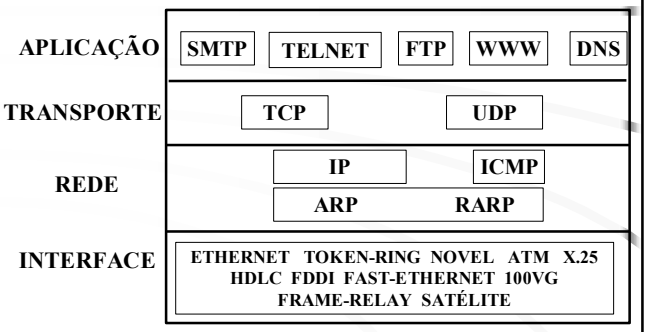
5 - Ferramentas Básicas

Emerson Valdir Pellis

Arquitetura TCP/IP



Protocolo ICMP
Internet Control Message Protocol

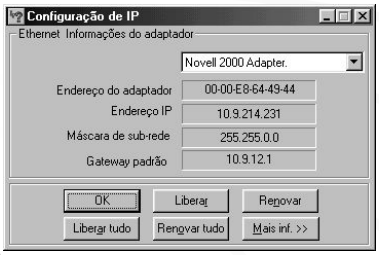
- Obrigatório em implementações da camada IP
- Usado em transferências de mensagens entre roteadores e estações na rede internet
- Usado para **mensagens de erro ou controle:**
  - Ex.: Congestionamento, não consegui rotear um pacote, etc

Protocolo ICMP (cont.)

- Utiliza o IP p/ enviar as mensagens (não tem garantia de entrega)
- Apesar de utilizar os serviços do protocolo IP também é considerado integrante da camada de rede

Obtendo Endereço IP

- **Windows 9X**
  - Programa **winipcfg**



Obtendo Endereço IP (cont.)

- **Windows NT/2000/XP**
  - **ipconfig**
  - **ipconfig /all** (informações detalhadas)
- **Linux**
  - **ifconfig**
    - Além de listar as interfaces, pode ser usado para ligar/desligar uma interface, ou para definir novas interfaces de rede.

PING

- **É utilizado para testar uma conexão.**
- Utiliza-se das mensagens **Echo Request** e **Echo Reply** do protocolo **ICMP** para determinar se uma máquina está ligada e funcional.
- Ele opera enviando um ICMP, se o software de IP da máquina destino recebe-o ele emite uma resposta de echo imediatamente.

PING (cont.)

- **Windows**
  - ping <IP> (dispara o echo 4 vezes)
  - ping -t <IP> (tempo indeterminado)
  - ping -l <IP> (tamanho do buffer)
  - ping /? (outras opções)

PING (cont.)

- **Linux**
  - ping <IP> (dispara o echo)
  - ping -s <IP> (tamanho do buffer)
  - outras opções: man ping
- Pelo TTL (Time to Live) podemos determinar o S. O. do "Alvo"

PING (cont.)

- ***DoS - Denial of Service***
  - Envio indiscriminado de requisições a um computador alvo, visam causar a indisponibilidade dos serviços oferecidos por ele.
- ***DDoS - Distributed Denial of Service***
  - Ataques DoS diferentes partindo de várias origens, disparados simultânea e coordenadamente sobre um ou mais alvos.

PING (cont.)

- Exemplo: **Ping of DEATH**
  - Ataque baseado em mensagens ICMP muito longas.
  - Atacando:
  - ping –l 65510 <Endereço IP>
  - Defendendo:
  - Filtro ICMP (Firewall)

Loopback

- **Utilizado pela máquina local para testar sua interface de comunicação.**
- A faixa 127.xx.yy.zz é reservada para teste de loopback (Ex.: 127.0.0.1).
- Datagrama com este endereço não trafega na rede.
- O datagrama retorna "antes" de ir.

Loopback

- Exemplo da utilização do loopback:
  - **ping 127.0.0.1**

Disparando contra 127.0.0.1 com 32 bytes de dados:
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128

O que podemos determinar com este comando?

Trace Route

- **Permite a determinação da rota a partir de uma máquina até seu destino.**
- Windows 9X/NT/2K
  - tracert <IP destino>
- Linux
  - traceroute <IP destino>

Trace Route

- O **traceroute** do **Unix/Linux** trabalha com pacotes **UDP**, o **tracert** trabalha com pacotes ICMP. Para usar pacotes ICMP com traceroute, pode ser usada a opção -I.
- Com este comando é possível tirar conclusões sobre a topologia da rede pesquisada.

PathPing

- Permite a determinação da rota a partir de uma máquina até seu destino, gerando detalhes sobre encaminhamento e perda de pacotes em cada roteador.
- **Windows 2000/XP**
  - **pathping [opções] destino**
- Detalhes:
  - pathping /?

