Tutorial Sobre Redes e Roteamento de Modens

Autor:
Paulo Ricardo de Oliveira

Capítulo I - Introdução ao Protocolo IP

Uma 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:

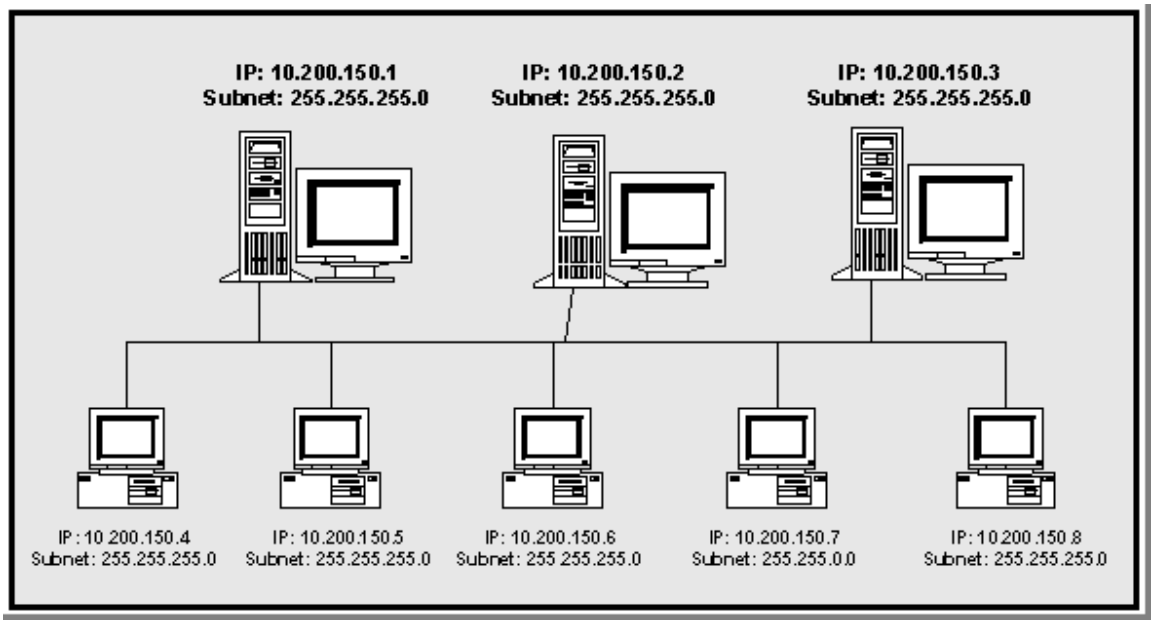


Figura - Uma rede baseada no protocolo TCP/IP.

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 mensagem. Nas próximas partes deste tutorial, falaremos um pouco mais sobre Broadcast.

Com 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".**

Nota: Existem configurações mais avançadas onde podemos subdividir uma rede TCP/IP em sub-redes menores. O conceito de sub-redes será tratado, em detalhes, na Parte 7 deste tutorial.

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.juliobattisti.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
```

Bem, estes são os aspectos básicos do protocolo TCP/IP. Nos endereços a seguir, você encontra tutoriais, em português, onde você poderá aprofundar os seus estudos sobre o protocolo TCP/IP:

- http://www.guiadohardware.info/tutoriais/enderecamento_ip/index.asp

- http://www.guiadohardware.info/curso/redes_guia_completo/22.asp
- http://www.guiadohardware.info/curso/redes_guia_completo/23.asp
- http://www.guiadohardware.info/curso/redes_guia_completo/28.asp
- http://www.vanquish.com.br/site/020608
- http://unsekurity.virtualave.net/texto1/texto_tcpip_basico.txt
- http://unsekurity.virtualave.net/texto1/tcpipI.txt
- http://www.rota67.hpg.ig.com.br/tutorial/protocolos/amfhp_tcpip_basico001.htm
- http://www.rota67.hpg.ig.com.br/tutorial/protocolos/amfhp_tcpip_av001.htm
- http://www.geocities.com/ResearchTriangle/Thinktank/4203/doc/tcpip.zip

Questão de exemplo para os exames de Certificação

A seguir coloco um exemplo de questão, relacionada ao TCP/IP, que pode aparecer nos exames de Certificação da Microsoft, onde são cobrados conhecimentos básicos do protocolo TCP/IP. Esta questão faz parte dos simulados gratuitos, disponíveis aqui no site.

Questão 01

A seguir estão as configurações básicos do TCP/IP de três estações de trabalho: micro01, micro02 e micro03.

Configurações do micro01:

Número IP: 100.100.100.3

Máscara de sub-rede: 255.255.255.0

Gateway: 100.100.100.1

Configurações do micro02:

Número IP: 100.100.100.4

Máscara de sub-rede: 255.255.240.0

Gateway: 100.100.100.1

Configurações do micro03:

Número IP: 100.100.100.5

Máscara de sub-rede: 255.255.255.0

Gateway: 100.100.100.2

O micro 02 não está conseguindo comunicar com os demais computadores da rede. Já o micro03 consegue comunicar-se na rede local, porém não consegue se comunicar com nenhum recurso de outras redes, como por exemplo a Internet. Quais alterações você deve fazer para que todos os computadores possam se comunicar normalmente, tanto na rede local quanto com as redes externas?

a) Altere a máscara de sub-rede do micro02 para 255.255.255.0
Altere o Gateway do micro03 para 100.100.100.1

b) Altere a máscara de sub-rede do micro01 para 255.255.240.0
Altere a máscara de sub-rede do micro03 para 255.255.240.0

c) Altere o Gateway do micro01 para 100.100.100.2
Altere o Gateway do micro02 para 100.100.100.2

d) Altere o Gateway do micro03 para 100.100.100.1

e) Altere a máscara de sub-rede do micro02 para 255.255.255.0

Resposta certa: a

Comentários: Pelo enunciado o computador micro02 não consegue comunicar com nenhum outro computador da rede. Este é um sintoma típico de problema na máscara de sub-rede. É exatamente o caso, o micro02 está com uma máscara de sub-rede 255.255.240.0, diferente da máscara dos demais computadores. Por isso ele está isolado e não consegue se comunicar com os demais computadores da rede. Já o micro03 não consegue comunicar-se com outras redes, mas consegue comunicar-se na rede local. Este é um sintoma de que a configuração do Gateway está incorreta. Por isso a necessidade de alterar a configuração do Gateway do micro03, para que este utilize a mesma configuração dos demais computadores da rede. Observe como esta questão testa apenas conhecimentos básicos do TCP/IP, tais como Máscara de sub-rede e Default Gateway.

Capítulo II – Classes de Endereço IP

Endereçamento IP – Classes de Endereços

Inicialmente foram definidas cinco classes de endereços, identificadas pelas letras: A, B, C, D e E. Vou iniciar com uma descrição detalhada de cada Classe de Endereços e, em seguida apresento um quadro resumo.

Redes Classe A

Esta classe foi definida com tendo o primeiro bit do número IP como sendo igual a zero. Com isso o primeiro número IP somente poderá variar de 1 até 126 (na prática até 127, mas o número 127 é um número reservado, conforme detalharei mais adiante). Observe, no esquema a seguir, explicado na Parte 2, que o primeiro bit sendo 0, o valor máximo (quando todos os demais bits são iguais a 1) a que se chega é de 127:

	0	**1**	**1**	**1**	**1**	**1**	**1**	**1**
Multiplica por:	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
equivale a:	128	64	32	16	8	4	2	1
Multiplicação:	0**x**128	1**x**64	1**x**32	1**x**16	1**x**8	1**x**4	1**x**2	1**x**1
Resulta em:	0	64	32	16	8	4	2	1
Somando tudo:	**0+64+32+16+8+4+2+1**							
Resulta em:	**127**							

O número 127 não é utilizado como rede Classe A, pois é um número especial, reservado para fazer referência ao próprio computador. O número 127.0.0.1 é um número especial, conhecido como localhost. Ou seja, sempre que um programa fizer referência a localhost ou ao número 127.0.0.1, estará fazendo referência ao computador onde o programa está sendo executado.

