

Configuração de Endereçamento IP no Equipamento de Acesso à Rede



5

Neste capítulo vamos aprender a configurar um endereço de rede nos equipamentos de acesso a rede. Mas antes de iniciarmos a configuração da rede você precisa compreender os endereços IPs e suas classes.

Neste capítulo você terá subsídios para:

- a) conhecer as classes dos endereços IPs;
- b) conhecer a máscara de rede;
- c) aprender a configurar um endereço IP no Windows;
- d) aprender a configurar um endereço IP no Linux;
- e) compreender o que é um gateway.

Para iniciar o capítulo, veja o que é um endereçamento IP. Vamos lá?

5.1 ENDEREÇAMENTO IP

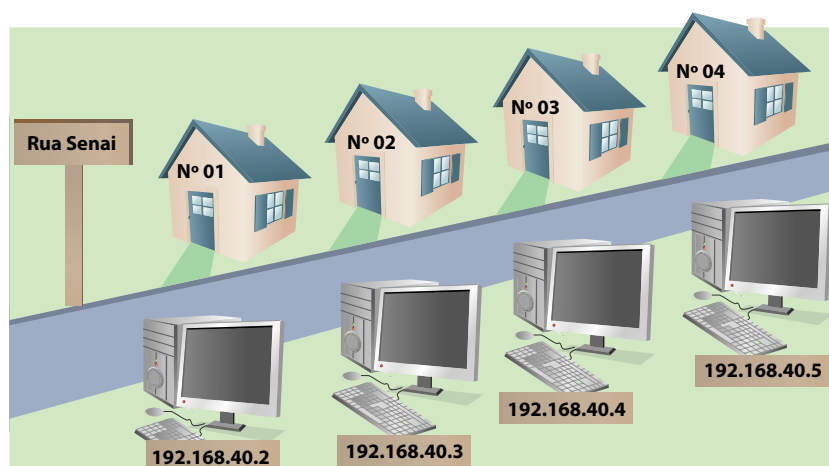
Toda configuração de rede em qualquer máquina ou dispositivo de rede deve possuir os seguintes endereços:

- IP;
- máscara de rede;
- gateway.

O endereço IP é um endereço único que cada equipamento (dispositivo de rede) possui em uma rede. Ele possui um tamanho de 32 bits divididos em 4 octetos de 8 bits separados por um ponto (.), como mostra o exemplo:

Binário: 11000000.10101000.00101000.01111111

Decimal: 192. 168. 40. 127



Denis Pachter (2012)

Figura 28 - Analogia número das casas/endereço IP

Como já falamos, o endereço está dividido em 4 octetos e cada octeto pode variar de zero (0) até 255. Vamos entender.

Cada posição binária possui um valor, como mostrado abaixo:

Tabela 1 - Tabela Binária

1	1	1	1	1	1	1	1	POSIÇÕES BINÁRIAS
128	64	32	16	8	4	2	1	= 255

Para entendermos como funciona o cálculo dos binários para decimal, basta apenas realizar a soma das posições que possuem 1 (um).

Ex:

1 1 0 0 0 0 0

128 + 64 = 192

5.1.1 CLASSES DOS ENDEREÇOS

Os endereços IPs estão divididos em quatro classes distintas, que servem para identificar quantos bits estão sendo utilizados para rede e quantos estão sendo utilizados para a máquina. As classes estão divididas da seguinte forma: classe A, classe B, classe C, classe D e classe E. Vamos estudar apenas as classes A, B e C, que são as mais utilizadas.

CLASSE A

Também conhecidas como redes /8, as redes desta classe possuem grande quantidade de máquinas.

- Os 8 bits primeiros representam a rede.
- Os 24 bits restantes representam as máquinas.
- Cada rede possui 16.777,224 ($2^{24}-2$) milhões de máquinas por rede.
- O intervalo de rede 1.0.0.0 a 126.255.255.255.

Tabela 2 - Intervalo de rede classe A

REDE ID	MÁQUINAS ID
1	. 0 . 0 . 0

CLASSE B

Também conhecidas como redes /16, as redes desta classe possuem uma quantidade de máquinas relativamente pequena.

- Os 16 bits primeiros representam a rede.
- Os 16 bits restantes representam as máquinas.
- Cada rede possui 65.536 ($2^{16}-2$) mil máquinas por rede.
- O intervalo de rede 128.0.0.0 a 191.255.0.0.

