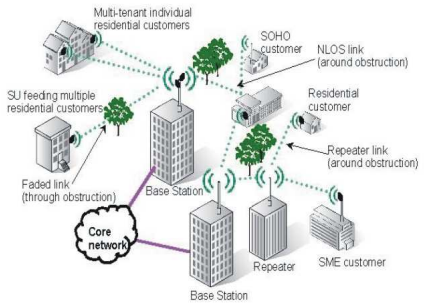
Rede de computadores

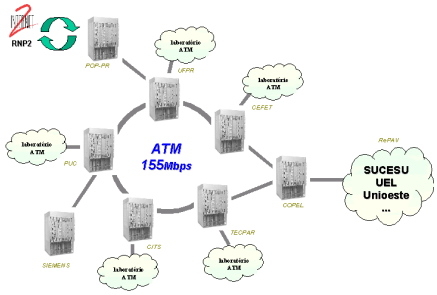
LAN: Local Area Newtork.É um grupo de computadores e dispositivos associados que dividem uma mesma linha de comunicação e, normalmente, os recursos de um único processador ou servidor em uma pequena área geográfica.

O servidor normalmente tem aplicação e armazenamentos de dados compartilhados por vários usuários, em diferentes computadores, ou seja, é o que chamamos de uma Rede Local (computadores próximos, altas taxas de transmissão dados 10Mbps a um Gbps, meios de transmissão privativos).

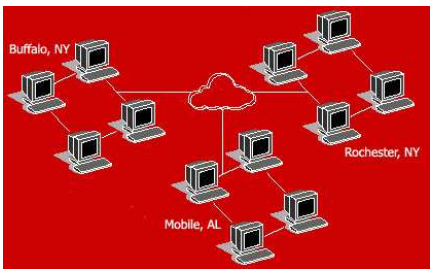
Um servidor de rede local pode ser até mesmo utilizado como servidor Web desde que tomem as medidas adotadas de seguranças para proteger as aplicações internas e os dados de acesso externo.



MAN:Metropolitan Area Newtork.É uma Rede Metropolitana, esta interconecta usuários com os recursos de computadores, com uma área maior de cobertura, apesar de que ser uma grande rede local, porém menor que a cobertura por uma WAN.Este aplicativo é usado para interconexão de várias redes em uma cidade dentro de uma única grande rede.



WAN:Wide Area Newtork.É uma Rede Geográfica com uma estrutura mais ampla de telecomunicação de uma LAN.



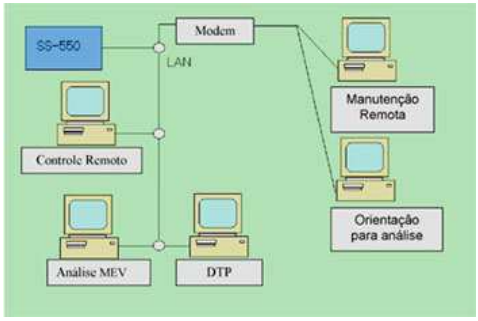
Redes Sem Fio (Wireless): As tecnologias de redes sem fio abrangem desde redes de dados e voz globais, que permitem que os usuários constituam conexões sem fio por longas distâncias, até tecnologias de freqüências de rádio e luz infravermelha, que são otimizadas para conexões sem fio de curta distância.

Entre os dispositivos utilizados com freqüência nas redes sem fio estão computadores portáteis, computadores de mesa, computadores bolso, assistentes digitais pessoais (PDAs), telefones celulares, computadores com caneta e pagers.

As tecnologias sem fio atende a várias demandas práticas, como por exemplo: os usuários de celulares podem usar seus aparelhos para acessar e-mails, os viajantes com computadores portáteis podem conectar-se à Internet através de estações base instaladas em aeroportos, estações ferroviárias e outros locais públicos; outro exemplo é o usuário através do seu computador de mesa poder conectar dispositivos para sincronizar dados e transferir arquivos.

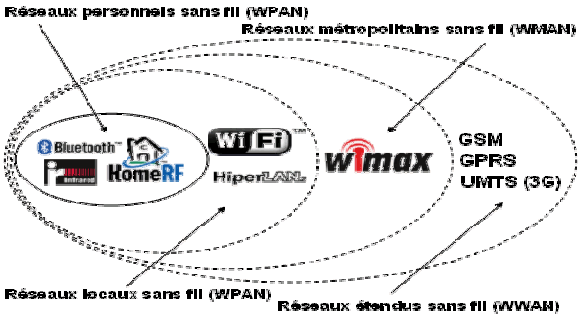
Enfim, assim como as redes tradicionais, as redes sem fio pode ser classificadas em diferentes tipos, com base nas distâncias por meio das quais os dados podem ser transmitidos.

WWAN: Rede de Longa distância: As tecnologias WWAN permitem que os usuários constituam conexões sem fio em redes remotas, privadas ou públicas.Estas conexões podem mantidas por meio de grandes extensões geográficas, como cidades ou países, através do uso de sites com várias antenas ou sistema de satélites sustentados por provedores de serviço sem fio.



As tecnologias WWAN atualmente são conhecidas como sistemas de segunda geração (2G), os principais sistemas 2G incluem o sistema global para comunicações móveis (GSM), os dados digitais de pacotes de celular (CDPD) e o acesso múltiplo de divisão de código (CDMA).Estão sendo analisadas para fazer a transição de redes 2G, algumas das quais apresentam recursos móveis limitados e incompatíveis entre si, para as tecnologias de terceira geração (3G) que acompanharão um padrão global e fornecerão recursos móveis mundiais.

WMAN:Rede sem fio metropolitanas, possibilitam que os usuários estabeleçam conexões sem fio entre vários locais em uma área metropolitana, sem custo elevado derivado da instalação de cabos de cobres ou de fibras e da concessão de linhas.Além do mais, as WMANs podem funcionar como backups das redes que utilizam cabos, caso as principais linhas destinatário dessas redes não estejam disponíveis. Portanto, as WMANs utiliza ondas de rádio ou luz infravermelha para transmitir dados.



WLAN: Redes sem fio locais permitem que os usuários constituam conexões sem fio em uma área local , esta pode ser usada em escritórios temporários ou em outros espaços em que a instalação extensiva de cabos teria um custo mais elevado, ou caso contrário para complementar um LAN existente de modo que os usuários possam trabalhar em diferentes locais e diferentes horários.

Estas podem funcionar de duas maneiras distintas: estação sem fio conectando-se a pontos de acessos sem fio, que trabalham como pontes entre as estações e o backbone de rede existente ou ponto a ponto (ad hoc), na qual 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.

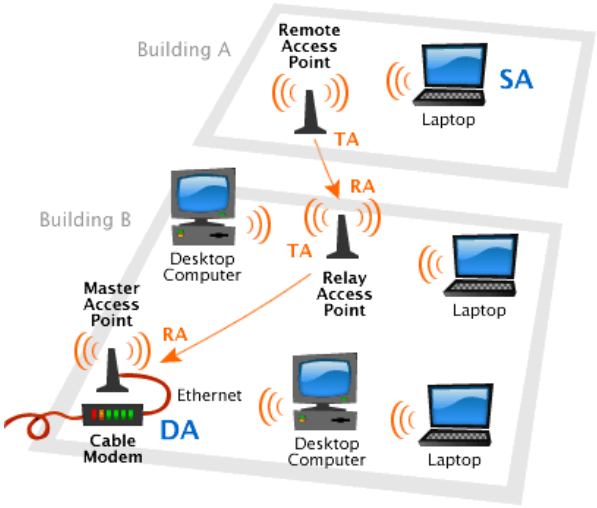
WPAN: Permitem que os usuários estabeleçam comunicações ad hoc sem fio, mas para isto é preciso ter dispositivos (telefone celulares ou laptops) que são utilizados em um espaço operacional pessoal (POS).Um POS é o espaço que cerca uma pessoa, até a distância de dez metros.

As duas principais tecnologias WPAN são: Bluetooth e a luz infravermelha. A Bluetooth é uma tecnologia de substituição de cabos, que usa ondas de rádio para transmitir dados a uma distância de dez metros.

Wi-Fi é o nome mais comum para as redes locais wireless, ou W-LAN 802,11b, esta trabalha em freqüência livre, a partir de 2,4GHz, oferece uma velocidade de acesso muito maior do que a de redes 3G. Enquanto na 3G a velocidade média de transmissão é de 384 Kbps (pico de 2Mbps), em Wi-Fi a taxa média varia entre 512 Kbps e 2Mbps (pico de 11 Mbps), dependendo de quantas pessoas estão naquele momento no raio de alcance do hotspot, como são chamados os pontos de conexão.

Por outro lado, as redes Wi-Fi não oferecem a mesma mobilidade que as celulares, pois tem finalidades diferentes dizem as operadoras.O fato é que este tipo de rede está se propagando rapidamente, segundo estimativas do Gartner Group, o número de usuários de WLAN na América do Norte deve chegar os 31 milhões em 2007.No Brasil a operadora que saiu na frente foi a Oi, com uma parceria com a rede de hotéis Accor.

