Apostila Rede

Professor Bruno Rafael de Oliveira Rodrigues

Um visão geral do protocolo TCP/IP

Para que os computadores de uma rede possam trocar informações entre si é necessário que todos os computadores adotem as mesmas regras para o envio e o recebimento de informações. Este conjunto de regras é conhecido como Protocolo de comunicação. Falando de outra maneira podemos afirmar: "Para que os computadores de uma rede possam trocar informações entre si é necessário que todos estejam utilizando o mesmo protocolo de comunicação". No protocolo de comunicação estão definidas todas as regras necessárias para que o computador de destino, "entenda" as informações no formato que foram enviadas pelo computador de origem. Dois computadores com diferentes protocolos instalados, não serão capazes de estabelecer uma comunicação e nem serão capazes de trocar informações.

Antes da popularização da Internet existiam diferentes protocolos sendo utilizados nas redes das empresas. Os mais utilizados eram os seguintes:

- TCP/IP
- NETBEUI
- IPX/SPX
- Apple Talk

Se colocarmos dois computadores ligados em rede, um com um protocolo, por exemplo o TCP/IP e o outro com um protocolo diferente, por exemplo NETBEUI, estes dois computadores não serão capazes de estabelecer comunicação e trocar informações entre si. Por exemplo, o computador com o protocolo NETBEUI instalado, não será capaz de acessar uma pasta ou uma Impressora compartilhada no computador com o protocolo TCP/IP instalado.

À medida que a Internet começou, a cada dia, tornar-se mais popular, com o aumento exponencial do número de usuários, o protocolo TCP/IP passou a tornar-se um padrão de fato, utilizando não só na Internet, como também nas redes internas das empresas, redes estas que começavam a ser conectadas à Internet. Como as redes internas precisavam conectar-se à Internet, tinham que usar o mesmo protocolo da Internet, ou seja: TCP/IP.

Dos principais Sistemas Operacionais do mercado, o UNIX sempre utilizou o protocolo TCP/IP como padrão. O Windows dá suporte ao protocolo TCP/IP desde as primeiras versões, porém, para o Windows, o TCP/IP somente tornou-se o protocolo padrão a partir do Windows 2000. Ser o protocolo padrão significa que o TCP/IP será instalado, automaticamente, durante a instalação do Sistema Operacional, se for detectada a presença de uma placa de rede. Até mesmo o Sistema Operacional Novell, que sempre foi baseado no protocolo IPX/SPX como protocolo padrão, passou a adotar o TCP/IP como padrão a partir da versão 5.0.

O que temos hoje, na prática, é a utilização do protocolo TCP/IP na esmagadora maioria das redes. Sendo a sua adoção cada vez maior. Como não poderia deixar de ser, o TCP/IP é o protocolo padrão do Windows 2000, Windows Server 2003, Windows XP e também do Windows Vista (a ser lançado em Fevereiro de 2007) e do Windows Longhorn Server (com lançamento previsto para o final de 2007). Se durante a instalação, o Windows detectar a presença de uma placa de rede, automaticamente será sugerida a instalação do protocolo TCP/IP.

Nota: Para pequenas redes, não conectadas à Internet, é recomendada a adoção do protocolo NETBEUI, devido a sua simplicidade de configuração. Porém esta é uma situação muito rara, pois dificilmente teremos uma rede isolada, sem conexão com a Internet ou com parceiros de negócios, como clientes e fornecedores.

Agora passaremos a estudar algumas características do protocolo TCP/IP. Veremos que cada equipamento que faz parte de uma rede baseada no TCP/IP tem alguns parâmetros de configuração que devem ser definidos, para que o equipamento possa comunicar-se com sucesso na rede e trocar informações com os demais equipamentos da rede.

Configurações do protocolo TCP/IP para um computador em rede

Quando utilizamos o protocolo TCP/IP como protocolo de comunicação em uma rede de computadores, temos alguns parâmetros que devem ser configurados em todos os equipamentos que fazem parte da rede (computadores, servidores, hubs, switchs, impressoras de rede, etc). Na Figura a seguir temos uma visão geral de uma pequena rede baseada no protocolo TCP/IP:

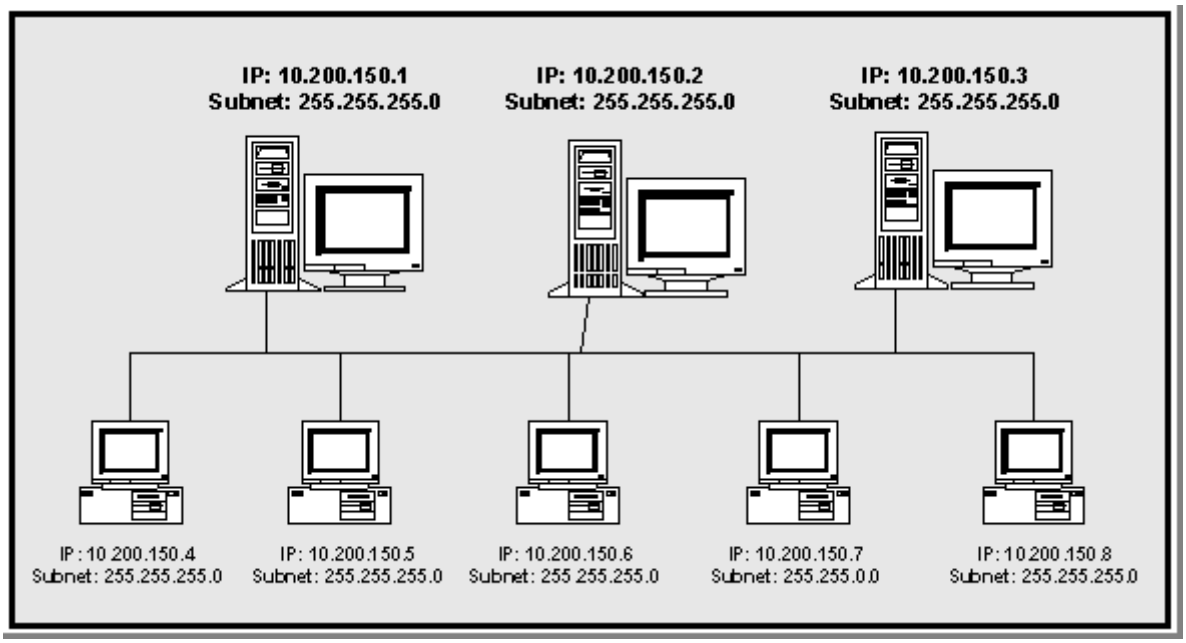


Figura - Uma rede baseada no protocolo TCP/IP.

No exemplo da Figura 1 temos uma rede local para uma pequena empresa. Esta rede local não está conectada a outras redes ou à Internet. Neste caso cada computador da rede precisa de, pelo menos, dois parâmetros configurados:

- Número IP
- Máscara de sub-rede

O Número IP é um número no seguinte formato:

x.y.z.w

ou seja, são quatro números separados por ponto. Não podem existir duas máquinas, com o mesmo número IP, dentro da mesma rede. Caso eu configure um novo equipamento com o mesmo número IP de uma máquina já existente, será gerado um conflito de Número IP e um dos equipamentos, muito provavelmente o novo equipamento que está sendo configurado, não conseguirá se comunicar com a rede. O valor máximo para cada um dos números (x, y, z ou w) é 255.

Uma parte do Número IP (1, 2 ou 3 dos 4 números) é a identificação da rede, a outra parte é a identificação da máquina dentro da rede. O que define quantos dos quatro números fazem parte da identificação da rede e quantos fazem parte da identificação da máquina é a máscara de sub-rede (subnet mask). Vamos considerar o exemplo de um dos computadores da rede da Figura 1:

- Número IP: 10.200.150.1
- Máscara de Sub-rede: 255.255.255.0

As três primeiras partes da máscara de sub-rede (subnet) iguais a 255 indicam que os três primeiros números representam a identificação da rede e o último número é a identificação do equipamento dentro da rede. Para o nosso exemplo teríamos a rede: 10.200.150, ou seja, todos os equipamentos do nosso exemplo fazem parte da rede 10.200.150 ou, em outras palavras, o número IP de todos os equipamentos da rede começam com 10.200.150.

Neste exemplo, onde estamos utilizando os três primeiros números para identificar a rede e somente o quarto número para identificar o equipamento, temos um limite de 254 equipamentos que podem ser ligados neste rede. Observe que são 254 e não 256, pois o primeiro número – 10.200.150.0 e o último número – 10.200.250.255 não podem ser utilizados como números IP de equipamentos de rede. O primeiro é o próprio número da rede: **10.200.150.0** e o último é o endereço de Broadcast: **10.200.150.255**. Ao enviar uma mensagem para o endereço de Broadcast, todas as máquinas da rede receberão a mensagemCom base no exposto podemos apresentar a seguinte definição:

"**Para se comunicar em uma rede baseada no protocolo TCP/IP, todo equipamento deve ter, pelo menos, um número IP e uma máscara de sub-rede, sendo que todos os equipamentos da rede devem ter a mesma máscara de sub-rede".**

No exemplo da figura anterior observe que o computador com o IP 10.200.150.7 está com uma máscara de sub-rede diferente da máscara de sub-rede dos demais computadores da rede. Este computador está com a máscara: 255.255.0.0 e os demais computadores da rede estão com a máscara de sub-rede 255.255.255.0. Neste caso é como se o computador com o IP 10.200.150.7 pertencesse a outra rede. Na prática o que irá acontecer é que este computador não conseguirá se comunicar com os demais computadores da rede, por ter uma máscara de sub-rede diferente dos demais. Este é um dos erros de configuração mais comuns. Se a máscara de sub-rede estiver incorreta, ou seja, diferente da máscara dos demais computadores da rede, o computador com a máscara de sub-rede incorreta não conseguirá comunicar-se na rede.

Na Tabela a seguir temos alguns exemplos de máscaras de sub-rede e do número máximo de equipamentos em cada uma das respectivas redes.

Tabela: Exemplos de máscara de sub-rede.

Máscara	**Número de equipamentos na rede**
255.255.255.0	254
255.255.0.0	65.534
255.0.0.0	16.777.214

Quando a rede está isolada, ou seja, não está conectada à Internet ou a outras redes externas, através de links de comunicação de dados, apenas o número IP e a máscara de sub-rede são suficientes para que os computadores possam se comunicar e trocar informações.

A conexão da rede local com outras redes é feita através de links de comunicação de dados. Para que essa comunicação seja possível é necessário um equipamento capaz de enviar informações para outras redes e receber informações destas redes. O equipamento utilizado para este fim é o Roteador. Todo pacote de informações que deve ser enviado para outras redes deve, obrigatoriamente, passar pelo Roteador. Todo pacote de informação que vem de outras redes também deve, obrigatoriamente, passar pelo Roteador. Como o Roteador é um equipamento de rede, este também terá um número IP. O número IP do roteador deve ser informado em todos os demais equipamentos que fazem parte da rede, para que estes equipamentos possam se comunicar com os redes externas. O número IP do Roteador é informado no parâmetro conhecido como Default Gateway. Na prática quando configuramos o parâmetro Default Gateway, estamos informando o número IP do Roteador.

Quando um computador da rede tenta se comunicar com outros computadores/servidores, o protocolo TCP/IP faz alguns cálculos utilizando o número IP do computador de origem, a máscara de sub-rede e o número IP do computador de destino (veremos estes cálculos em

detalhes nas próximas lições deste curso). Se, após feitas as contas, for concluído que os dois computadores fazem parte da mesma rede, os pacotes de informação são enviados para o barramento da rede local e o computador de destino captura e processa as informações que lhe foram enviadas. Se, após feitas as contas, for concluído que o computador de origem e o computador de destino, fazem parte de redes diferentes, os pacotes de informação são enviados para o Roteador (número IP configurado como Default Gateway) e o Roteador é o responsável por achar o caminho (a rota) para a rede de destino.

Com isso, para equipamentos que fazem parte de uma rede, baseada no protocolo TCP/IP e conectada a outras redes ou a Internet, devemos configurar, no mínimo, os seguintes parâmetros:

- Número IP
- Máscara de sub-rede
- Default Gateway

Em redes empresarias existem outros parâmetros que precisam ser configurados. Um dos parâmetros que deve ser informado é o número IP de um ou mais servidores DNS – Domain Name System. O DNS é o serviço responsável pela resolução de nomes. Toda a comunicação, em redes baseadas no protocolo TCP/IP é feita através do número IP. Por exemplo, quando vamos acessar o site: http://www.funam.com.br/, tem que haver uma maneira de encontrar o número IP do servidor onde fica hospedado o site. O serviço que localiza o número IP associado a um nome é conhecido como Servidor DNS. Por isso a necessidade de informarmos o número IP de pelo menos um servidor DNS, pois sem este serviço de resolução de nomes, muitos recursos da rede estarão indisponíveis, inclusive o acesso à Internet.

Existem aplicativos antigos que são baseados em um outro serviço de resolução de nomes conhecido como WINS – Windows Internet Name System. O Windows NT Server 4.0 utilizava intensamente o serviço WINS para a resolução de nomes. Com o Windows 2000 o serviço utilizado é o DNS, porém podem existir aplicações que ainda dependam do WINS. Nestes casos você terá que instalar e configurar um servidor WINS na sua rede e configurar o IP deste servidor em todos os equipamentos da rede.

Dica Importante: Em redes baseadas onde ainda existem clientes baseados em versões antigas do Windows, tais como o Windows 95, Windows 98 ou Windows Me, o WINS ainda é necessário. Sem o WINS, poderá haver erro no acesso a aos principais recursos da rede, tais como pastas e impressoras compartilhadas.

As configurações do protocolo TCP/IP podem ser definidas manualmente, isto é, configurando cada um dos equipamentos necessários com as informações do protocolo, como por exemplo o Número IP, Máscara de sub-rede, número IP do Default Gateway, número IP de um ou mais servidores DNS e assim por diante. Esta é uma solução razoável para pequenas redes, porém pode ser um problema para redes maiores, com um grande número de equipamentos conectados. Para redes maiores é recomendado o uso do serviço DHCP – Dynamic Host Configuration Protocol. O serviço DHCP pode ser instalado em um servidor com o Windows NT Server 4.0, Windows 2000 Server, Windows Server 2003 ou Windows Longhorn Server. Uma vez disponível e configurado, o serviço DHCP fornece, automaticamente, todos os parâmetros de configuração do protocolo TCP/IP para os equipamentos conectados à rede. Os parâmetros são fornecidos quando o equipamento é inicializado e podem ser renovados em períodos definidos pelo Administrador. Com o uso do DHCP uma série de procedimentos de configuração podem ser automatizados, o que facilita a vida do Administrador e elimina uma série de erros.

Dica Importante: Serviços tais como um Servidor DNS e um Servidor DHCP, só podem ser instalados em computadores com uma versão de Servidor do Windows, tais como o Windows NT Server 4.0, Windows 2000 Server, Windows Server 2003 ou Windows Longhorn Server. Estes serviços não estão disponíveis em versões Clientes do Windows, tais como o Windows 95/98/Me, Windows 2000 Professional, Windows XP Professional ou Windows Vista.

O uso do DHCP também é muito vantajoso quando são necessárias alterações no número IP dos servidores DNS ou WINS. Vamos imaginar uma rede com 1000 computadores e que não utiliza o DHCP, ou seja, os diversos parâmetros do protocolo TCP/IP são configurados manualmente em cada computador. Agora vamos imaginar que o número IP do servidor DNS foi alterado. Neste caso o Administrador e a sua equipe técnica terão que fazer a alteração do número IP do servidor DNS em todas as estações de trabalho da rede. Um serviço e tanto. Se esta mesma rede estiver utilizando o serviço DHCP, bastará alterar o número do servidor DNS, nas configurações do servidor DHCP. O novo número será fornecido para todas as estações da rede, automaticamente, na próxima vez que a estação for reinicializada. Muito mais simples e prático e, principalmente, com menor probabilidade de erros.

Você pode verificar, facilmente, as configurações do protocolo TCP/IP que estão definidas para o seu computador (Windows 2000, Windows XP ou Windows Vista). Para isso siga os seguintes passos:

1. Faça o logon com uma conta com permissão de Administrador.

2. Abra o Prompt de comando: Iniciar -> Programas -> Acessórios -> Prompt de comando.

3. Na janela do Prompt de comando digite o seguinte comando:

ipconfig/all

e pressione Enter.

4. Serão exibidas as diversas configurações do protocolo TCP/IP, conforme indicado a seguir, no exemplo obtido a partir de um dos meus computadores que eu uso na rede da minha casa:

```
Configuração de IP do Windows

        Nome do host . . . . . . . . . . . . :   servidor01
        Sufixo DNS primário. . . . . . . . . :   groza.com
        Tipo de nó . . . . . . . . . . . . . :   híbrido
        Roteamento de IP ativado . . . . . . :   não
        Proxy WINS ativado . . . . . . . . . :   não
        Lista de pesquisa de sufixo DNS. . . :   groza.com

Adaptador Ethernet Conexão local:

        Sufixo DNS específico de conexão  . :
        Descrição . . . . . . . . . . . . . . :  Realtek RTL8139 Family PCI Fast
                                                 Ethernet NIC
        Endereço físico . . . . . . . . . . . :  00-E0-7D-9F-6B-7C
        DHCP ativado. . . . . . . . . . . . . :  Não
        Endereço IP . . . . . . . . . . . . . :  10.204.123.2
        Máscara de sub-rede . . . . . . . . . :  255.255.255.0
        Gateway padrão. . . . . . . . . . . . :  10.204.123.100
        Servidores DNS. . . . . . . . . . . . :  10.204.123.1
                                                 10.204.123.3
        Servidor WINS primário. . . . . . . . :  10.204.123.1
```

O comando ipconfig exibe informações para as diversas interfaces de rede instaladas – placa de rede, modem, etc. No exemplo anterior temos uma única interface de rede instalada, a qual é relacionada com uma placa de rede Realtek RTL8139 Family PCI Fast Ethernet NIC. Observe que temos o número IP para dois servidores DNS e para um servidor WINS. Outra informação importante é o Endereço físico, mais conhecido como MAC-Address ou endereço da placa. O MAC-Address é um número que identifica a placa de rede. Os seis primeiros números/letras são uma identificação do fabricante da placa e os seis últimos uma identificação da placa. Não existem duas placas com o mesmo MAC-Address, ou seja, este endereço é único para cada placa de rede.

No exemplo da listagem a seguir, temos um computador com duas interfaces de rede. Uma das interfaces é ligada a placa de rede (Realtek RTL8029(AS) PCI Ethernet Adapter), a qual conecta o computador a rede local. A outra interface é ligada ao fax-modem (WAN (PPP/SLIP) Interface), o qual conecta o computador à Internet. Para o protocolo TCP/IP a conexão via Fax modem aparece como se fosse mais uma interface de rede, conforme pode ser conferido na listagem a seguir:

```
Configuração de IP do Windows XP

        Nome do host . . . . . . . . . . . . :   servidor
        Sufixo DNS primário. . . . . . . . . :   groza.com
        Tipo de nó . . . . . . . . . . . . . :   Híbrida

        Roteamento de IP ativado . . . . . . :   Não
        Proxy WINS ativado . . . . . . . . . :   Não
        Lista de pesquisa de sufixo DNS. . . :   groza.com

    Ethernet adaptador Conexão de rede local:

        Sufixo DNS específico de conexão . . :   groza.com
        Descrição. . . . . . . . . . . . . . :   Realtek RTL8029(AS) PCI
                                                 Ethernet Adapter
        Endereço físico. . . . . . . . . . . :   00-00-21-CE-01-11
        DHCP ativado . . . . . . . . . . . . :   Não
        Endereço IP. . . . . . . . . . . . . :   10.204.123.1
        Máscara de sub-rede. . . . . . . . . :   255.255.255.0
        Gateway padrão . . . . . . . . . . . :
        Servidores DNS . . . . . . . . . . . :   10.204.123.1
        Servidor WINS primário . . . . . . . :   10.204.123.1

    PPP adaptador TERRAPREMIUM:

        Sufixo DNS específico de conexão . . :
        Descrição. . . . . . . . . . . . . . :   WAN (PPP/SLIP) Interface
        Endereço físico. . . . . . . . . . . :   00-53-45-00-00-00
        DHCP ativado . . . . . . . . . . . . :   Não
        Endereço IP. . . . . . . . . . . . . :   200.176.166.146
        Máscara de sub-rede. . . . . . . . . :   255.255.255.255
        Gateway padrão . . . . . . . . . . . :   200.176.166.146
        Servidores DNS . . . . . . . . . . . :   200.176.2.10
                                                 200.177.250.10
        NetBIOS por Tcpip. . . . . . . . . . :   Desativado
```

Entendendo as máscaras de sub-rede

Além do endereço IP propriamente dito, é necessário fornecer também a máscara de sub-rede, ou "subnet mask" na configuração da rede. Ao contrário do endereço IP, que é formado por valores entre 0 e 255, a máscara de sub-rede é normalmente formada por apenas dois valores: 0 e 255, como em 255.255.0.0 ou 255.0.0.0, onde o valor 255 indica a parte endereço IP referente à rede, e o valor 0 indica a parte endereço IP referente ao host.

A máscara de rede padrão acompanha a classe do endereço IP: em um endereço de classe A, a máscara será 255.0.0.0, indicando que o primeiro octeto se refere à rede e os três últimos ao host. Em um endereço classe B, a máscara padrão será 255.255.0.0, onde os dois primeiros octetos referem-se à rede e os dois últimos ao host e, em um endereço classe C, a máscara padrão será 255.255.255.0, onde apenas o último octeto refere-se ao host.

Ex. de endereço IP	Classe do endereço	Parte referente à rede	Parte referente ao host	Máscara de sub-rede padrão
98.158.201.128	Classe A	98.	158.201.128	255.0.0.0 (rede.host.host.host)
158.208.189.45	Classe B	158.208.	189.45	255.255.0.0 (rede.rede.host.host)
208.183.34.89	Classe C	208.183.34.	89	255.255.255.0 (rede.rede.rede.host)

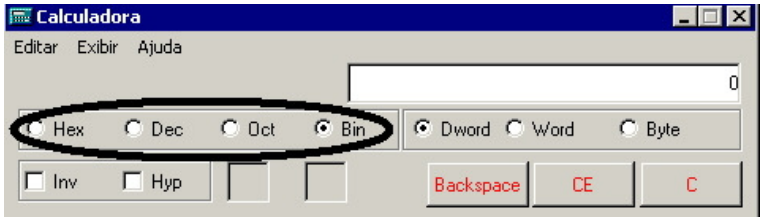
Mas, é possível usar máscaras diferentes para utilizar os endereços IP disponíveis de formas diferentes das padrão. O importante, neste caso, é que todos os micros da rede sejam configurados com a mesma máscara, caso contrário poderão não conseguir comunicar-se, pois pensarão estar conectados a redes diferentes.

Um exemplo comum é o uso da faixa de endereços 192.168.0.x para redes locais. Originalmente, esta é uma faixa de endereços classe C e por isso a máscara padrão é 255.255.255.0. Mesmo assim, muita gente prefere usar a máscara 255.255.0.0, o que permite mudar os dois últimos octetos (192.168.x.x). Neste caso, você poderia ter dois micros, um com o IP "192.168.2.45" e o outro com o IP "192.168.34.65" e ambos se enxergariam perfeitamente, pois entenderiam que fazem parte da mesma rede. Não existe problema em fazer isso, desde que você use a mesma máscara em todos os micros da rede.

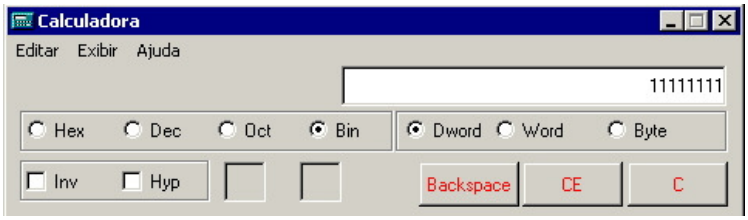
Até agora vimos apenas máscaras de sub-rede simples. Porém, o recurso mais refinado das máscaras de sub-rede é quebrar um octeto do endereço IP em duas partes, fazendo com que tenhamos dentro de um mesmo octeto uma parte que representa a rede e outra que representa o host. Chegamos às máscaras de tamanho variável (VLSM).

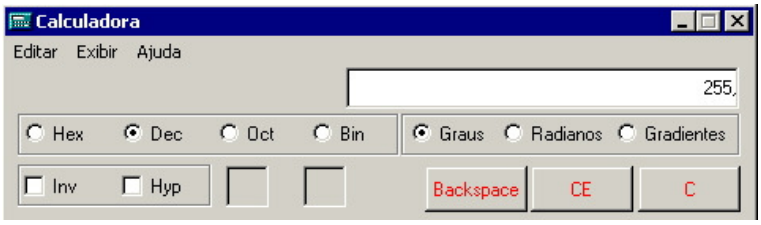
Este conceito é um pouco complicado, mas, em compensação, pouca gente sabe usar este recurso, por isso vale à pena fazer um certo esforço para aprender.

Configurando uma máscara complexa, precisaremos configurar o endereço IP usando números binários e não decimais. Para converter um número decimal em um número binário, você pode usar a calculadora do Windows ou o Kcalc no Linux. Configure a calculadora para o modo científico (exibir/científica) e verá que do lado esquerdo aparecerá um menu de seleção permitindo (entre outros) escolher entre decimal (dec) e binário (bin).



Configure a calculadora para binário e digite o número 11111111, mude a opção da calculadora para decimal (dec) e a calculadora mostrará o número 255, que é o seu correspondente em decimal. Tente de novo agora com o binário 00000000 e terá o número decimal 0.





Veja que 0 e 255 são exatamente os números que usamos nas máscaras de sub-rede simples. O número decimal 255 (equivalente a 11111111) indica que todos os 8 números binários do octeto se referem ao host, enquanto o decimal 0 (correspondente a 00000000) indica que todos os 8 binários do octeto se referem ao host. Numa rede com máscara 255.255.255.0 temos:

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

As máscaras de tamanho variável permitem dividir uma única faixa de endereços (seja de classe A, B ou C) em duas ou mais redes distintas, cada uma recebendo parte dos endereços disponíveis. Imagine o caso de um pequeno provedor de acesso, que possui um backbone com uma faixa de endereços de classe C e precisa dividi-lo entre dois clientes, onde cada um deles deve ter uma faixa completa de endereços.

O backbone do provedor utiliza a faixa de endereços 203.107.171.x onde o 203.107.171 é o endereço da rede e o "x" é a faixa de endereços de que eles dispõem para endereçar os micros das duas empresas. Como endereçar ambas as redes, se não é possível alterar o "203.107.171" que é a parte do seu endereço que se refere à rede?

Este problema poderia ser resolvido usando uma máscara de sub-rede complexa. Veja que podemos alterar apenas dos últimos 8 bits do endereço IP:

Decimal:	**203**	**107**	**171**	**x**
Binário:	**11001011**	**11010110**	**10101011**	**????????**

Usando uma máscara 255.255.255.0, são reservados todos os 8 bits para o endereçamento dos hosts, e não sobra nada para diferenciar as duas redes. Usando uma máscara complexa,

é possível "quebrar" os 8 bits do octeto em duas partes, usando a primeira para diferenciar as duas redes e a segunda para endereçar os hosts:

Decimal:	**203**	**107**	**171**	**x**
Binário:	**11001011**	**11010110**	**10101011**	**???? ????**
	rede	**rede**	**rede**	**rede host**

Para tanto, ao invés de usar a máscara de sub-rede 255.255.255.0 que, como vimos, reservaria todos os 8 bits para o endereçamento do host, usaremos uma máscara 255.255.255.240 (corresponde ao binário 11111111.111111.11111111.11110000). Veja que numa máscara de sub-rede os números binários "1" referem-se à rede e os números "0" referem-se ao host. Na máscara 255.255.255.240 temos exatamente esta divisão: os 4 primeiros binários do último octeto são positivos e os quatro últimos são negativos:

Decimal:	**255**	**255**	**255**	**240**
Binário:	**11111111**	**11111111**	**11111111**	**1111 0000**
	rede	**rede**	**rede**	**rede host**

Temos agora o último octeto dividido em dois endereços binários de 4 bits cada. Cada um dos dois grupos representa agora um endereço distinto, e deve ser configurado independentemente. Como fazer isso? Veja que 4 bits permitem 16 combinações diferentes. Se você converter o número 15 em binário terá "1111" e, se converter o decimal 0, terá "0000". Se converter o decimal 11 terá "1011" e assim por diante.

Neste caso, é possível usar endereços de 1 a 14 para identificar os hosts e as redes separadas. Note que os endereços 0 e 15 não podem ser usados, pois assim como os endereços 0 e 255, eles são reservados para pacotes de broadcast:

Decimal:	**203**	**107**	**171**	**12 _ 14**
Binário:	**11111111**	**11111111**	**11111111**	**1100 1110**
	rede	**rede**	**rede**	**rede host**

Estabeleça um endereço de rede para cada uma das duas sub-redes disponíveis e um endereço diferente para cada micro da rede, mantendo a formatação do exemplo anterior. Por enquanto, apenas anote em um papel os endereços escolhidos, junto como seu correspondente em binários.

Na hora de configurar o endereço IP nas estações, configure primeiro a máscara de sub-rede como 255.255.255.240 e, em seguida, converta os endereços binários em decimais, para ter o endereço IP de cada estação. No exemplo da ilustração anterior, havíamos estabelecido o endereço 12 para a rede e o endereço 14 para a estação; 12 corresponde a "1100" e 14 corresponde a "1110". Juntando os dois temos "11001110", que corresponde ao decimal "206". O endereço IP da estação será então 203.107.171.206, com máscara 255.255.255.240.

Se tivesse escolhido o endereço 10 para a rede e o endereço 8 para a estação, teríamos "10101000" que corresponde ao decimal 168. Neste caso, o endereço IP da estação seria 203.107.171.168.

Neste primeiro exemplo dividimos a faixa de endereços em 14 redes distintas, cada uma com 14 endereços. Isso permitiria que o provedor de acesso do exemplo fornecesse links para até 14 empresas diferentes, desde que cada uma não precisasse de mais de 14 endereços. É possível criar diferentes combinações, reservando números diferentes de bits para a rede e o host:

Máscara	Bits da rede	Bits do host	Número de redes	Número de hosts
255.255.255.240	1111	0000	14 endereços (de 1 a 14)	14 endereços (de 1 a 14)
255.255.255.192	11	000000	2 endereços (2 e 3)	62 endereços (de 1 a 62)
255.255.255.224	111	00000	6 endereços (de 1 a 6)	30 endereços (de 1 a 30)
255.255.255.248	11111	000	30 endereços (de 1 a 30)	6 endereços (de 1 a 6)
255.255.255.252	111111	00	62 endereços (de 1 a 62)	2 endereços (de 2 e 3)

Em qualquer um dos casos, para obter o endereço IP basta converter os dois endereços (rede e estação) para binário, "juntar" os bits e converter o octeto para decimal.

Usando uma máscara de sub-rede 192, por exemplo, e estabelecendo o endereço 2 (ou "10" em binário) para a rede e 47 (ou "101111" em binário) para o host, juntaríamos ambos os binários obtendo o octeto "10101111" que corresponde ao decimal "175".

Se usássemos a máscara de sub-rede 248, estabelecendo o endereço 17 (binário "10001") para a rede e o endereço 5 (binário "101") para o host, obteríamos o octeto "10001101" que corresponde ao decimal "141".

Claro que as instruções acima valem apenas para quando você quiser conectar vários micros à web, usando uma faixa de endereços válidos, como no caso de uma empresa que precisa colocar no ar vários servidores, ou de uma empresa de hospedagem que aluga servidores dedicados. Caso você queira apenas compartilhar a conexão entre vários PCs, você precisará de apenas um endereço IP válido.

O papel do Roteador em uma rede de computadores

Vimos que a máscara de sub-rede é utilizada para determinar qual "parte" do endereço IP representa o número da Rede e qual parte representa o número da máquina dentro da rede. A máscara de sub-rede também foi utilizada na definição original das classes de endereço IP. Em cada classe existe um determinado número de redes possíveis e, em cada rede, um número máximo de máquinas. Com base na máscara de sub-rede o protocolo TCP/IP determina se o computador de origem e o de destino estão na mesma rede local. Com base em cálculos binários, o TCP/IP pode chegar a dois resultados distintos:

- **O computador de origem e o computador de destino estão na mesma rede local:** Neste caso os dados são enviados para o barramento da rede local. Todos os computadores da rede recebem os dados. Ao receber os dados cada computador analisa o campo Número IP do destinatário. Se o IP do destinatário for igual ao IP do computador, os dados são capturados e processados pelo sistema, caso contrário são simplesmente descartados. Observe que com este procedimento, apenas o computador de destino é que efetivamente processa os dados para ele enviados, os demais computadores simplesmente descartam os dados.

- **O computador de origem e de destino não estão na mesma rede local:** Neste caso os dados são enviados o equipamento com o número IP configurado no parâmetro Default Gateway (Gateway Padrão). Ou seja, se após os cálculos baseados na máscara de sub-rede, o TCP/IP chegar a conclusão que o computador

de destino e o computador de origem não fazem parte da mesma rede local, os dados são enviados para o Default Gateway, o qual será encarregado de encontrar um caminho para enviar os dados até o computador de destino. Esse "encontrar o caminho" é tecnicamente conhecido como Rotear os dados até o destino (ou melhor, rotear os dados até a rede do computador de destino). O responsável por "Rotear" os dados é o equipamento que atua como Default Gateway o qual é conhecido como Roteador. Com isso fica fácil entender o papel do Roteador:

"O Roteador é o responsável por encontrar um caminho entre a rede onde está o computador que enviou os dados (computador de origem) e a rede onde está o computador que irá receber os dados (computador de destino)."

Quando ocorre um problema com o Roteador, tornando-o indisponível, você consegue se comunicar normalmente com os demais computadores da sua rede local, porém não conseguirá comunicação com outras redes de computadores, como por exemplo a Internet.

Como Verificar o Default Gateway no Windows 2000/Windos XP ou Windows Server 2003?

Você pode verificar as configurações do TCP/IP de um computador com o Windows 2000, Windows Server 2003 ou Windows XP de duas maneiras distintas: Acessando as propriedades da interface de rede ou com o comando ipconfig. A seguir descrevo estas duas maneiras:

Verificando as configurações do TCP/IP usando a interface gráfica:

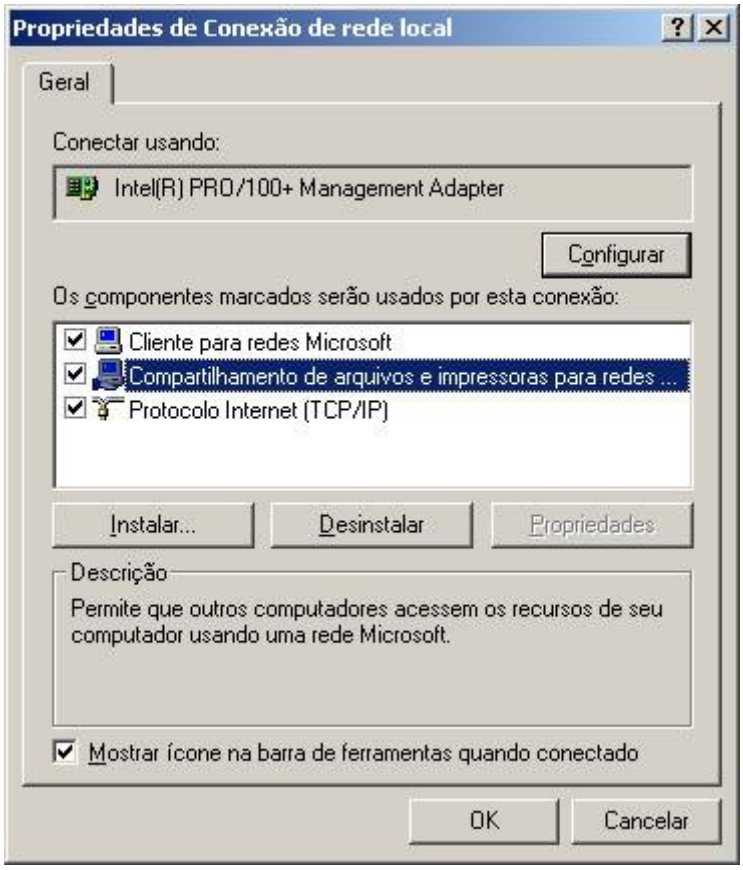
1. Clique com o botão direito do mouse no ícone Meus locais de rede, na Área de trabalho.

2. No menu que é exibido clique na opção Propriedades.

3. Será exibida a janela Conexões dial-up e de rede. Nessa janela é exibido um ícone para cada conexão disponível. Por exemplo, se o seu computador estiver conectado a uma rede local e também tiver uma conexão via Modem, será exibido um ícone para cada conexão. Nesta janela também está disponível o ícone "Fazer nova conexão". Com esse ícone você pode criar novas conexões. Na figura a seguir temos um exemplo onde está disponível apenas uma conexão de rede local:

4. Clique com o botão direito do mouse no ícone "Conexão de rede local". No menu de opções que é exibido clique em Propriedades.

5. Será exibida a janela de Propriedades da conexão de rede local, conforme indicado na figura a seguir:



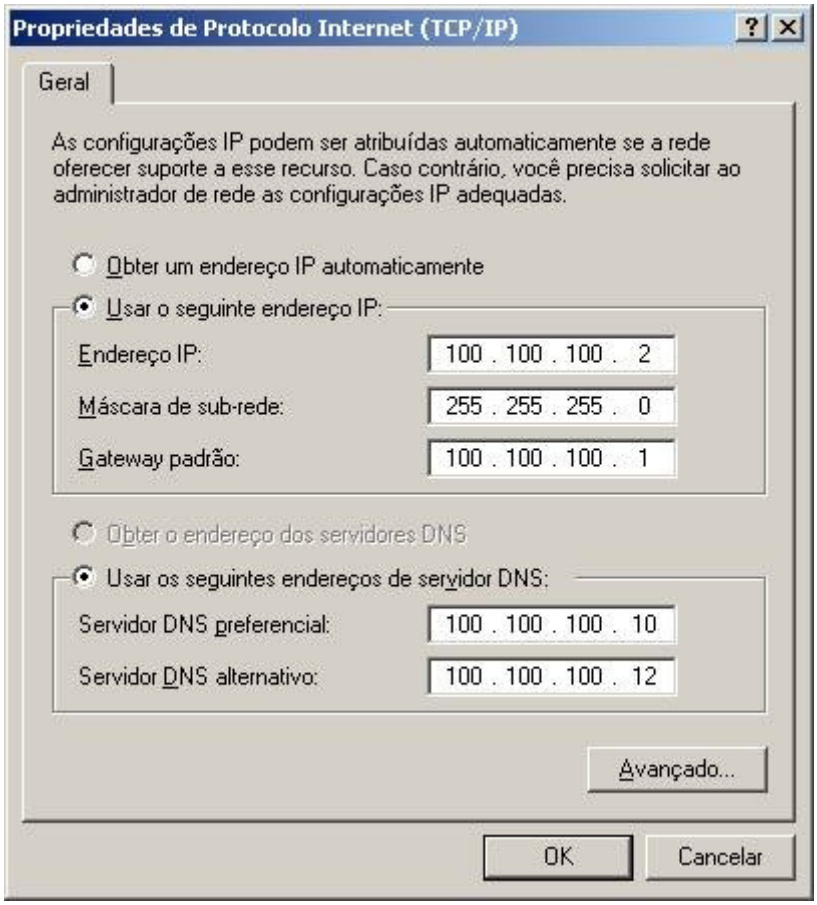
6. Clique na opção Protocolo Internet (TCP/IP) e depois clique no botão Propriedades.

7. A janela de propriedades do TCP/IP será exibida, conforme indicado na próxima figura. Nesta janela são exibidas informações sobre o número IP do computador, a máscara de sub-rede, o Gateway padrão e o número IP dos servidores DNS primário e secundário. Se a opção obter um endereço IP automaticamente estiver marcada, o computador tentará obter todas estas configurações a partir de um servidor DHCP, durante a inicialização do Windows. Neste caso as informações sobre as configurações TCP/IP, inclusive o número IP do Roteador (Gateway Padrão), somente poderão ser obtidas através do comando ipconfig, conforme descrevo logo a seguir.

8. Clique em OK para fechar a janela de Propriedades do protocolo TCP/IP.

9. Você estará de volta a janela de Propriedades da conexão de rede local. Clique em OK para fechá-la.

10. Você estará de volta à janela Conexões dial-up e de rede. Feche-a.



Verificando as configurações do TCP/IP usando o comando ipconfig

Para verificar as configurações do TCP/IP, utilizando o comando ipconfig, siga os seguintes passos:

1. Abra o Prompt de comando: Iniciar -> Programas -> Acessórios -> Prompt de comando.

2. Digite o comando ipconfig/all

3. Serão listadas as configurações do TCP/IP, conforme exemplo da listagem a seguir, onde uma das informações exibidas é o número IP do Gateway Padrão (Default Gateway):

Configuração de IP do Windows 2000

```
Nome do host . . . . . :          MICRO080
Sufixo DNS primário. . . . . :    abc.com.br
Tipo de nó . . . . . :            Híbrida
Roteamento de IP ativado . . . . . : Não
Proxy WINS ativado . . . . . :    Não
Lista de pesquisa de sufixo DNS. . : abc.com.br
                                  vendas.abc.com.br
                                  finan.abc.com.br
```

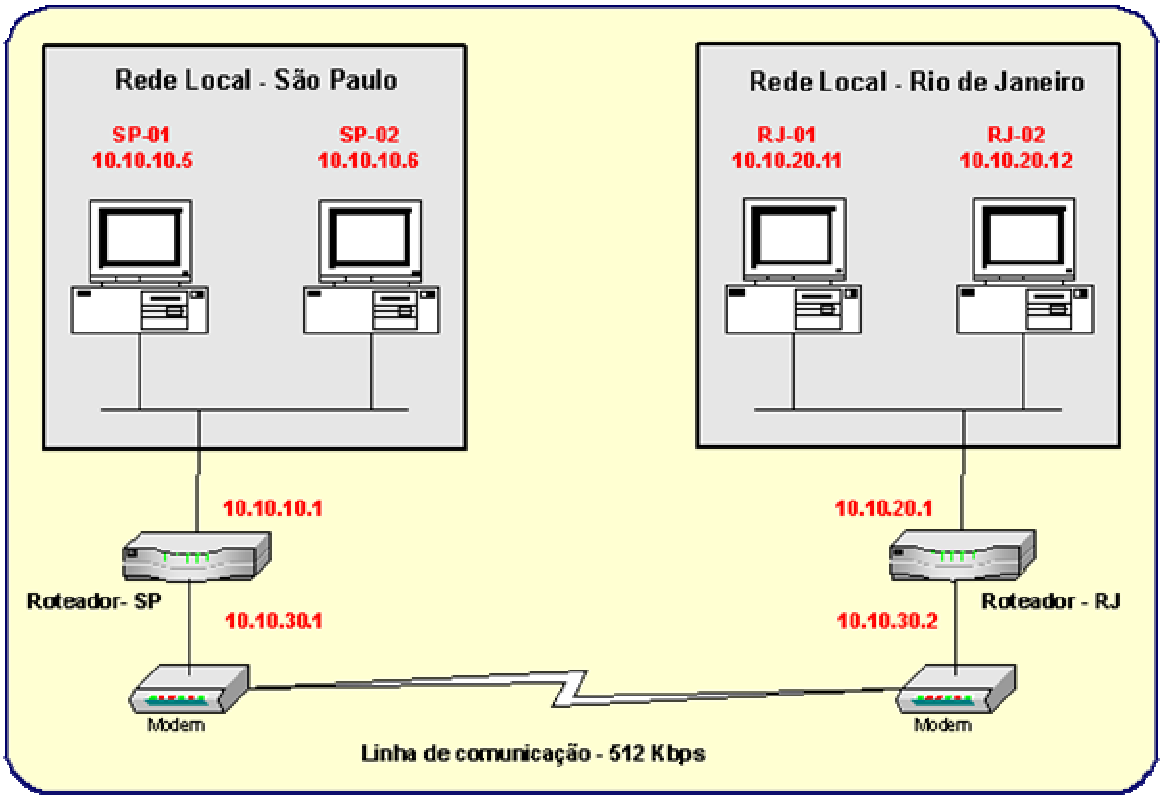
Ethernet adaptador Conexão de rede local:

```
Sufixo DNS específico de conexão . :    abc.com.br
Descrição. . . . . :                    3COM - AX 25
Endereço físico. . . . . :              04-02-B3-92-82-CA
```

```
DHCP ativado . . . . . :          Sim
Configuração automática ativada. . :          Sim
Endereço IP. . . . . :          10.10.10.222
Máscara de sub-rede. . . . . :          255.255.0.0
Gateway padrão . . . . . :          10.10.10.1
Servidor DHCP. . . . . :          10.10.10.2
Servidores DNS . . . . . :          10.10.10.2
Servidor WINS primário . . . . . :          10.10.10.2
```

Explicando Roteamento – um exemplo prático

Vou iniciar a explicação sobre como o roteamento funciona, através da análise de um exemplos simples. Vamos imaginar a situação de uma empresa que tem a matriz em SP e uma filial no RJ. O objetivo é conectar a rede local da matriz em SP com a rede local da filial no RJ, para permitir a troca de mensagens e documentos entre os dois escritórios. Nesta situação o primeiro passo é contratar um link de comunicação entre os dois escritórios. Em cada escritório deve ser instalado um Roteador. E finalmente os roteadores devem ser configurados para que seja possível a troca de informações entre as duas redes. Na figura a seguir temos a ilustração desta pequena rede de longa distância (WAN). Em seguida vamos explicar como funciona o roteamento entre as duas redes:



Nesta pequena rede temos um exemplo simples de roteamento, mas muito a explicar. Então vamos ao trabalho.

Como está configurado o endereçamento das redes locais e dos roteadores?

- **Rede de SP:** Esta rede utiliza um esquema de endereçamento 10.10.10.0, com máscara de sub-rede 255.255.255.0. Observe que embora, teoricamente, seria uma rede Classe A, estamos utilizando uma máscara de sub-rede classe C. Na prática, é uma rede Classe C, pois, na prática, consideramos a Máscara de Sub-rede como critério para definir a classe de rede e não as faixas teóricas.

- **Rede de RJ:** Esta rede utiliza um esquema de endereçamento 10.10.20.0, com máscara de sub-rede 255.255.255.0. Observe que embora, teoricamente, seria uma rede Classe A, estamos utilizando uma máscara de sub-rede classe C.
- **Roteadores:** Cada roteador possui duas interfaces. Uma é a chamada interface de LAN (rede local), a qual conecta o roteador com a rede local. A outra é a interface de WAN (rede de longa distância), a qual conecta o roteador com o link de dados. Na interface de rede local, o roteador deve ter um endereço IP da rede interna. No roteador de SP, o endereço é 10.10.10.1. Não é obrigatório, mas é um padrão normalmente adotado, utilizar o primeiro endereço da rede para o Roteador. No roteador do RJ, o endereço é 10.10.20.1

- **Rede dos roteadores:** Para que as interfaces externas dos roteadores possam se comunicar, eles devem fazer parte de uma mesma rede, isto é, devem compartilhar um esquema de endereçamento comum. As interfaces externas dos roteadores (interfaces WAN), fazem parte da rede 10.10.30.0, com máscara de sub-rede 255.255.255.0.

- **Na verdade - 3 redes**: Com isso temos, na prática três redes, conforme resumido a seguir:

    - **SP:** 10.10.**10**.0/255.255.255.0
    - **RJ:** 10.10.**20**.0/255.255.255.0
    - **Interfaces WAN dos Roteadores:** 10.10.**30**.0/255.255.255.0

- Na prática é como se a rede 10.10.30.0 fosse uma "ponte" entre as duas outras redes.

Como é feita a interligação entre as duas redes?

Vou utilizar um exemplo prático, para mostrar como é feito o roteamento entre as duas redes.

Exemplo: Vamos analisar como é feito o roteamento, quando um computador da rede em SP, precisa acessar informações de um computador da rede no RJ. O computador SP-01 (10.10.10.5), precisa acessar um arquivo que está em uma pasta compartilhada do computador RJ-02 (10.10.20.12). Como é feito o roteamento, de tal maneira que estes dois computadores possam trocar informações? Acompanhe os passos descritos a seguir:

1. O computador SP-01 é o computador de origem e o computador RJ-02 é o computador de destino. A primeira ação do TCP/IP é fazer os cálculos para verificar se os dois computadores estão na mesma rede. Os seguintes dados são utilizados para realização destes cálculos:

- SP-01: 10.10.10.5/255.255.255.0
- RJ-02: 10.10.20.12/255.255.255.0

2. Feitos os cálculos, o TCP/IP chega a conclusão de que os dois computadores pertencem a redes diferentes: SP-01 pertence a rede 10.10.10.0 e RJ-02 pertence a rede 10.10.20.0.

3. Como os computadores pertencem a redes diferentes, os dados devem ser enviados para o Roteador.

4. No roteador de SP chega o pacote de informações com o IP de destino: 10.10.20.12. O roteador precisa consultar a sua tabela de roteamento e verificar se ele conhece um caminho para a rede 10.10.20.0.

5. O roteador de SP tem, em sua tabela de roteamento, a informação de que pacotes para a rede 10.10.20.0 devem ser encaminhados pela interface 10.10.30.1. É isso que ele faz, ou seja, encaminha os pacotes através da interface de WAN: 10.10.30.1.

6. Os pacotes de dados chegam na interface 10.10.30.1 e são enviados, através do link de comunicação, para a interface 10.10.30.2, do roteador do RJ.

7. No roteador do RJ chega o pacote de informações com o IP de destino: 10.10.20.12. O roteador precisa consultar a sua tabela de roteamento e verificar se ele conhece um caminho para a rede 10.10.20.0.

8. O roteador do RJ tem, em sua tabela de roteamento, a informação de que pacotes para a rede 10.10.20.0 devem ser encaminhados pela interface de LAN 10.10.20.1, que é a interface que conecta o roteador a rede local 10.10.20.1. O pacote é enviado, através da interface 10.10.20.1, para o barramento da rede local. Todos os computadores recebem os pacotes de dados e os descartam, com exceção do computador 10.10.20.12 que é o computador de destino.

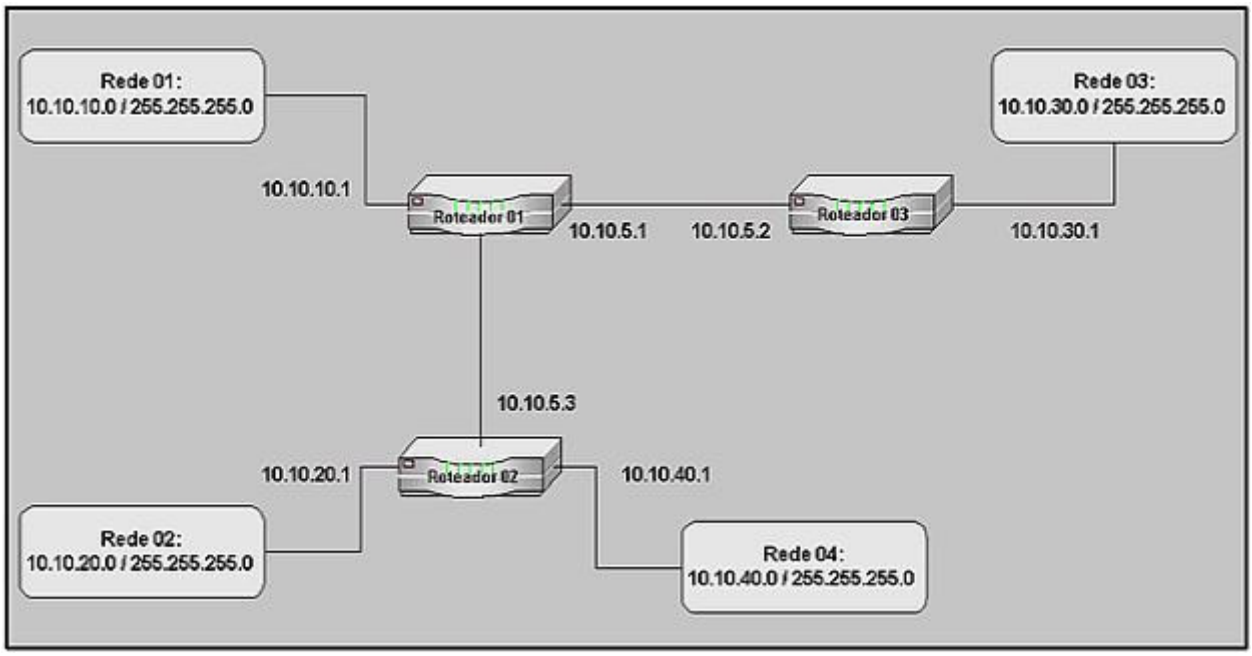
9. Para que a resposta possa ir do computador RJ-02 de volta para o computador SP-01, um caminho precisa ser encontrado, para que os pacotes de dados possam ser roteados do RJ para SP. Para tal todo o processo é executado novamente, até que a resposta chegue ao computador SP-01.

10. A chave toda para o processo de roteamento é o software presente nos roteadores, o qual atua com base em tabelas de roteamento.

Mais um exemplo de roteamento

Neste item vou analisar mais alguns exemplos de roteamento e falar sobre tabela de roteamento.

Exemplo 01: Considere a rede indicada no diagrama da Figura a seguir:



Primeiro alguns comentários sobre a WAN apresentada na Figura:

1. A WAN é formada pela conexão de quatro redes locais, com as seguintes características:

Rede	Número da rede	Máscara de sub-rede
01	10.10.10.0	255.255.255.0
02	10.10.20.0	255.255.255.0
03	10.10.30.0	255.255.255.0
04	10.10.40.0	255.255.255.0

2. Existe uma quinta rede que é a rede formada pelas interfaces de WAN dos roteadores. Este rede apresenta as seguintes características:

Rede	Número da rede	Máscara de sub-rede
Roteadores	10.10.5.0	255.255.255.0

3. Existem três roteadores fazendo a conexão das quatro redes existentes. Com as configurações apresentadas, qualquer rede é capaz de se comunicar com qualquer outra rede da WAN.

