Introdução:

Esta é a décima segunda parte do Tutorial de TCP/IP. Na Parte 1 tratei dos aspectos básicos do protocolo TCP/IP. Na Parte 2falei sobre cálculos binários, um importante tópico para entender sobre redes, máscara de sub-rede e roteamento. Na Parte 3 falei sobre Classes de endereços, na Parte 4 fiz uma introdução ao roteamento e na Parte 5apresentei mais alguns exemplos e análises de como funciona o roteamento. Na Parte 6 falei sobre a Tabela de Roteamento. Na Parte 7 tratei sobre a divisão de uma rede em sub-redes, conceito conhecido como subnetting. NaParte 8 fiz uma apresentação de um dos serviços mais utilizados pelo TCP/IP, que é o Domain Name System: DNS. O DNS é o serviço de resolução de nomes usado em todas as redes TCP/IP, inclusive pela Internet que, sem dúvidas, é a maior rede TCP/IP existente. Na Parte 9 fiz uma introdução ao serviço Dynamic Host Configuration Protocol – DHCP. Na Parte 10 fiz uma introdução ao serviço Windows Internet Name Services – WINS. Na Parte 11 falei sobre os protocolos TCP, UDP e sobre portas de comunicação. Nesta décima segunda parte, mostrarei como são efetuadas as configurações de portas em diversos aplicativos que você utiliza e os comandos do Windows 2000/XP/2003 utilizados para exibir informações sobre portas de comunicação.

Exemplos de utilização de portas

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

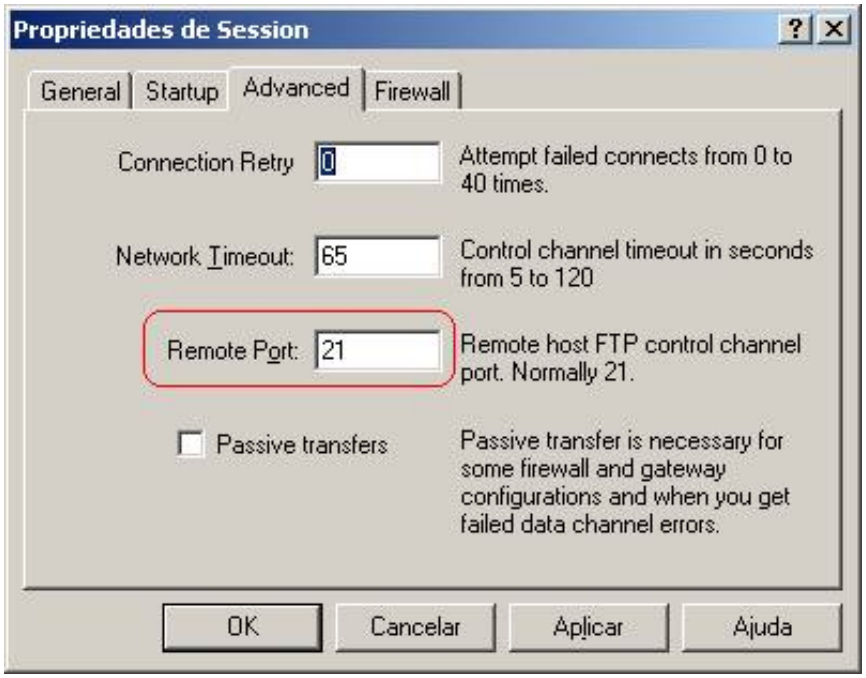
Quando você acessa um site na Internet, como por exemplowww.juliobattisti.com.br ouwww.certificacoes.com.br ouwww.uol.com.br, o navegador que você está utilizando se comunica com a porta 80 no servidor HTTP, do site que está sendo acessado. Você nem fica sabendo que está sendo utilizada a porta 80, pois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