Quanto à questão de segurança: se não houver criptografia e codificação, é possível que alguém com um notebook e cartão de acesso à rede Wi-Fi penetrar na rede.A seqüência de codificação é frágil e nem todos os dispositivos suportam chaves criptográficas de 128 bits.Outra limitação quanto à questão de segurança é a troca periódica de senhas, procedimentos padrão para a confiabilidade.

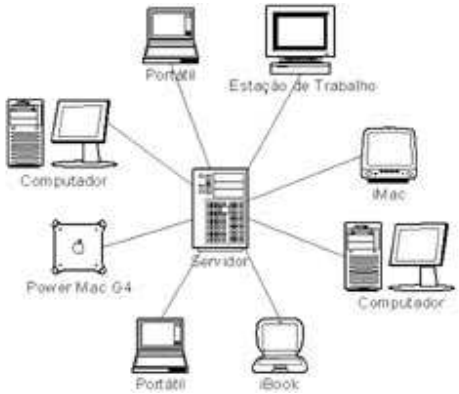


A troca de senhas das máquinas cadastradas no Acess Point (AP), dispositivo para comunicação com os cartões dos notebooks, não podem ser feita de forma dinâmica e sim manualmente, validando a nova senha cadastrada no AP em cada uma das estações de rede sem fio.

Topologia de redes

Estrela (Star): Neste tipo de rede, os equipamentos estão conectados ponto-a-ponto, por intermediário de linhas (cabos) independentes, a um gerenciador central que é responsável por toda a comunicação e transferência de dados, bem como pelo controle do armazenamento de dados e gerenciamento de rede.

Neste sentido, enquanto dois nós estiverem se comunicando, os demais não terão que aguardar e se ocorre à quebra do nó central interrompe o funcionamento de rede.



Anel (Ring): Estações conectadas através de um caminho fechado.Com esta configuração, muitas das estações remotas ao anel não se comunicam diretamente com o computador central.São capazes de trocar dados em qualquer direção, mas as configurações mais usadas são

unidirecionais, de forma a tornar menos sofisticados os protocolos de comunicação que asseguram a entrega da mensagem corretamente e em seqüência ao destinatário.

Quando a mensagem é enviada, esta entra no anel e circula até ser retirada pelo nó do destinatário, ou então até voltar ao nó fonte, dependo do protocolo utilizado.Este último procedimento é mais desejável porque permite o envio simultâneo de um pacote para múltiplas estações e além do mais permite que determinadas estações recebam pacotes enviados por qualquer outra estação de rede, independente de qual seja o nó destinatário.

Barramento (Bus): Utiliza uma topologia descentralizada, este tipo de rede local caracteriza-se pela ocorrência de apenas uma única linha conexão.O acesso ao barramento é dividido entre todos nós, sendo que cada uma das estações de trabalho pode enviar dados a todas as outras estações componentes da rede.

Neste tipo de rede são utilizados repetidores de sinal, quando a distância é maior que a permitida por um segmento de cabo.O tipo de ligação é multiponto, onde cada um dos nós possui endereço único, o que faz com que seu monitoramento ao barramento seja contínuo, propendendo à verificação de possíveis mensagens ou dados que a ele tenham sido enviados.

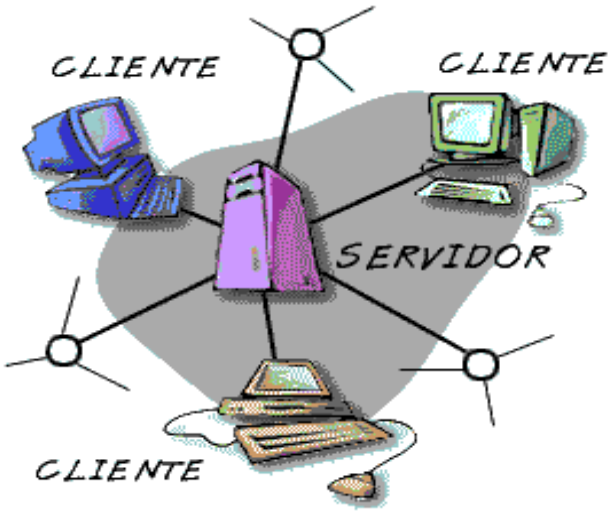
Uma das vantagens desse tipo de rede, sobre topologia diferente, é que com a queda de um nó, o restante da rede continua ativada normalmente.

Neste tipo de rede não existe hierarquia, no que se diz a respeito à ordem de transmissão dos dados, cada estação de trabalho que deseja transmitir pode fazê-lo sem que tenha que esperar

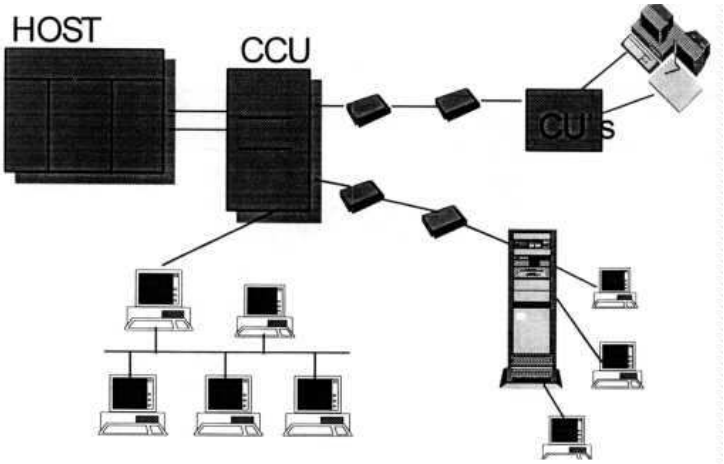
por algum tipo de permissão, podendo com isso vir a ocasionar o que se chama de “colisão de dados”(mistura de duas ou mais mensagens no transcorrer da transmissão), impedido que estes sejam reconhecidos pela estação destinatário.

Sistema Operacional

Cliente/Servidor: Há um ou mais computadores otimizados para prover unicamente serviço de rede, ou seja, não são utilizados como estações de trabalho e são chamados de servidores.As estações de trabalho ou clientes executam tanto aplicativos locais quanto aqueles instalados nos servidores, utilizando-se destes para conseguir serviços de redes como a validação de usuários, serviço de backup, acesso a Internet e outras redes.



Ponto a Ponto: Todas as estações de trabalho podem ser, simultaneamente, tanto servidores quanto terminais de redes.



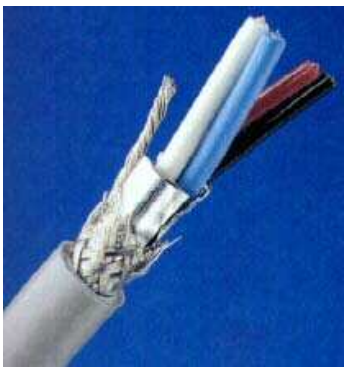
Modelo Misto: as redes começam com dois ou três computadores ligados ponto-a-ponto, que depois vão se expandindo até chegar ao modelo servidor/cliente ou, mais comum, em modelo misto com mais locais ponto-a-ponto interligados a um ou mais servidores dedicados a tarefas direcionadas.

Tipos de Meios de Transmissão

Cabo Coaxial é um condutor de cobre central, uma camada de isolamento flexível, uma blindagem com uma malha ou trança metálica e uma cobertura externa.O termo coaxial forma metade do circuito elétrico, além do mais funciona como uma blindagem para condutor interno.A cobertura do cabo exclui mais uma camada de isolamento e de revestimento de proteção e completa o conjunto.

Cabo Coaxial Fino (Thinnet) (10Base2) é conhecido como RG-58, com uma impedância de 52 Ohms, padronizado pelo IEEE 802.3a, com o nome de 10Base2, tamanho máximo de 185m.Esse tipo de cabo coaxial mais utilizado, porque sua bitola é menor que o cabo coaxial grosso.Nesta nomenclatura “10” significa taxa de transferência de 10Mbps e “2” a extensão máxima de cada segmento da rede.

Cabo Coaxial Grosso (Thicknet) (10Base2): é conhecido como RG-213, cada segmento de rede pode ter, no máximo, 500 metros e cada segmento de rede pode ter no máximo , 100 nós e além dos mais a distância mínima de 2,5 m entre cada nós da rede. Nesta nomenclatura “10” significa taxa de transferência de 10Mbps e que cada segmento da rede pode ter até 500 m de comprimento.



Par Trançado Sem Blindagem (UTP) é conhecido 10BaseT ou 100BaseT dependendo da taxa de transferência da rede, se de 10Mbps ou 100Mbps.Este cabo é composto por pares de fios, sendo que cada par isolado do outro e todos são trançados juntos dentro de uma cobertura externa.

Não há blindagem física no cabo UTP; ele obtém sua proteção do efeito de cancelamento dos pares de fios trançados. Este efeito de cancelamento reduz a diafonia entre os pares de fio e diminui o nível de interferência eletromagnética.

Cabo de par trançado

Tem cinco categorias UTP de acordo com as suas especificações:

Categoria 1 : Suporta os requisitos para transmissão de voz (POTS – plain old telephone service) velocidade de transmissão de até 19.2000bps.

Categoria 2 : Suporta os requisitos de uma rede Token Ring 4Mbps.Correspondente a categoria 3, definido pela IBM.