4. Existem pontos únicos de falha. Por exemplo, se o Roteador 03 apresentar problemas, a Rede 03 ficará completamente isolada das demais redes. Se o Roteador 02 apresentar problemas, as Redes 02 e 04 ficarão isoladas das demais redes e também isoladas entre si.

5. As redes 02 e 04 estão diretamente conectadas ao Roteador 02. Cada rede em uma interface do roteador. Este pode ser um exemplo de um prédio com duas redes locais, as quais são conectadas através do roteador. Neste caso, o papel do Roteador 02 é conectar as redes 02 e 04 entre si e estas redes com o restante da WAN.

6. A interface de conexão do roteador com a rede local utiliza sempre o primeiro número IP da faixa disponível (10.10.10.1, 10.10.20.1 e assim por diante). Não é obrigatório reservar o primeiro IP para a interface de LAN do roteador (número este que será configurado como Default Gateway nas estações de trabalho da respectiva rede, conforme descrito anteriormente). Embora não seja obrigatório é uma convenção comumente utilizada.

Agora que apresentei alguns comentários sobre a rede da figura anterior, vamos analisar como será feito o roteamento entre as diferentes redes.

Primeira análise: Analisar como é feito o roteamento, quando um computador da Rede 01, precisa acessar informações de um computador da Rede 03. Por exemplo, o computador 10.10.10.25 da Rede 01, precisa acessar um arquivo que está em uma pasta compartilhada do computador 10.10.30.144 da Rede 03. Neste caso a rede de origem é a rede 10.10.10.0 e a rede de destino é 10.10.30.0. Como é feito o roteamento, de tal maneira que estes dois computadores possam trocar informações?

Acompanhe os passos descritos a seguir:

1. O computador 10.10.10.25 é o computador de origem e o computador 10.10.30.144 é o computador de destino. A primeira ação do TCP/IP é fazer os cálculos para verificar se os dois computadores estão na mesma rede, conforme explicado no Capítulo 2. Os seguintes dados são utilizados para realização destes cálculos:

- Computador na Rede 01: 10.10.10.25/255.255.255.0
- Computador na Rede 03: 10.10.30.144/255.255.255.0

2. Feitos os cálculos, o protocolo TCP/IP "chega a conclusão" de que os dois computadores pertencem a redes diferentes: O computador 10.10.10.25 pertence a rede 10.10.10.0 e o computador 10.10.30.144 pertence a rede 10.10.30.0.

3. Como os computadores pertencem a redes diferentes, os dados devem ser enviados para o Roteador da rede 10.10.10.0, que é a rede do computador de origem.

4. O pacote é enviado para o roteador da rede 10.10.10.0, que está conectado através da interface 10.10.10.1. Neste roteador, pela interface 10.10.10.1, chega o pacote de informações com o IP de destino: 10.10.30.144. O roteador precisa consultar a sua tabela de roteamento e verificar se ele conhece um caminho para a rede 10.10.30.0, ou seja, se ele sabe para quem enviar um pacote de informações, destinado a rede 10.10.30.0.

5. O Roteador 01 tem, em sua tabela de roteamento, a informação de que pacotes para a rede 10.10.30.0 devem ser encaminhados pela interface de WAN 10.10.5.1. É isso que ele faz, ou seja, encaminha os pacotes através da interface de WAN: 10.10.5.1.

6. Os pacotes de dados chegam na interface de WAN 10.10.5.1 e são enviados, através do link de comunicação, para a interface de WAN 10.10.5.2, do roteador da Rede 03.

7. No Roteador 03 chega o pacote de informações com o IP de destino: 10.10.30.144. O roteador precisa consultar a sua tabela de roteamento e verificar se ele conhece um caminho para a rede 10.10.30.0.

8. O Roteador 03 tem, em sua tabela de roteamento, a informação de que pacotes para a rede 10.10.30.0 devem ser encaminhados pela interface de LAN 10.10.30.1, que é a interface que conecta o Roteador 03 à rede local 10.10.30.0. O pacote é enviado, através da interface 10.10.30.1, para o barramento da rede local. Todos os computadores recebem os pacotes de dados e os descartam, com exceção do computador 10.10.30.144 que é o computador de destino.

9. Para que a resposta possa retornar do computador 10.10.30.144 para o computador 10.10.10.25, um caminho precisa ser encontrado, para que os pacotes de dados possam ser roteados da Rede 03 para a Rede 01 (o caminho de volta no nosso exemplo). Para tal todo o processo é executado novamente, até que a resposta chegue ao computador 10.10.10.25.

10. A chave toda para o processo de roteamento é o software presente nos roteadores, o qual atua com base em tabelas de roteamento.

Segunda análise: Analisar como é feito o roteamento, quando um computador da Rede 03, precisa acessar informações de um computador da Rede 02. Por exemplo, o computador 10.10.30.25 da Rede 03, precisa acessar uma impressora que está compartilhada do computador 10.10.20.144 da Rede 02. Neste caso a rede de origem é a rede 10.10.30.0 e a rede de destino é 10.10.20.0. Como é feito o roteamento, de tal maneira que estes dois computadores possam trocar informações?

Acompanhe os passos descritos a seguir:

1. O computador 10.10.30.25 é o computador de origem e o computador 10.10.20.144 é o computador de destino. A primeira ação do TCP/IP é fazer os cálculos para verificar se os dois computadores estão na mesma rede, conforme explicado no Capítulo 2. Os seguintes dados são utilizados para realização destes cálculos:

- Computador na Rede 03: 10.10.30.25/255.255.255.0
- Computador na Rede 02: 10.10.20.144/255.255.255.0

2. Feitos os cálculos, o protocolo TCP/IP "chega a conclusão" de que os dois computadores pertencem a redes diferentes: O computador 10.10.30.25 pertence a rede 10.10.30.0 e o computador 10.10.20.144 pertence a rede 10.10.20.0.

3. Como os computadores pertencem a redes diferentes, os dados devem ser enviados para o Roteador da rede 10.10.30.0, que é a rede do computador de origem.

4. O pacote é enviado para o roteador da rede 10.10.30.0, que está conectado através da interface de LAN 10.10.30.1. Neste roteador, pela interface 10.10.30.1, chega o pacote de informações com o IP de destino: 10.10.20.144. O roteador precisa consultar a sua tabela de roteamento e verificar se ele conhece um caminho direto para a rede 10.10.20.0, ou seja, se ele sabe para quem enviar um pacote de informações, destinado a rede 10.10.20.0.

5. Não existe um caminho direto para a rede 10.10.20.0. Tudo o que o roteador pode fazer é saber para quem enviar o pacote, quando o destino for a rede 10.10.20.0. Neste caso ele enviará o pacote para outro roteador e não diretamente para a rede 10.10.20.0. O Roteador 03 tem, em sua tabela de roteamento, a informação de que pacotes destinados à rede 10.10.20.0 devem ser encaminhados pela interface de WAN 10.10.5.2. É isso que ele faz, ou seja, encaminha os pacotes através da interface de WAN: 10.10.5.2.

6. Os pacotes de dados chegam na interface de WAN 10.10.5.2 e são enviados, através do link de comunicação, para a interface de WAN 10.10.5.1, do Roteador 01.

7. No Roteador 01 chega o pacote de informações com o IP de destino: 10.10.20.144. O roteador precisa consultar a sua tabela de roteamento e verificar se ele conhece um caminho para a rede 10.10.20.0.

8. Na tabela de roteamento do Roteador 01, consta a informação que pacotes para a rede 10.10.20.0, devem ser enviados para a interface de WAN 10.10.5.3, do Roteador 02. É isso que ele faz, ou seja, roteia (encaminha) o pacote para a interface de WAN 10.10.5.3.

9. O pacote chega à interface de WAN do Roteador 02. O Roteador 02 tem, em sua tabela de roteamento, a informação de que pacotes para a rede 10.10.20.0 devem ser encaminhados pela interface de LAN 10.10.20.1, que é a interface que conecta o Roteador 02 à rede local 10.10.20.0. O pacote é enviado, através da interface 10.10.20.1, para o barramento da rede local. Todos os computadores recebem os pacotes de dados e os descartam, com exceção do computador 10.10.20.144 que é o computador de destino.

10. Para que a resposta possa retornar do computador 10.10.20.144 para o computador 10.10.30.25, um caminho precisa ser encontrado, para que os pacotes de dados possam ser roteados da Rede 02 para a Rede 03 (o caminho de volta no nosso exemplo). Para tal todo o processo é executado novamente, até que a resposta chegue ao computador 10.10.30.25.

Algumas considerações sobre roteamento

A chave toda para o processo de roteamento é o software presente nos roteadores, o qual atua com base em tabelas de roteamento. Ou o roteador sabe entregar o pacote diretamente para a rede de destino ou sabe para qual roteador enviar. Esse processo continua, até que seja possível alcançar a rede de destino. Claro que em redes mais complexas pode haver mais de um caminho entre origem e destino. Por exemplo, na Internet, pode haver dois ou mais caminhos possíveis entre o computador de origem e o computador de destino. Quando um arquivo é transmitido entre os computadores de origem e destino, pode acontecer de alguns pacotes de informação serem enviados por um caminho e outros pacotes por caminhos diferentes. Os pacotes podem, inclusive, chegar fora de ordem no destino. O protocolo TCP/IP é o responsável por identificar cada pacote e colocá-los na seqüência correta.

Existem também um número máximo de roteadores pelos quais um pacote pode passar, antes de ser descartado. Normalmente este número é de 16 roteadores. No exemplo da segunda análise, cada pacote passa por dois roteadores, até sair de um computador na Rede 03 e chegar ao computador de destino, na Rede 02. Este passar por dois roteadores é tecnicamente conhecido como "ter um caminho de 2 hopes". Um hope significa que passou por um roteador. Diz-se, com isso, que o caminho máximo de um pacote é de 16 hopes. Isso é feito para evitar que pacotes fiquem circulando indefinidamente na rede e congestionem os links de WAN, podendo até chegar a paralisar a rede.

Uma situação que poderia acontecer, por erro nas tabelas de roteamento, é um roteador x mandar um pacote para o y, o roteador y mandar de volta para o x, o roteador x de volta

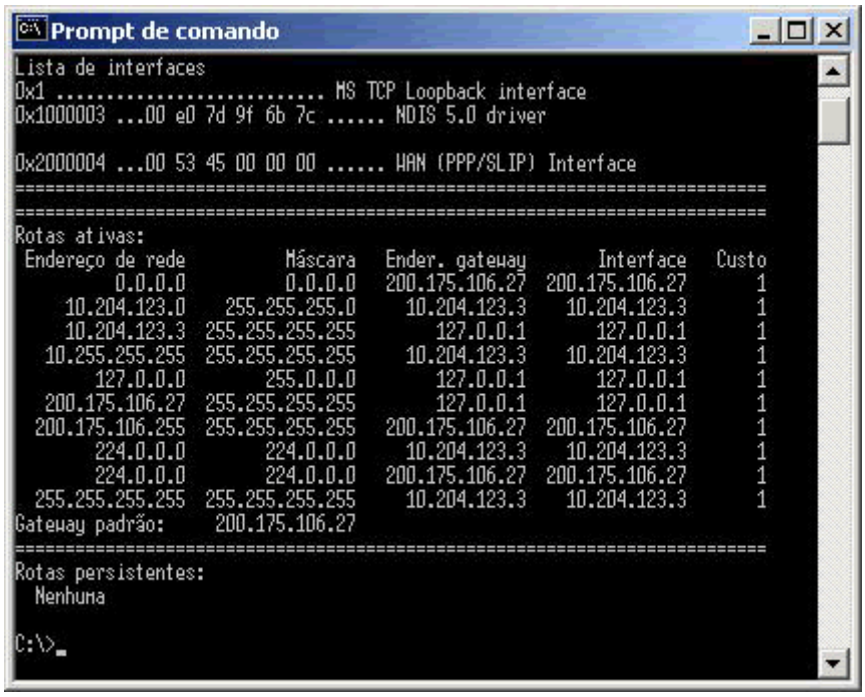
para y e assim indefinidamente. Esta situação ocorreria por erros nas tabelas de roteamento. Para evitar que estes pacotes ficassem circulando indefinidamente na rede, é que foi definido o limite de 16 hopes.

Outro conceito que pode ser encontrado, em relação a roteamento, é o de entrega direta ou entrega indireta. Vamos ainda utilizar o exemplo da rede da Figura 16.2. Quando dois computadores da mesma rede (por exemplo a rede 10.10.10.0) trocam informações entre si, as informações são enviadas para o barramento da rede local e o computador de destino captura e processa os dados. Dizemos que este é um caso de entrega direta. Quando computadores de redes diferentes tentam se comunicar (por exemplo, um computador da rede 10.10.10.0 e um da rede 10.10.20.0), os pacotes de informação são enviados através dos roteadores da rede, até chegar ao destino. Depois a resposta percorre o caminho inverso. Este processo é conhecido como entrega indireta.

Tabelas de roteamento

Toda a funcionalidade do Roteador é baseada em tabelas de roteamento. Quando um pacote chega em uma das interfaces do roteador, ele analisa a sua tabela de roteamento, para verificar se na tabela de roteamento, existe uma rota para a rede de destino. Pode ser uma rota direta ou então para qual roteador o pacote deve ser enviado. Este processo continua até que o pacote seja entregue na rede de destino, ou até que o limite de 16 hopes (para simplificar imagine um hope como sendo um roteador da rede) tenha sido atingido.

Na Figura a seguir apresento um exemplo de uma "mini-tabela" de roteamento:



Cada linha é uma entrada da tabela. Por exemplo, a linha a seguir é que define o Default Gateway da ser utilizado:

0.0.0.0 0.0.0.0 200.175.106.54 200.175.106.54 1

Neste tópico você aprenderá sobre os campos que compõem uma entrada da tabela de roteamento e o significado de cada campo. Também aprenderá a interpretar a tabela de roteamento que existe em um computador com o Windows 2000, Windows XP ou Windows Server 2003.

Campos de uma tabela de roteamento

Uma entrada da tabela de roteamento possui os campos indicados no esquema a seguir e explicados logo em seguida:

Netwkor ID	Network Mask	Next Hop	Interface	Metric
0.0.0.0	0.0.0.0	200.175.106.54	200.175.106.54	1
10.100.100.0	255.255.255.0	10.200.200.4	10.200.200.4	1

- **Network ID:** Este é o endereço de destino. Pode ser o endereço de uma rede (por exemplo: 10.10.10.0), o endereço de um equipamento da rede, o endereço de uma sub-rede ou o endereço da rota padrão (0.0.0.0). A rota padrão significa: "a rota que será utilizada, caso não tenha sido encontrada uma rota específica para o destino". Por exemplo, se for definida que a rota padrão deve ser envida pela interface com IP 10.10.5.2 de um determinado roteador, sempre que chegar um pacote, para o qual não existe uma rota específica para o destino do pacote, este será enviado pela rota padrão, que no exemplo seria a interface 10.10.5.2. Falando de um jeito mais simples: Se não souber para onde mandar, manda para a rota padrão.

- **Network Mask**: A máscara de sub-rede utilizada para a rede de destino.

- **Next Hop:** Endereço IP da interface para a qual o pacote deve ser enviado. Considere o exemplo a seguir, como sendo uma entrada de um roteador, com uma interface de WAN configurada com o IP número 10.200.200.4:

Netwkor ID	Network Mask	Next Hop	Interface	Metric
10.100.100.0	255.255.255.0	10.200.200.1	10.200.200.120	1

Esta entrada indica que pacotes enviados para a rede definida pelos parâmetros 10.100.100.0/255.255.255.0, deve ser enviada para o gateway 10.200.200.1 e para chegar a este gateway, os pacotes de informação devem ser enviados pela interface 10.200.200.120. Neste exemplo, esta entrada está contida na tabela interna de roteamento de um computador com o Windows Server 2003, cujo número IP é 10.200.200.120 e o default gateway configurado é 10.200.200.1. Neste caso, quando este computador quiser se comunicar com um computador da rede 10.100.100.0, será usada a entrada de roteamento descrita neste item. Nesta entrada está especificado que pacotes para a rede 10.100.100.0, com máscara 255.255.255.0, devem ser enviados para o default gateway 10.200.200.1 e que este envio deve ser feito através da interface de rede 10.200.200.120, que no nosso exemplo é a placa de rede do computador. Uma vez que o pacote chegou no default gateway (na interface de LAN do roteador), o processo de roteamento, até a rede de destino (rede 10.100.100.0) é o processo descrito nas análises anteriores.

- **Interface:** É a interface através da qual o pacote deve ser enviado. Por exemplo, se você estiver analisando a tabela de roteamento interna, de um computador com o Windows Server 2003, o número IP do campo interface, será sempre o número IP da placa de rede, a não ser que você tenha mais de uma placa de rede instalada.

- **Metric:** A métrica é um indicativo da "distância" da rota, entre destino e origem, em termos de hopes. Conforme descrito anteriormente, pode haver mais de um roteador entre origem e destino. Também pode haver mais de um caminho entre origem e destino. Se for encontrada duas rotas para um mesmo destino, o roteamento será feito pela rota de menor valor no campo Metric. Um valor menor indica, normalmente, um número menor de hopes (roteadores) entre origem e destino.

Analise da tabela de Roteamento

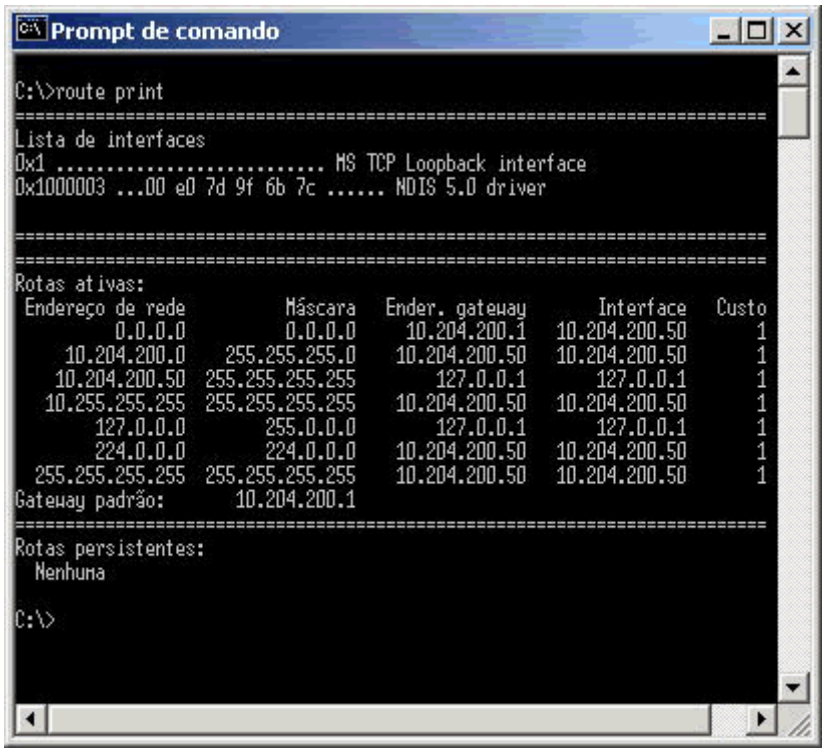
Agora que você já conhece os conceitos de tabelas de roteamento e também conhece os campos que formam uma entrada em uma tabela de roteamento, é hora de analisar as

entradas de uma tabela de roteamento em um computador com o Windows Server 2003 instalado. No Windows Server 2003, o protocolo TCP/IP é instalado automaticamente e não pode ser desinstalado (esta é uma das novidades do Windows Server 2003). Ao instalar e configurar o protocolo TCP/IP, o Windows Server 2003 cria, na memória do servidor, uma tabela de roteamento. Esta tabela é criada, dinamicamente, toda vez que o servidor é inicializado. Ao desligar o servidor o conteúdo desta tabela será descartado, para ser novamente recriado durante a próxima inicialização. A tabela de roteamento é criada com base nas configurações do protocolo TCP/IP. Existem também a possibilidade de adicionar entradas estáticas. Uma entrada estática fica gravada no HD do computador e será adicionada à tabela de roteamento durante a inicialização do sistema. Ou seja, além das entradas criadas automaticamente, com base nas configurações do TCP/IP, também podem ser acrescentadas rotas estáticas, criadas com o comando route, o qual descreverei mais adiante.

Para exibir a tabela de roteamento de um computador com o Windows Server 2003 (ou com o Windows 2000, ou Windows XP), abra um Prompt de comando (Iniciar -> Programas -> Acessórios -> Prompt de comando), digite o comando indicado a seguir e pressione Enter:

route print

Será exibida uma tabela de roteamento, semelhante a indicada na Figura a seguir, onde é exibida a tabela de roteamento para um servidor com o número IP: 10.204.200.50:



Vamos analisar cada uma destas entradas e explicar a função de cada entrada, para que você possa entender melhor os conceitos de roteamento.

Rota padrão

Endereço de rede	Máscara	Ender. gateway	Interface	Custo
0.0.0.0	0.0.0.0	10.204.200.1	10.204.200.50	1

Esta rota é indicada por uma identificação de rede 0.0.0.0 com uma máscara de sub-rede 0.0.0.0. Quando o TCP/IP tenta encontrar uma rota para um determinado destino, ele percorre todas as entradas da tabela de roteamento em busca de uma rota específica para a rede de destino. Caso não seja encontrada uma rota para a rede de destino, será utilizada a

rota padrão. Em outras palavras, se não houver uma rota específica, mande através da rota padrão. Observe que a rota padrão é justamente o default gateway da rede (10.204.200.1), ou seja, a interface de LAN do roteador da rede. O parâmetro Interface (10.204.200.50) é o número IP da placa de rede do próprio servidor. Em outras palavras: Se não houver uma rota específica manda para a rota padrão, onde o próximo hope da rede é o 10.204.200.1 e o envio para este hope é feito através da interface 10.204.200.50 (ou seja, a próprio placa de rede do servidor).

Endereço da rede local

Endereço de rede	Máscara	Ender. gateway	Interface	Custo
10.204.200.0	255.255.255.0	10.204.200.50	10.204.200.50	1

Esta rota é conhecida como Rota da Rede Local. Ele basicamente diz o seguinte: "Quando o endereço IP de destino for um endereço da minha rede local, envie as informações através da minha placa de rede (observe que tanto o parâmetro Gateway como o parâmetro Interface estão configurados com o número IP do próprio servidor). Ou seja, se for para uma das máquinas da minha rede local, manda através da placa de rede, não precisa enviar para o roteador.

Local host (endereço local)

Endereço de rede	Máscara	Ender. gateway	Interface	Custo
10.204.200.50	255.255.255.255	127.0.0.1	127.0.0.1	1

Este endereço faz referência ao próprio computador. Observe que 10.204.200.50 é o número IP do servidor que está sendo analisado (no qual executei o comando route print). Esta rota diz que os programas do próprio computador, que enviarem pacotes para o destino 10.204.200.50 (ou seja, enviarem pacotes para si mesmo, como no exemplo de dois serviços trocando informações entre si), devem usar como Gateway o endereço de loopback 127.0.0.1, através da interface de loopback 127.0.0.1. Esta rota é utilizada para agilizar as comunicações que ocorrem entre os componentes do próprio Windows Server 2003, dentro do mesmo servidor. Ao usar a interface de loopback, toda a comunicação ocorre a nível de software, ou seja, não é necessário enviar o pacote através das diversas camadas do protocolo TCP/IP, até que o pacote chegue na camada de enlace (ou seja, a placa de rede), para depois voltar. Ao invés disso é utilizada a interface de loopback para direcionar os pacotes corretamente. Observe que esta entrada tem como máscara de sub-rede o número 255.255.255.255. Esta máscara indica que a entrada é uma rota para um endereço IP específico (no caso o próprio IP do servidor) e não uma rota para um endereço de rede.

Network broadcast (Broadcast de rede)

Endereço de rede	Máscara	Ender. gateway	Interface	Custo
10.255.255.255	255.255.255.255	10.204.200.50	10.204.200.50	1

Esta rota define o endereço de broadcast da rede. Broadcast significa enviar para todos os computadores da rede. Quando é utilizado o endereço de broadcast, todos os computadores da rede recebem o pacote e processam o pacote. O broadcast é utilizado por uma série de serviços, como por exemplo o WINS, para fazer verificações periódicas de nomes, para enviar uma mensagem para todos os computadores da rede, para obter informações de todos os computadores e assim por diante. Observe que o gateway é o número IP da placa de rede do servidor e a Interface é este mesmo número, ou seja, para enviar um broadcast para a rede, envie através da placa de rede do servidor, não há necessidade de utilizar o roteador. Um detalhe interessante é que, por padrão, a maioria dos roteadores bloqueia o tráfego de broadcast, para evitar congestionamentos nos links de WAN.

Rede/endereço de loopback

Endereço de rede	Máscara	Ender. gateway	Interface	Custo
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1

Comentei anteriormente que os endereços da rede 127.0.0.0 são endereços especiais, reservados para fazer referência a si mesmo. Ou seja, quando faço uma referência a 127.0.0.1 estou me referindo ao servidor no qual estou trabalhando. Esta roda indica, em palavras simples, que para se comunicar com a rede de loopback (127.0.0.0/255.0.0.0), utilize "eu mesmo" (127.0.0.1).

Multicast address (endereço de Multicast):

Endereço de rede	Máscara	Ender. gateway	Interface	Custo
224.0.0.0	224.0.0.0	10.204.200.50	10.204.200.50	1

O tráfego IP, de uma maneira simples, pode ser de três tipos: Unicast é o tráfego direcionado para um número IP definido, ou seja, para um destinatário, definido por um número IP. Broadcast é o tráfego dirigido para todos os computadores de uma ou mais redes. E tráfego Multicast é um tráfego direcionado para um grupo de computadores, os quais estão configurados e "inscritos" para receber o tráfego multicast. Um exemplo prático de utilização do multicast é para uma transmissão de vídeo através da rede. Vamos supor que de uma rede de 1000 computadores, apenas 30 devam receber um determinado arquivo de vídeo com um treinamento específico. Se for usado tráfego unicast, serão transmitidas 30 cópias do arquivo de vídeo (o qual já é um arquivo grande), uma cópia para cada destinatário. Com o uso do Multicast, uma única cópia é transmitida através do link de WAN e o tráfego multicast (com base no protocolo IGMP), entrega uma cópia do arquivo apenas para os 30 computadores devidamente configurados para receber o tráfego multicast. Esta rota define que o tráfego multicast deve ser enviado através da interface de rede, que é o número IP da placa de rede do servidor. Lembrando quando falamos sobre classes de endereços, a classe D é reservada para tráfego multicast, com IPs iniciando (o primeiro número) a partir de 224.

Limited Broadcast (Broadcast Limitado)

Endereço de rede	Máscara	Ender. gateway	Interface	Custo
255.255.255.255	255.255.255.255	10.204.200.50	10.204.200.50	1

Esta é a rota utilizada para o envio de broadcast limitado. O endereço de broadcast limitado é formato por todos os 32 bits do endereço IP sendo iguais a 1 (255.255.255.255). Este endereço é utilizado quando o computador tem que fazer o envio de um broadcast na rede local (envio do tipo um para todos na rede), porém o computador não conhece a número da rede local (network ID). Você pode perguntar: Mas em que situação o computador não conhecerá a identificação da rede local? Por exemplo, quando você inicializa um computador, configurado para obter as configurações do TCP/IP a partir de um servidor DHCP, a primeira coisa que este computador precisa fazer é localizar um servidor DHCP na rede e requisitar as configurações do TCP/IP. Ou seja, antes de receber as configurações do DHCP, o computador ainda não tem endereço IP e nem máscara de sub-rede, mas tem que se comunicar com um servidor DHCP. Esta comunicação é feita via broadcast limitado, onde o computador envia um pacote de formato específico (chamado de DHCP Discovery), para tentar descobrir um servidor DHCP na rede. Este pacote é enviado para todos os computadores. Aquele que for um servidor DHCP irá responder a requisição do cliente. Aí o processo de configuração do DHCP continua, até que o computador esteja com as configurações do TCP/IP definidas, configurações estas obtidas a partir do servidor DHCP.

Definindo DNS

DNS é a abreviatura de Domain Name System. O DNS é um serviço de resolução de nomes. Toda comunicação entre os computadores e demais equipamentos de uma rede baseada no protocolo TCP/IP (e qual rede não é baseada no protocolo TCP/IP?) é feita através do número IP. Número IP do computador de origem e número IP do computador de destino. Porém não seria nada produtivo se os usuários tivessem que decorar, ou mais realisticamente, consultar uma tabela de números IP toda vez que tivessem que acessar um recurso da rede. Por exemplo, você digita http://www.microsoft.com/brasil, para acessar o site da Microsoft no Brasil, sem ter que se preocupar e nem saber qual o número IP do servidor onde está hospedado o site da Microsoft Brasil. Mas alguém tem que fazer este serviço, pois quando você digita http://www.microsoft.com/brasil, o protocolo TCP/IP precisa

"descobrir" (o termo técnico é resolver o nome) qual o número IP está associado com o endereço digitado. Se não for possível "descobrir" o número IP associado ao nome, não será possível acessar o recurso desejado.

O papel do DNS é exatamente este, "descobrir", ou usando o termo técnico, "resolver" um determinado nome, como por exemplo http://www.microsoft.com Resolver um nome significa, descobrir e retornar o número IP associado com o nome. Em palavras mais simples, o DNS é um serviço de resolução de nomes, ou seja, quando o usuário tenta acessar um determinado recurso da rede usando o nome de um determinado servidor, é o DNS o responsável por localizar e retornar o número IP associado com o nome utilizado. O DNS é, na verdade, um grande banco de dados distribuído em milhares de servidores DNS no mundo inteiro.

O DNS passou a ser o serviço de resolução de nomes padrão a partir do Windows 2000 Server. Anteriormente, com o NT Server 4.0 e versões anteriores do Windows, o serviço padrão para resolução de nomes era o WINS – Windows Internet Name Service. Versões mais antigas dos clientes Windows, tais como Windows 95, Windows 98 e Windows Me ainda são dependentes do WINS, para a realização de determinadas tarefas. O fato de existir dois serviços de resolução de nomes, pode deixar o administrador da rede e os usuários confusos.

Cada computador com o Windows instalado (qualquer versão), tem dois nomes: um host name (que é ligado ao DNS) e um NetBios name (que é ligado ao WINS). Por padrão estes nomes devem ser iguais, ou seja, é aconselhável que você utilize o mesmo nome para o host name e para o NetBios name do computador.

O DNS é um sistema para nomeação de computadores e equipamentos de rede em geral (tais como roteadores,hubs, switchs). Os nomes DNS são organizados de uma maneira hierárquica através da divisão da rede em domínios DNS.

O DNS é, na verdade, um grande banco de dados distribuído em váios servidoress DNS e um conjunto de serviços e funcionalidades, que permitem a pesquisa neste banco de dados. Por exemplo, quando o usuário digita www.abc.com.br na barra de endereços do seu navegador, o DNS tem que fazer o trabalho de localizar e retornar para o navegador do usuário, o número IP associado com o endereço www.abc.com.br Quando você tenta acessar uma pasta compartilhada chamada docs, em um servidor chamado srv-files01.abc.com.br, usando o caminho \\srv-files01.abc.com.br\docs, o DNS precisa encontrar o número IP associado com o nome srv-files01.abc.com.br. Se esta etapa falhar, a comunicação não será estabelecida e você não poderá acessar a pasta compartilhada docs.

Ao tentar acessar um determinado recurso, usando o nome de um servidor, é como se o programa que você está utilizando perguntasse ao DNS:

"DNS, você sabe qual o endereço IP associado com o nome tal?"

O DNS pesquisa na sua base de dados ou envia a pesquisa para outros servidores DNS (dependendo de como foram feitas as configurações do servidor DNS, conforme descreverei mais adiante). Uma vez encontrado o número IP, o DNS retorna o número IP para o cliente:

"Este é o número IP associado com o nome tal."

Nota: O DNS implementado no Windows 2000 Server e também no Windows Server 2003 é baseado em padrões definidos por entidades de padronização da Internet, tais como o IETF. Estes documentos são conhecidos como RFCs – Request for Comments. Você encontra, na Internet, facilmente a lista de RFCs disponíveis e o assunto relacionada com cada uma. São milhares de RFCs (literalmente milhares).

Entendendo os elementos que compõem o DNS

O DNS é baseado em conceitos tais como espaço de nomes e árvore de domínios. Por exemplo, o espaço de nomes da Internet é um espaço de nomes hierárquico, baseado no DNS. Para entender melhor estes conceitos, observe o diagrama da Figura a seguir:

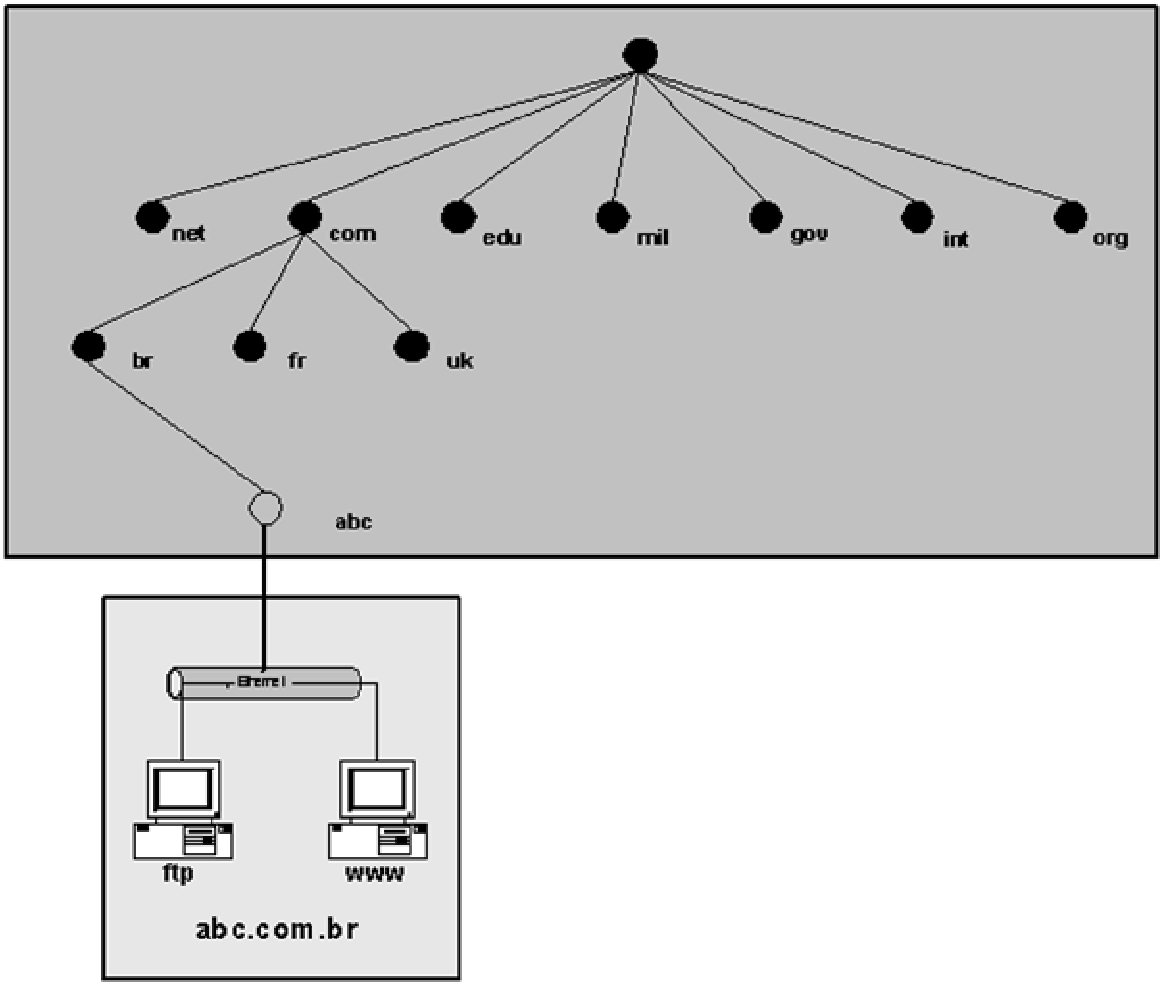


Figura - Estrutura hierárquica do DNS

Nesta Figura é apresentada uma visão abrevida da estrutura do DNS definida para a Internet. O principal domínio, o domínio root, o domínio de mais alto nível foi nomeado como sendo um ponto (.). No segundo nível foram definidos os chamados "Top-level-domains". Estes domínios são bastante conhecidos, sendo os principais descritos na Tabela a seguir:

Top-level-domains:

Top-level-domain	Descrição
com	Organizações comerciais
gov	Organizações governamentais
edu	Instituições educacionais
org	Organizações não comerciais
net	Diversos
mil	Instituições militares

Em seguida, a estrutura hierárquica continua aumentando. Por exemplo, dentro do domínio .com, são criadas sub domínios para cada país. Por exemplo: br para o Brasil (.com.br), .fr

para a França (.com.fr), uk para a Inglaterra (.com.uk) e assim por diante. Observe que o nome completo de um domínio é o nome do próprio domínio e mais os nomes dos domínios acima dele, no caminho até chegar ao domínio root que é o ponto. Nos normalmente não escrevemos o ponto, mas não está errado utilizá-lo. Por exemplo, você pode utilizar www.microsoft.com ou www.microsoft.com. (com ponto no final mesmo).

No diagrama da Figura anterior, representei até o domínio de uma empresa chamada abc (abc...), que foi registrada no subdomínio (.com.br), ou seja: abc.com.br. Este é o domínio DNS desta nossa empresa de exemplo.

Nota: Para registrar um domínio .br, utilize o seguinte endereço: www.registro.br

Todos os equipamentos da rede da empresa abc.com.br, farão parte deste domínio. Por exemplo, considere o servidor configurado com o nome de host www. O nome completo deste servidor será www.abc.com.br, ou seja, é com este nome que ele poderá ser localizado na Internet. O nome completo do servidor com nome de host ftp será: ftp.abc.com.br, ou seja, é com este nome que ele poderá ser acessado através da Internet. No banco de dados do DNS é que ficará gravada a informação de qual o endereço IP está associado com www.abc.com.br, qual o endereço IP está associado com ftp.abc.com.br e assim por diante. Mais adiante você verá, passo-a-passo, como é feita a resolução de nomes através do DNS.

O nome completo de um computador da rede é conhecido como FQDN – Full Qualified Domain Name. Por exemplo ftp.abc.com.br é um FQDN. ftp (a primeira parte do nome) é o nome de host e o restante representa o domínio DNS no qual está o computador. A união do nome de host com o nome de domínio é que forma o FQDN.

Internamente, a empresa abc.com.br poderia criar subdomínios, como por exemplo: vendas.abc.com.br, suporte.abc.com.br, pesquisa.abc.com.br e assim por diante. Dentro de cada um destes subdominios poderia haver servidores e computadores, como por exemplo: srv01.vendas.abc.com.br, srv-pr01.suporte.abc.com.br. Observe que sempre, um nome de domínio mais baixo, contém o nome completo dos objetos de nível mais alto. Por exemplo, todos os subdomínios de abc.com.br, obrigatoriamente, contém abc.com.br: vendas.abc.com.br, suporte.abc.com.br, pesquisa.abc.com.br. Isso é o que define um espaço de nomes contínio.

Dentro de um mesmo nível, os nomes DNS devem ser únicos. Por exemplo, não é possível registrar dois domínios abc.com.br. Porém é possível registrar um domínio abc.com.br e outro abc.net.br. Dentro do domínio abc.com.br pode haver um servidor chamado srv01. Também pode haver um servidor srv01 dentro do domínio abc.net.br. O que distingue um do outro é o nome completo (FQDN), neste caso: srv01.abc.com.br e o outro é srv01.abc.net.br.

Nota: Um método antigo, utilizado inicalmente para resolução de nomes era o arquivo hosts. Este arquivo é um arquivo de texto e contém entradas como as dos exemplos a seguir, uma em cada linha:

```
10.200.200.3        www.abc.com.br
10.200.200.4        ftp.abc.com.br
10.200.200.18       srv01.abc.com.br  srv-files
```

O arquivo hosts é individual para cada computador da rede e fica gravado (no Windows NT, Windows 2000, Windows Server 2003 ou Windows XP), na pasta system32\drivers\etc, dentro da pasta onde o Windows está instalado. Este arquivo é um arquivo de texto e pode ser alterado com o bloco de Notas.
O DNS é formado por uma série de componentes e serviços, os quais atuando em conjunto, tornam possível a tarefa de fazer a resolução de nomes em toda a Internet ou na rede interna da empresa. Os componentes do DNS são os seguintes:

- **O espaço de nomes DNS:** Um espaço de nomes hierárquico e contínuo. Pode ser o espaço de nomes da Internet ou o espaço de nomes DNS interno, da sua empresa. Pode ser utilizado um espaço de nomes DNS interno, diferente do nome DNS de

Internet da empresa ou pode ser utilizado o mesmo espaço de nomes. Cada uma das abordagens tem vantagens e desvantagens.

- **Servidores DNS:** Os servidores DNS contém o banco de dados do DNS com o mapeamento entre os nomes DNS e o respectivo número IP. Os servidores DNS também são responsáveis por responder às consultas de nomes envidas por um ou mais clientes da rede. Você aprenderá mais adiante que existem diferentes tipos de servidores DNS e diferentes métodos de resolução de nomes.

- **Registros do DNS (Resource Records):** Os registros são as entradas do banco de dados do DNS. Em cada entrada existe um mapeamento entre um determinado nome e uma informação associada ao nome. Pode ser desde um simples mapeamento entre um nome e o respectivo endereço IP, até registros mais sofisticados para a localização de DCs (controladores de domínio do Windows 2000 ou Windows Server 2003) e servidores de email do domínio.

- **Clientes DNS:** São também conhecidos como resolvers. Por exemplo, uma estação de trabalho da rede, com o Windows 2000 Professional, com o Windows XP professional ou com o Windows Vista tem um "resolver" instalado. Este componente de software é responsável por detectar sempre que um programa precisa de resolução de um nome e repassar esta consulta para um servidor DNS. O servidor DNS retorna o resultado da consulta, o resultado é retornado para o resolver, o qual repassa o resultado da consulta para o programa que originou a consulta.

Entendendo como funcionam as pesquisas do DNS

Imagine um usuário, na sua estação de trabalho, navegando na Internet. Ele tenta acessar o site www.funam.com.br O usuário digita este endereço e tecla Enter. O resolver (cliente do DNS instalado na estação de trabalho do usuário) detecta que existe a necessidade da resolução do nome www.funam.com.br, para descobrir o número IP associado com este nome. O resolver envia a pesquisa para o servidor DNS configurado como DNS primário, nas propriedades do TCP/IP da estação de trabalho (ou para o DNS informado pelo DHCP, caso a estação de trabalho esteja obtendo as configurações do TCP/IP, automaticamente, a partir de um servidor DHCP). A mensagem envida pelo resolver, para o servidor DNS, contém três partes de informação, conforme descrito a seguir:

- **O nome a ser resolvido**. No nosso exemplo: www.funam.com.br

- **O tipo de pesquisa a ser realizado**. Normalmente é uma pesquisa do tipo "resource record", ou seja, um registro associado a um nome, para retornar o respectivo endereço IP. No nosso exemplo, a pesquisa seria por um registro do tipo A, na qual o resultado da consulta é o número IP associado com o nome que está sendo pesquisado. É como se o cliente perguntasse para o sevidor DNS: "Você conhece o número IP associado com o nome www.funam.com.br?" E o servidor responde: "Sim, conheço. O número IP associado com o nome www.funam.com.br é o seguinte... Também podem ser consultas especializadas, como por exemplo, para localizar um DC (controlador de domínio) no domínio ou um servidor de autenticação baseado no protocolo Kerberos.

- **Uma classe associada com o nome DNS**. Para os servidores DNS baseados no Windows 2000 Server e Windows Server 2003, a classe será sempre uma classe de Internet (IN), mesmo que o nome seja referente a um servidor da Intranet da empresa.

Existem diferentes maneiras como uma consulta pode ser resolvida. Por exemplo, a primeira vez que um nome é resolvido, o nome e o respetivo número IP são armazenados em memória, no que é conhecido como Cache do cliente DNS, na estação de trabalho que fez a consulta. Na próxima vez que o nome for utilizado, primeiro o Windows procura no Cache DNS do próprio computador, para ver se não existe uma resolução anterior para o nome em

questão. Somente se não houver uma resolução no Cache local do DNS, é que será envida uma consulta para o servidor DNS.

Chegando a consulta ao servidor, primeiro o servidor DNS consulta o cache do servidor DNS. No cache do servidor DNS ficam, por um determinado período de tempo, as consultas que foram resolvidas anteriormente pelo servidor DNS. Esse processo agiliza a resolução de nomes, evitando repetidas resoluções do mesmo nome. Se não for encontrada uma resposta no cache do servidor DNS, o servidor pode tentar resolver a consulta usando as informações da sua base de dados ou pode enviar a consulta para outros servidores DNS, até que uma resposta seja obtida. A seguir descreverei detalhes deste procsso de enviar uma consulta para outros servidores, processo este chamado de recursão.

Em resumo, o processo de resolução de um nome DNS é composto de duas etapas:

1. A consulta inicia no cliente e é passada para o resolver na estação de trabalho do cliente. Primeiro o resolver tenta responder a consulta localmente, usando recursos tais como o cache local do DNS e o arquivo hosts.

2. Se a consulta não puder ser resolvida localmente, o resolver envia a consulta para o servidor DNS, o qual pode utilizar diferentes métodos (descritos mais adiante), para a resolução da consulta.

A seguir vou descrever as etapas envolvidas nas diferentes maneiras que o DNS utiliza para "responder" a uma consulta enviada por um cliente.

Nota: Vou utilizar algumas figuras da ajuda do Windows 2000 Server para explicar a maneira como o DNS resolve consultas localmente (resolver) e os diferentes métodos de resolução utilizados pelo servidor DNS.

Inicialmente considere o diagrama da Figura a seguir, contido na Ajuda do DNS, no Windows 2000 Server, diagrama este que apresenta uma visão geral do processo de resolução de nomes do DNS.

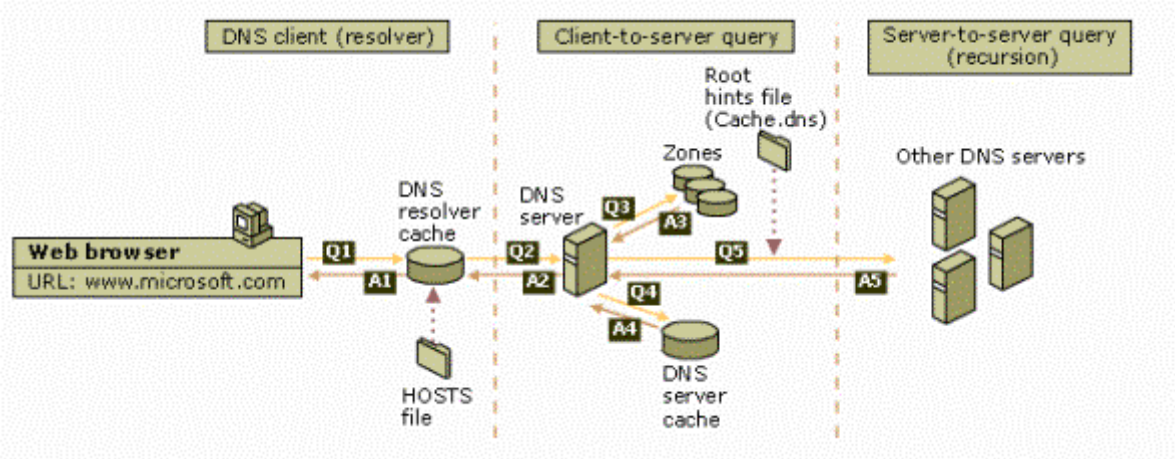


Figura - O processo de resolução de nomes do DNS.

No exemplo desta figura, o cliente está em sua estação de trabalho e tenta acessar o site da Microsoft: www.microsoft.com. Ao digitar este endereço no seu navegador e pressionar Enter, o processo de resolução do nome www.microsoft.com é iniciado. Uma série de etapas são executadas, até que a resoluçõa aconteça com sucesso ou falhe em definitivo, ou seja, o DNS não consegue resolver o nome, isto é, não consegue encontrar o número IP associado ao endereço www.microsoft.com

Primeira etapa: O DNS tenta resolver o nome, usando o resolver local:

Ao digitar o endereço www.microsoft.com e pressionar Enter, o processo de resolução é iniciado. Inicialmente o endereço é passado para o cliente DNS, na estação de trabalho do usuário. O cliente DNS é conhecido como resolver, conforme já descrito anteriormente, nome este que utilizarei a partir de agora. O cliente tenta resolver o nome utilizando um dos seguintes recursos:

- **O cache DNS local:** Sempre que um nome é resolvido com sucesso, o nome e a informação associada ao nome (normalmente o endereço IP), são mantidos na memória, o que é conhecido como cache local do DNS da estação de trabalho do cliente. Quando um nome precisa ser resolvido, a primeira coisa que o resolver faz é procurar no cache local. Encontrando no cache local, as informações do cache são utilizadas e a resolução está completa. O cache local torna a resolução mais rápida, uma vez que nomes já resolvidos podem ser consultados diretamente no cache, ao invés de terem que passar por todo o processo de resolução via servidor DNS novamente, processo este que você aprenderá logo a seguir. Pode acontecer situações onde informações incorretas foram gravadas no Cache Local e o Resolver está utilizando estas informações. Você pode limpar o Cache local, usando o comando ipconfig /flushdns Abra um prompt de Comando, digite o comando ipconfig /flushdns e pressione Enter. Isso irá limpar o Cache local.

- **O arquivo hosts:** Se não for encontrada a resposta no cache local do DNS, o resolver consulta as entradas do arquivos hosts, o qual é um arquivo de texto e fica na pasta onde o Windows Server foi instalado, dentro do seguinte caminho: \system32\drivers\etc (para o Windows NT 4, Windows 2000, Windows Server 2003 e Windos XP). O hosts é um arquivo de texto e pode ser editado com o bloco de notas. Este arquivo possui entradas no formato indicado a seguir, com um númeo IP por linha, podendo haver um ou mais nomes associados com o mesmo número IP:

```
10.200.200.3        www.abc.com.br     intranet.abc.com.br
10.200.200.4        ftp.abc.com.br      arquivos.abc.com.br
10.200.200.18       srv01.abc.com.br    pastas.abc.com.br    pastas
```

Se mesmo assim a consulta não for respondida, o resolver envia a consulta para o servidor DNS configurado nas propriedades do TCP/IP como servidor DNS primário ou configurado via DHCP, como servidor DNS primário.

Segunda etapa: Pesquisa no servidor DNS.

Uma vez que a consulta não pode ser resolvida localmente pelo resolver, esta é enviada para o servidor DNS. Quando a consulta chega no servidor DNS, a primeira coisa que o servidor DNS faz é consultar as zonas para as quais ele é uma autoridade. Por exemplo, vamos supor que o servidor DNS seja o servidor DNS primário para a zona vendas.abc.com.br (diz-se que ele é a autoridade para esta zona) e o nome a ser pesquisado é srv01.vendas.abc.com.br. Neste caso o servidor DNS irá pesquisar nas informações da zona vendas.abc.com.br (para a qual ele é a autoridade) e responder a consulta para o cliente. Diz-se que o servidor DNS respondeu com autoridade (authoritatively).

No nosso exemplo (Figura anterior) não é este o caso, uma vez que o nome pesquisado é www.microsoft.com e o servidor DNS não é a autoridade, ou seja, não é o servidor DNS primário para o domíno microsoft.com. Neste caso, o servidor DNS irá pesquisar o cache do servidor DNS (não confundir com o cache local do DNS no cliente).

À medida que o servidor DNS vai resolvendo nomes, ele vai mantendo estas informações em um cache no servidor DNS. As entradas são mantidas em cache por um tempo que pode ser configurado pelo administrador do DNS. O cache do servidor DNS tem a mesma função do cache local do resolver, ou seja, agilizar a consulta a nomes que já foram resolvidos previamente. Se for encontrada uma entrada no cache do servidor DNS, esta entrada será utilizada pelo servidor DNS para responder a consulta enviada pelo cliente. e o processo de consulta está completo.

Caso o servidor DNS não possa responder usando informações de uma zona local do DNS e nem informações contidas no cache do servidor DNS, o processo de pesquisa continua, usando um processo conhecido como recursão (recursion), para resolver o nome. Agora o servidor DNS fará consultas a outros servidores para tentar responder a consulta enviada pelo cliente. O processo de recursão é ilustrado na Figura a seguir, da ajuda do DNS. Em seguida comentarei os passos envolvidos no processo de recursão.