Por padrão, para a Classe A, foi definida a seguinte máscara de sub-rede: 255.0.0.0. Com esta máscara de sub-rede observe que temos 8 bits para o endereço da rede e 24 bits para o endereço da máquina dentro da rede. Com base no número de bits para a rede e para as máquinas, podemos determinar quantas redes Classe A podem existir e qual o número máximo de máquinas por rede. Para isso utilizamos a fórmula a seguir:

$$2^n - 2$$

,onde "n" representa o número de bits utilizado para a rede ou para a identificação da máquina dentro da rede. Vamos aos cálculos:

Número de redes Classe A

Número de bits para a rede: 7. Como o primeiro bit sempre é zero, este não varia. Por isso sobram 7 bits (8-1) para formar diferentes redes:

2^7-2 -> 128-2 -> **126 redes Classe A**

Número de máquinas (hosts) em uma rede Classe A

Número de bits para identificar a máquina: 24

2^{24}-2 -> 16777216 - 2 -> **16777214 máquinas em cada rede classe A.**

Na Classe A temos apenas um pequeno número de redes disponíveis, porém um grande número de máquinas em cada rede.

Já podemos concluir que este número de máquinas, na prática, jamais será instalado em uma única rede. Com isso observe que, com este esquema de endereçamento, teríamos poucas redes Classe A (apenas 126) e com um número muito grande de máquinas em cada rede. Isso causaria desperdício de endereços IP, pois se o endereço de uma rede Classe A fosse disponibilizado para um empresa, esta utilizaria apenas uma pequena parcela dos endereços disponíveis e todos os demais endereços ficariam sem uso. Para resolver esta questão é que passou-se a utilizar a divisão em sub-redes, assunto este que será visto na Parte 5 destes curso.

Redes Classe B

Esta classe foi definida com tendo os dois primeiros bits do número IP como sendo sempre iguais a 1 e 0. Com isso o primeiro número do endereço IP somente poderá variar de 128 até 191. Como o segundo bit é sempre 0, o valor do segundo bit que é 64 nunca é somado para o primeiro número IP, com isso o valor máximo fica em: 255-64, que é o 191. Observe, no esquema a seguir, explicado na Parte 2 deste curso, que o primeiro bit sendo 1 e o segundo sendo 0, o valor máximo (quando todos os demais bits são iguais a 1) a que se chega é de 191:

	1	**0**	**1**	**1**	**1**	**1**	**1**	**1**
Multiplica por:	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
equivale a:	128	64	32	16	8	4	2	1
Multiplicação:	1**x**128	0**x**64	1**x**32	1**x**16	1**x**8	1**x**4	1**x**2	1**x**1
Resulta em:	128	0	32	16	8	4	2	1
Somando tudo:	**128+0+32+16+8+4+2+1**							
Resulta em:	**191**							

Por padrão, para a Classe B, foi definida a seguinte máscara de sub-rede: **255.255.0.0**. Com esta máscara de sub-rede observe que temos 16 bits para o endereço da rede e 16 bits para o endereço da máquina dentro da rede. Com base no número de bits para a rede e para as máquinas, podemos determinar quantas redes Classe B podem existir e qual o número máximo de máquinas por rede. Para isso utilizamos a fórmula a seguir:

2^n- 2

,onde "n" representa o número de bits utilizado para a rede ou para a identificação da máquina dentro da rede. Vamos aos cálculos:

Número de redes Classe B

Número de bits para a rede: 14. Como o primeiro e o segundo bit são sempre 10, fixos, não variam, sobram 14 bits (16-2) para formar diferentes redes:

2^{14}-2 -> 16384-2 -> 16382 redes Classe B

Número de máquinas (hosts) em uma rede Classe B

Número de bits para identificar a máquina: 16

2^{16}-2 -> 65536-2 -> 65534 máquinas em cada rede classe B

Na Classe B temos um número razoável de redes Classe B, com um bom número de máquinas em cada rede.

O número máximo de máquinas, por rede Classe B já está mais próximo da realidade para as redes de algumas grandes empresas tais como Microsoft, IBM, HP, GM, etc. Mesmo assim, para muitas empresas menores, a utilização de um endereço Classe B, representa um grande desperdício de números IP. Conforme veremos na Parte 7 deste tutorial é possível usar um número diferentes de bits para a máscara de sub-rede, ao invés dos 16 bits definidos por padrão para a Classe B (o que também é possível com Classe A e Classe C). Com isso posso dividir uma rede classe B em várias sub-redes menores, com um número menor de máquinas em cada sub-rede. Mas isso é assunto para a Parte 7 deste tutorial.

Redes Classe C

Esta classe foi definida com tendo os três primeiros bits do número IP como sendo sempre iguais a 1, 1 e 0. Com isso o primeiro número do endereço IP somente poderá variar de 192 até 223. Como o terceiro bit é sempre 0, o valor do terceiro bit que é 32 nunca é somado para o primeiro número IP, com isso o valor máximo fica em: 255-32, que é 223. Observe, no esquema a seguir, explicado na Parte 2 deste tutorial, que o primeiro bit sendo 1, o segundo bit sendo 1 e o terceiro bit sendo 0, o valor máximo (quando todos os demais bits são iguais a 1) a que se chega é de 223:

	1	**1**	**0**	**1**	**1**	**1**	**1**	**1**
Multiplica por:	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
equivale a:	128	64	32	16	8	4	2	1
Multiplicação:	1**x**128	1**x**64	0**x**32	1**x**16	1**x**8	1**x**4	1**x**2	1**x**1
Resulta em:	128	64	0	16	8	4	2	1
Somando tudo:	**128+64+0+16+8+4+2+1**							
Resulta em:	**223**							

Por padrão, para a Classe C, foi definida a seguinte máscara de sub-rede: **255.255.255.0**. Com esta máscara de sub-rede observe que temos 24 bits para o endereço da rede e apenas 8 bits para o endereço da máquina dentro da rede. Com base no número de bits para a rede e para as máquinas, podemos determinar quantas redes Classe C podem existir e qual o número máximo de máquinas por rede. Para isso utilizamos a fórmula a seguir:

2^{n}- 2

,onde "n" representa o número de bits utilizado para a rede ou para a identificação da máquina dentro da rede. Vamos aos cálculos:

Número de redes Classe C

Número de bits para a rede: 21. Como o primeiro, o segundo e o terceiro bit são sempre 110, ou seja:fixos, não variam, sobram 21 bits (24-3) para formar diferentes redes:

2^{21}-2 -> 2.097.152-2 -> 2.097.150 redes Classe C

Número de máquinas (hosts) em uma rede Classe C:

Número de bits para identificar a máquina: 8

2^{8}-2 -> 256-2 -> 254 máquinas em cada rede classe C

Observe que na Classe C temos um grande número de redes disponíveis, com, no máximo, 254 máquinas em cada rede. É o ideal para empresas de pequeno porte.

Mesmo com a Classe C, existe um grande desperdício de endereços. Imagine uma pequena empresa com apenas 20 máquinas em rede. Usando um endereço Classe C, estariam sendo desperdiçados 234 endereços. Conforme já descrito anteriormente, esta questão do desperdício de endereços IP pode ser resolvida através da utilização de sub-redes.

Redes Classe D

Esta classe foi definida com tendo os quatro primeiros bits do número IP como sendo sempre iguais a 1, 1, 1 e 0. A classe D é uma classe especial, reservada para os chamados endereços de Multicast. Falaremos sobre Multicast, Unicast e Broadcast em uma das próximas partes deste tutorial.

Redes Classe E

Esta classe foi definida com tendo os quatro primeiros bits do número IP como sendo sempre iguais a 1, 1, 1 e 1. A classe E é uma classe especial e está reservada para uso futuro.

Quadro resumo das Classes de Endereço IP

A seguir apresento uma tabela com as principais características de cada Classe de Endereços IP:

Classe	**Primeiros bits**	**Núm. de redes**	**Número de hosts**	**Máscara padrão**
A	0	126	16.777.214	255.0.0.0
B	10	16.382	65.534	255.255.0.0
C	110	2.097.150	254	255.255.255.0
D	1110	Utilizado para tráfego Multicast		
E	1111	Reservado para uso futuro		

Endereços Especiais

Existem alguns endereços IP especiais, reservados para funções específicas e que não podem ser utilizados como endereços de uma máquina da rede. A seguir descrevo estes endereços.

