vários fins práticos. Por exemplo:

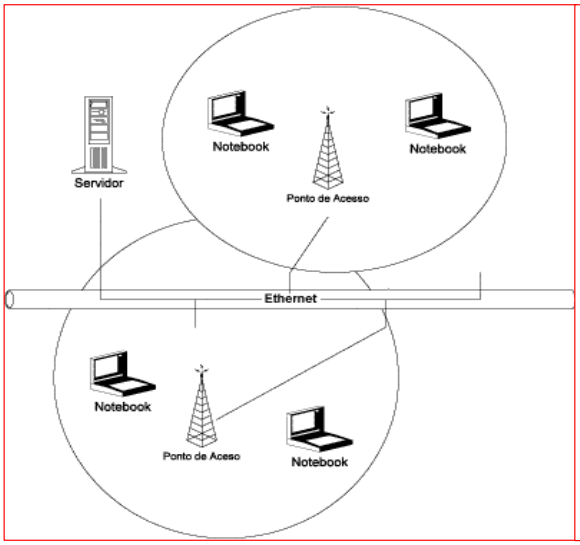
- Os usuários de celulares podem usar seus aparelhos para acessar e-mails.
- Os viajantes com computadores portáteis podem se conectar a Internet através de estações de base instaladas em aeroportos, estações ferroviárias e outros locais públicos.
- Em casa, os usuários podem conectar dispositivos em seus computadores de mesa para sincronizar dados e transferir arquivos.

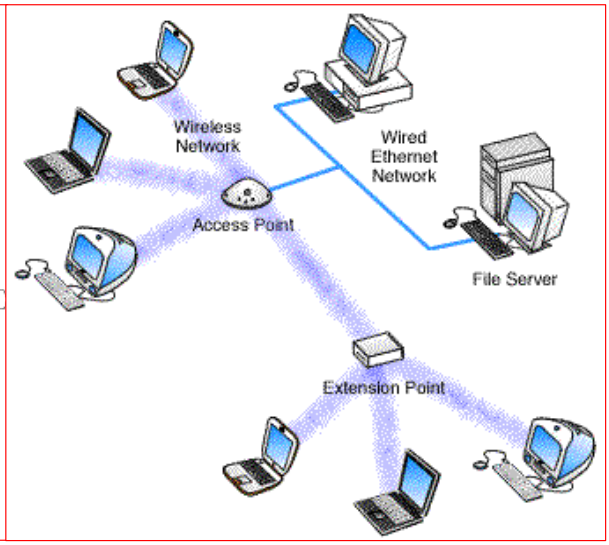
Transmissão não guiada ou Rede sem fio: (Infra-vermelho, Micro-ondas, Rádio freqüência)

Padrão I3Es: Diversos padrões, cada um com a sua tecnologia, usado para redes wireless.

Tecnologias usadas nos padrões I3Es:

- IRDA
- ZigBee
- Bluetooth
- WiMAX
- Mesh
- Wi-Fi





Access Point (ponto de acesso): Funciona como uma ponte de comunicação entre a rede sem fio e a rede convencional.

Vantagens da rede sem fio:

- Redução no tempo de instalação
  - redes temporárias: feiras, exposições, etc.
- Fácil planejamento
  - não exige cabeamento prévio
  - redes ad roc não exigem planejamento algum
- Instalação em áreas de difícil cabeamento
- Maior confiabilidade e robustez
  - áreas sujeitas a intempéries
  - sobrevive a desastres
- Permite a mobilidade dos equipamentos
- Estética (ausência de cabos)
- Flexibilidade
  - emissores e receptores podem ser colocados em qualquer lugar (dentro de dispositivos, muros, etc).
- Diminuição do custo de infra-estrutura
  - cabeamento, conectorização, etc

Desvantagens e dificuldades encontradas na rede sem fio:

- Baixa qualidade de serviço
  - Altas taxas de erros
- Restrições no uso de freqüências
  - regulação governamental
- Interferência do sinal de rádio
  - vulnerabilidade a ruídos atmosféricos e transmissões de outros sistemas.
  - propagação por múltiplos caminhos
- Segurança
  - baixa privacidade
  - intrusão, congestionamento da estação-base
- Riscos a saúde (polêmica – nada comprovado)

Tipos de rede sem fio:

Assim como as redes tradicionais, as redes sem fio podem ser classificadas em diferentes tipos com base nas distâncias através das quais os dados podem ser transmitidos.

Redes sem fio pessoais (WPANs)

As tecnologias WPAN permitem que os usuários estabeleçam comunicações ad hoc sem fio para dispositivos (como PDAs, telefones celulares ou laptops) que são utilizados em um espaço operacional pessoal (POS). Um POS é o espaço que cerca uma pessoa, até a distância de 10 metros. No momento, as duas principais tecnologias WPAN são a Bluetooth e a luz infravermelha. A Bluetooth é uma tecnologia de substituição de cabos que utiliza ondas de rádio para transmitir dados a uma distância de até 9 metros. Por meio dessa tecnologia, os dados podem ser transferidos através de paredes, bolsos e pastas. O desenvolvimento de tecnologia para Bluetooth é coordenado pelo Bluetooth Special Interest Group (SIG), que publicou a especificação Bluetooth versão 1.0 em 1999. De forma alternativa, para conectar dispositivos que estejam muito próximos (1 metro ou menos).

Para padronizar o desenvolvimento de tecnologias WPAN, o IEEE estabeleceu o grupo de trabalho 802.15 para WPANs.

Redes sem fio locais (WLANs)

As tecnologias WLAN permitem que os usuários estabeleçam conexões sem fio em uma área local (por exemplo, em um prédio corporativo ou de um campus, ou em um espaço público, como um aeroporto). As WLANs podem ser usadas em escritórios temporários ou em outros espaços em que a instalação extensiva de cabos teria um custo muito elevado, ou para complementar uma LAN existente de modo que os usuários possam trabalhar em diferentes locais em um prédio, em diferentes horários. As WLANs podem funcionar de duas maneiras distintas. Em WLANs de infra-estrutura, estações sem fio (dispositivos com placas de rede de rádio ou modems externos) se conectam a pontos de acesso sem fio que funcionam como pontes entre as estações e o backbone de rede existente . Em WLANs ponto a ponto (ad hoc), vários usuários em uma área limitada, como uma sala de conferências, podem formar uma rede temporária sem usar pontos de acesso, se não precisarem de acesso a recursos de rede.

Em 1997, o IEEE aprovou o padrão 802.11 para WLANs.

Redes sem fio metropolitanas (WMANs)

As tecnologias **WMAN** permitem que os usuários estabeleçam conexões sem fio entre vários locais em uma área metropolitana (por exemplo, entre vários prédios de escritórios em uma cidade ou em um campus universitário), sem o custo elevado proveniente da instalação de cabos de cobre ou fibra e da concessão de linhas. Além disso, as WMANs podem funcionar como backups das redes que utilizam cabos, caso as principais linhas dedicadas dessas redes não estejam disponíveis. As WMANs utilizam ondas de rádio ou luz infravermelha para transmitir dados. Há uma demanda crescente por redes de acesso sem fio de banda larga que forneçam aos usuários acesso de alta velocidade à Internet.

Criando uma rede sem fio

1) Desabilite o firewall do windows
2) Compartilhe o C:
3) Clique em Inciar/Painel de controle/conexões de rede sem fio/botão direito propriedades.
4) Clique na aba sem fio e depois no botão avançado.
5) Marque a opção “Apenas redes de computador ad-hoc” - OK
6) Agora clique no botão adicionar e dê um nome para a sua rede. Selecione a rede e clique em propriedades
7) Na opção “Autenticação de rede” escolha ABERTO
8) Criptografia de dados: WEP
9) Desative a opção “Chave fornecida automaticamente” e informe a senha 12345.
10) Depois clique em OK.
11) Informe um número de IP: 169.254.29.10 e máscara de sub-rede: 255.255.0.0
12) Crie no C: do notebook ao lado uma pasta com o seu nome.

Modem a cabo (Cable Modem)

Esta tecnologia, também conhecida por Cable Modem, utiliza as redes de transmissão de TV por cabo convencionais (chamadas de CATV - Community Antenna Television) para transmitir dados em velocidades que variam de 256 Kbps a 24 Mbps, fazendo uso da porção de banda não utilizada pela TV a cabo.

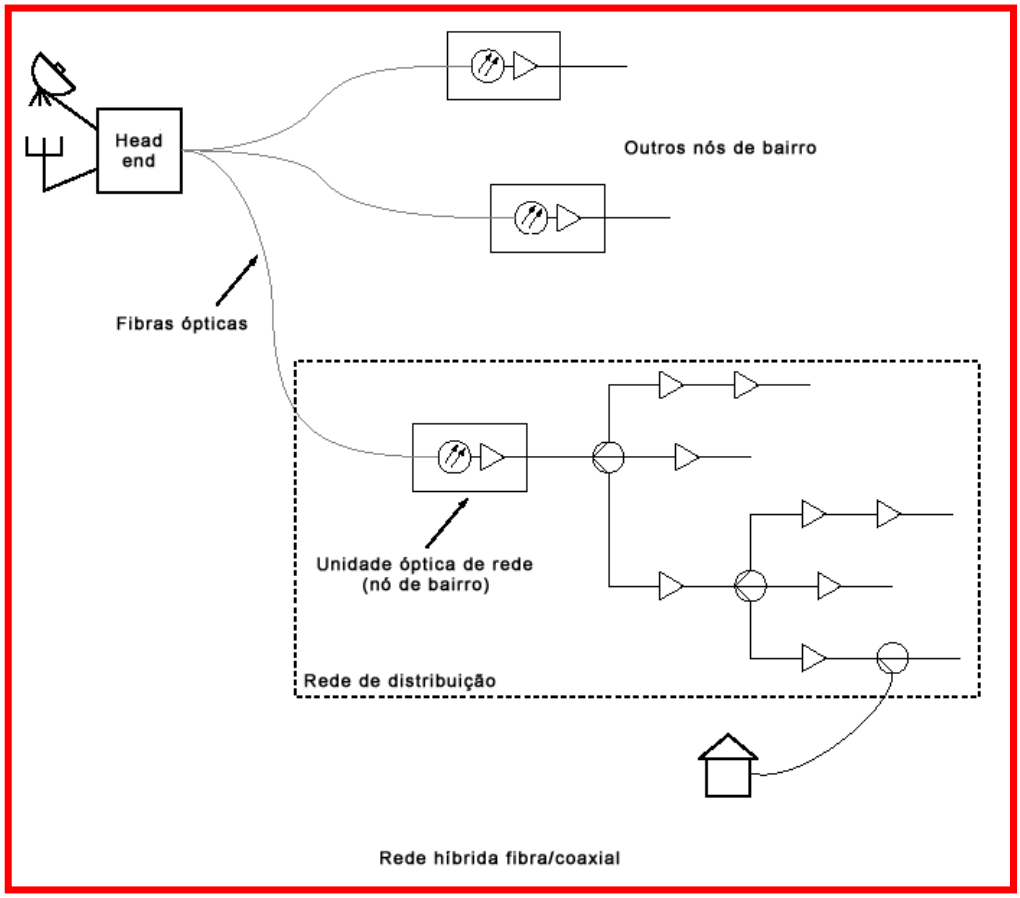
Utiliza uma topologia de rede partilhada, onde todos os utilizadores partilham a mesma largura de banda.

Para este tipo de acesso à internet utiliza-se um cabo coaxial e um modem. O computador do usuário deve estar equipado com placa de rede Ethernet. Nela, conecta-se um cabo par-trançado (UTP). A outra extremidade deste cabo deve ser ligada ao modem. Ao modem, também é conectado o cabo coaxial da TV, que servirá para conectar o usuário à Internet.

Uma operadora de televisão por assinatura deve obter uma licença da Anatel para fornecer seus serviços no Brasil

Funcionamento:

Para atingir a cobertura geográfica pelo bairro, os cabos, oriundos do head end (extremidade principal) são ramificados em múltiplos cabos e cada um dos assinantes recebe o sinal de todos os canais que são transmitidos - é uma estrutura em árvore. Assim como os aparelhos de TV possuem um sintonizador para escolher o canal desejado que é recebido via rádio, os aparelhos de recepção dos assinantes de TV a cabo, também possuem um sintonizador para escolha do canal recebido pelo cabo. Pelo fato de os sinais serem atenuados à medida em que viajam pelo cabo até os assinantes, amplificadores devem ser inseridos na planta para restaurar a potência do sinal. Quanto mais longo for o cabo ou quanto mais ele for ramificado, maior também será o número de amplificadores necessários. Uma inovação neste sistema trata-se da utilização de uma arquitetura mista entre cabo de cobre (cabos UTPs) e fibras. As fibras partem do head end e vão até o bairro, de onde os sinais passam a ser transportados por cabos coaxiais até a casa dos assinantes. Duas vantagens principais sobre o uso dessa tecnologia repousam na maior banda passante disponível e no fato de os sinais poderem ser transportados por distâncias mais longas sem amplificação além da imunidade que a mídia óptica apresenta em relação a interferências eletromagnéticas. A seguir pode ser visto um esquema no qual apresentamos a utilização de um sistema híbrido de cobre e fibra. Nesse esquema ainda fica clara a forma de árvore que a arquitetura que os sistemas de TV a cabo apresentam.



Rede híbrida fibra/coaxial

TECNOLOGIA VOIP

Imagine você fazendo uma ligação telefônica para um parente ou para um amigo que mora em outro país, mas pagando apenas o valor de uma chamada local, isso está se tornando realidade graças ao VoIP.

VoIP (Voice over Internet Protocol) é uma tecnologia que permite a transmissão de voz por IP, tornando possível a realização de chamadas telefônicas (com qualidade) pela internet. Também conhecida por Voz sobre IP, o VoIP está cada vez mais popular e surgem cada vez mais empresas que lidam com essa tecnologia.

O voIP faz com que as redes de telefonia se "misturem" às redes de dados. Dessa forma, é possível que, usando um microfone, caixas ou fones de som e um software apropriado, você faça uma ligação para telefones convencionais por meio de seu computador.

Funcionamento do VoIP

Para que a transmissão de voz seja possível, o VoIP captura a voz, que até então é transmitida de forma analógica e a transforma em pacotes de dados, que podem ser enviados por qualquer rede TCP/IP (Transport Control Protocol/Internet Protocol). Assim, é perfeitamente possível trabalhar com esses pacotes pela internet. Quando o destino recebe os pacotes, estes são retransformados em sinais analógicos e transmitidos a um meio no qual seja possível ouvir o som.