Tabela 3 - Intervalo de rede classe B

REDE ID	MÁQUINAS ID
128	. 0 . 0 . 0

CLASSE C

Também conhecidas como redes /24, as redes desta classe possuem uma pequena quantidade de máquinas.

- a) Os 24 bits primeiros representam a rede.
- b) Os 8 bits restantes representam as máquinas.
- c) Cada rede possui 256 (2^8-2) máquinas por rede.
- d) O intervalo de rede 192.0.0.0 a 223.255.255.0.

Tabela 4 - Intervalo de rede classe C

REDE ID				MÁQUINAS ID			
192	.	0	.	0	.	0	



FIQUE ALERTA

Para descobrir qual a classe da rede do endereço IP, observe apenas o primeiro octeto do número IP e analise o intervalo de rede de cada classe.

5.2 MÁSCARA DE REDE

Cada classe de rede possui uma máscara de padrão. As máscaras possuem uma função importante nos endereços IP, que é definir a qual rede o endereço pertence.

Classe A

255.0.0.0

Classe B

255.255.0.0

Classe C

255.255.255.0



VOCÊ SABIA?

Que a versão atual do endereçamento IP é chamada de endereçamento IPv4 e que a nova versão do endereçamento IP é o IPv6, que terá mais endereços disponíveis?

5.3 GATEWAY

O endereço *gateway* da rede é muito importante, pois é ele que define o ponto de entrada e saída da rede. Sempre que um equipamento (computador) não conhece o caminho para onde enviar a mensagem, esta será enviada para o *gateway*, que informará o caminho correto para a entrega da mensagem.

O *gateway* pode ser um computador ou um roteador, na maioria das vezes é o roteador que faz as vezes de *gateway*.

5.4 CONFIGURANDO O ENDEREÇO IP NO WINDOWS 7

A configuração do endereço de rede do computador em um ambiente com sistema operacional Windows 7 é bastante simples. Vamos acompanhar os passos abaixo:

PASSO 1:

Verificar se a placa de rede está instalada e configurada em seu equipamento corretamente.

Clicar em:

Iniciar > Painel de controle > Sistemas > Gerenciador de dispositivos > Duplo clique em adaptadores de rede.

Após executar essa ação, na tela do computador deverá aparecer da forma como mostra a figura. O modelo da placa de rede pode ser diferente, pois nem todos os equipamentos possuem o mesmo modelo.

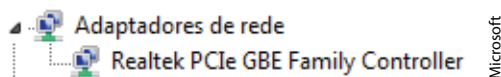


Figura 29 - Verificação de placa de rede



FIQUE ALERTA

Se ao clicar no adaptador de rede não estiver nenhum adaptador configurado, deverá ser efetuada a instalação de uma placa de rede. Havendo um adaptador e com um ponto de interrogação em amarelo, deverá ser verificado se o *drive* da placa está instalado.

PASSO 2:

Após a verificação do adaptador de rede, vamos à configuração do endereço IP.

Clicar em:

Iniciar > Painel de controle > Sistemas > Gerenciador de dispositivos > Central de rede e compartilhamento > Alterar as configurações do adaptador.

Irá surgir uma tela com os adaptadores, como mostra a tela abaixo.



Figura 30 - Tela com adaptadores

PASSO 3:

Clique com o botão direito do *mouse* no **adaptador de rede** que você irá configurar. Nesse caso, iremos configurar a placa de rede com fio ou conexão local.



Figura 31 - Propriedades da placa de rede

PASSO 4:

Na tela propriedades de conexão local, selecione TCP/IP Versão 4 (TCP/IPv4) e clique em **Propriedades**, como mostra a tela abaixo.

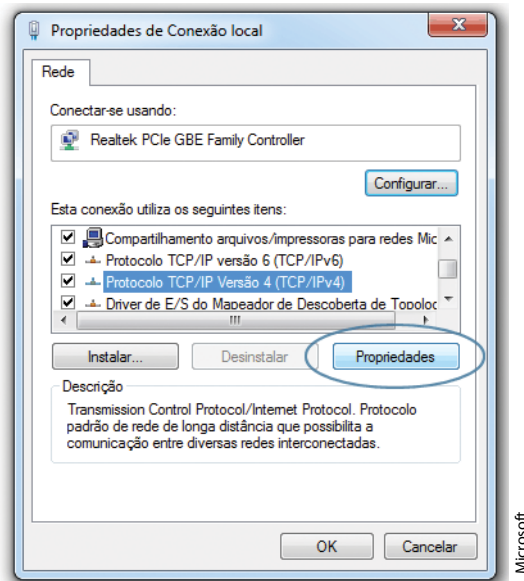


Figura 32 - Propriedades de conexão local

PASSO 5:

Na tela propriedades de protocolo TCP/IP Versão 4 (TCP/IPv4), clique em **Usar o seguinte endereço IP** e insira o endereço de rede como mostra a tela abaixo. Tenha em mãos o endereço que irá configurar.