Categoria 3 : Suporta os requisitos de uma rede Ethernet (10Mbps) em par traçado.Usa uma banda de 10Mhz.

Categoria 4 : Usa uma banda passante de 200Mhz e suporta a velocidade de 16Mbps para rede Token Ring e 20Mbps para ARCNet.

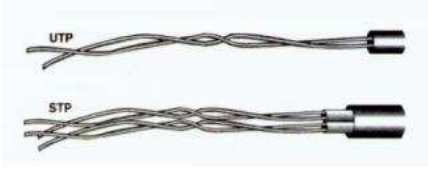
Categoria 5 : Utiliza uma banda passante de 100Mhz e suporta taxas de até 100Mbps desde que o cabo não tenha mais que 100 metros.

Par trançado Blindado (STP)

Os cabos de pares trançados blindados (STP) combinam as técnicas de blindagem e cancelamento para proteger o cabo contra a degradação do sinal.São de dois tipos:

STP de 100 ohms: Utilizado em Redes Ethernet, aumenta a resistência contra interferência eletromagnética/interferência de radiofreqüência do fio de par trançado.A blindagem não faz parte do circuito de dados, por isso tem que ser aterrada, pois se não for a blindagem irá se transformar em uma antena e os seus problemas se multiplicarão.

STP de 150 ohms: Usa a técnica de blindagem redundante, uma vez que é blindado, para reduzir a interferência eletromagnética e a interferência radiofreqüência , como cada par de fios trançados é separado um do outro por uma blindagem, o que faz diminuir a diafonia.Além do mais, cada par é trançado para que os efeitos do cancelamento sejam aproveitados.



Cabo de Fibra Ótica: Enquanto os fios de cobres transportam elétrons, os cabos de fibra ótica (cabos de fibra de vidro) transportam luz.Dentre algumas vantagens dos fios de fibras óticos estão a imunidade total contra a diafonia, contra interferência eletromagnética e contra interferência radiofreqüência.

A falta de ruídos internos e externos significa que os sinais têm alcance maior e se movem mais rápidos os que proporcionam uma velocidade e uma distância maiores do que as obtidas

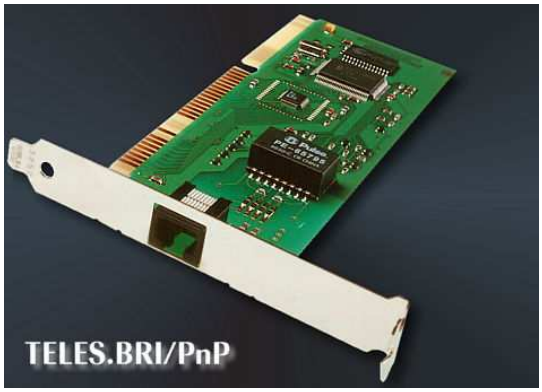
com cabos de cobre.Como não transporta eletricidade, a fibra é o meio mais adequado para conectar prédios com diferentes aterramentos elétricos.Além do mais, os cabos de fibra não atraem raios como os cabos de cobre.

O cabo de fibra ótica tem na parte externa, uma cobertura plástica para proteger o cabo inteiro.Sob essa cobertura, uma camada de fibra Kevlar (também usada em coletes à prova de bala), protege o fio de fibra de vidro contra impactos e proporciona maior robustez.Sob as fibras de Kevlar, outra camada plástica, denominada capa, que dá maior proteção.

Todo esse material protege o fio de fibra de vidro, que é tão fino quanto um fio de cabelo.Os dados percorrem o centro de cada fio de fibra de vidro, denominado núcleo, em forma de luz.A luz de um diodo ou laser entra no núcleo através de uma das extremidades do cabo e é absorvida por suas paredes (um evento chamado reflexão total interna).Os dados ainda podem ser transmitidos via satélite ou via rádio.

Equipamentos, Placas e Conectores.

Tem dois tipos básicos de placas de rede: ISA e PCI, a diferença entre elas fica por conta da taxa de transferência máxima que pode ser obtida.A comunicação em placas de rede ISA chega a somente a 10Mbps, enquanto que em placas de rede PCI a comunicação pode chegar a 100Mbps.



No caso de você optar por utilizar placas PCI, tome cuidado com o tipo de cabo e outros periféricos que serão utilizados (como hubs), já que nem todos trabalham com taxas acima de 10Mbps.Mesmo que sua rede seja composta somente por micros com placas de rede PCI, a taxa ficará limitada pela taxa do hub de 10Mbps.Da mesma forma, há cabos do tipo par trançado que não são indicados a trabalhar a 100Mbps.

Além do mais, devemos adquirir placas de rede de acordo com o tipo de cabo a ser utilizado.Nas placas de rede podem existir basicamente três tipos de conectores:

Conector RJ-45: Utilizado para conexão de cabos do tipo par trançados.Ao contrário do cabo coaxial, que possui somente dois fios: um interno e uma malha metálico ao redor, que elimina a interferência eletromagnética.O par trançado é composto por 8 fios (quatro pares), cada um com uma cor diferente.Cada trecho de cabo utiliza em suas pontas um conector do tipo RJ-45, que justamente possui oito pinos, para cada fio do cabo.

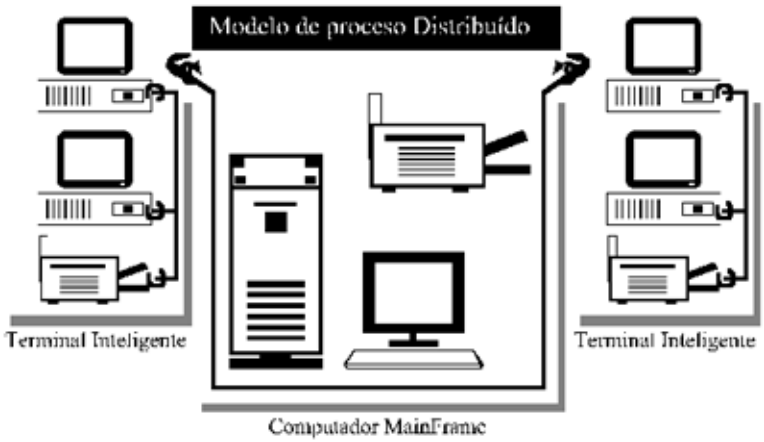
Teoricamente os cabos podem ser feitos de qualquer maneira, desde que um pino de uma extremidade seja conectado ao pino um da outra extremidade e assim sucessivamente para todos os oito pinos dos conectores.

A modificação aleatória da ordem dos fios pode causar a " Paradiafonia", que é o vazamento de energia elétrica entre pares de fios do mesmo cabo, podendo causar problemas na rede.Observa-se que, como o próprio nome diz, os fios formam par trançados onde estas tranças protegem os sinais de interferências externas.Esta proteção só existe quando esses pares fazem parte do mesmo circuito.Para evitar esse tipo de problema, existem dois padrões internacionais amplamente usados: T568A e T568B.

Conector BNC: Utilizado para conexões de cabos do tipo coaxial.

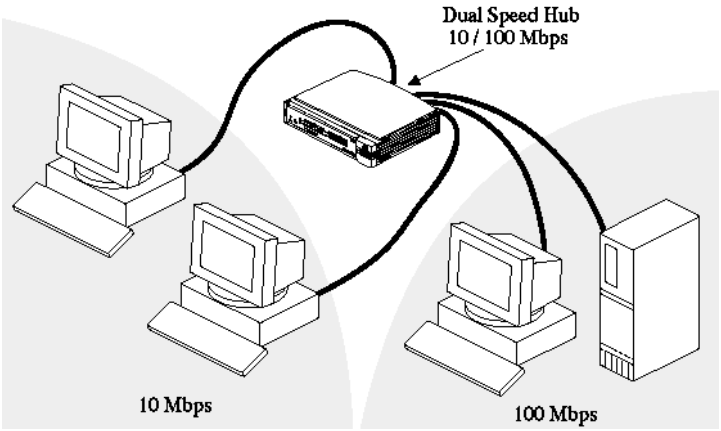
Repetidores: "Amplifica o sinal".São equipamentos utilizados quando se deseja repetir o sinal enviado por um equipamento, quando a distância a ser percorrida é maior do que o recomendado (180Mts).Ele realiza uma ampliação no sinal já fraco dando uma nova força para que chegue ao ponto destinado.

Constituem a parte mais simples de interligação, os repetidores são usados, geralmente, para interligação de duas ou mais redes idênticas.Atuando no nível físico, o repetidor é um dispositivo que propaga (regenera e amplifica) sinais elétricos em uma conexão de dados para estender o alcance da transmissão, sem fazer decisões de roteamento ou de seleção de pacotes.