Assim que começou a se popularizar, o VoIP foi encarado como um "inimigo" das empresas de telefonia tradicionais. Mas, logo, viu-se que essa tecnologia é, na verdade, um novo produto a ser explorado. Além das vantagens relativas aos custos, há ainda a questão do constante aumento de qualidade. Já há casos em que a qualidade sonora do VoIP supera a qualidade de uma ligação telefônica convencional.

Atualmente, a tecnologia VoIP não se limita às empresas. Graças ao programa Skype, criado por Niklas Zennström (o criador do KaZaA), o uso de voz sobre IP está sendo possível também a usuários domésticos. Isso é um sinal evidente de que o VoIP pode ser tornar um dos fenômenos da internet, assim como é o e-mail. Certamente, assistiremos uma grande mudança no ato de usar o telefone.

TECNOLOGIA ISDN

ISDN é a sigla para Integrated Services Digital Network. Essa tecnologia também recebe o nome de RDSI - Rede Digital de Serviços Integrados. Trata-se de um serviço disponível em centrais telefônicas digitais, que permite acesso à internet e baseia-se na troca digital de dados, onde são transmitidos pacotes sobre condutores de "par-trançado".

A tecnologia ISDN já existe há algum tempo, tendo sido consolidada entre os anos de 1984 e 1986. Através do uso de um equipamento adequado, uma linha telefônica convencional é transformada em dois canais de 64 Kbps, onde é possível usar voz e dados ao mesmo tempo, sendo que cada um ocupa um canal. Também é possível usar os dois canais para voz ou para dados. Visto de modo grosso, é como se a linha telefônica fosse transformada em duas.

A tecnologia ISDN possui um padrão de transmissão que possibilita aos sinais que trafegam internamente às centrais telefônicas serem gerados e recebidos em formato digital no computador do usuário, sem a necessidade de um modem. No entanto, para ser ativado o serviço ISDN em uma linha telefônica, é necessário que sejam colocados equipamentos ISDN na casa do usuário e que a central telefônica na qual a linha do assinante esteja conectada seja preparada para o serviço ISDN.

Enquanto as linhas telefônicas convencionais geralmente transmitem a uma taxa de 28,8 a 56 Kbps, os dispositivos ISDN comuns podem transmitir a 64 ou 128 Kbps por segundo. Essa velocidade é inferior à das redes locais que têm suporte de tecnologias de comunicação de dados de alta velocidade, mas superior à das linhas telefônicas analógicas.

Uma linha ISDN precisa ser instalada pela companhia telefônica no local e no servidor de acesso remoto. Além disso, um adaptador ISDN deve ser instalado no lugar de um modem no seu computador e no servidor de acesso remoto.

Como funcionam os equipamentos ISDN

A largura de banda de uma linha analógica convencional é de 4 KHz. Numa linha digital ISDN esse valor é de 128 Kbps, o que faz com que o sinal de 4 KHz não exista mais, pois a interface da central de comutação na outra "ponta da linha" não trabalha mais com sinais analógicos. Os circuitos eletrônicos da central telefônica efetuam a equalização e detecção do sinal digital a 128 Kbps transmitido a partir do equipamento do usuário.

Essa técnica de transmissão na linha digital é a conhecida como "Híbrida com Cancelamento de Eco". O equipamento do usuário recebe o fio do telefone proveniente da rede telefônica e disponibiliza duas ou mais saídas: uma para o aparelho telefônico e a outra para a conexão com o computador, geralmente via cabo serial.

Quando o equipamento do usuário é informado pela central telefônica que chegará até ele uma chamada telefônica, ou quando o usuário aciona o aparelho telefônico para realizar uma ligação, automaticamente um dos dois canais utilizados na transmissão à 128 Kbps passa a transmitir os dados à 64 Kbps enquanto o usuário utiliza o telefone para voz, no canal disponibilizado.

Após o término do uso de voz, o canal volta a ser usado para a transmissão de dados à 128 Kbps.

O Usuário pode acessar a internet e falar ao telefone no mesmo instante.

O ISDN é uma espécie de "upgrade" da linha telefônica, que não implica nenhuma alteração nas instalações dos cabos da rede pública no par de fios que chega à casa do usuário. Basta que nas pontas, na central telefônica e na casa do cliente, sejam implantados os equipamentos adequados. O par de fios usado pelas operadoras de comunicação no padrão analógico comporta atualmente apenas um canal de 64 Kbps. Não é à tôa que os modems de 56 kbps, os mais velozes até o momento, atingem menos dessa capacidade.

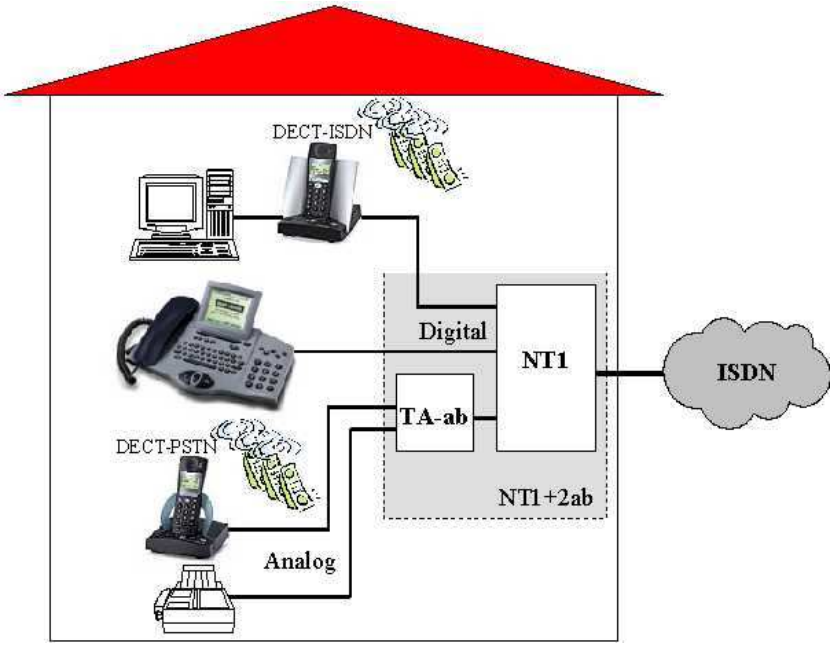
A transmissão via analógica é mais sujeita a interferências e ruídos, que fazem a qualidade cair, o que pode ser sentido na taxa de transferências de quem navega na Internet. Mesmo com 56 kbps, o usuário dificilmente atinge velocidades acima de 45 kbps.

Vantagens

- É a modalidade de acesso por banda larga mais barata do mercado. Na maioria dos casos, a mensalidade é um pouco mais cara do que a de um provedor convencional. Se o problema é dinheiro, trata-se de uma boa pedida.

Desvantagens

- Não deixa de ser acesso discado, ou seja, o usuário continua pagando pelos pulsos telefônicos. Claro que, com velocidades mais altas, você vai fazer mais em menos tempo;
- A velocidade está limitada a 128 kbps. Isso é o equivalente aos planos mais básicos oferecidos nas demais modalidades de acesso por banda larga;
- Além da mensalidade do provedor de acesso ISDN (uma operadora de telefonia), tem mais uma: a do provedor que vai oferecer a infra-estrutura de servidores de correio eletrônico (com suporte), conteúdo para banda larga e outros serviços.



TECNOLOGIA ADSL

ADSL é a sigla para Assymmetric Digital Subscriber Line ou "Linha Digital Assimétrica para Assinante". Trata-se de uma tecnologia que permite a transferência digital de dados em alta velocidade por meio de linhas telefônicas comuns. A cada dia, a tecnologia ADSL ganha novos usuários, tanto é que este é o tipo de conexão à internet em banda larga mais usado no Brasil e um dos mais conhecidos no mundo. Veja a seguir um pouco sobre funcionamento da tecnologia ADSL.

Funcionamento da tecnologia ADSL

A tecnologia ADSL basicamente divide a linha telefônica em três canais virtuais, sendo um para voz, um para download (de velocidade alta) e um para upload (com velocidade média se comparado ao canal de download). É por causa dessas características que o ADSL ganhou o termo "assymmetric" (assimétrica) no nome, pois indica que a tecnologia possui maior velocidade para download e menor velocidade para upload.

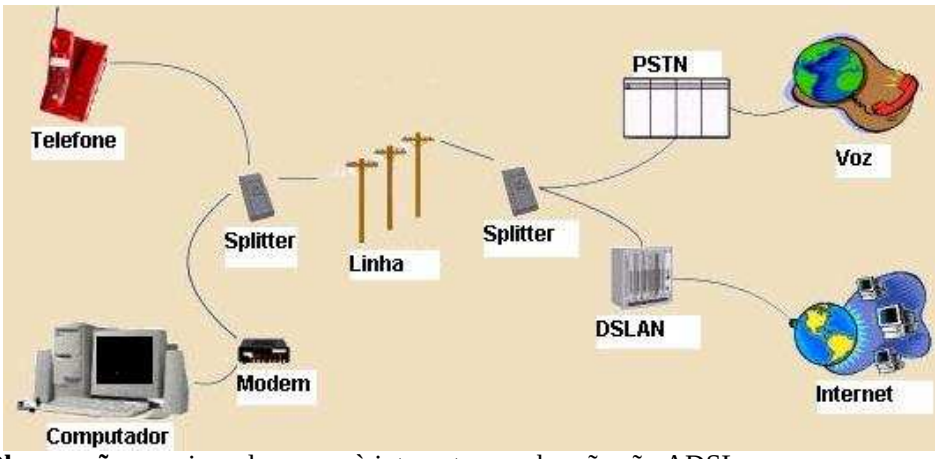
Repare que entre os três canais há um disponível para voz. Isso permite que o usuário fale ao telefone e ao mesmo tempo navegue na internet, ou seja, não é necessário desconectar para falar ao telefone. Para separar voz de dados na linha telefônica, é instalado na linha do usuário um pequeno aparelho chamado Splitter. Nele é conectado um cabo que sai do aparelho telefônico e outro que sai do modem.

Na central telefônica também há uma espécie de Splitter. Assim, quando você realiza uma chamada telefônica (voz), o sinal é encaminhado para a rede de comutação de circuitos da companhia e procede pelo seu caminho habitual. Quando você utiliza a internet, o sinal é encaminhado ao DSLAN.

Quando uma linha telefônica é usada somente para voz, as chamadas utilizam freqüências baixas. Na linha telefônica é possível usar taxas mais altas, mas elas acabam sendo desperdiçadas. Explicando de maneira simples, o que o ADSL faz é aproveitar para a transmissão de dados as freqüências que não são usadas. Como é possível usar mais de uma freqüência ao mesmo tempo na linha telefônica, é então possível usar o telefone para voz e dados ao mesmo tempo.

A tecnologia ADSL funciona instalando-se um modem específico para esse tipo de conexão na residência ou empresa do usuário e fazendo-o se conectar a um equipamento na central telefônica. Neste caso, a linha telefônica serve como "estrada" para a comunicação entre esses dois pontos. Essa comunicação ocorre em freqüências acima de 5000 Hz, não interferindo na comunicação de voz (que funciona entre 300 Hz e 4000 Hz). Como a linha telefônica é usada unicamente como um meio de comunicação entre o modem do usuário e a central telefônica, não é necessário pagar pulsos telefônicos, pois a conexão ocorre por intermédio do modem e não discando para um número específico, como é feito com o acesso à internet via conexão discada. Isso deixa claro que todo o funcionamento do ADSL não se refere à linha telefônica, pois esta é apenas um "caminho", mas sim ao modem. Quando seu modem estabelece uma conexão com o modem da central telefônica, o sinal vai para um roteador, em seguida para o provedor e finalmente para a internet. É importante frisar que é possível que este sinal saia diretamente do roteador para a internet. No Brasil, o uso de provedor é obrigatório por regras da Anatel (Agência Nacional de Telecomunicações).

Praticamente todas as empresas que fornecem ADSL só o fazem se o local do usuário não estiver a mais de 5 Km da central telefônica. Quanto mais longe estiver, menos velocidade o usuário pode ter e a conexão pode sofrer instabilidades ocasionais. Isso se deve ao ruído (interferência) que ocorre entre um ponto e outro. Quanto maior essa distância, maior é a taxa de ruído. Para que haja uma conexão aceitável é utilizado o limite de 5 Km. Acima disso pode ser possível, mas inviável o uso de ADSL.



Observação: serviços de acesso à internet por cabo não são ADSL.

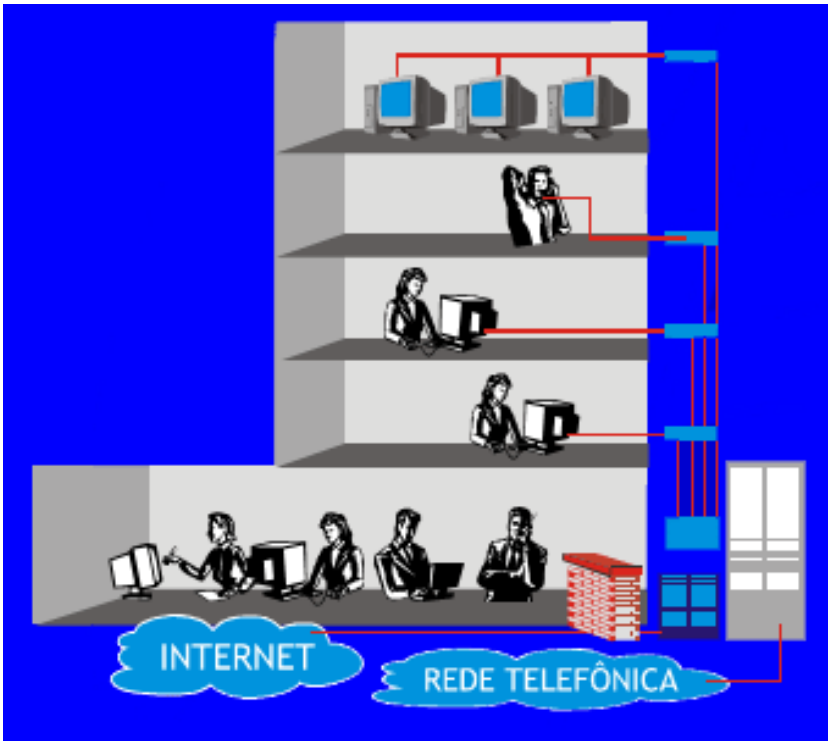
- Velox (Telemar)
- Speedy (Telefônica)
- Turbonet MAXX (GVT)
- Turbo (Brasil Telecom)
- NetSuper (CTBC)

Prova: 25/09/2007
Conteúdo: Até esta página da apostila.