No exemplo abaixo iremos utilizar um endereço IP de classe C.

IP: 192.168.10.2

Máscara de rede: 255.255.255.0

Gateway: 192.168.10.1

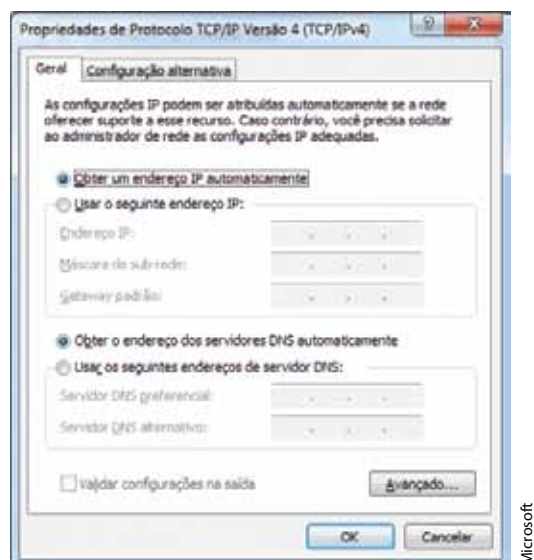


Figura 33 - Propriedades de protocolo TCP/IP Versão 4 (TCP/IPv4)

Após a configuração do endereço IP clique em OK e pronto! Está configurado o IP de forma manual no Windows 7.

5.5 CONFIGURANDO ENDEREÇO IP NO LINUX

No Linux a maneira de configurar o endereço IP é um pouco diferente do Windows, por ser em modo texto, mas é bastante simples. Acompanhe.



SAIBA MAIS

Lendo o livro de Marco Aurélio Filippetti, CCNA 4.1, você terá mais informações sobre os endereços IPs.

PASSO 1:

Estando logado no Linux, vamos trocar para o usuário *root* (usuário com poderes administrativos). Acompanhe as telas.

Digite “su” e pressione *enter* e digite a senha do usuário *root* e pressione *enter*.

```
mauro@asterisk:~$ su
Senha:
```

Linux

Figura 34 - Usuário root

```
root@asterisk:~#
root@asterisk:~#
root@asterisk:~#
root@asterisk:~#
root@asterisk:~#
```

Linux

Figura 35 - Tela usuário máster



FIQUE ALERTA

Sempre que for configurar um endereço IP em um dispositivo de rede, seja ele qual for, nunca se esqueça de informar as três informações mais importantes de uma configuração de endereço de rede: IP, máscara e *gateway*.

PASSO 2:

Depois de feita a troca do usuário comum para usuário master, vamos configurar o endereço de rede.

No Linux, para se configurar o endereço IP de forma manual, devemos configurar o arquivo interfaces que está localizado em `/etc/network`. Para editarmos vamos usar o editor de arquivos “nano”. Vamos à configuração.

Digite o comando abaixo para editar o arquivo interfaces.

```
#nano /etc/network/interfaces
```

Após o comando o arquivo interfaces será mostrado na tela. O arquivo interfaces vem configurado de forma automática (dhcp).

Com o arquivo aberto localize a linha:

```
iface eth0 inet dhcp
```

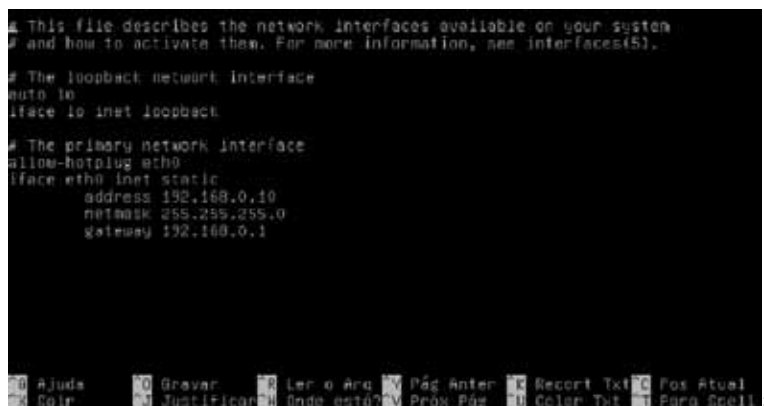
Altere o dhcp por static e acrescente o número IP, máscara e gateway, ficando desta forma:

```
iface eth0 inet static
```

```
Address 192.168.0.10
```

```
Netmask 255.255.255.0
```

```
Gateway 192.168.0.1
```



```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
    address 192.168.0.10
    netmask 255.255.255.0
    gateway 192.168.0.1
```

