GOVERNO DO ESTADO DO ESPÍRITO SANTO
SECRETARIA DE ESTADO DA EDUCAÇÃO
GERÊNCIA DE DESENVOLVIMENTO DA EDUCAÇÃO
SUBGERÊNCIA DE DESENVOLVIMENTO DA ED. BÁSICA E PROFISSIONAL
PROGRAMA DE INFORMÁTICA NA EDUCAÇÃO

CURSO

ALUNO

TÉCNICO

Um pouco mais sobre redes

NTE METROPOLITANO
Av César Hilal nº 1111 – 3º andar – salas: 325 a 329
Telefones: 3137-4328 e 3137-4329
nte_metropol@educacao.es.gov.br

Olá Alunos-Técnicos,

Nesta apostila, vamos entender mais sobre as redes. Descobrir que existem dois tipos básicos de redes e vários tipos de cabeamento.

Também vamos conhecer como o Windows NT Server pode auxiliar a vida do administrador de rede, no quesito segurança, tão importante nos dias de hoje.

E então, vamos começar?

O conceito de rede

Em seu nível mais elementar, uma rede consiste em dois computadores conectados uns aos outros por um cabo para que possam compartilhar dados. Todas as redes, não importam o quanto sejam sofisticadas derivam desse sistema simples. Se a idéia de dois computadores conectados por um cabo pode não parecer extraordinária, no passado representou uma grande conquista nas comunicações.

As redes surgiram da necessidade de compartilhar dados em tempo hábil. Os computadores pessoais são ferramentas de trabalho ótimas para produzir dados, planilhas, gráficos e outros tipos de informação, mas não possibilitam que você compartilhe rapidamente os dados que criou. Sem uma rede, os documentos devem ser impressos para que outras pessoas possam modificá-los ou utilizá-los. Na melhor das hipóteses, você entrega os arquivos em disquetes para que outras pessoas copiem em seus computadores. Se fizerem modificações no documento, não há como mescla-las. Isto era, e ainda é, conhecido como trabalhar em um ambiente autônomo.

Ambiente autônomo

Se uma pessoa tivesse que conectar seu computador a outros, poderia compartilhar os dados dos outros computadores e as impressoras. Um conjunto de computadores e outros dispositivos conectados juntos chama-se rede, assim como o conceito de computadores compartilhados os recursos.

Os computadores que fazem parte de uma rede podem compartilhar:

- Dados,
- Mensagens,
- Gráficos,
- Impressoras,
- Aparelhos de fax,
- Modems,
- Outros recursos de hardwares.

Essa lista está sempre crescendo conforme são encontrados novas maneiras de compartilhar e se comunicar através dos computadores.

Redes locais

As redes começaram pequenas, com talvez dez computadores conectados a uma impressora. A tecnologia limitou o tamanho da rede, incluindo o número de computadores conectados, assim como a distância física que poderia ser abrangida pela rede. Por exemplo, no início dos anos 80, o método mais popular de cabeamento possibilitaria cerca de 30 usuários em uma extensão máxima de cabo de pouco mais de 180 metros. Esse tipo de rede deveria estar em um único andar de um prédio ou em uma empresa pequena. Atualmente, para empresas muito pequenas, essa configuração ainda é adequada. Esse tipo de rede, dentro de uma área limitada, chama-se rede local (LAN).

A expansão das redes

As primeiras LAN não conseguiram atender adequadamente às necessidades de uma grande empresa com escritório em vários locais. À medida que as vantagens das redes foram se tornando conhecidas e mais aplicativos para ambientes de rede foram sendo desenvolvidos, as empresas perceberam a necessidade de expandir suas redes para continuarem competitivas. Hoje em dia, as LAN se transformaram nos blocos de construção de sistemas maiores.

À medida que o alcance geográfico da rede aumenta com a conexão de usuários em cidades ou estados diferentes, a LAN torna-se uma rede de longa distância (WAN, Wide Área Network). O número de usuários na rede de uma empresa agora poderá aumentar de dez para milhares.