Hubs: Em comunicação de dados, hub é o local de convergência onde os dados chegam de uma ou mais direção e são encaminhados para uma ou mais direções.Um hub , geralmente, inclui uma chave comutadora (switching), de algum tipo.Central de conexão de cabos.Os mais comuns são

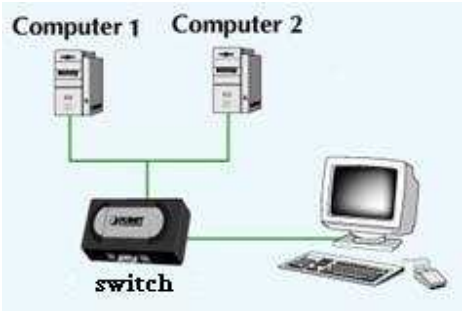
hubs Ethernet 10Base-T (conectores RJ-45), sendo eventualmente parte integrante de bridges e roteadores.



Switch: É um aparelho com múltiplas portas para conexão de dispositivos ligados a uma rede.Realiza a operação de comutação (switching), ou seja, recebe dados de uma estação ou do roteador conectado ao mundo externo e os envia para as estações locais, conforme o endereço destinado.A sua função é segmentar uma rede muito grande em LAN's menores e menos congestionadas, de modo que melhore o desempenho da rede.

Esse aumento de performance é obtido fornecendo a cada porta do switch uma largura de banda dedicada.No caso de redes locais diferentes serem conectadas em cada uma dessas portas, podem-se transmitir dados essas LAN's conforme o necessário.

O switch também provê uma filtragem de pacotes entre LAN's que sejam separadas. Este, porém ao contrário da ponte, que usa o barramento interno compartilhado, deve permitir que estações em segmentos separados comuniquem-se simultaneamente, já que comuta pacotes usando caminhos destinados.



Ponte (bridges): Conectam duas LAN's que usam o mesmo protocolo.Podemos visualizar uma ponte como um dispositivo que decide se uma mensagem que parte do usuário para outra pessoa irá para a rede local no seu prédio ou para alguém na rede local no prédio do outro lado da rua.Filtra os dados que não necessitam seguir adiante.

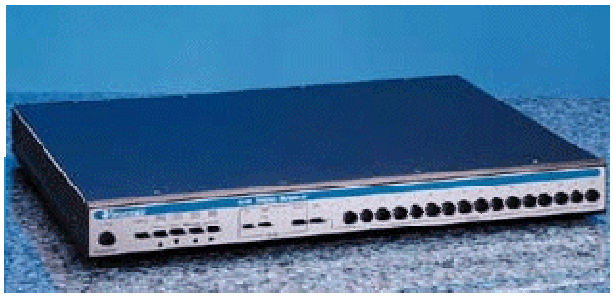
Roteadores (Router): Na Internet, um roteador é um aparelho, ou em alguns casos, um software do computador que determina o próximo ponto da rede para onde um pacote deve ser encaminhado.Este é conectado a pelo menos duas redes e decide para que lugar enviar cada pacote de informação baseado em seu conhecimento atual do estado da rede em que ele está conectado.

Modem Analógico: Modulador/Demodulador.Transforma sinais digitais(aquele que o computador entende –sinais binários: zero e um) em analógicos (aqueles que são passíveis de transmissão em uma linha de comunicação) e vice e versa.É padronizado pelo CCITT(Comitê Consultivo Internacional de Telefonia e Telegrafia) e é usado em comunicações de longas distâncias .Taxa de transmissão é pré – determinada.

Modem Digital ou Modem Banda Base ou Data Set: Não é necessariamente um modem (apesar de ter esse nome), já que este não transforma sinais digitais em analógicos.Ele transforma os sinais digitais em outro tipos de sinais digital (na verdade este faz uma codificação) que tolera com mais resistência uma distância maior que o sinal original suportaria.

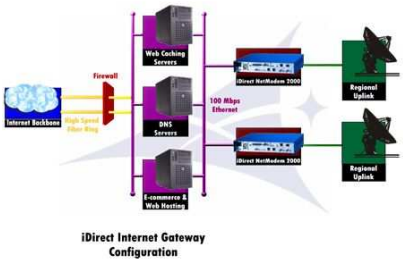
É apropriado para pequenas distâncias e, pela simplicidade, é mais barato que os analógicos.Uma das características mais importante do Modem Digital é o seu alcance diminui conforme aumenta a velocidade de transmissão, que não é padronizado pelo CCITT.

Multiplexador: Equipamento que permite a transmissão de dois ou mais sinais sobre uma mesma via de comunicação para otimização dessa via.Este aceita a combinação de diversas interfaces digitais de baixa velocidade numa interface digital de alta velocidade.



Concentrador/Conversor:Armazena várias informações antes de transmiti-las, compatibilizando velocidades e códigos diferentes.Também realiza o serviço de um multiplexador.

Gateway: É um ponto da rede que trabalha como entrada para outra rede.Na Internet, um nó, ou ponto parado, pode ser um nó gateway ou host (ponto final).Tanto os computadores de usuários de Internet quanto os que provêem páginas aos usuários são nós host.Os computadores que controlam os tráfegos da rede de uma mesma empresa ou provedor de acesso Internet (ISP) são os nós gateway.



iDirect Internet Gateway Configuration

Tipos de transmissão

Série: Cada bit é transmitido em seqüência, um após o outro.

Paralelo: Os bits são transmitidos juntos, e o seu uso é restrito a operações internas do computador ou a pequenas distâncias sobre cabos de fios múltiplos.Taxa de transmissão aumenta, mais a transmissão fica mais sujeita a erros.

Tipos de Sinais

Analógico: Os sinais elétricos podem assumir, no tempo, infinitos valores possíveis de amplitude permitidos pelos meios de transmissões.Tais sinais analógicos são usados em telefonia e televisão, por exemplo.

Digitais: Os sinais elétricos que representam informações assumem valores de amplitude predeterminados no tempo.Tais sinais são normalmente usados em telegrafia e transmissão de dados.Num determinado instante, o valor do sinal sempre será pré - determinado.

Sentido de Transmissão ou Modo de Operação

Simplex: O sinal vai apenas da origem (previamente determinada) para o destino (previamente determinado).

Half Duplex ou Semi Duplex: O sinal pode ser transmitido da origem para o destino e vice-versa, mais não é ao mesmo tempo.

Duplex ou Full Duplex: Os sinais podem ser transmitidos ao mesmo tempo, entre as duas extremidades que estão se comunicando, em ambos sentidos.

Modo de Transmissão.

Síncrono: Transmissão em massa de caracteres, a partir de uma sincronização entre equipamentos terminais de dados, obtidos através de caracteres de controle.

A velocidade de saída de dados na origem é a mesma da chegada de dados no destino, uma vez que os dois equipamentos trabalhem de forma sincronizada.A sincronização é feita para transmissão através de um oscilador.

Assíncrono (Start e Stop): Transmissão caractere, controlada por um sinal de START e outro STOP, indicando inicio e fim, de forma a ser identificada no destino.

Para cada byte transmitido são enviados um bit no início (bit de Start) e um bit no fim (bit de Stop).Esses bits têm desígnio de informar equipamento de destino o início e o fim de um byte transmitido.Isso é preciso porque os equipamentos não trabalham de forma sincronizada.

Protocolo TCP/IP: As redes são todas baseadas no protocolo TCP/IP.Uma das grandes vantagens desse protocolo é o processo de roteamento, que consiste no processo de guiar os pacotes de dados que trafegam pela rede para que eles encontrem seu caminho até o computador destino.Os dados trafegam pela rede em pequenos blocos, que saem de um emissor e chegam ao seu destino.Eles necessitam ser guiado para chegar lá.

O TCP/IP é um aglomerado de protocolo que trabalham em conjunto, que foram aglutinando ao protocolo IP original, que resultou de um trabalho do departamento de defesa dos EUA.Estes desejavam um sistema para interligar equipamentos dos mais diversos tipos e fabricantes, mas como uma característica notável e marcante: a rede deveria ser mantida e os dados deveriam atingir seu destino mesmo que uma ou mais estações retransmissoras deixassem funcionar, fosse por defeito, manutenção ou mesmo devido ataques inimigos.

Se uma rota desaparecesse, os dados deveriam imediatamente procurar um percurso alternativo, mantendo a rede em funcionamento mesmo que fosse numa velocidade menor.

O desenvolvimento desta tecnologia deu origem a Internet, e depois também foi aplicada nas redes locais que podem ser ligadas formando as denominadas intranets.As máquinas têm que ter a sua própria identidade.Com isso, pode-se ter a certeza de que o pacote de dados chegou ao seu destino, pois cada computador da rede é único e tem um endereço exclusivo.

O IP é composto por números binários de 32 posições, que geralmente é expresso em quatro grupos de números decimais.Cada grupo pode ir de 0 a 255, representando números binários de oito dígitos, isto é, números entre 00000000 a 11111111.Ele funciona em sintonia com mais itens

que, em conjunto, especificam a qual rede pertence cada IP e como os pacotes de dados podem encontrar a porta de saída para atingir outras redes.

Endereço IP: Números atribuídos a cada computador de rede TCP/IP.

Máscara de sub-rede - Em conjunto com o endereço IP marca a qual rede o computador integra.

Gateway: A porta de saída para que os pacotes de dados atingir demais redes partindo da rede local.

O comitê gestor, inicialmente organizou a Internet da seguinte maneira: três tamanhos de rede: grandes, médias e pequenas, que passaram a ser denominada de classe A, classe B e classe C. A diferença entre elas era o uso de 1, 2 ou 3 setores de 8 bits dos 32 possíveis para marcar as diferenças entre as classes.