Figura 36 - Arquivo interfaces



CASOS E RELATOS

Portão errado

O caso aconteceu na Infraero de Florianópolis. A empresa recebeu computadores novos para substituição do parque de tecnologia. Realizada a troca, todos os equipamentos estavam funcionando corretamente. Um determinado dia, o setor de TI começou a receber ligações dizendo que os computadores não estavam acessando a rede. O técnico foi até o local e constatou o problema de acesso.

Realizaram testes nos cabos, nos *switches*, nas placas de redes e nenhum problema foi encontrado. Até que alguém teve a ideia de verificar se a máquina estava pegando IP, abrindo o *prompt* do MS-DOS e executando o comando *ip config*. A resposta foi:

IP = 10.112.13.40

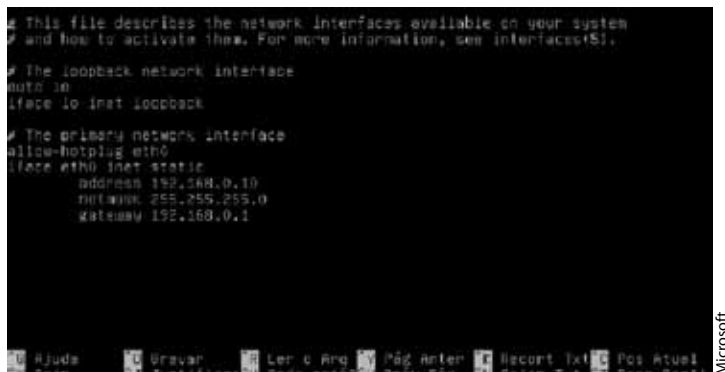
Máscara = 255.255.254.0

Gateway= 10.112.13.1

Perceberam então que quem havia trocado os computadores configurou a máscara de rede das máquinas do setor e por engano colocou 255.255.254.0 em vez do padrão 255.255.255.0, tirando assim as máquinas da rede das demais da Infraero. Foi realizada a troca da máscara e todos voltaram a se comunicar na rede.

PASSO 3:

Para salvar as alterações realizadas no arquivo *interfaces* pressione a tecla "ctrl" + "o" e pressione *enter*. Depois pressione "ctrl" + "x" para sair do arquivo.



```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
    address 192.168.0.10
    netmask 255.255.255.0
    gateway 192.168.0.1
```

Figura 37 - Salvando o arquivo interfaces

PASSO 4:

Depois de realizada a configuração do arquivo interfaces, devemos reiniciar o Linux ou resetar o serviço de rede com o comando abaixo. Digite o comando e pressione a tecla enter.

```
#restart /etc/init.d/networking
```

Desta forma está realizada a configuração do endereço no sistema operacional Linux.



RECAPITULANDO

Neste capítulo você foi apresentado às classes de endereçamento IP, conhecendo as três classes de endereços, A, B e D. Aprendeu que cada classe possui uma determinada quantidade de computadores, viu como configurar um endereço de rede em sistema operacional Windows e Linux e como é importante a perfeita configuração.

Protocolos de Rede e Suas Funcionalidades



6

Neste capítulo você será apresentado a alguns protocolos de rede bastante utilizados, que possuem um papel importante nas redes de computadores.

Neste capítulo você terá subsídios para:

- a) conhecer os protocolos de rede;
- b) compreender a funcionalidade dos protocolos de rede.

Vamos começar conhecendo os protocolos?

6.1 ICMP

O *Internet Control Message Protocol* é um protocolo que faz parte do protocolo IP (*internet protocol*). Sua finalidade é fornecer erros a sua fonte de origem e apenas reportar erros no nível do endereço IP de origem.

6.2 IP

O *Internet Protocol* é um protocolo que é responsável por elaborar e transportar os pacotes de dados através da rede.