- **Endereços da rede 127.0.0.0:** São utilizados como um aliás (apelido), para fazer referência a própria máquina. Normalmente é utilizado o endereço 127.0.0.1, o qual é associado ao nome localhost. Esta associação é feita através do arquivo hosts. No Windows 95/98/Me o arquivo hosts está na pasta onde o Windows foi instalado e no Windows 2000/XP/Vista/2003, o arquivo hosts está no seguinte caminho: system32/drivers/etc, sendo que este caminho fica dentro da pasta onde o Windows foi instalado.
- **Endereço com todos os bits destinados à identificação da máquina, iguais a 0:** Um endereço com zeros em todos os bits de identificação da máquina, representa o endereço da rede. Por exemplo, vamos supor que você tenha uma rede Classe C. A

máquina a seguir é uma máquina desta rede: 200.220.150.3. Neste caso o endereço da rede é: 200.220.150.0, ou seja, zero na parte destinada a identificação da máquina. Sendo uma rede classe C, a máscara de sub-rede é 255.255.255.0.

- **Endereço com todos os bits destinados à identificação da máquina, iguais a 1:** Um endereço com valor 1 em todos os bits de identificação da máquina, representa o endereço de broadcast. Por exemplo, vamos supor que você tenha uma rede Classe C. A máquina a seguir é uma máquina desta rede: 200.220.150.3. Neste caso o endereço de broadcast desta rede é o seguinte: 200.220.150.255, ou seja, todos os bits da parte destinada à identificação da máquina, iguais a 1. Sendo uma rede classe C, a máscara de sub-rede é 255.255.255.0. Ao enviar uma mensagem para o endereço do broadcast, a mensagem é endereçada para todos as máquinas da rede.

Capítulo III – Números Binários e Máscara de Sub-Rede

Sistema de Numeração Binário

Vou iniciar falando do sistema de numeração decimal, para depois fazer uma analogia ao apresentar o sistema de numeração binário.Todos nos conhecemos o sistema de numeração decimal, no qual são baseados os números que usamos no nosso dia-a-dia, como por exemplo: 100, 259, 1450 e assim por diante. Você já parou para pensar porque este sistema de numeração é chamado de sistema de numeração decimal? Não? Bem, a resposta é bastante simples: este sistema é baseado em dez dígitos diferentes, por isso é chamado de sistema de numeração decimal. Todos os números do sistema de numeração decimal são escritos usando-se uma combinação dos seguintes dez dígitos:

0 1 2 3 4 5 6 7 8 9

Dez dígitos -> Sistema de numeração decimal.

Vamos analisar como é determinado o valor de um número do sistema de numeração decimal. Por exemplo, considere o seguinte número:

4538

O valor deste número é formado, multiplicando-se os dígitos do número, de trás para frente, por potências de 10, começando com 10^0. O último dígito (bem à direita) é multiplicado por 10^0, o penúltimo por 10^1, o próximo por 10^2 e assim por diante. O valor real do número é a soma dos resultados destas multiplicações. Observe o esquema a seguir que será bem mais fácil de entender:

	4	**5**	**3**	**8**
Multiplica por:	**10^3**	**10^2**	**10^1**	**10^0**
ou seja:	1000	100	10	1
Resultado:	4x1000	5x100	3x10	8x1
Igual a:	4000	500	30	8
Somando tudo:	**4000+500+30+8**			
É igual a:	**4538**			

Observe que 4538 significa exatamente:

4 milhares (10^3)
+5 centenas (10^2)
+3 dezenas (10^1)
+ 8 unidades (10^0)

E assim para números maiores, com mais dígitos, teríamos potências de 10^4, 10^5 e assim por diante. Observe que multiplicando cada dígito por potências de 10, obtemos o número original. Este princípio aplicado ao sistema de numeração decimal é válido para qualquer sistema de numeração. Se for o sistema de numeração Octal (baseado em 8 dígitos), multiplica-se por potências de 8: 8^0, 8^1, 8^2 e assim por diante. Se for o sistema Hexadecimal (baseado em 10 dígitos e 6 letras) multiplica-se por potências de 16, só que a letra A equivale a 10, já que não tem sentido multiplicar por uma letra, a letra B equivale a 11 e assim por diante.

Bem, por analogia, se o sistema decimal é baseado em dez dígitos, então o sistema binário deve ser baseado em dois dígitos? Exatamente. Os números no sistema binários são escritos usando-se apenas os dois seguintes dígitos:

0 1

Isso mesmo, números no sistema binário são escritos usando-se apenas zeros e uns, como nos exemplos a seguir:

01011100
11011110
00011111

Também por analogia, se, no sistema decimal, para obter o valor do número, multiplicamos os seus dígitos, de trás para frente, por potências de 10, no sistema binário fizemos esta mesma operação, só que baseada em potências de 2, ou seja: 2^0, 2^1, 2^2, 2^3, 2^4 e assim por diante.

Vamos considerar alguns exemplos práticos. Como faço para saber o valor decimal do seguinte número binário: **11001110**

Vamos utilizar a tabelinha a seguir para facilitar os nossos cálculos:

	1	**1**	**0**	**0**	**1**	**1**	**1**	**0**
Multiplica por:	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
equivale a:	128	64	32	16	8	4	2	1
Multiplicação:	1**x**128	1**x**64	0**x**32	0**x**16	1**x**8	1**x**4	1**x**2	0**x**1
Resulta em:	128	64	0	0	8	4	2	0
Somando tudo:	**128+64+0+0+8+4+2+0**							
Resulta em:	**206**							

Ou seja, o número binário 11001110 equivale ao decimal 206. Observe que onde temos um a respectiva potência de 2 é somada e onde temos o zero a respectiva potência de 2 é anulada por ser multiplicada por zero. Apenas para fixar um pouco mais este conceito, vamos fazer mais um exemplo de conversão de binário para decimal. Converter o número **11100010** para decimal:

	1	**1**	**1**	**0**	**0**	**0**	**1**	**0**
Multiplica por:	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
equivale a:	128	64	32	16	8	4	2	1
Multiplicação:	1**x**128	1**x**64	1**x**32	0**x**16	0**x**8	0**x**4	1**x**2	0**x**1
Resulta em:	128	64	32	0	0	0	2	0
Somando tudo:	**128+64+32+0+0+0+2+0**							
Resulta em:	**226**							

Como Converter de Decimal para Binário

Bem, e se tivéssemos que fazer o contrário, converter o número 234 de decimal para binário, qual seria o binário equivalente??

Nota: Nos exemplos deste tutorial vou trabalhar com valores decimais de, no máximo, 255, que são valores que podem ser representados por 8 dígitos binários, ou na linguagem do computador 8 bits, o que equivale exatamente a um byte. Por isso que cada um dos quatro números que fazem parte do número IP, somente podem ter um valor máximo de 255, que é um valor que cabe em um byte, ou seja, 8 bits.

Existem muitas regras para fazer esta conversão, eu prefiro utilizar uma bem simples, que descreverei a seguir e que serve perfeitamente para o propósito deste tutorial.

Vamos voltar ao nosso exemplo, como converter 234 para um binário de 8 dígitos?

Eu começo o raciocínio assim. Primeiro vamos lembrar o valor decimal correspondente a cada um dos oito dígitos binários:

128 64 32 16 8 4 2 1

Lembrando que estes números representam potências de 2, começando, de trás para frente, com 2^0, 2^1, 2^2 e assim por diante, conforme indicado logo a seguir:

128 64 32 16 8 4 2 1
2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

Pergunto: 128 cabe em 234? Sim, então o primeiro dígito é 1. Somando 64 a 128 passa de 234? Não, dá 192, então o segundo dígito também é 1. Somando 32 a 192 passa de 234? Não, dá 224, então o terceiro dígito também é 1. Somando 16 a 224 passa de 234? Passa, então o quarto dígito é zero. Somando 8 a 224 passa de 234? Não, da 232, então o quinto dígito é 1. Somando 4 a 232 passa de 234? Passa, então o sexto dígito é zero. Somando 2 a 232 passa de 234? Não, dá exatamente 234, então o sétimo dígito é 1. Já cheguei ao valor desejado, então todos os demais dígitos são zero. Com isso, o valor 234 em binário é igual a:

11101010

Para exercitar vamos converter mais um número de decimal para binário. Vamos converter o número 144 para decimal.