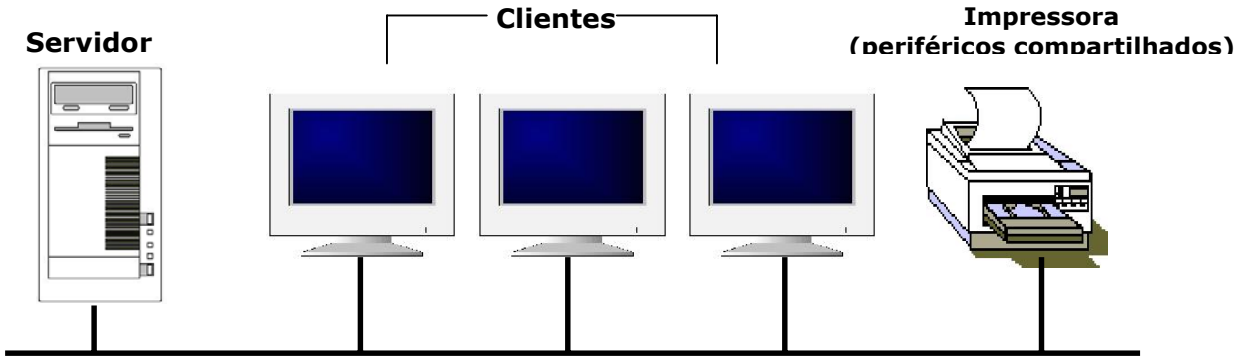
Hoje, a maioria das grandes empresas armazena e compartilha enormes quantidades de dados importantes em um ambiente de rede, motivo pelo qual as redes são atualmente tão importantes para as empresas quanto às máquinas de escrever e os gabinetes de arquivos eram no passado.

Os dois tipos principais de rede

Visão geral das redes

Todas as redes, de forma geral, têm certos componentes, funções e recursos em comum. Estes incluem:

- Servidores – Computadores que fornecem recursos compartilhados para os usuários da rede,
- Clientes – Computadores que acessam recursos fornecidos por um servidor e compartilhados na rede,
- Mídia – A maneira como os computadores estão conectados,
- Dados compartilhados – Arquivos fornecidos pelos servidores através da rede.
- Impressoras e outros periféricos compartilhados – Outros recursos fornecidos pelos servidores,
- Recursos – Arquivos, impressoras ou outros itens a serem utilizados pelos usuários da rede.



Mesmo com essas semelhanças, as redes podem ser divididas em duas categorias mais amplas:

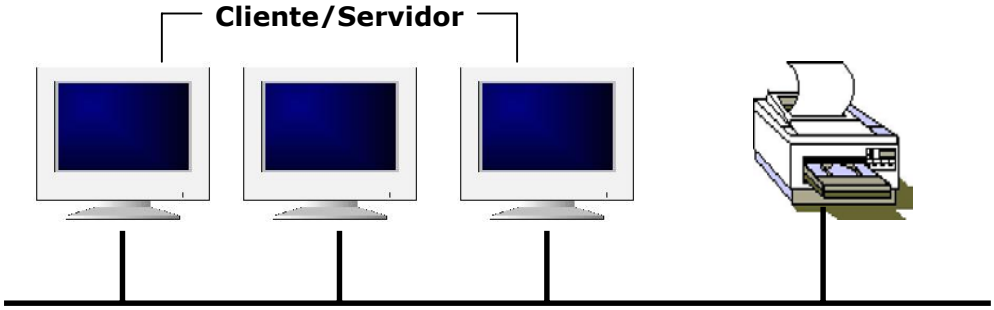
- Par a par,
- Baseadas em servidor.

A distribuição entre as redes par a par baseada em servidor é importante, pois cada uma possui capacidades diferentes. O tipo de rede que for escolhida para ser implementada vai depender de inúmeros fatores, incluindo:

- Tamanho da empresa,
- Nível de segurança requerido,
- Tipo de empresa,
- Nível de suporte administrativo disponível,
- Intensidade de tráfego na rede,
- Necessidades dos usuários da rede,
- Orçamento da rede.

Redes par a par

Em uma rede par a par, não existem servidores dedicados ou hierárquicos entre os computadores. Todos os computadores são iguais e, portanto, chamados pares. Normalmente, cada computador funciona tanto como clientes quanto como servidor, e nenhum deles é designado para ser um administrador responsável por toda a rede. O usuário de qualquer computador determina quais dados de seu computador são compartilhados na rede.



Rede Par a Par

Tamanho:

As redes par a par também são chamadas de grupos de trabalho. Pelo termo grupo de trabalho subentende-se um pequeno grupo de pessoas. Em uma rede par a par há, tipicamente, pouco menos do que 10 computadores na rede.

Custo:

As redes par a par são relativamente simples. Uma vez que cada computador funciona como clientes e servidor, não há necessidades de um servidor central complexo ou de outros componentes necessários para uma rede de grande capacidade. As redes par a par podem ser mais baratas do que as redes baseadas em servidor.