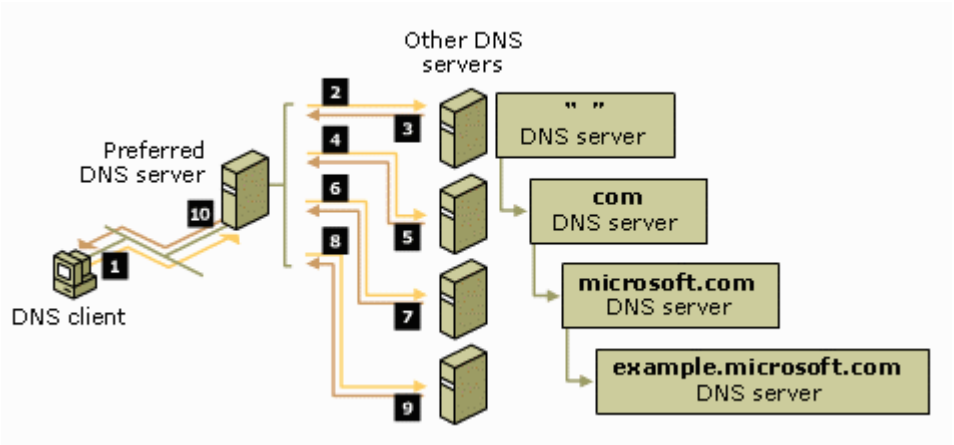


Figura - Resolução de nomes usando recursão

O servidor DNS irá iniciar o processo de recursão com o auxílio de servidores DNS da Internet. Para localizar estes servidores, o servidor DNS utiliza as configurações conhecidas como "root hints". Root hints nada mais é do que uma lista de servidores DNS e os respectivos endereços IP, dos servidores para o domínio root (representado pelo ponto .) e para os domínios top-level (.com, .net, gov e assim por diante). Esta lista é criada automaticamente quando o DNS é instalado e pode ser acessada através das propriedades do servidor DNS. Na Figura a seguir é exibida uma lista de root hints configuradas por padrão, em um servidor DNS, baseado no Windows 2000 Server:

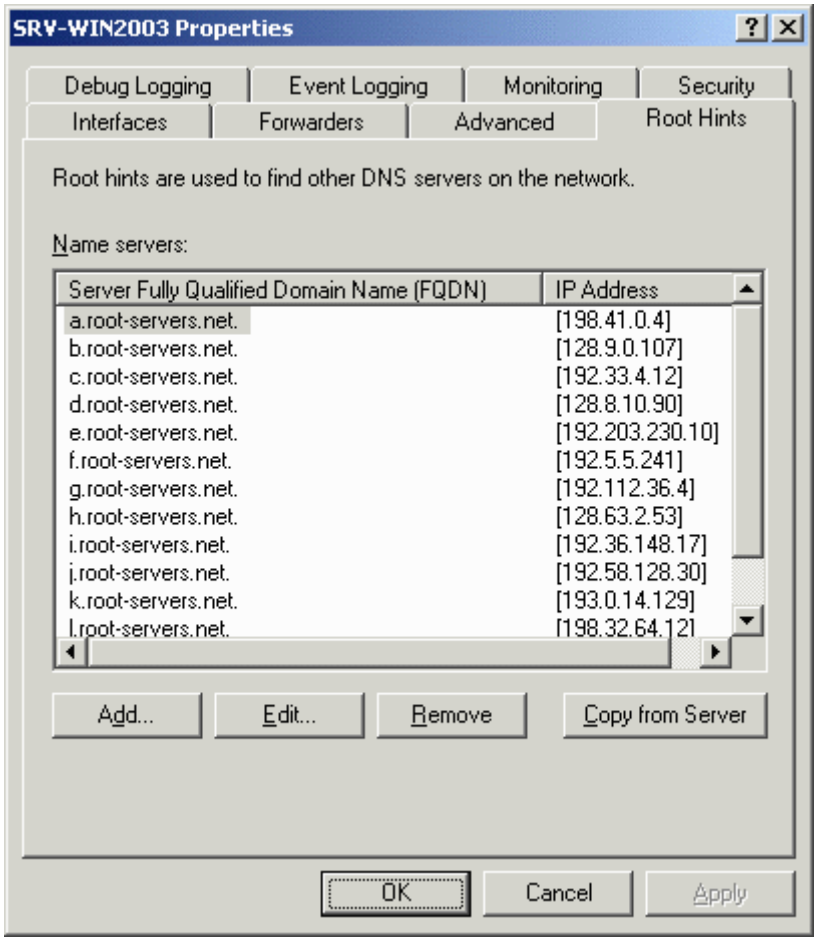


Figura - Lista de root hints do servidor DNS.

Com o uso da lista de servidores root hints, o servidor DNS consege localizar (teoricamente), os servidores DNS responsáveis por quaisquer domínio registrado.

Vamos novamente considerar um exemplo, para entender como o processo de recursão funciona. Imagine que a consulta enviada pelo cliente é para descobrir o endereço IP associado ao nome srv01.vendas.abc.com. O cliente que fez esta consulta está usando um computador da rede xyz.com, o qual está configurado para usar, como DNS primário, o DNS da empresa xyz.com.

Primeiro vamos assumir que o nome não pode ser resolvido localmente no cliente (usando o cache DNS local e o arquivo hosts) e foi enviado para o servidor DNS primário da empresa xyz.com. Este DNS é dono, é autoridade apenas para o domínio xyz.com e não para vendas.abc.com (lembrando sempre que a primeira parte do nome é o nome da máquina, conhecido como nome de host). Com isso o servidor DNS primário da empresa xyz.com.br irá pesquisar no cache do servidor DNS. Não encontrando a resposta no cache, é iniciado o processo de recursão, com os passos descritos a seguir:

1. O servidor DNS retira apenas a parte correspondente ao domínio (o nome todo, menos a primeira parte. No nosso exemplo seria vendas.abc.com, srv01 é o nome de host). Usando a lista de servidores DNS configurados como root hints, o servidor DNS localiza um servidor que seja o dono, a autoridade para o domínio root da Internet, representado pelo ponto (o processo é assim mesmo, de trás para frente).

2. Localizado o servidor responsável pelo domínio root, o servidor DNS da empresa xyz.com envia uma consulta interativa para o servidor DNS responsável pelo domínio root, perguntando: **"Você sabe quem é o servidor DNS responsável pelo domínio .com?"**. O servidor DNS root responde com o endereço IP de um dos servidores DNS responsáveis pelo domínio .com. Ou seja, o servidor DNS root não sabe responder diretamente o nome que

está sendo resolvido, mas sabe para quem enviar, sabe a quem recorrer. Talvez daí venha o nome do processo recursão.

3. O servidor DNS do domínio xyz.com recebe a resposta informando qual o servidor DNS responsável pelo domínio .com.

4. O servidor DNS do domínio xyz.com envia uma consulta para o servidor DNS responsável pelo .com (informado no passo 3), perguntando: **"Você é a autoridade para abc.com ou saberia informar quem é a autoridade para abc.com?"**

5. O servidor DNS responsável pelo domínio .com não é a autoridade para abc.com, mas sabe informar quem é a autoridade deste domínio. O servidor DNS responsável pelo .com retorna para o servidor DNS do domínio xyz.com, o número IP do servidor DNS responsável pelo domínio abc.com.

6. O servidor DNS do domínio xyz.com recebe a resposta informando o número IP do servidor responsável pelo domínio abc.com.

7. O servidor DNS do domínio xyz.com envia uma consulta para o servidor DNS responsável pelo abc.com (informado no passo 6), perguntando: **"Você é a autoridade para vendas.abc.com ou saberia informar quem é a autoridade para vendas.abc.com?"**

8. O servidor DNS responsável pelo abc.com não é a autoridade para vendas.abc.com, mas sabe informar quem é a autoridade deste domínio. O servidor DNS responsável pelo abc.com retorna para o servidor DNS do domínio xyz.com, o número IP do servidor DNS responsável pelo domínio vendas.abc.com.

9. O servidor DNS do domínio xyz.com recebe a resposta informando o número IP do servidor responsável pelo domínio vendas.abc.com.

10. O servidor DNS do domínio xyz.com envia uma consulta para o servidor DNS responsável pelo vendas.abc.com (informado no passo 9), perguntando: **"Você é a autoridade para vendas.abc.com ou saberia informar quem é a autoridade para vendas.abc.com?"**

11. O servidor DNS para vendas.abc.com recebe a consulta para resolver o nome srv01.vendas.abc.com. Como este servidor é a autoridade para o domínio, ele pesquisa a zona vendas.abc.com, encontra o registro para o endereço serv01.vendas.abc.com e retornar esta informação para o servidor DNS do domínio xyz.com.

12. O servidor DNS do domínio xyz.com recebe a resposta da consulta, faz uma cópia desta resposta no cache do servidor DNS e retornar o resultado para o cliente que originou a consulta.

13, No cliente o resolver recebe o resultado da consulta, repassa este resultado para o programa que gerou a consulta e grava uma cópia dos dados no cache local do DNS.

Evidentemente que a descrição do processo demora muito mais tempo do que o DNS realmente leva para resolver um nome usando este método. Claro que a resolução é rápida, senão ficaria praticamente impossível usar a Internet. Além disso, este método traz algumas vantagens. Durante esta espécie de "pingue-pongue" entre o servidor DNS e os servidores DNS da Internet, o servidor DNS da empresa vai obtendo informações sobre os servidores DNS da Internet e grava estas informações no cache local do servidor DNS. Isso agiliza futuras consultas e reduz, significativamente, o tempo para a resolução de nomes usando o processo de recursão. Estas informações são mantidas na memória do servidor e com o passar do tempo podem ocupar um espaço considerável da memória. Toda vez que o serviço DNS for parado e iniciado novamente, estas informações serão excluídas da memória e o processo de cache inicia novamente.

Considerações e tipos especiais de resoluções

O processo descrito anteriormente, termina com o servidor DNS (após ter consultado vários outros servidores) retornando uma resposta positiva para o cliente, isto é, conseguindo resolver o nome e retornando a informação associada (normalmente o número IP associado ao nome) para o cliente. Mas nem sempre a resposta é positiva, muitos outros tipos de resultados podem ocorrer em resposta a uma consulta, tais como:

- **An authoritative answer (resposta com autoridade):** Este tipo de resposta é obtido quando o nome é resolvido diretamente pelo servidor DNS que é a autoridade para o domínio pesquisado. Por exemplo, um usuário da Intranet da sua empresa (abc.com.br), tenta acessar uma página da intranet da empresa, por exemplo: rh.abc.com.br. Neste caso a consulta será enviada para o servidor DNS da empresa, o qual é a autoridade para a zona abc.com.br, com isso o servidor DNS da empresa, responde diretamente à consulta, informando o número IP do servidor rh.abc.com.br. É também uma resposta positiva só que com autoridade, ou seja, respondida diretamente pelo servidor DNS que é a autoridade para o domínio pesquisado, sem a necessidade de usar recursão.

- **A positive answer (resposta positiva):** É uma resposta com o resultado para o nome pesquisado, isto é, o nome pôde ser resolvido e uma ou mais informações associadas ao nome são retornadas para o cliente.

- **A referral answer (uma referência):** Este tipo de resposta não contém a resolução do nome pesquisado, mas sim informações e referência a recursos ou outros servidores DNS que podem ser utilizados para a resolução do nome. Este tipo de resposta será retornado para o cliente, se o servidor DNS não suportar o método de recursão, descrito anteriormente. As informações retornadas por uma resposta deste tipo são utilizadas pelo cliente para continuar a pesquisa, usando um processo conhecido como interação (o qual será descrito mais adiante). O cliente faz a pesquisa em um servidor DNS e recebe, como resposta, uma referência a outro recurso ou servidor DNS. Agora o cliente irá interagir com o novo recurso ou servidor DNS, tentando resolver o nome. Este processo pode continuar até que o nome seja resolvido ou até que uma resposta negativa seja retornada, indicando que o nome não pode ser resolvido. O processo de interação será descrito mais adiante.

- **A negative answer (uma resposta negativa):** Esta resposta pode indicar que um dos seguintes resultados foi obtido em resposta à consulta: Um servidor DNS que é autoridade para o domínio pesquisado, informou que o nome pesquisado não existe neste domínio ou um servidor DNS que é autoridade para o domínio pesquisado, informou que o nome pesquisado exsite, mas o tipo de registro não confere.

Uma vez retornada a resposta, o resolver interpreta o resultado da resposta (seja ela positiva ou negativa) e repassa a resposta para o programa que fez a solicitação para resolução de nome. O resolver armazena o resultado da consulta no cache local do DNS.

Dica Importante: O administrador do DNS pode desabilitar o recurso de recursão em um servidor DNS em situações onde os usuários devem estar limitados a utilizar apenas o servidor DNS da Intranet da empresa.

O servidor DNS também define tempos máximos para determinadas operações. Uma vez atingido o tempo máximo, sem obter uma resposta à consulta, o servidor DNS irá retornar uma resposta negativa:

- **Intervalo de reenvio de uma consulta recursiva – 3 segundos:** Este é o tempo que o DNS espera antes de enviar novamente uma consulta (caso não tenha recebido uma resposta) feita a um servidor DNS externo, durante um processo recursivo.

- **Intervalo de time-out para um consulta recursiva – 15 segundos:** Este é o tempo que o DNS espera antes de determinar que uma consulta recursiva, que foi reenviada falhou.

Estes parâmetros podem ser alterados pelo Administrador do DNS.

Como funciona o processo de interação

O processo de interação é utilizado entre o cliente DNS (resolver) e um ou mais servidores DNS, quando ocorrerem as condições indicadas a seguir:

- O cliente tenta utilizar o processo de recursão, discutido anteriormente, mas a recursão está desabilitada no servidor DNS.

- O cliente não solicita o uso de recursão, ao pesquisar o servidor DNS.

- O cliente faz uma consulta ao servidor DNS, informando que é esperada a melhor resposta que o servidor DNS puder fornecer imediatamente, sem consultar outros servidores DNS.

Quando o processo de interação é utilizado, o servidor DNS responde à consulta do cliente com base nas informações que o servidor DNS tem sobre o domínio pesquisado. Por exemplo, o servidor DNS da sua rede interna pode receber uma consulta de um cliente tentando resolver o nome www.abc.com. Se este nome estiver no cache do servidor DNS ele responde positivamente para o cliente. Se o nome não estiver no cache do servidor DNS, o servidor DNS responde com uma lista de servidores de referência, que é uma lista de registros do tipo NS e A (você aprenderá sobre os tipos de registro na parte prática), registros estes que apontam para outros servidores DNS, capazes de resolver o nome pesquisado. Ou seja, o cliente recebe uma lista de servidores DNS para os quais ele deve enviar a consulta. Observem a diferença básica entre o processo de recursão e o processo de interação. Na recursão, o servidor DNS é que entra em contato com outros servidores (root hints), até conseguir resolver o nome pesquisado. Uma vez resolvido o nome, ele retorna a resposta para o cliente. Já no processo de interação, se o servidor DNS não consegue resolver o nome, ele retorna uma lista de outros servidores DNS que talvez possam resolver o nome pesquisado. O cliente recebe esta lista e envia a consulta para os servidores DNS informados. Este processo (esta interação) continua até que o nome seja resolvido ou que uma resposta negativa seja recebida pelo cliente, informando que o nome não pode ser resolvido. Ou seja, no processo de interação, a cada etapa do processo, o servidor DNS retorna para o cliente, uma lista de servidores DNS a serem pesquisados, até que um dos servidores responde positivamente (ou negativamente) à consulta feita pelo cliente.

Como funciona o cache nos servidores DNS

O trabalho básico do servidor DNS é responder às consultas enviadas pelos clientes, quer seja utilizando recursão ou interação. A medida que os nomes vão sendo resolvidos, esta informação fica armazenada no cache do servidor DNS. Com o uso do cache, futuras consultas à nomes já resolvidos, podem ser respondidas diretamente a partir do cache do servidor DNS, sem ter que utilizar recursão ou interação. O uso do cache agiliza o processo de resolução de nomes e também reduz o tráfego de rede gerado pelo DNS.

Quando as informações são gravadas no cache do servidor DNS, um parâmetro chamado Time-To-Live (TTL) é associado com cada informação. Este parâmetro determina quanto tempo a informação será mantida no cache até ser descartada. O parâmetro TTL é utilizado para que as informações do cache não se tornem desatualizadas e para minimizar a possibilidade de envio de informações desatualizadas em resposta às consultas dos clientes. O valor padrão do parâmetro TTL é 3600 segundos (uma hora). Este parâmetro pode ser configurado pelo administrador do DNS, conforme será mostrado na parte prática, nas partes de 21 a 50, as quais constituem o Módulo 2 deste curso.

Aviso Importante: Por padrão o Servidor DNS utiliza um arquivo chamado Cache.dns, o qual fica gravado na pasta systemroot\System32\Dns, onde systemroot representa a pasta onde o Windows 2000 Server ou Windows Server 2003 está instalado. Este arquivo não tem a ver com o Cache de nomes do servidor DNS. Neste arquivo está contida a lista de servidores root hints (descritos anteriormente). O conteúdo deste arquivo é carregado na memória do servidor, durante a inicialização do serviço do DNS e é utilizado para localizar os servidores root hints da Internet, servidores estes utilizados durante o processo de recursão, descrito anteriormente.

Definindo DHCP

O DHCP é a abreviatura de Dynamic Host Configuration Protocol. O DHCP é um serviço utilizado para automatizar as configurações do protocolo TCP/IP nos dispositivos de rede (computadores, impressoras, hubs, switchs, ou seja, qualquer dispositivo conectado à rede e que esteja utilizando o protocolo TCP/IP).

Sem o uso do DHCP, o administrador da rede e a sua equipe teriam que configurar, manualmente, as propriedades do protocolo TCP/IP em cada dispositivo de rede (genericamente denominados hosts). Com o uso do DHCP esta tarefa pode ser completamente automatizada. O uso do DHCP traz diversos benefícios, dentro os quais podemos destacar os seguintes:

- Automação do processo de configuração do protocolo TCP/IP nos dispositivos da rede.

- Facilidade de alteração de parâmetros tais como Default Gateway, Servidor DNS e assim por diante, em todos os dispositivos da rede, através de uma simples alteração no servidor DHCP.

- Eliminação de erros de configuração, tais como digitação incorreta de uma máscara de sub-rede ou utilização do mesmo número IP em dois dispositivos diferentes, gerando um conflito de endereço IP.

Introdução ao DHCP

Neste tópico apresentarei uma série de conceitos teóricos sobre o funcionamento do DHCP. Você aprenderá como funciona o processo de concessão de endereços IP (também conhecido como lease), aprenderá sobre os conceitos de escopo, superescopo, reserva de endereço, ativação do servidor DHCP no Active Directory e demais conceitos relacionados ao DHCP.

O que é o DHCP - Dynamic Host Configuration Protocol?

Você aprendeu sobre os fundamentos do protocolo TCP/IP, que um equipamento de rede, que utiliza o protocolo TCP/IP precisa que sejam configurados uma série de parâmetros. Os principais parâmetros que devem ser configurados para que o protocolo TCP/IP funcione corretamente são os seguintes:

- Número IP
- Máscara de sub-rede
- Default Gateway (Gateway Padrão)
- Número IP de um ou mais servidores DNS
- Número IP de um ou mais servidores WINS
- Sufixos de pesquisa do DNS

Em uma rede com centenas ou até mesmo milhares de estações de trabalho, configurar o TCP/IP manualmente, em cada estação de trabalho é uma tarefa bastante trabalhosa, que envolve tempo e exige uma equipe técnica para executar este trabalho. Além disso, sempre que houver mudanças em algum dos parâmetros de configuração (como por exemplo uma mudança no número IP do servidor DNS), a reconfiguração terá que ser feita manualmente

em todas as estações de trabalho da rede. Por exemplo, imagine que o número IP do Default Gateway teve que ser alterado devido a uma reestruturação da rede. Neste caso a equipe de suporte teria que ir de computador em computador, alterando as propriedades do protocolo TCP/IP, para informar o novo número IP do Default Gateway, isto é, alterando o número IP antigo do Default Gateway para o novo número. Um trabalho e tanto.

Além disso, com a configuração manual, sempre podem haver erros de configuração. Por exemplo, basta que o técnico que está configurando uma estação de trabalho, digite um valor incorreto para a máscara de sub-rede, para que a estação de trabalho não consiga mais se comunicar com a rede. E problemas como este podem ser difíceis de detectar. Muitas vezes o técnico pode achar que o problema é com a placa de rede, com o driver da placa ou com outras configurações. Até descobrir que o problema é um simples erro na máscara de sub-rede pode ter sido consumido um bom tempo: do técnico e do funcionário que utiliza o computador, o qual ficou sem poder acessar a rede. E hoje em dia sem acesso á rede significa, na prática, sem poder trabalhar.

Bem, descrevo estas situações apenas para ilustrar o quanto é difícil e oneroso manter a configuração do protocolo TCP/IP manualmente, quando temos um grande número de estações de trabalho em rede. Pode até nem ser "tão grande" este número, com redes a partir da 30 ou 50 estações de trabalho já começa a ficar difícil a configuração manual do protocolo TCP/IP.

Para resolver esta questão e facilitar a configuração e administração do protocolo TCP/IP é que foi criado o DHCP. DHPC é a abreviatura de: Dynamic Host Configuration Protocol (Protocolo de configuração dinâmica de hosts). Você pode instalar um ou mais servidores DHCP em sua rede e fazer com que os computadores e demais dispositivos que precisem de configurações do TCP/IP, obtenham estas configurações, automaticamente, a partir do servidor DHCP.

Por exemplo, considere uma estação de trabalho configurada para utilizar o DHCP. Durante a inicialização, esta estação de trabalho entra em um processo de "descobrir" um servidor DHCP na rede (mais adiante detalharei como é este processo de "descoberta" do servidor DHCP). Uma vez que a estação de trabalho consegue se comunicar com o servidor DHCP, ela recebe todas as configurações do protocolo TCP/IP, diretamente do servidor DHCP. Ou seja, com o uso do DHCP, o administrador pode automatizar as configurações do protocolo TCP/IP em todas os computadores da rede.

Com o uso do DHCP, a distribuição de endereços IP e demais configurações do protocolo TCP/IP (máscara de sub-rede, default gateway, número IP do servidor DNS e assim por diante) é automatizada e centralizadamente gerenciada. O administrador cria faixas de endereços IP que serão distribuídas pelo servidor DHCP (faixas estas chamadas de escopos) e associa outras configurações com cada faixa de endereços, tais como um número IP do Default Gateway, a máscara de sub-rede, o número IP de um ou mais servidores DNS, o número IP de um ou mais servidores WINS e assim por diante.

Todo o trabalho de configuração do protocolo TCP/IP que teria que ser feito manualmente, agora pode ser automatizado com o uso do DHCP. Imagine somente uma simples situação, mas que serve para ilustrar o quanto o DHCP é útil. Vamos supor que você é o administrador de uma rede com 3000 estações de trabalho. Todas as estações de trabalho estão configuradas com o protocolo TCP/IP. As configurações são feitas manualmente, não é utilizado um servidor DHCP na rede. Você utiliza um único servidor externo, do seu provedor de Internet, com servidor DNS. O número IP deste servidor DNS está configurado em todas as estações de trabalho da rede. O seu Provedor de Internet sofreu uma reestruturação e teve que alterar o número IP do servidor DNS (veja que é uma situação que está fora do controle do administrador da rede, já que a alteração foi no servidor DNS do provedor). Como você configura o TCP/IP manualmente nos computadores da rede, só resta uma solução: pôr a sua equipe em ação para visitar as 3000 estações de trabalho da rede, alterando o número IP do servidor DNS em cada uma delas. Em cada estação de trabalho o técnico terá que acessar as propriedades do protocolo TCP/IP e alterar o endereço IP do servidor DNS para o novo endereço. Um trabalho e tanto, sem contar que podem haver erros durante este processo.

Agora imagine esta mesma situação, só que ao invés de configurar o TCP/IP manualmente você está utilizando o DHCP para fazer as configurações do TCP/IP automaticamente. Nesta situação, quando houve a alteração do número IP do servidor DNS, bastaria alterar esta opção nas propriedades do escopo de endereços IP no servidor DHCP e pronto. Na próxima reinicialização, os computadores da rede já receberiam o novo número IP do servidor DNS, sem que você ou um único membro da sua equipe tivesse que reconfigurar uma única estação de trabalho. Bem mais simples, mais produtivo e menos propenso a erros.

Isso é o DHCP, um serviço para configuração automática do protocolo TCP/IP nos computadores e demais dispositivos da rede que utilizam o protocolo TCP/IP. Configuração feita de maneira automática e centralizada. Em redes baseadas em TCP/IP, o DHCP reduz a complexidade e a quantidade de trabalho administrativo envolvido na configuração e reconfiguração do protocolo TCP/IP.

Nota: A implementação do DHCP no Windows 2000 Server e no Windows Server 2003 é baseada em padrões definidos pelo IETF. Estes padrões são definidos em documentos conhecidos como RFCs (Request for Comments). As RFCs que definem os padrões do DHCP são as seguintes:

- RFC 2131: Dynamic Host Configuration Protocol (substitui a RFC 1541)
- RFC 2132: DHCP Options and BOOTP Vendor Extensions

As RFCs a seguir também podem ser úteis para compreender como o DHCP é usado com outros serviços na rede:

- RFC 0951: The Bootstrap Protocol (BOOTP)
- RFC 1534: Interoperation Between DHCP and BOOTP
- RFC 1542: Clarifications and Extensions for the Bootstrap Protocol
- RFC 2136: Dynamic Updates in the Domain Name System (DNS UPDATE)
- RFC 2241: DHCP Options for Novell Directory Services
- RFC 2242: Netware/IP Domain Name and Information

O site oficial, a partir da qual você pode copiar o conteúdo integral das RFCs disponíveis é o seguinte:

http://www.rfc-editor.org/

Termos utilizados no DHCP

O DHCP é composto de diverses elementos. O servidor DHCP e os clientes DHCP. No servidor DHCP são criados escopos e definidas as configurações que os clientes DHCP irão receber. A seguir apresento uma série de termos relacionados ao DHCP. Estes termos serão explicados em detalhes até o final desta lição.

Termos utilizados no DHCP:

- **Servidor DHCP:** É um servidor com o Windows 2000 Server ou com o Windows Server 2003, onde foi instalado e configurado o serviço DHCP. Após a instalação de um servidor DHCP ele tem que ser autorizado no Active Directory, antes que ele possa, efetivamente, atender a requisições de clientes. O procedimento de autorização no Active Directory é uma medida de segurança, para evitar que servidores DHCP sejam introduzidos na rede sem o conhecimento do administrador. O servidor DHCP não pode ser instalado em um computador com o Windows 2000 Professional, Windows XP Professional ou Windows Vista.

- **Cliente DHCP:** É qualquer dispositivo de rede capaz de obter as configurações do TCP/IP a partir de um servidor DHCP. Por exemplo, uma estação de trabalho com o Windows 95/98/Me, Windows NT Workstation 4.0, Windows 2000 Professional,

Windows XP, Windows Vista, uma impressora com placa de rede habilitada ao DHCP e assim por diante.

- **Escopo**: Um escopo é o intervalo consecutivo completo des endereços IP possíveis para uma rede (por exemplo, a faixa de 10.10.10.100 a 10.10.10.150, na rede 10.10.10.0/255.255.255.0). Em geral, os escopos definem uma única sub-rede física, na rede na qual serão oferecidos serviços DHCP. Os escopos também fornecem o método principal para que o servidor gerencie a distribuição e atribuição de endereços IP e outros parâmetros de configuração para clientes na rede, tais como o Default Gateway, Servidor DNS e assim por diante..

- **Superescopo**: Um superescopo é um agrupamento administrativo de escopos que pode ser usado para oferecer suporte a várias sub-redes IP lógicas na mesma sub-rede física. Os superescopos contêm somente uma lista de escopos associados ou escopos filho que podem ser ativados em cojunto. Os superescopos não são usados para configurar outros detalhes sobre o uso de escopo. Para configurar a maioria das propriedades usadas em um superescopo, você precisa configurar propriedades de cada escopo associado, individualmente. Por exemplo, se todos os computadores devem receber o mesmo número IP de Default Gateway, este número tem que ser configurado em cada escopo, individualmente. Não tem como fazer esta configuração no Superescopo e todos os escopos (que compõem o Superescopo), herdarem estas configurações.
-
- **Intervalo de exclusão**: Um intervalo de exclusão é uma seqüência limitada de endereços IP dentro de um escopo, excluído dos endereços que são fornecidos pelo DHCP. Os intervalos de exclusão asseguram que quaisquer endereços nesses intervalos não são oferecidos pelo servidor para clientes DHCP na sua rede. Por exemplo, dentro da faixa 10.10.10.100 a 10.10.10.150, na rede 10.10.10.0/255.255.255.0 de um determinado escopo, você pode criar uma faixa de exclusão de 10.10.10.120 a 10.10.10.130. Os endereços da faixa de exclusão não serão utilizados pelo servidor DHCP para configurar os clientes DHCP.

- **Pool de endereços**: Após definir um escopo DHCP e aplicar intervalos de exclusão, os endereços remanescentes formam o pool de endereços disponíveis dentro do escopo. Endereços em pool são qualificados para atribuição dinâmica pelo servidor para clientes DHCP na sua rede. No nosso exemplo, onde temos o escopo com a faixa 10.10.10.100 a 10.10.10.150, com uma faixa de exclusão de 10.10.10.120 a 10.10.10.130, o nosso pool de endereços é formado pelos endereços de 10.10.10.100 a 10.10.10.119, mais os endereços de 10.10.10.131 a 10.10.10.150.

- **Concessão:** Uma concessão é um período de tempo especificado por um servidor DHCP durante o qual um computador cliente pode usar um endereço IP que ele recebeu do servidor DHCP (diz-se atribuído pelo servidor DHCP). Uma concessão está ativa quando ela está sendo utilizada pelo cliente. Geralmente, o cliente precisa renovar sua atribuição de concessão de endereço com o servidor antes que ela expire. Uma concessão torna-se inativa quando ela expira ou é excluída no servidor. A duração de uma concessão determina quando ela irá expirar e com que freqüência o cliente precisa renová-la no servidor.

- **Reserva:** Você usa uma reserva para criar uma concessão de endereço permanente pelo servidor DHCP. As reservas asseguram que um dispositivo de hardware especificado na sub-rede sempre pode usar o mesmo endereço IP. A reserva é criada associada ao endereço de Hardware da placa de rede, conhecido como MAC-Address. No servidor DHCP você cria uma reserva, associando um endereço IP com um endereço MAC. Quando o computador (com o endereço MAC para o qual existe uma reserva) é inicializado, ele entre em contato com o servidor DHCP. O servidor DHCP verifica que existe

uma reserva para aquele MAC-Address e configura o computador com o endereço IP associado ao Mac-address. Caso haja algum problema na placa de rede do computador e a placa tenha que ser substituída, mudará o MAC-Address e a reserva anterior terá que ser excluída e uma nova reserva terá que ser criada, utilzando, agora, o novo Mac-Address.

- **Tipos de opção**: Tipos de opção são outros parâmetros de configuração do cliente que um servidor DHCP pode atribuir aos clientes. Por exemplo, algumas opções usadas com freqüência incluem endereços IP para gateways padrão (roteadores), servidores WINS (Windows Internet Name System) e servidores DNS (Domain Name System). Geralmente, esses tipos de opção são ativados e configurados para cada escopo. O console de Administração do serviço DHCP também permite a você configurar tipos de opção padrão que são usados por todos os escopos adicionados e configurados no servidor. A maioria das opção é predefinida através da RFC 2132, mas você pode usar o console DHCP para definir e adicionar tipos de opção personalizados, se necessário.

Como o DHCP funciona

O DHCP utiliza um modelo cliente/servidor. O administrador da rede instala e configura um ou mais servidores DHCP. As informações de configuração – escopos de endereços IP, reservas e outras opções de configuração – são mantidas no banco de dados dos servidores DHCP. O banco de dados do servidor inclui os seguintes itens:

- Parâmetros de configuração válidos para todos os cliente na rede (número IP do Default Gateway, número IP de um ou mais servidores DNS e assim por diante). Estas configurações podem ser diferentes para cada escopo.

- Endereços IP válidos mantidos em um pool para serem atribuídos aos clientes além de reservas de endereços IP.

- Duração das concessões oferecidas pelo servidor. A concessão define o período de tempo durante o qual o endereço IP atribuído pode ser utilizado pelo cliente. Conforme mostrarei mais adiante, o cliente tenta renovar esta concessão em períodos definidos, antes que a concessão expire.

Com um servidor DHCP instalado e configurado na rede, os clientes com DHCP podem obter os endereços IP e os parâmetros de configuração relacionados, dinamicamente, sempre que forem inicializados. Os servidores DHCP fornecem essa configuração na forma de uma oferta de concessão de endereço para os clientes solicitantes.

Clientes suportados pelo DHCP

O termo Cliente é utilizado para descrever um computador ligado à rede e que obtém as configurações do protocolo TCP/IP a partir de um servidor DHCP. Qualquer computador com o Windows (qualquer versão) instalado ou outros dispositivos, capazes de se comunicar com o servidor DHCP e obter as configurações do TCP/IP a partir do servidor DHCP, é considerado um cliente DHCP.

Os clientes DHCP podem ser quaisquer clientes baseados no Microsoft Windows ou outros clientes que oferecem suporte e são compatíveis com o comportamento do cliente descrito no documento padrão de DHCP, que é a RFC 2132, publicado pela Internet Engineering Task Force - IETF.

Exemplo prático: Configurando um cliente baseado no Windows para que seja um cliente do DHCP: Para configurar um computador com o Windows 2000 para ser um cliente DHCP, siga os passos indicados a seguir:

1. Faça o logon com a conta de Administrador ou com uma conta com permissão de administrador.

2. Abra o Painel de controle: Iniciar -> Configurações -> Painel de controle.

3. Abra a opção Conexões dial-up e de rede.

4. Clique com o botão direito do mouse na conexão de rede local a ser configurada. No menu de opções que é exibido clique em Propriedades.

5. Será exibida a janela de propriedades da conexão de rede local.

6. Clique na opção Protocolo Internet (TCP/IP) para selecioná-la. Clique no botão Propriedades, para abrir a janela de propriedades do protocolo TCP/IP.

7. Nesta janela você pode configurar o endereço IP, a máscara de sub-rede e o Gateway padrão, manualmente. Para isso basta marcar a opção Utilizar o seguinte endereço IP e informar os endereços desejados.

8. Para configurar o computador para utilizar um servidor DHCP, para obter as configurações do TCP/IP automaticamente, marque a opção **Obter um endereço IP automaticamente**, conforme indicado na Figura a seguir. Marque também a opção Obter o endereço dos servidores DNS automaticamente, para obter o endereço IP do servidor DNS a partir das configurações fornecidas pelo DHCP.

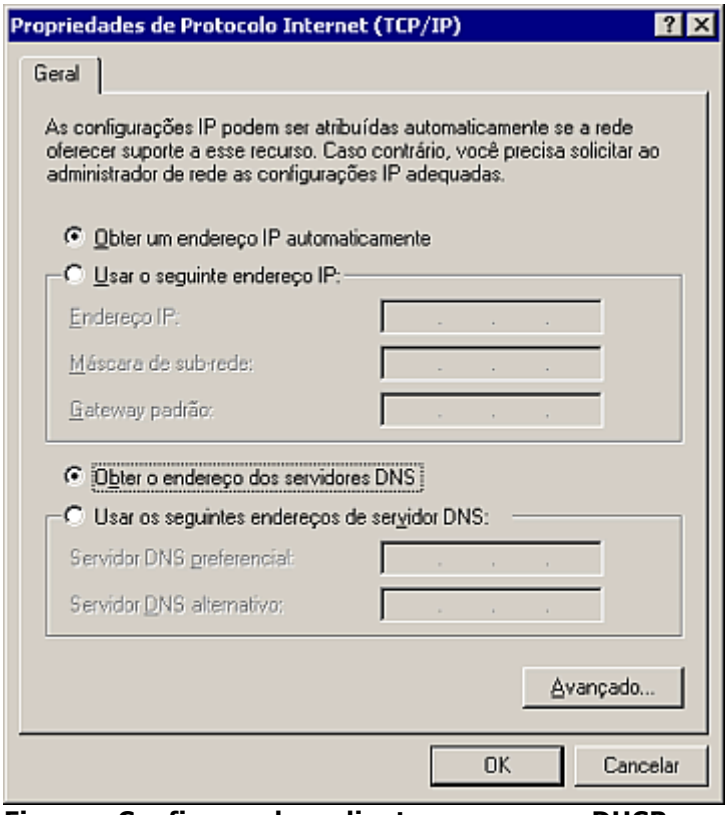


Figura - Configurando o cliente para usar o DHCP.

9. Clique em OK para fechar a janela de propriedades do TCP/IP.

10. Você estará de volta à janela de propriedades da conexão de rede local.

11. Clique em OK para fechá-la e aplicar as alterações efetudas. Ao clicar em OK, o cliente DHCP já tentará se conectar com um servidor DHCP e obter as configurações do protocolo TCP/IP, a partir do servidor DHCP.

O servidor DHCP dá suporte as seguintes versões do Windows (e do MS- DOS) com clientes DHCP:

- Windows Longhorn Server
- Windows Vista
- Windows Server 2003 (todas as edições)
- Windows 2000 Server (todas as edições)
- Windows XP Home e Professional
- Windows NT (todas as versões lançadas)
- Windows Me
- Windows 98
- Windows 95
- Windows for Workgroups versão 3.11 (com o Microsoft 32 bit TCP/IP VxD instalado)
- Microsoft-Network Client versão 3.0 para MS-DOS (com o driver TCP/IP de modo real instalado)
- LAN Manager versão 2.2c

Um recurso de nome esquisito APIPA

APIPA é a abreviatura de Automatic Private IP Addressing. Esta é uma nova funcionalidade que foi introduzida no Windows 98, está presente no Windows 2000, Windows XP, Windows Vista, Longhorn Server e no Windows Server 2003. Imagine um cliente com o protocolo TCP/IP instalado e configurado para obter as configurações do protocolo TCP/IP a partir de um servidor DHCP. O cliente é inicializado, porém não consegue se comunicar com um servidor DHCP. Neste situação, o Windows, usa o recurso APIPA, e automaticamente atribui um endereço IP da rede 169.254.0.0/255.255.0.0. Este é um dos endereços especiais, reservados para uso em redes internas, ou seja, este não seria um endereço de rede, válido na Internet. A seguir descrevo mais detalhes sobre a funcionalidade APIPA.

Não esqueça: O número de rede usado pelo recurso APIPA é o seguinte:
169.254.0.0/255.255.0.0

Nota: O recurso APIPA é especialmente útil para o caso de uma pequena rede, com 4 ou 5 computadores, onde não existe um servidor disponível. Neste caso você pode configurar todos os computadores para usarem o DHCP. Ao inicializar, os clientes não conseguirão localizar um servidor DHCP (já que não existe nenhum servidor DHCP nesta rede do nosso exemplo). Neste caso o recurso APIPA atribuirá endereços da rede 169.254.0.0/255.255.0.0 para todos os computadores da rede. O resultado final é que todos ficam configurados com endereços IP da mesma rede e poderão se comunicar, compartilhando recursos entre si. É uma boa solução para um rede doméstica ou de um pequeno escritório.

Configuração automática do cliente

Se os clientes estiverem configurados para usar um servidor DHCP (em vez de serem configurados manualmente com um endereço IP e outros parâmetros), o serviço do cliente DHCP entrará em funcionamento a cada vez que o computador for inicializado. O serviço do cliente DHCP usa um processo de três etapas para configurar o cliente com um endereço IP e outras informações de configuração.

- O cliente DHCP tenta localizar um servidor DHCP e obter as configurações do protocolo TCP/IP, a partir desse servidor.

- Se um servidor DHCP não puder ser encontrado, o cliente DHCP configura automaticamente seu endereço IP e máscara de sub-rede usando um endereço selecionado da rede classe B reservada, 169.254.0.0, com a máscara de sub-rede,

255.255.0.0 (recurso APIPA). O cliente DHCP irá fazer uma verificação na rede, para ver se o endereço que ele está se auto-atribuindo (usando o recurso APIPA) já não está em uso na rede. Se o endereço já estiver em uso será caracterizado um conflito de endereços. Se um conflito for encontrado, o cliente selecionará outro endereço IP. A cada conflito de endereço, o cliente irá tentar novamente a configuração automática após 10 tentativas ou até que seja utilizado um endereço que não gere conflito.

- Depois de selecionar um endereço no intervalo de rede 169.254.0.0 que não está em uso, o cliente DHCP irá configurar a interface com esse endereço. O cliente continua a verificar se um servidor DHCP não está disponível. Esta verificação é feita a cada cinco minutos. Se um servidor DHCP for encontrado, o cliente abandonará as informações configuradas automaticamente (endereço da rede 169.254.0.0/255.255.0.0). Em seguida, o cliente DHCP usará um endereço oferecido pelo servidor DHCP (e quaisquer outras informações de opções de DHCP fornecidas) para atualizar as definições de configuração IP.

Caso o cliente DHCP já tenha obtido previamente uma concessão de um servidor DHCP (durante uma inicialização anterior) e esta concessão ainda não tenha expirado, ocorrerá a seguinte seqüência modificada de eventos, em relação a situação anterior:

- Se a concessão de cliente ainda estiver válida (não expirada) no momento da inicialização, o cliente irá tentar renovar a concessão com o servidor DHCP.

- Se durante a tentativa de renovação o cliente não conseguir localizar qualquer servidor DHCP, ele irá tentar efetuar o ping no gateway padrão que ele recebeu do servidor DHCP anteriormente. Dependendo do sucesso ou falha do ping, o cliente DHCP procederá conforme o seguinte:

1. Se um ping para o gateway padrão for bem-sucedido, o cliente DHCP presumirá que ainda está localizado na mesma rede em que obteve a concessão atual e continuará a usar a concessão. Por padrão, o cliente irá tentar renovar a concessão quando 50 por cento do tempo de concessão tiver expirado.

2. Se uma solicitação de ping do gateway padrão falhar, o cliente presumirá que foi movido para uma rede em que não estão disponíveis servidores DHCP, como uma rede doméstica ou uma rede de uma pequena empresa, onde não está disponível servidor DHCP (pode ser o exemplo de um vendedor conectando um notebook em um ponto da rede de um pequeno cliente).

O cliente irá configurar automaticamente o endereço IP conforme descrito anteriormente. Uma vez que configurado automaticamente, o cliente continua a tentar localizar um servidor DHCP a cada cinco minutos e obter uma nova concessão de endereço IP e de demais configurações.

Não esqueça: APIPA é isso. A sigla é mais complicada do que a funcionalidade. Se você está se preparando para os exames de Certificação do Windows 2000 Server, fique atento a esta funcinalidade. Normalmente aparecem questões envolvendo conhecimentos desta funcionalidade.

Entendendo o que é e como funciona o WINS

O Windows Internet Name Service – WINS é um serviço para resolução de nomes. Mais um, pode perguntar o amigo leitor. Sim, além do DNS o Windows 2000 Server (a exemplo do Windows Server 2003 e do NT Server 4.0) também fornece mais um serviço para resolução de nomes – WINS.

O WINS tem muitas diferenças em relação ao DNS. A primeira e fundamental delas é que o WINS não forma um espaço de nomes hierárquico como o DNS. O espaço de nomes do WINS é plano (flat).

Em uma base de dados WINS fica registrado apenas o nome NetBios do computador e o respectivo número IP. Poderíamos até dizer que o WINS está para a resolução de nomes NetBios, assim como o DNS está para a resolução de nomes FQDN.

A grande questão que continua é: "Porque dois serviços diferentes para a resolução de nomes"?? O que acontece é que até o NT Server 4.0, o WINS era o serviço de resolução de nomes mais utilizado e o suporte ao DNS só erá obrigatório se aglum serviço dependesse do DNS. Na época do NT Server 4.0, com a maioria dos clientes baseados em Windows 95/98 (ou até mesmo Windows 3.11), o WINS era o serviço de nomes mais utilizado. Porém a partir do Windows 2000 Server, com o Active Directory, o DNS passou a ser o serviço preferencial para a resolução de nomes (e obrigatório para o caso do Active Directory).

Porém da mudança do WINS para o DNS, obviamente que existe um período de transição. É exatamente este período que estamos vivendo, ou seja, com clientes (Windows 95/98/Me) e aplicativos que ainda dependem do WINS. Por isso que, muito provavelmente, você ainda precsará do WINS para dar suporte a estes clientes e aplicativos mais antigos, ainda dependentes do WINS.

Com o WINS, sempre que um cliente configurado para utilizar um servidor WINS, é inicializado, o cliente, automaticamente, registra o seu nome NetBios e o respectivo endereço IP, na base de dados do servidor configurado como Wins Primário, nas propriedades do TCP/IP do cliente. Os nomes NetBios podem ter até 15 caracteres. Na verdade são 16 caracteres, mas o décimo sexto é reservado para uso do sistema operacional. O Windows 2000 Server registra, para um mesmo computador, o nome NetBios mais de uma vez, apenas mudando o décimo sexto caractere. Este caractere indica um serviço específico no computador. Falarei mais sobre estes nomes logo adiante.

Algumas características do WINS

O WINS apresenta as seguintes características:

- Um banco de dados dinâmico de nomes NetBios para endereço IP, o qual fornece o suporte para resolução e registro do nome NetBios dos computadores da rede. O serviço WINS é instalado em um ou mais servidores da rede. O número IP do servidor WINS deve ser informado nos clientes, quer seja configurando manualmente as propriedades do protocolo TCP/IP do cliente, quer seja através do uso do DHCP para efetuar estas configurações.

- Gerenciamento centralizado do banco de dados de nome para endereço, minorando a necessidade de gerenciamento de arquivos Lmhosts. O arquivo Lmhosts é um arquivo de texto, na qual podem ser criadas entradas para resolução de nomes NetBios. O arquivo Lmhosts fica na pasta systemroot\system32\drivers\etc, onde systemroot representa a pasta onde está instalado o Windows 2000 Server, Windows XP ou Windows Server 2003. Podemos dizer que o Lmhosts representa para o WINS, o mesmo que o arquivo hosts representa para o DNS. Na verdade, na pasta indicada anteriormente, é gravado, por padrão, um arquivo chamado Lmhosts.sam. O administrador, caso necessite utilizar um arquivo Lmhosts, pode renomear este arquivo (de Lmhosts.sam para Lmhosts) e criar as entradas necessárias.
- O uso do WINS fornece Redução de tráfego de broadcast, gerado para a reoslução de nome NetBios. Se os clientes dependentes do WINS, não estiverem configurados com o número IP de pelo menos um servidor WINS, eles irão gerar tráfego de Broadcast na rede local, para tentar resolver nomes. Por padrão os roteadores

bloqueiam tráfego de broadcast. Com isso, sem o uso do WINS, para clientes que dependem do WINS, não haveria como fazer a resolução de nomes de servidores que estão em outras redes (redes remotas, ligadas através de links de WAN e roteadores). Através do mecanismo de replicação, é possível manter vários servidores WINS, em diferentes redes, com o mesmo banco de dados, com informações de todos os computadores da rede, mediante o uso de replicação.

- É possível integrar o WINS com o DNS, para que o WINS possa respodner consultas às quais o DNS não conseguiu responder.

Como saber se ainda devo utilizar o WINS?

Pode parecer que o WINS tem muitas vantagens, então deve realmente ser utilizado. Não é bem assim. Só é justificado o uso do WINS se houver versões antigas do Windows (Windows 3.11, Windows 95, Windows 98 ou Windows Me) ou aplicações que dependam do WINS. Neste ítem vou detalhar um pouco mais sobre em que situações você ainda terá que utilizar o WINS.

Antes de mostrar quando você deve utilizar, vou descrever algumas situações em que, **com certeza, você não precisará utilizar o WINS**:

- A sua rede é baseada apenas em servidores como Windows 2000 Server ou Windows Server 2003 e os clientes são baseados no Windows 2000 Professional, Windows XP Professional ou Windows Vista. Com uma rede nesta situação, com certeza o DNS está instalado e funcionando. Nesta situação não existe nenhuma dependência do WINS para a resolução de nomes, uma vez que o DNS atende perfeitamente a necessidade de resolução de nomes no cenário proposto.

- Se você tem uma pequena rede, com até 20 computadores, localizados em um único escritório, e a rede é utilizada para compartilhamento de arquivos, impressoras e para aplicações, não é necessário o uso do WINS. Mesmo que alguns clientes ou aplicações necessitem de resolução de nome NetBios, poderão fazê-lo, sem problemas, usando broadcast. Devido ao pequeno número de computadores, o tráfego de broadcast, devido à resolução de nomes NetBios não representará um problema.

Ao decidir se precisa usar o WINS, você deve primeiro considerar as seguintes questões:

- Tenho computadores na rede que exigem o uso de nomes de NetBIOS? Lembre que todos os computadores em rede que estiverem sendo executados com um sistema operacional da Microsoft antigo, como as versões do MS-DOS, Windows 95/98 ou Windows NT 3.51/4.0, exigem suporte a nomes de NetBIOS. O Windows 2000 é o primeiro sistema operacional da Microsoft que não requer mais a nomeação de NetBIOS. Portanto, os nomes de NetBIOS ainda podem ser exigidos na rede para fornecer serviços de compartilhamento de arquivo e impressão básicos e para oferecer suporte a diversas aplicações existentes, as quais ainda dependam da resolução de nomes NetBios. Por exemplo, um cliente baseado no Windows 95, depende do nome NetBios do servidor, para poder acessar uma pasta compartilhada no servidor. Você não conseguirá usar o nome DNS do sevidor, como por exemplo: \\srv01.abc.com\documentos, em clientes com versões antigas do Windows, conforme as descritas no início deste parágrafo. Nestes clientes você tem que usar o nome NetBios do servidor, como por exemplo: \\srv01\documentos.

- Todos os computadores na rede estão configurados e são capazes de oferecer suporte ao uso de outro tipo de nomeação de rede, como por exemplo o DNS (Domain Name System, sistema de nomes de domínios)? A nomeação de rede é um serviço vital para a localização de computadores e recursos por toda a rede, mesmo quando os nomes NetBIOS não sejam exigidos. Antes de decidir eliminar o suporte a nomes de NetBIOS ou WINS, certifique-se de que todos os computadores e programas na rede são capazes de funcionar usando outro serviço de nomes, como o DNS. Nesta etapa é muito importante que você tenha um inventário de software

atualizado. Com o inventário de software você tem condição de saber quais programas ainda dependem da resolução de nomes NetBios.

Os clientes WINS que estejam executando sob o Windows 2000, Windows Server 2003 ou Windows XP Professional, são configurados por padrão para usar primeiro o DNS para resolver nomes com mais de 15 caracteres ou que utilizem pontos (".") dentro do nome. Para nomes com menos de 15 caracteres e que não utilizem pontos, o Windows primeira tenta resolver o nome usando WINS (se este estiver configurado), caso o WINS venha a falhar, o DNS será utilizado na tentativa de resolver o nome.

Clientes suportados pelo WINS

O WINS é suportado por uma grande variedade de clientes, conforme descrito na lista a seguir:

- Windows Server 2003
- Windows 2000
- Windows NT 3.5 ou superior
- Windows 95/98/Me
- Windows for Workgroups 3.11
- MS-DOS com Cliente de Rede Microsoft versão 3
- MS-DOS com LAN Manager versão 2.2c
- Clientes Linux e UNIX, rodando o servço Samba

Nota: É possível criar entradas estáticas no WINS (criadas manualmente), para clientes não suportados pelo WINS. Porém esta não é uma prática recomendada e somente deve ser utilizada quando for absolutamente necessária.

Não esqueça: Fique atento a este ponto, ou seja, criação de entradas estáticas. Por exemplo, se você tem clientes antigos, como o Windows 95 ou Windows 98, que precisam acessar recursos em um servidor UNIX ou Linux, o qual não pode ser cliente do WINS, ou seja, não é capaz de registrar seu nome no WINS, o que fazer? Neste caso você deve criar uma entrada estática no WINS, para o nome do servidor UNIX ou Linux e o respectivo endereço IP. Com isso, os clientes mais antigos poderão acessar os recursos do servidor UNIX.

Como funciona o WINS

Os servidores WINS mantém uma base de dados com nomes dos clientes configurados para utilizar o WINS e os respectivos endereços IP. Quando uma estação de trabalho configurada para utilizar o WINS é inicializada, ela registra o seu nome NetBios e o seu endereço IP no banco de dados do servidor WINS. A estação de trabalho utiliza o servidor WINS, cujo endereço IP está configurado como WINS Primário, nas propriedades do protocolo TCP/IP (quer estas configurações tenham sido feitas manualmente ou via DHCP. Para informações detalhadas sobre o DHCP). Quando o cliente é desligado, o registro do nome e do endereço IP é liberado no servidor WINS. Com isso a base de dados do WINS é criada e mantida, dinamicamente.

Os nomes NetBios podem ter, no máximo 15 caracteres. Um 16º caractere é registrado pelo serviço WINS. Este caractere adicional é utilizado para indicar um determinado tipo de serviço. Por exemplo, um servidor pode ter o seu nome registrado no WINS várias vezes. O que diferencia um registro do outro é o 16º caractere, o qual indica diferentes serviços. O 16º caractere está no formato de número Hexadecimal. A seguir, a título de exemplo, alguns dos valores possíveis para o 16º caractere e o respectivo significado:

- nome_de_domínio[1Bh]: Registrado por cada controlador de domínio do Windows NT Server 4.0 que esteja executando como PDC (Primary Domain Controller) do respectivo domínio. Esse registro de nome é usado para permitir a procura remota de domínios. Quando um servidor WINS é consultado para obtenção desse nome, ele retorna o endereço IP do computador que registrou o nome.

- nome_de_computador[1Fh]: Registrado pelo serviço Network Dynamic Data Exchange (NetDDE, intercâmbio dinâmico de dados de rede). Ele aparecerá somente se os serviços NetDDE forem iniciados no computador.

Você pode exibir a lista de nomes (na verdade o mesmo nome, apenas diferenciando o 16º caractere) registrados para um determinado computador, utilizando o seguinte comando:

nbtstat –a nome_do_computador

Por exemplo, o comando a seguir retorna a lista de nomes registrados no WINS, pelo computador chamado servidor:

nbtstat –a servidor

Este comando retorna o resultado indicado a seguir:

C:\>nbtstat -a servidor

Local Area Connection:
Node IpAddress: [10.10.20.50] Scope Id: []

NetBIOS Remote Machine Name Table

Name	Type	Status
SERVIDOR	<00> UNIQUE	Registered
SERVIDOR	<20> UNIQUE	Registered
GROZA	<00> GROUP	Registered
GROZA	<1C> GROUP	Registered
GROZA	<1B> UNIQUE	Registered
GROZA	<1E> GROUP	Registered
SERVIDOR	<03> UNIQUE	Registered
GROZA	<1D> UNIQUE	Registered
..__MSBROWSE__.	<01> GROUP	Registered
INet~Services	<1C> GROUP	Registered
IS~SERVIDOR....	<00> UNIQUE	Registered
ADMINISTRADOR	<03> UNIQUE	Registered

MAC Address = 00-00-21-CE-01-11

Para que as estações de trabalho da rede possam utilizar o servidor WINS, basta informar o número IP do servidor WINS nas propriedades avançadas do protocolo TCP/IP da estação de trabalho. Uma vez configurado com o número IP do servidor WINS, o cliente, durante a inicialização, registra o seu nome NetBios, automaticamente com o servidor WINS.