Cabeamento Estruturado

- **Componentes Ativos**: São os equipamentos eletrônicos que permitem a transmissão de dados entre eles.

- **Componentes Passivos**: É o meio físico pelo qual os dados são transmitidos, compostos por cabos, tubulações e os componentes de conexão.



Descrição de um Cabeamento Estruturado

Muitos projetistas de rede dão grande importância a decisões como a marca do sistema operacional de rede que deverá ser usado ou o tipo de hardware de servidor a ser adquirido. No entanto, em muitas estações, a seleção do cabo é a principal etapa do projeto da rede. Decisões finais sobre o software e hardware a serem usados no computador podem esperar, mas o tipo de cabo que a rede deverá ter representa a primeira providência que os arquitetos e a equipe de instalação deverão tomar.

Sugerimos que você leve em consideração os seguintes fatores ao se decidir pelo uso de um determinado cabo:

- Qual a necessidade atual em termos de velocidade de sinalização? Do que as aplicações precisam?
- Você pode prever a necessidade futura de velocidade de sinalização?
- Pretende utilizar gráficos de alta velocidade?
- Terá que obedecer a códigos de engenharia e de proteção contra incêndio? Você tem espaço para conduites de cabo? Deverá levar em considerção questões arquitetônicas? Há restrições locais quanto à utilização de determinados materiais?

Quando souber tudo isso, tomas as seguintes decisões:

- Vai querer usar cabos de cobre ou de fibra óptica? Os nós estão muito distantes ums dos outros? Qual é a verba de que dispões? Trata-se de uma unidade central ou de lóbulo de um nó da rede local (entrelaçamento na rede)?
- O que mais se adequa à sua rede? Cabos de pares trançados ou cabos coaxiais? Você já investiu em algum desses tipos de cabo?
- Se você optar por cabos de pares trançados, o que irá preferir: com ou sem blindagem (STP ou UTP)? O seu ambiente elétrico necessita de cabos blindados?
- Cada uma dessas decisões o leva a uma determinada área de padrões e especificações.
- O Sistema de Cabeamento de rede é tão forte quanto a sua ligação mais fraca. Em geral, a ligação mais fraca de um sistema de cabeamento é o

cabo de estação, que liga o computador à tomada da parede. Uma instalação de cabeamento de primeira classe merece conectores de alta qualidade. Caso contrário, esse excelente sistema funcionará tão mal quanto um sistema de terceira classe – ou pior ainda. Em um sistema de cabeamento estruturado, a ligação entre o gabinete de fiação e o nó da rede é feita normalmente por um fio de par trançado sem blindagem, apesar de você também poder usar um cabo de fibra óptica.

Um projeto de cabeamento estruturado deve seguir as normas EIA/TIA

A principal vantagem do **EIA/TIA** está em sua publicação como um padrão aberto que não contém a marca de qualquer fornecedor, ou seja, você pode escolher um cabo que obedece a uma categoria específica deste padrão que terá várias opções de fornecedores.

Em uma rede utilizando cabeamento estruturado é necessário que a mesma apresente características flexíveis, principalmente no que diz respeito às mudanças diversas que ocorrem freqüentemente com qualquer rede local e também suporte as inovações tecnológicas à que as redes locais estão sujeitas.

Entende-se por rede interna estruturada aquela que é projetada de modo a prover uma infra-estrutura que permita evolução e flexibilidade para serviços de telecomunicações, sejam de voz, dados, imagens, sonorização, controle de iluminação, sensores de fumaça, controle de acesso, sistema de segurança, controles ambientais (ar-condicionado e ventilação).

Deve-se considerar também a quantidade e complexidade destes sistemas, é imprescindível a implementação de um sistema que satisfaça às necessidades iniciais e futuras em telecomunicações e que garanta a possibilidade de reconfiguração ou mudanças imediatas, sem a necessidade de obras civis adicionais.

Um sistema de cabeamento estruturado consiste de um conjunto de produtos de conectividade empregado de acordo com regras específicas de engenharia cujas características principais são:

- Arquitetura aberta

- Meio de transmissão e disposição física padronizados
- Aderência a padrões internacionais
- Projeto e instalação sistematizados

Esse sistema integra diversos meios de transmissão (cabos metálicos, fibra óptica, rádio etc...) que suportam múltiplas aplicações incluindo voz, vídeo, dados, sinalização e controle. O conjunto de especificações garante uma implantação modular com capacidade de expansão programada. Os produtos utilizados asseguram conectividade máxima para os dispositivos existentes e preparam a infra-estrutura para as tecnologias emergentes. A topologia empregada facilita os diagnósticos e manutenções.

Assim, um sistema de cabeamento estruturado (SCS - Structured Cabling Systems) é uma concepção de engenharia fundamental na integração de aplicações distintas tais como voz, dados, vídeo e o sistema de gerenciamento predial (BMS - Building Management Systems).

Ao planejar a organização dos cabos lembre-se das seguintes regras:

- Nunca instale cabos de dados de cobre em posições paralelas a fios elétricos de 120 volts em distância inferiores a 2 ou 2,5 centímetros. Mantenha os cabos de dados a pelo menos um metro de distância das linhas de voltagens mais altas.

- Mantenha cada cabo de cobre o mais longe possível de fontes elétricas de ruídos, inclusive luzes fluorescentes, motores, relés de elevador, transmissores de rádio, transmissores de microondas para alarmes anti-roubo e qualquer outra coisa que consuma energia.

- Utilize um percurso o mais reto possível ao instalar os cabos.

- Em caso de teto falso, utilize prendedores de cabo (ganchos, presilhas) para impedir seu contato direto com teto.

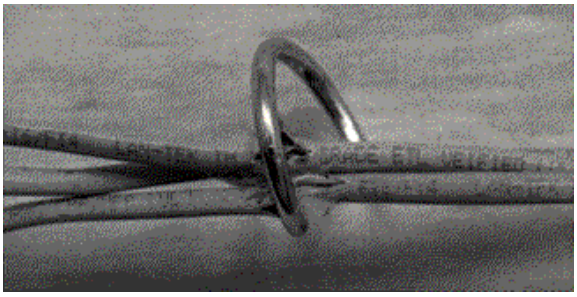
- Não instale fios UTP dentro do mesmo trecho de cabo de fios de telefone (voz). O sistema de voz causará interferência e diafonia, que adulteram o sistema de dados.

- Da mesma forma, mantenha os fios que transportam dados e os que transportam vozes em diferentes blocos perfurados.

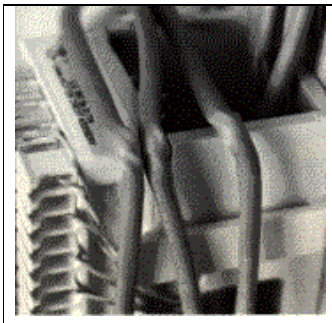
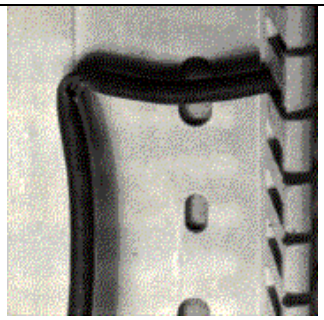
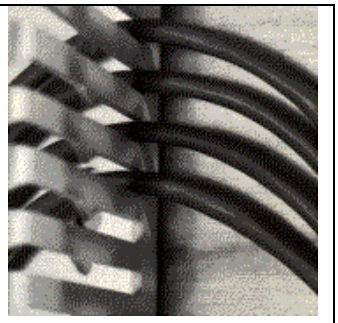
- Retire o mínimo possível da cobertura externa do cabo. Se você retirar a cobertura externa principalmente nas partes em que os fios entram em conduítes, os condutores poderão ficar próximos demais uns dos outros, gerando diafonia.

- Preliminarmente à passagem dos cabos, deve ser feita uma numeração provisória com fita adesiva nas duas extremidades para identificação durante a montagem.

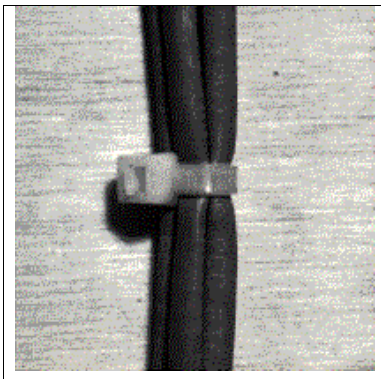
- Durante o lançamento do cabo não deverá ser aplicada força de tração excessiva. Para um cabo UTP categoria 5e, o máximo esforço admissível deverá ser o que equivale ao peso de uma massa de 10 Kg. Um esforço excessivo poderá prejudicar o desempenho do cabo.



- O raio de curvatura admissível de um cabo UTP categoria 5e deverá ser de, no mínimo, quatro vezes o seu diâmetro externo ou 30 mm

		
Incorreto	**Incorreto**	**correto**

- Os cabos não devem ser apertados. No caso de utilização de cintas plásticas ou barbantes parafinados para o enfaixamento dos cabos, não deve haver compressão excessiva que deforme a capa externa ou tranças internas. Pregos ou grampos não devem ser utilizados para fixação. A melhor alternativa para a montagem e acabamento do conjunto é a utilização de faixas ou fitas com velcro.

		
Incorreto	**Incorreto**	**Correto**

- Caso encontre alguma empresa que não disponha de paredes ou tetos com facilidade para instalação de conduítes ou teto falso, pode-se utilizar “Canais de superfície” que abrigam os cabos em dutos externos de metal.

Na figura abaixo apresentamos a ilustração de uma rede local típica, que possui os seguintes elementos pertencentes ao sistema de cabeamento estruturado:

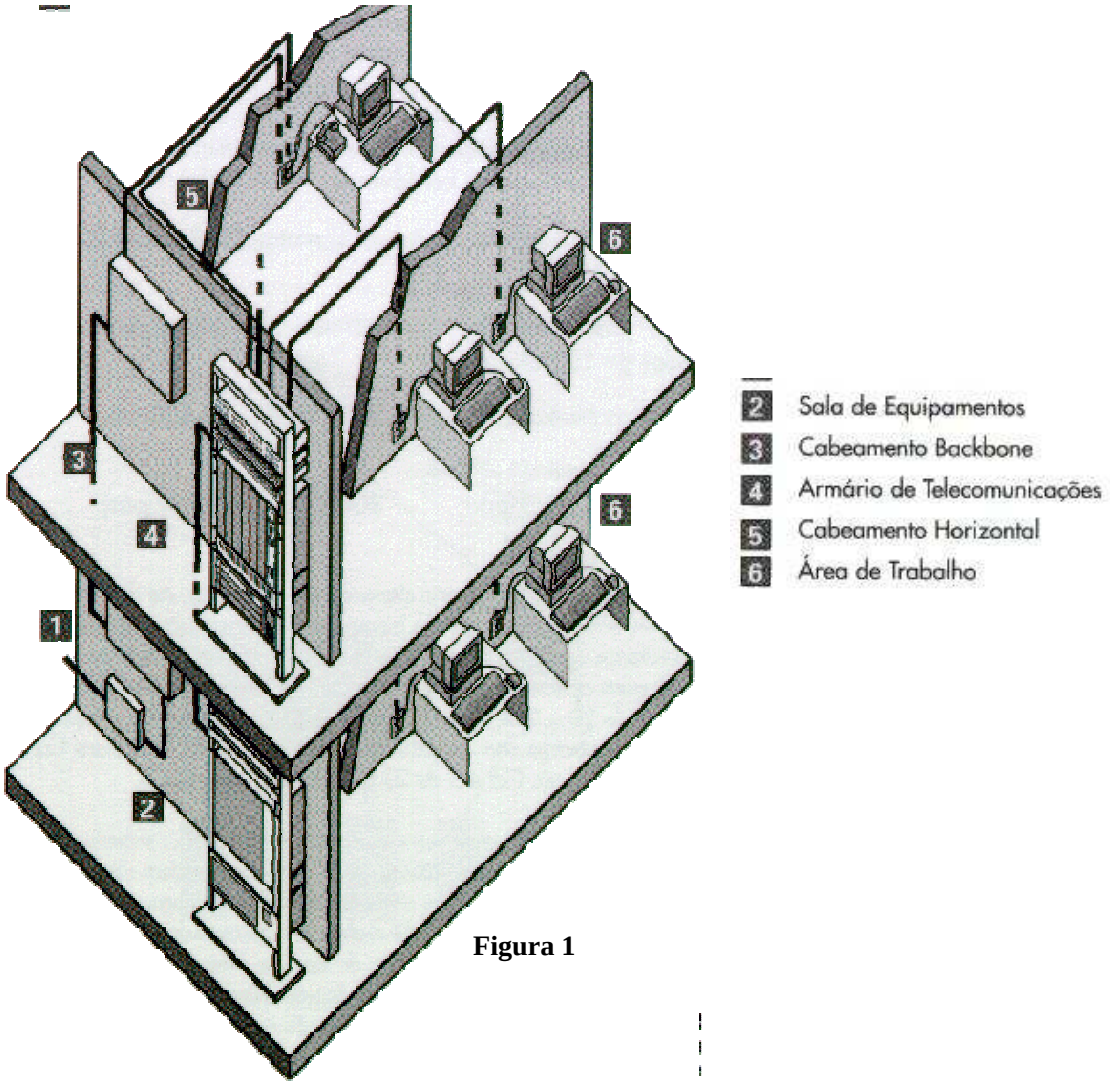


Figura 1

Figura 1 - Estrutura de uma Rede Local típica

2) Sala de Equipamentos - Funções:

- Receber os cabos do backbone (nós) das redes de outras salas (andares).
- Acomodar equipamentos de comunicação das operadoras de Telecomunicações;
- Acomodar os equipamentos principais e outros componentes da rede local;
- Permitir acomodação e livre circulação do pessoal de manutenção;
- Restringir o acesso a pessoas autorizadas.