Sistema operacional par a par:

Em uma rede par a par, o software de comunicação de rede não requer o mesmo nível de desempenho e segurança de um software de comunicação de rede projetado para servidores dedicados. Os servidores dedicados funcionam apenas como servidores e não são utilizados como um cliente ou uma estação de trabalho. Eles serão discutidos com maiores detalhes posteriormente nesta apostila.

Em sistemas operacionais, como o Microsoft Windows NT Workstation, Microsoft Windows 2000, Microsoft Windows para Workgroups e Microsoft Windows 95, 98, Me e XP, as redes par a par são construídas dentro do sistema operacional. Não se exige nenhum outro software para configurar uma rede par a par.

Implementação:

Em um ambiente par a par típico, há várias questões de rede que possuem soluções padronizadas. Estas soluções de implementação incluem:

- Computadores localizados nas mesas dos usuários,
- Usuários que atuam como seus próprios administradores e planejam sua própria segurança,
- Utilização de um sistema simples de cabeamento de fácil visualização, que conectar computador a computador na rede.

Onde a rede par a par é adequada:

As redes par a par são uma boa escolha para ambiente onde:

- Há menos de 10 usuários,
- Todos os usuários estão localizados na mesma área geral,
- A segurança não é uma questão importante,
- A empresa e a rede terão um crescimento limitado em um futuro previsível.

Considerando-se essas diretrizes, há ocasiões em que uma rede par a par será uma solução melhor do que uma rede baseada em servidor.

Considerações sobre redes par a par:

Enquanto uma rede par a par pode atender às necessidades das pequenas empresas, este tipo de abordagem pode não ser adequada a certos ambientes. As áreas de redes a seguir ilustram alguns problemas de rede par a par que um planejador de rede deverá resolver antes de decidir sobre o tipo de rede a implementar.

Administração:

A administração de rede envolve uma gama de tarefas, incluindo:

- Gerenciamento de usuários e de segurança,
- Disponibilização de recursos,
- Manutenção de aplicativos e de dados,
- Instalação e atualização de softwares de aplicativos.

Em uma rede par a par, não existe um gerente de sistemas que supervisione a administração de toda a rede. Cada usuário administra seu próprio computador.

Compartilhando recursos:

Todos os usuários podem compartilhar qualquer um de seus recursos da maneira que escolher. Esses recursos incluem dados em pastas compartilhadas, impressoras, placas de fax modem, assim por diante.

Requisitos do servidor:

Em um ambiente par a par, cada computador deve:

- Utilizar uma grande porcentagem de seus recursos para suportar o usuário local (o usuário do computador).
- Utilizar recursos adicionais para suportar cada usuário remoto (o usuário que está acessando o servidor na rede) que estiver acessando seus recursos.

Uma rede baseada em servidor precisa de servidores dedicados mais complexos para atender às demandas de todos os clientes na rede.

Segurança:

A segurança consiste em estabelecer uma senha em um recurso, como uma pasta que é compartilhada na rede. Pelo fato de todos os usuários de redes par a par estabelecerem sua própria segurança e o compartilhamento poder existir em qualquer computador e não apenas em um servidor centralizado, o controle centralizado é muito difícil. Isso tem um grande impacto na segurança da rede, pois alguns usuários podem não implementar nenhuma segurança. Se a segurança for uma questão importante, você deve considerar uma rede baseada em servidor.

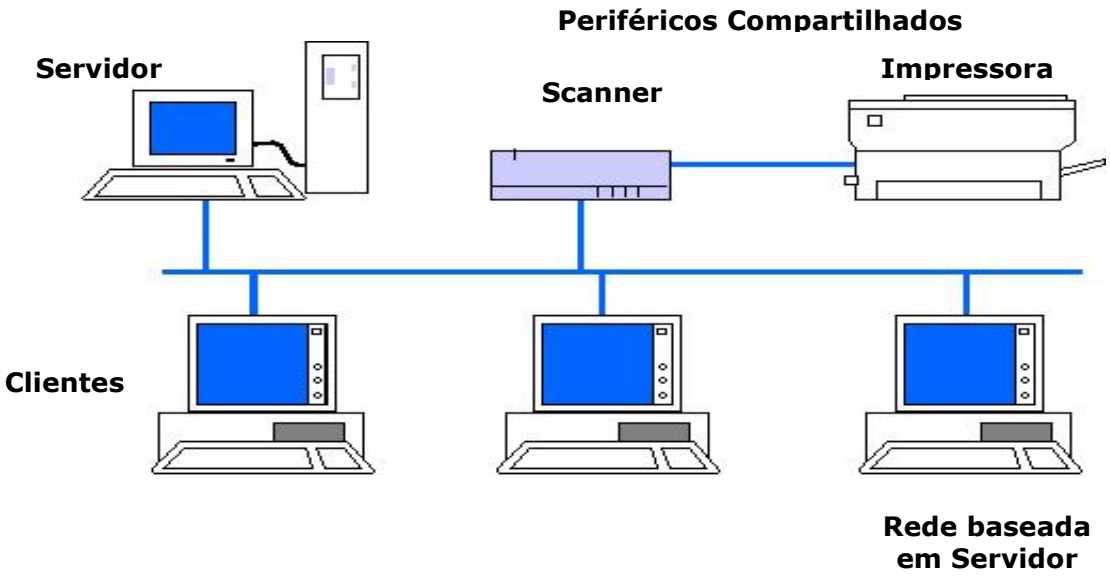
Treinamento:

Uma vez que todos os computadores em um ambiente par a par podem atuar tanto como servidores quanto como clientes, os usuários devem ser treinados para que sejam capazes de agir adequadamente tanto como usuários quanto como administradores de seus próprios computadores.

Redes baseadas em servidor

Em um ambiente com mais de 10 usuários, uma rede par a par – com os computadores agindo como servidores e clientes – provavelmente não será adequada. Portanto, a maior parte das redes possui servidores dedicados.

Um servidor dedicado é aquele que funciona apenas como servidor e não é utilizado como um cliente ou estação de trabalho. Os servidores são "dedicados" porque são otimizados para processar rapidamente as requisições dos clientes da rede e para garantir a segurança dos arquivos e pastas. As redes baseadas em servidor tornaram-se o modelo padrão para a comunicação de rede e serão utilizadas como exemplos básicos em toda essa apostila.



Conforme o tamanho e o tráfego das redes aumentam o número de servidores na rede. A distribuição de tarefas entre vários servidores garante que cada tarefa seja desempenhada da maneira mais eficiente possível.

Servidores especializados:

A diversidade de tarefas que os servidores devem desempenhar é variada e complexa. Os servidores de grandes redes se tornaram especializados para acomodar as necessidades crescentes dos usuários. Por exemplo, em uma rede Windows NT Server, os diferentes tipos de servidores incluem:

- **Servidores de arquivos e impressão:**

Os servidores de arquivos e impressão gerenciam o acesso do usuário e a utilização dos recursos de arquivos e impressora. Por exemplo, se você estivesse executando um aplicativo de processamento de texto, como o Word, este seria executado no seu computador. O documento do processamento de texto armazenado no servidor de arquivos e impressão é carregado na memória de seu computador para que você possa editá-lo ou utilizá-lo localmente. Em outras palavras, os servidores de arquivos e impressão destinam-se ao armazenamento de arquivos e de dados.

- **Servidores de aplicativos:**

Os servidores de aplicativos constituem a parte do servidor dos aplicativos cliente/servidor, assim como os dados, disponíveis para cada cliente. Por exemplo, os servidores armazenam enormes quantidades de dados que estão estruturados para facilitar sua recuperação. Eles são diferentes de um servidor de arquivo e impressão. Com um servidor de arquivo e impressão, os dados ou o arquivo são carregados para o computador que fez a requisição. Com um servidor de aplicativos, o banco de dados fica no servidor e apenas os resultados requeridos são carregados no computador que fez a requisição.
Um aplicativo de cliente sendo executado localmente teria acesso aos dados no servidor de aplicativos. Ao invés de todo o banco de dados ser carregado do servidor para o seu computador local, apenas os resultados das suas consultas seriam carregados nele. Por exemplo, você poderia procurar no banco de dados de funcionários todos os funcionários nascidos em novembro.