O cliente WINS utiliza diferentes métodos para a resolução de nomes NetBios. Estes diferentes métodos são identificados como: b-node, p-node, m-node e h-node. A seguir descrevo a diferença entre estes métodos:

- **b-node:** Um cliente configurado com este método de resolução utiliza somente broadcast para a resolução de nomes NetBios. Se não houver um servidor WINS na rede ou o servidor WINS não estiver configurado nas propriedades avançadas do TCP/IP, este é o método padrão utilizado.

- **p-node:** Utiliza somente o servidor WINS. Se o WINS falhar em resolver o nome, o cliente não tentará outro método.

- **m-node:** Utiliza primeiro broadcast, se não conseguir resolver o nome usando broadcast, então utiliza o servidor WINS.

- **h-node:** Primeiro utiliza o servidor WINS, somente se o WINS falhar é que será tentado o broadcast. Este método reduz o tráfego de broadcast na rede. É o método padrão para clientes configurados para utilizar um servidor WINS.

Um pouco sobre Pacotes e sobre os protocolos de Transporte

O TCP/IP, na verdade, é formado por um grande conjunto de diferentes protocolos e serviços de rede. O nome TCP/IP deriva dos dois protocolos mais importantes e mais utilizados, que são os seguintes:

- **IP:** É um protocolo de endereçamento, um protocolo de rede. Eu me arriscaria a afirmar que as principais funções do protocolo IP são endereçamento e roteamento, ou de uma maneira mais simples, fornecer uma maneira para identificar unicamente cada máquina da rede (endereço IP) e uma maneira de encontrar um caminho entre a origem e o destino (Roteamento).

- **TCP:** O TCP é um protocolo de transporte e executa importantes funções para garantir que os dados sejam entregues de uma maneira confiável, ou seja, sem que os dados sejam corrompidos ou alterados.

Vamos imaginar uma situação prática, onde você deseja enviar um arquivo com cerca de 10 MB de um computador de origem para um computador de destino. Uma das primeiras coisas que tem que ser feitas é encontrar uma rota, um caminho entre a origem e o destino. Este é o papel do protocolo IP, mais especificamente da função de roteamento. Uma vez encontrado o caminho, o próximo passo é dividir o arquivo de 10 MB em pacotes de tamanhos menores, os quais possam ser enviados pelos equipamentos da rede. Além da divisão em pacotes menores, o TCP/IP tem que garantir que os pacotes sejam entregues sem erros e sem alterações. Pode também acontecer de os pacotes chegarem fora de ordem. O TCP/IP tem que ser capaz de identificar a ordem correta e entregar os pacotes para o programa de destino, na ordem correta. Por exemplo, pode acontecer de o pacote número 10 chegar antes do pacote número 9. Neste caso o TCP tem que aguardar a chegada do pacote número 9 e entregá-los na ordem correta. Pode também acontecer de serem perdidos pacotes durante o transporte. Neste caso, o TCP tem que informar à origem de que determinado pacote não foi recebido no tempo esperado e solicitar que este seja retransmitido. Todas estas funções – garantir a integridade, a seqüência correta e solicitar retransmissão – são exercidas pelo protocolo TCP – Transmission Control Protocol. Além do TCP existe também o UDP, o qual não faz todas estas verificaçõe e é utilizado por determinados serviços. A seguir apresento uma descrição dos protocolos TCP e UDP e um estudo comparativo.

TCP – Uma Visão Geral

O Transmission Control Protocol (TCP) é, sem dúvidas, um dos mais importantes protocolos da família TCP/IP. É um padrão definido na RFC 793, "Transmission Control Protocol (TCP)", que fornece um serviço de entrega de pacotes confiável e orientado por conexão. Ser orientado por conexão, significa que todos os aplicativos baseados em TCP como protocolo de transporte, antes de iniciar a troca de dados, precisam estabelecer uma conexão. Na conexão são fornecidas, normalmente, informações de logon, as quais identificam o usuário que está tentando estabelecer a conexão. Um exemplo típico são os aplicativos de FTP (Cute – FTP, ES-FTP e assim por diante). Para que você acesse um servidor de FTP, você deve fornecer um nome de usuário e senha. Estes dados são utilizados para identificar e autenticar o usuário. Após a identificação e autenticação, será estabelecida uma sessão entre o cliente de FTP e o servidor de FTP.

Algumas características do TCP:

- **Garante a entrega de datagramas IP:** Esta talvez seja a principal função do TCP, ou seja, garantir que os pacotes sejam entregues sem alterações, sem terem sido corrompidos e na ordem correta. O TCP tem uma série de mecanismos para garantir esta entrega.

- **Executa a segmentação e reagrupamento de grandes blocos de dados enviados pelos programas e Garante o seqüenciamento adequado e entrega ordenada de dados segmentados:** Esta característica refere-se a função de dividir grandes arquivos em pacotes menores e transmitir cada pacote separadamente. Os pacotes podem ser enviados por caminhos diferentes e chegar fora de ordem. O TCP tem mecanismos para garantir que, no destino, os pacotes sejam ordenados corretamente, antes de serem entregues ao programa de destino.

- **Verifica a integridade dos dados transmitidos usando cálculos de soma de verificação:** O TCP faz verificações para garantir que os dados não foram alterados ou corrompidos durante o transporte entre a origem e o destino.

- **Envia mensagens positivas dependendo do recebimento bem-sucedido dos dados. Ao usar confirmações seletivas, também são enviadas confirmações negativas para os dados que não foram recebidos**: No destino, o TCP recebe os pacotes, verifica se estão OK e, em caso afirmativo, envia uma mensagem para a origem, confirmando cada pacote que foi recebido corretamente. Caso um pacote não tenha sido recebido ou tenha sido recebido com problemas, o TCP envia uma mensagem ao computador de origem, solicitando uma retransmissão do pacote. Com esse mecanismo, apenas pacotes com problemas terão que ser reenviados, o que reduz o tráfego na rede e agiliza o envio dos pacotes.

- **Oferece um método preferencial de transporte de programas que devem usar transmissão confiável de dados baseada em sessões, como bancos de dados cliente/servidor e programas de correio eletrônico:** Ou seja, o TCP é muito mais confiável do que o UDP (conforme mostrarei mais adiante) e é indicado para programas e serviços que dependam de uma entrega confiável de dados.

Funcionamento do TCP

O TCP baseia-se na comunicação ponto a ponto entre dois hosts de rede. O TCP recebe os dados de programas e processa esses dados como um fluxo de bytes. Os bytes são agrupados em segmentos que o TCP numera e seqüência para entrega. Estes segmentos são mais conhecidos como "***Pacotes***".

Antes que dois hosts TCP possam trocar dados, devem primeiro estabelecer uma sessão entre si. Uma sessão TCP é inicializada através de um processo conhecido como um tree-way handshake (algo como Um Aperto de Mão Triplo). Esse processo sincroniza os números de seqüência e oferece informações de controle necessárias para estabelecer uma conexão virtual entre os dois hosts.

De uma maneira simplificada, o processo de tree-way handshake, pode ser descrito através dos seguintes passos:

- **O computador de origem solicita o estabelecimento de uma sessão com o computador de destino:** Por exemplo, você utiliza um programa de FTP (origem) para estabelecer uma sessão com um servidor de FTP (destino).

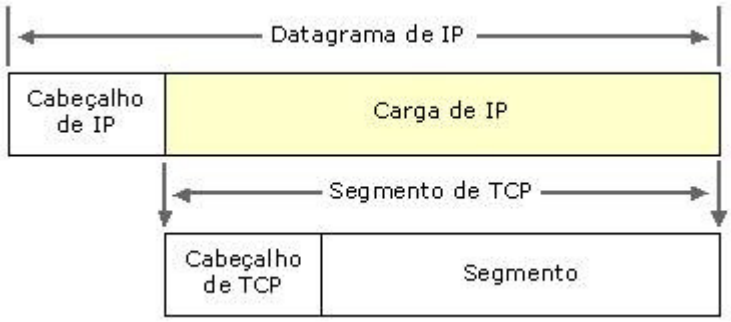
- O computador de destino recebe a requisição, verifica as credenciais enviadas (tais como as informações de logon e senha) e envia de volta para o cliente, informações que serão utilizadas pelo cliente, para estabelecer efetivamente a sessão. As informações enviadas nesta etapa são importantes, pois é através destas informações que o servidor irá identificar o cliente e liberar ou não o acesso.

- O computador de origem recebe as informações de confirmação enviadas pelo servidor e envia estas confirmações de volta ao servidor. O servidor recebe as informações, verifica que elas estão corretas e estabelece a sessão. A partir deste momento, origem e destino estão autenticados e aptos a trocar informações usando o protocolo TCP. Se por algum motivo, as informações enviadas pela origem não

estiverem corretas, a sessão não será estabelecida e uma mensagem de erro será enviada de volta ao computador de origem.

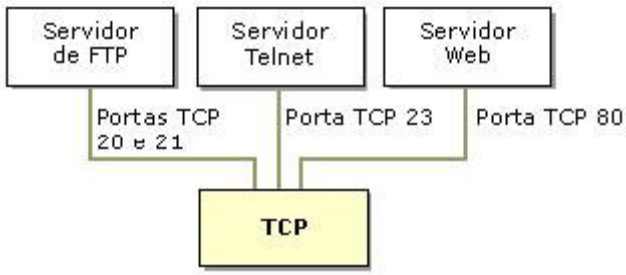
Depois de concluído o tree-way handshake inicial, os segmentos são enviados e confirmados de forma seqüencial entre os hosts remetente e destinatário. Um processo de handshake semelhante é usado pelo TCP antes de fechar a conexão para verificar se os dois hosts acabaram de enviar e receber todos os dados.

Os segmentos TCP são encapsulados e enviados em datagramas IP, conforme apresentado na figura a seguir, obtida na ajuda do Windows 2000 Server:



O conceito de Portas TCP

Os programas TCP usam números de porta reservados ou conhecidos, conforme apresentado na seguinte ilustração, da ajuda do Windows 2000 Server:



O que é uma Porta TCP?

Bem, sem entrar em detalhes técnicos do TCP/IP, vou explicar, através de um exemplo prático, o conceito de porta. Vamos imaginar um usuário, utilizando um computador com conexão à Internet. Este usuário, pode, ao mesmo tempo, acessar um ou mais sites da Internet, usar o Outlook Express para ler suas mensagens de email, estar conectado a um servidor de FTP, usando um programa como o WS-FTP, para fazer download de um ou mais arquivos, estar jogando DOOM através da Internet e assim por diante.

Todas as informações que este usuário recebe estão chegando através de pacotes que chegam até a placa de Modem ou até o Modem ADSL, no caso de uma conexão rápida. A pergunta que naturalmente surge é:

Como o sistema sabe para qual dos programas se destina cada um dos pacotes que estão chegando no computador?

Por exemplo, chega um determinado pacote. Este pacote é para uma das janelas do Navegador, é para o cliente de FTP, é um comando do DOOM, é referente a uma mensagem de email ou quem é o destinatário deste pacote? A resposta para esta questão é o mecanismo de portas utilizado pelo TCP/IP. Cada programa trabalha com um

protocolo/serviço específico, ao qual está associado um número de porta. Por exemplo, o serviço de FTP, normalmente opera na porta 21 (na verdade usa duas portas, uma para controle e outra para o envio de dados). Todo pacote que for enviado do servidor FTP para o cliente, terá, além dos dados que estão sendo enviados, uma série de dados de controle, tais como o número do pacote, código de validação dos dados e também o número da porta. Quando o pacote chega no seu computador, o sistema lê no pacote o número da porta e sabe para quem encaminhar o pacote. Por exemplo, se você está utilizando um cliente de FTP para fazer um download, os pacotes que chegarem, com informação de Porta = 21, serão encaminhados para o cliente de FTP, o qual irá ler o pacote e dar o destino apropriado. Outro exemplo, o protocolo HTTP, utilizado para o transporte de informações de um servidor Web até o seu navegador, opera, por padrão, na porta 80. Os pacotes que chegarem, destinados à porta 80, serão encaminhados para o navegador. Se houver mais de uma janela do navegador aberta, cada uma acessando diferentes páginas, o sistema inclui informações, além da porta, capazes de identificar cada janela individualmente. Com isso, quando chega um pacote para a porta 80, o sistema identifica para qual das janelas do navegador se destina o referido pacote.

Em resumo: O uso do conceito de portas, permite que vários programas estejam em funcionamento, ao mesmo tempo, no mesmo computador, trocando informações com um ou mais serviços/servidores.

O lado do servidor de cada programa que usa portas TCP escuta as mensagens que chegam no seu número de porta conhecido. Todos os números de porta de servidor TCP menores que 1.024 (e alguns números mais altos) são reservados e registrados pela Internet Assigned Numbers Authority (IANA, autoridade de números atribuídos da Internet). Por exemplo, o serviço HTTP (servidor Web), instalado em um servidor, fica sempre "escutando" os pacotes que chegam ao servidor. Os pacotes destinados a porta 80, serão encaminhados pelo sistema operacional para processamento do servidor Web.

A tabela a seguir é uma lista parcial de algumas portas de servidor TCP conhecidas usadas por programas baseados em TCP padrão.

Número de porta TCP	Descrição
20	Servidor FTP (File Transfer Protocol, protocolo de transferência de arquivo) (canal de dados)
21	Servidor FTP (canal de controle)
23	Servidor Telnet
53	Transferências de zona DNS (Domain Name System, sistema de nomes de domínios)
80	Servidor da Web (HTTP, Hypertext Transfer Protocol, protocolo de transferência de hipertexto)
139	Serviço de sessão de NetBIOS

Para obter uma lista atualizada e completa de todas as portas TCP conhecidas e registradas atualmente, consulte o seguinte endereço:

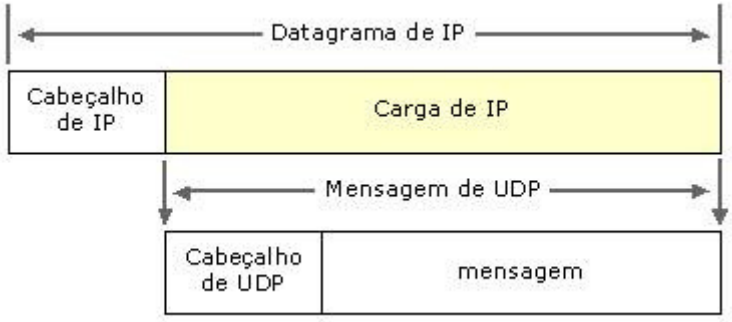
http://www.iana.org/assignments/port-numbers

UDP – Uma Visão Geral

O User Datagram Protocol (UDP) é um padrão TCP/IP e está definido pela RFC 768, "User Datagram Protocol (UDP)." O UDP é usado por alguns programas em vez de TCP para o transporte rápido de dados entre hosts TCP/IP. Porém o UDP não fornece garantia de entrega e nem verificação de dados. De uma maneira simples, dizemos que o protocolo UDP manda os dados para o destino; se vai chegar ou se vai chegar corretamente, sem erros, só Deus sabe. Pode parecer estranho esta característica do UPD, porém você verá que em determinadas situações, o fato de o UDP ser muito mais rápido do que o TCP (por não fazer verificações e por não estabelecer sessões), o uso do UDP é recomendado.

O protocolo UDP fornece um serviço de pacotes **sem conexão** que oferece entrega com base no melhor esforço, ou seja, UDP não garante a entrega ou verifica o seqüenciamento para qualquer pacote. Um host de origem que precise de comunicação confiável deve usar TCP ou um programa que ofereça seus próprios serviços de seqüenciamento e confirmação.

As mensagens UDP são encapsuladas e enviadas em datagramas IP, conforme apresentado na seguinte ilustração, da ajuda do Windows 2000 Server:



Portas UDP

O conceito de porta UDP é idêntico ao conceito de portas TCP, embora tecnicamente, existam diferenças na maneira como as portas são utilizadas em cada protocolo. A idéia é a mesma, por exemplo, se um usuário estiver utilizando vários programas baseados em UDP, ao mesmo tempo, no seu computador, é através do uso de portas, que o sistema operacional sabe a qual programa se destina cada pacote UDP que chega.

O lado do servidor de cada programa que usa UDP escuta as mensagens que chegam no seu número de porta conhecido. Todos os números de porta de servidor UDP menores que 1.024 (e alguns números mais altos) são reservados e registrados pela Internet Assigned Numbers Authority (IANA, autoridade de números atribuídos da Internet).

Cada porta de servidor UDP é identificada por um número de porta reservado ou conhecido. A tabela a seguir mostra uma lista parcial de algumas portas de servidor UDP conhecidas usadas por programas baseados em UDP padrão.

Número de porta UDP	**Descrição**
53	Consultas de nomes DNS (Domain Name System, sistema de nomes de domínios)
69	Trivial File Transfer Protocol (TFTP)
137	Serviço de nomes de NetBIOS
138	Serviço de datagrama de NetBIOS
161	Simple Network Management Protocol (SNMP)
520	Routing Information Protocol (RIP, protocolo de informações de roteamento)

Para obter uma lista atualizada e completa de todas as portas TCP conhecidas e registradas atualmente, consulte o seguinte endereço:

http://www.iana.org/assignments/port-numbers

Comparando UDP e TCP:

Geralmente, as diferenças na maneira como UDP e TCP entregam os dados assemelham-se às diferenças entre um telefonema e um cartão postal. O TCP funciona como um telefonema,

verificando se o destino está disponível e pronto para a comunicação. O UDP funciona como um cartão postal — as mensagens são pequenas e a entrega é provável, mas nem sempre garantida.

UDP é geralmente usado por programas que transmitem pequenas quantidades de dados ao mesmo tempo ou têm necessidades em tempo real. Nessas situações, a baixa sobrecarga do UDP (pois este não faz as verificações que são feitas pela TCP) e as capacidades de broadcast do UDP (por exemplo, um datagrama, vários destinatários) são mais adequadas do que o TCP.

O UDP contrasta diretamente com os serviços e recursos oferecidos por TCP. A tabela a seguir compara as diferenças em como a comunicação TCP/IP é tratada dependendo do uso de UDP ou TCP para o transporte de dados.

UDP	**TCP**
Serviço sem conexão; nenhuma sessão é estabelecida entre os hosts.	Serviço orientado por conexão; uma sessão é estabelecida entre os hosts.
UDP não garante ou confirma a entrega ou seqüência os dados.	TCP garante a entrega através do uso de confirmações e entrega seqüenciada dos dados.
Os programas que usam UDP são responsáveis por oferecer a confiabilidade necessária ao transporte de dados.	Os programas que usam TCP têm garantia de transporte confiável de dados.
UDP é rápido, necessita de baixa sobrecarga e pode oferecer suporte à comunicação ponto a ponto e ponto a vários pontos.	TCP é mais lento, necessita de maior sobrecarga e pode oferecer suporte apenas à comunicação ponto a ponto.

Tanto UDP quanto TCP usam portas para identificar as comunicações para cada programa TCP/IP, conforme descrito anteriormente.

Exemplos de utilização de portas

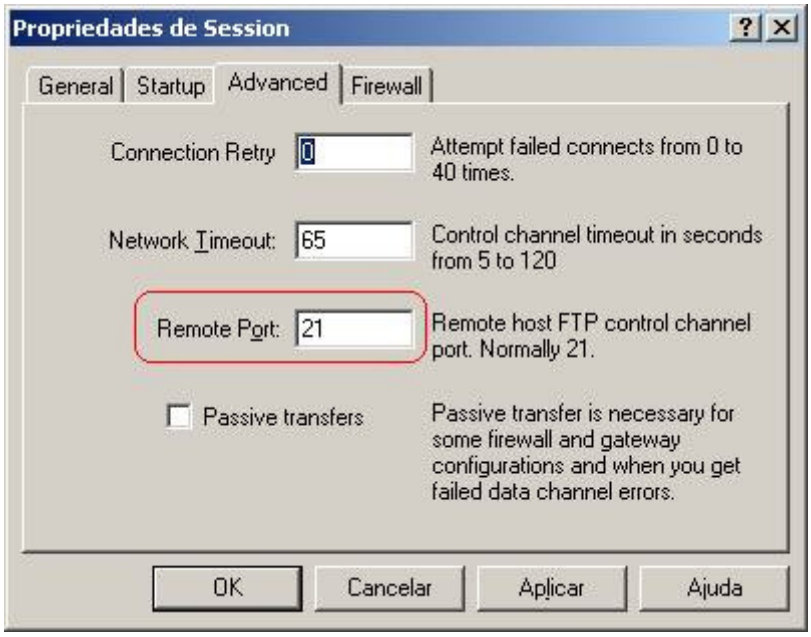
Embora provavelmente você nunca tenha notado, você utiliza portas de comunicação diversas vezes, como por exemplo ao acessar o seu email, ao fazer um download de um arquivo ou ao acessar uma página na Internet.

Quando você acessa um site na Internet, como por exemplo www.funam.com.br ou www.certificacoes.com.br ou www.uol.com.br, o navegador que você está utilizando se comunica com a porta 80 no servidor HTTP, do site que está sendo acessado. Você nem fica sabendo que está sendo utilizada a porta 80, pois esta é a porta padrão de comunicação, para o protocolo HTTP (Hypertext Transfer Protocol). Um detalhe interessante é que não é obrigatório que seja utilizada a porta padrão número 80, para a comunicação do HTTP. Por exemplo, o Administrador do IIS – Internet Information Services, que é o servidor Web da Microsoft, pode configurar um site para "responder" em uma porta diferente da Porta 80, conforme exemplo da Figura a seguir, onde o site foi configurado para responder na porta 470:

Quando for utilizada uma porta diferente da porta padrão 80, o número da porta deve ser informada após o endereço, colocando o sinal de dois pontos (:) após o endereço e o número da porta após o sinal de dois pontos, como no exemplo a seguir:

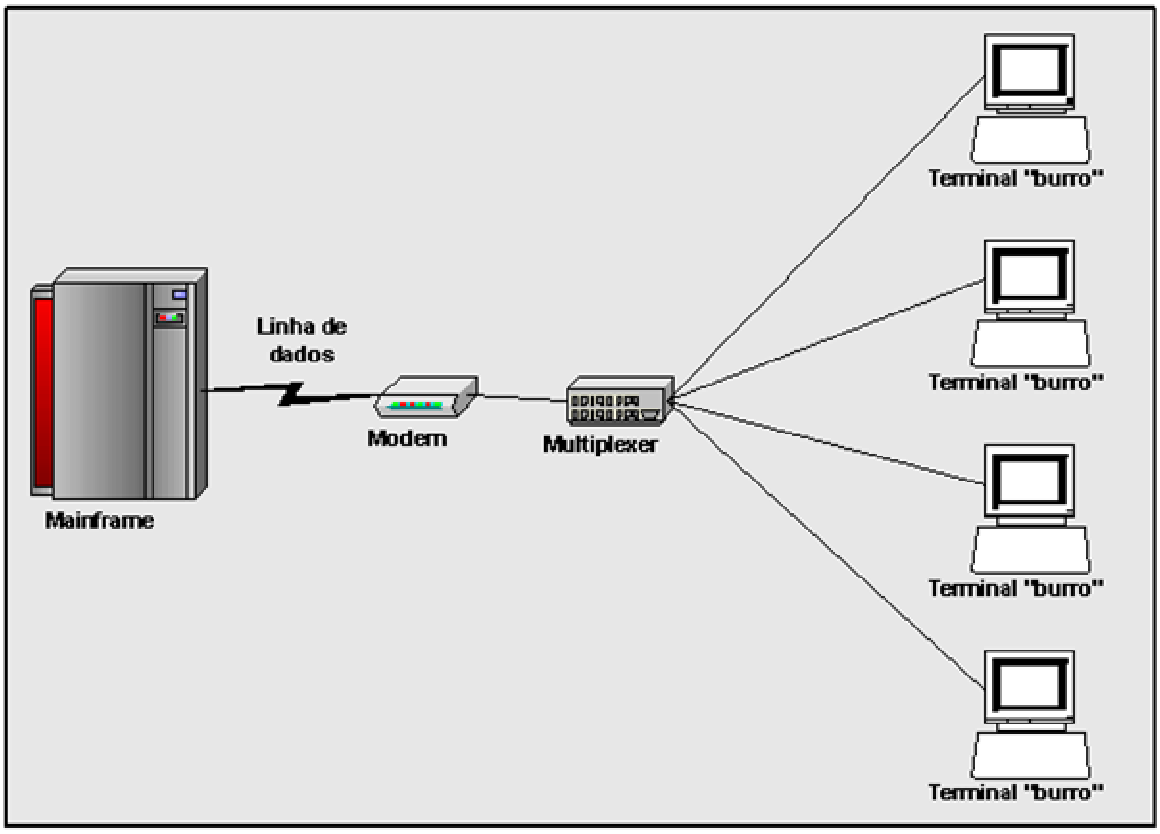
http://www.abc.com.br:470

Um outro exemplo do dia-a-dia, onde utilizamos o conceito de portas de comunicação, é quando você utiliza um cliente de FTP para se conectar a um servidor de FTP e fazer o download de um ou mais arquivos. Ao criar uma nova conexão de FTP, você deve informar o nome do servidor (ftp.abc.com.br, ftp.123.com.br, ftp.juliobattisti.com.br e assim por diante) e definir a porta de comunicação. Os principais clientes de FTP, já sugerem como padrão a porta 21, a qual é utilizada pelo protocolo FTP. No exemplo da figura a seguir, mostro uma tela do cliente de FTP **Cute FTP**, o qual é um dos mais utilizados. Nesta figura, mostro as configurações para conexão com o meu servidor de ftp, onde é utilizada a porta 21:

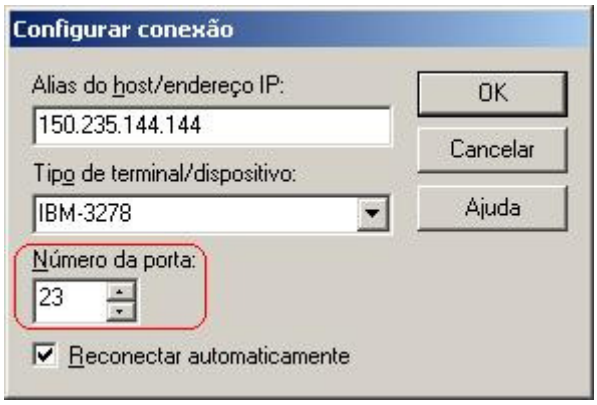


Outro uso muito comum nas redes da sua empresa é a criação de sessões de programas emuladores de terminal com sistemas que rodam no Mainframe da empresa. Apesar de terem anunciado a morte do Mainframe há algum tempo atrás, o fato é que o Mainframe continua mais vivo do que nunca e com grande parte dos sistemas empresariais ainda rodando no Mainframe.

A próxima figura descreve, resumidamente, como funciona a criação de seções, usando um software emulador de terminal, para acessar sistemas no Mainframe. Nas estações de trabalho da rede da empresa, é instalado um programa emulador de terminal. Estes progrmas, na maioria das vezes, emulam terminais no padrão **TN23270**. Este é um padrão da IBM muito utilizado para acesso à aplicações que estão no Mainframe. O programa emulador de terminal faz a conexão com o Mainframe, o usuário informa o seu logon e senha e, de acordo com as permissões atribuídas ao logon do usuário, são disponibilizados um ou mais sistemas. Quando o usuário vai criar uma sessão com o Mainframe, ele precisa informar o nome ou o número IP do Mainframe. Normalmente estas seções são feitas com base no serviço de Telnet (Terminal Emulator Link Over Network), o qual é baseado na porta de comunicação 23.



Na Figura a seguir, mostro o uso de um software emulador de terminal, no momento emque está sendo configurada uma nova seção, a qual será estabelecida via Telnet, utilizando a porta 23:



Estas são apenas três situações bastante comuns – acessar a Internet, fazer download de arquivos a partir de um servidor FTP e criar uma sessão com o Mainframe, - utilizados diariamente por usuários das redes de empresas de todo o mundo, onde são utilizados, na prática, o conceito de Portas de Comunicação, do TCP/IP, conceito este que foi discutido. A seguir apresentarei alguns comandos do Windows 2000/XP/2003, os quais exibem informações sobre as portas de comunicação que estão sendo utilizadas no seu computador. Se você não está conectado à rede de uma empresa, poderá utilizar estes comandos quando você estiver conectado á Internet, situação onde, certamente, estarão sendo utilizadas portas de comunicação.

O comando netstat – exibindo informações sobre portas

O comando netstat está disponível no Windows 2000, Windows XP e Windows Server 2003. Este comando exibe estatísticas do protocolo TCP/IP e as conexões atuais da rede TCP/IP. O comando netstat somente está disponível se o protocolo TCP/IP estiver instalado. A seguir apresento alguns exemplos de utilização do comando netstat e das opções de linha de comando disponíveis.

- **netstat –a**: O comando netstat com a opção –a Exibe todas as portas de conexões e de escuta. Conexões de servidor normalmente não são mostradas. Ou seja, o comando mostra as portas de comunicação que estão na escuta, isto é, que estão aptas a se comunicar. Na listagem a seguir mostro um exemplo do resultado da execução do comando netstat –a, em um computador com o nome micro01. O estado LISTENING significa, esperando, na escuta, ou seja, aceitando conexões na referida porta. O estado ESTABLISHED significa que existe uma conexão ativa na respectiva porta:

Conexões ativas

Proto	Endere‡o local	Endere‡o externo	Estado
TCP	MICRO01:epmap	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:microsoft-ds	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:1046	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:1051	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:1058	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:1097	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:1595	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:2176	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:2178	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:2216	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:2694	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:2706	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:3236	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:3279	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:3282	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:3285	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:3302	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:3322	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:3335	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:3336	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:3691	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:4818	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:4820	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:4824	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:4829	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:6780	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:6787	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:9495	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:42510	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:netbios-ssn	MICRO01.abc.com:0	LISTENING
TCP	MICRO01:microsoft-ds	MICRO02:1352	ESTABLISHED
TCP	MICRO01:1595	SERVIDOR02:microsoft-ds	ESTABLISHED
TCP	MICRO01:2694	SERVIDOR02:microsoft-ds	ESTABLISHED
TCP	MICRO01:2706	SERVIDOR03:1352	ESTABLISHED
TCP	MICRO01:3236	SERVFILES01:microsoft-ds	ESTABLISHED
TCP	MICRO01:3279	EMAILSERVER:microsoft-ds	ESTABLISHED
TCP	MICRO01:3282	EMAILSERVER:microsoft-ds	ESTABLISHED
TCP	MICRO01:3285	EMAILSERVER:microsoft-ds	ESTABLISHED
TCP	MICRO01:3323	DRFSTMSRV22:1352	TIME_WAIT
TCP	MICRO01:3335	66.139.77.16:http	CLOSE_WAIT
TCP	MICRO01:3336	66.139.77.16:http	CLOSE_WAIT
TCP	MICRO01:3691	SRV01:microsoft-ds	ESTABLISHED

```
  TCP    MICRO01:4200       MICRO01.abc.com:0  LISTENING
  TCP    MICRO01:4829       a209-249-123-216.deploy.akamaitechnologies.com:https
CLOSE_WAIT
  UDP    MICRO01:microsoft-ds  *:*
  UDP    MICRO01:1027       *:*
  UDP    MICRO01:1042       *:*
  UDP    MICRO01:1403       *:*
  UDP    MICRO01:3632       *:*
  UDP    MICRO01:3636       *:*
  UDP    MICRO01:38037      *:*
  UDP    MICRO01:38293      *:*
  UDP    MICRO01:netbios-ns  *:*
  UDP    MICRO01:netbios-dgm  *:*
  UDP    MICRO01:isakmp     *:*
  UDP    MICRO01:42508      *:*
  UDP    MICRO01:1186       *:*
  UDP    MICRO01:3212       *:*
  UDP    MICRO01:3221       *:*
  UDP    MICRO01:3555       *:*
```

- **netstat –e**: Esta opção exibe estatísticas sobre a interface Ethernet do computador. A interface Ethernet é, normalmente, a placa de rede local, que conecta o computador a rede da empresa. Esta opção pode ser combinada com a opção –s, que será descrita mais adiante. A seguir um exemplo da execução do comando netstat –e:

```
C:\>netstat -e
Estatísticas de interface

                           Recebido            Enviado

Bytes                     418376586          3178900324
Pacotes unicast             1801720             2703889
Pacotes não unicast          170291                5018
Descartados                       0                   0
Erros                             0                   0
Prot. desconhecidos           21303
```

- **netstat –n**: Exibe endereços e números de porta em forma numérica (em vez de tentar pesquisar o nome). A seguir um exemplo da execução do comando netstat –n:

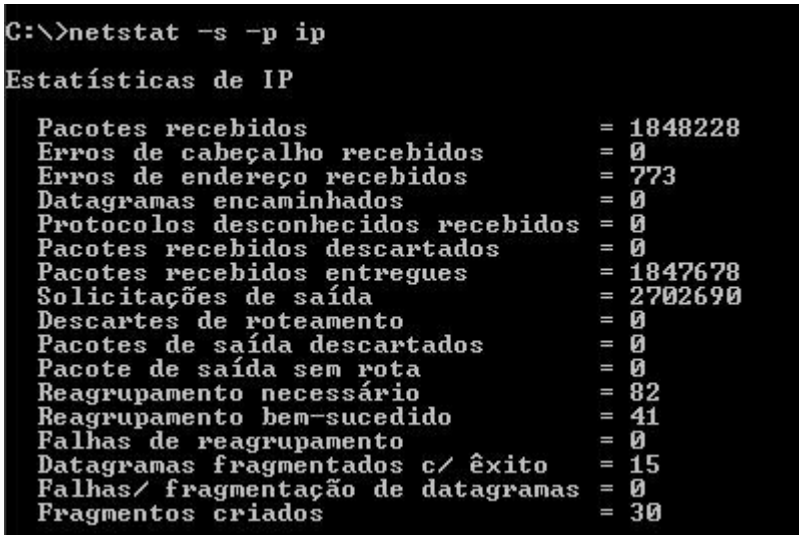
```
Conexões ativas

  Proto  Endereço local         Endereço externo       Estado
  TCP    100.200.50.50:1595     100.200.50.60:445      ESTABLISHED
  TCP    100.200.50.50:2694     100.200.50.45:445      ESTABLISHED
  TCP    100.200.50.50:2706     100.200.50.45:1352     ESTABLISHED
  TCP    100.200.50.50:3236     100.200.50.102:445     TIME_WAIT
  TCP    100.200.50.50:3381     100.200.50.45:1352     TIME_WAIT
  TCP    100.200.50.50:3399     100.200.50.40:445      ESTABLISHED
  TCP    100.200.50.50:3691     100.200.50.222:445     ESTABLISHED
  TCP    100.200.50.50:4829     135.200.240.133:443    CLOSE_WAIT
```

- **netstat –s**: Exibe estatística por protocolo. Por padrão, são mostradas estatísticas para TCP, UDP, ICMP (Internet Control Message Protocol, protocolo de acesso às mensagens de Internet) e IP. A opção -p pode ser utilizada para especificar um ou mais protocolos para os quais devem ser exibidas estatísticas. A seguir um exemplo da execução do comando netstat –n:

```
Estatisticas de IP
```

```
  Pacotes recebidos                = 1847793
  Erros de cabeçalho recebidos     = 0
  Erros de endereço recebidos      = 772
  Datagramas encaminhados          = 0
  Protocolos desconhecidos recebidos = 0
  Pacotes recebidos descartados    = 0
  Pacotes recebidos entregues      = 1847244
  Solicitações de saida            = 2702298
  Descartes de roteamento          = 0
  Pacotes de saida descartados     = 0
  Pacote de saida sem rota         = 0
  Reagrupamento necess rio         = 82
  Reagrupamento bem-sucedido       = 41
  Falhas de reagrupamento          = 0
  Datagramas fragmentados c/êxito  = 15
  Falhas/ fragmentação de datagramas = 0
  Fragmentos criados               = 30

Estatisticas de ICMP

                                Recebidos      Enviados
  Mensagens                         2767          4037
  Erros                             0             0
  Destino inatingivel               18            1280
  Tempo excedido                    0             0
  Problemas de parâmetro            0             0
  Retardamentos de origem           4             0
  Redirecionamentos                 0             0
  Echos                             1134          1623
  Respostas de eco                  1611          1134
  Carimbos de data/hora             0             0
  Respostas de carimbos de data/hora 0            0
  M scaras de endere‡o              0             0
  Respostas m scaras end.           0             0

Estatisticas de TCP

  Abertos ativos                = 14052
  Abertos passivos              = 175
  Falha em tentativas de conexão  = 493
  Conexões redefinidas          = 3563
  Conexões atuais               = 5
  Segmentos recebidos           = 1679289
  Segmentos enviados            = 2576364
  Segmentos retransmitidos      = 2841

Estatisticas de UDP

  Datagramas recebidos    = 159044
  Nenhuma porta           = 7777
  Erros de recebimento    = 0
  Datagramas enviados     = 119031
```

- **netstat –p**: Mostra conexões para o protocolo especificado por protocolo, que pode ser tcp ou udp. Se utilizado com a opção -s para exibir estatísticas por protocolo, protocolo pode ser tcp, udp, icmp ou ip. . A seguir um exemplo da execução do comando netstat –p, onde são exibidas informações somente sobre o protocolo ip: netstat –s –p ip:



- **netstat –r**: Exibe o conteúdo da tabela de roteamento do computador. Exibe os mesmos resultados do comando route print.
- **A opção intervalo**: Você pode definir um intervalo, dentro do qual as estatísticas geradas pelo comando netstat serão atualizadas. Por exemplo, você pode definir que sejam exibidas as estatísticas do protocolo ICMP e que estas sejam atualizadas de cinco em cinco segundos. Ao especificar um intervalo, o comando ficará executando, indefinidamente e atualizando as estatísticas, dentro do intervalo definido. Para suspender a execução do comando, basta pressionar Ctrl+C. O comando a seguir irá exibir as estatísticas do protocolo IP e irá atualizá-las a cada 10 segundos:

netstat –s –p ip 10

Permissões de Compartilhamento e NTFS

Segurança, sem dúvidas, é um dos temas mais debatidos hoje, no mundo da informática. Algumas opções do Windows 2000 (e também do Windows XP Professional) ajudam a manter os seus arquivos mais protegidos, longe do alcance de intrusos.

Trataremos sobre as permissões de compartilhamento e também permissões NTFS. Veremos como a correta configuração dessas permissões pode tornar o acesso aos seus arquivos bem mais seguro e protegido, com o acesso permitido apenas para os usuários habilitados através das permissões. É importante salientar que com o Windows 95/98 ou Me não existe como configurar permissões de acesso, ou seja, não temos como proteger os arquivos do computador. Qualquer pessoa que tenha acesso ao computador poderá ligá-lo e acessar, alterar ou excluir qualquer arquivo que esteja no disco rígido. Com as permissões NTFS do Windows 2000 (e também do Windows XP Professional) podemos resolver esse problema.

Veremos como compartilhar uma Pasta, disponibilizando o seu conteúdo, para que seja acessado através da rede. Também aprenderemos a atribuir permissões de segurança – permissões NTFS, para que somente usuários autorizados possam acessar as pastas compartilhadas. Veremos alguns detalhes importantes sobre Sistemas de Arquivos suportados pelo Windows 2000 Server.

Compartilhando Pastas e Definição de Permissões - Teoria.

Primeiro vamos ver alguns detalhes sobre compartilhamento de pastas e permissões de compartilhamento.

Quando compartilhamos uma pasta, estamos permitindo que o seu conteúdo seja acessado através da rede. Quando uma pasta é compartilhada, os usuários podem acessá-la através da rede, bem como o todo o conteúdo da pasta que foi compartilhada. Por exemplo, poderíamos criar uma pasta compartilhada onde seriam colocados documentos, orientações e manuais, de tal forma que estes possam ser acessados por qualquer estação conectada a

rede.

Ao compartilharmos uma pasta todo o conteúdo dessa pasta passa a estar disponível para ser acessada através da rede. Todas as subpastas da pasta compartilhada também estarão disponíveis para acesso através da rede. Considere o exemplo da Figura 1. Se a pasta C:\Documentos for compartilhada, todo o seu conteúdo e também o conteúdo das subpastas C:\Documentos\Ofícios e C:\Documentos\Memorandos estarão disponíveis para acesso através da rede.

Porém quando uma pasta é compartilhada, não significa que o seu conteúdo deva ser acessado por todos os usuários da rede. Podemos restringir o acesso, de tal maneira que somente usuários autorizados tenham acesso à pasta compartilhada, isso é feito através de **"Permissões de compartilhamento"**.

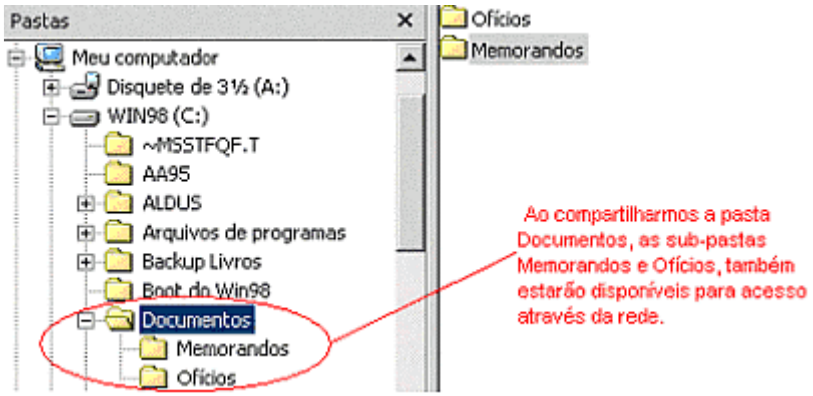


Figura 1 Ao compartilhar uma pasta, todo o seu conteúdo estará disponível.

Com o uso de permissões, podemos definir quais os usuários poderão acessar o conteúdo da pasta compartilhada. Para isso, é criada uma lista com o nome dos usuários e grupos que terão permissão de acesso. Além disso é possível limitar o que os usuários com permissão de acesso podem fazer. Pode haver situações em que alguns usuários devam ter permissão apenas para ler o conteúdo da pasta compartilhada, podem haver outras situações em que alguns usuários devem ter permissão de leitura e escrita, enquanto outros devem ter permissões totais, tais como leitura, escrita e até exclusão de arquivos.

Na Figura 2, temos um exemplo, em que o grupo Gerentes possui permissões de "Controle total", enquanto o grupo "Usuários" possui permissões apenas para leitura.

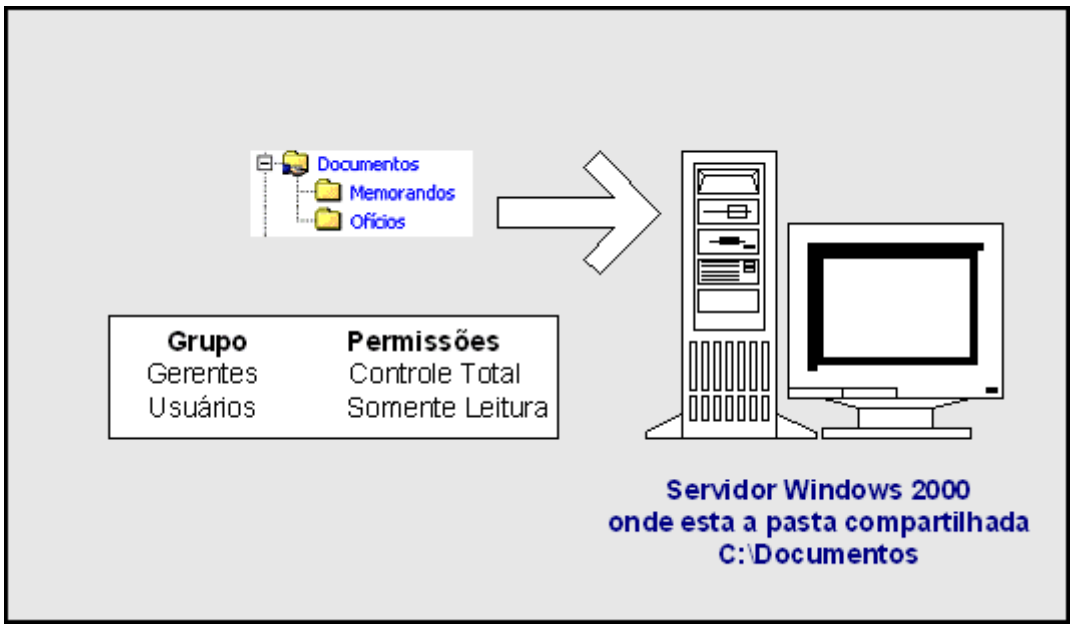


Figura 2 Grupos diferentes com permissões diferentes.

Conforme pode ser visto na Figura 2, o Windows 2000 Server indica que uma pasta está compartilhada através da figura de uma "mãozinha" , segurando a pasta.

IMPORTANTE: As permissões definem o que o usuário pode fazer com o conteúdo de uma pasta compartilhada, desde somente leitura, até um controle total sobre o conteúdo da pasta compartilhada.

Aprenderemos a compartilhar uma pasta e atribuir permissões de acesso.

JAMAIS ESQUEÇA O SEGUINTE DETALHE: Permissões de compartilhamento, não impedem o acesso ao conteúdo da pasta localmente, isto é, se um usuário fizer o logon no computador onde está a pasta compartilhada, este usuário terá acesso a todo o conteúdo da pasta, a menos que as "Permissões NTFS" estejam configurados de acordo. Permissões NTFS é assunto para daqui a pouco. Vamos falar de um jeito diferente: Permissões de compartilhamento somente tem efeito quando o usuário está acessando a pasta através da rede, para acesso local, no próprio computador onde está a pasta, as permissões de compartilhamento não tem nenhum efeito, é como se não existissem.

Ao criarmos um compartilhamento em uma pasta, por padrão o Windows 2000 Server atribui a permissão **"Controle total"** para o grupo **"Todos"**, que conforme o nome sugere, significa qualquer usuário com acesso ao computador, seja localmente, seja pela rede. Por isso ao criar um compartilhamento, já devemos configurar as permissões necessárias, a menos que estejamos compartilhando uma pasta de domínio público, onde todos os usuários possam ter Controle total sobre os arquivos e subpastas da pasta compartilhada..

Existem três níveis de permissões de compartilhamento, conforme descrito a seguir:

☐ **Leitura:** Permite ao usuário exibir a listagem de pastas e arquivos, ler o conteúdo de arquivos e executar programas. O usuário também pode verificar os atributos dos arquivos e navegar através das pastas e subpastas. O usuário não pode alterar nem eliminar arquivos ou pastas. Também não é permitido criar novos arquivos ou pastas.

OBS.: Pastas e arquivos possuem atributos, que o Windows 2000 Server utiliza para gerenciamento. Por exemplo, existe um atributo "Leitura", que uma vez marcado torna o arquivo somente leitura, isto é, não podem ser feitas alterações no arquivo. Para ver os atributos de um arquivo ou pasta, basta dar um clique com o botão direito do mouse sobre o arquivo ou pasta, e no menu que surge dê um clique na opção "Propriedades", e o Windows 2000 Server exibe uma janela onde é possível verificar e modificar os atributos do arquivo ou pasta, desde que o usuário tenha as devidas permissões.

☐ **Alteração:** Permite ao usuário criar pastas, criar novos arquivos, alterar arquivos, alterar os atributos dos arquivos, eliminar arquivos e pastas, mais todas as ações para a permissão de Leitura. Não permite que sejam alteradas permissões dos arquivos nem alterações no usuário "dono" dos arquivos e pastas.

OBS.: No Windows 2000 Server, objetos como pastas e arquivos possuem um "dono", o qual normalmente é o usuário que cria a pasta ou arquivo. Falaremos mais sobre o dono do arquivo mais adiante.

Controle total: Permite ao usuário alterar as permissões dos arquivos e tornar-se dono de pastas e arquivos criados por outros usuários, além de todas as ações para a permissão Alteração.
As permissões de compartilhamento Leitura, Alteração e Controle total, podem ser **Permitidas** ou **Negadas**. Vamos considerar um exemplo prático. Vamos supor que todos os usuários do grupo Gerentes deve ter acesso de Leitura a uma pasta compartilhada, com exceção de um gerente cuja conta de usuário é jsilva. Para simplificar a atribuição de permissões fazemos o seguinte:
☐ Permissão de Leitura para o grupo Gerentes – Permitir

☐ Permissão de Leitura para o usuário jsilva – Negar
Com isso todos os usuários do grupo Gerentes terão permissão de leitura, com exceção do usuário "jsilva", o qual teve a permissão de leitura negada.

Outra recomendação é que sempre devemos atribuir permissões para grupos de usuários, ao invés de atribuir para usuários individuais, pois isso facilita a administração. É a famosa estratégia AGLP – Account -> Global -> Local -> Permission. Em um dos próximos tutoriais irei detalhar a estratégia AGLP.

O que acontece quando um usuário pertence a mais de um grupo??

Quando um usuário pertence, por exemplo, a dois grupos e os dois grupos recebem permissão para acessar um compartilhamento, sendo que os dois grupos possuem permissões diferentes, por exemplo, um tem permissão de Leitura e o outro de Alteração, como é que ficam as permissões do usuário que pertence aos dois grupos?

Para responder a esta questão, considere o seguinte: "Quando um usuário pertence a mais de um grupo, cada qual com diferentes níveis de permissões para uma pasta compartilhada, o nível de permissão para o usuário que pertence a mais de um grupo, é a combinação das permissões atribuídas aos diferentes grupos".

No nosso exemplo, o usuário pertence a dois grupos, um com permissão de somente leitura e outro com permissão de alterações. A nível de permissão do usuário é de alterações, pois é a soma das permissões dos dois grupos, conforme indicado na Figura 3.

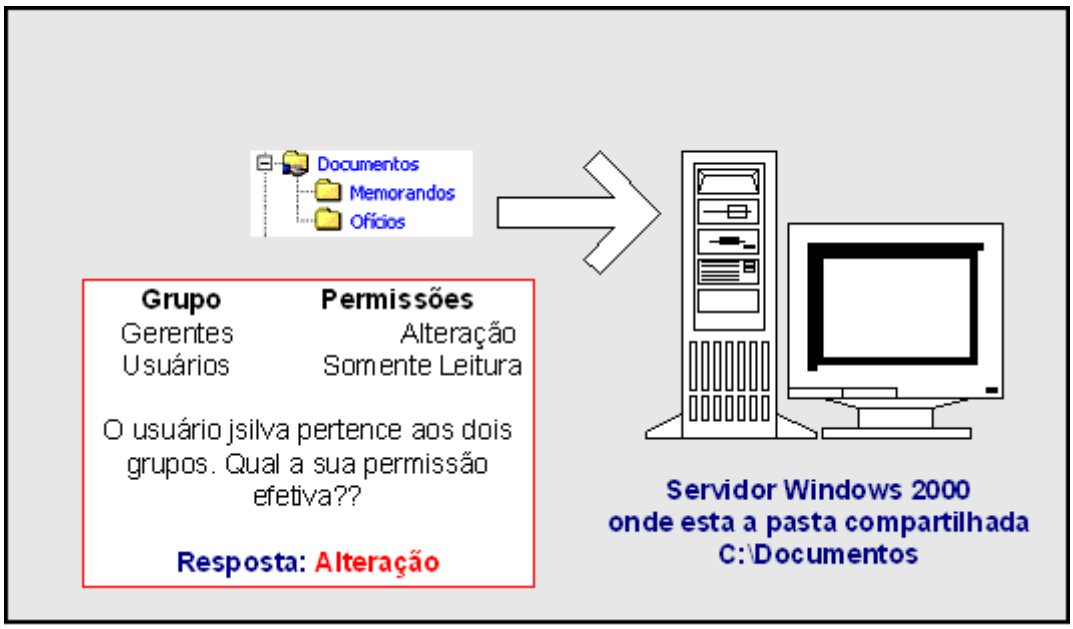


Figura 3 Usuário que pertence a mais de um grupo.

Negar têm precedência sobre quaisquer outras permissões: Vamos considerar o exemplo do usuário que pertence a três grupos. Se em um dos grupos ele tiver permissão de leitura e em outro grupo permissão de alteração. Mas se para o terceiro grupo, for "negado" o acesso à pasta compartilhada, o usuário terá o acesso negado, uma vez que "Negar" tem precedência sobre quaisquer outras permissões, conforme indicado pela Figura 4.

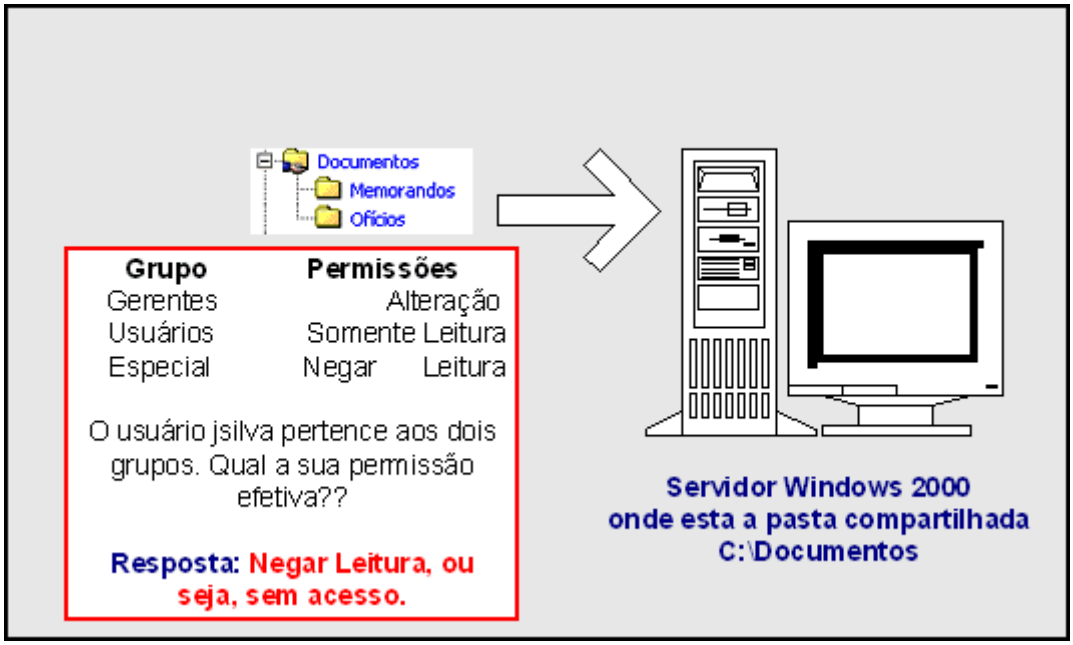


Figura 4 Negar tem precedência sobre permitir.