2.1 Características Técnicas:

- Localização próxima ao centro geográfico do prédio e de utilização exclusiva;
- Dimensões mínimas: 3,00 m x 4,00 m ou 12 m^2;
- Livre de infiltração de água;
- Ambiente com porta e de acesso restrito;
- Temperatura entre 18 e 24°C com umidade relativa entre 30% e 55%;
- Uma boa iluminação com sistema elétrico independente;
- Piso composto de material anti-estático;
- Alimentação elétrica com circuitos dedicados direto do distribuidor principal com instalação de quadro de proteção no local;
- Mínimo de 3 tomadas elétricas.

3) Cabeamento Tronco - Funções:

O cabeamento tronco, também denominado cabeamento vertical ou cabeamento do backbone da rede local, deverá ser interligado à Sala de Equipamento, núcleo da rede, através de um cabo exclusivo. Não é recomendável utilizar mais do que um nível hierárquico de interconexão entre todo o sistema.

3.1) Cabeamento tronco ou Cabeamento vertical - meios de transmissão:

O cabeamento tronco será constituído por um dos seguintes meios de transmissão: **Cabo de fibra óptica ou Cabo UTP**.

3.2) Distâncias – Padrão TIA/EIA

A distância máxima do cabeamento vertical é dependente do meio de transmissão, da aplicação e dos comprimentos totais empregados no sistema de distribuição horizontal (cabos, cabos de manobra, etc..). Os valores a seguir são adotados para preservar os investimentos e garantir desempenho satisfatório nas diversas modalidades:

cabo UTP → distância máxima de 90 metros;

fibra óptica → distância máxima de 220 metros;

4) Armários de Telecomunicações (AT) - Funções:

A função primária dos Armários de Telecomunicações (wiring closets – armários da fiação) é servir como um centro de telecomunicações, isto é, a terminação dos cabos do sistema de distribuição horizontal. É considerado o ponto de transição do cabeamento tronco e o horizontal.

Eles diferem das Salas de Equipamentos pela quantidade e localização, pois são geralmente áreas (salas ou simplesmente estruturas de armários) que servem a um pavimento ou a regiões de um andar em uma edificação.

A existência de um ou mais Armários de Telecomunicações em um determinado pavimento deve-se ao fato de que os cabos no sistema de distribuição horizontal apresentam restrições na distância máxima.

A técnica de conexão adotada isto é, a maneira como serão interligados os componentes ativos e passivos, será a da interconexão, ou seja, os cabos terminados em um painel de conexão (patch panel) serão interligados diretamente aos equipamentos por um cabo de manobra (patch cord).

4.1 Características Técnicas:

Existem duas alternativas sugeridas para a criação desses Armários de Telecomunicações: sala de utilização exclusiva ou gabinetes.

4.1.1) Salas

Caso seja definido um local para desempenhar essas funções, esta área deve possuir as seguintes características:

- Localização central à área potencialmente atendida, respeitando a restrição de distância inferior a 90 metros da área de trabalho;
- Temperatura: 10 a 35°C.
- Mínimo de 3 tomadas elétricas;
- Ambiente com porta e acesso restrito;
- Uma boa iluminação;
- Dentro da sala, os equipamentos e acessórios de cabeamento devem ser instalados preferencialmente em racks do tipo aberto (open racks).
- Livre de infiltração de água.

4.1.2) Armários Externos

Em caso de falta de espaço e a reformulação de locais para a criação de Armários de Telecomunicações seria onerosa, uma alternativa econômica é a modelagem destes Armários em estruturas modulares geralmente conhecidos como gabinetes ou racks.

5) Cabeamento horizontal - Funções:

O cabeamento horizontal interliga os equipamentos de redes, elementos ativos, às Áreas de Trabalho onde estão as estações. Assim como no cabeamento tronco, utiliza-se uma topologia em estrela, isto é, cada ponto de telecomunicações localizado na Área de Trabalho será interligado a um único cabo dedicado até um painel de conexão instalado no Armário de Telecomunicações.

5.1)Cabeamento horizontal - Meios de transmissão:

O cabeamento horizontal poderá ser constituído por um dos seguintes meios de transmissão :

- **cabo UTP**
- **cabo de fibra óptica**

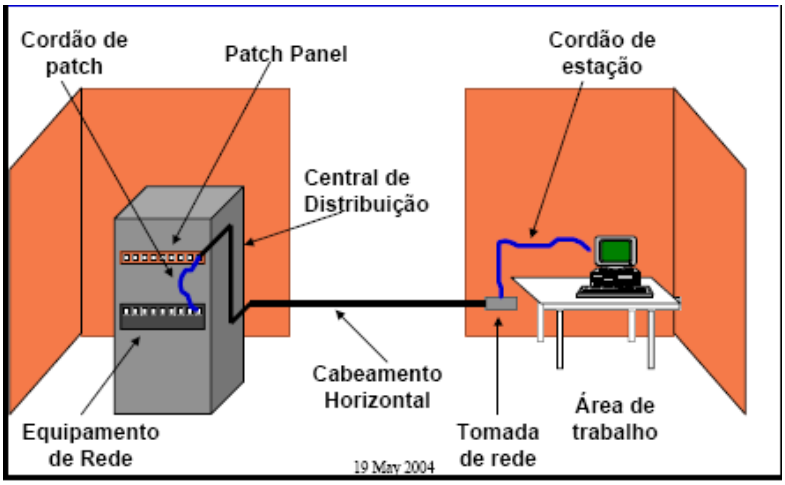
Como a maior parcela dos custos de instalação de uma rede local corresponde ao sistema de cabeamento horizontal, e o mesmo deverá suportar uma larga faixa de aplicações, recomenda-se o emprego de materiais de excelente qualidade e de desempenho superior (categoria 6 ou 7).

5.2 Cabeamento horizontal - Distâncias:

O comprimento máximo de um segmento horizontal, isto é, a distância entre o equipamento eletrônico instalado no Armário de Telecomunicações e a estação de trabalho é de 100 metros. As normas TIA/EIA e ISO definem as distâncias máximas do cabeamento horizontal independente do meio físico. considerando duas parcelas desse subsistema:

O comprimento máximo de um cabo horizontal será de 90 metros. Essa distância deve ser medida do ponto de conexão mecânica no Armário de Telecomunicações, centro de distribuição dos cabos, até o ponto de telecomunicações na Área de Trabalho;

Os 10 metros de comprimento restantes são permitidos para os cabos de estação, cabos de manobra e cabos do equipamento.



Componentes de um sistema de cabeamento horizontal

5.3) Cabo de Manobra (patch cord)

Também conhecido como patch cord, consiste de um cordão de cabo UTP categoria 5e (enhanced) composto de fios ultra-flexíveis (fios retorcidos)

com plugs RJ45 nas extremidades. Sua função é interligar dois painéis de conexão ou um painel e um equipamento facilitando as manobras de manutenção ou de alterações de configuração. A distância máxima prevista para um cabo de manobra é de 10 metros.

5.4) Painel de Conexão

Patch Panels são painéis de conexão utilizados para a manobra de interligação entre os pontos da rede e os equipamentos concentradores da rede. É constituído de um painel frontal, onde estão localizados os conectores RJ-45 fêmea e de uma parte traseira onde estão localizados os conectores que interligarão os cabos de par trançado que chegam dos pontos da rede. Os cabos denominados patch cables fazem a ligação entre o concentrador e o painel (Patch Panel).

Também chamado de patch panel, deverá ser composto pelo agrupamento de 24 tomadas RJ45 na dimensão de 1 UA (unidade de altura).

O patch panel é um painel intermediário de distribuição de cabos que fica entre os pontos de conexão de equipamentos e o hub. Esse painel distribuidor concentra os cabos que vêm dos pontos de rede com ou sem equipamentos e do patch-panel saem os cabos para conexão ao switch.

Quando colocamos uma nova estação (novo nó de rede) num ponto ainda não utilizado, basta conectarmos essa posição do patch-panel ao switch, sem a necessidade de passar um novo cabo do local da nova estação. Ou seja, os cabos são instalados em todos os pontos que possam ter estações e deixados no patch-panel, e poderão ser ligados ao switch quando necessário.

A ligação dos blocos de distribuição citados aos hubs ou switches se dá através de patch cords. **A utilização de Patch Panels confere melhor organização, maior flexibilidade e consequentemente, facilita a manutenção**.

5.5) Cabo UTP

Cabo de par-trançado com 4 pares, constituído por fios sólidos. A especificação mínima de desempenho para esse cabo deverá ser compatível com a TIA/EIA, Categoria 5e (enhanced). Para instalações novas, recomenda-se a utilização de cabos Categoria 6 ou 7. Conforme exposto, o comprimento

máximo permitido para cabos UTP é de 90 metros. Adotou-se como padrão a capa externa do cabo na cor azul.

2.7 Área de Trabalho (ATR)

A Área de Trabalho para as redes locais é onde se localizam as estações de trabalho, os aparelhos telefônicos e qualquer outro dispositivo de telecomunicações operado pelo usuário. Para efeito de dimensionamento, são instalados no mínimo dois pontos de telecomunicações em uma área de 10 m2.

É fundamental que um projeto criterioso avalie detalhadamente cada local de instalação dos pontos, pois problemas de subdimensionamento podem onerar as expansões. Já em alguns casos será preciso substituir a infra-estrutura projetada.

Como o comprimento máximo dos cabos na área de trabalho é de 3 metros o correto posicionamento dos pontos de telecomunicações deve ser avaliado. Deve-se procurar posicionar os pontos em locais distribuídos dentro da área de alcance dos cabos de estação.

Quando não existir vários pontos de telecomunicações distribuídos na Área de Trabalho, as mudanças no posicionamento destes pontos ocorrerão com maior freqüência. Para isso, deve-se procurar inicialmente instalar os pontos nos locais mais afastados do encaminhamento principal do prédio (eletrocalhas nos corredores); assim, será relativamente fácil alterar esse posicionamento, pois não será necessária a passagem de novo cabo horizontal.

O cabeamento na Área de Trabalho pode variar com a aplicação. Assim, adaptações que possam ser necessárias nesses locais deverão obrigatoriamente ser providas por dispositivos externos ao ponto de telecomunicações. Alguns desses produtos são:

Normas para Cabeamento Interno:

O cabeamento horizontal (subrede) deverá ser implementado seguindo as seguintes normas

Meio físico de transmissão (em conformidade com o padrão EIA 568A categoria 5e):

Cabo par-trançado não blindado (UTP-unshielded twisted pair): cabo constituído por fios metálicos trançados aos pares com 4 pares de fios bitola 24 AWG a impedância de 100 ohms.

O comprimento máximo de cada segmento de cabo deverá ser inferior a 90 metros. Essa distância deve ser medida do ponto de conexão mecânica no armário de telecomunicações, centro de distribuição dos cabos, até o ponto de telecomunicações na área de trabalho. Os 10 metros de comprimento restantes, segundo a norma EIA568A, são reservados para os cabos de estação, cabos de manobra e cabos do equipamento.

Cabo de manobra

Conhecido como patch cord, consiste de um cordão de cabo UTP categoria 5e (enhanced) composto de fios ultra flexíveis (fios retorcidos) com conectores RJ45 nas extremidades. Sua função é interligar o painel de conexão ao equipamento de distribuição de rede, facilitando as manobras de manutenção ou de alterações de configuração. A montagem dos pinos deve obedecer à codificação de pinagem T568-A. O comprimento máximo previsto para um cabo de manobra é de 6 metros.

Painel de conexão - patch panel

Composto pelo agrupamento de 12, 24 ou 48 tomadas RJ45 na dimensão de 1 UA (unidade de altura) para instalação em gabinetes de 19 polegadas; a montagem dos pinos deverá obedecer à codificação de pinagem T568 A . As tomadas instaladas no painel deverão atender à especificação dos procedimentos de teste da TIA/EIA 568 A.

Ponto de telecomunicação (PTR)

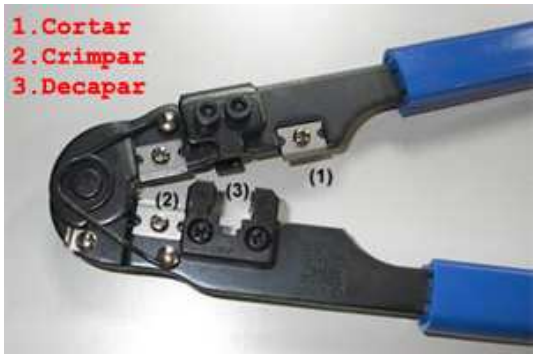
O ponto de telecomunicação (ponto de estação) contitui-se de 1 tomada RJ45/8 fêmea; a montagem dos pinos deverá obedecer à codificação de pinagem T568 A. Recomenda-se que seja integrada a esse subsistema, uma caixa de superfície de 4 x 2 polegadas.

Cabo de estação

Consiste de um cordão de cabo com características elétricas idênticas ao cabo UTP categoria 5e, composto de fios ultra-flexíveis (fios retorcidos) com plugs RJ45 nas extremidades, projetado para interligar a estação até o ponto de telecomunicação. A montagem dos pinos deve obedecer à codificação T568-A; a distância máxima prevista para um cabo de estação é de 3 metros.

Alicate de crimpagem

Alicate de crimpagem é usado para prender as pontas do cabo UTP aos conectores RJ-45. Estes, por sua vez, são conectados à placa de rede do computador ou ao hub.



Quando queremos montar um cabo para interligar dois computadores, não precisamos utilizar dispositivos como hubs, já que pode-se ligar uma máquina à outra diretamente. Neste caso, o cabo do tipo "**crossover**" (cruzado ou invertido) deve ser utilizado.

Por outro lado, quando três ou mais computadores devem ser interligados, um equipamento como o hub se mostra ideal. Neste caso, é necessário criar um cabo para cada computador e conectá-los ao hub. No entanto, o cabo tipo crossover não serve a esse propósito, devendo ser utilizado o cabo do tipo "direto", também conhecido como "patch cable".

Em resumo, para ligar computador a computador, usa-se cabo **crossover**. Para ligar computador a hub, usa-se cabo **direto**. A diferença entre eles é que o cabo crossover tem a disposição de seus fios de maneira diferente em uma ponta em relação à outra, enquanto que o cabo direto tem a disposição dos fios iguais em cada extremidade.

OBS.: o cabo crossover também deve ser usado quando é necessário conectar um hub a outro.