Classe A: Ficam definidos apenas os oito bits à esquerda com valores de zero e 126, permitindo que existam apenas 127 redes do tipo A. Cabe ao administrador da rede interna determinar o restante dos 24 bits.Isso faz com que a rede possa possuir dois elevados 34 computadores ligados diretamente à Internet.

Classe B: Ficam definidos os primeiros 16 bits, deixando os 16 adicionais para serem distribuídos pelo administrador da rede interna.De 128 a 191 no primeiro quadrante e entre 0 a 255 no segundo, isto faz com que a rede possa ter 16.384 números de IPs.Cada um deles com possíveis 65.536 computadores.A Microsoft tem uma rede dessa.

Classe C: Fica definido os primeiros 24 bits e o administrador define os 8 bits que falta para completar os 32 bits.O primeiro quadrante na faixa de 192 e 223, o segundo e terceiro entre 0 a 225.Por esse motivo, as redes têm no máximo dois elevados a oito servidores.

VOIP: Voice over IP, ou voz sobre IP.Consiste em trafegar voz e dados através da rede de pacotes no protocolo IP.Esta tecnologia é baseada em padrões e recomendações e é aprovada por institutos de padronização internacional.

VPN: Significa Virtual Private Newtork, ou rede privada virtual, é uma rede para uso exclusivo dos usuários autorizados por uma empresa, para que se conectem a ela de qualquer lugar do mundo.A VPN permite que os dados trafeguem pela Web de forma segura, criptografados, como se passassem por dentro de um túnel.Os usuários autorizados podem ser conectar a essa rede de qualquer lugar.

Há dois tipos de VPN: A Client que conecta determinado cliente a empresa.Já a site-to-site conecta um determinado local a empresa.

GSM: Significa Global Sytem for Mobile Communications, ou sistema global para comunicações móveis.Padrão digital para telefonia móvel.É um sistema celular, com arquitetura aberta, que utiliza transmissão digital baseado na banda de 900 MHz, especificada pelo ETSI (European Telecommunications Stardards Institute)

Política de Segurança

Política de Segurança é um conjunto de regras e práticas que regulam como uma organização gerencia, protege e distribui suas informações e recursos.Sua implementação baseia-se na aplicação de regras que limitam o acesso às informações e recursos de uma determinada organização, com base na comparação dos níveis de autorização relativos ao acesso dessas informações e recursos.

Temos praticamente duas filosofias por trás de qualquer política de segurança: Proibitiva tudo que não é expressivamente permitido é proibido.E Permissiva tudo que não é proibido é permitido.

Elementos de uma Política de Segurança: Um sistema de computadores pode ser considerado como um conjunto de recursos, que é disponibilizado para ser utilizado pelos usuários autorizados.A política de segurança deve contemplar cinco elementos:

Disponibilidades: O sistema deve está disponível quando o usuário necessitar usar.Dados críticos devem estar disponíveis de forma ininterrupta.

Utilização: O sistema e os dados devem ser utilizados para as devidos objetivos.

Integridade: O sistema e os dados devem estar completamente íntegros e em condições perfeitas de ser usado.

Autenticidade: O sistema deve ter condições de verificar a identidade do usuário, e este ter condições de analisar a identidade do sistema.

Confidencialidade: Dados privados devem ser apresentados somente para os donos dos dados ou para grupos de usuários para a qual o dono dos dados permitir.

Orientações, Mecanismo e Técnica.

A segurança em uma rede relacionada à necessidade de proteção dos dados contra à leitura, modificação ou em qualquer tipo de manipulação das informações, e à utilização não autorizada dos computadores e seus periféricos.

Algumas das principais ameaças e ataques as redes de computadores são: Destruição de informações ou de outros recursos; modificação ou deturpação da informação; roubo, remoção ou extravio da informação ou de outros recursos; revelação de informações e interrupção de serviços.

Estes tipos de ataques podem ser ativos ou passivos.Os ataques ativos envolvem alterações de informações contidas no sistema.Ataques passivos são os que, quando realizados, não resultam em qualquer prejuízo das informações.Os principais ataques que podem ocorrer em uma rede de computadores são os seguintes:

Personificação: uma pessoa ou sistema faz-se passar por outro (a);

Replay: uma mensagem é interceptada e posteriormente transmitida;

Modificação: o conteúdo de uma mensagem é alterado, sem que o sistema possa identificar a alteração;

Ataques Internos: comportamento não autorizado por parte de usuários legítimos;

Armadilhas: modificações do processo de autenticação de usuários para desvendar senha, em resposta a uma combinação especificam;

Cavalo de Tróia: um login modificado que, ao iniciar a sua sessão, grava as senhas em um novo arquivo desprotegido.

Os serviços de segurança em uma rede de computador têm como função:

Confidencialidade: proteger os dados contra leitura por pessoas não autorizadas;

Integridade dos dados: evitar que pessoas não autorizadas modifiquem o contexto original de mensagens;

Autenticação: verificação da identidade do originador de cada mensagem, libera o envio de documentos eletronicamente assinados e a permissão de acesso de usuários aos sistemas através de senhas.

Uma política de segurança adequada às redes de computadores pode ser implementada a com a utilização de diversos mecanismos cujos principais são:

Criptografia: aprova o envio de informações delicadas por meios de comunicação não confiáveis, ou seja, em meio onde não é aceitável garantir que um intruso não irá interceptar o fluxo de dados para leitura (passivo) ou para modificá-lo (ativo). Ela modifica o texto original da mensagem a ser transmitida, provocando um texto criptografado na origem, através de um processo de codificação definido pelo método de criptografia utilizado. O texto criptografado é então transmitido e, ao alcançar o destinatário, passa pelo processo inverso, retornando ao formato original.

Assinatura digital: proporciona absoluta garantia ao usuário de que uma determinada mensagens provém de quem assina. É uma forma de autenticação usuário a usuário.Esta também permitir ao computador saber se uma mensagem foi alterada, total ou parcialmente, quando em circulação.

Autenticação: identificação de usuários usando a sintaxe de nomes hierárquicos do padrão X.500. Essa autenticação é bidirecional, isto é, o servidor autentica a identidade do usuário e este autentica a identidade do servidor. É usada todas as vezes que um
Usuário e um servidor, ou mais, estão se comunicando.

Controle de acesso: os mecanismos de controle de acesso são usados para garantir que o acesso a um recurso seja limitado aos usuários devidamente cadastrados.

Integridade dos dados: integridade atua em dois níveis. O controle da integridade de dados isolados e controle da integridade de uma conexão, ou seja, das unidades de dados e da seqüência de unidades de dados comunica-se no contexto da conexão.

Enchimento de tráfego: a geração de tráfego ilegítimo e o enchimento das unidades de transmissão de dados (pacotes), fazendo com que estas proporcionem um comprimento constante, são formas de fornecer proteção contra a análise do tráfego (sniffer).

Controle de roteamento: a possibilidade de controlar o roteamento, mencionando trajetos preferenciais para as transferências de dados. Pode ser utilizado para garantir que os dados sejam enviados em rotas fisicamente seguras ou para garantir que a informação sensível seja transportada, usando canais de comunicação que forneçam os níveis apropriados de proteção.

Segurança física e de pessoal: a segurança de algum sistema depende, em última instância, da segurança física dos seus recursos e do grau de confiabilidade do pessoal que o opera.

Hardware e Software de Seguranças: qualquer das identidades que fazem parte de um sistema deve fornecer garantias de que funcionam corretamente, para que se possa confiar nos mecanismos de segurança que pratica a política de segurança do mesmo.

Detecção e informe de eventos: a detecção de eventos relevantes no contexto da segurança inclui a detecção de violações aparentes à segurança e deve incluir, adicionalmente, a detecção de eventos "normais", como por exemplo, um acesso bem sucedido ao sistema (login).

Registro de eventos: o registro de eventos que podem significar ameaças à segurança de um princípio constitui-se em um respeitável mecanismo de proteção, pois possibilita a detecção e investigação de possíveis infrações, além de tornar possível a realização de auditorias.

FIREWALL

É um aparelhamento com duas ou mais interfaces de rede, que roteia apenas pacotes que corresponde a regras predefinidas em função de origem, destino, serviço (porta). O Firewall deve ser o único caminho entre duas sub-redes unidas por ele.Deve-se cortar qualquer outro caminho entre essas sub-redes.

Segurança é um dos pontos mais críticos na Internet, mas, na maioria das vezes, a discussão se sintetiza a problemas de violação de correspondências e dificuldades para se proteger a transmissão de números de cartões de crédito.

À medida que a maior parte das organizações conecta sua redes privadas à grande rede, a demanda principal passa a ser como impedir que usuários não autorizados ganhem acesso livre a dados sensíveis. O principal meio de proteger as redes privadas são os denominados firewalls.

Um firewall é simplesmente uma barreira entre duas redes, na maioria das vezes uma rede interna, chamada rede confiável ou trusted, e uma rede externa não confiável ou untrusted. Firewall examinam o tráfego nos dois sentidos e bloqueiam ou permitem a passagem de dados de acordo com um conjunto de regras definido pelo administrador. São usualmente constituídos de um conjunto de hardware e software e são muito usados para aumentar a segurança de redes privadas conectadas à Internet.