IMPORTANTE: Quando copiamos uma pasta compartilhada, a pasta original permanece compartilhada, porém a cópia não é compartilhada. Quando movemos uma pasta compartilhada, esta deixa de ser compartilhada.

Algumas orientações para a criação de pastas compartilhadas:

☐ Todo compartilhamento, obrigatoriamente, deve ter um nome, para que ele possa ser acessado pela rede, conforme veremos mais adiante. O nome do compartilhamento pode ser diferente do nome da pasta. Uma recomendação importante é para que seja escolhido um nome descritivo do conteúdo da pasta, de tal maneira que esta seja mais facilmente localizada na rede. Você não colocaria um nome "Projetos" em uma pasta com documentos contábeis? Após compartilhada, a pasta passa a ter um caminho na rede. O caminho segue o padrão UNC –Universal Name Convection. No padrão UNC, um caminho e formado por duas barras invertidas, depois o nome do computador, mais uma barra invertida e, por último, o nome do compartilhamento. Por exemplo, o caminho UNC da pasta Documentos, compartilhada no servidor SRV01 é o seguinte: \\SRV01\Documentos; o caminho da pasta Projetos (nome de compartilhamento), compartilhada no servidor SRV02 é o seguinte: \\SRV02\Projetos e assim por diante.

☐ Organize os recursos, de tal maneira que todos os pastas que devam ser acessadas pelo mesmo grupo de usuários, com o mesmo nível de permissão, estejam dentro da mesma pasta compartilhada. Por exemplo, se você possui sete pastas com documentos e programas, os quais devem ser acessados pelos grupos Contabilidade e Marketing. Coloque estas pastas dentro de uma pasta principal e compartilhe a pasta principal, ao invés de criar sete compartilhamentos individuais.

☐ Configure o nível de permissão mínimo necessário para que os usuários realizem o seu trabalho. Por exemplo se os usuários precisam apenas ler os documentos em uma pasta compartilhada, atribua permissão de Leitura e não de Alteração ou Controle total.

☐ Sempre que possível, atribua permissões para grupos de usuários e não para usuários individuais, pois isso facilita a administração das permissões.

☐ Determine quais grupos necessitam acesso a quais pastas compartilhadas e com quais níveis de permissão. Documente bem todo esse processo, para que você possa ter um bom controle sobre os recursos compartilhados e as permissões atribuídas.

Sistemas de Arquivos e Permissões NTFS - Teoria

Agora vamos ver alguns detalhes sobre os sistemas de arquivos que o Windows 2000 Server reconhece e também sobre permissões NTFS.

Um sistema de arquivos determina a maneira como o Windows 2000 Server organiza e recupera as informações no Disco rígido ou em outros tipos de mídia. O Windows 2000 Server reconhece os seguintes sistemas de arquivos:

- ☐ FAT
- ☐ FAT32
- ☐ NTFS
- ☐ NTFS 5

O sistema FAT vem desde a época do bom e velho MS-DOS e tem sido mantido por questões de compatibilidade. Além disso se você tiver instalado mais de um Sistema Operacional no seu computador, alguns sistemas mais antigos (DOS, Windows 3.x e as primeiras versões do Windows 95) somente reconhecem o sistema FAT. Com o sistema de arquivos FAT, a única maneira de restringir o acesso ao conteúdo de uma pasta compartilhada, é através das permissões de compartilhamento, as quais, conforme descrito anteriormente, não terão nenhum efeito se o usuário estiver logado localmente, na máquina onde a pasta foi criada. Com a utilização do sistema FAT, alguns recursos avançados, tais como compressão, criptografia, auditoria e definição de cotas não estarão disponíveis.

O sistema FAT32 apresenta algumas melhorias em relação ao sistema FAT. Existe um melhor aproveitamento do espaço no disco, com conseqüente menor desperdício. Um grande inconveniente do sistema FAT32 é que ele não é reconhecido pelo Windows NT 4.0 – Server ou Workstation. Com o sistema de arquivos FAT32, a única maneira de restringir o acesso ao conteúdo de uma pasta compartilhada, é através das permissões de compartilhamento, as quais, conforme descrito anteriormente, não terão nenhum efeito se o usuário estiver logado localmente, na máquina onde a pasta foi criada. Com a utilização do sistema FAT32, alguns recursos avançados, tais como compressão, criptografia, auditoria e definição de cotas não estarão disponíveis.

O sistema de arquivos NTFS é utilizado no Windows NT Server 4.0 e foi mantido no Windows 2000 Server por questões de compatibilidade. É um sistema bem mais eficiente do que FAT e FAT32, além de permitir uma série de recursos avançados, tais como:

- ☐ Permissões de acesso para arquivos e pastas
- ☐ Compressão
- ☐ Auditoria de acesso
- ☐ Partições bem maiores do que as permitidas com FAT e FAT32
- ☐ Desempenho bem superior do que com FAT e FAT32

Uma das principais vantagens do NTFS é que ele permite que sejam definidas permissões de acesso para arquivos e pastas, isto é, posse ter arquivos em uma mesma pasta, com permissões diferentes para usuários diferentes. Além disso, as permissões NTFS têm efeito localmente, isto é, mesmo que o usuário faça o logon no computador onde um determinado arquivo existe, se o usuário não tiver as permissões NTFS necessárias, ele não poderá acessar o arquivo. Isso confere um alto grau de segurança, desde que as permissões NTFS sejam configuradas corretamente.

No Windows 2000 Server, temos também o NTFS 5, o qual apresenta diversas melhorias em relação ao NTFS, tais como:

- ☐ **Criptografia de arquivos e pastas:** (a criptografia é uma maneira de "embaralhar" a informação de tal forma que mesmo que um arquivo seja copiado, ele se torna ilegível, a não ser para a pessoa que possui a "chave" para descriptografar o arquivo).

- ☐ **Cotas de usuário:** Com o uso de cotas é possível limitar o espaço em disco que cada usuário pode utilizar.

- ☐ Gerenciamento e otimização melhorados.

Nota: Um inconveniente do NTFS 5 , é que ele não é reconhecido pelas versões anteriores, tais como o Windows NT Server 4.0.
Conforme descrito anteriormente, podemos definir permissões de acesso a nível da pasta ou arquivo, mas somente em unidades formatadas com o sistema de arquivos NTFS (seja na versão do NT Server 4.0 ou o NTFS 5 do Windows 2000 Server). Por isso que é aconselhável instalar o Windows 2000 Server sempre em unidades formatadas com NTFS, pois isso melhora a segurança.

Com relação as permissões NTFS, temos um conjunto diferente de permissões quando

tratamos de pastas ou arquivos. Nas Tabelas 1(para pastas) e 2 (para arquivos) , são apresentadas as permissões e o nível de acesso para cada uma delas.

Tabela 1 Permissões NTFS para pastas

Permissão	Nível de Acesso
Leitura	Permite ao usuário listar as pastas e arquivos dentro da pasta, permite que sejam exibidas as permissões, donos e atributos.
Gravar	Permite ao usuário criar novos arquivos e subpastas dentro da pasta, alterar os atributos da pasta e visualizar o dono e as permissões da pasta.
Listar	Conteúdo de pastas Permite ao usuário ver o nome dos arquivos e subpastas
Ler e executar	Permite ao usuário navegar através das subpastas para chegar a outras pastas e arquivos, mesmo que o usuário não tenha permissão de acesso às pastas pelas quais está navegando, além disso possui os mesmos direitos que as permissões Leitura e Listar Conteúdo de pastas.
Modificar	Permite ao usuário eliminar a pasta, mais todas as ações permitidas pela permissão Gravar e pela permissão Ler e executar.
Controle total	Permite que sejam alteradas as permissões, permite ao usuário tornar-se dono da pasta, eliminar subpastas e arquivos, mais todas as ações permitidas por todas as outras permissões NTFS.

Tabela 2 Permissões NTFS para arquivos.

Permissão	Nível de Acesso
Leitura	Permite ao usuário ler o arquivo, permite que sejam exibidas as permissões, dono e atributos.
Gravar	Permite ao usuário gravar um arquivo com o mesmo nome sobre o arquivo, alterar os atributos da pasta e visualizar o dono e as permissões da pasta.
Ler e executar	Permite ao usuário executar aplicativos (normalmente programas .exe, .bat ou .com), mais todas os direitos da permissão Leitura.
Modificar	Permite ao usuário modificar e eliminar o arquivo, mais todas as ações permitidas pela permissão Gravar e pela permissão Ler e executar.
Controle total	Permite que sejam alteradas as permissões, permite ao usuário tornar-se dono do arquivo, mais todas as ações permitidas por todas as outras permissões NTFS.

Todo arquivo ou pasta em uma unidade formatada com NTFS, possui uma "Lista de controle de acesso (Access control list) – ACL. Nessa ACL ficam uma lista de todas as contas de usuários e grupos para os quais foi garantido acesso para pasta/arquivo, bem como o nível de acesso de cada um deles.

Existem alguns detalhes que devemos observar sobre permissões NTFS:

☐ Permissões NTFS são cumulativas, isto é , se um usuário pertence a mais de um grupo, o qual tem diferentes níveis de permissão para um recurso, a permissão efetiva do usuário é a soma das permissões.

☐ Permissões NTFS para um arquivo têm prioridade sobre permissões NTFS para pastas: Por exemplo se um usuário têm permissão NTFS de escrita em uma pasta, mas somente permissão NTFS de leitura para um arquivo dentro desta pasta, a sua permissão efetiva será somente a de leitura, pois a permissão para o arquivo tem prioridade sobre a permissão para a pasta.

☐ Negar uma permissão NTFS tem prioridade sobre permitir: Por exemplo, se um usuário pertence a dois grupos diferentes. Para um dos grupos foi dado permissão de leitura para um arquivo e para o outro grupo foi Negada a permissão de leitura, o usuário não terá o direito de leitura, pois Negar tem prioridade sobre Permitir.

Agora que já vimos a teoria necessária, vamos praticar um pouco. Nos próximos tópicos iremos aprender a compartilhar pastas, atribuir permissões de compartilhamento. Iremos aprender a acessar pastas compartilhadas através da rede. Depois vamos trabalhar um pouco com as permissões NTFS. Veremos como atribuir permissões NTFS e testar uma série de situações práticas.

Criando e Compartilhando uma Pasta - Prática

Neste tópico vamos criar e compartilhar uma pasta chamada Memorandos. Depois utilizaremos o comando Iniciar -> Executar para verificar se a pasta compartilhada já aparece disponível na listagem de recursos da rede.

Alguns pontos que devem ser observados:

☐ Crie a pasta documentos em uma unidade formatada com NTFS, pois caso contrário você somente poderá atribuir permissões de compartilhamento, mas não poderá atribuir permissões NTFS – lembre-se permissões NTFS somente são possíveis em unidades formatadas com o sistema de arquivos NTFS. Para verificar o sistema de arquivos de uma unidade é extremamente simples. Basta abrir o "Meu computador", dar um clique com o botão direito sobre a unidade e no menu que surge escolha "Propriedades". Surge uma janela com uma série de informações sobre a unidade, dentre as quais está o sistema de arquivos. Na Figura 5.5, podemos ver um exemplo das propriedades de uma unidade (G:\), onde o sistema de arquivos é NTFS.

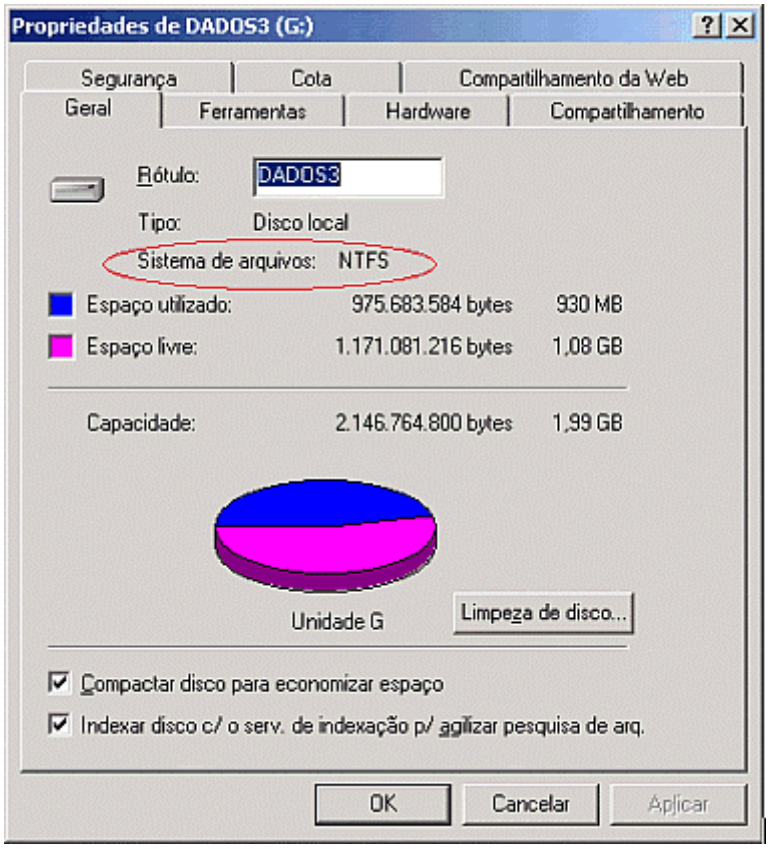


Figura 5 Unidade G: formatada com NTFS.

Então chega de conversa e vamos praticar um pouco.

Exemplo: Para criar uma pasta chamada Memorandos, siga os seguintes passos:
1. Abra o Windows Explorer: Iniciar -> Programas -> Acessórios -> Windows Explorer.

2. No painel da esquerda localize uma unidade formatada com NTFS e dê um clique sobre ela para selecioná-la, conforme indicado na Figura 6.

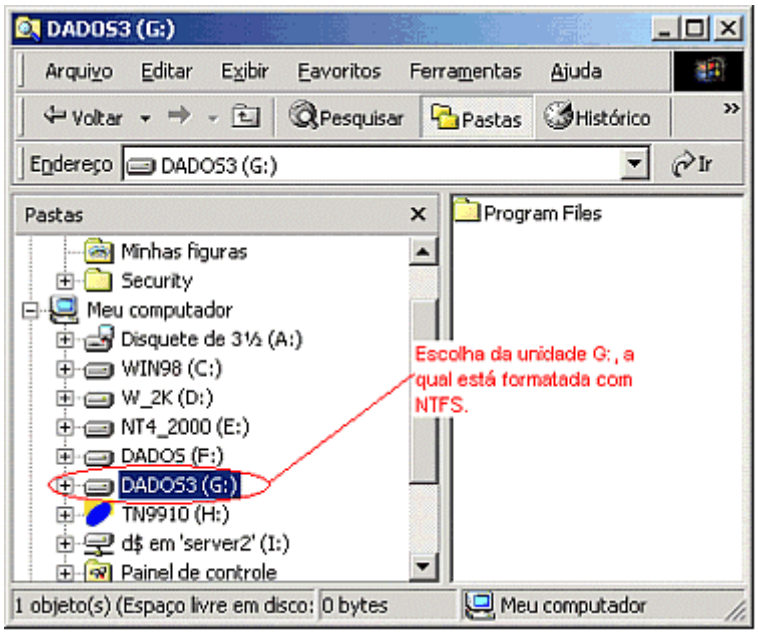


Figura 6 Selecionando uma unidade formatada com NTFS.

OBS.: Provavelmente no computador que você esteja usando exista uma quantidade diferente de unidades. Pode até ser que exista somente o Disco rígido (C:\) e o CD-ROM

(D:\). O importante é que exista uma unidade de Disco rígido formatada com NTFS.

3. No painel da direita, dê um clique com o botão direito do mouse em qualquer espaço livre (área em branco).

4. No menu que surge, selecione o comando Novo -> Pasta.

5. No painel da direita o Windows 2000 Server exibe uma caixa com o nome Nova pasta já selecionado.

6. Não clique em lugar nenhum nem tecle Enter, simplesmente digite o nome da pasta que está sendo criada, no nosso exemplo digite Memorandos e tecle Enter.

7. A pasta Memorandos será criada.
Para compartilhar a pasta Memorandos, siga os seguintes passos:
1. Ainda com o Windows Explorer aberto, dê um clique com o botão direito do mouse na pasta Memorandos.

2. No menu que surge dê um clique na opção Compartilhamento.

3. Irá surgir a janela indicada na Figura 7, a qual indica que a pasta Memorandos não está compartilhada. Isso acontece por que ao criar uma pasta, essa não é automaticamente compartilhada pelo Windows 2000 Server.

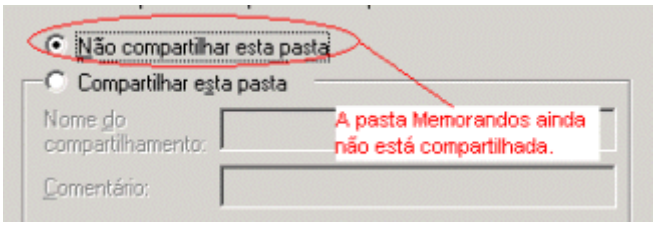


Figura 7 Pasta Memorandos não compartilhada.

4. Para compartilhar a pasta, dê um clique na opção "Compartilhar esta pasta".

5. Agora você precisa especificar um nome do compartilhamento, o qual pode ser diferente do nome da pasta, e um comentário, o qual é utilizado para facilmente identificar o conteúdo da pasta.

6. Digite o nome do compartilhamento e um comentário, conforme indicado pela Figura 8.

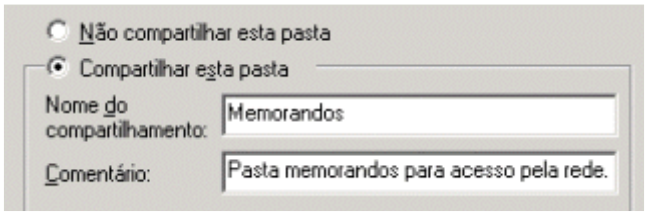


Figura 8 Especificando um Nome do compartilhamento e um comentário.

IMPORTANTE: Se na rede existem somente clientes que utilizam Windows 95/98 ou Windows 2000/XP, você pode utilizar um nome de compartilhamento de até 12 caracteres. Caso você tenha clientes mais antigos, tais como DOS, Windows 3.1 e Windows for Workgroups, limite os nomes de compartilhamento a 8 caracteres.

7. Nesta tela você também pode definir o número máximo de acessos simultâneos permitidos à esse compartilhamento. Por padrão é permitido o número Máximo de usuários, conforme o número de licenças ou capacidade do servidor.

8. Para limitar o número de usuários que podem acessar o compartilhamento ao mesmo tempo, dê um clique na opção Permitir e especifique o número de usuários simultâneos permitidos.

9. Dê um clique no botão OK para criar o compartilhamento.

10. Observe que surgiu uma maozinha "segurando", a pasta Memorandos. Isto é um indicativo de que a pasta está compartilhada.

11. Feche o Windows Explorer.
Para verificar se o compartilhamento foi realmente criado, siga os seguintes passos:
OBS: Caso você tenha acesso a outro comutador da rede, faça o logon como Administrador e acompanhe este exercício no outro computador. "servidor" é o nome do computador onde foi criada a pasta compartilhada Memorandos. Caso você tenha criado em um computador com outro nome, substitua servidor pelo nome do computador que você está utilizando.

1. Selecione o comando Iniciar -> Executar.

2. No campo Abrir, digite: \\nome do computador. No nosso exemplo, o nome do computador onde foi criada e compartilhada a pasta Memorandos é: servidor, conforme indicado na Figura 9:

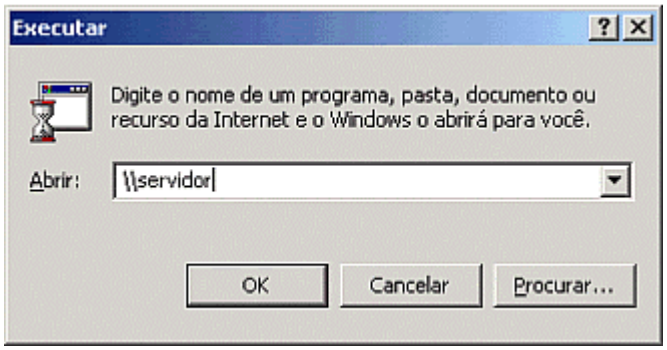


Figura 9 Acessando os recursos do computador cujo nome é: servidor

3. Clique em OK e pronto, o Windows 2000 abre uma janela com todos os recursos compartilhados no computador cujo nome é servidor, dentre os quais está a pasta compartilhada Memorandos, conforme indicado na Figura 10:

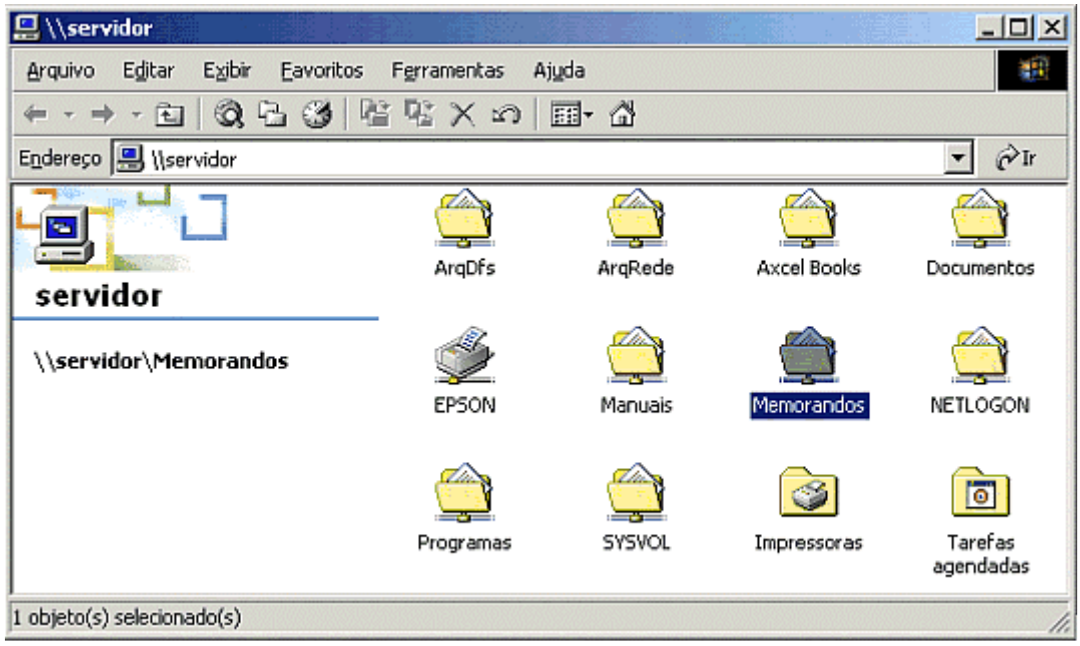


Figura 10 A pasta compartilhada Memorandos em servidor.

IMPORTANTE: Todo recurso compartilhado em uma rede Microsoft Windows, pode ser acessada através do seu nome UNC – Universal Name Convention. O nome UNC inicia com duas barras invertidas, depois o nome do computador onde está o recurso, mais uma barra

invertida e finalmente o nome do compartilhamento. No nosso exemplo temos \\servidor\Memorandos, o que indica o recurso Memorandos no computador servidor. Exercício: Crie uma pasta chamada Projetos, em uma unidade formatada com NTFS, compartilhe esta pasta com o nome de compartilhamento "Secreto" e permita um número máximo de apenas 5 usuários acessando a pasta simultaneamente. Utilize o comando Iniciar -> Executar para verificar se a pasta foi compartilhada com sucesso.

Configurando as Permissões de Compartilhamento - Prática

Conforme descrito no início, quando um compartilhamento é criado, é atribuída a permissão Controle total para o grupo Todos, ou seja, qualquer usuário pode fazer qualquer operação sobre a pasta compartilhada e o seu conteúdo, inclusive eliminar todo o seu conteúdo.

Neste tópico iremos atribuir permissões de compartilhamento e testar o efeito dessas permissões, tanto localmente quanto através da rede. Para que você possa acompanhar todos os exemplos propostos nesta lição, é necessário que você tenha acesso a mais um computador em rede, além do computador onde foi criada a pasta compartilhada Memorandos na lição anterior.

Nos exemplos, utilizarei o computador servidor como sendo o computador onde se encontra a pasta compartilhada Memorandos e micro01 o outro computador em rede. Caso os nomes dos computadores que você está utilizando para acompanhar esta lição, sejam diferentes, utilize-os no lugar dos nomes aqui descritos.

Exemplo: Para atribuir permissões de compartilhamento, siga os seguintes passos:
1. Efetue o logon como Administrador, no computador Server1.

2. Abra o Windows Explorer.

3. No painel da esquerda, se Meu computador não estiver aberto, dê um clique no sinal de + ao lado de Meu computador para abri-lo.

4. Abaixo de Meu computador, surge uma listagem com todas as unidades disponíveis no computador. Inclusive unidade de diskete (A:\) e a unidade de CD-ROM.

5. Localize a unidade onde você criou a pasta Memorandos, no tópico anterior, abra a unidade e localize a pasta Memorandos.

6. Dê um clique com o botão direito do mouse sobre a pasta Memorandos, e no menu de opções que surge dê um clique em Compartilhamento...

7. Na janela que surge, dê um clique no botão "Permissões", localizado na parte mais de baixo da janela, conforme indicado pela Figura 11.

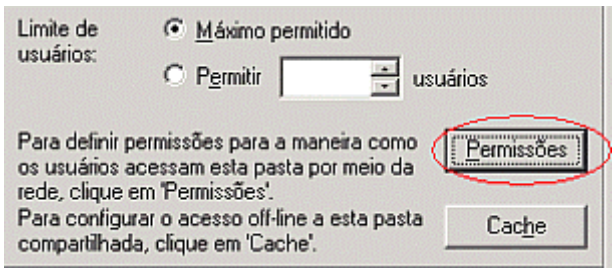


Figura 11 Botão Permissões, para configurar as permissões de compartilhamento.

8. Surge a janela "Permissões para Memorandos", na qual podemos constatar que o grupo Todos possui permissões de "Controle total" sobre a pasta Memorandos.

9. Dê um clique sobre o grupo Todos para marcá-lo, depois clique no botão "Remover", para retirar as permissões para o grupo Todos. Sua janela deve ficar conforme indicado na Figura 12.

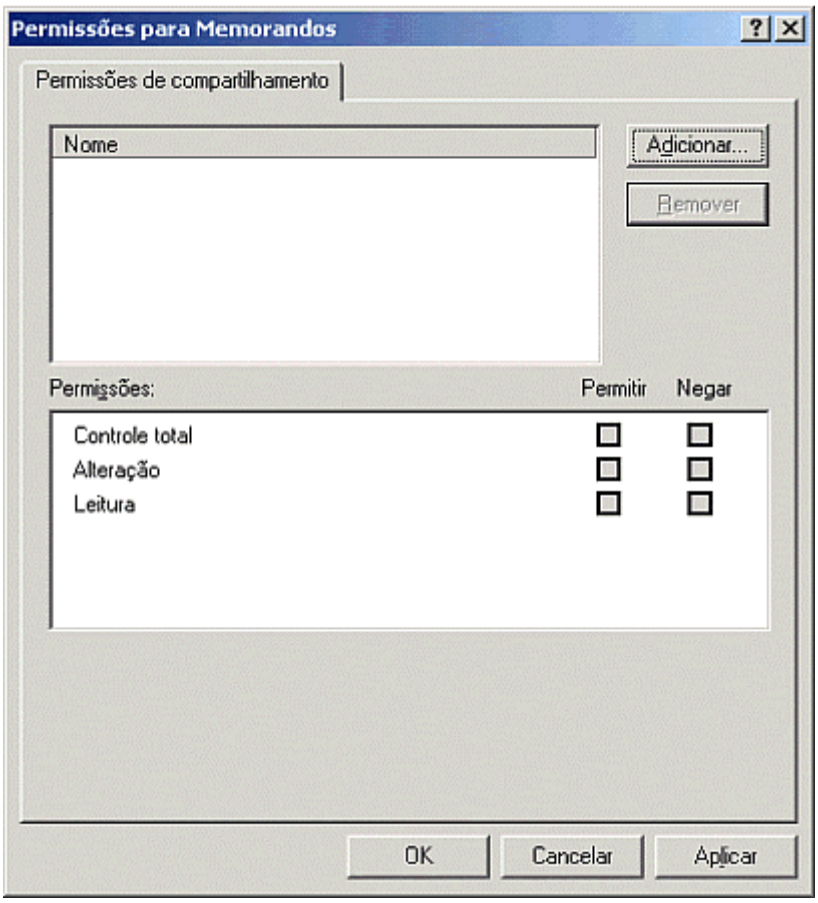


Figura 12 Removendo as permissões para o grupo Todos.

10. Agora vamos dar permissões de acesso, apenas para os usuários jsilva2 e maria (utilize os nomes de usuários que você criou na sua rede). Não daremos permissão para o usuário paulo.

11. Clique no botão Adicionar. Surge uma janela com uma listagem dos usuários, grupos e computadores disponíveis.

12. Localize o usuário José da Silva (jsilva2) na listagem, dê um clique para marcá-lo e depois um clique no botão Adicionar. Repita a operação para o usuário Maria do Socorro (maria).

13. Sua janela deve ficar conforme a indicada na Figura 13, onde foram adicionados os usuários José da Silva e Maria do Socorro.

14. Dê um clique no botão OK e você estará de volta a janela "Permissões para Memorando".

15. Além de adicionar os dois usuários, devemos configurar o nível de acesso para cada um dos usuários.

16. Vamos permitir um acesso com nível apenas de leitura.

17. Dê um clique em José da Silva para marcá-lo. Na parte do meio da janela, onde tem Permissões, deixe marcada somente a caixa Leitura, da coluna Permitir.

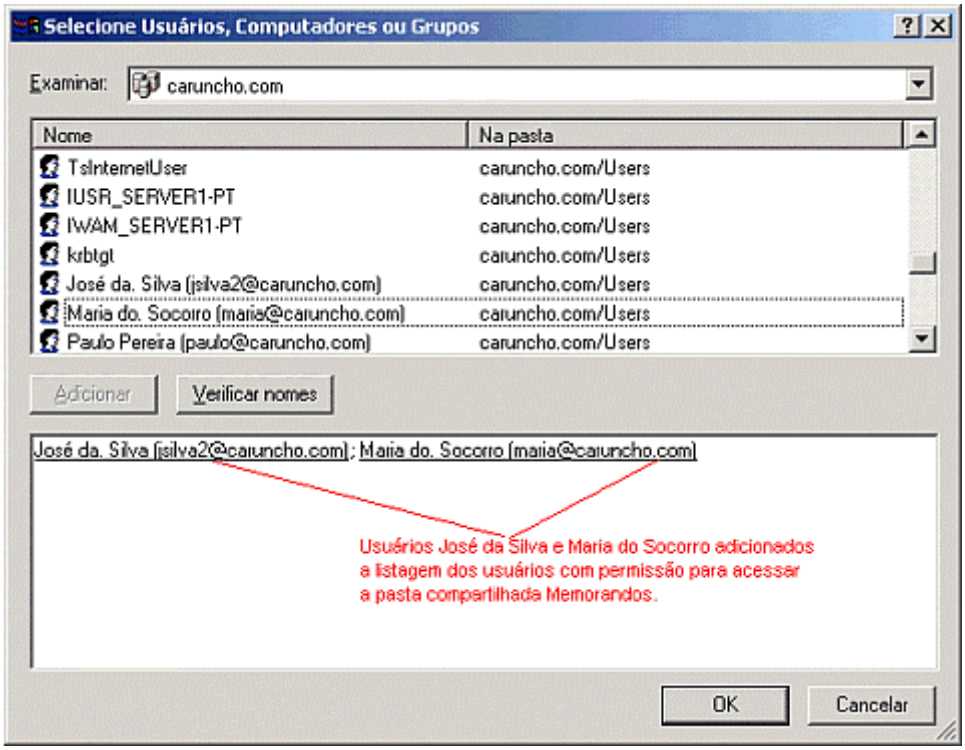


Figura 13 Adicionando os usuários José da Silva e Maria do Socorro.

18. Repita a operação para o usuário Maria do Socorro, conforme indicado pela Figura 14.

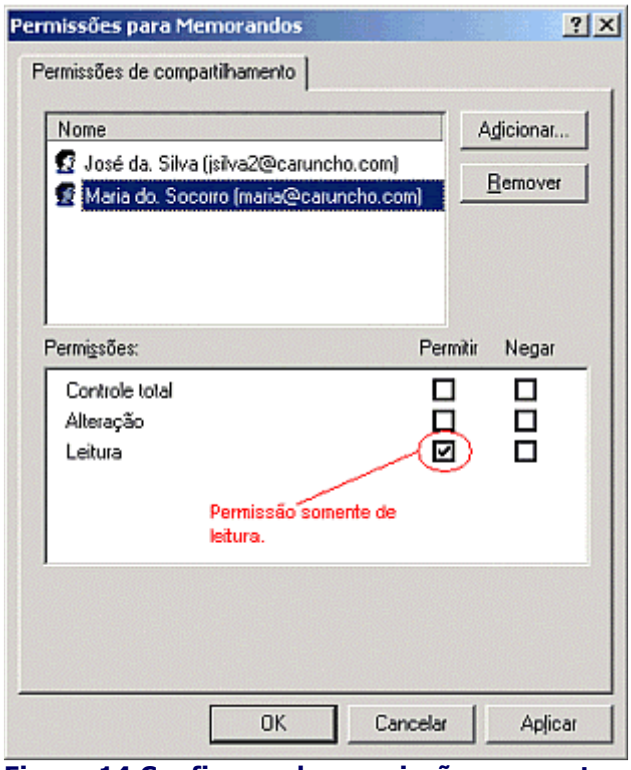


Figura 14 Configurando permissões somente para leitura.

19. Dê um clique no botão OK para fechar a janela "Permissões para Memorandos".

20. Dê um clique no botão OK, para fechar a janela "Propriedades de Memorandos".

IMPORTANTE: Acabamos de atribuir permissão de leitura apenas para os usuários José da

Silva (jsilva2) e Maria do Socorro (maria). O usuário Paulo Pereira (paulo), não recebeu permissão. Vamos testar o efeito destas permissões.

Para testar o funcionamento das permissões de compartilhamento através da rede, siga os seguintes passos:

1. Faça o logon no computador micro01 com a conta de usuário maria e para a senha digite senha123 (ou utilize uma conta de usuário da sua rede, para a qual você configurou as permissões no exemplo anterior).

2. Utilize o comando Iniciar -> Executar, para acessar a pasta compartilhada Memorandos, conforme descrito anteriormente. Dê um clique duplo para tentar acessar a pasta compartilhada Memorandos. Você conseguiu ?

3. É claro que sim, uma vez que o usuário Maria do Socorro (maria) tem permissão para acessar esse compartilhamento.

4. Faça o logoff do usuário maria.

5. Faça o logon no computador micro01 com a conta de usuário paulo e para a senha digite paulo123. (ou utilize uma conta de usuário da sua rede, para a qual você não configurou as permissões no exemplo anterior)

6. Utilize o comando Iniciar -> Executar, para acessar a pasta compartilhada Memorandos, conforme descrito anteriormente. Dê um clique duplo para tentar acessar a pasta compartilhada Memorandos. Você conseguiu ?

7. É claro que não, pois o usuário Paulo Pereira (paulo) não tem permissão para acessar esse compartilhamento através da rede. Você deve ter recebido uma mensagem semelhante a indicada na Figura 15:

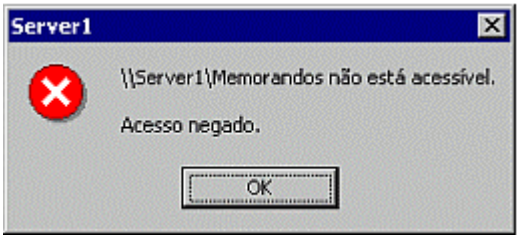


Figura 15 Acesso negado para o usuário Paulo Pereira (paulo).

8. Faça o logoff do usuário paulo no computador micro01.

IMPORTANTE: Observe que através da rede, as permissões de compartilhamento se comportaram conforme o esperado, isto é, o usuário paulo que não possuía as devidas permissões, teve o seu acesso negado.

Para testar o funcionamento das permissões de compartilhamento localmente, siga os seguintes passos:

1. Faça o logon no computador servidor com a conta de usuário paulo e para a senha digite paulo123. (ou utilize uma conta de usuário da sua rede, para a qual você não configurou as permissões no exemplo anterior).

2. Utilize o comando Iniciar -> Executar, para acessar a pasta compartilhada Memorandos, conforme descrito anteriormente. Dê um clique duplo para tentar acessar a pasta compartilhada Memorandos. Você conseguiu ?

3. Sim. Mas como é possível se o usuário paulo não possui as permissões de compartilhamento necessárias? Lembre-se de que você fez o logon no computador servidor, onde a pasta Memorandos foi criada, e conforme citado no início, as permissões de compartilhamento não tem efeito para acessos locais, somente para acessos através da rede. Para garantir a segurança para acessos locais é que vamos aprender a utilizar as permissões NTFS, nos próximos tópicos.

Configurando as permissões NTFS - Prática.

Neste tópico iremos atribuir permissões NTFS e testar o efeito das permissões, tanto localmente quanto através da rede. Para que você possa acompanhar todos os exemplos propostos neste tópico, é necessário que você tenha acesso a mais um computador em rede, além do computador onde foi criada a pasta compartilhada Memorandos.

Nos exemplos, utilizarei o computador servidor como sendo o computador onde se encontra a pasta compartilhada Memorandos e micro01 o outro computador em rede. Caso os nomes dos computadores que você está utilizando para acompanhar este tópico, sejam diferentes, utilize-os no lugar dos nomes aqui descritos.

Exemplo: Para atribuir permissões NTFS à pasta Memorandos, siga os seguintes passos:

1. Efetue o logon como Administrador, no computador servidor.

2. Abra o Windows Explorer.

3. No painel da esquerda, se Meu computador não estiver aberto, dê um clique no sinal de + ao lado de Meu computador para abri-lo.

4. Abaixo de Meu computador, surge uma listagem com todas as unidades disponíveis no computador. Inclusive unidade de diskete (A:\) e a unidade de CD-ROM. Localize a unidade onde você criou a pasta Memorandos, na lição anterior, abra a unidade e localize a pasta Memorandos.

5. Dê um clique com o botão direito do mouse sobre a pasta Memorandos, e no menu de opções que surge dê um clique em Propriedades.

6. Surge a janela "Propriedades de Memorandos", com a guia Geral selecionado por padrão. Dê um clique na guia "Segurança", que é a guia que utilizaremos para configurar as permissões NTFS para a pasta Memorandos. Surge a janela indicada na Figura 16.

IMPORTANTE: Observe que as opções na coluna Permitir estão marcadas para o grupo Todos, porém se tentarmos alterá-las clicando com o mouse, nada acontece. Isso acontece, porque quando criamos a pasta Memorandos, ela **"herdou"** as permissões do objeto pai, que no caso é a pasta raiz da unidade onde a pasta Memorandos foi criada. Esse é o comportamento padrão do Windows 2000 Server.

Outro detalhe importante, é que as permissões NTFS herdadas não podem ser alteradas, a menos que desativemos o mecanismo de herança. Podemos identificar que o mecanismo de herança está ativado, pelo fato da opção "Permitir que permissões herdadas do pai se propaguem para esse objeto", está marcada (que é o padrão no Windows 2000 Server).

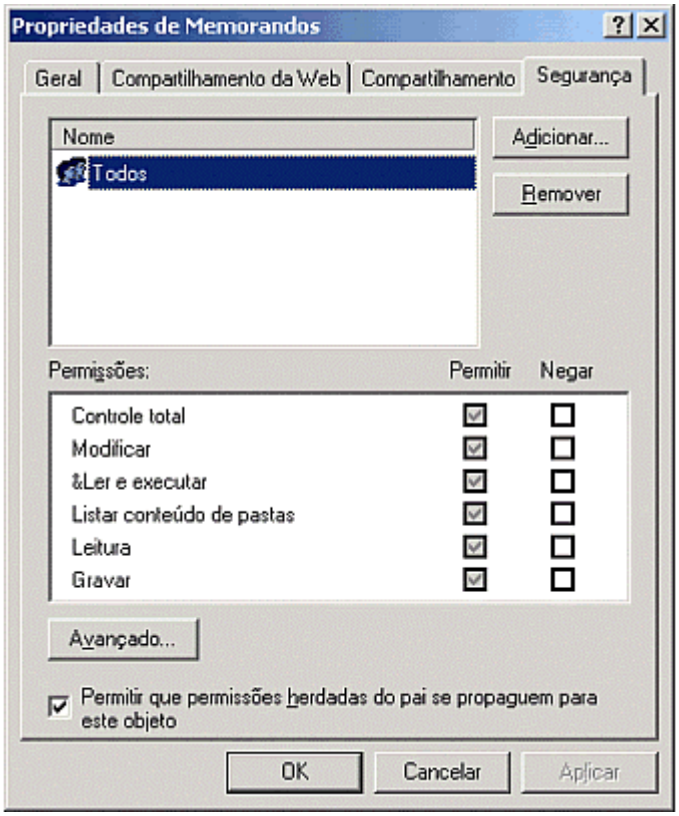


Figura 16 A guia "Segurança" da janela "Propriedades de Memorandos".

Além das permissões herdadas, podemos adicionar permissões NTFS para usuários ou grupos. Permissões adicionadas desta maneira são conhecidas como "Permissões explícitas", as quais podem ser alteradas a qualquer momento pelo Administrador do sistema, conforme a necessidade.

O Mecanismo de herança pode ser desativado. Para isso basta clicar na opção "Permitir que permissões herdades do pai se propaguem para esse objeto", para desmarcá-la. Ao fazer isso o Windows 2000 abre uma janela perguntando se você deseja Copiar as permissões herdados – caso em que o Windows 2000 as transforma como se tivessem sido explicitamente definidas – ou se você deseja removê-las, caso em que todas as permissões herdadas serão removidas. A janela onde o Windows 2000 Server pergunta o que você deseja fazer com as permissões herdadas, é indicada na Figura 17.

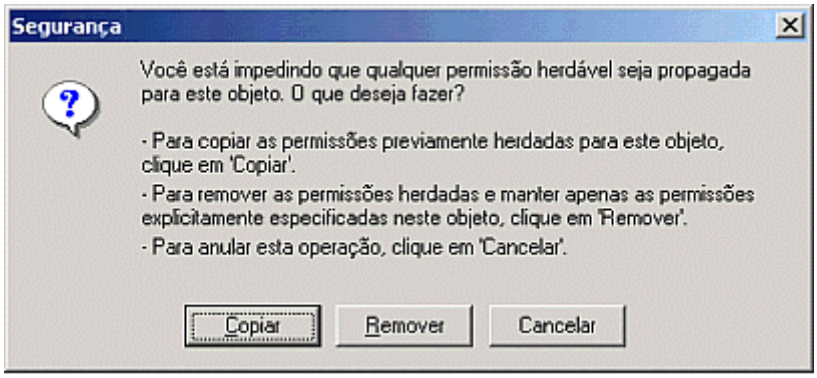


Figura 17 Você pode Copiar ou simplesmente Remover as permissões herdadas.

7. Vamos remover as permissões herdadas. Para isso dê um clique na opção "Permitir que permissões herdadas do pai se propaguem para esse objeto", para desativar as permissões herdadas. Na janela que surge dê um clique no botão Remover.

8. Você estará de volta a guia Segurança, mas agora o grupo Todos foi removido, juntamente com as permissões que o mesmo possuía.

9. Vamos adicionar permissão de Alteração para os usuários José da Silva e Maria do Socorro. Clique no botão "Adicionar". Surge uma janela com uma listagem dos usuários, grupos e computadores para o domínio Caruncho.

10. Localize o usuário José da Silva na listagem, dê um clique para marcá-lo e depois um clique no botão Adicionar. Repita a operação para o usuário Maria do Socorro.

11. Sua janela deve ficar conforme a indicada na Figura 18, onde foram adicionados os usuários José da Silva e Maria do Socorro.

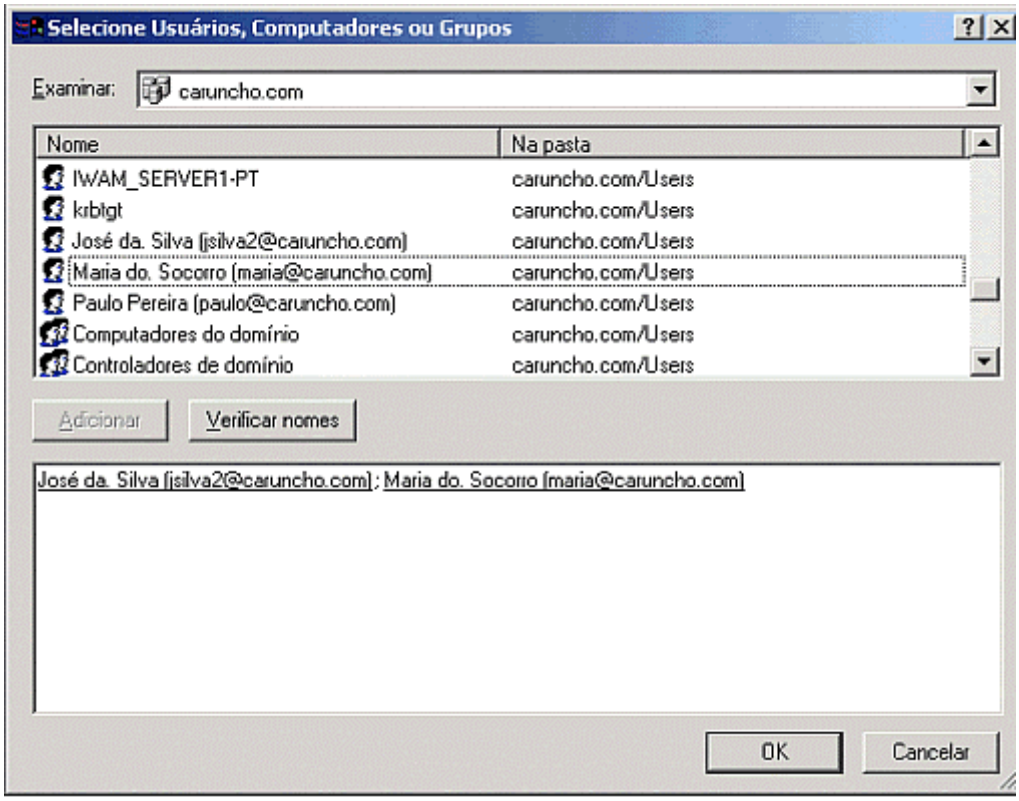


Figura 18 Adicionando os usuários José da Silva e Maria do Socorro.

12. Adicione também o usuário Administrador. Dê um clique no botão OK e você estará de volta a janela "Propriedades de Memorandos". Além de adicionar os dois usuários, devemos configurar o nível de acesso das permissões NTFS de cada usuário.

13. Vamos atribuir uma permissão NTFS de alteração para ambos.

14. Dê um clique em José da Silva para marcá-lo. Na parte do meio da janela, onde tem Permissões, dê um clique na opção Modificar , da coluna Permitir. Observe que todas as outras opções abaixo de Modificar, são automaticamente selecionadas.

15. Repita a operação para o usuário Maria do Socorro.

16 Repita a operação para o usuário Administrador. Porém para o usuário Administrador, na coluna Permitir marque a permissão Controle total, conforme indicado pela Figura 19.

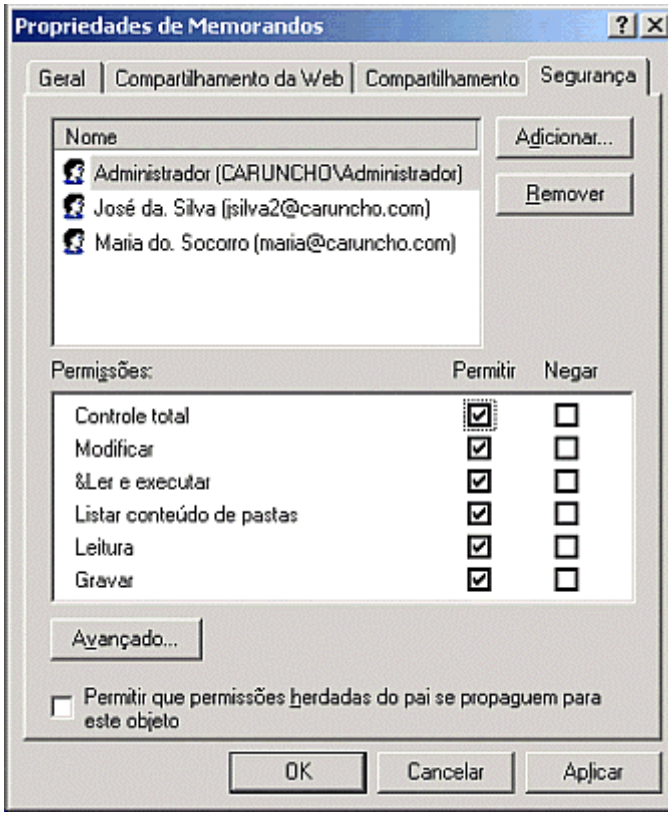


Figura 19 Permissão Controle total para o usuário Administrador

17. Dê um clique no botão OK, para fechar a janela "Propriedades de Memorandos".

18. Agora a pasta Memorandos possui permissões NTFS Modificar para os usuários jsilva2 e maria, bem como Controle Total para o usuário Administrador. Vamos testar estas permissões, tanto através da rede, quanto localmente.

Para testar o funcionamento das permissões NTFS através da rede, siga os seguintes passos:

1. Faça o logon no computador micro01 com a conta de usuário maria e para a senha digite senha123. (ou utilize uma conta de usuário da sua rede, para a qual você configurou as permissões NTFS no exemplo anterior).

2. Utilize o comando Iniciar -> Executar, para acessar a pasta compartilhada Memorandos, conforme descrito anteriormente. Dê um clique duplo para tentar acessar a pasta compartilhada Memorandos. Você conseguiu ?

3. É claro que sim, uma vez que o usuário Maria do Socorro (maria) tem permissão para acessar esse compartilhamento e também tem as permissões NTFS necessárias.

4. Faça o logoff do usuário maria.

5. Faça o logon no computador micro01 com a conta de usuário paulo e para a senha digite paulo123. (ou utilize uma conta de usuário da sua rede, para a qual você não configurou as permissões no exemplo anterior)

6. Utilize o comando Iniciar -> Executar, para acessar a pasta compartilhada Memorandos, conforme descrito anteriormente. Dê um clique duplo para tentar acessar a pasta compartilhada Memorandos. Você conseguiu ?

7. É claro que não, pois o usuário Paulo Pereira (paulo) não tem permissão para acessar esse compartilhamento através da rede e nem as permissões NTFS necessárias. Você deve ter recebido uma mensagem de acesso negado.

8. Faça o logoff do usuário paulo no computador Server2.

Para testar o funcionamento das permissões NTFS localmente, siga os seguintes passos:
1. Faça o logon no computador servidor com a conta de usuário paulo e para a senha digite paulo123. (ou utilize uma conta de usuário da sua rede, para a qual você não configurou as permissões NTFS na pasta Memorandos).

2. Utilize o comando Iniciar -> Executar, para acessar a pasta compartilhada Memorandos, conforme descrito anteriormente. Dê um clique duplo para tentar acessar a pasta compartilhada Memorandos. Você conseguiu ?

3. Não. Mas como é possível se você está acessando a pasta Memorandos localmente, isto é, no computador onde ela foi criada ?

4. Lembre-se de que você fez o logon no computador servidor, onde a pasta Memorandos foi criada, mas utilizando a conta de usuário paulo, a qual não possui as permissões NTFS para acessar a pasta Memorandos. Não esqueça que as permissões NTFS tem efeito tanto localmente quanto através da rede, diferente das permissões de compartilhamento, as quais não tem nenhum efeito localmente. Porém existe uma situação onde as permissões de compartilhamento são a única alternativa, que é no caso de unidades formatadas com FAT. Para estas unidades não existem permissões NTFS.

5. Abra o Windows Explorer e tente acessar a pasta Memorandos. Você conseguiu? É claro que não, pois o usuário logado (paulo) não tem permissões NTFS de acesso à pasta Memorandos. Veja que com as permissões NTFS é possível proteger o acesso a pastas e arquivos locais, o que não era possível com o Windows 95/98 ou Me, conforme descrito no início.

6. Feche a mensagem de acesso negado e efetue o logoff do usuário paulo.
Agora vamos criar um arquivo de texto chamado teste.txt dentro da pasta Memorando e atribuir permissões NTFS para esse arquivo:

Para criar um arquivo teste.txt e atribuir permissões NTFS para esse arquivo, siga os seguintes passos:
1. Efetue o logon como Administrador, no computador servidor.

2. Abra o Windows Explorer.

3. No painel da esquerda, se Meu computador não estiver aberto, dê um clique no sinal de + ao lado de Meu computador para abri-lo.

4. Abaixo de Meu computador, surge uma listagem com todas as unidades disponíveis no computador. Inclusive unidade de diskete (A:\) e a unidade de CD-ROM. Localize a unidade onde você criou a pasta Memorandos, na lição anterior, abra a unidade e localize a pasta Memorandos.