- **Servidores de correio:**

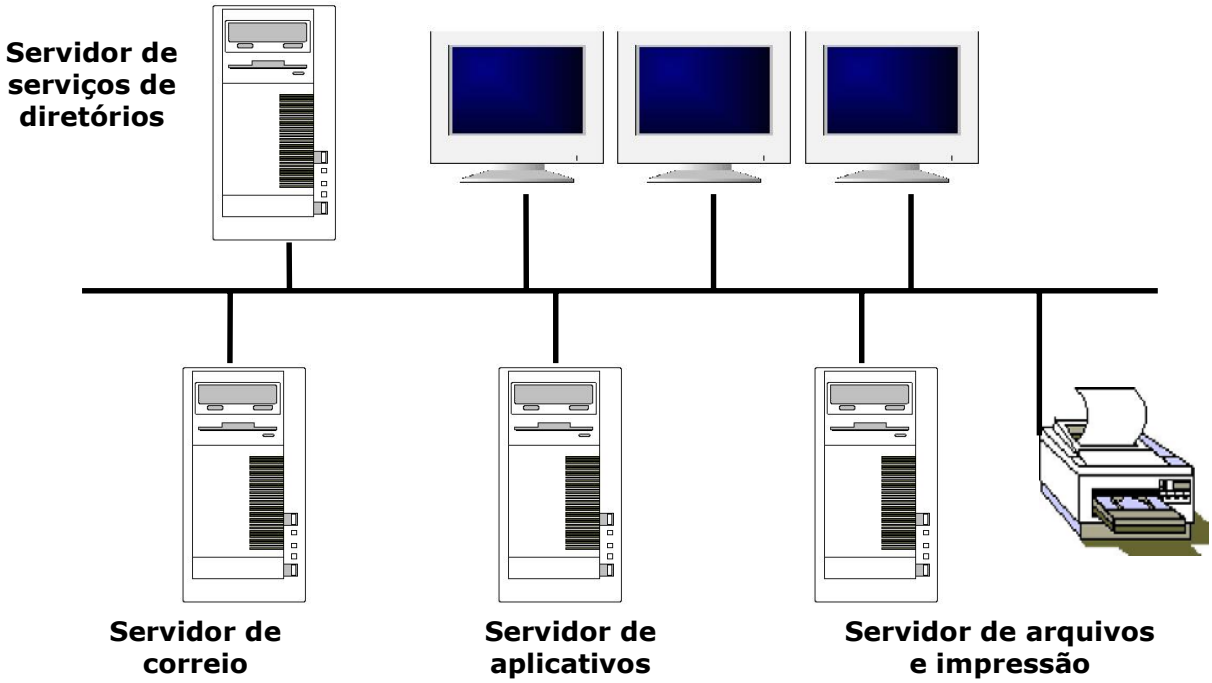
Os servidores de correio gerenciam mensagens eletrônicas entre os usuários da rede.

- **Servidores de fax:**

Os servidores de fax gerenciam o tráfego de fax para dentro e para fora da rede compartilhando uma ou mais placas de fax modem.

- **Servidores de comunicação:**

Os servidores de comunicação manipulam o fluxo de dados e as mensagens de correio eletrônico entre a própria rede do servidor e outras redes, computadores mainframe ou usuários remotos utilizando modems e linhas telefônicas para discar para o servidor.
Os servidores de serviços de pastas permitem aos usuários localizar, armazenar e dar segurança às informações na rede. O windows NT Server combina os computadores em grupos lógicos, chamados domínios, que permitem que qualquer usuário tenha acesso a todos os recursos da rede.



O planejamento para vários servidores se torna importante em uma rede expandida. O planejador deve considerar qualquer crescimento antecipado da rede, para que sua utilização não seja interrompida caso a função de um servidor específico precise ser modificada.

Vantagens da rede baseada em servidor

Compartilhando recursos:

Um servidor é projetado para fornecer acesso a muitos arquivos e impressoras, ao mesmo tempo em que mantém o desempenho e a segurança para o usuário. O compartilhamento de dados baseado em um servidor pode ser administrativo e controlado centralmente. Em geral, os recursos são localizados centralmente e são mais fáceis de localizar e suportar do que os recursos localizados em computadores aleatórios.

Segurança:

A segurança é, na maioria das vezes, o motivo principal para escolher uma abordagem de rede baseado em servidor, como uma rede do Windows NT Server, a segurança pode ser controlada por um administrador, que estabelece e aplica o plano a cada servidor na rede.

Backup:

Como os dados estão centralizados em um ou em poucos servidores, é mais fácil garantir que seja feito backup com agendamento regular.

Número de usuários:

Uma rede baseada em servidor pode dar suporte a milhares de usuários. Este tipo de rede, jamais poderia ser gerenciado como uma rede par a par, mas a monitoração atual e os utilitários de gerenciamento de rede possibilitam a operação de uma rede baseada em servidor por um grande número de usuários.

Planejando a segurança da rede

Em um ambiente de rede, é preciso que haja a segurança de que dados importantes permanecerão particulares, de modo que somente usuários autorizados possam acessá-los. É importante que não só informações importantes sejam protegidas, mas também as operações de rede. Toda rede deve ficar salvo de danos intencionais ou acidentais.