6.3 TCP

O *Transfer Control Protocol* é um protocolo para envio de pacotes da camada de transporte do modelo OSI. O TCP é um protocolo confiável, pois possui garantia de entrega nos pacotes enviados.



**SAIBA
MAIS**

Quer saber mais sobre a camada de transporte e as outras camadas do modelo OSI, que são sete, leia o livro de Marco Aurélio Filippetti, CCNA 4.1, que terá um conhecimento profundo das sete camadas do modelo OSI.

6.4 UDP

O *User Datagram Protocol* é um protocolo para envio de pacotes da camada de transporte do modelo OSI. O UDP é um protocolo não confiável, pois não possui garantia de entrega nos pacotes enviados.



**VOCÊ
SABIA?**

Que o YouTube disponibiliza suas imagens através de protocolos UDP, sem nenhum tipo de garantia?

6.5 DNS

O *Domain Name System* é um protocolo responsável pela resolução dos nomes das máquinas, ou seja, resolve o endereço IP em nome de máquina. Desta forma é permitido acessar computadores e dispositivos de rede sem a necessidade de conhecimento do endereço IP do equipamento.

FUNCIONAMENTO DO DNS

O funcionamento do DNS é bastante simples. Quando você digita um endereço em um navegador (ex. www.sc.senai.br), no momento em que é pressionado o botão *enter*, o seu computador irá fazer uma consulta em um servidor DNS mais próximo para resolver o endereço IP do endereço digitado no navegador.

Se o servidor não souber resolver o endereço, este servidor irá realizar a consulta em outro servidor DNS.

6.6 DHCP

É através do *Dynamic Host Configuration Protocol* (protocolo de configuração dinâmica de endereço de rede) que equipamentos em rede recebem suas configurações de rede como IP, máscara e *gateway* de forma automática.

FUNCIONAMENTO DO DHCP

A máquina que irá solicitar o IP envia o pacote em *broadcast* para o endereço 255.255.255.255, que é enviado para todas as máquinas da rede e que será recebido pelo servidor ou equipamento responsável por fornecedor IP. Este recebe o pacote e devolve um pacote destinado ao endereço 0.0.0.0 que é enviado para toda a rede e que será lido apenas pela máquina que solicitou o IP. Isto acontece porque o pacote que contém o endereço IP, máscara e *gateway* é enviado para o endereço MAC do equipamento.

6.7 FTP

O *File Transfer Protocol* é um protocolo para transferência de arquivos na *internet*, é o protocolo padrão para transferência na pilha de protocolos TCP/IP.

FUNCIONAMENTO DO FTP

A transferência do arquivo acontece através de uma solicitação de um computador (cliente) para um computador (servidor). É necessário que exista um usuário e senha previamente cadastrados no servidor FTP, para que seja liberado o acesso ao servidor.

Para que uma máquina seja considerada um servidor FTP é necessária a instalação de um *software* específico (ex. Filezilla, Cesar, TFTP Server 9.1, Cerberus FTP Server).

6.8 TFTP

O *Trivial File Transfer Protocol* é um protocolo semelhante ao FTP utilizado para transferência de arquivo. Esse protocolo, por trabalhar com o protocolo UDP, não necessita de usuário e senha, é considerado mais simples que o protocolo FTP.



FIQUE ALERTA

Sempre que for configurar um servidor de arquivos FTP, nunca esqueça de criar um usuário *master*, com permissões de alterações e um usuário comum, com permissão apenas para baixar arquivos.

6.9 SSH

O *Secure Shell* é um serviço que cria um canal seguro de comunicação entre um usuário remoto e o servidor de rede ou entre máquinas. Nesse canal todo tráfego é criptografado e, caso alguém queira capturar os pacotes para possíveis tentativas de quebra, não irá ter sucesso.

Esse serviço é quase um padrão nas distribuições GNU/Linux porque o SSH proporciona segurança ao sistema e isso sempre agrega mais estabilidade, principalmente em servidores de rede que necessitam trabalhar com missão crítica. Pode ser utilizado também para conexão entre máquinas Windows e Linux.



CASOS E RELATOS

FTP gratuito

Uma escola de São José necessitava de um servidor para disponibilizar arquivos para seus alunos, algo que fosse confiável e seguro. Solicitou orçamento de algumas empresas e os valores foram altos, fazendo o diretor desistir de ter um servidor de arquivos para a escola. Em conversa com esse diretor, passei algumas ideias para que ele criasse um servidor de FTP. Indiquei que ele utilizasse o Filezilla, pois é um programa para FTP gratuito, e passei também indicações de como configurar o programa.