5. No painel da esquerda, dê um clique sobre a pasta Memorandos para abrí-la.

6. No painel da direita, em qualquer espaço livre, dê um clique com o botão direito do mouse, e no menu que surge aponte para Novo e nas opções do menu Novo dê um clique sobre a opção Documento de texto.

7. Surge uma caixa onde está escrito "Novo documento de texto", conforme indicado pela Figura 20.

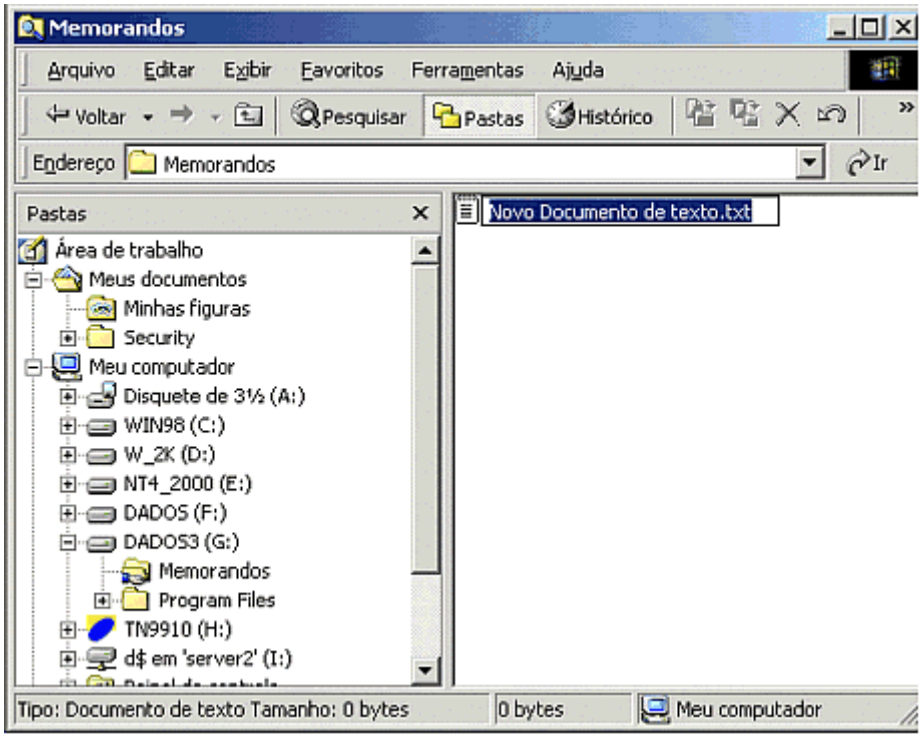


Figura 20 Criando um novo documento de texto.

8. Não clique em lugar nenhum nem tecle Enter, simplesmente digite o nome do arquivo que está sendo criada, no nosso exemplo digite teste.txt e tecle Enter. O Windows 2000 Server cria um documento de texto em branco, com o nome de teste.txt.

9. Dê um clique com o botão direito sobre teste.txt e no menu que surge dê um clique sobre Propriedades.

10. Surge a janela "Propriedades de teste.txt", com a guia Geral selecionado por padrão.

11. Dê um clique na guia "Segurança", que é a guia que utilizaremos para configurar as permissões NTFS para o arquivo teste.txt. Surge a janela indicada na Figura 21.

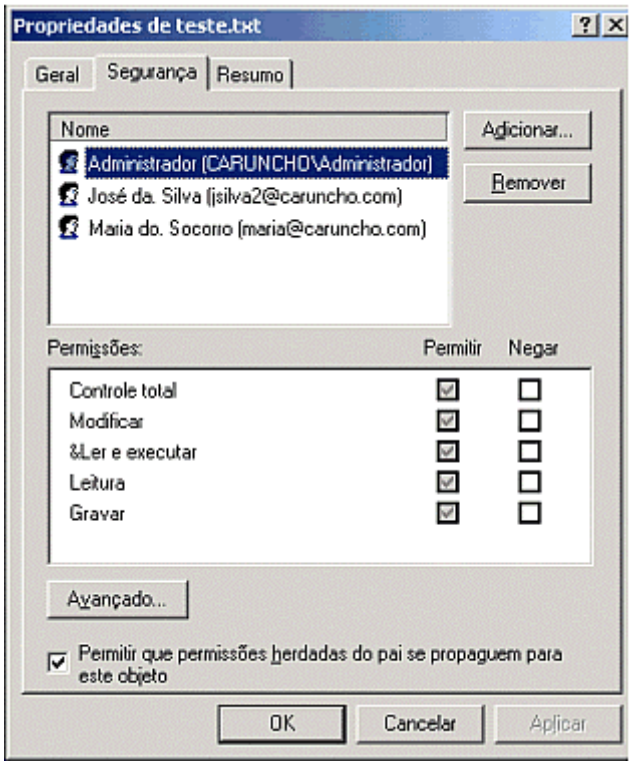


Figura 21 A guia "Segurança" da janela "Propriedades de teste.txt".

IMPORTANTE: Observe que algumas opções na coluna Permitir estão marcadas para os usuários Administrador, José da Silva e Maria do Socorro , porém se tentarmos alterá-las clicando com o mouse, nada acontece. Isso acontece, porque quando criamos o arquivo teste.txt ele "herdou" as permissões do objeto pai, que no caso é a pasta Memorandos. Esse é o comportamento padrão do Windows 2000.

Outro detalhe importante, é que as permissões NTFS herdadas não podem ser alteradas, a menos que desativemos o mecanismo de herança. Podemos identificar que o mecanismo de herança está ativado, pelo fato da opção "Permitir que permissões herdadas do pai se propaguem para esse objeto", está marcada (que é o padrão no Windows 2000).

Além das permissões herdadas, podemos adicionar permissões NTFS para usuários ou grupos. Permissões adicionadas desta maneira são conhecidas como "Permissões explícitas", as quais podem ser alteradas a qualquer momento pelo Administrador do sistema, conforme a necessidade.

O Mecanismo de herança pode ser desativado. Para isso basta clicar na opção "Permitir que permissões herdades do pai se propaguem para esse objeto", para desmarcá-la. Ao fazer isso o Windows 2000 abre uma janela perguntando se você deseja Copiar as permissões herdados – caso em que o Windows 2000 Server as transforma como se tivessem sido explicitamente definidas – ou se você deseja removê-las, caso em que todas as permissões herdadas serão removidas.

12. Vamos Copiar as permissões herdadas. Para isso dê um clique na opção "Permitir que permissões herdadas do pai se propaguem para esse objeto", para desativar as permissões herdadas. Na janela que surge dê um clique no botão Copiar. Com isso copiamos as permissões herdados, transformando-as em permissões explícitas, as quais podem ser alteradas.

13. Dê um clique em José da Silva para marcá-lo. Na parte do meio da janela, onde tem Permissões, deixe apenas o opção Leitura marcada.

14. Repita a operação para o usuário Maria do Socorro.

15. Dê um clique no botão OK, para fechar a janela "Propriedades de teste.txt".

16. Agora a pasta Memorandos possui permissões NTFS Modificar para os usuários jsilva2 e maria e Controle total para o usuário Administrador. Já o arquivo teste.txt tem permissão somente de Leitura para os usuários jsilva2 e maria e Controle total para o usuário Administrador.

17. Agora temos permissões NTFS para a pasta memorandos e permissões NTFS diferentes para o arquivo teste.txt que está dentro da pasta Memorandos. Vamos testar estas permissões, tanto através da rede, quanto localmente.

Para testar o funcionamento das permissões NTFS através da rede, siga os seguintes passos:

1. Faça o logon no computador micro01 com a conta de usuário maria e para a senha digite senha123. (ou utilize uma conta de usuário da sua rede, para a qual você configurou as permissões NTFS na pasta Memorandos).

2. Utilize o comando Iniciar -> Executar, para acessar a pasta compartilhada Memorandos, conforme descrito anteriormente. Dê um clique duplo para tentar acessar a pasta compartilhada Memorandos. Você conseguiu ?

3. É claro que sim, uma vez que o usuário Maria do Socorro (maria) tem permissão para acessar esse compartilhamento e também tem as permissões NTFS necessárias.

4. Dê um clique duplo na pasta Memorandos para acessá-la. Dentro da pasta Memorandos deve estar o arquivo teste.txt. Dê um clique para marcá-lo e pressione a tecla Delete para eliminá-lo.

5. Você conseguiu eliminar o arquivo teste.txt ?

6. Não. Isso porque o usuário maria possui permissões NTFS modificar na pasta Memorandos, mas no arquivo teste.txt, as permissões do usuário maria são apenas Leitura. Como as permissões de arquivo tem prioridade sobre as permissões de pasta, a permissão efetiva do usuário maria sobre o arquivo teste.txt é Leitura, a qual não permite que o arquivo seja deletado.

7. Você deve ter recebido uma mensagem semelhante a da Figura 5.22. Dê um clique em OK para fechá-la.

Figura 22 Mensagem de acesso negado.

8. Faça o logoff do usuário maria.

Para testar o funcionamento das permissões NTFS localmente, siga os seguintes passos:

1. Faça o logon no computador servidor com a conta de usuário maria e para a senha digite senha123.

2. Utilize o comando Iniciar -> Executar, para acessar a pasta compartilhada Memorandos, conforme descrito anteriormente. Dê um clique duplo para tentar acessar a pasta compartilhada Memorandos. Você conseguiu ?

3. É claro que sim, uma vez que o usuário Maria do Socorro (maria) tem permissão para acessar esse compartilhamento e também tem as permissões NTFS necessárias.

4. Dentro da pasta Memorandos deve estar o arquivo teste.txt. Dê um clique para marcá-lo e pressione a tecla Delete para eliminá-lo.

5. Você conseguiu eliminar o arquivo teste.txt ?

6. Não. Isso porque o usuário maria possui permissões NTFS modificar na pasta Memorandos, mas no arquivo teste.txt, as permissões do usuário maria são apenas Leitura. Como as permissões de arquivo tem prioridade sobre as permissões de pasta, a permissão efetiva do usuário maria sobre o arquivo teste.txt é Leitura, a qual não permite que o arquivo seja deletado.

7. Além disso nunca é demais lembrar que as permissões NTFS são válidas tanto para acessos através da rede, quanto para acessos locais.

8. Você deve ter recebido uma mensagem de erro. Dê um clique em OK para fechá-la.

9. Faça o logoff do usuário maria.

Combinando permissões de compartilhamento e permissões NTFS.

Você pode estar se perguntando como é que o Windows 2000 trata quando existem diferenças entre as permissões de compartilhamento e as permissões NTFS. Por exemplo se nas permissões de compartilhamento o usuário maria tem direito de Controle total e nas permissões NTFS o usuário maria tem direito de Leitura. Qual a permissão efetiva do usuário maria ?

NÃO ESQUEÇA: Quando existe diferenças entre as permissões de compartilhamento e as permissões NTFS, a permissão efetiva é a mais restritiva, isto é, aquele que restringe mais as ações que podem ser tomadas. No nosso exemplo, a permissão efetiva para o usuário maria seria Leitura, a qual é mais restritiva do que Controle total.

Vamos analisar algumas situações práticas para fixar bem a combinação entre permissões de compartilhamento e NTFS.

Exemplo 01: Considere a situação indicada na Figura 23. Qual a permissão efetiva do usuário jsilva2 sobre a pasta compartilhada Memorandos ?

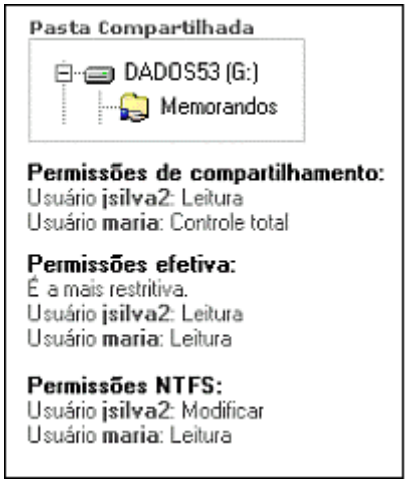


Figura 23 A permissão efetiva é a mais restritiva.

Para entender a situação da Figura 5.26, devemos lembrar que no caso de diferenças entre as Permissões de compartilhamento e permissões NTFS, a permissão efetiva é a mais restritiva.

No exemplo da figura a permissão efetiva do usuário jsilva2 é leitura a qual é a mais restritiva entre Modificar (a permissão NTFS do usuário jsilva2) e Leitura (permissão de compartilhamento do usuário jsilva2). A mesma análise é válida em relação ao usuário maria.

Exemplo 02: Vamos considerar uma situação um pouco mais complexa, onde temos que considerar a combinação das permissões dos diferentes grupos aos quais pertence um usuário, além da combinação entre permissões de compartilhamento e permissões NTFS.

Vamos admitir que o usuário jsilva2 pertença aos grupos Contabilidade e Marketing. Com base na Figura 24, quais seria a permissão efetiva para o usuário paulo sobre a pasta compartilhada Memorandos?

Figura 24 Usuário jsilva2 pertence aos grupos Marketing e Contabilidade.

Para definir a permissão efetiva para o usuário jsilva2, temos que levar em conta diversas regras.

☐ Quando um usuário pertence a vários grupos, os quais recebem diferentes permissões (quer sejam permissões de compartilhamento ou NTFS), a permissão efetiva é a soma das permissões. Além disso devemos lembrar que Negar tem prioridade sobre permitir. No caso das permissões de compartilhamento, um dos grupos ao qual o usuário jsilva2 pertence – grupo Contabilidade – tem a permissão de leitura negada. Logo a permissão efetiva de compartilhamento para jsilva2 é Negar leitura.

☐ A permissão efetiva NTFS para o usuário jsilva2 é a soma das permissões do usuário com as permissões dos grupos Marketing e Contabilidade. Com isso a permissão NTFS efetiva é Permitir Controle total.

Com isso podemos reduzir a nossa situação a uma situação mais simplificada, conforme indicado na Figura 25:

Figura 25 Simplificando a situação.

☐ Agora temos que lembrar que quando existe diferença entre as permissões de compartilhamento e NTFS vale a mais restritiva.

Com isso podemos determinar que a permissão efetiva do usuário jsilva2 sobre o compartilhamento Memorandos é "Negar Leitura", isto é, o usuário não conseguirá nem listar o conteúdo da pasta.

Mapeamento de unidades de rede.

Até agora acessávamos uma pasta compartilhada, utilizando o comando Iniciar -> Executar. Porém essa não é a maneira mais prática quando precisamos acessar um determinado compartilhamento seguidamente. Quando isso acontece, devemos "Mapear uma unidade".

Mapear uma unidade significa que vamos associar uma determinada letra com o compartilhamento da rede. Por exemplo, poderíamos associar a unidade M:\ como o

compartilhamento Memorandos do computador servidor. Com isso ao acessar a unidade M:\, na verdade estaremos acessando o conteúdo da pasta compartilhada Memorandos. Além disso podemos fazer com que o Windows 2000 restabeleça este mapeamento toda vez que for feito o logon. Com isso a unidade estará sempre disponível.

Exemplo: Vamos mapear o drive M: para a pasta compartilhada Memorandos no computador servidor.

Para mapear uma unidade de rede usando o Meu computador.
1. Faça o logon como Administrador no computador micro01.

2. Dê um clique duplo em Meu computador para abrí-lo.

3. Dê um clique no menu Ferramentas e dentro de Ferramentas dê um clique na opção "Mapear unidade de rede...". Surge a janela "Mapear unidade de rede", indicada na Figura 26:

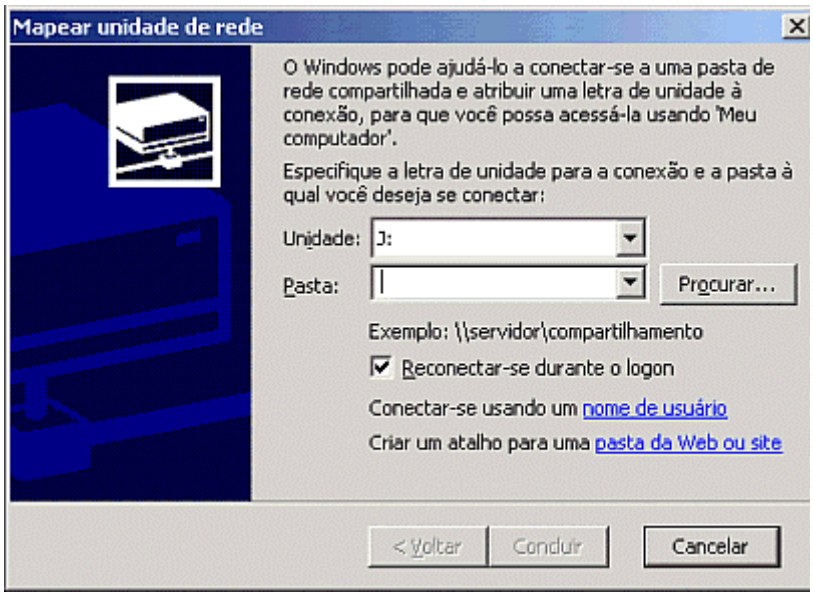


Figura 26 Janela "Mapear unidade de rede".

4. Na lista Unidade selecione M:

5. No campo Pasta: digite \\servidor\Memorandos. Conforme vimos antes este é o nome UNC do compartilhamento Memorandos no computador servidor.

6. Certifique-se que a opção "Reconectar-se durante o logon" esteja marcada, conforme indicado na Figura 27. Essa opção faz com que o drive M: seja mapeado cada vez que o usuário Administrador fizer o logon.

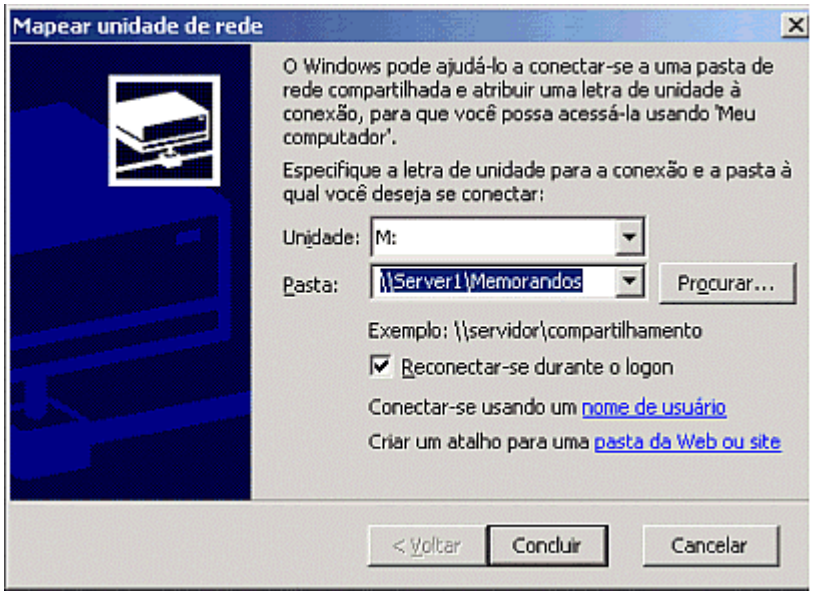


Figura 27 Definindo o mapeamento do drive M:

7. Dê um clique no botão Concluir.

8. O Windows 2000 Server abre uma janela mostrando o conteúdo do drive mapeado. Feche essa janela.

9. Você estará de volta na janela Meu computador.

10. Procure por um drive M:. Se esse ainda não aparece, tecle F5 para atualizar a listagem. O drive M: deve aparecer na listagem, conforme indicado na Figura 28.

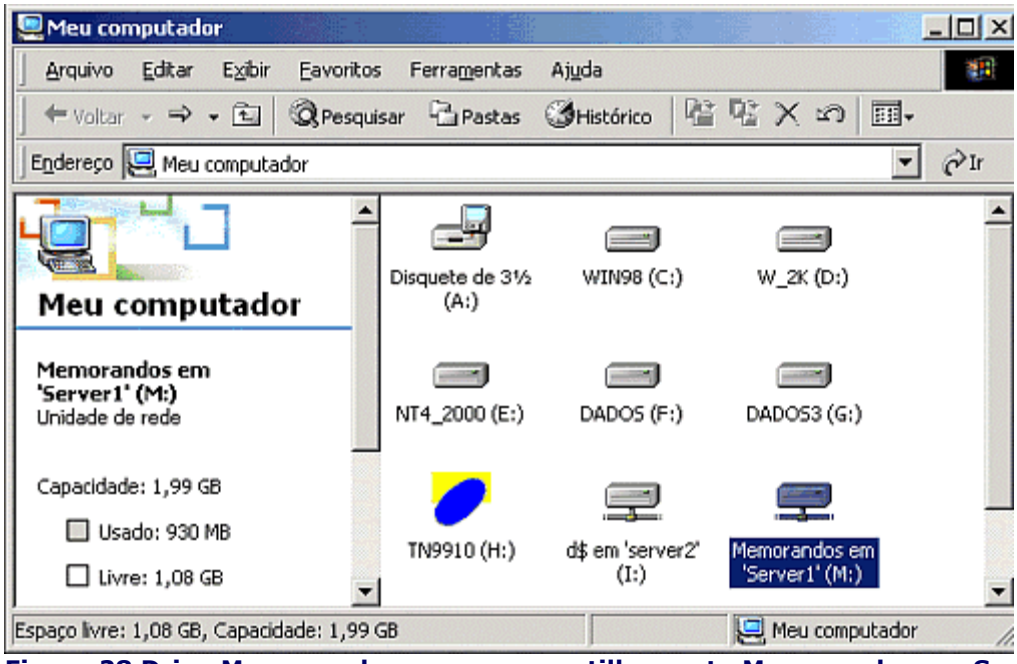


Figura 28 Drive M: mapeado para o compartilhamento Memorandos em Server1.

DICA: Uma maneira mais fácil de mapear um drive é localizar o compartilhamento através do comando Iniciar -> Executar, conforme descrito anteriormente; clicar no compartilhamento com o botão direito do mouse e no menu que surge clique em "Mapear unidade de rede". O Windows 2000 abre uma janela, semelhante a da Figura 28, com o nome UNC já preenchido. A única coisa que você precisa fazer é escolher a letra da unidade para o mapeamento e dar um clique em OK.

Você pode acrescentar o símbolo do cifrão ($) no final do nome de um compartilhamento. O efeito de acrescentar o cifrão é que você torna o compartilhamento oculto, isto é, ele não pode ser localizado através do ícone "Meus locais de rede". Por exemplo, se você criar um compartilhamento no computador servidor, cujo nome de compartilhamento é Dados$, a única maneira de acessá-lo é através do nome UNC: \\Server1\Dados$. Compartilhamentos deste tipo, são chamados de compartilhamentos ocultos. Podemos mapear uma unidade de rede para um compartilhamento oculto, desde que saibamos o caminho completo.

Existem alguns compartilhamentos ocultos especiais, para os quais somente o grupo Administradores tem acesso e cujas permissões de acesso não podem ser modificadas. Por padrão o Windows 2000 Server cria compartilhamentos administrativos para todas as unidades de disco rígido do computador. Por exemplo, se você tem duas unidades de disco rígido C: e D:, o Windows 2000 Server irá criar dois compartilhamentos administrativos C$ e D$, para os quais somente o grupo Administradores tem acesso, podendo inclusive mapear uma unidade para um compartilhamento administrativo.

Quando não precisamos mais de um drive mapeado podemos, facilmente, desconectá-lo.

Para desconectar um drive mapeado, siga os seguintes passos:
1. Faça o logon como Administrador no computador micro01.

2. Dê um clique duplo em Meu computador para abrí-lo.

3. Localize o drive a ser desconectado e dê um clique com o botão direito no drive.

4. No menu que surge dê um clique na opção "Desconectar-se" e pronto.

5. Caso o drive ainda esteja aparecendo tecle F5 para atualizar a listagem.

Mais alguns detalhes importantes:

Quando copiamos ou movemos pastas, considere os seguintes fatos a respeito das permissões NTFS resultantes:

☐ Quando movemos ou copiamos uma pasta para uma partição formatada com FAT ou FAT32, as permissões NTFS serão perdidas.

☐ Quando copiamos uma pasta ou arquivo para a mesma partição ou para uma partição diferente, o Windows 2000 considera a cópia como se fosse uma nova pasta/arquivo. Neste caso, a cópia irá herdar as permissões NTFS da pasta onde a cópia está sendo feita.

☐ Quando movemos uma pasta/arquivo dentro da mesma partição, a pasta/arquivo mantém as permissões NTFS que estavam atribuídas.

☐ Quando movemos uma pasta/arquivo para uma partição diferente é como se estivéssemos fazendo uma cópia na nova partição e excluindo na partição atual. Neste caso, a pasta/arquivo vai herdar as permissões NTFS da pasta de destino.

WINXP - Descricao do Compartilhamento da Conexao de Internet no Windows XP

Com o Compartilhamento da Conexão de Internet, você pode conectar computadores na sua casa ou pequeno escritório a Internet através de uma única conexão. Por exemplo, se você ativa o Compartilhamento da Conexão de Internet num computador que se conecta a Internet usando uma conexão dial-up, outros computadores na rede podem conectar a Internet através da conexão dial-up no computador host do Compartilhamento da Conexão de Internet.
Você pode usar o Compartilhamento da Conexão de Internet para permitir você e outros na sua rede local (LAN) executarem tarefas diferentes simultaneamente. Por exemplo, uma pessoa pode enviar e receber mensagens de e-mail, enquanto outra pessoa faz download de um arquivo, e ainda outra pessoa navega
na Internet. Você também pode ganhar aceso às suas contas de e-mail corporativas a partir de um computador cliente enquanto outros na sua rede não podem. Você pode usar programas preparados para Web (como fazer download de atualizações) bem como o Microsoft NetMeeting e outros programas de vídeo conferência.

Capacidades do Compartilhamento da Conexão de Internet
· Múltiplos usuários podem ganhar acesso a Internet através de uma única conexão usando conexões dial-up e rede local.

· Dispositivos conectados recebem configurações de rede transparentes usando DNS (Domain Name System) e DHCP (Dynamic Host Configuration Protocol) para resolver nomes da Internet.· Qualquer dispositivo anexado pode se conectar, incluindo versões antigas de clientes baseados no Windows, clientes não baseados no Windows, clientes baseados no Microsoft Windows 98, clientes baseados no Microsoft Windows 2000 e clientes baseados no Microsoft Windows XP sem nenhum software de cliente
adicional requerido.

· Dispositivos conectados e software tem suporte de protocolo compreensível. Por exemplo, você pode executar jogos da Internet sem configurações adicionais, ou você pode usar PPTP (Point-to-Point Tunneling Protocol) e VPN (Virtual Private Networking) para ganhar acesso a sua rede corporativa.

Suporte do Windows para Compartilhamento da Conexão Para conectar múltiplos computadores a Internet através de uma única conexão de Internet, você tem que ativar o Compartilhamento da Conexão de Internet no computador que você quer usar como host do Compartilhamento da Conexão de Internet.
Outros computadores na sua rede local podem ganhar acesso a Internet através da conexão no computador host do Compartilhamento da Conexão de Internet. NOTA: o Compartilhamento da Conexão de Internet é um recurso interno do Windows e não é um componente disponível para download. Além de computadores baseados no Windows XP, você pode ativar o Compartilhamento da Conexão de Internet em computadores executando o Windows 98 Segunda Edição, Windows Millennium Edition (Me) e Windows 2000.

Componentes do Compartilhamento da Conexão de Internet
A seguinte lista componentes do Compartilhamento da Conexão de Internet:
· Alocador DHCP – Um serviço DHCP simplificado que atribui endereços IP, gateway padrão e servidor de nomes na rede local.

· DNS Proxy - Resolve nomes no lado dos clientes da rede local
e encaminha consultas.

· NAT (Network Address Translation) - Mapeia um bloco de endereços privados para um conjunto de endereços públicos. A tradução NAT pesquisa endereços IP de origem privada e endereços IP de destino público para requisições de saída. Este altera as informações do endereço IP e edita o as informações
do cabeçalho de IP requisitado dinamicamente.
· Auto-discagem – Disca automaticamente conexões.
· APIs (Application Programming Interfaces) – Para
configuração, status e controle de discagem para programas.

Configurando uma Rede com o Compartilhamento da Conexão de Internet Sua rede do Compartilhamento da Conexão de Internet é um tipo de rede local que confia num único computador chamado gateway, através do qual todos os outros computadores e dispositivos capacitados para TCP/IP conectam-se a Internet. O hardware e software necessários para uma rede doméstica
incluem:
· Um computador primário, chamado gateway, que fornece conectividade de rede para a Internet. Este computador tem que estar executando o Windows XP, Windows 2000, Windows Me ou Windows 98 Segunda Edição com o Compartilhamento da Conexão de Internet ativado.

· Um ou mais computadores executando o Windows 95, Windows 98, Microsoft Windows NT 4.0, Windows 2000, Windows XP ou outro software de cliente capacitado para TCP-IP.
· Dispositivos que são capazes de se conectarem a Internet.

· Um dispositivo de conexão de rede para cada computador.
· Cabos e hubs, dependendo do tipo de dispositivos de conexão que você usa.
· Um único modem (ou uma linha ISDN ou ADSL) para a rede inteira.
· Software de navegação da Internet e drivers de TCP/IP
instados em cada dispositivo que compartilha a conexão.

Ative o Compartilhamento da Conexão de Internet Antes de você poder ativar o Compartilhamento da Conexão de Internet num computador host, o computador tem que ter duas conexões de rede presentes. Um adaptador de rede configurado para a rede doméstica ou do pequeno escritório interna, e outra
conexão usando um modem de 56K, ISDN, DSL ou modem a cabo para conectar a pequena rede doméstica ou do escritório a Internet.

Como configurar o Compartilhamento de Conexão com a Internet no Windows XP

INTRODUÇÃO

Vamos descrever como configurar e usar o recurso de Compartilhamento de Conexão com a Internet no Microsoft Windows XP. Com o Compartilhamento de Conexão com a Internet, é possível usar computadores em rede para compartilhar uma única conexão com a Internet.

Como Usar o Compartilhamento de Conexão com a Internet

Para usar o Compartilhamento de Conexão com a Internet para compartilhar a conexão da Internet, o computador host deve ter um adaptador de rede configurado para conectar-se à rede interna e um adaptador de rede ou modem configurado para conectar-se à Internet.

No computador host

No computador host, execute as seguintes etapas para compartilhar a conexão com a Internet:

1. Faça logon no computador host como Administrador ou como Proprietário.
2. Clique em **Iniciar** e em **Painel de controle**.
3. Clique em **Conexões de rede e de Internet**.
4. Clique em **Conexões de rede**.
5. Clique com o botão direito sobre a conexão que você usa para conectar-se à Internet. Por exemplo, se você se conecta à Internet usando um modem, clique com o botão direito do mouse sobre a conexão que deseja em **Dial-up**.
6. Clique em **Propriedades**.
7. Clique na guia **Avançadas**.
8. Em **Compartilhamento de Conexão com a Internet**, marque a caixa de seleção **Permitir que outros usuários da rede se conectem através da conexão deste**

computador com a Internet.

9. Se você estiver compartilhando uma conexão de Internet dial-up, marque a caixa de seleção **Estabelecer uma conexão discada sempre que um computador na minha rede tentar acessar a Internet**, se desejar permitir que o computador se conecte automaticamente à Internet.

10. Clique em **OK**. Você receberá a seguinte mensagem:
Quando o Compartilhamento de Conexão com a Internet for ativado, o adaptador de rede local será configurado para usar o endereço IP 192.168.0.1. O computador poderá perder a conectividade com outros computadores da rede. Se esses computadores tiverem endereços IP estáticos, você deverá configurá-los
para obter os endereços IP automaticamente. Tem certeza de que deseja ativar o Compartilhamento de Conexão com a Internet?

11. Clique em **Sim**.

A conexão com a Internet é compartilhada com outros computadores na rede local. O adaptador de rede que está conectado à rede local está configurado com um endereço IP estático de 192.168.0.1 e uma máscara de sub-rede de 255.255.255.0

No computador cliente

Para se conectar com a Internet usando uma conexão compartilhada, é necessário verificar a configuração de IP do adaptador de rede local e configurar o computador cliente. Para verificar a configuração de IP do adaptador de rede local, execute as seguintes etapas:

1. Faça logon no computador cliente como Administrador ou como Proprietário.
2. Clique em **Iniciar** e em **Painel de controle**.
3. Clique em **Conexões de rede e de Internet**.
4. Clique em **Conexões de rede**.
5. Clique com o botão direito do mouse em **Conexão local** e clique em **Propriedades**.
6. Clique na guia **Geral**, em **Protocolo (TCP/IP)** na lista **Esta conexão usa os seguintes itens** e clique em **Propriedades**.

   Na caixa de diálogo **Propriedades do Protocolo de Internet (TCP/IP)**, clique em **Obter um endereço IP automaticamente** (caso já não esteja selecionado) e, em seguida, em **OK**.

7. **Observação** Também é possível atribuir um endereço IP único estático que varie de 192.168.0.2 a 192.168.0.254. Por exemplo, é possível atribuir o endereço estático IP, máscara de sub-rede e gateway padrão:
   Endereço IP 192.168.0.2
   Máscara de sub-rede 255.255.255.0
   Gateway padrão 192.168.0.1

8. Na caixa de diálogo **Propriedades de Conexão de Área Local**, clique em **OK**.
9. Feche o Painel de controle.

Para configurar o computador cliente para usar a conexão compartilhada com a Internet, execute as seguintes etapas:

1. Clique em **Iniciar** e em **Painel de controle**.
2. Clique em **Conexões de rede e de Internet**.
3. Clique em **Opções da Internet**.
4. Na caixa de diálogo **Opções da Internet**, clique na guia **Conexões**.
5. Clique no botão **Configurar**.

   O Assistente para novas conexões é iniciado.
6. Na página **Bem-Vindo ao Assistente para novas conexões**, clique **Avançar**.
7. Clique em **Conectar-me à Internet** e, em seguida, clique em **Avançar**.
8. Clique em **Configurar conexão manualmente** e, em seguida, em **Avançar**.

9. Clique em **Conectar usando conexão banda larga sempre ativa** e, em seguida, em **Avançar**.
10. Na página **Concluindo o 'Assistente para novas conexões'**, clique em **Concluir**.
11. Encerre o Painel de controle.

Solução de Problemas

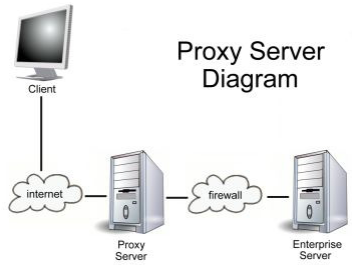
Ao ativar o Compartilhamento de Conexão com a Internet no computador host, o adaptador de rede local do computador host é automaticamente atribuído ao endereço IP de 192.168.0.1. Por isso, uma das seguintes situações pode ocorrer:

- **Conflito de endereço IP**
  Cada computador na rede local deve ter seu próprio endereço IP. Se mais de um computador tiver o mesmo endereço IP, um conflito IP ocorre e um dos adaptadores de rede é desativado até que o conflito seja resolvido. Para resolver este conflito, configure o computador cliente para obter automaticamente um endereço IP ou atribuir-lhe um endereço IP próprio.
- **Perda de conectividade de rede.**
  Se a rede estiver configurada com um intervalo de endereços IP diferente do usado pelo Compartilhamento de Conexão com a Internet, irá haver perda conectividade de rede com o computador host. Para resolver este problema, configure os computadores clientes para que obtenham o endereço IP automaticamente, ou atribua a cada computador cliente o seu próprio endereço IP no intervalo de 192.168.0.2 a 192.168.0.254.

Para que Serve?

Um servidor proxy recebe pedidos de computadores ligados à sua rede e, caso necessário, efetua esses mesmos pedidos e os encaminha ao resto da Internet, usando como identificação o seu próprio número IP e não o número IP do computador que requisitou o serviço.

Exemplo



Suponha que você queira acessar o site do Senado Federal (http://www.senado.gov.br) através do servidor de proxy do Senado.

Se o seu web browser estiver corretamente configurado, a busca será feita, primeiramente, no servidor proxy do próprio site. Se a página deste já estiver neste servidor (alguém a acessou anteriormente) a transferência será feita deste ponto. Caso contrário, a transferência será feita do próprio site do Senado.

Vantagens

Esse tipo de serviço agiliza os acessos pois, em vez de transferir os dados de sites distantes ou com conexões de baixa velocidade, os dados são transferidos de um servidor do Próprio Senado.

Cache

A idéia básica no cache é simples: armazenar os documentos retornados em um arquivo local para uso posterior de forma que não seja necessário se conectar ao servidor remoto na próxima vez que o documento seja requisitado

Configuração e segurança

Manter o seu servidor Proxy bem configurado é uma prática que o administrador de rede deve ter em mente sempre.

Alguns problemas de Proxy nos afetam diariamente. A correta configuração do Proxy no Gateway de Comunicações pode evitar muitos aborrecimentos e ainda evitar que o nome de nossa empresa seja notificado à NBSO.

Qual o problema da minha máquina ser um "Open Proxy"?

A anonimidade proporcionada por um "Open Proxy" pode ser usada para cometer crimes, tais como envio de mensagens caluniosas, difamatórias ou ameaçadoras e divulgação de pornografia envolvendo crianças.

O que é um "Open Relay"?

Uma situação de "open relay" ocorre quando um servidor de e-mails processa uma mensagem onde nem o remetente nem o destinatário são usuários locais deste servidor. Spammers geralmente usam servidores que permitem essa operação para entregar milhares de mensagens não solicitadas para outros sites na Internet.

O que é "Spamvertised website"?

Indica que uma URL foi mencionada, referenciada ou notificada em uma mensagem considerada spam. É importante ressaltar que a URL normalmente tem relação direta com o conteúdo do spam.

Windows 2003 Server

Conceitos Fundamentais

Domínio está presente em uma rede cliente/servidor onde um computador central (Servidor) contém informações relacionadas com os usuários (os nomes, senhas e outras informações a respeito de pessoas autorizadas a utilizar o sistema) é mantida de forma centralizada.

Grupos de Trabalho é um agrupamento lógico de computadores em rede que compartilham recursos sem existir um servidor dedicado, responsável pelo gerenciamento e funcionamento da rede.

Active Directory

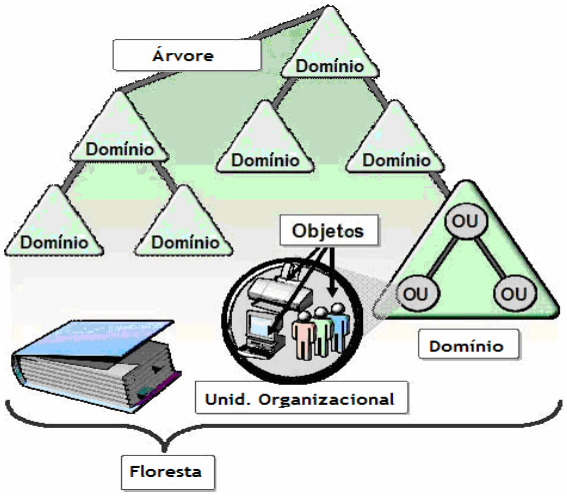
O serviço de diretório Active Directory® proporciona a estrutura e as funções para organizar, administrar e controlar o acesso aos recursos de rede. Para implementar e administrar uma rede do Windows Server 2003.
O Active Directory é o serviço de diretório de uma rede do Windows Server 2003. Um serviço de diretório armazena informações sobre os recursos da rede e permite que os mesmos estejam acessíveis aos usuários e aos aplicativos. Os serviços de diretório proporcionam uma forma coerente de nomear, descrever, localizar, obter acesso, administrar e proteger as informações relativas aos recursos da rede.

DNS

Em função do AD usar DNS como sua forma de denominação de domínios e localização de serviços, os nomes de domínio do Windows 2003 são também nomes DNS. Windows 2000 Server utiliza DNS dinâmico, o qual habilita computadores clientes com associação de endereços dinamicamente registrados no servidor DNS e com atualização da tabela também de forma dinâmica.
O DNS dinâmico pode eliminar a necessidade de outros serviços de nome Internet, como o Windows Internet Naming Service (WINS).

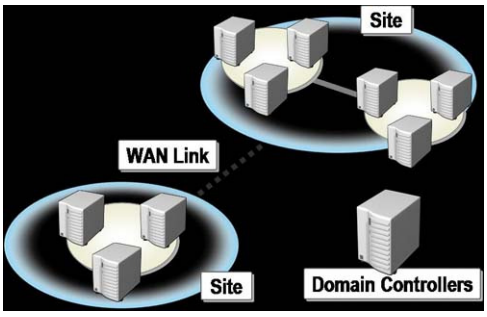
Estrutura Lógica

Nos serviços do AD você organiza recursos em uma estrutura lógica. O agrupamento lógico de recursos possibilita localizar um recurso pelo seu nome ao invés de sua localização física.
A estrutura lógica do Active Directory inclui os seguintes componentes:
Objeto: Um objeto é qualquer usuário, sistema, recurso ou serviço rastreado dentro do AD.
Atributos: descrevem objetos no Active Directory.
Contêiner: é um tipo de objeto especial utilizado para organizar o AD.
Unidades Organizacionais:Uma unidade organizacional é um objeto contêiner usado para organizar objetos como contasde usuários, grupos, computadores, impressoras, aplicações, compartilhamento de arquivos e outros.
Domínios: é uma coleção de objetos administrativos definidos que compartilham, através de um banco de dados comum do diretório, diretivas de segurança e relações de confiança com outros Domínios.
Árvores de domínio: São Domínios agrupados em estruturas hierárquicas.
Florestas: Uma floresta é um agrupamento de uma ou mais árvores.



Estrutura física do Active Directory
Em comparação com a estrutura lógica e os requisitos administrativos dos modelos, a estrutura física do Active Directory otimiza o tráfego da rede, determinando como e quando ocorre a replicação e o tráfego do logon.
Para otimizar o uso da largura de banda da rede Active Directory, você precisa entender a sua estrutura física.
Controladores de domínio: Estes computadores executam o Microsoft® Windows® Server 2003 ou o Windows 2000 Server e o Active Directory. Cada Controlador de Domínio realiza funções de armazenamento e replicação e, além disso, oferece suporte a apenas um domínio. Para garantir uma disponibilidade contínua do Active Directory, cada domínio deve ter mais de um controlador de domínio.

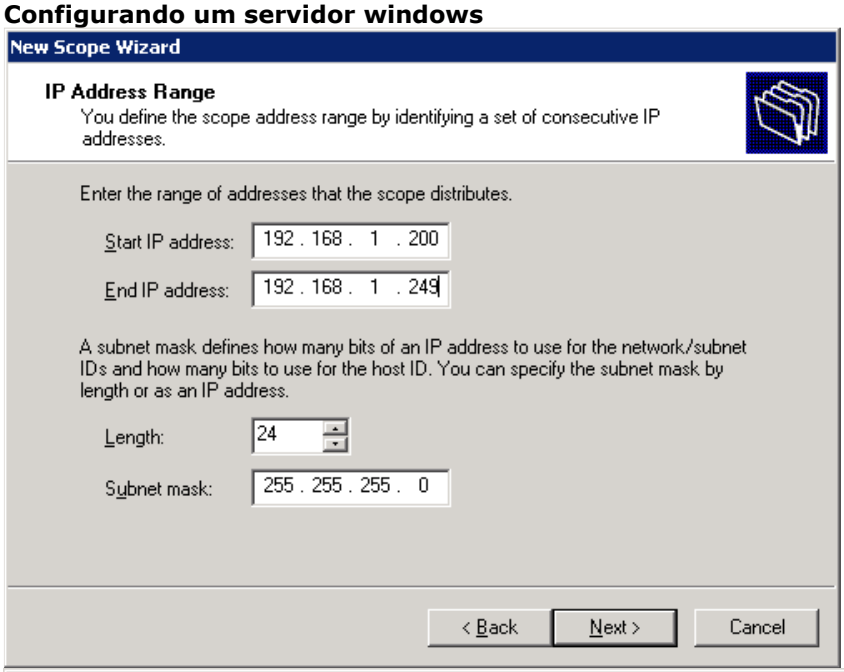
Sites do Active Directory: são grupos de computadores conectados. Quando você estabelece sites os Controladores de Domínios que estão dentro de um mesmo site podem se comunicar com freqüência. Essa comunicação reduz ao mínimo o estado de latência dentro do site, isso é, o tempo necessário para que uma
modificação realizada em um Controlador de Domínio seja duplicada nos outros controladores de domínio.
Partições do Active Directory Cada Controlador de Domínio contém as seguintes partições do Active Directory:
Partições de Domínio, que contêm a replicação de todos os objetos neste domínio. Essa partição é duplicada apenas para outros Controladores de Domínio do mesmo domínio.
Partição de Configuração, que contém a topologia da floresta. A topologia registra todas as conexões dos Controladores de Domínio na mesma floresta.
Partição de Esquema, que contém o esquema da floresta. Cada floresta tem um esquema de modo que a definição de cada classe do objeto seja constante. As partições de Configuração e Esquema de Partições são duplicadas para cada Controlador de **Domínio na floresta.**
Opções de Partição de Aplicativos que contêm os objetos relacionados à segurança e são utilizados por um ou mais aplicativos. As partições de aplicativos são duplicadas em Controladores de Domínio específicos na floresta.

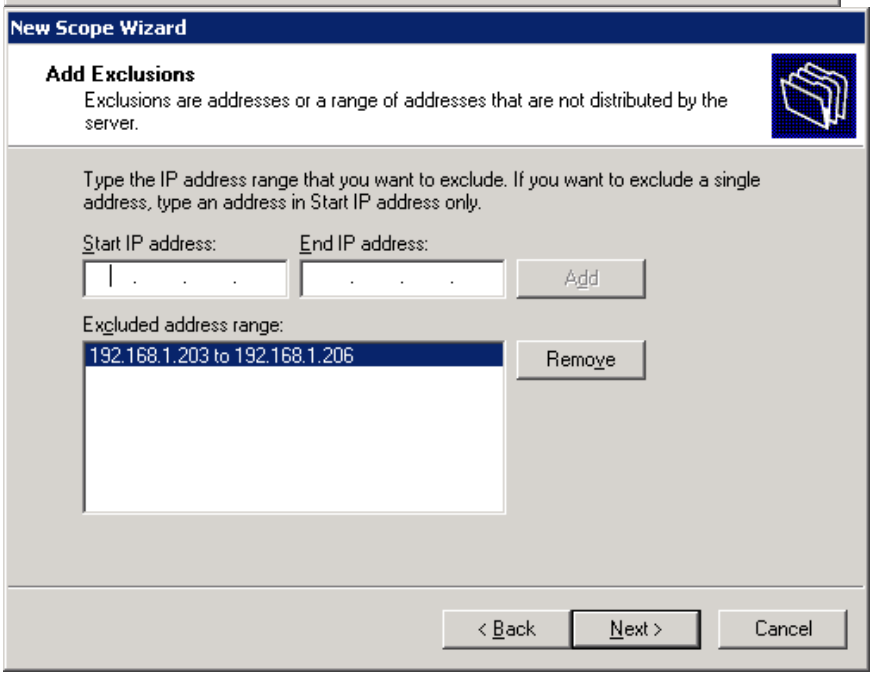


Para instalar o servidor DHCP, acesse o "Configure Your Server Wizard" e selecione a opção "DHCP Server" na lista de funções. Isso dispara um wizard que permite configurar o escopo de endereços que será usado pelo servidor.

DHCP

Configurando um servidor windows





As opções incluem o range de endereços que será usado pelo servidor e a máscara de sub-rede (que pode ser fornecida no sistema CIDR ou na notação tradicional). Na tela seguinte, você pode definir uma lista de exclusões, ou seja, faixas de endereços dentro da faixa definida na primeira opção que não devem ser usadas pelo servidor DHCP.

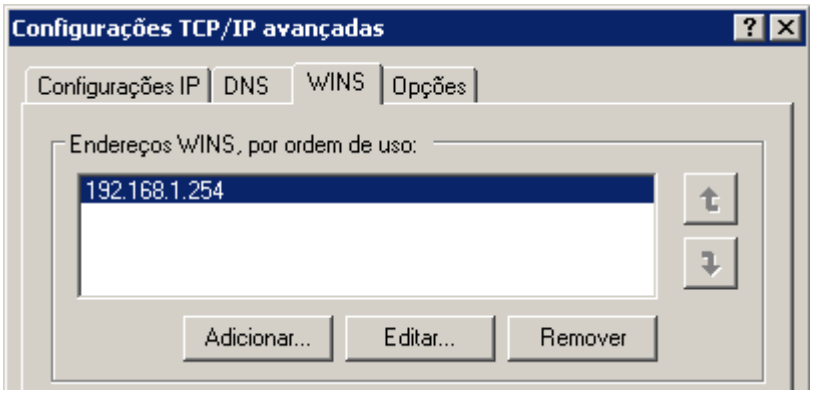
Em seguida são definidos o gateway da rede, servidores DNS e servidor WINS (caso usado). No final do processo, você terá a opção de inicializar a configuração imediatamente, ou de deixar para aplicá-la mais tarde (o que pode ser feito se você precisar verificar a configuração da rede ou consultar outro administrador antes de ativar o servidor DHCP, por exemplo).

Você pode também aproveitar para ativar o servidor **WINS**, que tem um papel secundário dentro das redes Microsoft, funcionando como uma base de dados que relaciona os nomes das máquinas com os endereços IP correspondentes, ajudando na navegação da rede. Sem ele, os clientes Windows que não foram configurados para fazer parte de um domínio

precisam recorrer a pacotes de broadcast para a navegação da rede, o que aumenta o tráfego e torna a navegação no ambiente de redes mais lenta.

Para ativar o servidor WINS, acesse o "Configure Your Server Wizard" e selecione a opção "WINS Server". A menos que você precise utilizar vários servidores WINS na mesma rede, a configuração é basicamente automática. Basta ativar o serviço e o servidor passa a manter a base de nomes e a responder às requisições dos clientes.

A partir daí, falta apenas configurar os clientes para utilizarem seu servidor. Ao usar o DHCP, você pode especificar o endereço do servidor WINS como parte da configuração. No caso dos clientes com configuração manual, a opção fica escondida nas propriedades da conexão de rede, no Protocolo TCP/IP > Propriedades > Avançado > WINS:



O WINS está lentamente entrando em desuso, já que a mesma tarefa realizada por ele pode ser executada de forma mais eficiente por um servidor DNS corretamente configurado. Apesar disso, ele ainda é um serviço importante, que vai demorar para deixar de ser usado completamente.

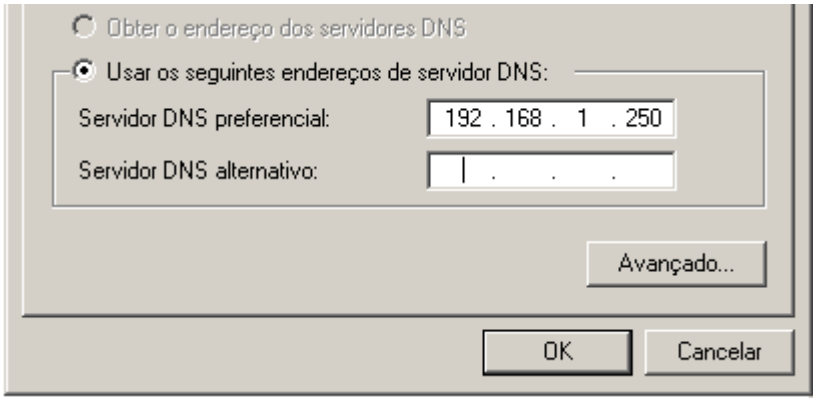
Servidor DNS

Em seguida temos a configuração do **DNS**. Como bem sabemos, o DNS é o protocolo usado para converter nomes de domínio em endereços IP. Dentro das redes Microsoft, o DNS é especialmente importante, pois a partir do Windows 2000 ele passou a ser usado como serviço primário para resolução de nomes dentro da rede (substituindo o antigo protocolo WINS) e passou a ser uma das bases do Active Directory. A rede passa então a utilizar um domínio, que pode ser dividido em subdomínios e em endereços individuais para os PCs e servidores da rede.

Se você pretende implantá-lo na sua rede, então você precisa primeiro configurar o servidor DNS, para só então ativar o Active Directory. Você pode rodar os dois serviços em servidores diferentes, mas de qualquer forma é necessário que o servidor DNS esteja disponível na rede. Os dois serviços são inseparáveis.

Embora recomendável, não é obrigatório usar um domínio registrado. Se o servidor é destinado apenas à sua rede local, ou se você está apenas montando uma rede de teste para estudar o funcionamento do servidor, é perfeitamente possível inventar um nome de domínio.

Nesse caso é necessário configurar todos os PCs para utilizarem o endereço IP do seu servidor DNS local como único servidor DNS. Qualquer estação que utilize um servidor DNS externo não conseguirá encontrar o domínio, já que ele existirá apenas dentro da sua própria rede:



Mas, em um ambiente real de produção, é importante fazer a configuração da forma correta, registrando um domínio válido. Você pode fazer o registro diretamente no registro.br ou contratar os serviços de uma empresa de hospedagem. É muito comum aproveitar o domínio usado pelo site da empresa, criado um subdomínio para a rede interna, como "intranet.empresa.com.br". Para usar o domínio, é necessário que o servidor de DNS responsável pela rede tenha uma conexão com endereço IP fixo e que o DNS responsável pelo domínio principal seja configurado para encaminhar para ele as requisições referentes à zona usada pela rede interna.