Pergunto: 128 cabe em 144? Sim, então o primeiro dígito é 1. Somando 64 a 128 passa de 144? Sim, dá 192, então o segundo dígito é 0. Somando 32 a 128 passa de

144? Sim, dá 160, então o terceiro dígito também é 0. Somando 16 a 128 passa de 144? Não, dá exatamente 144, então o quarto dígito é 1. Já cheguei ao valor desejado, então todos os demais dígitos são zero. Com isso, o valor 144 em binário é igual a:

10010000

Bem, agora que você já sabe como converter de decimal para binário, está em condições de aprender sobre o operador "**E**" e como o TCP/IP usa a máscara de sub-rede (subnet mask) e uma operação "E", para verificar se duas máquinas estão na mesma rede ou em redes diferentes.

O Operador E

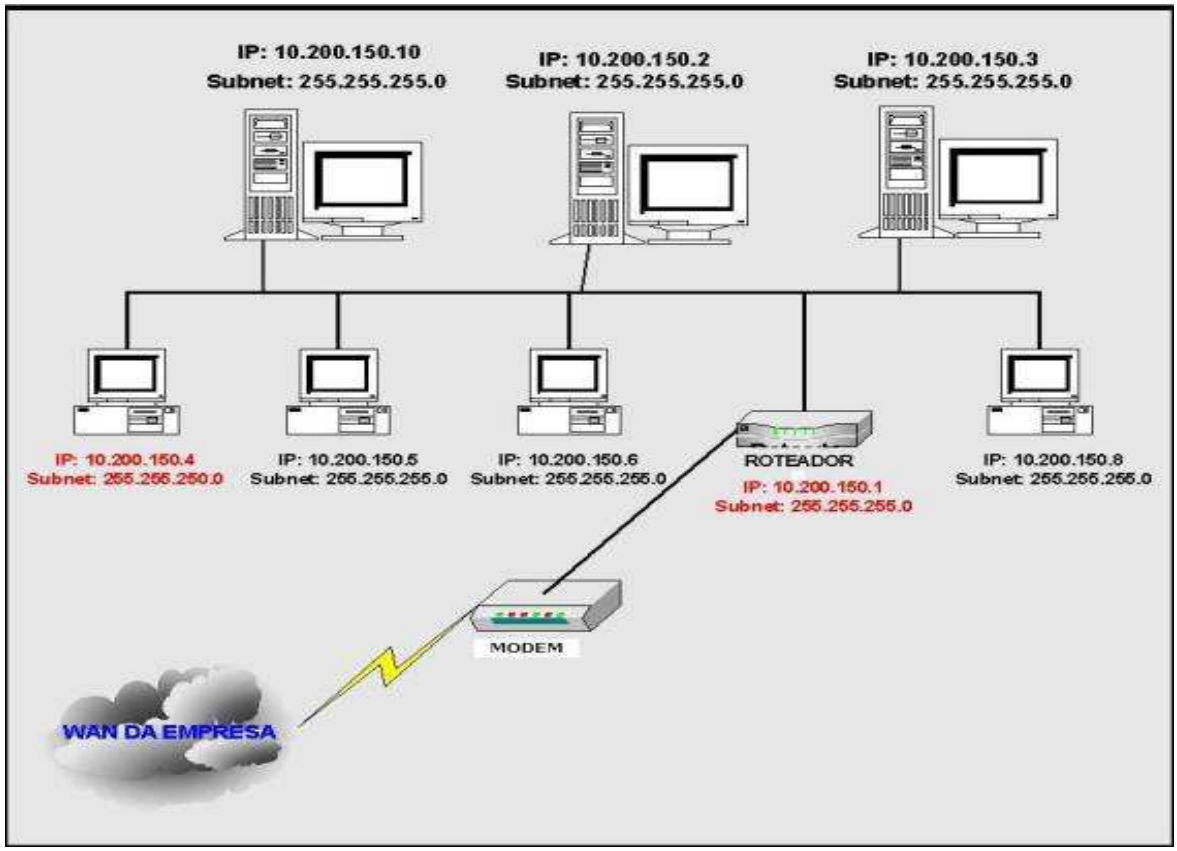
Existem diversas operações lógicas que podem ser feitas entre dois dígitos binários, sendo as mais conhecidas as seguintes: "E", "OU", "XOR" e "NOT".

Para o nosso estudo interessa o operador E. Quando realizamos um "E" entre dois bits, o resultado somente será 1, se os dois bits forem iguais a 1. Se pelo menos um dos bits for igual a zero, o resultado será zero. Na tabela a seguir temos todos os valores possíveis da operação E entre dois bits:

bit-1	**bit-2**	**(bit-1) E (bit-2)**
1	**1**	**1**
1	**0**	**0**
0	**1**	**0**
0	**0**	**0**

Como o TCP/IP usa a máscara de sub-rede:

Considere a figura a seguir, onde temos a representação de uma rede local, ligada a outras redes da empresa, através de um roteador.



Temos uma rede que usa como máscara de sub-rede 255.255.255.0 (uma rede classe C, mas ainda não abordamos as classes de redes, o que será feito na Parte 3 deste curso). A rede é a 10.200.150.0, ou seja, todos os equipamentos da rede tem os três primeiras partes do número IP como sendo: 10.200.150. Veja que existe uma relação direta entre a máscara de sub-rede a quantas das partes do número IP são fixas, ou seja, que definem a rede, conforme foi descrito na Parte 1 deste curso.

A rede da figura anterior é uma rede das mais comumente encontradas hoje em dia, onde existe um roteador ligado à rede e o roteador está conectado a um Modem, através do qual é feita a conexão da rede local com a rede WAN da empresa, através de uma linha de dados (também conhecido como link de comunicação). Nas próximas partes lições vou detalhar a função do roteador e mostrarei como funciona o roteamento entre redes.

Como o TCP/IP usa a máscara de sub-rede e o roteador

Quando dois computadores tentam trocar informações em uma rede, o TCP/IP precisa, primeiro, determinar se os dois computadores pertencem a mesma rede ou a redes diferentes. Neste caso podemos ter duas situações distintas:

Situação 1: Os dois computadores pertencem a mesma rede: Neste caso o TCP/IP envia o pacote para o barramento local da rede. Todos os computadores recebem o pacote, mas somente o computador que é o destinatário do pacote é que o captura e passa para processamento pelo Windows e pelo programa de destino. Como é que o computador sabe se ele é ou não o destinatário do pacote? Muito simples, no

pacote de informações está contido o endereço IP do computador destinatário. Em cada computador, o TCP/IP compara o IP de destinatário do pacote com o IP do computador, para saber se o pacote é ou não para o respectivo computador.

Situação 2: Os dois computadores não pertencem a mesma rede: Neste caso o TCP/IP envia o pacote para o Roteador (endereço do Default Gateway configurado nas propriedades do TCP/IP) e o Roteador se encarrega de fazer o pacote chegar ao seu destino. Em uma das partes deste tutorial veremos detalhes sobre como o Roteador é capaz de rotear pacotes de informações até redes distantes.

Agora a pergunta que tem a ver com este tópico:

"Como é que o TCP/IP faz para saber se o computador de origem e o computador de destino pertencem a mesma rede?"

Vamos usar alguns exemplos práticos para explicar como o TCP/IP faz isso:

Exemplo 1: Com base na figura anterior, suponha que o computador cujo IP é 10.200.150.5 (origem) queira enviar um pacote de informações para o computador cujo IP é 10.200.150.8 (destino), ambos com máscara de sub-rede igual a 255.255.255.0.

O primeiro passo é converter o número IP das duas máquinas e da máscara de sub-rede para binário. Com base nas regras que vimos anteriormente, teríamos a seguinte conversão:

Computador de origem:

10	**200**	**150**	**5**
00001010	11001000	10010110	00000101

Computador de destino:

10	**200**	**150**	**8**
00001010	11001000	10010110	00001000

Máscara de sub-rede:

255	**255**	**255**	**0**
11111111	11111111	11111111	00000000

Feitas as conversões para binário, vamos ver que tipo de cálculos o TCP/IP faz, para determinar se o computador de origem e o computador de destino estão na mesma rede.