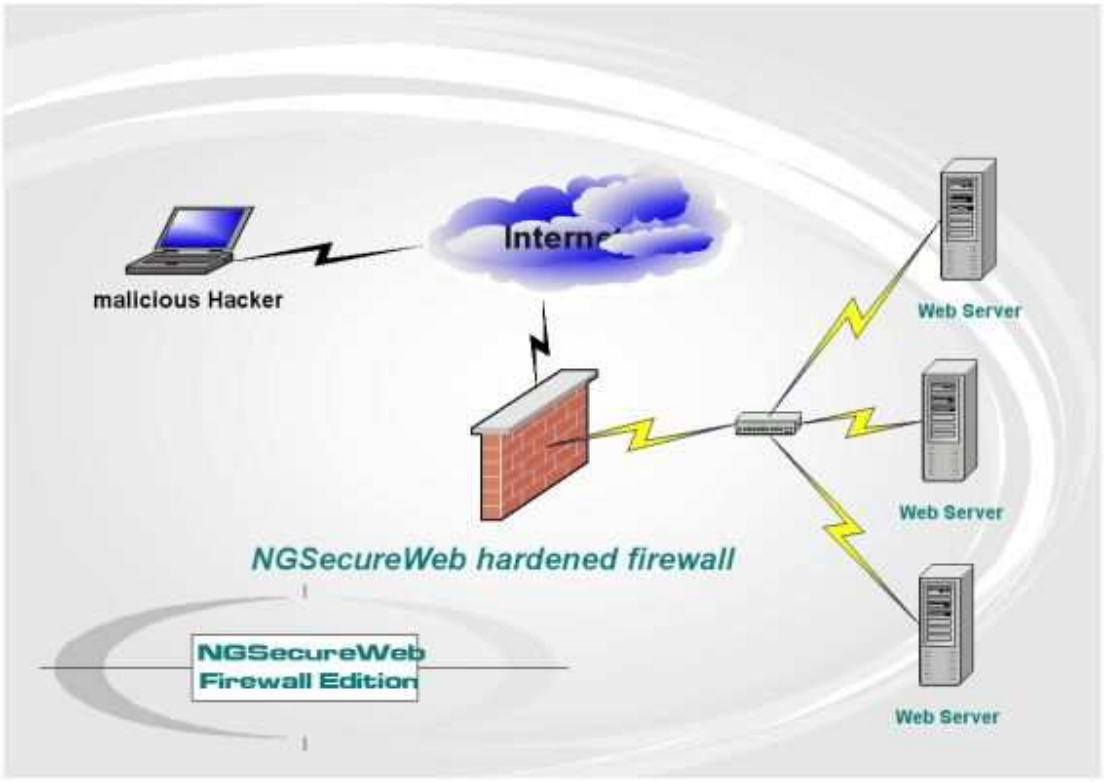
Pode-se utilizar também firewalls internos à rede para proteção adicional de dados de alta confidencialidade que pertençam aos altos níveis de tomada de decisões da empresa, tais como os gabinetes executivos, departamento de recursos humanos, departamento financeiro etc.

Um firewall é um sistema ou um grupo de sistemas que garante uma política de controle de acesso entre duas redes (normalmente a Internet e uma rede local). Em princípio, firewalls podem ser vistos como um par de mecanismos: um que existe para bloquear o tráfego e outro que existe para permitir o tráfego. Alguns firewalls dão maior ênfase ao bloqueio de trafego, enquanto outros enfatizam a permissão do mesmo.

O importante é configurar o firewall de acordo com a política de segurança da organização que o utiliza, estabelecendo o tipo de acesso que deve ser permitido ou negado. Com relação aos dados, existem três características principais que precisam ser protegidas:

- Segredo (privacidade);
- Integridade;
- Disponibilidade.

Mesmo que o intruso não danifique os dados, a simples utilização dos computadores e suas informações pode ter conseqüências danosas. Os recursos representam um substancial investimento da organização e as informações neles contidas, algo demasiado precioso para ser deixado à serviço de invasores.



Tarefas cabíveis a um firewall:

- Ele é um checkpoint, isto é, este é um foco para as decisões referentes à segurança, é o ponto de conexão com o mundo externo, tudo o que chega à rede interna passa por ele;
- Pode aplicar a política de segurança definida pela organização;
- Pode registrar eficientemente as atividades na Internet;
- Limita a exposição da organização ao mundo externo.

Existem firewalls que atuam na camada de rede (analisando pacotes IP) e outros que operam na camada de aplicação (analisando os dados dentro dos pacotes IP).Como seria de se esperar, quanto mais diligente e rigoroso for o firewall, mais difícil será para o ataque ter sucesso e mais fácil será investigá-lo posteriormente.

Criptografia é simplesmente o possesso de aplicar uma fórmula, chamada algoritmo de criptografia, para traduzir um texto normal para uma linguagem cifrada incompreensível· Esta

mensagem cifrada é então enviada pela rede pública e depois traduzida de volta para o texto normal ao ser recebida. O fator essencial para a criptografia é um valor numérico chamado chave, o qual se torna parte do algoritmo de criptografia, iniciando o processo de codificação.

Existem dois tipos principais de algoritmos de criptografia: o simétrico, ou de chave privada, e o assimétrico, ou de chave pública.

No algoritmo simétrico ou de chave privada, a mesma chave é utilizada para a codificação e decodificação.Este necessita de uma chave separada para cada par de usuários trocarem informação e também requer o estabelecimento e a distribuição de chaves secretas, o que simula uma carga administrativa expressiva.

Criptografia assimétrica usa duas chaves separadas.Cada participante numa transação criptografada possui umas chaves privadas, conhecidas somente por aquelas pessoas, e uma chave pública, que pode ser vista por todos.A mesma chave não pode ser utilizada para a codificação e decodificação.Uma mensagem é cifrada com a chave pública do receptor e só pode ser decodificada com a sua chave privada.

A vantagem desse método é deste processo é que há menos chaves para administrar.Já a desvantagem é de que ele exige muita capacidade de processamento, resultando em desempenho reduzido.Sendo assim, as maiorias das transações cifradas usam chaves simétricas para codificar e decodificar a informação que é transmitida para o destinatário, juntamente com a chave privada, embutida no texto, utilizando criptografia assimétrica.

Este método combinado de criptografia não só assegura privacidade dos dados como também habilita um mecanismo de autenticação denominado Assinatura Digital.

Autenticação/Assinatura Digital: O princípio da assinatura digital é que qualquer valor criptografado usa a chave privativa do remetente e autentica e qualquer valor decifrado usando a chave privada do recipiente e autentica.

As chaves públicas normalmente são autenticadas com certificados digitais que acompanham as transações, e são assinadas por uma autoridade certificadora, estas que oficialmente relaciona a chave pública com o usuário, pode existir internamente numa organização que utilize certificados digitais ou pode ser terceirizada para uma empresa de confiança de uma comunidade de usuários.

A técnica da assinatura digital pode ser utilizada para autenticar documentação oficial em forma digital on line.

Sniffers: São aplicativos que farejam uma rede à procura de pontos fracos que possam ser aproveitados por intruso a fim de penetrar com intenção maliciosa.Paradoxalmente, esse mesmo aplicativo também pode ser usado como ferramenta de proteção e segurança.

Os sniffers simulam determinadas funções normais de operação, podendo ser elas operacionais ou administrativas.Possuem vários tipos, mas o mais básico é o que penetra na rede e se instala numa posição estratégica para decifrar senhas.Outro tipo se habilita em serviços de rede e

máscara e sua própria presença, possibilitando assim a sua permanência por tempos indefinidos, com o objetivo de modificar aplicativos para destruir ou roubar dados.

Outros ainda provocam a intervenção dos administradores cujas contas e senhas são decifradas e armazenadas para futuras intrusões, com direito de modificar o sistema, bloquear serviços, mudar níveis de acesso, etc.

Os administradores de rede deve usar os sniffers para detectar falhas e pontos fracos na segurança da rede, da mesma maneira que fazem os intrusos.A detecção dessas falhas na segurança possibilita a implementação de um ambiente seguro.

A maior prevenção de invasão é a manutenção de uma rede segura, isso só pode ser obtido através de um ambiente conhecido e controlado.

Instalar uma ferramenta de segurança em um sistema que acabou de ser invadido, sem que se tenha um conhecimento preciso do estado do sistema, pode ter conseqüências catastróficas, além do mais destruir todos os vestígios que possam ter sido deixado pelo invasor.

Dispositivos e políticas que consigam captar o momento exato de uma invasão são extremamente úteis para que administrador da rede possa tomar as medidas necessárias.Um reconhecimento tardio de uma invasão pode tomar uma dimensão sem controle e comprometer inúmeros outros sites e sistemas de forma irremediável, sem poder ser rastreada.

Proteção Antivírus: Os vírus de computadores são a forma mais comum de ataque a sistemas. Eles penetram computadores pessoais e servidores, na forma de programas executáveis modificados ou macros, que se atrelam a documentos.