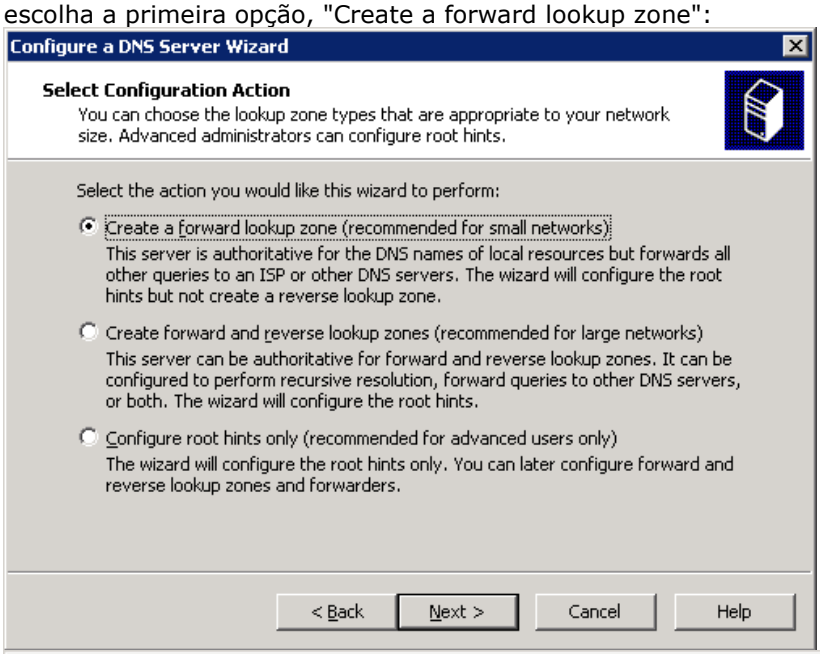
A configuração do servidor propriamente dito é feita através da opção "DNS Server" do "Configure Your Server Wizard":

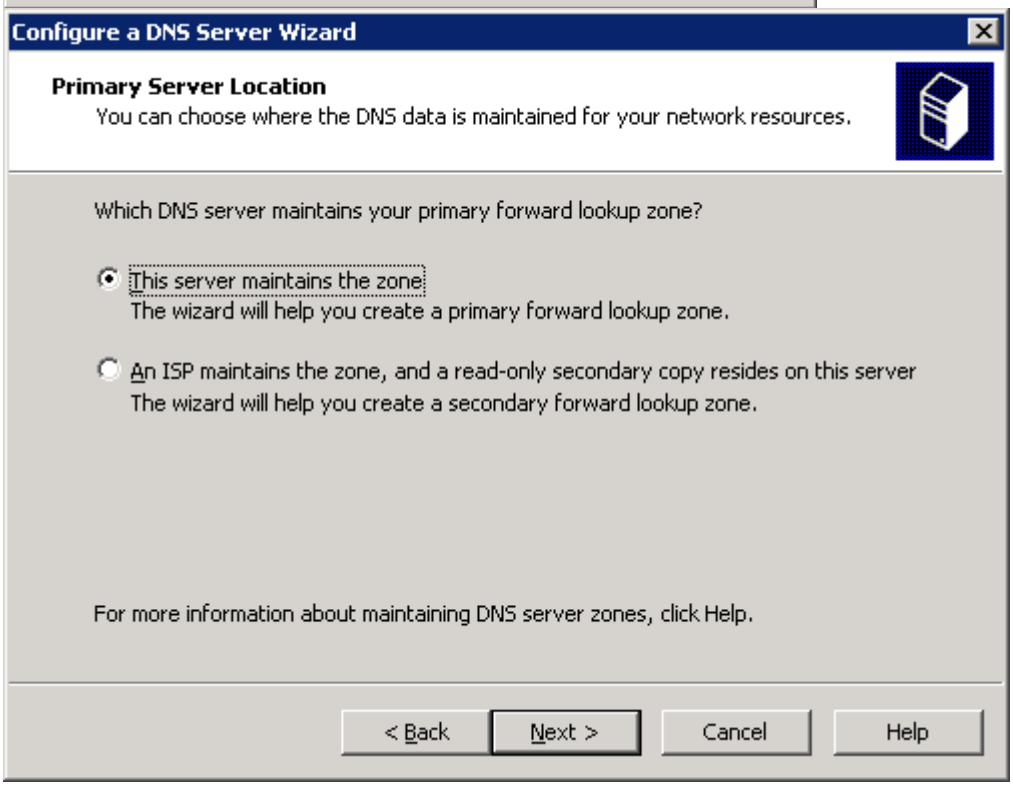
A configuração do servidor DNS inclui dois passos. O primeiro é a configuração da zona de pesquisa, que permite que o servidor faça a resolução dos nomes. Esta é a principal parte da configuração. A segunda é configurar a zona reversa (DNS reverso), que é um passo opcional, necessário apenas se o seu servidor usa um DNS válido e é usado como servidor de e-mails.

O DNS reverso é utilizado por diversos servidores SMTP para verificar a autenticidade dos endereços, ou seja, verificar se o servidor é realmente o responsável pelo domínio especificado no remetente dos e-mails, de forma a dificultar o envio de spam. Sem configurar a zona reversa, os e-mails provenientes do seu servidor serão rotulados como spam e descartados por muitos servidores.

A primeira pergunta (Select the action you would like this wizard to perform) do assistente se refere justamente a isso. Se você está configurando um DNS local (mesmo que utilizando

um domínio válido), em um servidor que não ficará diretamente disponível via Internet, escolha a primeira opção, "Create a forward lookup zone":

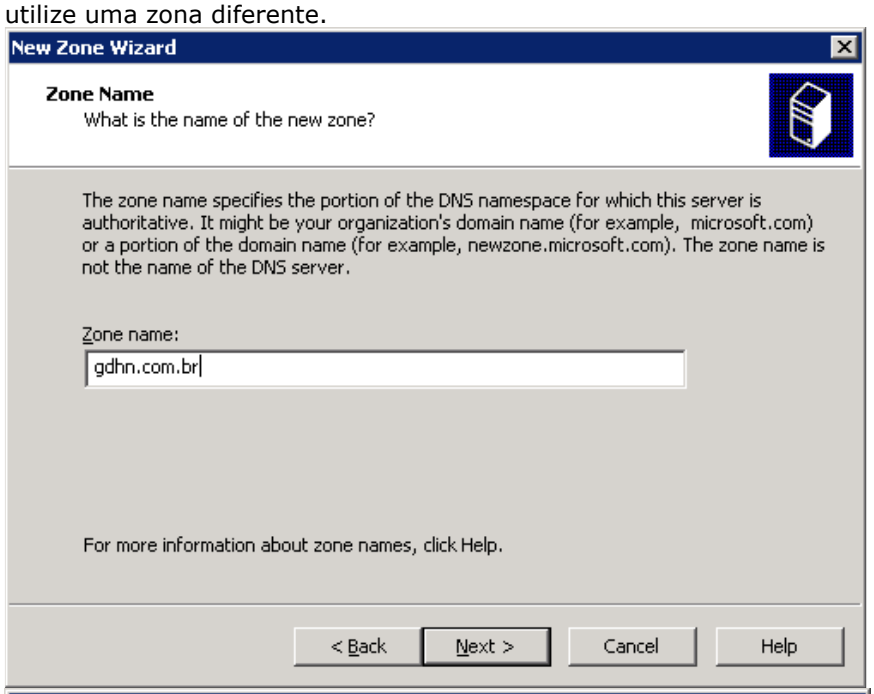


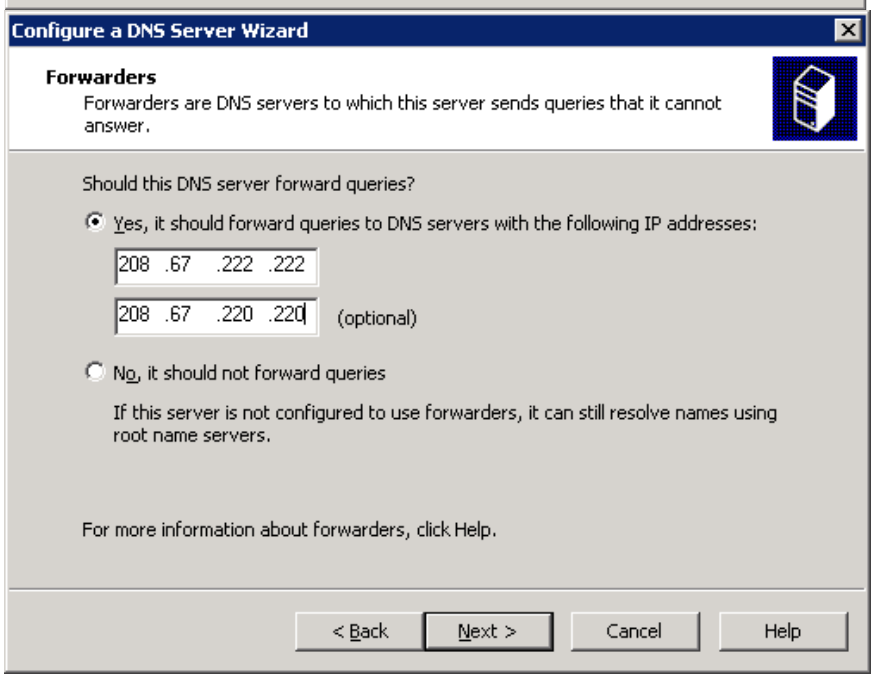


A segunda pergunta (Which server maintains your primary forward lookup zone) se refere à manutenção do domínio. Se você não está usando um domínio registrado, ou se você mesmo realizou o registro e está configurando o servidor para responder por ele, use a opção "This server maintains the zone". A segunda opção (An ISP maintains the zone and a read-only secondary copy resides on the server) é usada apenas caso o domínio tenha sido configurado por uma empresa de hospedagem ou provedor de acesso (que já configurou um servidor externo para responder por ele) e seu servidor está sendo configurado como servidor DNS secundário.

Na opção "Zone Name" vem a parte mais importante (e mais simples), que é especificar a zona, ou seja, o domínio que será utilizado pelo servidor. É possível tanto usar um domínio primário, como "gdhn.com.br" quanto um subdomínio, como "intranet.gdhn.com.br". O uso

de subdomínios é muito comum em grandes redes, de forma a permitir que cada subrede utilize uma zona diferente.

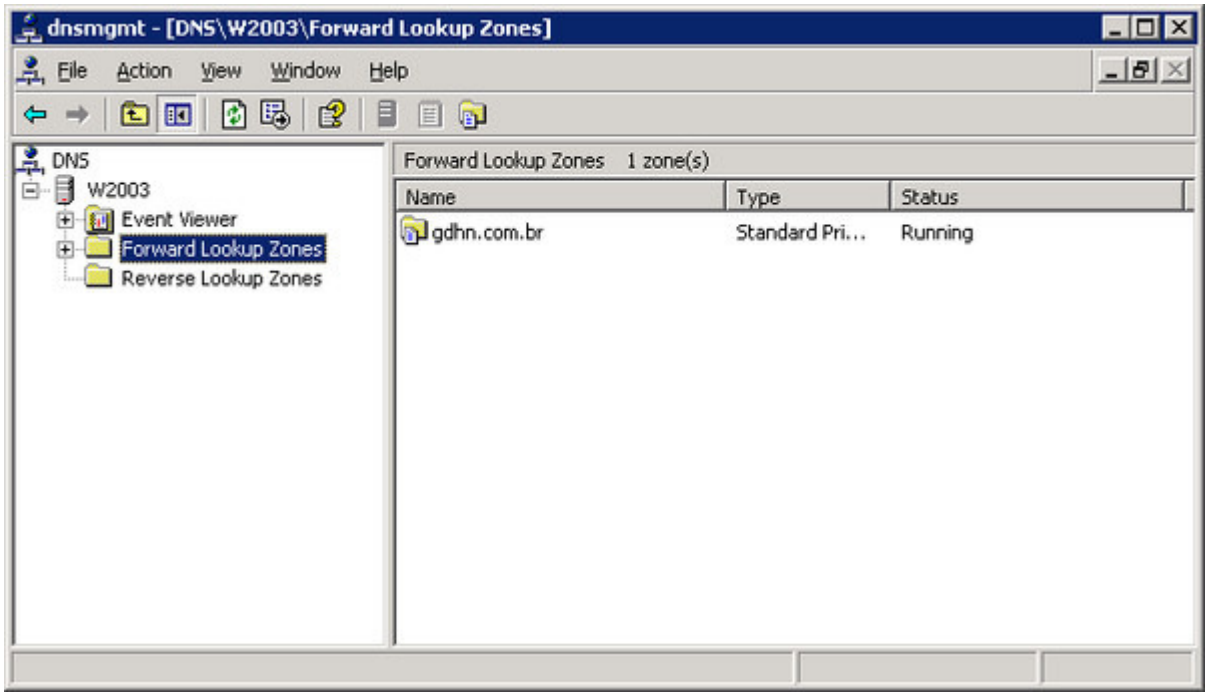




No final do wizard, na opção "Forwarders", marque a opção "Yes, it should forward queries to DNS servers with the following IP address" e preencha os dois campos com os endereços dos servidores DNS usados para acessar a Internet. Isso faz com que o servidor encaminhe as requisições de domínios da Internet para eles, permitindo que as máquinas da rede local acessem normalmente.

Com isso, o servidor DNS responde diretamente requisições dentro de sua própria zona (ou seja, dentro do domínio especificado na configuração) e repassa todas as demais uma os servidores DNS do provedor.

Depois de concluído o assistente, você pode alterar a configuração do servidor DNS e ter acesso às opções avançadas através do "Administrative Tools > DNS" no iniciar:



Active Directory

Em uma pequena rede, você pode usar o simple sharing do Windows XP (configurar um servidor Samba com acesso para a conta "guest") para criar compartilhamentos de rede de acesso fácil, porém sem segurança. É possível também centralizar os compartilhamentos em um servidor central, criando contas de acesso separadas para cada usuário. Mas, em uma grande rede, nenhuma das duas opções são satisfatórias, já que deixar os compartilhamentos escancarados deixaria a rede incrivelmente vulnerável e tentar sincronizar manualmente listas de usuários entre vários servidores seria um trabalho contínuo, fonte de muita dor de cabeça.

A partir do Windows NT foi introduzido o conceito de domínios, onde um servidor central, chamado de PDC (Primary Domain Controller, ou controlador primário de domínio) armazena um diretório central, contendo os logins e senhas de acesso, permissões de segurança e outras informações. O PDC passa então a funcionar como um servidor de autenticação para toda a rede, centralizando a administração.

Ao cadastrar um novo usuário no servidor PDC, ele automaticamente pode fazer logon em qualquer uma das estações configuradas como membros do domínio. Ao remover ou bloquear uma conta de acesso, o usuário é automaticamente bloqueado em todas as estações. Isso elimina o problema de sincronismo entre as senhas no servidor e nas estações e centraliza a administração de usuários e de permissões de acesso no servidor, simplificando bastante seu trabalho de administração.

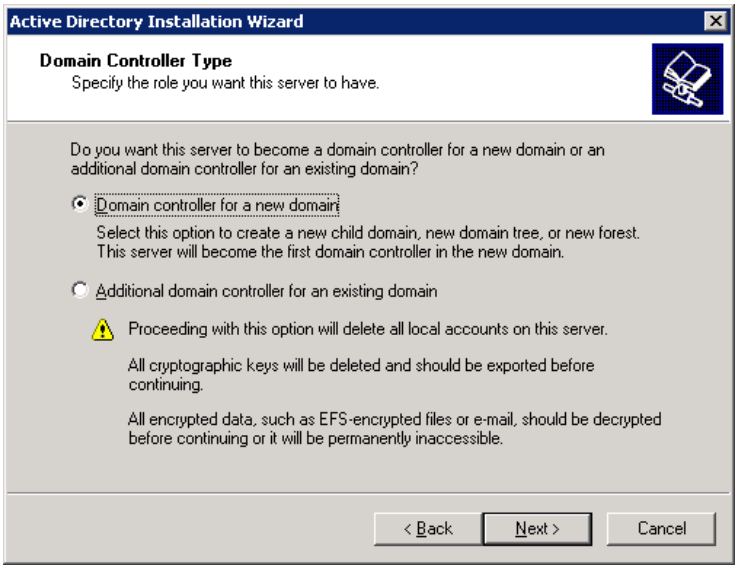
A partir do Windows 2000, este recurso foi expandido, dando origem ao Active Directory. Ele é baseado em uma implementação do LDAP e permite armazenar um volume muito maior de informações, além de facilitar o uso de diversos servidores no mesmo domínio. Essencialmente, o Active Directory oferece as mesmas funções oferecidas por um domínio NT, combinadas com novos recursos.

No Linux, existe a opção de configurar o Samba como controlador de domínio, inclusive participando do Active Directory, como se fosse um servidor Windows. Entretanto, o Samba 3 ainda não é capaz de atuar como servidor primário do Active Directory, tarefa que por enquanto pode ser desempenhada apenas por um servidor Windows. O suporte a Active Directory está sendo incluído na versão 4 do Samba que (início de 2008), está em estágio alpha.

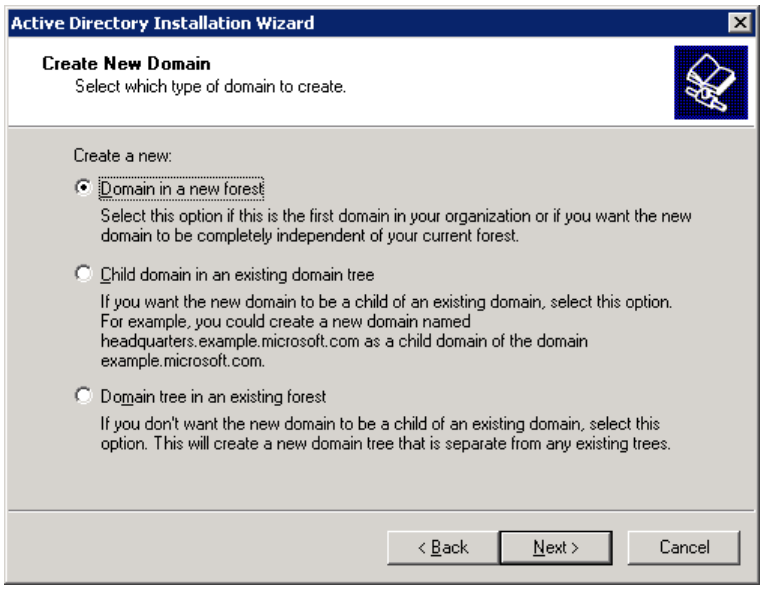
Vamos então à configuração:

Depois de ativar o DNS, você pode acessar o assistente para ativar o Active Directory e promover o servidor a Controlador de Domínio usando a opção "Domain Controller (Active Directory)" do "Manage Your Server" ou chamando o "dcpromo.exe" através do "Iniciar > Executar".

Para o primeiro controlador de domínio da rede, escolha a opção "Domain controller for a new domain" e em seguida a opção "Domain in a new forest". A opção "Additional domain controller for an existing domain" é usada apenas quando você já tem um domínio ativo e está adicionando novos servidores a ele:



Na pergunta seguinte (Create New Domain), você pode escolher entre três opções. SE este é o seu primeiro servidor de domínio, escolha a opção "Domain in a new forest":



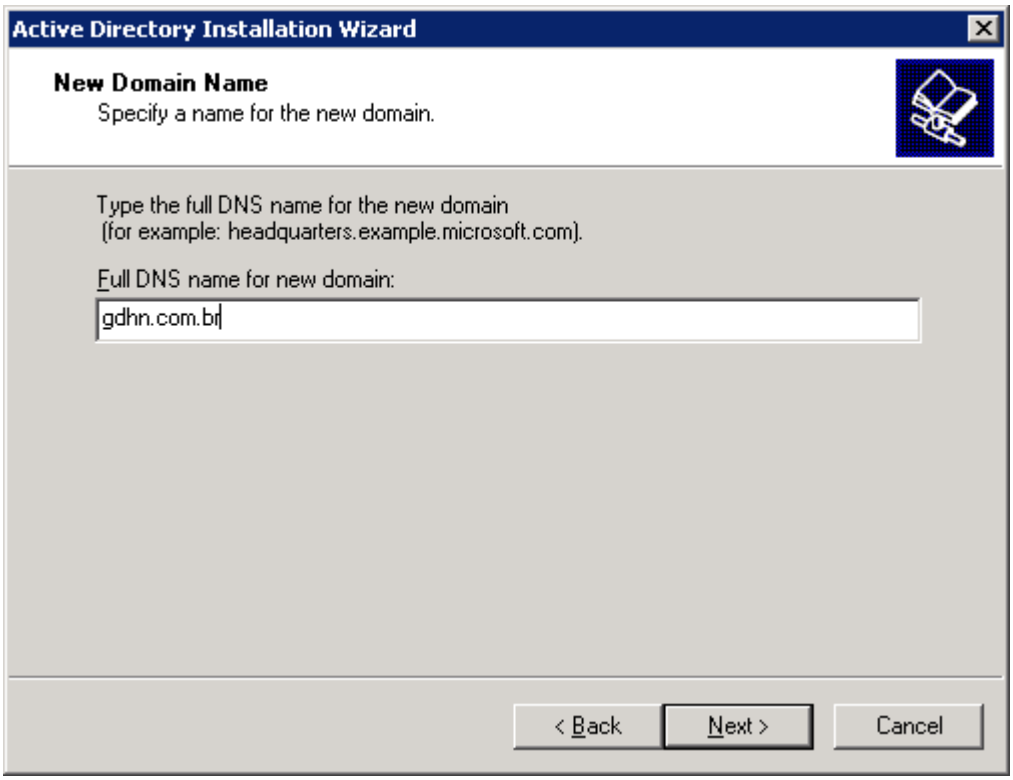
O Active Directory é organizado dentro do conceito de árvores e florestas. Tudo começa com o primeiro servidor do domínio, que passa a ser a raiz da primeira árvore. É possível criar sub-domínios (child domains) como "adm.gdhn.com.br" e "vendas.gdhn.com.br" entram na analogia como galhos na árvore. Você pode então cadastrar novos servidores, criando um

subdomínio diferente para cada um (um para cada departamento da empresa, por exemplo). Nesse caso, você usaria a opção "Child domain in an existing domain tree" ao cadastrá-los.

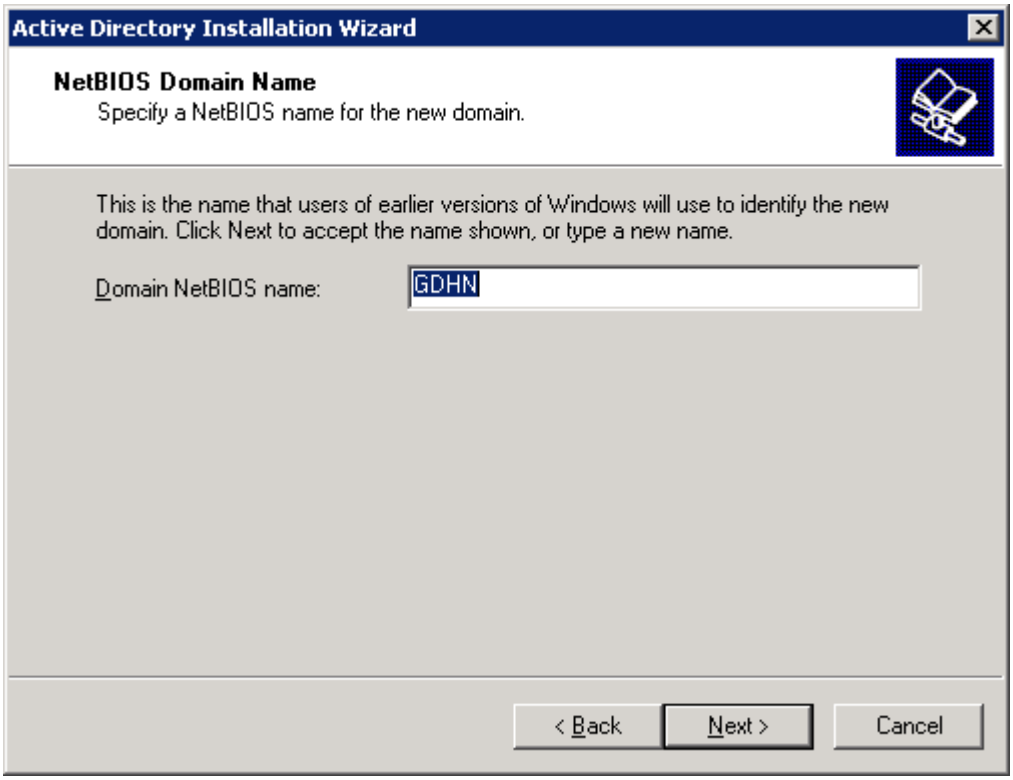
É possível também adicionar novos domínios (que façam parte da mesma organização), que entram na analogia como novas árvores. Ao cadastrá-los, você usaria a terceira opção (Domain tree in an existing forest), que faz com que a nova árvore (o novo domínio) seja adicionado à árvore (ou seja, ao domínio) já existente, formando uma floresta.

As florestas são compostas por diversos domínios (e, consequentemente, por diversos servidores) que formam um único diretório. Você pode imaginar um grande volume de servidores, espalhados por diferentes cidades de um país, ou mesmo por países diferentes, que mantém uma base de dados comum (replicada de forma automática) e podem ser administrados de forma centralizada. A grande bandeira do Active Directory é justamente o fato de oferecer os recursos que permitem a criação dessa estrutura.

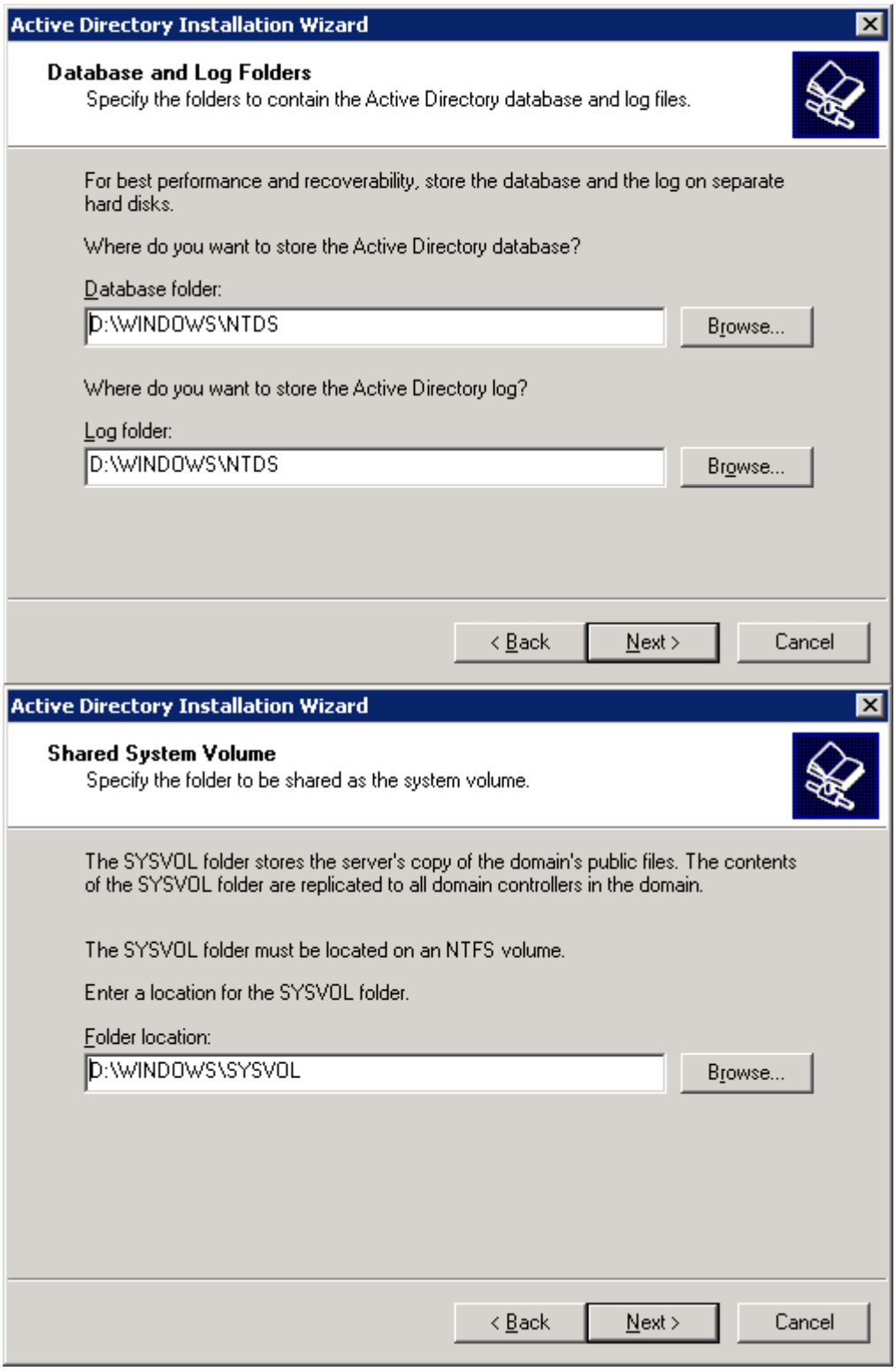
Continuando, temos a pergunta seguinte (New Domain Name) onde você deve indicar o domínio que está sendo criado, como "gdhn.com.br":



O "Domain NetBIOS name" é um nome alternativo para o servidor, que será fornecido aos clientes com versões antigas do Windows (95/98/ME/SE ou NT), que ainda utilizam o WINS ou pacotes de broadcast para localizar as máquinas na rede. O nome NetBIOS pode conter até 15 caracteres, incluindo letras e números, mas é fortemente recomendado que você não utilize pontos, para que ele não seja confundido com o nome de domínio. Uma boa opção é simplesmente usar a parte principal do domínio como nome NetBIOS, como em "GDHN".



Em seguida você tem a opção de definir onde serão armazenadas as bases de dados do servidor e os logs. Por default são sugeridas pastas dentro do diretório \Windows, mas em um servidor de produção é recomendável reserver um HD separado apenas para isso. Isso facilita a recuperação dos dados e a migração para outro servidor em caso de pane e também melhora o desempenho de acesso aos arquivos, já que eles não precisarão compartilhar os ciclos de leitura do HD com os demais arquivos, bibliotecas e aplicativos do sistema:

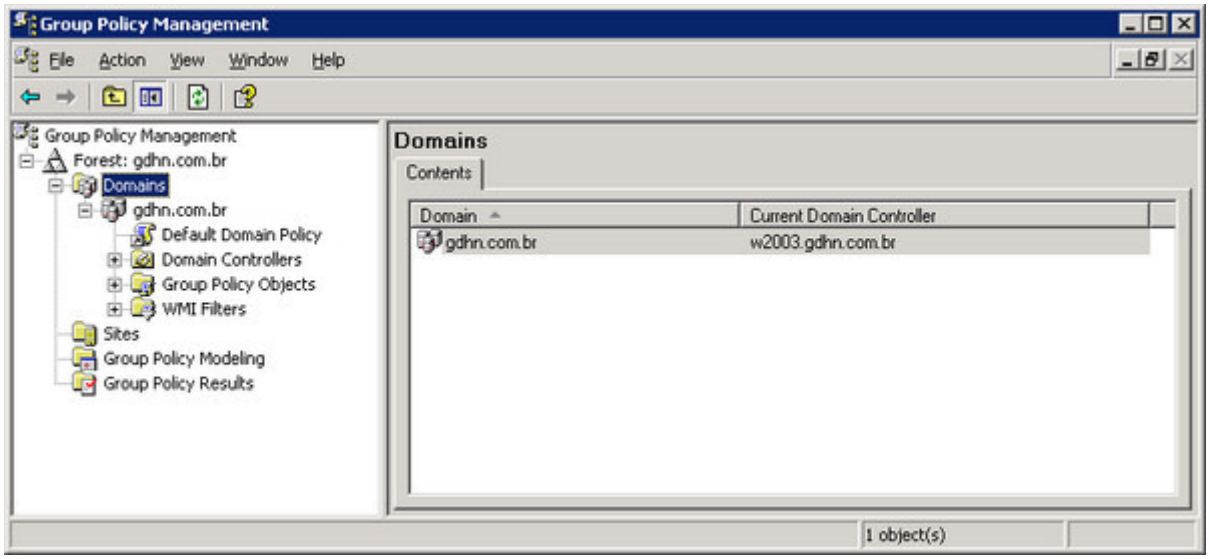


A pergunta seguinte é sobre a localização do SYSVOL, que armazena arquivos que ficarão acessíveis a todas as máquinas que fazem parte do domínio. Além de permitir disponibilizar atualizações de segurança, drivers, patches e outros arquivos que precisam ser instalados em diversas máquinas da rede (que seria a aplicação mais óbvia), ele armazena também os arquivos com as políticas de grupo, e os scripts de logon, que são executados pelas estações quando o usuário faz logon. Isso faz com que o SYSVOL também seja um componente importante.

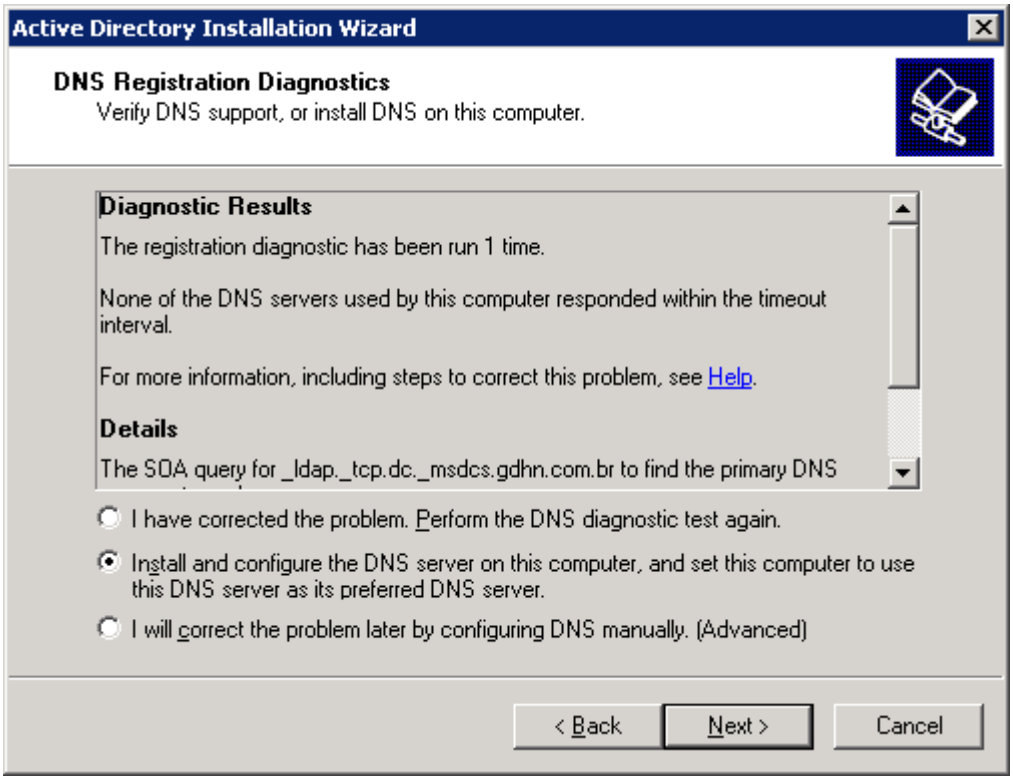
As políticas de grupo (group policies) permitem limitar o ambiente dos usuários, bloqueando o uso do task manager, restringindo os aplicativos disponíveis, bloqueando alterações no ambiente de trabalho, bloqueando a instalação de programas e assim por diante. A idéia é restringir as opções e as alterações que podem ser feitas pelos usuários, reduzindo assim o volume de trabalho das equipes de manutenção e de suporte.

Para criar políticas de grupo para o domínio, é preciso instalar o GPMC (Group Policy Management Console), disponível no http://www.microsoft.com/windowsserver2003/gpmc/.

Depois de instalado, você pode abrir o editor através do "Administrative Tools > Group Policy Management" ou chamando o "gpmc.msc" através do "Start > Run".



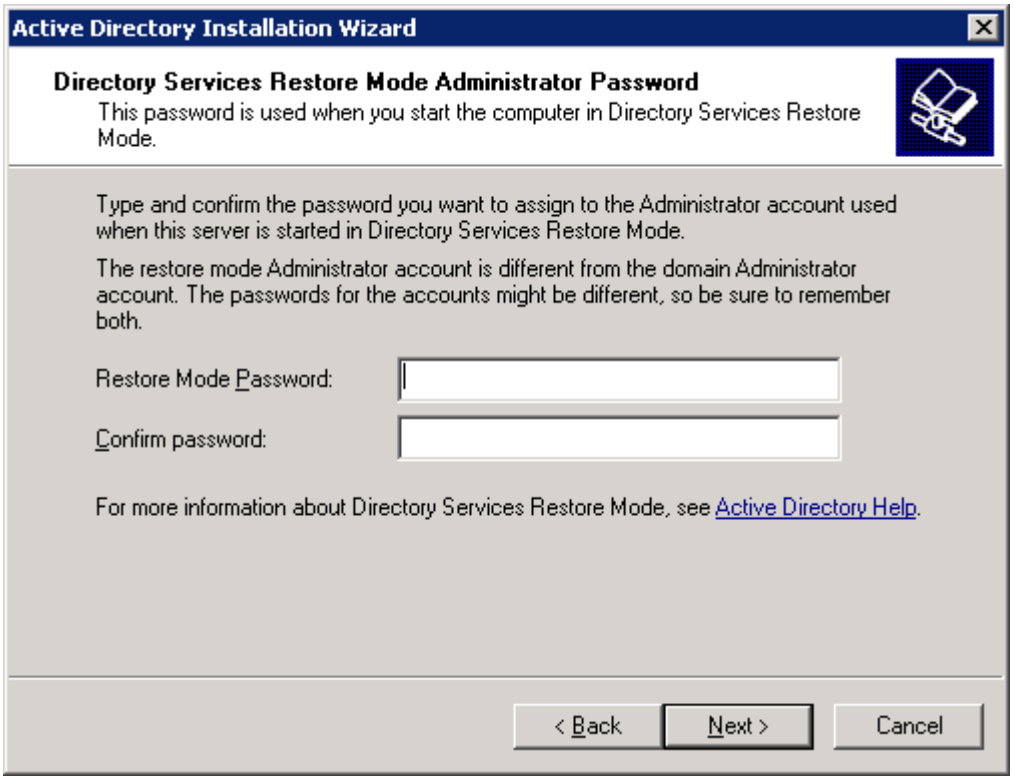
Continuando, se houver qualquer problema com a configuração do servidor DNS, que impeça seu uso em conjunto com o Active Directory, o assistente exibe o menu abaixo, onde você tem a opção corrigir o problema manualmente e executar o teste novamente, deixar que o assistente corrija o problema automaticamente ou concluir a configuração e deixar para solucionar o problema manualmente mais tarde:



Em configurações simples, ou seja, um único DNS local, respondendo por um único domínio, o wizard costuma fazer um bom trabalho na resolução do problema, por isso você pode arriscar usar a segunda opção sem medo, mas no caso de um servidor de produção seria recomendável estudar o problema com mais calma.

Como parte do processo, é solicitada que você defina uma senha de restauração para o Active Directory. Esta senha é solicitada ao acessar o Directory Restore Mode, um modo de recuperação que pode ser acessado ao pressionar a tecla F8 durante a inicialização do sistema (acesse a opção "Windows Advanced Options > Directory Services Restore Mode").

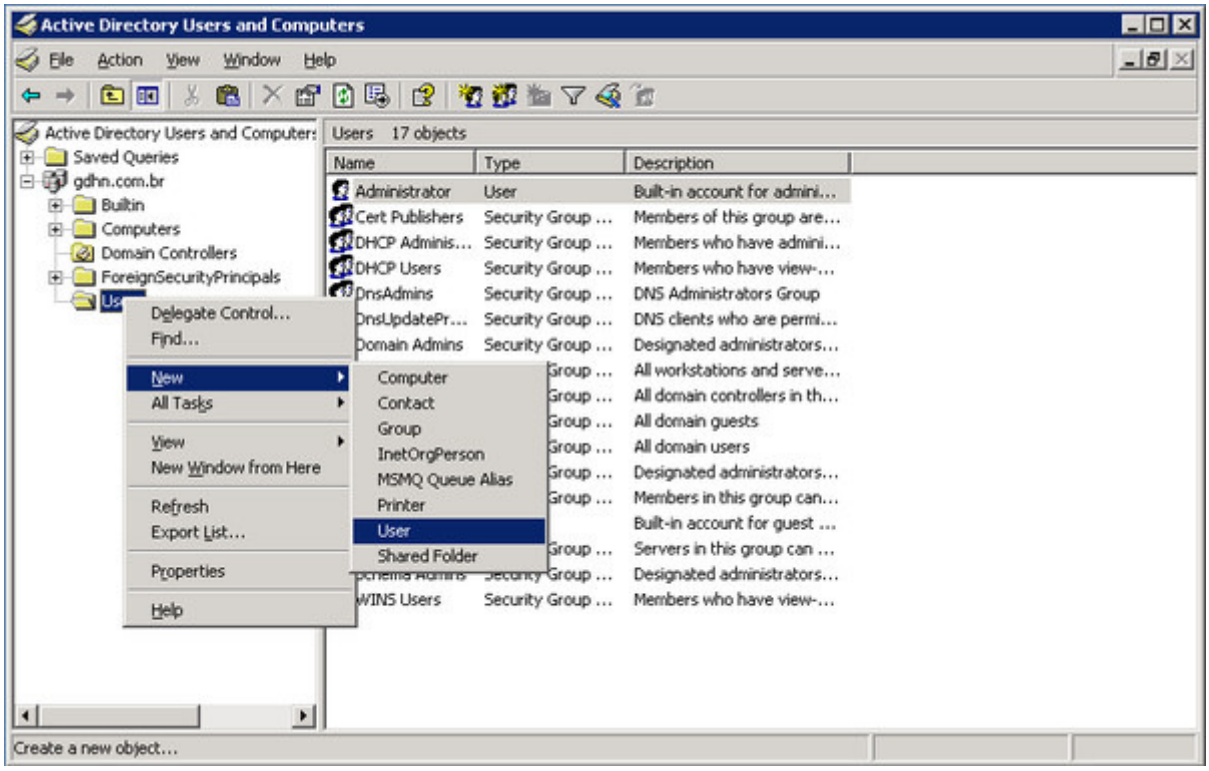
Através dele você pode executar diversas tarefas que não podem ser executadas enquanto o sistema está ativo, como transferir os arquivos do banco de dados para outro servidor ou realizar uma desfragmentação do BD em modo offline. Naturalmente, é essencial que seja escolhida uma boa senha.



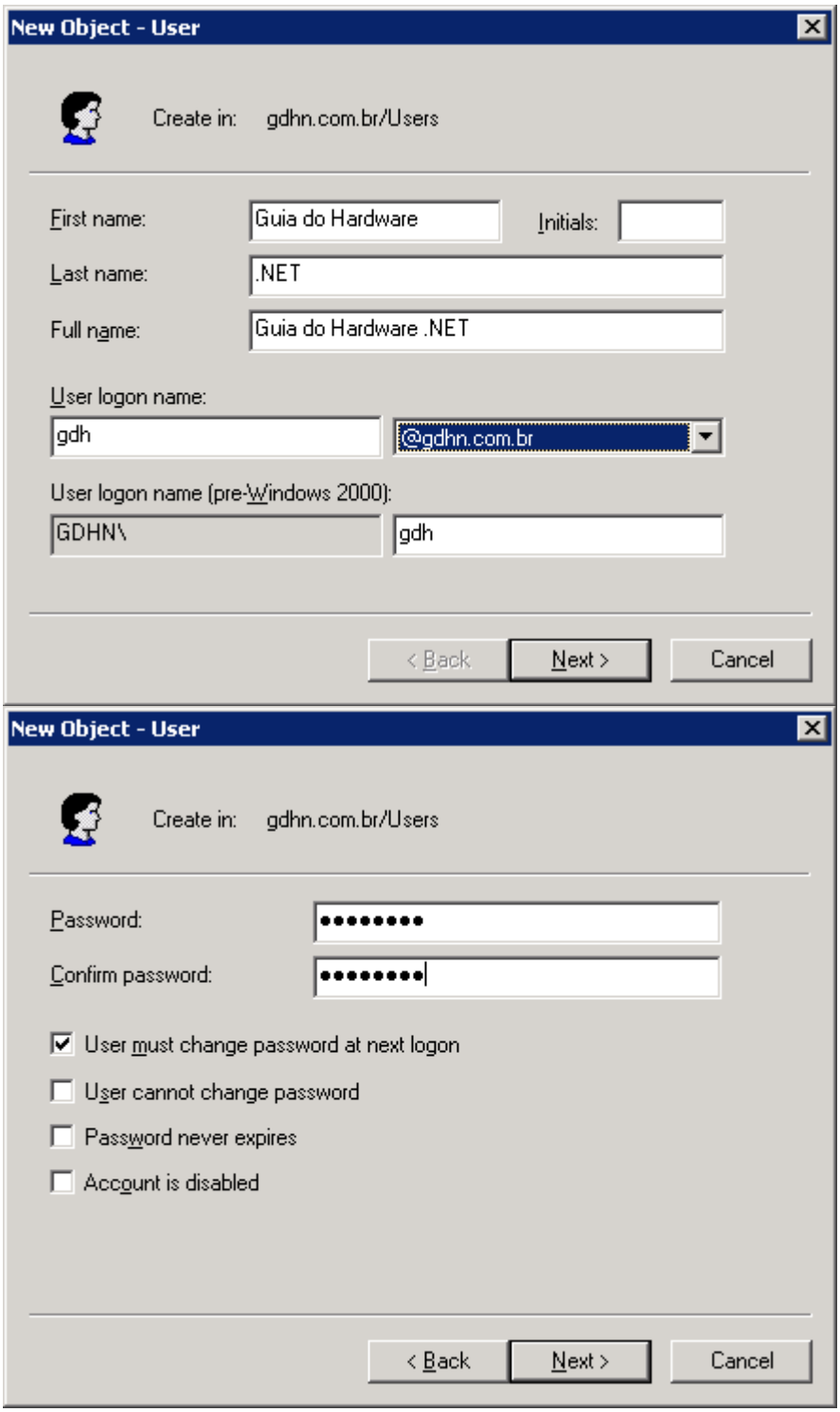
No final do processo é necessário reiniciar o servidor, para que todas as mudanças sejam aplicadas.

Depois de ativar o Active Directory, várias coisas mudam na administração do servidor, a começar pelo gerenciamento de usuários. A opção "Administrative Tools > Computer Management > System Tools > Local Users and Groups" desaparece e o "lusrmgr.msc" passa a exibir uma mensagem de erro quando aberto, avisando que não pode ser usado em um controlador de domínio.

Isso acontece por que ambas as ferramentas permitem administrar usuários locais e, ao ativar o Active Directory, deixamos de usar contas locais e passamos a usar contas cadastradas no diretório. A administração passa então a ser feita através do "Administrative Tools > Active Directory Users and Computers":



Dentro do utilitário, expanda a árvore do domínio (na coluna da esquerda), clique com o botão direito sobre a pasta "Users" e selecione a opção "New > User". Veja que o campo "User logon name" inclui o domínio do qual ele faz parte:

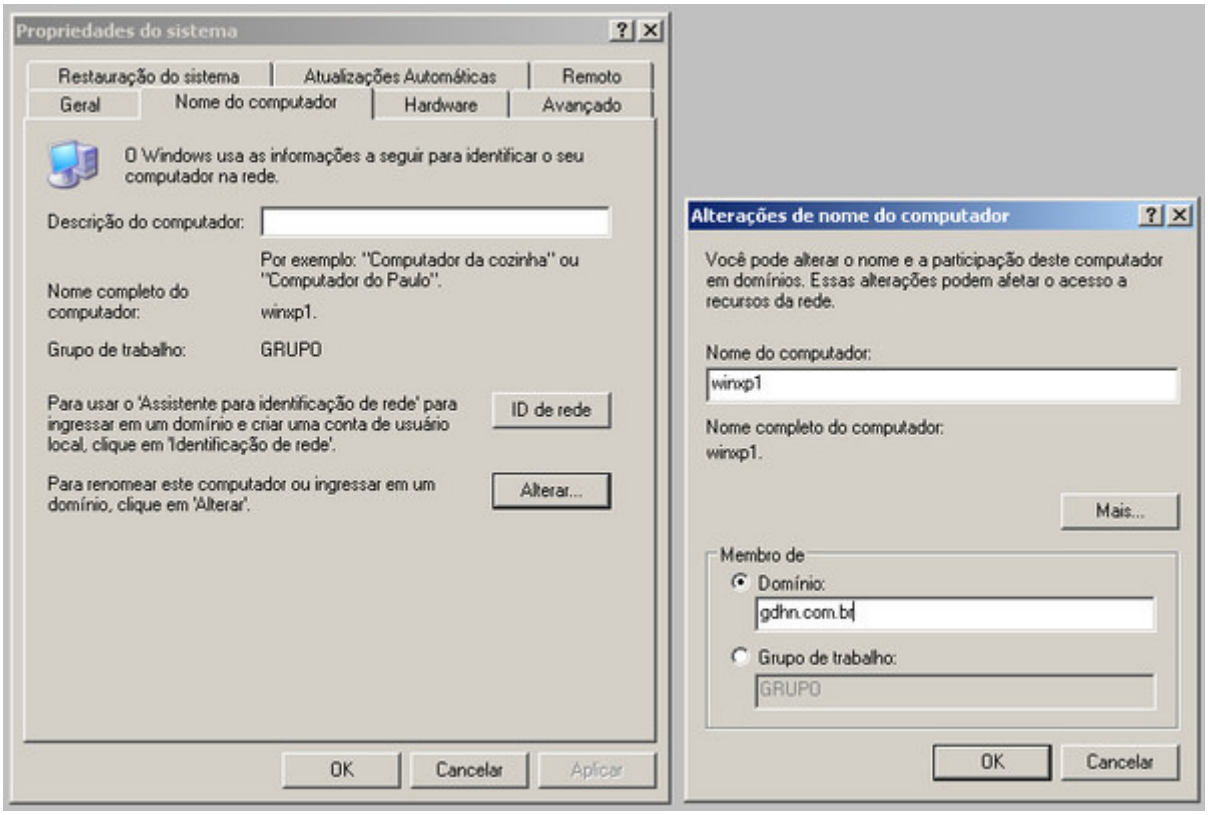


Esta mesma ferramenta é usada para criar grupos, criar compartilhamentos de rede e impressoras, entre outros recursos. Toda a configuração feita aqui é salva no diretório e é automaticamente replicada para os demais servidores, passando a valer para toda a rede.

Cadastrando as máquinas

O próximo passo é cadastrar as demais máquinas da rede no domínio, o que precisa ser feito manualmente em cada cliente, seja localmente ou seja usando a assistência remota.

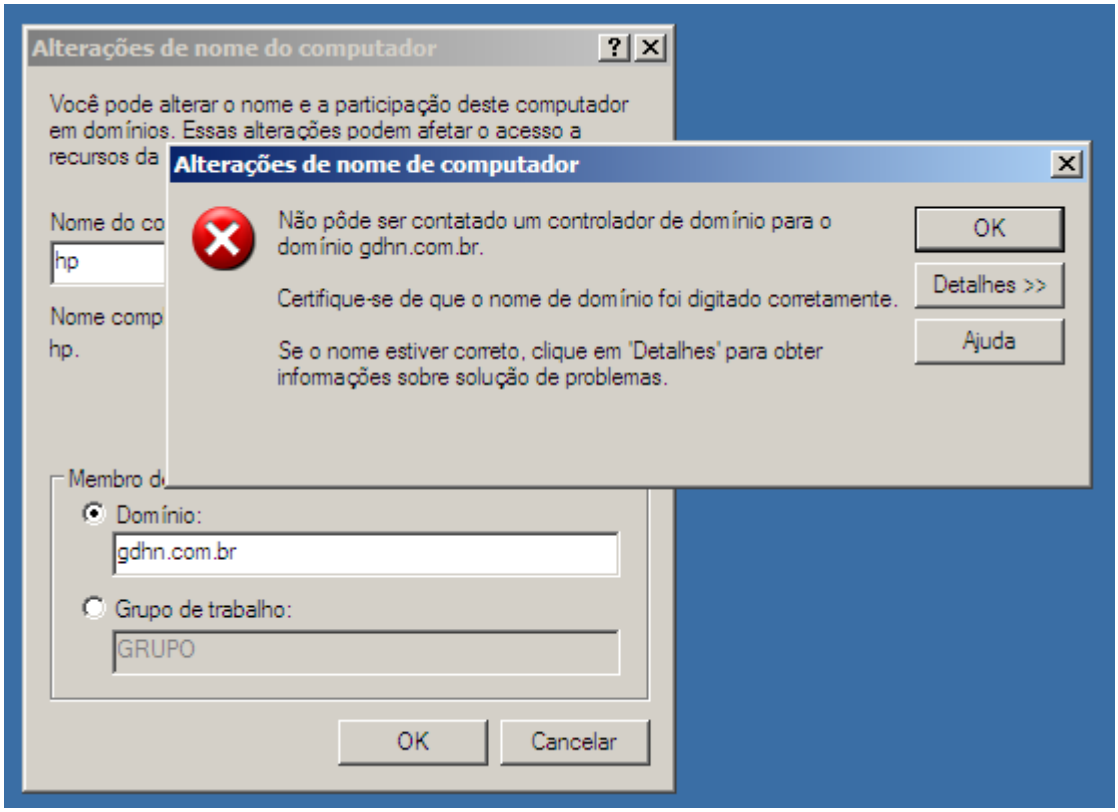
Nas estações com o Windows **XP Professional**, acesse o "Painel de Controle > Sistema > Nome do Computador" e use a opção "Alterar...". No menu seguinte, defina o nome da máquina e indique o domínio. Para ter acesso a esta opção você deve estar logado (na estação) como administrador:



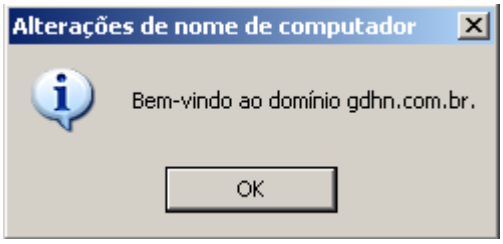
Na tela de identificação que será aberta a seguir, você deve efetuar um login no servidor usando o login "administrator", "administrador" ou outra conta administrativa, com permissão para ingressar máquinas no domínio.

Fornecer a senha da conta administrativa ao cadastrar o cliente no domínio, prova que quem está fazendo a operação é o administrador, ou alguém autorizado por ele. Se qualquer um pudesse adicionar e remover máquinas do domínio, ele não seria muito diferente de um grupo de trabalho e a configuração perderia todo o sentido.