Em primeiro lugar é feita uma operação "E", bit a bit, entre o Número IP e a máscara de Sub-rede do computador de origem, conforme indicado na tabela a seguir:

10.200.150.5	00001010	11001000	10010110	00000101	
255.255.255.0	11111111	11111111	11111111	00000000	**E**

10.200.150.0	00001010	11001000	10010110	00000000	**Resultado**

Agora é feita uma operação "E", bit a bit, entre o Número IP e a máscara de sub-rede do computador de destino, conforme indicado na tabela a seguir:

10.200.150.8	00001010	11001000	10010110	00001000	**E**
255.255.255.0	11111111	11111111	11111111	00000000	
10.200.150.0	00001010	11001000	10010110	00000000	**Resultado**

Agora o TCP/IP compara os resultados das duas operações. Se os dois resultados forem iguais, aos dois computadores, origem e destino, pertencem a mesma rede local. Neste caso o TCP/IP envia o pacote para o barramento da rede local. Todos os computadores recebem o pacote, mas somente o destinatário do pacote é que o captura e passa para processamento pelo Windows e pelo programa de destino. Como é que o computador sabe se ele é ou não o destinatário do pacote? Muito simples, no pacote de informações está contido o endereço IP do destinatário. Em cada computador, o TCP/IP compara o IP de destinatário do pacote com o IP do computador, para saber se o pacote é ou não para o respectivo computador.

É o que acontece neste exemplo, pois o resultado das duas operações "E" é igual: 10.200.150.0, ou seja, os dois computadores pertencem a rede: 10.200.150.0

Como você já deve ter adivinhado, agora vamos a um exemplo, onde os dois computadores não pertencem a mesma rede, pelo menos devido às configurações do TCP/IP.

Exemplo 2: Suponha que o computador cujo IP é 10.200.150.5 (origem) queira enviar um pacote de informações para o computador cujo IP é 10.204.150.8 (destino), ambos com máscara de sub-rede igual a 255.255.255.0.

O primeiro passo é converter o número IP das duas máquinas e da máscara de sub-rede para binário. Com base nas regras que vimos anteriormente, teríamos a seguinte conversão:

Computador de origem:

10	**200**	**150**	**5**
00001010	11001000	10010110	00000101

Computador de destino:

10	**204**	**150**	**8**
00001010	11001100	10010110	00001000

Máscara de sub-rede:

255	**255**	**255**	**0**
11111111	11111111	11111111	00000000

Feitas as conversões para binário, vamos ver que tipo de cálculos o TCP/IP faz, para determinar se o computador de origem e o computador de destino estão na mesma rede. Em primeiro lugar é feita uma operação "E", bit a bit, entre o Número IP e a máscara de Sub-rede do computador de origem, conforme indicado na tabela a seguir:

10.200.150.5	00001010	11001000	10010110	00000101	
255.255.255.0	11111111	11111111	11111111	00000000	**E**
10.200.150.0	00001010	11001000	10010110	00000000	**Resultado**

Agora é feita uma operação "E", bit a bit, entre o Número IP e a máscara de sub-rede do computador de destino, conforme indicado na tabela a seguir:

10.204.150.8	00001010	11001100	10010110	00001000	
255.255.255.0	11111111	11111111	11111111	00000000	**E**
10.204.150.0	00001010	11001100	10010110	00000000	**Resultado**

Agora o TCP/IP compara os resultados das duas operações. Neste exemplo, os dois resultados são diferentes: 10.200.150.0 e 10.204.150.0. Nesta situação o TCP/IP envia o pacote para o Roteador (endereço do Default Gateway configurado nas propriedades do TCP/IP) e o Roteador se encarrega de fazer o pacote chegar a rede do computador de destino. Em outras palavras o Roteador sabe entregar o pacote para a rede 10.204.150.0 ou sabe para quem enviar (um outro roteador), para que este próximo roteador possa encaminhar o pacote. Este processo continua até que o pacote seja entregue na rede de destino ou seja descartado, por não ter sido encontrada uma rota para a rede de destino.

Observe que, na figura anterior, temos dois computadores que, apesar de estarem fisicamente na mesma rede, não conseguirão se comunicar devido a um erro de configuração na máscara de sub-rede de um dos computadores. É o caso do computador 10.200.150.4 (com máscara de sub-rede 255.255.250.0). Como este computador está com uma máscara de sub-rede diferente dos demais computadores da rede (255.255.255.0), ao fazer os cálculos, o TCP/IP chega a conclusão que este computador pertence a uma rede diferente, o que faz com que ele não consiga se comunicar com os demais computadores da rede local.

Capítulo IV – Introdução ao 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. Ele possui várias características, as quais descreverei nesta parte do tutorial de TCP/IP.

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 (WINS é o assunto da Parte 9 deste tutorial). 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:

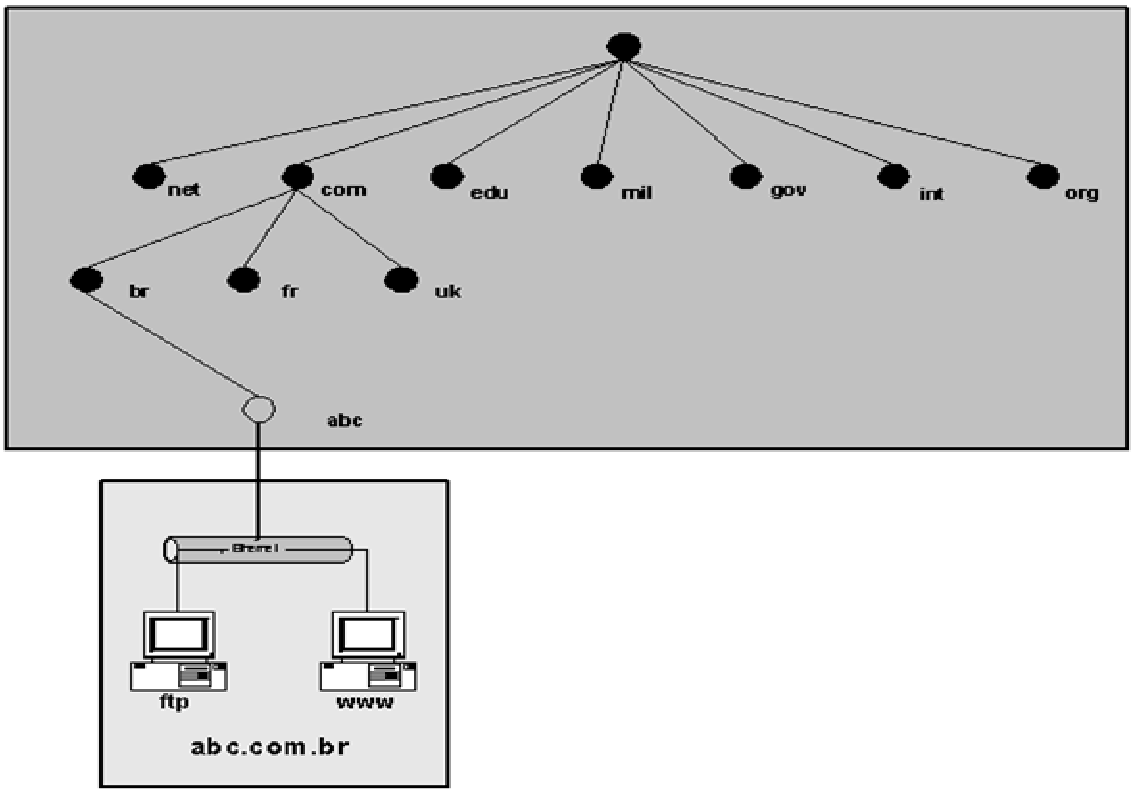


Figura - Estrutura hierárquica do DNS

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.juliobattisti.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.juliobattisti.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 – assunto da Parte 10 deste tutorial). 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.juliobattisti.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.juliobattisti.com.br?" E o servidor responde: "Sim, conheço. O número IP associado com o nome www.juliobattisti.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.