Todavia, um bom administrador de rede deve ter em mente que segurança requer equilíbrio. Uma rede não precisa ser tão segura a ponto de as pessoas terem dificuldade de utilizá-la a fim de realizar o seu trabalho. Embora as redes lidem com dados comerciais extremamente importantes e valiosos, a segurança de dados, às vezes, fica relegada ao segundo plano. Existem quatro grandes ameaças à segurança da rede:

- Acesso não autorizado,
- Alteração indevida de arquivos,
- Roubo,
- Dano intencional ou acidental.

Ainda que essas ameaças sejam concretas, a segurança de dados nem sempre é compreendida ou recebe o suporte que merece. Cabe ao administrador assegurar que a rede continue sendo uma ferramenta comercial segura e confiável, livre dessas ameaças.

Nível de segurança:

O nível e a extensão do sistema de segurança da rede dependem do tipo de ambiente no qual a rede funciona. Uma rede que armazena dados para um grande banco, por exemplo, requer mais segurança extensiva do que uma LAN que vincula os computadores de um laboratório de informática da sua escola.

Prevenção:

Os melhores planos de segurança de dados utilizam uma abordagem pró-ativa e preventiva. Evitando o acesso ou comportamentos não-autorizados, os dados permanecerão seguros. Um sistema baseado na prevenção requer que o administrador conheça as ferramentas e métodos disponíveis para manter os dados em segurança.

Autenticação:

Para poder acessar uma rede, você deve digitar um nome de usuário válido e uma senha válida. Como as senhas estão vinculadas as contas de usuários, um sistema de autenticação de senhas é sua primeira linha de segurança contra usuários não autorizados.

Modelos de segurança

Depois de aprender um pouco sobre segurança em redes, vamos ver como é possível o administrador da rede garantir que os recursos da mesma estarão salvos de acessos não-autorizados e de danos acidentais ou intencionais. Planos para conceder permissões e direitos de acesso a recursos da rede são primordiais para transformar a rede em uma ferramenta comercial de sucesso.

Foram desenvolvidos dois modelos diferentes para garantir que os dados e recursos de hardware permaneçam ilesos:

- Compartilhamento protegido por senha,
- Permissões de acesso.

Esses modelos também são denominados segurança em nível de compartilhamento (para compartilhamento protegido por senha) e segurança em nível de usuário (para permissões de acesso).

Compartilhamento protegido por senha:

A implementação de compartilhamento protegido por senha implica a atribuição de uma senha para cada recurso compartilhado. O acesso ao recurso compartilhado é concedido

quando o usuário digita a senha correta. Em muitos sistemas, os recursos podem ser compartilhados com diferentes tipos de permissões. Por exemplo, no Windows 98, diretórios (pastas) podem ser compartilhados como Somente Leitura, Completo ou Depende de Senha:

- Somente Leitura:

Se um compartilhamento é definido como somente leitura, os usuários têm acesso de leitura aos arquivos daquele diretório. Em outras palavras eles podem visualizar os documentos, copiá-los para sua máquina e imprimí-los, mas não podem alterar o documento original.

- Completo:

Com o acesso completo, os usuários têm acesso completo aos arquivos daquele diretório. Em outras palavras, eles podem visualizar, modificar, adicionar e excluir os arquivos do diretório compartilhado.

- Depende de Senha:

O acesso Depende de Senha implica estabelecer um compartilhamento que utiliza dois níveis de senhas: Acesso de leitura e Acesso Total. Os usuários que conhecem a senha de acesso de leitura tem acesso de leitura e aqueles que conhecem a senha de acesso total tem acesso total.

O sistema de compartilhamento protegido por senha é um método de segurança simples que permite a qualquer pessoa que conheça a senha obter acesso àquele recurso específico.

Permissões de acesso:

A segurança da permissão de acesso implica à atribuição de determinados direitos por usuário. Um usuário digita a sua senha ao efetuar logon na rede. O servidor valida essa combinação de nome de usuário e senha e a utiliza para conceder ou negar acesso a recursos compartilhados, confrontando o acesso ao recurso contra um banco de dados de usuário no servidor.

A segurança da permissão de acesso proporciona um nível mais elevado de controle sobre os direitos de acesso, bem como segurança de sistema mais rígida, do que o proporcionado por compartilhamento protegido por senha. É muito mais fácil uma pessoa dar a outra uma senha de impressora, como no caso de segurança em nível de compartilhamento. É bem menos provável que essa pessoa entregue a alguém sua senha pessoal.

Uma vez que a segurança em nível de usuário é mais ampla e pode determinar diversos níveis de segurança, este tipo de segurança é geralmente o modelo preferido em empresas maiores.