Cuidados necessários ao conectorizar um cabo:

- É importante encaixar o conector RJ-45, tomando-se o cuidado de fazer com que cada fio entre no orifício correspondente. Para isso, segure o conector firmemente em uma mão e a ponta do cabo na outra. Insira os fios vagarosamente, certificando-se de que nenhum ficou pelo caminho. Se ao atingir o final do conector você notar que algum fio tem alguma diferença de tamanho ou está mais atrás em relação aos outros, refaça o procedimento. Os fios devem ter o mesmo tamanho e todos devem chegar ao final dos orifícios do conector.
- É muito importante que o revestimento do cabo também entre no conector. Do contrário, será mais fácil ocorrer o rompimento dos fios. Não exagerar na força ao crimpar o conector.
- Se você notar algum problema após crimpar o cabo, não será possível tirar o conector. A saída é cortar o cabo nesse ponto e repetir todos os passos.

Tabela de combinação dos fios condutores

Ordem no conector	Norma EIA/TIA 568 A	Norma EIA/TIA 568 B
1	Branco com verde	Branco com laranja
2	Verde	Laranja
3	Branco com laranja	Branco com verde
4	Azul	Azul
5	Branco com Azul	Branco com Azul
6	Laranja	Verde
7	Branco com Marrom	Branco com marrom
8	Marrom	Marrom

Norma EIA/TIA 568 A

Norma EIA/TIA 568 B

Passos para criação de um cabo direto

1) **Desencapar as extremidades do cabo:** de posse do alicate e de cabo devemos desencapar a extremidade do cabo em um comprimento máximo de 2 cm, tomando o cuidado de não cortar os fios condutores. Para evitar isto, deve-se inserir o cabo no orifício específico do alicate. Assim podemos retirar a capa protetora sem o risco de danificar os fios condutores.
2) **Organizar os fios**: Após retirar a capa protetora devemos desenrolar os fios e organizá-los na ordem correta da norma que vamos utilizar, que no caso será: BV, V, BL, A, BA, L, BM, M;
3) **Cortar as pontas de cada fio:** Depois de organizados os fios, devemos cortar as pontas de cada fio para que fiquem alinhados, de maneira que possam ser inseridas uniformemente nos conectores. Para fazer isto, devemos utilizar o alicate de crimpagem com a lâmina específica.
4) **Inserir os 08 fios no conector:** devemos inserir os 8 fios no conector RJ-45 de forma que todas as pontas estejam encostando no final do conector.
5) **Pressionar o conector com o alicate de crimpagem:** uma vez que os fios estejam bem inseridos e alinhados nos conectores, devemos inserir o conector na posição apropriada do alicate de crimpagem e pressionar bem.
6) **Crimpar a outra ponta:** feito todos estes passos, a primeira ponta do nosso cabo está pronta. Para confeccionar a outra ponta devemos repetir os passos anteriores.

Cabo cross-over

Cabo cross-over é semelhante fisicamente ao cabo UTP, sendo que possui as mesmas características. O processo de confecção do cabo, que deverá ser diferente, ou seja, uma ponta deve ser do padrão A e outra do padrão B.

Padrão A Conector (X)	Padrão B Conector (Y)	Legenda	Cor dos fios
1 BV	1BL	BV	Branco com verde
2 V	2 L	V	Verde
3 BL	3 BV	BL	Branco com laranja
4 A	4 A	A	Azul
5 BA	5 BA	BA	Branco com azul
6 L	6 V	L	Laranja
7 BM	7 BM	BM	Branco com marron
8 M	8 M	M	Marron

LAN Tecnologias de Frame

As tecnologias de frame são baseadas na utilização de “quadros” para a transmissão das mensagens. Quando se usa o termo “quadro” ou “frame” , estamos mencionando um protocolo na camada 2 do modelo OSI.

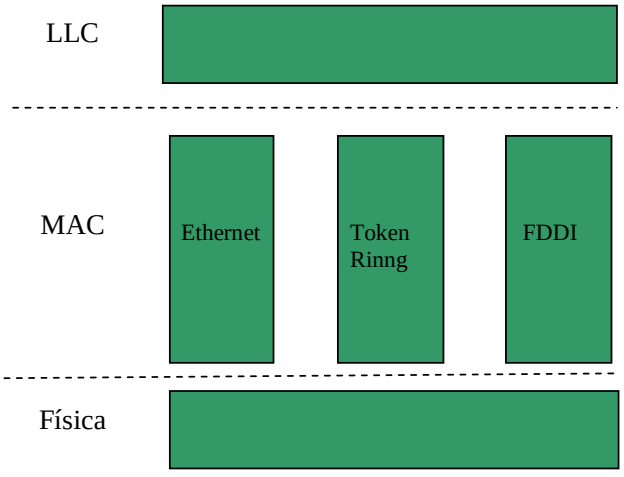
Camada de Enlace (camada 2 do modelo OSI):

- ❖ Entende os dados no formato de bits transformado pela camada física.
- ❖ Já entende o endereço físico (endereço único em cada placa de rede.)
- ❖ Trata as topologias de rede
- ❖ Dispositivos: switch, placa de rede
- ❖ Recebe os dados em formato de bits e os converte de maneira inteligível, os transforma em unidade de dados, subtrai o endereço físico e encaminha para a camada de rede que continua o processo.
- ❖ PDU → formato → quadro

A camada 2 do modelo OSI, como já citamos, é subdividida em duas camadas:

LLC: realiza o controle lógico da conexão, como controle de erros e de fluxo;

MAC: realiza o controle de acesso ao meio. Essa subcamada realiza a comunicação direta com a placa adaptadora da rede e a camada física.



A camada MAC, como é dependente do meio, possui especificação diferente para cada tecnologia. A figura acima apresentou as subcamadas enlace.

Esses protocolos foram especificados pelo IEEE, em 1980, na norma 802.x, criando padrões que especificam as topologias, tecnologias e protocolos do nível MAC, visto que a subcamada LLC é compartilhada por todos os padrões.

A norma 802.x definiu os seguintes padrões de frame para redes locais:

802.3 (Ethernet) → mais utilizado no mundo

802.4 (token bus) → não vingou

802.5 (token ring) → utilizadas em redes baseadas em produtos IBM.

802.6 (FDDI) → Exclusivo para uso com fibras ópticas.

Esse padrão definiu a tecnologia de Frame que atualmente é a mais utilizada em todo o mundo: “o Ethernet”.

As principais tecnologias de Frame são:

- **Ethernet**
- **Token Ring**
- **FDDI**

O padrão 802.3 é especificado em duas topologias:

Barramento: a partir da utilização de um cabo coaxial que permite que todas as estações compartilhem o meio.

Estrela: nessa topologia é necessário utilizar um equipamento de concentração como um hub ou switch para criar uma topologia em estrela. As estações são então conectadas ao equipamento de concentração pelos cabos UTP, respeitando a distância limite da norma de 100 metros.

No barramento, as estações enviam e recebem sinais diretamente do cabo. O cabo utilizado nessa topologia pode ser tanto coaxial fino, o Thinnet, um cabo mais simples, porém que limita a distância máxima de 185 metros, como o Thicknet, um cabo coaxial grosso com blindagem dupla que alcança distância de até 500 metros.

Endereçamento MAC

Nos frames estão os endereços MAC que são únicos para cada placa de rede e dispositivo e compostos por 6 bytes ou 48 bits. Os primeiros identificam o fabricante da placa de rede. Esses endereços são utilizados para identificar tanto a origem do frame (MAC origem) como o destino (MAC destino). As informações são utilizadas para que o frame seja retirado do barramento pela estação que contenha o endereço MAC destino. Como o frame contem o endereço MAC de origem, a estação sabe para quem deve responder.

Método de acesso ao meio

O método de acesso ao meio utilizado em redes Ethernet é o CSMA/CD (Carrier Sense Multiple Access / Carrier Detect). Traduzindo este nome complicado “Método de Acesso Múltiplo com Verificação de Portadora e Detecção de Colisão”. Embora o nome seja complicado, método de funcionamento é relativamente simples. Quando uma estação deseja transmitir no meio, a primeira ação que a estação deve fazer é ouvir o meio, mas o que significa isso? Bem, ouvir o meio é verificar o sinal de portadora do barramento. Se não houver sinal de portadora no barramento, quer dizer que não existe nenhuma estação utilizando o meio naquele momento, portanto a estação pode transmitir.

Enquanto uma estação está transmitindo no meio, as outras estações não transmitem, aguardando o cabo ficar livre. Isso ocorre pelo mesmo procedimento que descrevemos no parágrafo anterior. Como existe portadora no barramento, quer dizer que está ocorrendo uma transmissão. Por causa disso as outras estações aguardam o final da transmissão para utilizarem o meio.

Esse processo parece ser ideal, entretanto nada é perfeito. Imagine um caso em que duas estações desejam transmitir na rede um determinado instante, e nesse instante não existe portadora no cabo, portanto o cabo está livre para a transmissão. De acordo com o padrão, o que ocorre? Acontece um problema muito sério, as duas estações vão tentar enviar seus quadros no meio ao mesmo tempo, gerando um fenômeno conhecido como “COLISÃO”.

Quando a colisão ocorre, uma estação “suja” o que a outra estava transmitindo. Como o meio é compartilhado, os sinais se misturam, gerando uma informação sem utilidade nenhuma. O CSMA/CD possui um mecanismo que consegue detectar que ocorreu a colisão. A partir do momento da detecção, é enviado um sinal no meio que termina de sujar o quadro e sinaliza para todas as estações que houve colisão na rede.

O próximo passo é todas as estações interromperem seus processos de transmissão e aguardarem um tempo randômico, que é definido por um algoritmo conhecido como “backoff”, para novamente tentarem transmitir. Esse algoritmo determina o tempo que a estação deve esperar para retransmitir, baseado no número de tentativas que ela já fez para retransmitir o quadro. Quanto maior o número de tentativas, mais tempo a estação irá aguardar. A idéia é simples. Se a estação está tentando mais de uma vez transmitir sem sucesso, é que provavelmente o meio está congestionado e muitas estações estejam tentando transmitir ao mesmo tempo, gerando ainda mais colisões. Assim, a estação recebe um tempo maior para tentar retransmitir, que permite que o meio se descongestione, possibilitando à estação retransmitir a mensagem.

O algoritmo backoff limita o número de tentativas em dez. Se mesmo assim o meio ainda se encontra ocupado, a retransmissão da mensagem é abortada, indicando um erro de transmissão para a aplicação.

Analisando o comportamento da colisão, é fato que quanto mais estações estiverem compartilhando o mesmo meio, mais sujeito esse meio estará a colisões. Isso ocorre porque a probabilidade de duas ou mais estações tentarem transmitir ao mesmo tempo aumenta. Além da quantidade de

estações, as aplicações também afetam diretamente o número de colisões. Aplicações que demandam muito da rede, ou seja, fazem acessos constantes à rede, acabam monopolizando o meio e sendo causa do aumento do número de colisões.

Frame Ethernet

O frame Ethernet é formado pelos seguintes campos devidamente delimitados:

Preâmbulo: Consiste em 8 bits, usado para marcação do sincronismo. Essa marcação é formada pela seqüência de bits 10101010, que garante a sincronização.

Delimitador de início de frame (SFD): é formado pelo byte 101010110 e indica início do frame.

Endereço MAC destino: esse campo possui 6 bytes que correspondem ao endereço MAC da estação destino. Como já citamos, é formado por uma porção que identifica o fabricante da interface de rede e uma porção que identifica a placa. Essa porção na verdade funciona como se um número de série da placa (único para cada placa de rede).

Endereço MAC origem: campo com 6 bytes que identifica o endereço MAC de quem está originando o frame ou da estação transmissora.

Comprimento do campo de dados: esse valor especifica o tamanho total do campo de dados. Lembre-se de que um pacote Ethernet pode transportar de 64 a 1.500 bytes, de acordo com a MTU (maximium transfer unit) configurada. Quadros maiores ou menores que estes limites em geral descartados por equipamentos como switches.

Campo de dados: nesse campo encontramos a informação efetiva que será transmitida. A norma estabelece um tamanho mínimo de 46 bytes, entretanto os fabricantes adotaram o tamanho mínimo de 64 bytes, e o máximo de 1500 bytes. Para o Ethernet, quando existe a necessidade de transmitir ou

receber informações das camadas superiores com mais de 1.500 bytes, faz-se necessária a realização de fragmentação dos quadros de origem e remontagem no destino.

FCS (Frame Check Sequence): essa informação é um código de redundância cíclica utilizado para a verificação de possíveis erros no quadro.

Campos	Bits	Bytes
Preâmbulo	56	7
SFD (delimitador início frame)	8	1
MAC Destino	48	6
MAC Origem	48	6
Tamanho do campo de Dados	**Min**: 8	46
	Max: 12.000	1500
Frame Check Sequence	32	4

O Ethernet evoluiu muito nos últimos anos, principalmente no que diz respeito ao aumento da velocidade de operação, porém respeitando as diretrizes do padrão estabelecido. Assim surgiu inicialmente o Fast Ethernet e recentemente o Gigabit Ethernet.

Fast Ethernet

O Fast Ethernet trabalha com velocidade de 100 Mbps, o qual pode ser considerando um Ethernet acelerado. Nessa tecnologia encontramos switches e hubs. O Fast Ethernet está padronizado e existem interfaces em fibra óptica e em cabos de par trançado (UTP).

Com o rápido crescimento do número de usuários em todo o mundo as redes e também com aumento de aplicativos gráficos, multimídia e sistemas coorporativos, a performance das redes locais com tecnologia Ethernet a 10Mbit/s já não era mais satisfatória. Então existia a necessidade de um outro padrão para atender as necessidades atuais, surgindo o padrão 100 BASE-T de Ethernet a 100Mbit/s que mantém as principais características do padrão Ethernet 10Mbit/s, tais como o formato do frame, a quantidade de dados que

um frame pode carregar, e o mecanismo de controle de acesso ao meio “CSMA/CD”, diferenciando do padrão original apenas na velocidade de transmissão de pacotes, que no padrão 100BASE-T é 10 vezes maior que no original. A Fast Ethernet vem se tornando a tecnologia com melhor custo/ beneficio e economicamente viável de rede de alta velocidade, por ter sido elaborada para integrar-se às redes Ethernet existentes, com mínima ruptura. Fast Ethernet roda a 100 Mbps, pode ser implementada num projeto comutado (e não compartilhado) e os switches da Fast Ethernet são utilizados freqüentemente para criar um backbone de 100 Mbps, que suporta uma combinação de usuários de 10 e 100 Mbps. Sem duvida a Fast Ethernet está se tornando uma das tecnologias mais utilizadas em todo mundo, porque a migração poderá ser feita gradualmente, de acordo com a necessidade de cada setor/usuário. É também a mais econômica, pois poderão ser aproveitadas todas as estruturas de cabeamento existentes na rede atual (desde que a estrutura física antiga não seja implementada em cabo coaxial, para o qual a Fast Ethernet não possui suporte).