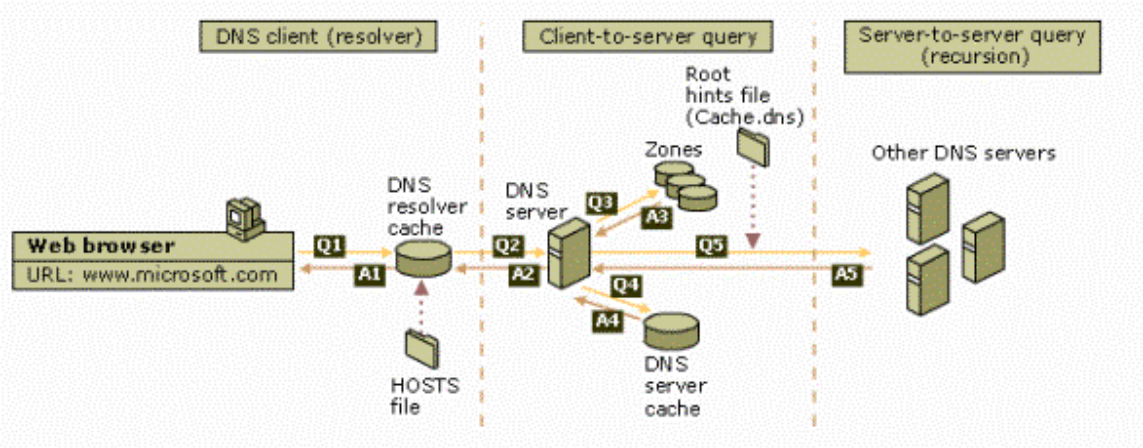


Figura - O processo de resolução de nomes do DNS.

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 (para uma descrição completa sobre zonas e domínios e a criação de zonas e domínios no DNS consulte o Capítulo 3 do meu livro Manual de Estudos para o Exame 70-216, 712 páginas, o qual está esgotado em formato impresso, mas está a venda em formato de E-book, em PDF. Todos os detalhes em: http://www.juliobattisti.com.br/cursos/70216/default.asp).

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.

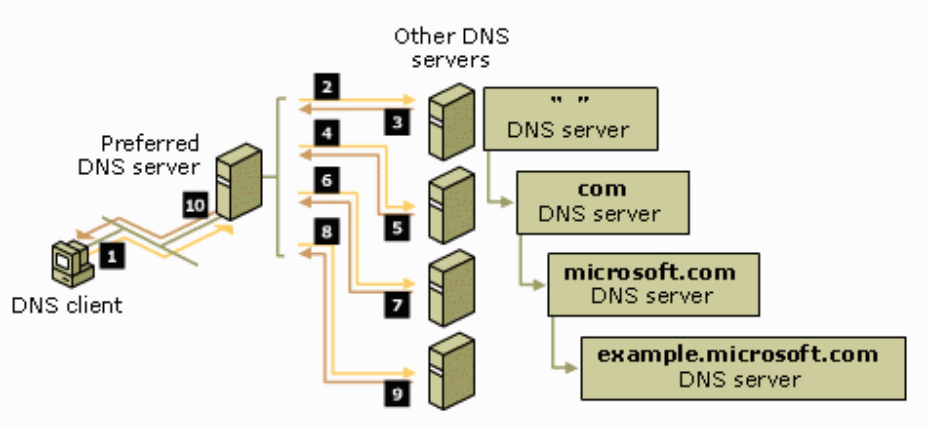


Figura - Resolução de nomes usando recursão

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:

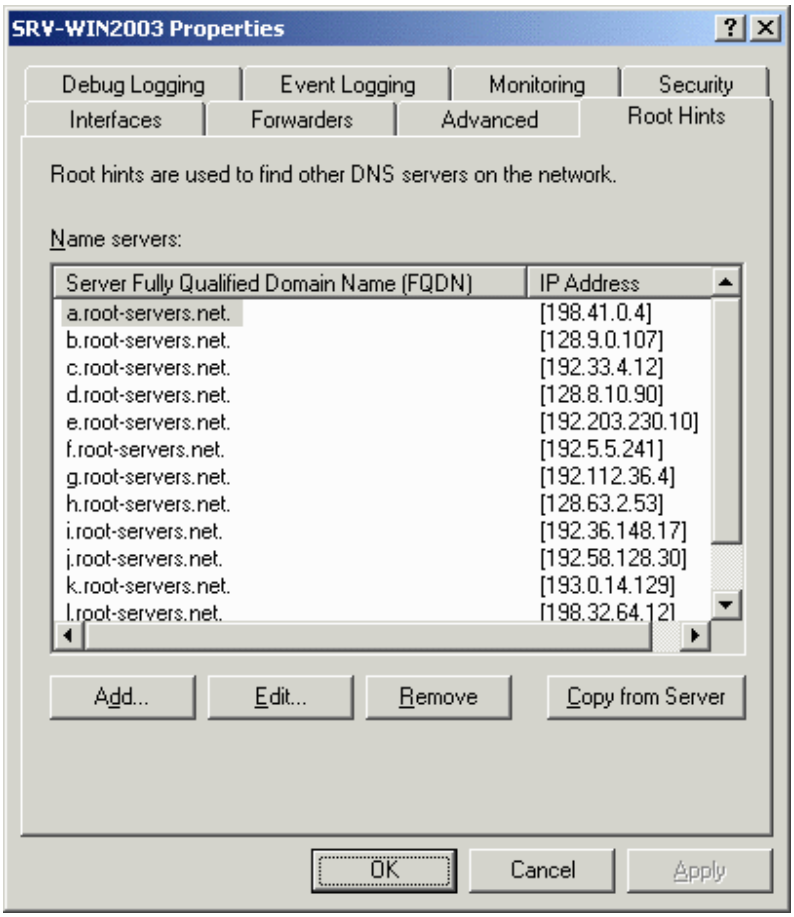


Figura - Lista de root hints do servidor DNS.

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 resonsável 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 resonsável 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 inforamação 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, duranto 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.

Sei que e difícil de aceitar mais teremos que dar uma revisada no protocolo TCP/IP

Pois e ele o grande responsável pela internet e já que estamos aqui mão a obra

O protocolo TCP/IP foi criado especialmente para internet ele se baseia em dois principais pilares: Endereço e aplicação cliente servidor, muitas pessoas ainda não entenderam que pra se logar em uma maquina remota ela estando na sua rede local ou WAN (internet).

Ela terá que ter um aplicativo cliente o outro servidor.

No caso do servidor terá quer ter usuários cadastrado para aceitar a conexão remota (quando eu falo conexão remota e o computador que esta em outra localidade ou outra rede local) e ser autenticado isso trará todos os benefícios que o protocolo que esta sendo usado lhe oferece exemplo FTP transferência de arquivo, TELNET sessão remota, VPN ligação entre duas redes, e assim por diante, isso para qualquer aplicativo que funcione em rede.

No caso do cliente ele terá que ter o mesmo protocolo instalado e configurado corretamente para pode dar o ponta pé inicial fazendo o pedido de conexão, pois o servidor estará lá para servi-lo isso que significa ser um servidor e esta sempre pronto para servi o seus clientes

Endereço essa e outra parte importante a se entender, quando você vai na casa de uma pessoa que você nunca foi o que você pede. Lógico o endereço assim também e na internet quando um pacote precisa chegar a um determinado computador no mundo ele precisa do endereço do computador.

Foi pesando nesta teoria que os engenheiros criaram o endereço através de números, pois os números são infinitos, eles sabiam que no começo são poucos computadores mais que isso iria crescer desesperadamente.

Foi ai que surgiu o endereço de IP, o nome TCP/IP e a grande revolução das redes, pois ele possibilita uma pessoa conversa em tempo real com outra em qual que lugar do mundo e só você saber o endereço dela , desculpe o endereço de IP.

O endereço de IP e constituído por 32 bit ou quatro casa de 4 byte ficando assim
0.0.0.0
10.0.0.0
176.168.0.0
192.168.0.

Obs. (Os endereços WAN nunca se repetem, você encontrado através dele ex: ´200.204.25.159).

Estes esquemas de endereço são para rede local ou rede privada. Fora estes endereços ainda temos os de diagnostico que não da para ser usada como IPs valido exemplo

127.0.0.1 LOOPBACK este causa um auto retorno e indica a própria maquina

169.254.0.0 APIPA este indica que não foi encontrado nenhum servidor DHCP

BROADCAST este manda pacotes pra toda a rede há mesmo tempo

Os endereços de IP são divididos em 5 classes de A E cada classe representa um esquema de rede diferente. como isso e só um resumo do protocolo estou colocando os tópicos mais importante que você precisa saber para trabalha com roteamento de modem , você quiser saber mais sobre o protocolo de rede TCP/IP faço o outro curso da minha autoria que esta disponível no site www.redeestruturada.e1.com.br Pronto existem ainda alguns tipos de IPs que não foram mencionados incluindo os que se referem a paises .