Segurança de recursos:

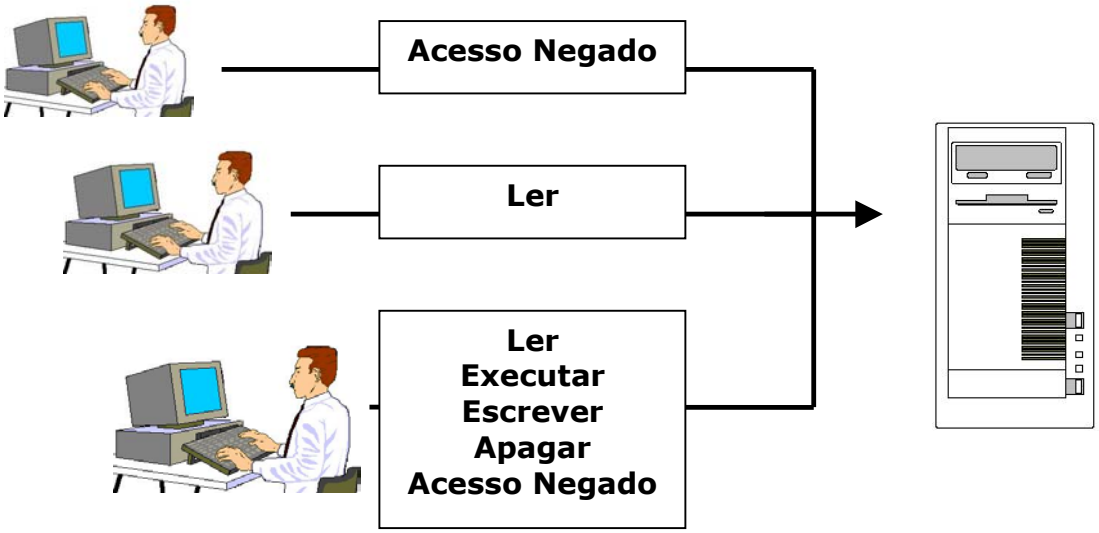
Depois que o usuário é autenticado e recebe permissão para entrar na rede, o sistema de segurança lhe concede acesso aos recursos apropriados. Usuários possuem senhas, ao passo que recursos possuem permissões. De certa maneira, cada recurso é protegido por uma "cerca de segurança". A "cerca" possui vários portões, através dos quais os usuários podem passar para acessar o recurso. Determinados portões permitem que usuários utilizem mais o recurso do que outros portões. Certos portões, em outras palavras, oferecem ao usuário mais privilégios com o recurso.

Cabe ao administrador determinar quais usuários poderão passar por quais portões. Um portão concede ao usuário acesso completo ou controle completo do recurso. Outro portão concede ao usuário somente acesso de leitura.

Cada recurso ou arquivo compartilhado é armazenado com uma lista de usuários ou grupos e suas respectivas permissões (portões). A lista a seguir contém permissões comuns de acesso atribuídas a diretórios ou arquivos compartilhados.

Obs: Diferentes sistemas operacionais de rede dão diferentes nomes a essas permissões. A tabela a seguir mostra algumas permissões típicas que podem ser estabelecidas nos diretórios do Windows NT Server.

Permissão	Funcionalidade
Leitura	Ler e copiar arquivos no diretório compartilhado
Execução	Executar os arquivos do diretório
Gravação	Criar novos arquivos no diretório
Exclusão	Excluir arquivos do diretório
Sem acesso	Impede que o usuário tenha acesso ao diretório, arquivo ou recurso.



Permissões para grupos:

Cabe ao administrador conceder a cada usuário as devidas permissões a cada recurso. A maneira mais eficiente de fazer isto é por meio da formação de grupos, principalmente em se tratando de uma grande empresa com um grande número de usuários e de recursos. O Windows NT Server utiliza o Gerenciador de arquivos para estabelecer permissões de grupo para diretórios e arquivos.

Permissões para grupos funcionam da mesma maneira que as permissões individuais. O administrador verifica quais permissões estão sendo solicitadas por cada conta e atribui as contas para um grupo apropriado. Está e a maneira de conceder permissões, ao invés de fazê-lo individualmente para cada conta.