Passado algum tempo, fui até a escola para conversar com o diretor sobre outro assunto. Em meio à conversa, ele me relatou que havia baixado o Filezilla e configurado um usuário para os alunos, e que todos estavam adorando o funcionamento do programa. Essa foi uma solução gratuita e de muita utilidade, sendo que um diretor sem conhecimento nenhum de informática montou um servidor FTP para mais de 700 alunos. Isso mostra como não é difícil aprender a configurar uma rede ou um servidor.

FUNCIONAMENTO DO SSH

Vamos detalhar o funcionamento do SSH no Windows e Linux.

Windows – para realizar uma conexão entre uma máquina Windows e uma Linux com o SSH é necessário o programa *Putty*. É um programa que não é necessário instalar, basta baixar o aplicativo através do site <www.superdownloads.com.br/> para sua máquina executá-lo e informar o endereço da máquina Linux que deseja acessar, como mostrado abaixo.

Em *host name (or IP address)* insira o nome ou endereço.

Em *Port* deixe 22 mesmo (que é a porta padrão do SSH).

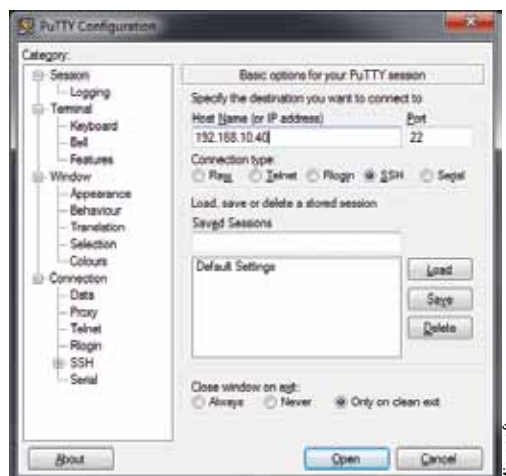


Figura 38 - Putty

Linux – no Linux a conexão também é bastante simples, apesar de ser através de comandos.

Primeiro vamos instalar o SSH no Linux. Digite o comando:

```
#apt-get install openssh-server
```

Após a execução deste comando o serviço SSH está instalado.

Para acessar uma máquina Linux através de outra máquina Linux basta apenas executar o comando abaixo:

```
#ssh suporte@192.168.10.40
```

Legenda:

SSH – comando.

suporte – usuário cadastrado na máquina remota.

@192.168.10.40 – endereço da máquina remota.

6.10 TELNET

Esse é um protocolo cliente-servidor também utilizado para comunicação remota entre máquinas. É um protocolo sem segurança, pois os dados não são criptografados.

FUNCIONAMENTO DO TELNET

O acesso remoto entre máquinas utilizando o TELNET é bastante simples. Ele é um protocolo nativo nos sistemas operacionais, por isso não precisamos instalar, a sua execução deve ser realizada através de comandos e através do *prompt* do MS-DOS do Windows. Veja:

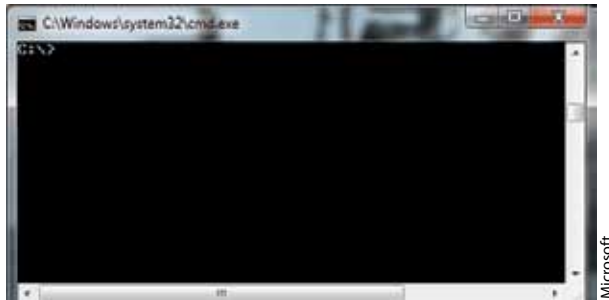


Figura 39 - Tela MS-DOS

C:\telnet 192.168.10.40

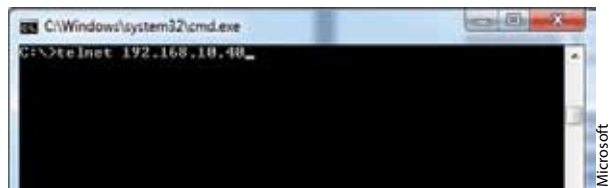


Figura 40 - Telnet



RECAPITULANDO

Neste capítulo você foi apresentado a alguns protocolos de redes, onde descobriu que algumas mensagens possuem garantia de entrega e outras não, através de dois protocolos. Viu também como acessar uma máquina Linux através de uma máquina Windows com o aplicativo *Putty* e que o SSH é um protocolo de comunicação entre máquinas Linux e que seus dados são criptografados, fazendo dele a melhor forma de comunicação entre máquinas Linux e máquinas Windows/Linux.