Protocolos que funcionam Junto ao TCP/IP

Agora que você já conhece um pouco de endereço de IP podemos falar sobre os protocolos que funcionam dentro do TCP/IP

- **TELNET** Este serve para iniciar uma sessão com o computador remoto e usar comando do UNIX
- **FTP** Este outro e para transferência de arquivo ele tem uma capacidade muito grande de compartilha arquivos remoto com arquivo locais também e muito importante
- **DHCP** Este e responsável com distribuição de endereços de IPs na rede , ele e muito importante pois muita gente depois que roteia o modem e ver as maquinas conectando automaticamente sem precisar de configuração nem imagina que quem faz isso e o protocolo DHCP .Mais adiante falaremos mais sobre ele.
- **NAT** Este e o responsável pelo roteamento dos dados ele que e o grande segredo do roteador
- **DNS** Outro que e de suma importância, pois ele faz a tradução de nomes na rede ele troca o nome pelo numero de IP associado ainda vamos falar mais dele.
- **ATM** Este faz a ligação da sua casa o da empresa com o provedor de serviço em parceria com a Telefônica

Lembrando que só estou destacando os principais protocolos que são usados no roteamento de modem. O protocolo TCP/IP tem muito mais protocolos que você imagina cada um com a sua devida função ao longo do curso vou falando mais sobre o protocolo que ainda não foram mencionados.

Neste Capitulo estaremos falando como funciona o roteador, lembrando que este curso e voltado somente para técnicos de computadores e rede, devido ao roteamento não esta voltado a iniciantes que não conhecem os fatores técnicos das redes de computadores.

O roteador e feito para ligar uma rede com outras redes, portanto e existe uma diferença entre o modem ADSL com os roteadores dedicados.

A primeira e que o modem ADSL e uma versão resumida, e com outras utilidades mais importante do que apenas fazer o roteamento.

Só e possível fazer o modem funcionar como roteador, devido a um protocolo que esta incluso no aparelho, chamado de **(PROTOCOLO NAT)**

Se você na hora de tentar fazer um modem funcionar como roteador e você ver que não tem essa opção nas configurações esqueça, pois ele só vai ser apenas um modem.

A vantagem e que a maioria deles tem esse protocolo, devido a algumas regras do TCP/IP.

Ex: para você se conectar na internet você precisa de um endereço publico, este endereço que te dar e o seu provedor, então se eu tenho uma rede com 40 computadores eu teria que ter 40 endereços validos. Para que cada um possa entra na internet, isso resultaria em um grande gasto de IPs validos, e como os números de IPs tem um limite, estes endereços ficariam em uso muito rápido, resultado: iria acontecer de maquinas tentarem se conectar na internet e não poderem pois todos IPs já estariam sendo usado naquele momento.

Pesando nisso e que os engenheiros criaram os protocolos de compartilhamento de Internet para que uma maquina só pudesse dar acesso à internet a uma rede inteira

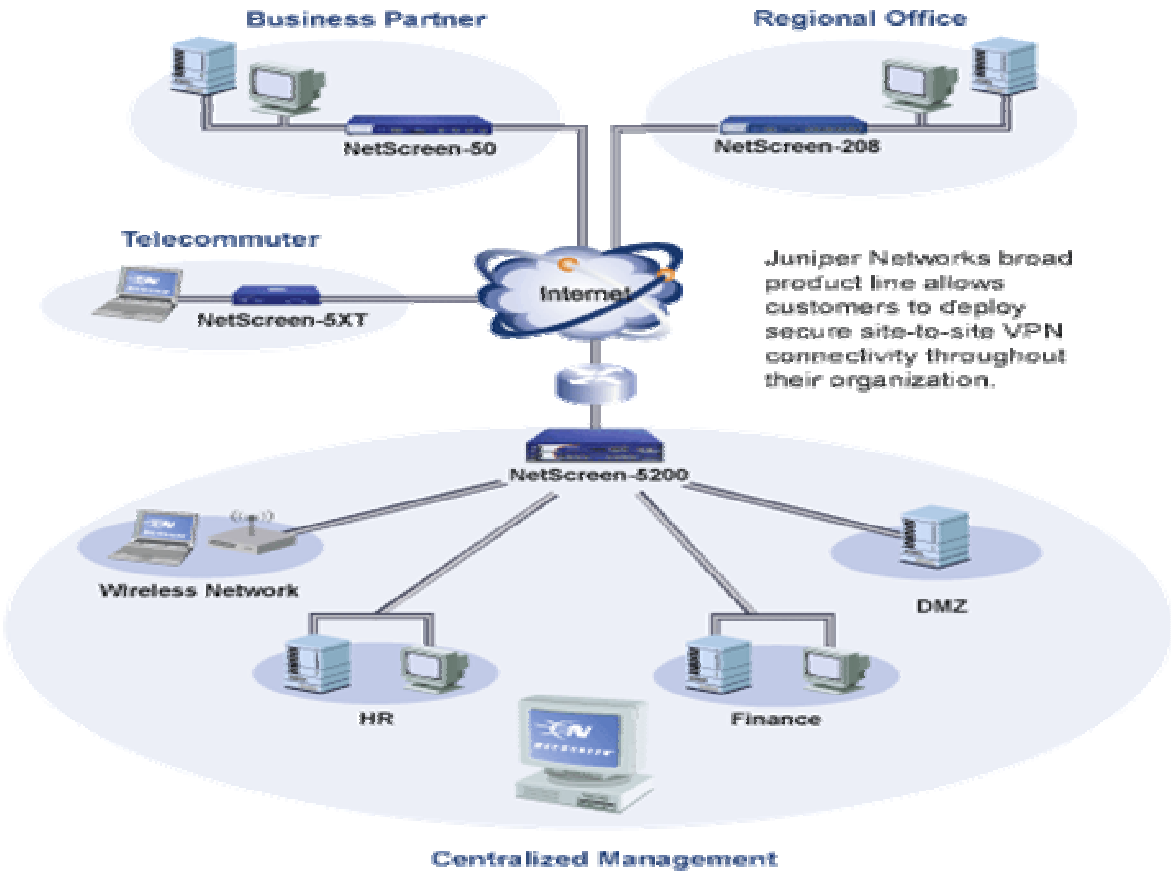
com apenas um numero de IP, deixando a internet bem mais aliviada, pois uma maquina esta representando mais de 250 maquinas.

Os protocolos responsáveis por isso são chamados de protocolos de compartilhamento, existem vários os mais usados são o NAT e Proxy. Entre os dois os que têm mais recursos e o NAT devido à praticidade que ele oferece, mais pra frente falarão mais sobre ele.