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

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

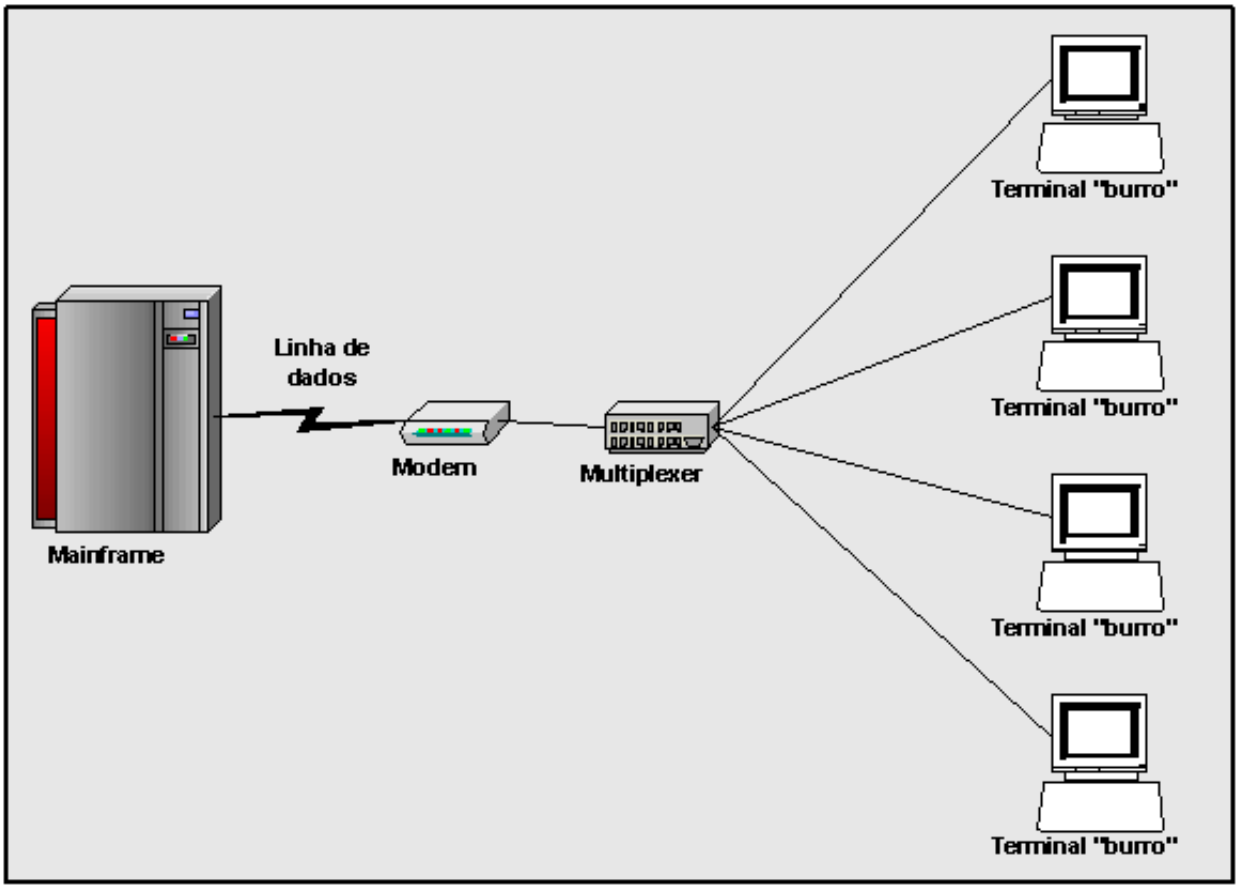
Um outro exemplo do dia-a-dia, onde utilizamos o conceito de portas de comunicação, é quando você utiliza um cliente de FTP para se conectar a um servidor de FTP e fazer

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

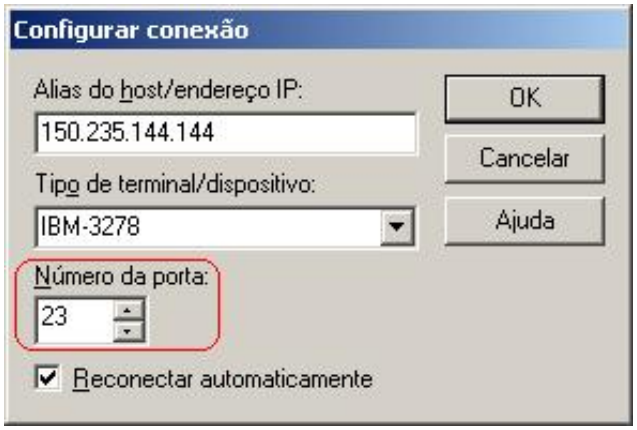


Outro uso muito comum nas redes da sua empresa é a criação de sessões de programas emuladores de terminal com sistemas que rodam no Mainframe da empresa. Apesar de terem anunciado a morte do Mainframe há algum tempo atrás, o fato é que o Mainframe continua mais vivo do que nunca e com grande parte dos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

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



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



Estas são apenas três situações bastante comuns – acessar a Internet, fazer download de arquivos a partir de um servidor FTP e criar uma sessão com o Mainframe, - utilizados diariamente por usuários das redes de empresas de todo o mundo, onde são utilizados, na prática, o conceito de Portas de Comunicação, do TCP/IP, conceito este que foi discutido na Parte 11 deste tutorial. A seguir apresentarei alguns comandos do Windows 2000/XP/2003, os quais exibem informações sobre as portas de comunicação que estão sendo utilizadas no seu computador. Se você não está conectado à rede de uma empresa, poderá utilizar estes comandos quando você estiver conectado á Internet, situação onde, certamente, estarão sendo utilizadas portas de comunicação.