Este capítulo irá apresentar a você que tão importante quanto saber configurar a rede corretamente é realizar testes para verificar como está a nossa conexão: se está congestionada, com falhas, se possui invasor etc. Os testes de rede são responsáveis pela qualidade da rede e pela segurança dos dados. Vários são os *softwares* responsáveis por esses testes. Você terá oportunidade conhecer alguns durante os estudos deste capítulo.

Neste capítulo você terá subsídios para:

- a) conhecer alguns comandos utilizados para monitoração de rede;
- b) compreender a funcionalidade destes comandos;
- c) conhecer alguns *softwares* para monitoração de rede.

Vamos começar por um comando para testar a conexão entre máquinas. Pronto para prosseguir?

7.1 PING

É um protocolo ICMP utilizado para realização de testes de conexão entre máquinas e dispositivos de rede.



SAIBA MAIS

Quer conhecer outros acessórios do *ping*? Em seu próprio computador acesse o *prompt* do MS-DOS. Digite: *Ping/?*. Com esse comando serão apresentados vários acessórios do comando *ping*.

FUNCIONAMENTO DO PING

Para utilizarmos o *ping* devemos apenas abrir o *prompt* do MS-DOS e digitar *ping 192.168.10.40*.

Executando o *ping*, com o *prompt* do MS-DOS aberto:

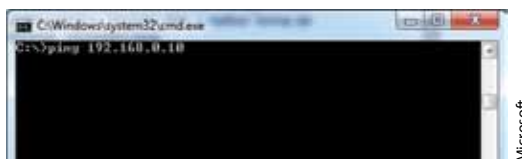


Figura 41 - Ping

Vamos apresentar alguns usos do *ping*:

O *ping* possui alguns acessórios que complementam o comando, que informam ao usuário informações mais detalhadas. Vamos detalhar alguns desses acessórios.

- a) "*-a*": este acessório irá resolver um endereço de IP para um nome de máquina;

Ex. *ping -a 192.168.10.40*

- b) "*-n count*": este acessório determina a quantidade de ecos que o comando *ping* irá enviar a um determinado equipamento. O *ping* padrão executa 4 ecos;

- c) ECO: é o tempo que um *byte* leva para ir e voltar de um computador a outro através do comando *ping*;

Ex. *ping -n 6 192.168.1.40*

(neste exemplo será executado 6 ecos no endereço IP).

- d) "*-t*": este acessório é bastante utilizado; quando colocamos o "*-t*" o comando fica em execução até que o usuário resolva para a execução do comando, pressionando a tecla *ctrl + c*.

Ex. *ping -t 192.168.10.40*

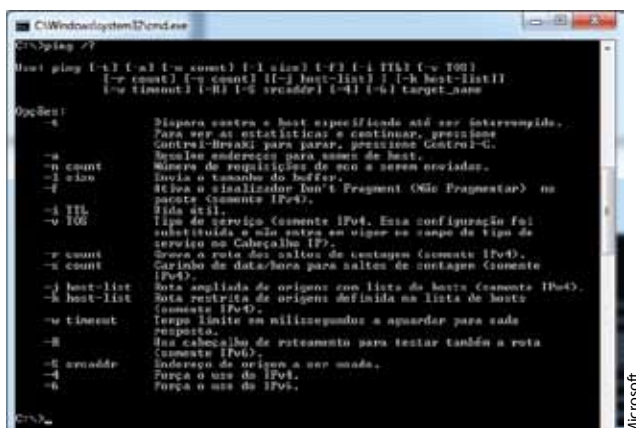


Figura 42 - Ajuda do ping



CASOS E RELATOS

Prata da casa

Uma empresa estava com um problema em sua rede: em alguns momentos no período noturno a rede parava de funcionar, causando falhas nos envios de *backup* para a sua matriz. Foi acionada uma empresa para verificação e esta pediu uma quantia relativamente alta para implementar um programa na rede para verificar em qual horário correto a rede parava de funcionar. Como o valor foi alto, a empresa desistiu.