Falaremos um agora dos roteadores dedicados para que você sinta a diferença entre o roteador e o modem ADSL

Roteadores

Os roteadores foram feitos para controlar o trafico de dados na internet e a ligação de uma rede particular para outra veja a figura



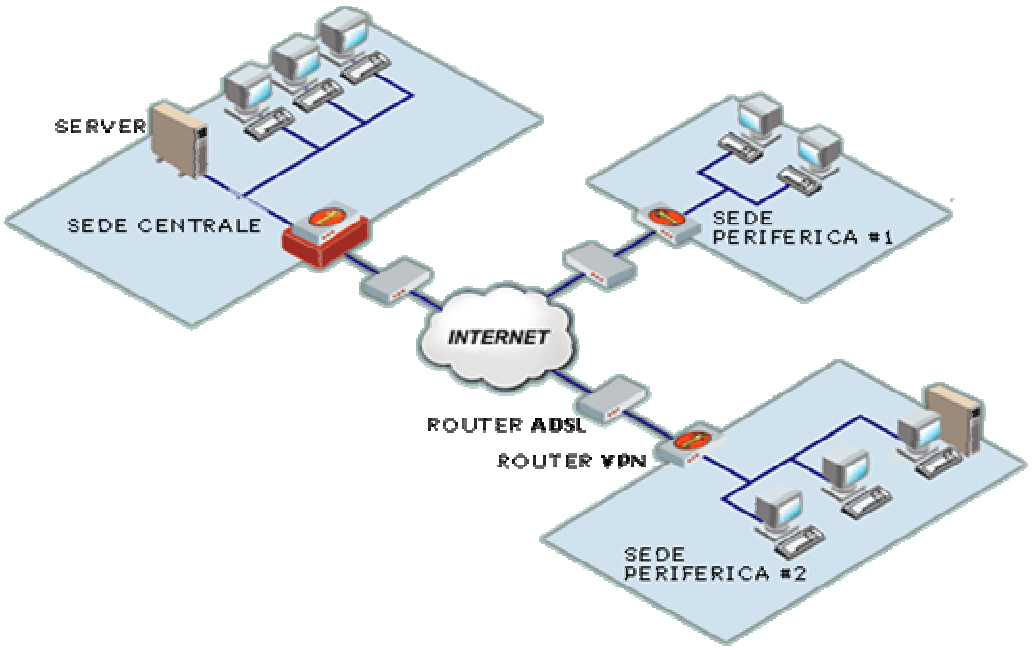
Os roteadores funcionam com base em uma tabela de roteamento, essa tabela que mostra pra onde os dados serão direcionados, se essa tabela sofre alguma alteração errada o roteador para imediatamente de trabalha ate que a tabela seja reparada. Seria impossível que um administrador esteja atualizando essa tabela manualmente em uma rede de grande porte, pensado nisso que fizeram os protocolos de

comunicação entre roteadores, estes protocolos reparam automaticamente essa tabela de roteamento. O tempo de espera no repara e chamado de convergência, é tempo que demora para o roteador se atualizar com as novas rotas .

Existem dois protocolos que fazem esse serviço de atualização nas tabelas:

- RIP este protocolo trabalha por envio de mensagens, ele emite uma atualização a cada 30 segundos.Mais ele só e usado em rede de pequeno porte devido algumas falhas que ele tem, já existe a versão RIPv2 que é um pouco melhor
- OSPF este protocolo já e usado em rede de grande porte, com a configuração bem mais complicada mais tem muito mais vantagens do que o RIP, uma delas e que quando ele envia a atualização da tabela de roteamento ele só emiti as mudanças que a tabela sofre, diferente do RIP que manda todo conteúdo a cada 30 segundo

Muitas empresas usam os roteadores pra ligar a matriz com as filiais e com pequenos escritórios através de links dedicados ou links virtuais que hoje em dia o preço é bem mais acessível do que os links dedicados



Modem ADSL

Vou explicar o valor que tem o modem ADSL, pois eles representam uma melhoria de 80% nas conexões, facilitando a vida de muitas empresas que depende de um bom trafico de Internet para poderem trabalhar.

A palavra modem significa MODULADOR e DEMODULADOR o seu papel e transformar um sinal digital em analógico que e o sinal que corre nas linhas telefônicas

Quando você usa uma conexão discada para de conectar na Internet, e o modem que faz a mudança do sinal digital em analógico que você ouve quando esta estabelecendo

uma conexão , naquele momento você esta usando uma linha telefônica para conectar-se ao seu provedor, a partir daquele momento o seu computador já tem um sinal modulador para conversar com o provedor.

Diferente de quando você se conectar a um computador na rede local que já tem um sinal digital, ele não precisa ser modulado isso torna a conexão muito mais rápida.

Quando você estabelece a conexão com o provedor ele imediatamente manda os endereços de IPs que você precisa para trafegar os dados na Internet ex

IP 200.205.3.68
Máscara 255.255.255.192
Gateway 200.205.3.1
DNS primário 200.204.0.10
sécundário..... 200.204.125.57

Agora que a conexão já esta estabelecida você só precisa se autenticar como cliente via discado ou através do browser como funciona no ig ai pronto você já pode navegar na Internet lentamente!

Mais agora não com tecnologia ADSL a situação muda de figura você contrata um serviço de banda larga e eles emitem um sinal digital direto na sua linha telefônica SPEEDY, AJATO, VIRTUA ai você não precisa mais modular os pacotes, resultando em uma conexão bem mais rápida e segura.

Ai você se pergunta por que eu preciso de um modem já que eu não tenho mais que modular os pacotes para serem enviados?

Por dois motivos, ainda não existe uma placa nos micros computadores que reconheçam o sinal que e enviado na sua linha telefônica, segundo porque você utiliza a mesma linha para fazer ligações telefônicas e o serviço de banda larga precisa organiza aos pacotes de dados e voz.

Lembrando que se você não tiver essa teoria você não terá ferramentas para repara eventuais problemas que acontece no aparelho , pois e muito fácil ir ate o site www.abusar.org pegar o manual e fazer funcionar sendo que você nem sabe porque esta mudando as opções e se der algum problema que não esta no manual ai você perde o aparelho , por isso estou passando toda essa teoria pra quando a gente entra na parte de configuração você saiba o que esta fazendo ...

O protocolo NAT é ele que determina se o modem pode funcionar como roteador, se o modem não tiver esse protocolo, não e possível estabelecer o roteamento na rede.

Temos dois principais tipos de sinais o PPPOE e PPPOA. Eles são os dois principais que vamos falar, sendo que existem outros. Quando você tem uma conexão PPPOE você precisa de um discado para estabelecer a conexão com o provedor, sendo que toda a vês que você disca, sempre muda o endereço de IP da sua maquina. No caso do PPPOA você recebe um endereço fixo de IP e quando você liga a maquina, ela sincroniza o sinal e você já esta conectado a coisa funciona bem melhor, pois IP fixo facilita muito a implantação de qualquer servidor.

Existem também alguns casos em que você tem IP fixo, mais depois de sincroniza ainda precisa se autenticar no browser. Quando você vai fazer o roteamento no modem você precisa saber se a conexão onde vai ser usado o aparelho è PPPOE ou PPPOA, porque a maneira de configura o modem é diferente de um para o outro.Eu já vi vários casos de Técnicos pegarem o modem fazerem a configuração e na hora de implantar na rede descobri que deve reconfigurar o aparelho. Lembrando que nem todo o modem aceita as duas principais configurações PPPOE e PPPOA

O centro do roteamento e o protocolo NAT ele que faz toda a tarefa difícil da rede imagine o seguinte, você vai é um carteiro, e vai entregar varias cartas em uma viela onde moram oito famílias, e na entrada da viela tem apenas um numero pra todas as casas, veja que fica difícil de entregar as cartas, pois você devera ir perguntando nas oito casa ate descobri de quem são as cartas certas, isso com certeza levaria algum tempo e acabaria atrasando o seu trabalho, pois um das oito casa trabalha a noite o outro só vem no final de semana à outra foi à fera, veja que ai demoraria um pouco mais pra descobri as casas corretas para entrega as cartas.

Sabe qual é a solução mais simples? Ligar o numero da viela com uma letra, o numero da viela e 200.205.156.14, então a identificação da primeira casa seria 200.205.156.14: A... A segunda casa seria 200.205.156.14:B e assim por diante ate completar os oitos casas (acredito que vocês estão entendendo o espírito da coisa). Agora quando você for entregar as cartas e só ir as casa em que a identificação esta batendo.

Por incrível que pareça é exatamente isso que o protocolo NAT faz.Você esta dentro de uma rede com um roteador fazendo o compartilhamento de internet, só que a sua maquina dentro da rede esta usando um endereço privado, portanto você não pode se conectar a internet direta, você precisa de um endereço publico certo.

Então quando você vai mandar um pacote para fora, esse pacote vai direto o para o seu GATEWAY padrão, sendo que o seu GATEWAY padrão e o seu roteador, o roteador pega anota na memória dele o numero de IP`que saio o pacote e liga em uma das 65536 portas ,então o endereço fica assim 192.168.0.68:3685 , depois de ligar o endereço com a porta e anotar na memória , ele mascara o pacote com o endereço dele mesmo que no caso seria 200.205.156.14 então o pacote sai para fora com esse numero de IP ...

Quando a resposta retorna, ela volta para o IP do roteador, mais como ele anotou na memória que aquele pacote saio da maquina com IP 192.168.0.68: 3685, ele rapidamente encaminha para a maquina que fez o pedido. Pronto, isso que é a essência do roteamento, e o responsável por tudo isso é o protocolo NAT, agora você sabe porque se não tiver esse protocolo no modem ele não pode funcionar como roteador.