É muito mais conveniente conceder usuários para grupos apropriados do que ter que conceder permissões individuais para cada usuário. Para ter um exemplo de como isto funciona, imagine o acesso dos professores de uma escola a arquivos dos estudantes. Os mediadores precisam ter acesso total a arquivos dos estudantes, enquanto os professores só precisariam somente de acesso de leitura aos arquivos. O administrador poderia criar um grupo denominado Mediadores, conceder a esse grupo permissões de acesso total aos arquivos dos estudantes. Um outro grupo chamado Professores, teria somente permissões de leitura no acesso dos arquivos dos estudantes. Os professores que tivessem acesso aos trabalhos, poderiam apenas visualizar, e não fazer alterações.

Cabeamento de redes

Nos últimos anos muito se tem discutido e falado sobre as novas tecnologias de hardware e software de rede disponíveis no mercado. Engana-se, porém quem pensa que estes produtos podem resolver todos os problemas de processamento da empresa. Infelizmente, o investimento em equipamentos envolve cifras elevadas, mas é preciso que se dê também atenção especial à estrutura de cabeamento, uma das peças chaves para o sucesso de ambientes distribuídos. Conforme pesquisas de órgãos internacionais, o cabeamento é hoje responsável por 80% das falhas físicas de uma rede, e oito em cada dez problemas detectados referem-se a cabos mal-instalados ou em estado precário.

Tipos de cabeamento:

Cabo Coaxial:

O primeiro tipo de cabeamento que surgiu no mercado foi o cabo coaxial. Há alguns anos, esse cabo era o que havia da mais avançado, sendo que a troca de dados entre dois computadores era coisa do futuro. Até hoje existem vários tipos de cabos coaxiais, cada um com suas características específicas. Alguns são melhores para transmissão em alta freqüência, outros têm atenuação mais baixa, e outros são imunes a ruídos e interferências. Os cabos coaxiais de alta qualidade não são maleáveis e são difíceis de instalar e os cabos de baixa qualidade podem ser inadequados para trafegar dados em alta velocidade e longas distâncias.

As maiorias dos sistemas de transmissão de banda base utilizam cabos de impedância com características de 50 Ohm, geralmente utilizados nas TVs a cabo e em redes de banda larga. Isso se deve ao fato de a transmissão em banda base sofrer menos reflexões, devido às capacidades introduzidas nas ligações ao cabo de 50 Ohm. Os cabos coaxiais possuem uma maior imunidade a ruídos eletromagnéticos de baixa freqüência e, por isto, eram os meios de transmissão mais usado em redes locais.

Par Trançado:

Com o passar do tempo, surgiu o cabeamento de par trançado. Esse tipo de cabo tornou-se muito usado devido à falta de flexibilidade de outros cabos e por causa da necessidade de se ter um meio físico que conseguisse uma taxa de transmissão alta e mais rápida. Os cabos de par trançado possuem dois ou mais fios entrelaçados em forma de espiral e, por isso, reduzem o ruído e mantém constantes as propriedades elétricas do meio, em todo seu comprimento.

O cabo par trançado é o meio de transmissão de menos custo por comprimento no mercado. A ligação de nós ao cabo é também extremamente simples e de baixo custo. Hoje em dia, o par trançado também está sendo usado com sucesso em conjunto com sistemas ATM para viabilizar o tráfego de dados a uma velocidade alta: 155 megabits/seg.

Fibra Óptica:

Quando se fala em tecnologia de ponta, o que existe de mais moderno são os cabos de fibra óptica. A transmissão de dados por fibra óptica é realizada pelo envio de um sinal de luz codificado, dentro do domínio de freqüência do infravermelho a uma velocidade de 10 a 15 MHz. O cabo óptico consiste em um filamento de sílica e de plástico, onde é feita a transmissão de luz. As fontes de transmissão de luz podem ser diodos emissores de luz (LED) ou laser semicondutores. O cabo óptico com transmissão de raio lazer é o mais eficiente em potência devido a sua espessura. Já os cabos com diodos emissores de luz são muito mais baratos, além de serem mais adaptáveis a temperatura ambiente e de terem um ciclo de vida maior que o de laser.

Portanto, quem deseja ter uma rede segura, preservar dados de qualquer tipo de ruído e ter velocidade na transmissão de dados, os cabos de fibra óptica são a melhor opção do mercado. O tipo de cabeamento mais usado em ambientes internos (LAN) é o par trançado, enquanto a fibra óptica é o mais usado em ambientes externos.

SEDU – Secretaria de Estado da Educação

ProInfo – Programa Estadual de Informática na Educação

NTE – Núcleo de Tecnologia Educacional Metropolitano

Esta apostila foi produzida por **Bruna de Carvalho**,
especialmente para o **ProInfo ES.**
brunacrv@bol.com.br