A empresa possuía um funcionário que era aluno de Ciência da Computação da UFSC, e o funcionário programou um *script* que executa um *ping* para o destino na qual o *backup* seria enviado. Assim, se por acaso o *ping* falha durante a noite, seria gerado um log informando a hora de falha. Uma solução barata, que levou 10 minutos para ser realizada e não houve nenhum custo para a empresa, evitando assim uma despesa desnecessária. Principalmente porque, após os resultados, foi constatado que o problema era causado quando o vigia desligava os disjuntores, sempre às 22h30, voltando a ligar no dia seguinte.

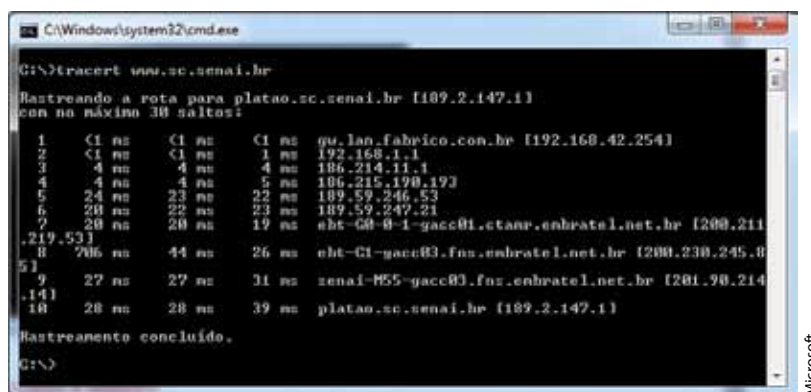
7.2 TRACERT

O *tracert* é um comando responsável por informar os caminhos de todos os roteadores por onde um pacote de dados passa até chegar ao destino.

FUNCIONAMENTO DO TRACERT:

Para utilizar o *tracert* devemos abrir o prompt do MS-DOS e executar o comando *tracert* mais o destino.

Ex. c:\>tracert www.sc.senai.br



```

C:\Windows\system32\cmd.exe
G:\>tracert www.sc.senai.br

Rastreando a rota para platao.sc.senai.br [189.2.147.11]
com no máximo 30 saltos:

 1  0 ms  0 ms  0 ms  gw.lan.fabrico.con.br [192.168.42.254]
 2  1 ms  1 ms  1 ms  192.168.1.1
 3  4 ms  4 ms  4 ms  186.214.11.1
 4  4 ms  4 ms  4 ms  186.215.190.193
 5  24 ms  23 ms  22 ms  189.59.246.53
 6  20 ms  22 ms  23 ms  189.59.247.21
 7  20 ms  20 ms  19 ms  ebt-G0-0-1-gacc01.ctanr.enbratel.net.br [200.211.219.55]
 8  706 ms  44 ms  26 ms  ebt-G1-gacc03.fns.enbratel.net.br [200.230.245.0]
 9  27 ms  27 ms  31 ms  senai-M55-gacc03.fns.enbratel.net.br [201.90.214.141]
10  28 ms  28 ms  39 ms  platao.sc.senai.br [189.2.147.11]

Rastreamento concluído.
G:\>
  
```

Figura 43 - Tracert



FIQUE ALERTA

Ao executar o comando *tracert* e aparecer alguns asteriscos no lugar "ms", isso indica que existe algum erro na localidade.

7.3 SNIFFER PARA REDE

Também conhecidos como "farejadores", são programas utilizados para capturar o tráfego da rede para análise. Com este programa os administradores de redes conseguem verificar que tipo de informação está circulando em sua rede, quais os *sites* que estão sendo acessados.



VOCÊ SABIA?

Que os *sniffers* são programas para verificação de rede? Podem até parecer espiões, mas possuem papel importante no desempenho de uma rede de grande porte.

Os relatórios gerados pelos programas *sniffer* detalham os *sites* acessados e a máquina que originou o acesso ao *site* de origem.

Alguns exemplos de farejadores:

a) TCPDump;

- b) Wireshark;
- c) WinpCap;
- d) SmartSniff.



RECAPITULANDO

Neste capítulo você foi apresentado ao comando *ping*. Apesar de ser um comando bastante simples, possui uma funcionalidade imensa, para verificar a disponibilidade de equipamentos. Viu também que para descobrirmos o caminho completo por onde uma informação passa até chegar a seu destino utilizamos o comando *tracert*. Viu também que existem no mercado diversos programas responsáveis pela monitoração de uma rede, que verificam os *sites* que os computadores estão acessando.