Uma vez dentro desses sistemas eles iniciam a sua operação disseminação e destruição.Os vírus se proliferam através do contato e uma vez dentro do sistema eles se multiplicam com grande velocidade.

Um dos meios mais comuns de introdução de vírus em sistemas é através de mensagens enviadas por correio eletrônicos.Outra maneira é através da troca de arquivo em disquetes ou por instalação de programas “pirateados” nos computadores pessoais.

Um programa de proteção antivírus deve ser implementado, essa proteção existe na forma de aplicativos antivírus que dever ser instalado em todos os servidores e cliente da rede.

Neste sentido, devemos instalar um mecanismo de proteção de vírus para que este possa identificar as infecções no momento em que elas ocorrem, isolando e inoculando de imediato o sistema infectado.

Segurança IPSec: é um framework (um conjunto de diversas ferramentas, compondo um sistema) de padrões abertos que visa a garantir uma comunicação segura em redes IP.

A segurança IPSec é a direção de longo prazo para redes seguras. Ela fornece uma linha de defesa fundamental contra ataques de rede privada e da Internet, equilibrando segurança com facilidade de uso. Esta tem dois objetivos:

- Proteger o conteúdo dos pacotes IP.

- Assegurar a defesa contra ataques de rede por meio da filtragem de pacotes e da aplicação de comunicações confiáveis.

Ambos os objetivos são atendidos através do uso de serviços de proteção baseados em criptografia, de protocolos de segurança e do gerenciamento dinâmico de chaves.

Essa base fornece a segurança e flexibilidade para proteger comunicações entre computadores de redes privadas domínios, sites, sites remotos, extranets e clientes dial-up.Ela pode ser usada até para bloquear o recebimento ou a transmissão de tipos de tráfego específicos.

A segurança IPSec baseia-se em um modelo de segurança ponto a ponto, estabelecendo relações de confiança e a segurança entre um endereço IP de origem e um de destino. Não é estritamente preciso que os próprios endereços sejam considerados uma identidade. É o sistema subjacente ao endereço IP que possui uma identidade a ser validada através de um processo de autenticação.

Os únicos que devem ter conhecimento do tráfego protegido são os computadores do remetente e do destinatário. Cada computador controla a segurança em sua respectiva extremidade, pressupondo que o meio através do qual a comunicação ocorre não é seguro.

Não é necessário que um computador que apenas encaminhe dados da origem para o destino ofereça suporte à segurança IPSec, a menos que a filtragem de pacotes do tipo firewall ou a conversão de endereços de rede esteja sendo feita entre os dois computadores. Esse modelo permite que a segurança IPSec seja implantada com êxito nas seguintes situações empresariais:

- Rede local (LAN): cliente/servidor e ponto a ponto.
- Rede de longa distância (WAN): roteador a roteador e gateway a gateway.
- Acesso remoto: clientes dial-up e acesso à Internet a partir de redes privadas.

Geralmente, ambos os lados necessitam da configuração de IPSec , para definir opções e configurações de segurança que permitirão que dois sistemas cheguem a um acordo sobre como proteger o tráfego entre si. A implementação da segurança IPSec pelo Microsoft Windows XP baseia-se em padrões de indústria desenvolvidos pelo grupo de trabalho sobre IPSec da Internet Engineering Task Force (IETF).

Os serviços relacionados à segurança IPSec foram, em grande parte, desenvolvidos em conjunto pela Microsoft e pela Cisco Systems, Inc.

Proxy não é mais que um intermediário que atua como cliente/servidor e que possibilita o acesso a redes exteriores à nossa rede, com o intuito de criar uma porta de segurança entre a nossa Intranet e a Internet. Tipicamente, um Proxy está implementado de forma a permitir o acesso, de dentro de uma Intranet protegida por um Firewall, às redes exteriores à mesma, ou seja, à Internet.

Na maioria das situações este Proxy executa serviços de Gateway. Geralmente, dois computadores estabelecem uma conexão TCP/IP do tipo cliente/servidor. Com o crescimento exponencial da utilização da Internet, o tráfego WWW nacional e internacional também cresceu exponencialmente, levando ao aparecimento de milhões de máquinas com endereços IP.

A criação de Routers com tabelas estáticas e/ou dinâmicas de encaminhamento veio ajudar para que o tráfego na Internet se tornasse mais fluido. Mas não bastando, era necessário criar máquinas que suportassem serviços e protocolos que os clientes e servidores não pudessem ou não tivessem implementado (o caso do serviço de DNS), de forma a que o primeiro encaminhamento de uma ligação se tornasse o mais rápido possível.

Deram o nome de servidor Proxy a essa máquina, sendo um dos seus serviços o encaminhamento de uma ligação para o Router mais próximo do destinatário.

Podemos então dizer que: o objetivo operacional de um servidor Proxy é estabelecer sessões para troca de dados entre clientes e servidores que não têm ou não podem estabelecer uma ligação IP diretamente entre eles.

No nível da segurança, um servidor Proxy implementa o controle de acesso que tipicamente o software de cliente ou servidor não suportam ou não têm implementado.

Invasão

Hacker: Indivíduo com facilidade de análise, assimilação, compreensão e capacidade surpreendente de conseguir fazer o que quiser com o computador. Este sabe perfeitamente que nenhum sistema é completamente livre de falhas e sabe onde procurar por elas, utilizando técnicas das mais variadas.

Cracker: Possuem tanto conhecimento quanto os hackers, mas com a diferença de que, para eles, não basta entrar no sistema, quebrar senhas e descobrir falhas. Eles precisam deixar avisos de que estiveram lá, geralmente recados malcriados, algumas vezes destruindo partes do sistema, e até aniquilando com tudo o que vêem pela frente.

Também são atribuídos aos crackers programas que retiram travas em softwares, bem como os que alteram suas características, adicionando ou modificando opções.

Vírus: Como o nome já sugere, é um programa que infecto um arquivo ou outro programa de computador. Inserindo nos mesmos uma cópia de si (do vírus). E enquanto o arquivo ou programa é executado, também executa o vírus continuando, assim, a infecção. Para que haja a infecção, é preciso que um programa infectado. de um modo qualquer seja executado. Isso, basicamente, pode acontecer de três maneiras:

- Esquecendo um disquete no drive: quando liga o computador;
- Instalando programas de procedência duvidosa ou desconhecida retirados da Internet, disquetes ou CD-

- ROM, através de compartilhamento de recursos que abrem arquivos armazenados em outros micros;
- Abrindo arquivos do Word, Excel ou anexados aos e-mails.

Formas de ataque

Vírus de Macro: Macros são comandos organizados e armazenados em algum aplicativo, para serem usados na automatização de algumas tarefas repetitivas. Para escrever um vírus de macro é necessário que se tenha em mente essa facilidade de automatização e que seja parte de um arquivo manipulado por aplicativo que utilize macro, pois somente assim ele poderá ser executado.

Porém o arquivo que contém precisa ser aberto para que o vírus execute vários comandos automaticamente, contaminando outros arquivos no computador.Dentre os arquivos mais suscetíveis a esse ataque temos o Word, Excel, Power Point e Access.

Worm: Este não é um vírus, mas tem a capacidade de se propagar automaticamente através de redes e enviar cópias suas de uma máquina a outra.Esse não necessita ser explicitamente executado para que aconteça sua propagação, ela se dá na verificação da vulnerabilidade contida ou na falha na configuração de programas instalados nos computadores.

Cavalo de Tróia: Na maioria das vezes este irá instalar programas para permitir que um invasor tenha controle total sobre o computador.

Dos- Denial Of Service- Negação de Serviço: Processo pelo qual um invasor entra num computador para impedir a operação de um serviço ou computador conectado a Internet.Exemplo: sobrecarregar o processamento de dados do computador a tal ponto que o usuário fique impedido de utilizá-lo ou retirar do ar serviços importantes, inviabilizando o acesso dos usuários aos seus e-mails ou seu servidor Web.

Bombas Lógicas: Ativam e provocam danos num sistema contaminado, unicamente quando se reúne uma ou mais condições.Não são considerados propriamente vírus, já que não se reproduzem, mas depende das ações realizadas pelo usuário.

Vírus de programas (Program Files): Infectam programas, uma vez executado o programa contaminado, o vírus entra em ação, produzindo os efeitos para qual foi programado.

A Internet

É uma rede mundial com milhões de máquinas conectadas ao redor do mundo, a maior parte destes equipamentos é composto por PC's tradicionais, por estações de trabalho com sistema Unix e pelos denominados servidores que armazenam e transmitem informações, como as páginas da Web (World Wide Web-WWW) e mensagens de e-mail.

Os computadores que usamos pode ser chamado de hospedeiros (host) ou sistemas finais, porque hospedam programas de aplicação e além do mais situam na periferia da Internet.

O modelo cliente/servidor, um programa cliente que roda em um sistema final pede e recebe informações de um servidor que roda em outro sistema final, esta estrutura se denomina Internet.

Os sistemas finais operam protocolos que controlam o envio e o recebimento de informações da Internet.O TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) e o IP (Internet Protocol – Protocolo da Internet) são os protocolos mais importantes da Internet.Estes são conhecidos copletivamente como TCP/IP.