Lembre-se de que para encontrarem o domínio, as estações devem ter sido configuradas para utilizarem o endereço IP do servidor DNS interno e não o DNS do provedor ou qualquer outro servidor externo. Sem isso, você receberá uma mensagem como a abaixo, avisando que a estação não conseguiu encontrar o servidor. Nesse caso, altere a configuração de rede da estação, adicionando o endereço IP do servidor como DNS primário e tente novamente.



Mesmo que toda a configuração esteja correta, é normal que a conexão inicial demore um ou até dois minutos. Se tudo der certo, você é saudado com uma mensagem de boas vindas:



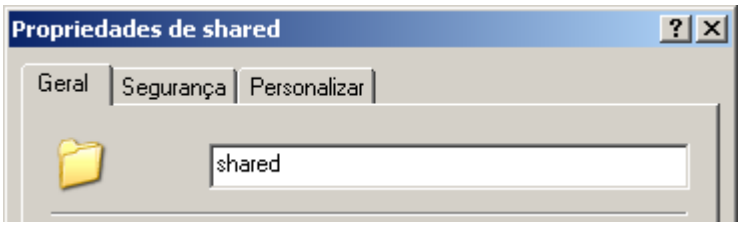
Quando a máquina passa a fazer parte do domínio, é criada uma "relação de confiança" entre ela e o servidor. Uma senha (chamada de "machine trust account password") é usada pela máquina para comprovar sua identidade ao contatar o servidor de domínio. Esta é uma senha interna, gerada automaticamente pelo sistema durante a conexão inicial.

Depois de reiniciar a estação, o default da tela de login passa a ser realizar o login no domínio em vez de na máquina local. Isso permite fazer logon usando qualquer uma das contas cadastradas no servidor. Continua disponível também a opção de fazer um login local, mas neste caso perde-se o acesso aos recursos relacionados ao domínio e é usado o perfil do usuário local:

Uma vez que a máquina é adicionada ao domínio, passa a existir uma distinção entre as contas locais (que são válidas quando é usada a opção de fazer logon na máquina local, na tela de logon) e as contas do domínio.

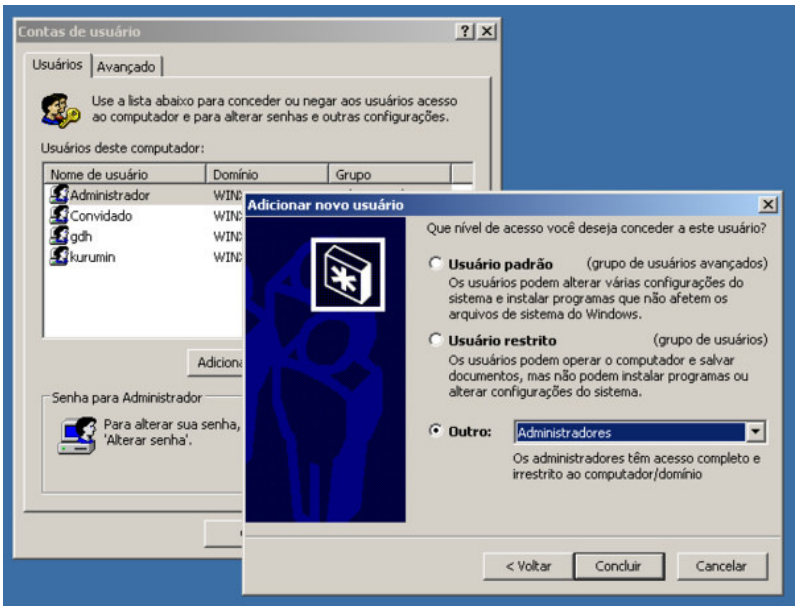
Quando o usuário se loga na estação, usando uma das contas cadastradas no servidor, ele é na verdade logado (na estação local) usando uma conta limitada, onde ele não tem permissão para compartilhar arquivos, para alterar as configurações da rede, nem para alterar a maior parte das configurações do sistema.

Em muitas situações, é exatamente isso que você quer, mas em outras isso pode ser um grande problema, já que o usuário não conseguirá compartilhar pastas com outros usuários da rede, por exemplo. Veja que a aba de compartilhamento sequer fica disponível nas propriedades da pasta:

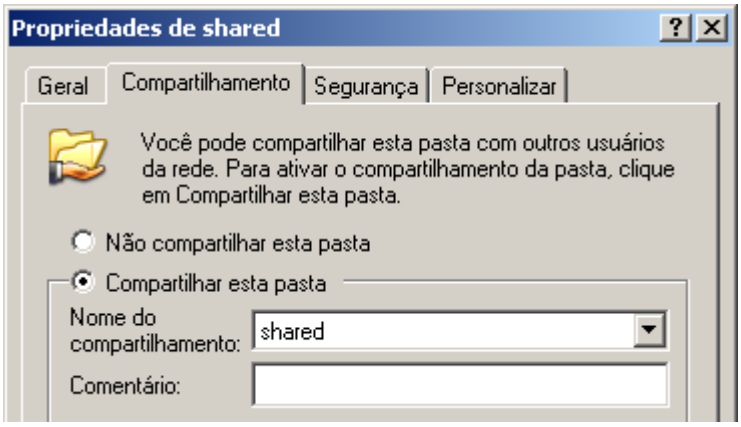


Para mudar isso, é necessário ajustar as permissões da máquina local, de forma que a conta do domínio tenha permissão para alterar as configurações. Para isso, logue-se localmente na estação Windows, usando uma conta (local) com privilégios administrativos:

Acesse o "Painel de controle > Contas de usuário" e clique no "Adicionar". Especifique o login do usuário e o nome do domínio e na tela seguinte especifique o nível de permissão na máquina local (Administrador, Usuário avançado, etc.). Você pode adicionar outros usuários se desejar:



Faça logoff (na estação) e logue-se novamente no domínio com a conta que foi cadastrada. Se você a cadastrou com privilégios administrativos, você notará que a aba de compartilhamento voltou a aparecer e o acesso às demais configurações foi destravado. Com isso o usuário assume o controle de sua máquina local e pode criar compartilhamentos e alterar as demais configurações:



Note que esta configuração é necessária apenas se você quiser que os usuários das estações possam criar compartilhamentos locais. Outra opção é simplesmente adicionar compartilhamentos no servidor e orientar os usuários a usarem os compartilhamentos criados para compartilharem os arquivos desejados. Centralizar todos os compartilhamentos no servidor é mais seguro e facilita bastante os backups, já que você precisará apenas em fazer backup dos arquivos do servidor.

Concluindo, para remover a máquina do domínio, é preciso acessar a mesma opção e mudar a opção de "Membro de Domínio:" para "Membro de Grupo de trabalho:". O sistema solicita novamente a senha do servidor, como uma forma de comprovar que o usuário está autorizado a realizar a operação. Isso evita que os usuários da rede desfaçam a configuração, removendo as máquinas do domínio.

No Windows **Vista**, a opção de adicionar a máquina ao domínio está no Painel de Controle > Sistema > Configurações avançadas do sistema (na lista à esquerda) > Nome do Computador > Alterar.

A forma como você escolhe se quer se logar ao domínio ou fazer um login na máquina local na tela de login do Vista segue uma lógica um pouco curiosa. Depois que a máquina é adicionada ao domínio, a tela de login mostra a opção de fazer logon no domínio, onde o último login utilizado fica pré-selecionado. Para usar outro login, é necessário clicar no botão "Trocar Usuário" e fornecê-lo na tela seguinte. Entretanto, não existe uma opção para fazer logon na máquina local. Para isso, é necessário especificar o nome da máquina seguido pelo nome do usuário no campo de login, como em: Vista\gdhn. Outra opção é usar um ".\" antes do nome do usuário, como em ".\gdhn".

No Windows **2000**, o procedimento é basicamente o mesmo do Windows XP, muda apenas a localização da opção, que está disponível no "Meu Computador > Propriedades > Identificação de rede > Propriedades".

Nem todas as versões do Windows suportam o uso de um domínio. Como controladores de domínio são usados principalmente em redes de médio ou grande porte em empresas, a Microsoft não inclui suporte no Windows XP Home e no XP Starter, assim como no Vista Starter, Vista Home Basic e Vista Home Premium, de forma a pressionar as empresas a comprarem as versões mais caras.

Administrando Contas de Usuários
Contas de usuários precisam ser criadas para dar a estes a capacidade de logar-se em um domínio para acessar recursos da rede ou logar-se em um computador para acessar recursos locais.
Uma conta de usuário contém as credenciais exclusivas e é um registro que define este usuário para o Windows 2000. Deve incluir o nome e a senha (se requerida), os grupos do qual o usuário é
membro e os direitos e permissões que o usuário possui para uso do computador e da rede e para

acesso à recursos. Cada pessoa que utiliza regularmente a rede deve ter uma conta de usuário.
O Windows 2000 suporta dois tipos de contas de usuários: do domínio e local. Com uma conta de usuário do domínio, um usuário pode logar-se em um domínio para ganhar acesso à
recursos da rede. Com uma conta de usuário local, um usuário pode logar-se em um computador
específico para ganhar acesso aos recursos daquele computador.
Além destes dois tipos, o Windows 2000 também provê contas de usuário internas (*buit-in user accounts*), que são usadas para desempenhar tarefas administrativas ou ganhar acesso à
recursos da rede. As contas de usuário internas são criadas automaticamente durante a instalação do Windows 2000 e a instalação do Active Directory.

Planejando Novas Contas de Usuários
Para tornar mais eficiente o processo de gerenciamento das contas de usuários é importante adotar e seguir determinadas convenções e diretrizes através do planejamento das seguintes áreas:

- Convenções de nomes para as contas de usuário;
- Diretrizes para as senhas;
- Opções de conta.

Convenções para Nomes de Contas de Usuário
A convenção de nomes estabelece como as contas de usuário são identificadas no domínio (ou no computador local). Uma convenção de nomes consistente facilita lembrar nomes de *logon* de usuários e localizá-los em listas. Os seguintes aspectos devem ser considerados na determinação de uma convenção de nomes para uma organização:

Os nomes de *logon* para contas de usuário devem ser exclusivos no Active Directory. Os nomes completos de contas de usuário de domínio devem ser exclusivos na OU onde a conta de usuário foi criada. Os nomes de contas de usuário local devem ser exclusivos no computador em que foram criadas.

Os nomes de *logon* de usuário podem conter até 20 caracteres maiúsculos ou minúsculos (não existe diferenciação, mas o Windows 2000 preservará a forma como for digitado). Apesar do campo aceitar mais de vinte caracteres, o Windows 2000 só reconhecerá os primeiros vinte. Os caracteres não permitidos são: " / \ [ ] : ; | = , + * ? < > Se existir um grande número de usuários, a convenção de nomes deve considerar os funcionários com nome igual, utilizando tratamentos como:

- Usar concatenações de nome e sobrenome de forma diferenciada. Por exemplo, se existirem dois Pedro Silva, utilizar PedroSil e PedroSilva.
- Usar números após o nome, como por exemplo Pedro1 e Pedro2.

Em algumas organizações pode ser útil identificar determinados tipos de usuários pela sua conta. Para usuários temporários, por exemplo, pode-se acrescentar a letra T e um hífen no início do nome da conta de usuário: T-Pedro.

Diretrizes para as Senhas
Para proteger o acesso ao domínio ou a um computador, todas as contas de usuário devem ter uma senha associada. Estas são as recomendações para o uso de senhas:

- Atribuir sempre uma senha para a conta Administrator para impedir o acesso não autorizado à conta. Na verdade, é recomendável a alteração do nome da conta Administrator. Uma vez que para obter acesso ao domínio é necessário um nome de conta e uma senha, um invasor já terá metade do que precisa se a conta Administrator permanecer com seu nome padrão.
- Determinar se o administrador da rede ou os usuários controlarão as senhas. É possível atribuir senhas exclusivas para as contas de usuário e impedir que os usuários as alterem, ou então pode-se permitir que os próprios usuários definam suas senhas no primeiro logon.
- Orientar os usuários para o uso de senhas complexas bem como manter o sigilo sobre sua senha. Algumas recomendações:
- Evitar senhas com associação óbvia, como o próprio nome, sobrenome ou nome de alguém da família.
- Usar senhas longas. As senhas no Windows 2000 podem ter até 128 caracteres, mas ecomenda-se o tamanho mínimo de 8 caracteres.

- Usar combinações de letras maiúsculas e minúsculas e caracteres não-alfanuméricos permitidos. Os mesmos caracteres não permitidos para nomes de conta também não são permitidos nas senhas.

Opções de Conta

As opções de conta de usuário controlam a maneira como um usuário acessa o domínio ou um computador. É possível, por exemplo, limitar as horas durante as quais um usuário pode efetuar
logon no domínio e os computadores nos quais ele pode efetuar logon. Também pode-se especificar a data de expiração de uma conta de usuário.

Horas de Logon

É possível definir as horas de logon para os usuários que só precisam de acesso em horários específicos. Esta configuração está disponível nas propriedades de cada usuário, através do botão
'Logon Hours' na guia 'Account'.

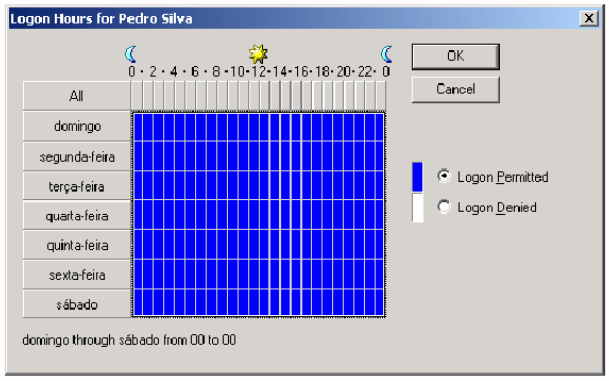


Figura 22 – Definição dos horários nos quais o usuário pode logar-se

Computadores Permitidos para Logon3

Por padrão, os usuários podem efetuar logon em qualquer computador do domínio, mas é possível especificar os computadores nos quais os usuários podem efetuar logon. Isso ajuda a restringir o acesso a informações armazenadas localmente nos computadores do domínio. Esta configuração também está disponível nas propriedades de cada usuário, através do botão 'Log On To' na guia 'Accounts'.

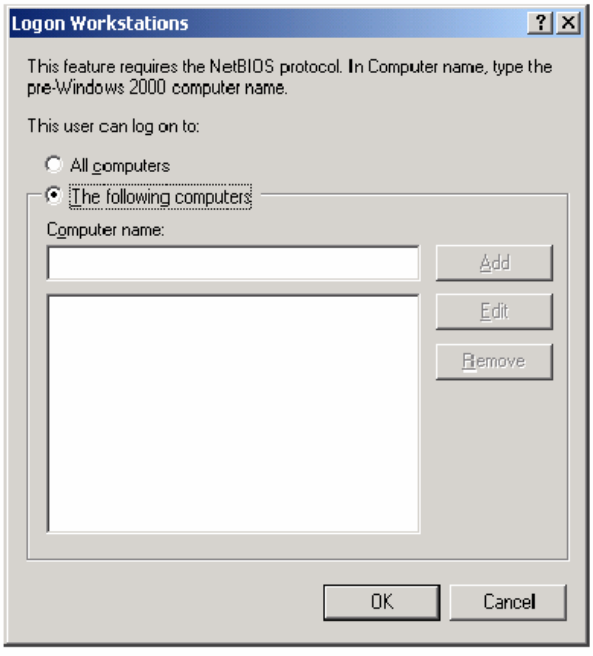


Figura 23 – Definição de Computadores para Logon

Expiração de Conta
A definição de uma data para expiração de uma conta é um recurso bastante útil, principalmente para utilização em contas de usuários temporários. Com esta configuração, uma data de expiração para a conta é definida e, a partir desta data, o usuário não obtém mais acesso à rede.
Este recurso está acessível na guia 'Account' das propriedades de cada usuário.

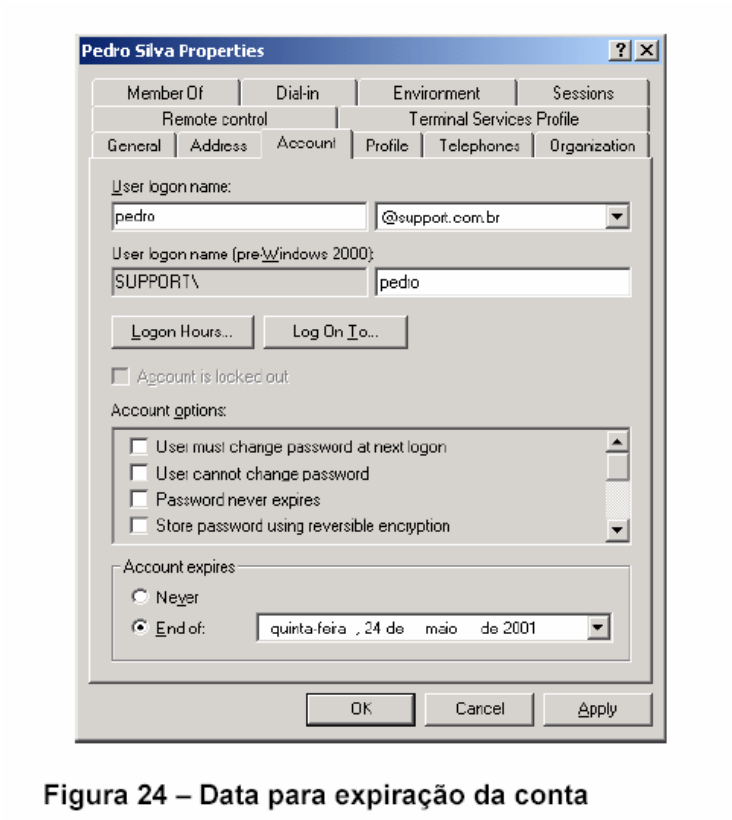


Figura 24 – Data para expiração da conta

Contas de Usuário Local
Uma conta de usuário local é uma conta que só existe em um determinado computador (Windows 2000 Professional ou Windows 2000 Server Stand Alone ou Member). Este tipo de conta só deve ser usada em ambientes de redes menores, como grupos de trabalho ou em computadores autônomos que não estão conectados em uma rede. Não é recomendável a criação de contas locais em computadores que façam parte de um domínio, pois o domínio não as reconhece e, como resultado, elas só conseguiriam obter acesso aos recursos do computador no qual foram criadas.
As contas de usuário local residem no banco de dados SAM, que é o banco de contas de segurança local. Elas não são armazenadas no Active Directory do domínio. Além disso, as contas de usuário local possuem um menor número de propriedades que as contas de domínio.

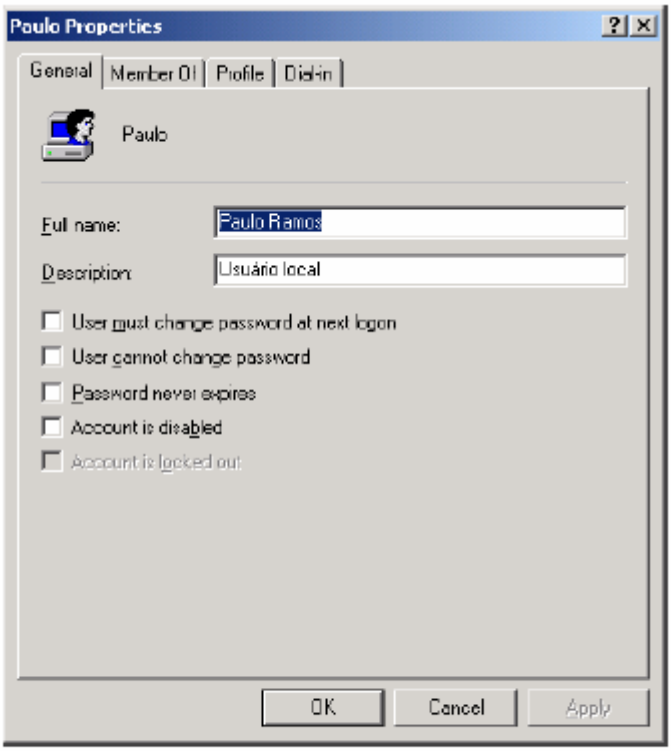


Figura 25 – Propriedades do usuário local

Para criação de contas locais deve ser utilizado no 'Computer Management', o snap-in 'Local Users and Groups'. Com o botão direito na pasta Users, clica-se em New User e a seguinte tela será exibida.

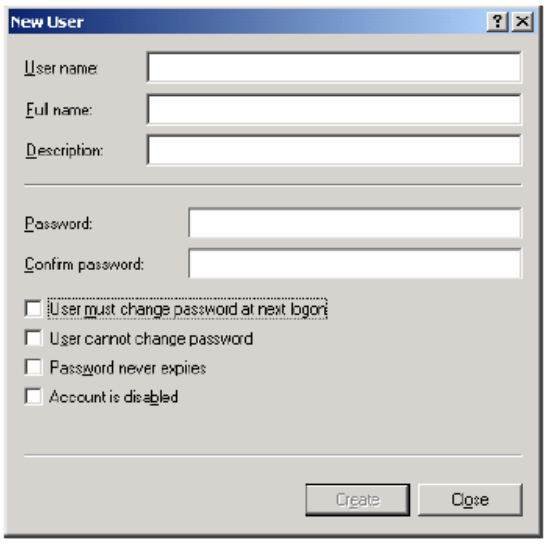


Figura 26 – Novo usuário local

Importante destacar que em um servidor Windows 2000 que seja controlador de domínio, este snap-in não estará disponível. Neste caso, devem ser criadas contas do domínio usando a ferramenta Active Directory Users and Computers, conforme será descrito posteriormente.

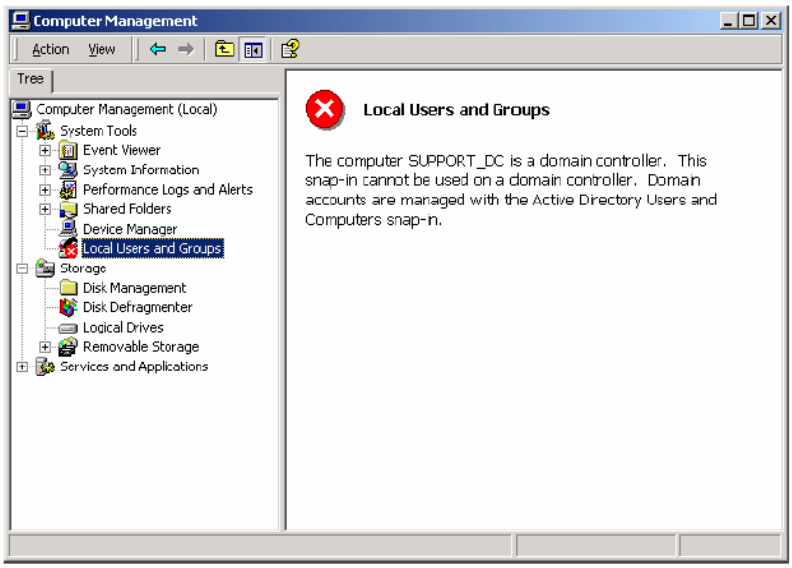


Figura 27 – Snap-in Local Users and Groups não disponível em um controlador de domínio

Contas de Usuário do Domínio

Para criar contas de usuários do domínio é preciso utilizar o snap-in Active Directory Users and Computers. Este snap-in sempre estará disponível em um controlador de domínio. Já um servidor membro não terá este snap-in, a menos que sejam instaladas as Ferramentas Administrativas do Windows 2000.

Para instalar estas ferramentas, basta executar o pacote de instalação Adminpak.msi encontrado na pasta I386 do CD de instalação do Windows 2000 Server. Ao executar este pacote, a seguinte tela é exibida:

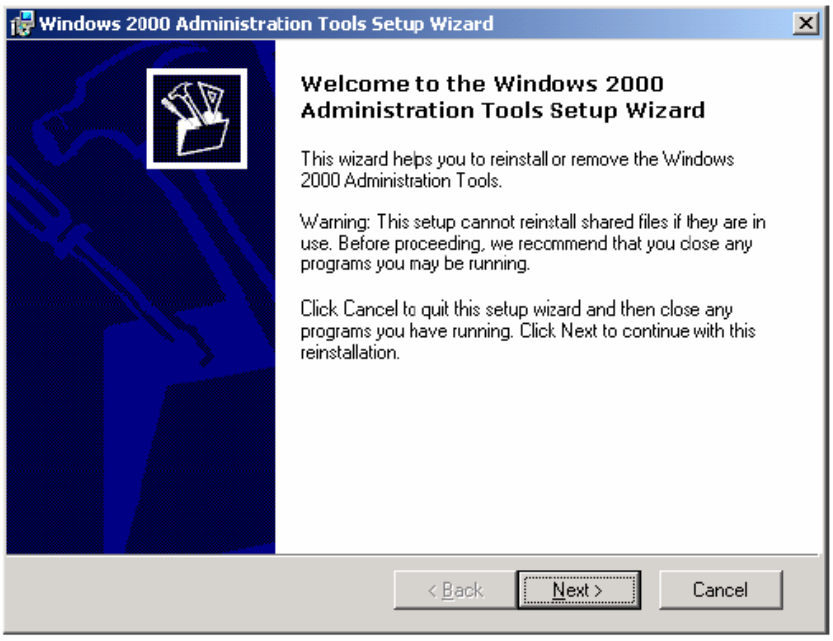


Figura 28 – Wizard para instalação das Ferramentas Administrativas

Prosseguindo com a instalação, pode-se optar pela instalação ou desinstalação das Ferramentas Administrativas.

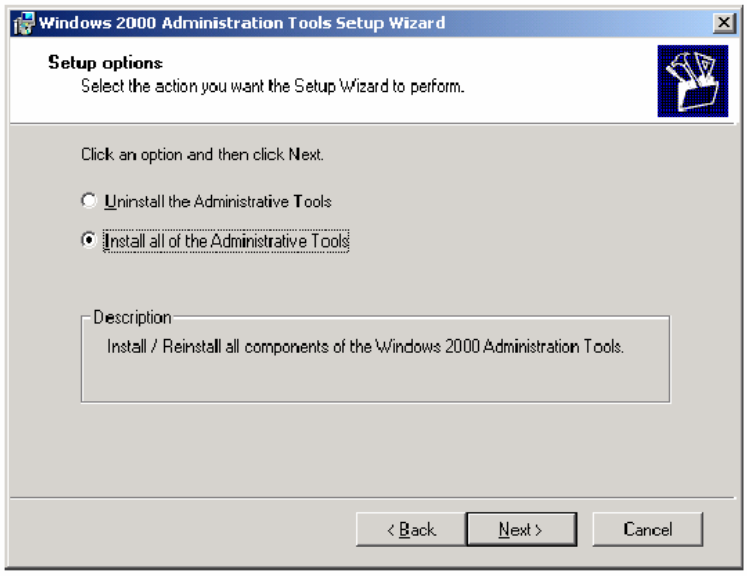


Figura 29 – Opções de instalação das Ferramentas Administrativas

O programa passa então a instalar os componentes das Ferramentas Administrativas.

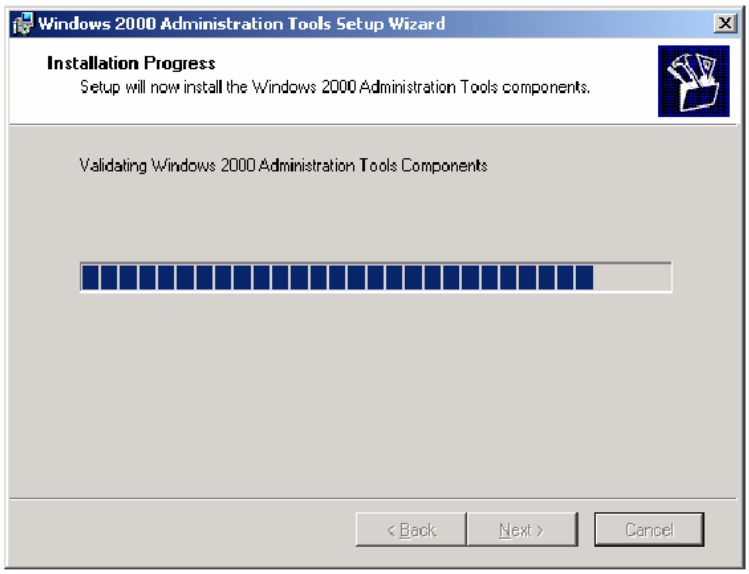


Figura 30 – Instalação dos componentes

Uma vez concluída a instalação estarão disponíveis em um servidor membro (não controlador
de domínio) as Ferramentas Administrativas do Windows 2000 e um usuário com uma conta que faça parte do grupo Domain Administrators poderá executar atividades administrativas (como a criação de usuários do domínio) neste servidor membro.
O snap-in Active Directory Users and Computers permite a criação de contas de usuários do domínio.

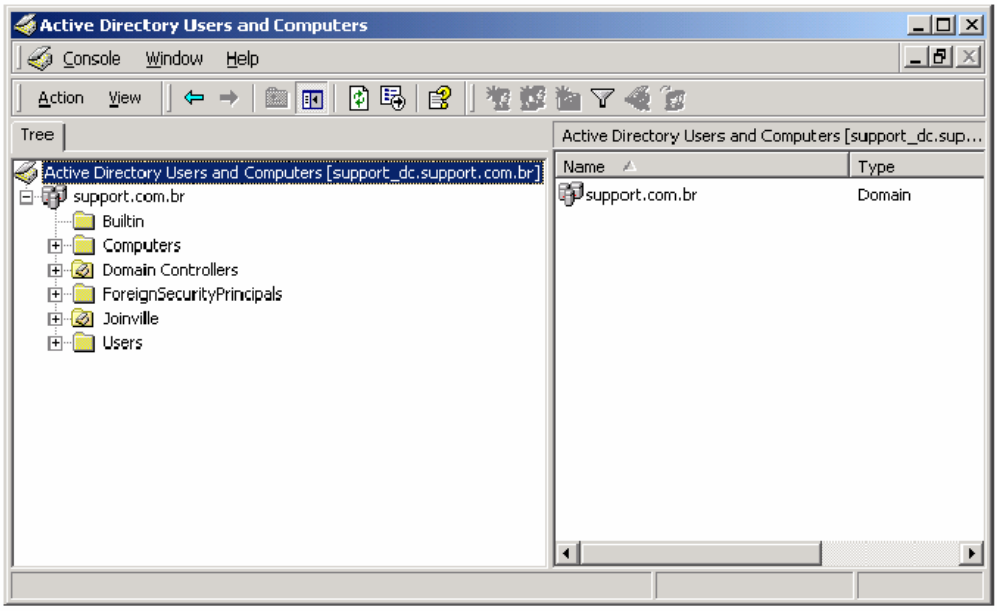


Figura 32 – Snap-in Active Directory Users and Computers

Basta selecionar a Unidade Organizacional na qual deseja-se criar um novo usuário ou mesmo usar a Unidade Organizacional padrão Users, e no menu Action selecionar New e escolher
User. A seguinte caixa de diálogo será exibida:

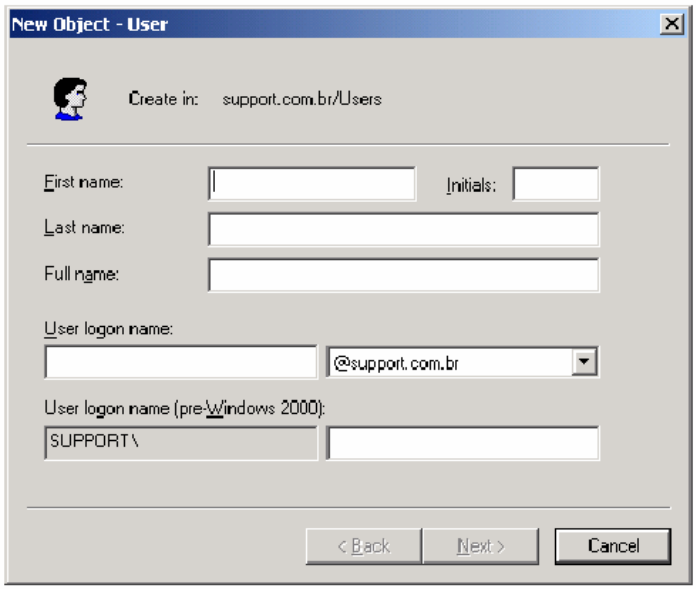


Figura 33 – Caixa para criação de uma nova conta de usuário do domínio

A tabela a seguir descreve as informações que deverão ser preenchidas nesta caixa de diálogo.

Opção	Descrição
First name	O primeiro nome do usuário. Este ou o último nome são requeridos
Last name	O último nome do usuário. Este ou o primeiro nome são requeridos
Full name	O nome completo do usuário e é preenchido automaticamente de acordo com as informações digitadas nas caixas anteriores
User logon name	O nome exclusivo de logon do usuário, baseado na convenção de nomes adotada. Esta informação é requerida e precisa ser única no domínio
User logon name (pre-Windows 2000)	O nome exclusivo de logon do usuário para clientes com sistemas operacionais anteriores ao Windows 2000, como Windows NT 4.0 ou 3.51. Esta informação é requerida e precisa ser única no domínio

Na tela seguinte deverá ser informada uma senha e deverão ser feitas algumas opções.

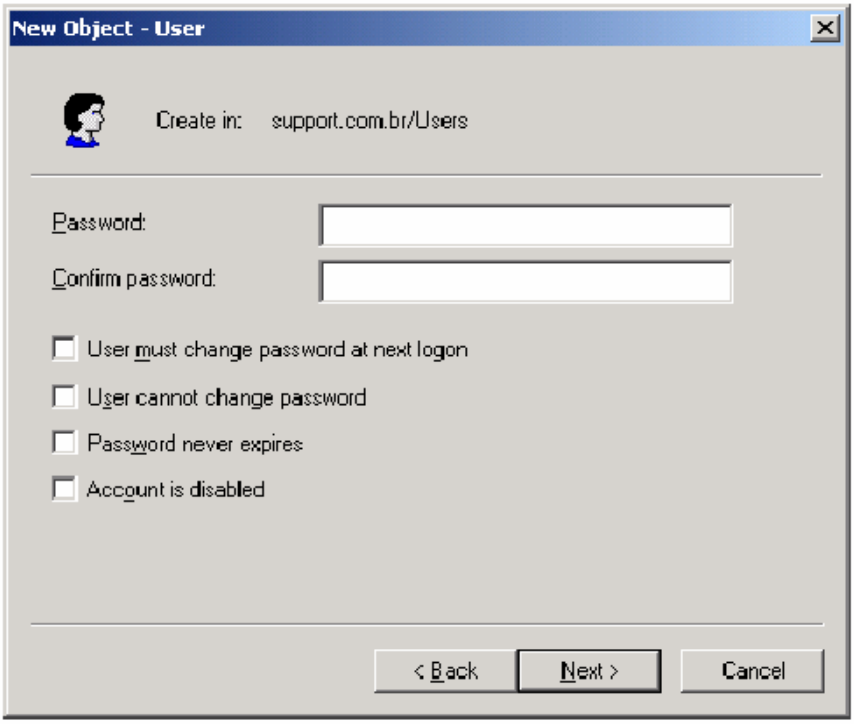


Figura 34 – Informações complementares para uma nova conta

Opção	Descrição
Password	A senha que será usada pelo usuário
Confirm password	Confirmação da senha definida na caixa anterior, para assegurar que não ocorreram erros de digitação
User must change password at next logon	Selecionar esta caixa obrigará ao usuário efetuar a troca da senha definida na caixa Password na primeira vez que efetuar logon. Esta opção assegura a privacidade da senha do usuário, de tal forma que nem o administrator a conhecerá
User cannot change password	Selecionar esta senha impedirá que o usuário proceda a troca de sua senha. Esta opção é útil quando mais de uma pessoa estiver usando a mesma conta
Password never expires	Selecionar esta caixa fará com que a senha do usuário nunca expire, mesmo que estejam definidas diretivas que definam expirações de senhas em determinados períodos. Esta opção é útil em contas de determinados programas ou serviços
Account is disabled	Selecionar esta opção fará com que a conta não esteja disponível para uso. Esta opção é útil quando um usuário irá afastar-se por um período ou quando um novo funcionário ainda não iniciou suas atividades

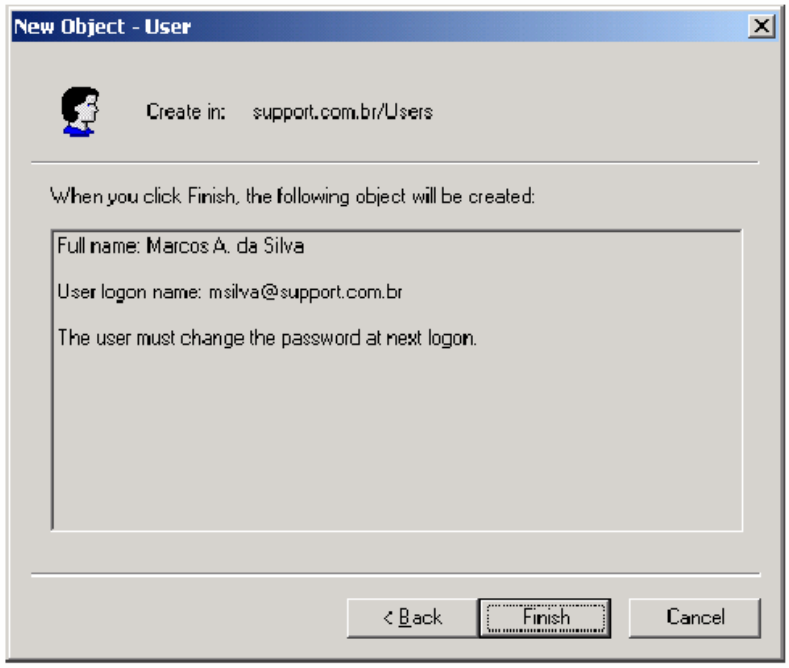


Figura 35 – Finalização da criação de uma nova conta

Propriedades para Contas de Usuários do Domínio

Um conjunto de propriedades padrão está associado a cada conta de usuário criada no domínio. Estas propriedades podem ser usadas para localizar usuários no Active Directory e, por esta razão, estas informações devem ser preenchidas para cada conta de usuário.

As propriedades da conta de usuário são acessadas no snap-in Active Directory Users and Computers, clicando com o botão direito no usuário desejado e escolhendo o comando Properties.

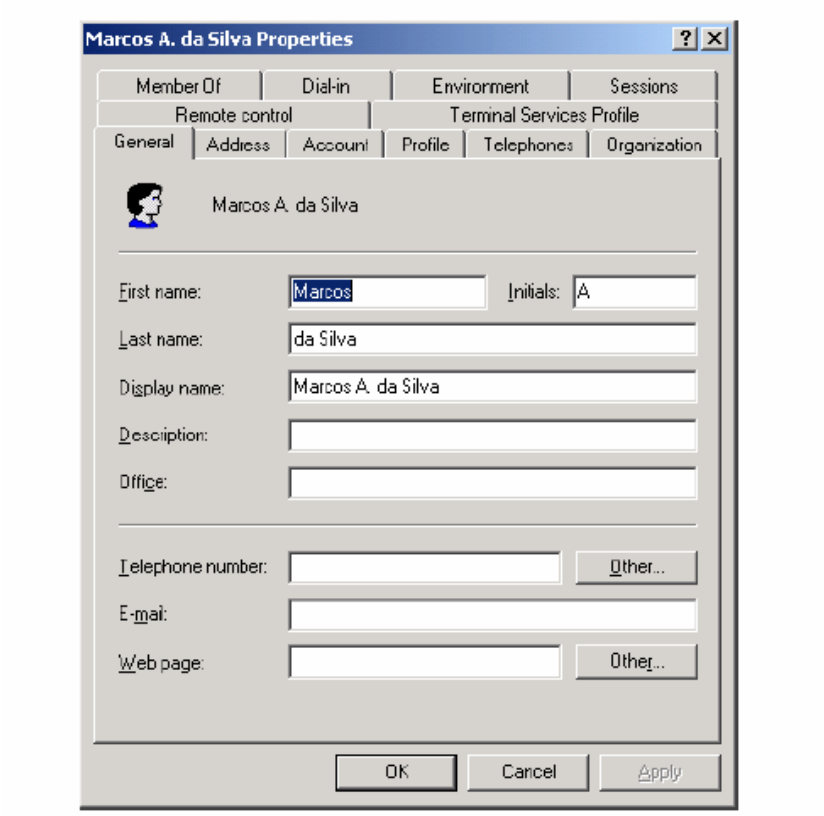


Figura 36 – Caixa de propriedades da conta de usuário

A tabela a seguir descreve as guias da caixa de diálogo Properties referente ao usuário.

Guia	Finalidade
General	Documenta o nome, a descrição, o local do escritório, o número de telefone, o alias de e-mail e as informações sobre a página inicial referentes ao usuário
Address	Documenta o endereço do usuário, caixa postal, cidade, estado ou município, CEP e país
Account	Atribui o nome de logon do usuário, define opções de conta e especifica a expiração de contas
Profile	Atribui o caminho do perfil e a pasta base do usuário
Telephones	Documenta o endereço, pager, celular, fax e números de telefone IP e permite digitar observações que contêm informações descritivas sobre o usuário
Organization	Documenta o cargo, o departamento, o gerente da empresa e os relatórios diretos do usuário
Member of	Especifica os grupos aos quais o usuário pertence
Dial-in	Define as permissões de acesso, as opções de retorno de chamada e as rotas e endereços IP estáticos
Environment	Especifica um ou mais aplicativos a serem iniciados e os dispositivos aos quais conectar durante o logon do usuário
Sessions	Especifica configurações do Terminal Services
Remote control	Especifica configurações de controle remoto do Terminal Services
Terminal Services Profile	Define o perfil do usuário no Terminal Services

Cópia de Contas de Usuário do Domínio5

Para simplificar o processo de criação de novas contas de usuário de domínio é possível efetuar uma cópia de uma conta já existente. Com a cópia, uma série de propriedades da conta são copiadas para o novo usuário, evitando a necessidade de digitação de dados repetidos.

As propriedades de usuário copiadas da conta de usuário de domínio existente para a nova

conta são descritas a seguir:

Guia	Propriedades copiadas
General	Nenhuma
Address	Nenhuma
Account	Todas, exceto Logon Name
Profile	Todas, exceto as entradas Profile Path e Home Folder, que são alteradas para refletir o nome de logon do novo usuário
Telephones	Nenhuma
Organization	Todas, exceto Title
Member of	Todas
Dial-in	Nenhuma, as configurações padrão aplicam-se à nova conta
Environment	Nenhuma, as configurações padrão aplicam-se à nova conta
Sessions	Nenhuma, as configurações padrão aplicam-se à nova conta
Remote control	Nenhuma, as configurações padrão aplicam-se à nova conta
Terminal Services Profile	Nenhuma, as configurações padrão aplicam-se à nova conta

O recurso de cópia de contas permite o uso de modelo de conta de usuário, que nada mais é do que uma conta de usuário padrão criada para conter as propriedades que aplicam-se aos usuários com necessidades em comum.
Algumas recomendações importantes para o uso de modelos de conta são:

- Criar um modelo para cada categoria de funcionário ou para cada setor da empresa;
- Utilizar nomes nos modelos de conta que iniciem com caractere não-alfabético, como o caractere de sublinhado (_), já que desta forma os modelos sempre aparecerão juntos na parte superior da lista do painel de detalhes da janela do Active Directory Users and Computers;
- Marcar nos modelos de conta a caixa de seleção Account is disabled na guia Account para evitar que os modelos sejam utilizados para obter acesso à rede da empresa, lembrando sempre de desmarcar esta opção nas cópias geradas.

Gerenciamento de Grupos
Um grupo é uma coleção de contas de usuários usada para gerenciar o acesso de usuários a recursos como pastas, arquivos e impressoras compartilhados na rede. Grupos simplificam a administração permitindo associar permissões e direitos a grupos de usuários em vez de associar a cada usuário individualmente. Usuários podem ainda participar de vários grupos simultaneamente.

Grupos em um Domínio
As características dos grupos em um domínio são:
São criados somente em controladores de domínio;
Residem no serviço de diretório do Active Directory;
São usados para conceder permissões a recursos e direitos para tarefas do sistema em qualquer computador do domínio;
Os grupos em um domínio podem diferir quanto ao tipo a ao escopo.
Esta última característica merece um melhor detalhamento, uma vez que é importante conhecer as diferenças entre os tipos de grupos e os escopos de grupos.

Tipos de Grupos
Há dois tipos de grupo no Active Directory:
Grupos de segurança: usados para fins relacionados à segurança, como a concessão de permissões para acesso a recursos.
Grupos de distribuição6: usados pro aplicativos como listas para funções não relacionadas à segurança, como o envio de mensagens de e-mail para grupos de usuários. Não é possível conceder permissões a grupos de distribuição.

Escopos de Grupos
O escopo de um grupo determina onde usar esse grupo no domínio, ou seja, qual a sua abrangência. São três os escopos de grupos do Windows 2000: Globais, Locais e Universais.

Grupos Globais
Usados para organizar os usuários que compartilham requisitos semelhantes de acesso à rede. É possível utilizar um grupo global para conceder permissões de acesso a recursos localizados em qualquer domínio.

Têm participação limitada. Pode-se adicionar contas de usuário e grupos globais somente provenientes do domínio em que o grupo global foi criado.

Podem ser aninhados em outros grupos. Essa função permite adicionar um grupo global a outro no mesmo domínio ou a grupos de domínio local e universal de outros domínios.

Grupos Locais
Usados para conceder permissões a recursos de domínio localizados no mesmo domínio em que o grupo de domínio local foi criado. Os recursos não precisam residir em um controlador de domínio.

Têm participação aberta. Pode-se adicionar contas de usuário, grupos universais e globais de qualquer domínio.

Não podem ser aninhados em outros grupos, significando que não é possível adicionar um grupo de domínio local a nenhum grupo, nem aos localizados no mesmo domínio.

Grupos Universais
Concedem permissões a recursos relacionados em vários domínios. Devem ser usados para conceder permissões de acesso a recursos localizados em qualquer domínio.

Têm participação aberta. Todas as contas de usuário e grupos de domínio podem ser participantes.

Podem ser aninhados em outros grupos de domínio. Essa capacidade permite adicionar um grupo universal a grupos de domínio local ou universal em qualquer domínio.

Estratégias de Grupos
Uma estratégia bastante recomendada pela Microsoft para uso de grupos em um domínio único é conhecida como A G L P. Consiste em colocar as contas de usuário (A, de Account) em grupos globais (G), colocar os grupos globais em grupos de domínio local (L) e conceder permissões (P) ao grupo de domínio local. Um exemplo desta estratégia seria o seguinte:

Em uma empresa seria recomendável identificar os usuários com responsabilidades comuns e adicionar suas contas de usuário a um grupo global. Por exemplo, poderiam ser criados grupos globais para um departamento de vendas (Grupo Vendas), para os diretores (Grupo Diretoria) e para o departamento de marketing (Grupo Marketing).

Nesta mesma empresa existirá uma impressora laser colorida que poderá ser usada pelos diretores e pelos funcionários do marketing. Poderia então ser criado um grupo de domínio local chamado Usuarios Laser Colorida.

Os grupos globais Diretoria e Marketing seriam então incluídos no grupo de domínio local Usuarios Laser Colorida.

Por fim a impressora seria compartilhada e seriam concedidas as permissões adequadas para o grupo de domínio local Usuarios Laser Colorida.

Antes da criação de um novo grupo de domínio local é recomendável verificar se já não existe
um grupo de domínio local interno que atenda as necessidades. Por exemplo, se o administrador
precisa de um grupo para incluir as contas de usuários que executarão o backup diário, não será
necessário criar um novo grupo. Basta utilizar o grupo de domínio local interno Backup Operators.

Criação de Grupos de Domínio
Para criar-se grupos em um domínio utiliza-se o snap-in Active Directory Users And Computers. Os grupos podem ser criados na Unidade Organizacional Users ou em alguma outra Unidade Organizacional criada pelo administrador. Com o botão direito do mouse sobre a Unidade Organizacional desejada escolhe-se a opção New e o comando Group, surgindo então a seguinte
caixa de diálogo.

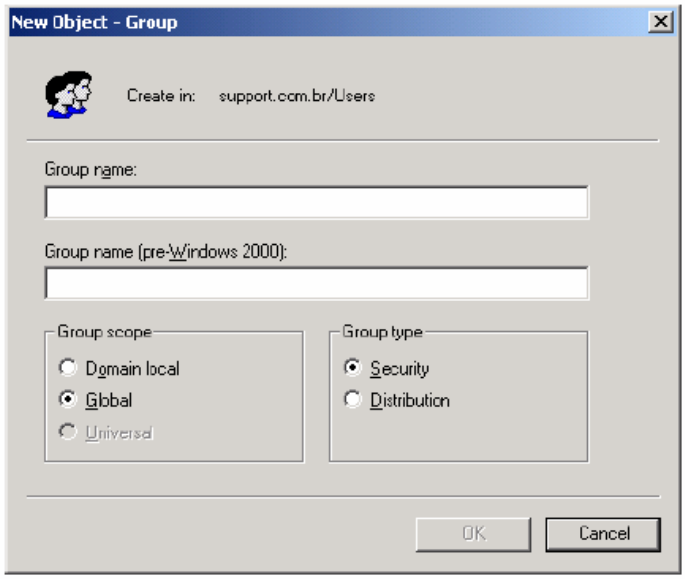


Figura 37 – Criação de um novo grupo

Opção	Descrição
Group name	Nome do novo grupo, que deve ser exclusivo no domínio em que o grupo for criado
Group name (pre-Windows 2000)	Nome usado para dar suporte a clientes e servidores de versões anteriores do Windows
Group scope	Escopo do grupo. Lembrando que a opção Universal só estará disponível em redes formadas por mais de um domínio e que estejam funcionando em modo nativo
Group type	Tipo de grupo

Inclusão de Participantes
Para incluir participantes em um grupo também utiliza-se o snap-in Active Directory Users and
Computers clicando nas propriedades do grupo desejado (botão direito do mouse).

Figura 38 – Inclusão de participantes em um grupo global

Nesta caixa de diálogo, obtém-se acesso à lista de objetos que podem ser incluídos no grupo (neste exemplo um grupo global) clicando-se em Add.

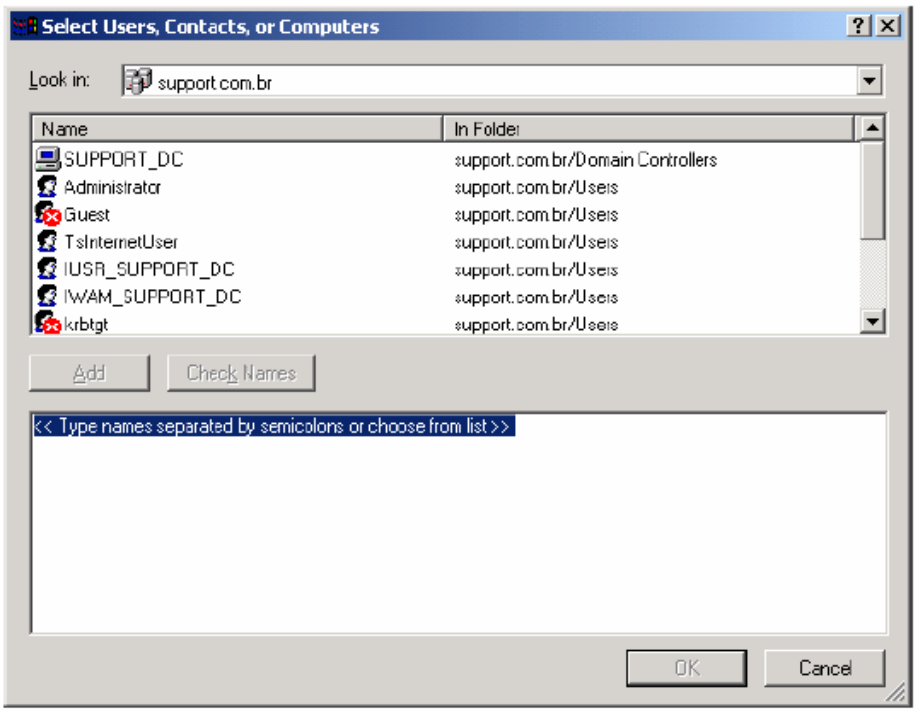


Figura 39 – Seleção de objetos para o grupo global

Também é possível definir-se os grupos dos quais um usuário fará parte nas propriedades da conta de usuário.

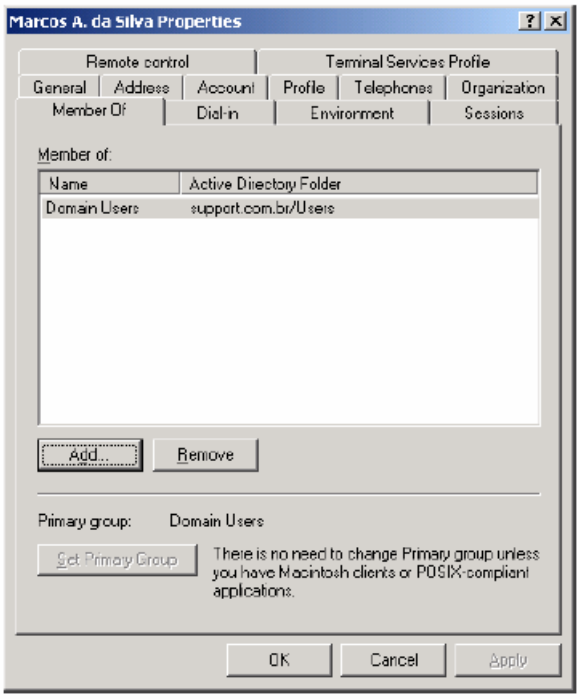


Figura 40 – Propriedades do usuário

Referencias de sites:

www.juliobattisti.com.br

www.guiadohardware.net

http://imasters.uol.com.br/

http://www.baboo.com.br/

www.apostilando.com

www.microsoft.com/brasil/technet