Fast Ethernet ainda oferece outras vantagens:

- É compatível com a Ethernet de 10 Mbps;

- Oferece um preço relativamente baixo para 100 Mbps;

- Fornece um caminho de migração eficiente e flexibilidade para as redes Ethernet existentes, através do uso de adaptadores de 10/100 (chamados "autosense");

- É uma tecnologia conhecida pelos usuários atuais da Ethernet, não exigindo, portanto, qualquer treinamento....

Gigabit Ethernet

Já o Gigabit Ethernet traz uma série de inovações, entre elas o funcionamento apenas na topologia de switching, não observamos o fenômeno da colisão. A alta velocidade de interfaces Gigabit o torna incompatível com a utilização de cabos UTP, alcançando com o uso destas distâncias máximas de 25 metros. No caso deste padrão o correto é utilizar fibras ópticas para alcance de até 20Km.

Introdução ao Frame Switching

O que é switch?

É um equipamento de rede que trabalha na mesma camada do modelo OSI do hub, a camada de enlace ou camada 2. Enquanto o hub trabalha apenas como um repetidor de sinais, ou seja, todo o sinal que chega a uma porta é repetido para todas as outras, o switch trabalha de uma maneira mais inteligente. Os frames de uma estação origem são copiados apenas para a porta em que se encontra a estação destino da mensagem, criando em cada porta do switch um domínio de colisão distinto.

O Switch mantém internamente uma tabela na qual ficam armazenados os endereços MAC das estações que estão diretamente ligadas àquela porta. Lembre-se de que, em geral, numa mesma porta switch podem existir várias estações utilizando um hub que está diretamente conectado ao switch. Isso significa que essa tabela pode possuir diversos endereços MAC para a mesma porta.

O funcionamento do switch é relativamente simples. Ele examina o endereço MAC destino do frame e verifica na tabela a porta que corresponde àquele endereço e simplesmente comuta aquele frame para a porta destino.

O Switch cria essa tabela de endereços MAC a partir do MAC origem dos frames que chegam ao switch. Quando um frame originário com um novo MAC chega, é criada uma nova entrada na tabela de endereços MAC do switch.

Bem, daí surge a dúvida crucial. O que ocorre quando o switch é ligado pela primeira vez na rede? Como ele sabe os endereços MAC que correspondem às portas? A resposta é simples: ele não sabe. O switch, quando é iniciado, trabalha como um hub e copia os frames que não conhecem o endereço MAC destino para todas as portas. A partir do momento que estação destino responde, a informação de porta fica armazenada na tabela de

MACs, e da próxima vez que houver um envio de informação para o dado endereço, ela será diretamente encaminhada para a porta correta.

Todo esse processo permite ao switch separar os domínios de colisão. Se antes tínhamos um único barramento com o hub, podemos imaginar agora N barramentos, em que N é o número de portas do switch, interconectados pelo switch. O switch trabalha, portanto, como uma bridge multiportas. Como um hub o switch também regenera o sinal e permite aumentarmos a distância da abrangência da Ethernet. O benefício mais rapidamente sentido quando mudamos de um hub central numa rede para um switch é uma diminuição significativa da quantidade de colisões na rede.

Uma das grandes vantagens do switch é que todo esse processo que já descrevemos de aprendizado das portas ocorre de forma automática. Isso quer dizer que a instalação de um switch é praticamente plug in play, ou seja, desconectam-se os cabos do hub anteriormente instalado, substitui-se pelo switch e a rede já está funcionando. A única preocupação do técnico que for instalar o equipamento é configurar corretamente os endereços da estação de gerência, endereço do switch e verificar se a imagem do software do switch encontra-se na versão mais atualizada.

Existem switches de pequeno porte, os chamados switches departamentais, que geralmente possuem uma quantidade de portas fixas 12, 24 ou 48 e módulos para inserção de cartões com duas ou quatro portas de uplink.

As portas de uplink em geral são utilizadas para a conexão de servidores departamentais ou para conectar os switches departamentais em switches de backbone. Essas portas utilizam uma tecnologia de maior velocidade de forma a não criar um gargalo nelas. Por exemplo, em um switch com 12 portas 10 Mbps Ethernet, em geral a porta uplink é baseada em tecnologia Fast Ethernet a 100 Mbps.

Os switches de backbone, em geral possuem um chassi com muitos slotes. Em cada slot podemos incluir placas de diferentes tecnologias, como Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI e token ring.

Diz-se que um switch de backbone realiza translation bridge quando um frame necessita sofrer adaptação de uma tecnologia para outra. Um exemplo é quando um quadro padrão ethernet precisa ser transformado em uma célula ATM para ser transportado pela porta ATM, ou a origem é uma porta ethernet e o destino é uma porta ATM. O processo de translation bridge ocorre ainda entre as tecnologias:

- Ethernet para FDDI e vice-versa
- Ethernet para token ring e vice-versa
- FDDI para ATM e vice-versa
- Token Ring para ATM e vice-versa
- Token ring para FDDI e vice-versa

Quando não há necessidade de adaptação, como do ethernet para o Fast ethernet, ou mesmo para o Gigabit ethernet, diz-se que o switch executa a função de transparent bridging. Na verdade, toda a comutação que ocorre em um switch baseada na mesma tecnologia nas duas portas também recebe o nome de transparent bridging.

A literatura mais moderna sobre redes recomenda, mesmo com um investimento maior, que as estações estejam ligadas diretamente em uma porta de switch. Com isso garantimos uma performance privilegiada, procurando reduzir ao máximo o nível de colisão da rede. No projeto de uma rede Fast Ethernet, procuramos também conectar as estações a 100 Mbps e estações banda também podem ser ligadas diretamente em uma porta 1 Gbps. Um exemplo é o usuário de aplicação CAD que geralmente trabalha com arquivos muito grandes e precisa de uma performance privilegiada se comparado com usuários comuns da rede.

Congestionamento de Rede

A solução tradicional, simples e barata do uso do hub pode se tornar uma grande dor de cabeça com a adição, sem controle, de outros usuários. Quanto mais usuários existirem num barramento, maior será a competição pelo acesso ao meio. Isso acaba gerando um número excessivo de colisões e uma degradação na performance da rede. Esse processo de degradação é chamado de congestionamento da rede.

O ponto ótimo de uma rede Ethernet em topologia de barramento é alcançado quando temos uma taxa de utilização da rede de 35%. Com esses números e descontando os cabeçalhos dos frames, chegamos a uma taxa líquida de transmissão do meio de 2,5 Mbps. Parece pouco, pois todo o overhead (armazenamento em excesso) significa uma perda de 7,5 Mbps. No caso do Fast Ethernet a situação ainda é pior, pois temos apenas 25 Mbps de banda livre perdendo 75 Mbps. Esses dados correspondem ao caso da adoção de tecnologia de barramento em um mesmo domínio de colisão. No caso de utilização do switch vamos ver que a história muda.

O que muda se não estamos no ponto ótimo? Bem, aí começam os problemas do uso do barramento. Se uma rede já se encontra com uma taxa de utilização acima de 35%, começam a surgir os primeiros problemas de performance, e acima de 60% a rede já está congestionada.

Por que ocorre a colisão?

O Ethernet puro é baseado no uso de um meio compartilhado chamado de barramento, pois as estações escutam o barramento e transmitem apenas quando não há presença de sinais, ou seja, o barramento está livre.

Como todo o evento provado estatisticamente que pode ocorrer, acaba ocorrendo. Existe um determinado instante em que duas estações escutaram que o meio estava livre, e as duas tentaram transmitir no mesmo instante. Nesse momento ocorre a colisão, pois os dados emitidos pelas duas estações se encontram na rede, e literalmente colidem, embaralhando as mensagens transmitidas pelas duas estações, gerando assim, um dado incompreensível.

Quando isso ocorre, a estação que detectou a colisão envia um sinal no meio para que as estações esperem um tempo randômico baseado no número de tentativas de transmissão (algoritmo de backoff) e tentem novamente a colisão.

O problema de possuirmos muitas estações disputando o mesmo meio é que a chance de ocorrer colisão aumenta potencialmente, e quanto maior a taxa de utilização da rede maior a chance da ocorrência de colisão.

Como o switch implementa diversos barramentos, ou seja, cada porta do switch passa a ser considerada um novo barramento, quando substituímos um hub por um switch multiportas, diminuímos a quantidade de colisões. Isso acontece porque com o hub existe um grande domínio de colisão e agora com o switch temos múltiplos domínios de colisões, com um total de colisões significativamente menor do que na adoção do hub. Como as colisões, com um total de colisões geram retransmissões na rede, a performance com o switch tende a aumentar. Com a diminuição das retransmissões sobra mais banda útil para os dados trafegarem. Recomenda-se uma taxa de colisões máxima de 10% como aceitável.

Devemos lembrar sempre dos números mágicos: da taxa máxima de utilização de 35% e de colisão de 10%.

Backbone da rede e Rede Colapsada (collapsed backbone)

Existe uma topologia de rede de switches padrão conhecida como “topologia colapsada”. Imagine, por exemplo, uma empresa localizada em um prédio, em que cada andar seja um departamento.

Os departamentos serão então atendidos por switches departamentais, que, como já falamos antes, possuem 12, 24 ou 48 portas Ethernet ou Fast Ethernet. Na topologia colapsada, os switches departamentais ficam localizados nos andares no shaft do prédio, ou acomodados em um rack num local apropriado.

Caso exista algum servidor de aplicação específico do departamento no andar, ele pode também ser conectado nesse switch usando uma porta pré-configurada a 100 Mbps.

Case 1 – Rede Colapsada Prédio de Dez Andares

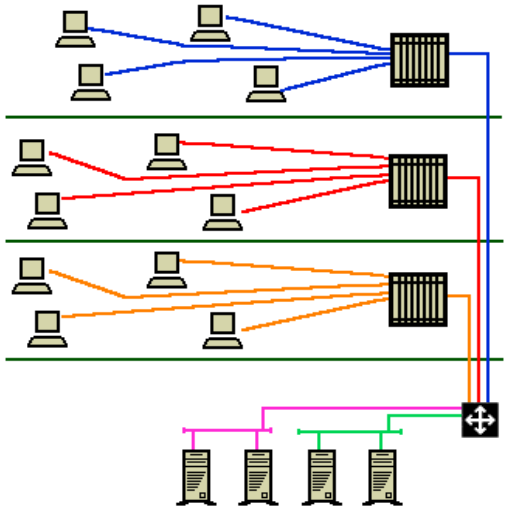
Vamos imaginar um prédio com dez andares, e cada andar com 20 usuários. Teremos, portanto, dez switches departamentais com 24 portas 10/100 cada um, um por andar. Esses switches devem estar conectados ao equipamento central chamado equipamento de backbone.

Esse equipamento de backbone é um switch de alta capacidade da ordem de alguns gigabits/segundo, capaz de dar vazão a todo o tráfego requerido pelos dez switchs departamentais, espalhados nos andares.

A conexão entre o equipamento de central de backbone e os switches departamentais será baseada em fibra óptica utilizando Gigabit Ethernet. Cada switch departamental será configurado com um módulo de uplink com duas portas gigabits. A segunda porta provê redundância no caso de um par de fibras se partir.

Nos switch central ficam conectados os switches departamentais e os servidores corporativos da empresa ligados em Gigabit Ethernet. Esse switch está localizado na sala de equipamentos no térreo do edifício.

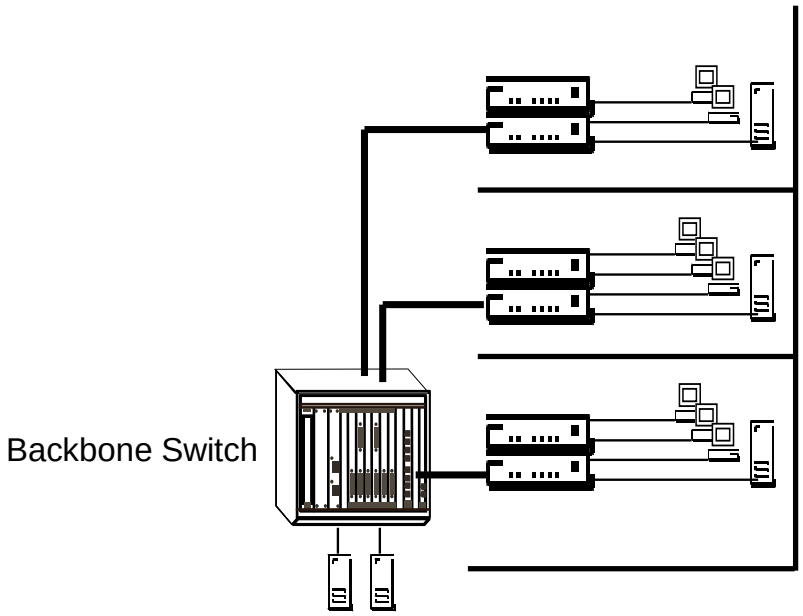
Figura demonstrando o projeto de "backbone colapsado" que acabamos de descrever.