Estes sistemas são conectados entre si por enlaces de comunicação (Links) que podem utilizar diferentes meios físicos para sua ligação.

A velocidade de transmissão do link é chamada de largura de banda e é medida em bits por segundos (bps).Indiretamente são os roteadores que conectam os sistemas finais.Um roteador encaminha a informação que está chegando por um dos links de saída.

O protocolo IP especifica o formato da informação que é enviada e recebida entre os roteadores e os sistemas finais.O caminho que a informação transmitida percorre do sistema final de origem, passando por uma série de enlaces de comunicação e roteadores, para um sistema final de destino, é conhecido como rota ou caminho pela rede.

Em vez de fornece um caminho dedicado entre os sistemas finais comunicantes, a Internet usa uma técnica conhecida como comutação de pacotes, que permite múltiplos sistemas finais comunicantes compartilhem um caminho, ou parte de um caminho ao mesmo tempo.

Esta estrutura toda interconectada demanda uma hierarquia em termos de rede de acesso.Sistemas finais conectados a provedores de acesso(ISP).Uma rede de acesso pode ser uma rede local de uma empresa, uma linha telefônica acoplada a um modem ou a uma rede de acesso de alta velocidade dedicada ou comutada.

Em linhas gerais isto seria o conceito de Internet no âmbito público.Têm as redes privadas de empresas ou governos, cujos computadores não são acessíveis às máquinas externas a estas.Essas redes privadas são as chamadas intranets.

Como funciona a Internet.

A Internet é como uma rede telefônica, onde, em lugar de um aparelho telefônico, está um computador, o que transforma em uma rede telefônica audiovisual.A rede telefônica mundial é o conjunto das redes de cada país, sendo que no Brasil, a rede telefônica nacional é subdividida em

redes estaduais; as estaduais em metropolitanas; as metropolitanas, em centrais telefônicas onde estão conectados os vários aparelhos telefônicos de um determinado bairro.

A rede mundial da Internet também se subdivide em países e, dentro dos países, se subdivide em vários níveis até chegar ao provedor de acesso, que faz o papel da central telefônica.E, assim como do seu telefone, você pode ligar para qualquer lugar do mundo, desde que do lado de lá também exista um aparelho, uma linha e uma companhia telefônica. Com o computador você também pode ligar para qualquer outro computador, desde que cada um tenha um modem, uma linha e um provedor de acesso.

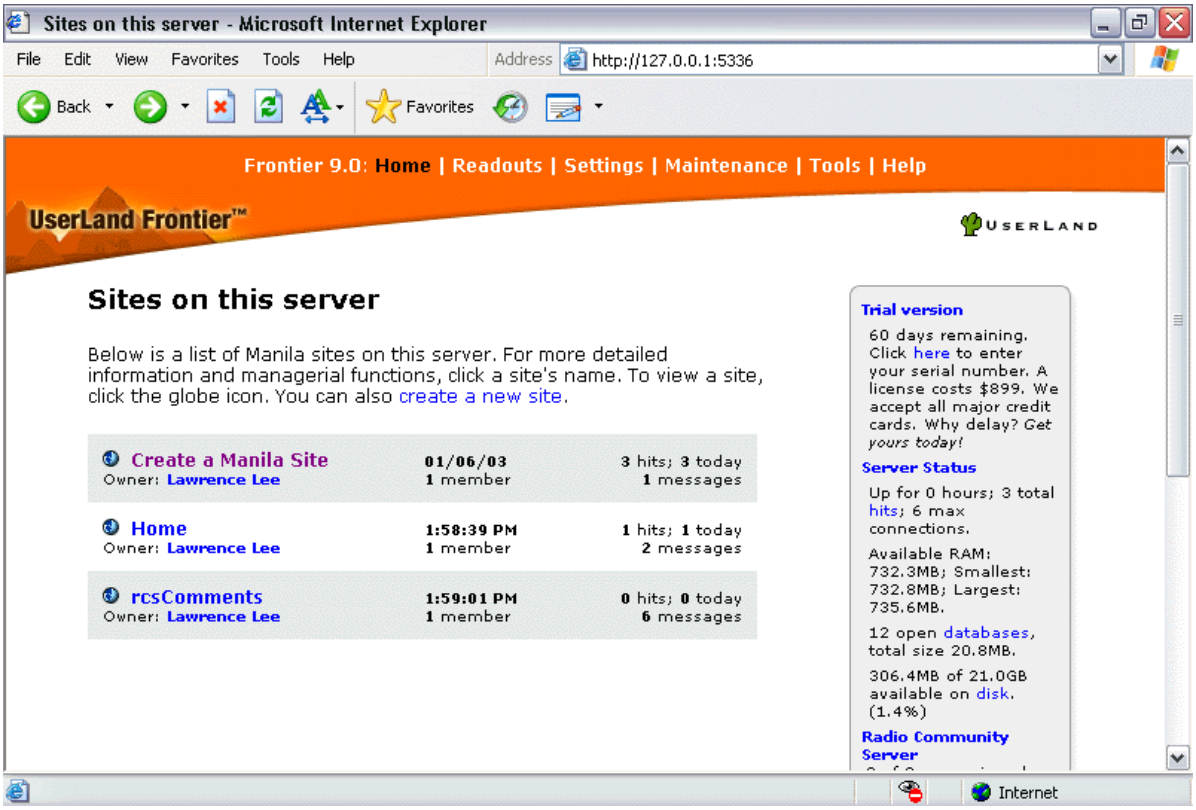
O computador do provedor de acesso (ISP) tem o nome de Host cuja tradução é anfitrião, porque é ele quem vai ser o nosso anfitrião na Internet.A passagem para a Internet chama-se Sateway (guêituei), cuja tradução é porta, abertura, isto é, o provedor de acesso é a nossa porta de entrada na Internet.

Quando dizemos que entramos na Internet quer dizer que nos conectamos com algum computador que está na rede. Ninguém entra na rede sem se conectar com outro computador, assim como você só entra na rede telefônica quando completa a chamada.

Quando o Modem instalado em sua máquina liga para o modem do seu provedor de acesso, eles trocam as primeiras informações para definir a velocidade, paridade e outros dados daquela conexão. E quando nós escutamos aquele ruído característico, o shakíng hands, que significa aperto de mão, cumprimento.

Cada modem envia o seu protocolo para informar que tipo de equipamento está pedindo e recebendo a conexão; então, protocolo é um padrão de comunicação entre dois computadores, que possibilita a troca de mensagens para a transmissão de dados. O mais comum desses padrões hoje em dia, é o HTTP, e ao conjunto de recursos, usuários e computadores (ligados na Internet pelo protocolo HTTP dá-se o nomede WWW (World Wide Web - ou simplesmente Web)).

Na Internet existem computadores que estão abertos ao público, são aqueles que têm alguma coisa para mostrar, com ou sem finalidade comercial. Pode ser um texto, uma foto, uma música, um filme, ou qualquer combinação entre eles. A área da memória deste computador, que pode ser visitada, chama-se SITE.



A Web é um banco de dados ou servidor de aplicações que contém informações que podem ser manipuladas através de software de navegação (browser). Cada página de um site ou ponto de presença WWW pode conter informações textuais e gráficas e informações na forma de vídeo ou de áudio.

Nas páginas da WWW, qualquer palavra, frase, figura ou ícone pode ser marcada para funcionar como um endereço de outras páginas em um sistema hipertexto. Isto possibilita o deslocamento entre páginas com o simples uso do mouse (apontando com o ponteiro do mouse o que está marcado e apertando o botão principal do mouse). Esta codificação é feita usando uma linguagem de marcação de texto denomina da HTML, que permite indicar, em cada página, o que é texto, o que é figura, ou o que é um ícone de ligação com outras páginas.

Intranet e Extranet.

A Intranet é uma forma de agilizar o trânsito de informações dentro de uma empresa. através da criação de verdadeiros sites departamentais. É fundamentada no protocolo de rede TCPIIP, padrão de uso da Internet e largamente utilizado por aplicações cliente-servidor e conexão de equipamentos em geral. Isto é, todos os recursos que o protocolo possibilita poderão ser utilizados na rede (browser, e-mails.).

Consiste da instalação de um servidor, Sistema Operacional (Windows 2000, Unix...), que provê páginas de informação e/ou aplicações da mesma maneira como é feito na Internet, ou seja, por meio de softwares gerenciadores de serviços de rede.

O Servidor é o responsável pelo processamento das informações arquivadas. Este atenderá a todas as solicitações de páginas realizadas pelas diversas estações de trabalho. Na configuração da rede TCP/IP atribui-se um endereço para cada equipamento e a configuração do browser já pré-instalado.

O termo Intranet é também usado para qualquer rede corporativa de acesso remoto (redes LAN e WAN) que não tenham qualquer conexão com a Internet; então podemos dizer que existem Intranets com ou sem acesso à Internet.

Intranet é semelhante a um site da Web e usa protocolos da Internet, mas é uma rede interna exclusiva de uma empresa.

Extranet também é um site da Web interno ou privado, mas os
Privilégios de acesso também se estendem aos clientes, parceiros e/ou outros usuários encolhidos A Extranet seria uma tecnologia usada para interligar várias Intranets.