O comando netstat – exibindo informações sobre portas

O comando netstat está disponível no Windows 2000, Windows XP e Windows Server

2003. Este comando exibe estatísticas do protocolo TCP/IP e as conexões atuais da rede TCP/IP. O comando netstat somente está disponível se o protocolo TCP/IP estiver instalado. A seguir apresento alguns exemplos de utilização do comando netstat e das opções de linha de comando disponíveis.

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

Conexões ativas

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

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

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

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

                           Recebido            Enviado

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

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

Conexões ativas

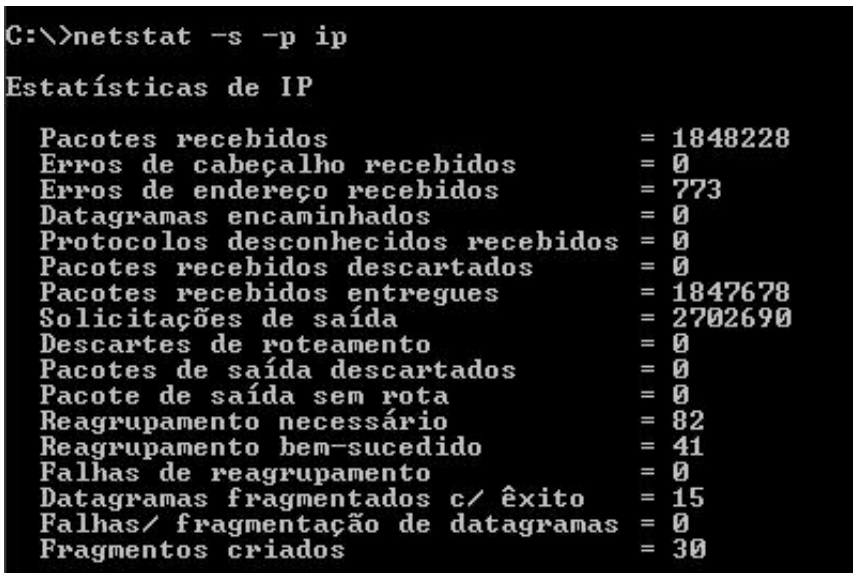
Proto	Endereço local	Endereço externo	Estado
TCP	100.200.50.50:1595	100.200.50.60:445	ESTABLISHED
TCP	100.200.50.50:2694	100.200.50.45:445	ESTABLISHED
TCP	100.200.50.50:2706	100.200.50.45:1352	ESTABLISHED
TCP	100.200.50.50:3236	100.200.50.102:445	TIME_WAIT
TCP	100.200.50.50:3381	100.200.50.45:1352	TIME_WAIT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

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

```
Estat¡sticas de IP

  Pacotes recebidos                   = 1847793
  Erros de cabeçalho recebidos        = 0
  Erros de endereço recebidos         = 772
```

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

Estat¡sticas de ICMP

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

Estat¡sticas de TCP

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

Estat¡sticas de UDP

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

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



netstat –r: Exibe o conteúdo da tabela de roteamento do computador. Exibe os mesmos resultados do comando route print, discutido em uma das primeiras partes deste tutorial.

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

netstat –s –p ip 10

Conclusão

Na Parte 11 do tutorial fiz uma apresentação dos protocolos TCP e UDP, os quais são responsáveis pelo transporte de pacotes em redes baseadas no TCP/IP. Você também aprendeu sobre as diferenças entre os protocolos TCP e UDP e sobre o conceito de porta de comunicação.

Nesta parte do tutorial mostrei como o conceito de portas é utilizado, na prática, em diversas atividades do dia-a-dia, tais como o acesso a sites da Internet, conexão com um servidor de FTP e conexão com um servidor de Telnet. Na segunda parte do tutorial, você aprendeu sobre o comando netstat.