Tipos de switches:

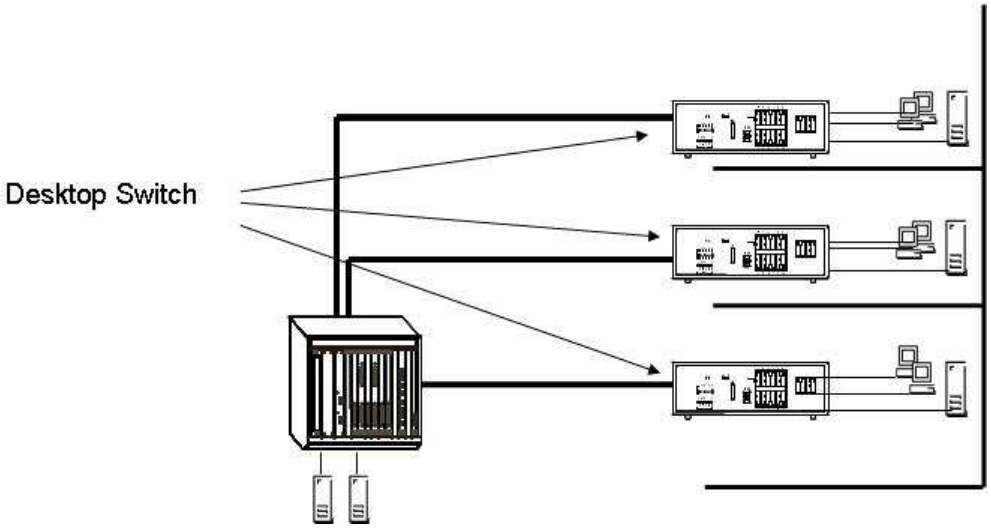
Switch Frame: Classificação

1) Backbone Switch
    - Ligação entre diversas LANs
    - Suporta uma grande quantidade de MACs



2) Workgroup Switch (switch departamental)
    - Ideal para segmentar grupos de trabalho pequenos (até 50 estações)
    - Número reduzido de MACs

3) Desktop Switch



Tecnologias de Switching

1) Tecnologia de comutação (troca)
2) Capacidade de comutação
3) Switches Multicamada
4) Gerenciamento

1. Tecnologia de Comutação:

1.1. Cut-Through
1.2. Store and forward
1.3. Fragment-free (livre de fragmentos)

Existem ainda switchs que são híbridos e têm a capacidade de trabalhar nos dois modos.

O **switch store and Forward** (armazenar e encaminhar) tem uma performance inferior devido principalmente a analisar todo o frame antes de tomar a decisão de comutação. Switches Store-and-Forward guardam cada quadro em um buffer antes de encaminhá-lo para a porta de saída. Enquanto o quadro está no buffer, o switch calcula o CRC e mede o tamanho do quadro. Se o CRC falha, ou o tamanho é muito pequeno ou muito grande (um quadro Ethernet tem de 64 bytes a 1500 bytes) o quadro é descartado. Se estiver tudo OK, o quadro é encaminhado para a porta de saída.

Esse método assegura operações sem erro e aumenta a confiabilidade da rede. Contudo, o tempo gasto para guardar e checar cada quadro adiciona um tempo de latência grande ao processamento dos quadros.

A latência total é proporcional ao tamanho dos pacotes: quanto maior o pacote, maior o delay.

Este tipo de switch é projetado para redes corporativas, onde a checagem de erros é necessária.

O **switch Cut-Through** (corta caminho) foram projetados para reduzir a essa latência. Esses switches minimizam o delay lendo apenas os 6 primeiros bytes de dados do pacote, que contém o endereço de destino, e logo encaminham o pacote.

Contudo, esse switch não detecta pacotes corrompidos causados por colisões, nem erros de CRC. Quanto maior o número de colisões na rede, maior será a largura de banda gasta com o encaminho de pacotes corrompidos. É a tecnologia que apresenta maior performance de comutação.

Switche **cut-through** é melhor utilizado em pequenos grupos de trabalho e pequenos departamentos.

O **Fragment-free** (livre de fragmentos) funciona como um cut-through, mas armazena os primeiros 64 bytes do frame antes de enviá-lo.

O motivo é que a maioria dos erros e todas as colisões acontecem nos 64 bytes iniciais de um frame.

Adaptative Cut-Through os switches que processam frames no modo adaptativo suportam tanto **store-and-forward** quanto **cut-through**. Qualquer dos modos pode ser ativado pelo gerente da rede, ou o switch pode ser inteligente o bastante para escolher entre os dois métodos, baseado no número de quadros com erro passando pelas portas.

Quando o número de quadros corrompidos atinge um certo nível, o switch pode mudar do modo **cut-through** para **store-and-forward**, voltando ao modo anterior quando a rede se normalizar.

2. Capacidade de Comutação

Quanto a capacidade de comutação, um switch pode ser:

2.1. Non Blocking
2.2. Blocking

Um switch é chamado de Non Blocking se tiver a capacidade de comutação em sua matriz de comutação tão rápida que consegue dar vazão ao máximo de quadros Ethernet possível pela velocidade da porta. Em geral, equipamentos Non Blocking não trabalha com buffers na entrada, justamente por terem a capacidade de dar vazão a todo o tráfego de entrada. Esses switches, por trabalharem com componentes de maior desempenho, possuem um custo mais elevado que um switching Blocking.

Vamos calcular a performance mínima para um switch, imaginando um equipamento com capacidade de 16 portas e que todas as portas estejam configuradas na capacidade máxima, ou seja, 200 Mbps (Fast Ethernet full duplex). A matriz de comutação deveria ter “teoricamente” uma performance de 3.2 Gbps para que o switch seja Non Blocking. Na verdade, isso não ocorre porque nunca uma porta Fast Ethernet trabalha com velocidade full. Normalmente a taxa de utilização de uma porta nunca excede os 50%, portanto neste caso uma matriz com performance de 1.6 Gbps já é o suficiente.

Um Switching é chamado de blocking justamente pelo contrário. Ele bloqueia o tráfego utilizando para isso buffers de entrada. O equipamento, na verdade, não consegue dar vazão a todo o tráfego de uma vez, armazenando esse tráfego de entrada do switch em um buffer para depois tratá-lo. Esse processo é conhecido como blocking. Devemos bloquear o frame para depois trata-lo. Esses switches em geral são mais baratos, mas possuem as seguintes limitações:

- Performance limitada;
- Geram congestionamento na rede;
- Podem perder muitos frames caso o buffer não seja suficiente para armazenar todas as informações.

Quando o switch está congestionado, ele pode enviar sinais para que outros switches a ele conectados parem de enviar frames. Esse mecanismo é conhecido como *backpressure* **(contrapressão).** Durante a congestão, um switch, pode simplesmente dropar os pacotes que estão chegando. Isso ocorre porque a capacidade de buffer do switch não é o suficiente para armazenar todo o tráfego que chega, mesmo no caso do congestionamento.

3. Switches Multicamada

Os novos switches do mercado possuem uma capacidade extra. Além de trabalharem na camada 2 do modelo OSI como qualquer switch, também trabalham na camada 3, examinando o pacote IP que está encapsulado no frame Ethernet e tomando decisões de comutação baseadas nessa informação. Esses switches são tambpem chamados de IP switches ou Routing Switches (roteadores) e em geral trabalham de forma muito parecida com um roteador.

Quando um switch multicamadas, além de analisar o endereço IP para tomar a decisão de comutação, analisa a porta TCP do pacote IP encapsulado no frame Ethernet, dizemos que é um switch camada 4.

Quanto à forma de segmentação das sub-redes, podem ser classificados como switches de camada 2 switches de camada 3 ou switches de camada 4.

Switch da camada 2 (enlace) → São os switches tradicionais, que efetivamente funcionam como bridges multi-portas. Sua principal finalidade é de dividir uma LAN em múltiplos domínios de colisão. Estes switch trabalha apenas com o endereço MAC.

Switch da camada 3 (rede – endereçamento) → São os switches que, além das funções tradicionais da camada 2, incorporam algumas funções de roteamento, como por exemplo, a determinação do caminho de repasse baseado em informações de camada de rede, endereço do IP.

Switch da camada 4 (transporte) → Basicamente incorpora às funcionalidades de um switch de camada 3, a habilidade de se implementar a

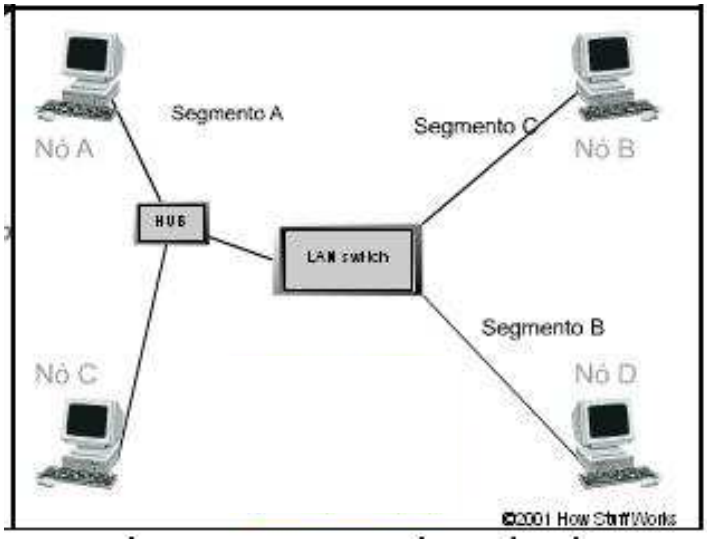
aplicação de políticas e filtros de tráfego a partir de informações de camada 4 ou superiores.

4. Gerenciamento

O gerenciamento é uma ferramenta muito importante para o diagnostico de problemas na rede. Cada switch possui uma MIB (Management Information Base), uma base de dados composta de informações, como o status das portas, taxas de colisão e de utilização, quantidades de pacotes dropados, temperatura do equipamento, entre outras.

Todas essas informações são essenciais para gerenciar a rede de switches. O gerenciamento auxilia de diversas maneiras, sendo uma ferramenta primordial para realizar mudanças na rede, monitorar a performance e tratar problemas antes que se tornem críticos, ocasionando a paralisação da rede. A maioria das corporações, quando projetada e implementa uma rede de switches, inclui também o software de gerenciamento, facilitando a vida do administrador de rede e obtendo como resultado final uma melhor performance da rede.

Funcionamento de um Switch



O switch é adicionado à rede e vários segmentos são ligados às portas do switch.

Um computador (nó A) no primeiro segmento (segmento A) envia dados para um computador (nó B) em outro segmento (segmento C).

O switch pega o primeiro pacote de dados do nó A, seu endereço MAC (endereço MAC origem) e o salva na lista de endereços do segmento A. O switch agora sabe onde achar o nó A toda vez que um pacote de dados for endereçado para ele. Este processo é chamado de aprendizado **(learning).**

Já que o switch não sabe onde está o nó B, ele envia o pacote para todos os segmentos, com exceção do segmento A. O processo de enviar um pacote para todos os segmentos para encontrar um nó específico é conhecido como enchente **(flooding)**.

O nó B pega o pacote e envia-o novamente para o nó A para avisá-lo que o pacote foi recebido.

O pacote do nó B chega ao switch. Agora o switch pode adicionar o endereço MAC do nó B à lista de endereços do segmento C. Como o switch já sabe o endereço do nó A, ele envia o pacote diretamente para ele. O nó A está num segmento diferente do nó B, por isso o switch deve conectar os dois segmentos para enviar o pacote. Isto é conhecido como encaminhamento **(forwarding).**

Um novo pacote do nó A para o nó B chega ao switch. O switch agora sabe onde está o nó B, então direciona o pacote diretamente para o nó B.

O nó C envia informação para que o switch localize o nó A. O switch consulta o endereço MAC do nó C e o adiciona à lista de endereços do segmento A. O switch já sabe o endereço do nó A e entende que os 2 nós estão no mesmo segmento. Então, ele não precisa conectar o segmento A a outro segmento para que os dados viajem do nó C para o nó A. Portanto, o switch vai ignorar os pacotes que viajam entres nós de um mesmo segmento. Isto é a filtragem (**filtering**).

Os processos de **learning** e **flooding** continuam até que todos os nós estejam armazenados nas listas de endereços. A maioria dos switches tem muita memória disponível para administrar estas listas de endereços.

Entretanto, para otimizar o uso da memória, eles removem informações antigas para que o switch não perca tempo com endereços obsoletos. Para fazer isso, eles utilizam uma técnica chamada envelhecimento (**aging**). Quando uma nova informação é adicionada à lista de endereços, o switch atribui uma data e hora ao endereço. Toda vez que um pacote é enviado para um nó, a data e a hora são atualizadas. O switch tem um timer configurável que apaga o endereço depois de um certo tempo de inatividade daquele nó, que libera a memória para a inclusão de outros endereços. Como você pode ver, uma ponte transparente é uma maneira fácil e prática de adicionar e gerenciar todas as informações que um switch precisa para realizar o seu trabalho.

No nosso exemplo, 2 nós estávamos no segmento A, enquanto o switch criava segmentos independentes para os nós B e D. Em uma rede comutada ideal, cada nó deve ter o seu próprio segmento. Isto eliminaria a possibilidade de colisões e também a necessidade da filtragem.

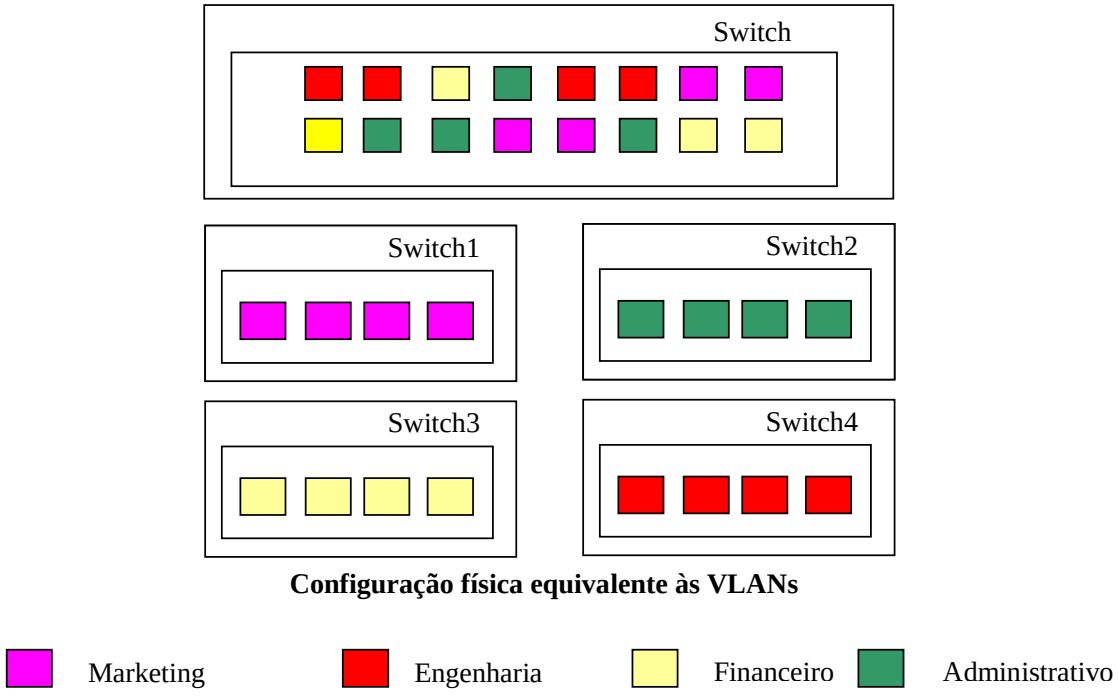
Broadcast

Este termo costuma ser traduzido como "radio difusão", apesar de atualmente este termo ter ganho novos significados. Um sinal de broadcast é irradiado para uma grande área geográfica, um bom exemplo são os sinais de TV. Numa rede de computadores, um sinal de broadcast é um aviso enviado simultaneamente para todos os micros da rede. Existem vários exemplos de sinais de broadcast, como por exemplo, os avisos de colisões de pacotes enviados pelas placas.

VLAN – Virtual Lan

As VLANs ou virtuais LANs nada mais são do que redes virtuais. Que é rede Virtual?

É uma rede local logicamente conectada, podendo ser criada em um único switch ou entre vários switches. Imagine um switch com 16 portas. Suponha agora que possuímos a capacidade de criar quatro switches virtuais no mesmo equipamento. Teríamos, portanto, quatro switches completamente independentes. Fisicamente seria um único equipamento, porém logicamente a solução pode ser exagerada como quatro switches lógicos.



Configuração física equivalente às VLANs

Qual o objetivo de criarmos VLANs? Elas são a resposta a uma série de necessidades em uma rede baseada em switches. Inicialmente as VLANs resolvem um problema que também existia em uma rede com hubs e só era resolvido com o uso de roteadores, o tráfego de broadcoast.

Um quadro de broadcoast , por sua própria funcionalidade, quando chega em um switch, deve ser copiado para todas as portas de um switch. No caso que um switch esteja conectado com outro, o mesmo procedimento vai se propagar, ou seja, o quadro de broadcast será recebido em uma das portas e replicados em todas as portas do segundo switch. Esse procedimento faz com que a rede de switches comporte-se como uma única LAN e esteja sujeita a que todos os pacotes de broadcast trafeguem e sejam enviados para todas as estações.

Quando a rede é pequena, não existem maiores problemas com o tráfego de broadcast, entretanto, quando a rede é grande e a quantidade de quadros de broadcast também é grande, esse processo impacta consideravelmente a performance da rede, causando um fenômeno que os administradores chamam de “tempestades de broadcast”. Os efeitos desse fenômeno é o aumento da taxa de utilização da rede e do tempo de resposta e diminuição da performance da rede.

Outra vantagem de separarmos as redes em VLANs é a segurança. Podemos limitar apenas as máquinas dos usuários à VLAN de seu departamento. Por exemplo, uma empresa que possua as seguintes VLANs: Marketing, Engenharia, Financeiro e Administração. Como os usuários do marketing estão na VLAN do marketing, não conseguem acessar as máquinas que estejam nas VLANs da Engenharia, do Financeiro e da administração e vice-versa.

Esta tecnologia ajuda, portanto, a aumentar a segurança da rede, isolando logicamente os usuários de sub-redes. Lembre-se de que a maior preocupação do administrador de segurança não é com os hackers que vêm pela Internet e sim com os hackers internos.

Normalmente podem ser criadas 1024 VLANs, más este número varia de Switch para Switch.

Vantagens:

- Ganho de velocidade
- Segurança
- Organização lógica das informações

Mais um pouquinho de Vlan

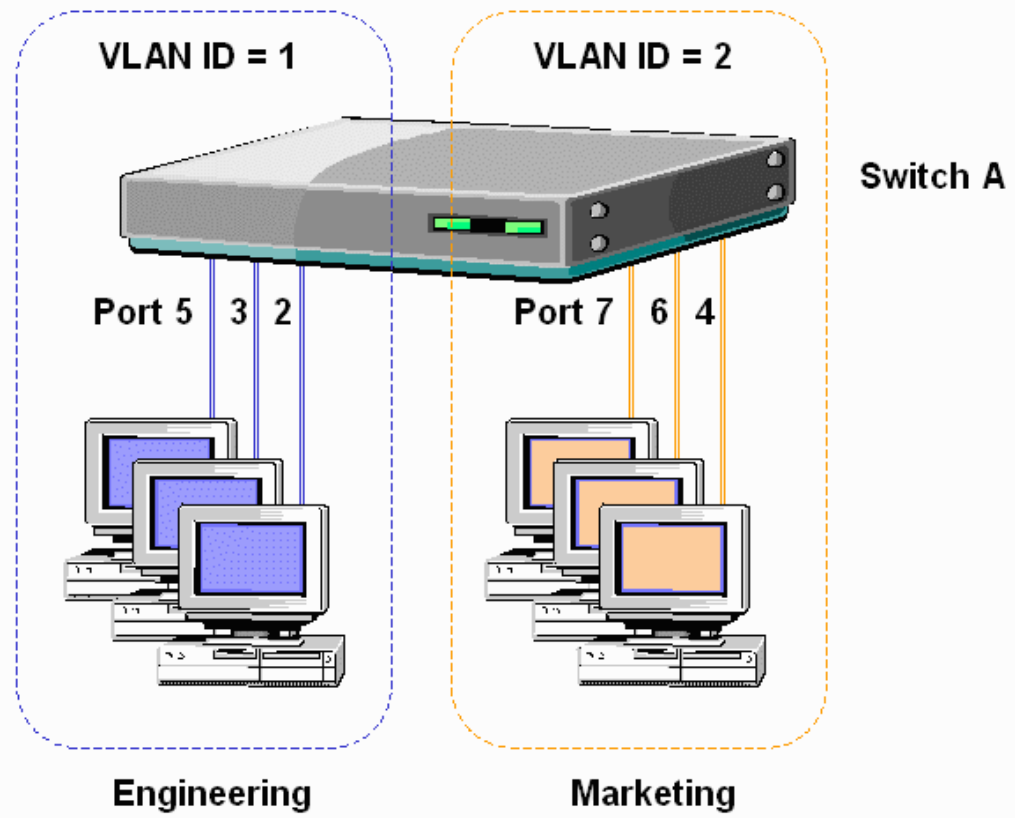
Em uma topologia onde existe apenas switches ethernet nível 2 ou em um segmento que contenha muitas portas, este é conhecido como topologia de rede simples.

Nela, possuímos apenas um domínio de broadcast. Isso significa que, todos os dispositivos conectados aos swicths, receberão os pacotes de broadcast.

Isso em uma rede com poucos dispositivos, não é problema, mas quando aumentamos a quantidade de dispositivos conectados, passa a ser um grande problema.

Para solucionar esse problema, foi criada a técnica conhecida como VLAN. Ela é utilizada na segmentação de redes. O termo VLAN (Virtual LAN) refere-se a criação de LANs virtuais em um mesmo equipamento ou pilha de equipamentos de rede.

Com isso pacotes de broadcast só são recebidos pelos dispositivos pertencentes a uma determinada VLAN.


VLAN ID = 1
VLAN ID = 2
Switch A
Port 5
3
2
Port 7
6
4
Engineering
Marketing

As Vlans podem ser Estáticas ou Dinâmicas.

VLAN Estáticas

Estas são baseadas em portas, ou seja, você diz que qualquer dispositivo que se conecte a uma determinada porta do swicth pertence a uma determinada VLAN.

VLAN Dinâmicas

Estas são baseadas em endereços **MAC**. O administrador da rede, deve previamente cadastrar os endereços MAC das estações e associar os mesmos a suas respectivas VLANS. Com isso, quando o usuário logar seu micro na rede, independente da porta, ele será alocado para a Vlan correta.

Tipos de VLANs

Quanto a forma de identificação dos seus membros, as redes locais virtuais podem ser classificadas em:

VLANs baseadas em:

- **Portas: camada 1**

Os membros de uma VLAN podem ser definidos de acordo com as portas da ponte/comutador utilizado. Por exemplo, em um comutador com dez portas, as portas 1, 2, 3 e 8 pertencem a VLAN 0. Já as portas 4, 9 e 10 fazem parte da VLAN 1. As demais pertencem a VLAN 2, como visto na figura 1

Portas	1	2	3	4	5	6	7	8	9	10
VLAN	0	0	0	1	2	2	2	0	1	1

Figura 1 - Associação de portas a diferentes VLANs

Este método vem sendo o mais utilizado na implementação de VLANs, pois sua configuração é rápida e simples.

Caso um usuário se mova para um local diferente, fora da ponte/comutador onde estava conectado, o administrador da rede deve reconfigurar a VLAN. Esta é a principal desvantagem deste método.

Além disso, deve se ressaltar que ao conectar um repetidor, um hub ou outro comutador a uma porta pertencente a uma VLAN, todos as estações conectadas e este dispositivo se tornaram membros desta VLAN.

Endereço MAC (Media Access Control): camada 2

Neste caso os membros da rede virtual são identificados pelo endereço MAC (Media Access Control) da estação de trabalho. O comutador reconhece o endereço MAC pertencente a cada VLAN. A associação entre endereços MAC e VLANS é exemplificado na figura 2

Endereço MAC	1212389145121	5043834758445	6673573385843
VLAN	0	1	1

Figura 2 - Associação de endereços MAC a diferentes VLANs

Quando uma estação de trabalho é movida, não é necessário reconfigurá-la para que esta continue pertencendo a mesma VLAN, já que o endereço MAC faz parte da sua placa de interface de rede. Isto é uma vantagem em relação as VLANs baseadas em portas, onde a tabela de membros tem de ser reconfigurada.

O grande problema deste método é que um membro de uma VLAN deve ser inicialmente especificado, obrigatoriamente. Em redes com milhares de usuários isto não é uma tarefa simples.

Protocolo: camada 2

Os membros de uma VLAN camada 2 também podem ser identificados de acordo com o campo "tipo de protocolo" encontrado no cabeçalho da camada 2, como visto na figura 3.

Protocolo	IP	IPX	NetBios
VLAN	0	0	1

Figura 3 - Associação de protocolos a diferentes VLANs

Endereço IP (Internet Protocol): camada 3

Neste método os membros pertencentes a uma VLAN são determinados pelo cabeçalho da camada 3. O endereço IP pode ser usado nesta classificação.

Endereço IP	146.164.69.2	146.164.69.28	146.164.69.10
VLAN	1	0	1

Figura 4 - Associação de endereço IP a diferentes VLANs

Embora um membro seja identificado por uma informação da camada 3, este processo não é realizado pelo roteador e também não há nenhuma relação com o roteamento nesta rede. Neste método, o endereço IP é usado somente como um mapeamento para determinar os usuários de uma VLAN.

Em VLANs camada 3, os usuários podem mover suas estações de trabalho sem reconfigurar os seus endereços de rede. O único problema é que geralmente o tempo para o encaminhamento de pacotes usando informações da camada 3 é maior do que utilizando o endereço MAC.

Diferenças entre Hub, Switch e Roteador

Muita gente sabe que hub, switch e roteador são nomes dados a equipamentos que possibilitam a conexão de computadores em redes. Porém, dessas pessoas, muitas não sabem exatamente a diferença entre esses dispositivos. O texto abaixo explicará o que cada equipamento faz e indicará quando usar cada um.

Hub

hub é um dispositivo que tem a função de interligar os computadores de uma rede local. Sua forma de trabalho é a mais simples se comparado ao switch e ao roteador: o hub recebe dados vindos de um computador e os transmite às outras máquinas. No momento em que isso ocorre, nenhum outro computador consegue enviar sinal. Sua liberação acontece após o sinal anterior ter sido completamente distribuído.

Em um hub é possível ter várias portas, ou seja, entradas para conectar o cabo de rede de cada computador. Geralmente, há aparelhos com 8, 16, 24 e 32 portas. A quantidade varia de acordo com o modelo e o fabricante do equipamento.

Caso o cabo de uma máquina seja desconectado ou apresente algum defeito, a rede não deixa de funcionar, pois é o hub que a "sustenta". Também é possível adicionar um outro hub ao já existente. Por exemplo, nos casos em que um hub tem 8 portas e outro com igual quantidade de entradas foi adquirido para a mesma rede. Para interligar estes Hubs utiliza-se cabo cross-over.

Hubs são adequados para redes pequenas e/ou domésticas. Havendo poucos computadores é muito pouco provável que surja algum problema de desempenho.

Switch

O switch é um aparelho muito semelhante ao hub, mas tem uma grande diferença: os dados vindos do computador de origem somente são repassados ao computador de destino. Isso porque os switchs criam uma espécie de canal de comunicação exclusiva entre a origem e o destino. Dessa forma, a rede não fica "presa" a um único computador no envio de informações. Isso aumenta o desempenho da rede já que a comunicação está sempre disponível, exceto

quando dois ou mais computadores tentam enviar dados simultaneamente à mesma máquina. Essa característica também diminui a ocorrência de erros (colisões de pacotes, por exemplo).

Assim como no hub, é possível ter várias portas em um switch e a quantidade varia da mesma forma.

O hub está cada vez mais em desuso. Isso porque existe um dispositivo chamado "hub switch" que possui preço parecido com o de um hub convencional. Trata-se de um tipo de switch econômico, geralmente usado para redes com até 24 computadores. Para redes maiores, mas que não necessitam de um roteador, os switchs são mais indicados.

Roteadores

O roteador (ou router) é um equipamento utilizado em redes de maior porte. Ele é mais "inteligente" que o switch, pois além de poder fazer a mesma função deste, também tem a capacidade de escolher a melhor rota que um determinado pacote de dados deve seguir para chegar em seu destino. É como se a rede fosse uma cidade grande e o roteador escolhesse os caminhos mais curtos e menos congestionados. Daí o nome de roteador.
Existem basicamente dois tipos de roteadores:

Estáticos: este tipo é mais barato e é focado em escolher sempre o menor caminho para os dados, sem considerar se aquele caminho tem ou não congestionamento;

Dinâmicos: este é mais sofisticado (e conseqüentemente mais caro) e considera se há ou não congestionamento na rede. Ele trabalha para fazer o caminho mais rápido, mesmo que seja o caminho mais longo. De nada adianta utilizar o menor caminho se esse estiver congestionado. Muitos dos roteadores dinâmicos são capazes de fazer compressão de dados para elevar a taxa de transferência.

Os roteadores são capazes de interligar várias redes e geralmente trabalham em conjunto com hubs e switchs.