PathPing

- Exemplo:

```
pathping.exe -n 201.14.143.254

Rastreando a rota para 201.14.143.254 com no máximo 30 saltos

  0  201.3.214.132
  1  201.14.143.254

Calculando estatísticas para 25 segundos...
           Origem aqui   Este nó/vínculo
Salto  RTT    Perdido/Enviado = Pct  Perdido/Enviado = Pct
  0                                        201.3.214.132
                               0/ 100 =  0%   |
  1   52ms     0/ 100 =  0%     0/ 100 =  0%  201.14.143.254

Rastreamento concluído.
```


NetStat

- Permite obter informações e estatísticas sobre serviços e conexões de rede.
- Windows
  - netstat (Conexões ativas)
  - netstat -a (Conexões e portas de escuta)
  - netstat -r (Tabela de roteamento)
  - netstat -s (Estatísticas)

NetStat

- Linux
  - netstat (Conexões ativas)
  - netstat -a (Conexões e portas de escuta)
  - netstat -r (Tabela de roteamento)
  - netstat -s (Estatísticas)
  - netstat -l (portas ativas)
  - man netstat (muitas outras opções)

Qual programa está escutando qual porta?

- Windows XP com SP2
  - **netstat /ba**
- Windows XP com SP1 ou inferior:
  - Esta pergunta pode ser respondida com o programa **insider**, disponível em:
    - **http://www.ntsecurity.nu/toolbox/inzider**

Qual programa está escutando qual porta? (cont.)

- Linux (cont.)
  - **netstat -l** (exibe os programas que estão ouvindo em cada porta)
  - **netstat -l -p** (exibe os programas)
  - **ps -aux |grep <PID>** reconhece o programa

Qual programa está escutando qual porta? (cont.)

- Listas de portas podem ser encontradas em:
  - **http://www.iss.net/security_center/advice/Exploits/Ports/default.htm**
  - **http://www.seifried.org/security/ports**

DNS - Domain Name Service

- Sistema hierárquico distribuído;
- Tradução de nomes para números IP;
- Não existe um repositório único de informações;
- Informação distribuída entre milhares de computadores;
- Estrutura em árvore, semelhante à estrutura de diretórios de sistemas Unix.

Registro de Domínios

- NIC - Network Information Center
- No Brasil:
  - **FAPESP** (Fundação de Amparo à Pesquisa de São Paulo) - http://registro.br
- No mundo - Vários locais:
  - **Registrocom.com** http://www.registrocom.com

NSLOOKUP

- **Ferramenta utilizada para interrogar servidores de nomes;**
- Permite a qualquer usuário consultar um servidor de nomes e recuperar qualquer informação conhecida por este servidor;
- Extremamente útil para identificar problemas com servidores de nomes;
- Consulta a servidores remotos.

NSLOOKUP (cont.)

- Windows NT/2000/XP e Linux
  - O nslookup pode ser utilizado de duas maneiras:
- **Modo não interativo**
  - As opções são passadas na linha de comando.
- **Modo interativo**
  - As opções são digitadas no prompt interno do comando.

NSLOOKUP (cont.)

- **Modo não interativo**
  - nslookup unerj.br (informações geral)
  - nslookup -q=MX unerj.br (informação do server de e-mail)
  - nslookup terra.com.br

NSLOOKUP (cont.)

- Modo interativo
  - nslookup
    - www.terra.com.br (Exibe diretamente o IP)
      Nome = www.terra.com.br
      Address: 200.176.3.142
    - exit (Sair do comando)

NSLOOKUP (cont.)

- Modo interativo (cont.)
  - nslookup
    - **server** ns.nasa.gov (alterna para outro server)
    - cade.com.br (consulta)
    - terra.com.br (consulta)
    - exit (Sair do comando)

NSLOOKUP (cont.)

- Modo interativo (cont.)
  - nslookup
    - set type=mx (verifica server e-mail)
    - unerj.br
    - set type=any (todas as opções)
    - unerj.br
    - exit (Sair do comando)

Verificar DNS

- Para verificar problemas ou informações do DNS de um domínio:
  - **http://www.dnsstuff.com**
    - **DNS Report**
    - **Spam database lookup**
    - **Reverse DNS lookup**
    - **WHOIS Lookup**
    - **DNS lookup**

TELNET

- Usado para estabelecer sessões de trabalho (não seguras).
- O TELNET é também pode ser utilizado para testar alguns protocolos e verificar banners de programas.

TELNET (cont.)

- Windows 2000/XP
  - **telnet** (executa o comando)
    - **set localecho** (ativa retorno dos comandos)
    - **help** (lista comandos disponíveis)
    - **open unerj.br 25**
      (Abre uma conexão no servidor e verifica serviço de e-mail está ativo neste servidor)
    - **quit** (fecha a conexão)

TELNET (cont.)

- Enviando e-mail por telnet no servidor:
  - **SMTP relay** é a retransmissão ou encaminhamento de e-mail para um servidor. Existem dois tipos de relay:
  - **Relay Interno –** utilizado normalmente pelos programas de e-mail.
  - **Relay Externo –** Utilizado por spanners e normalmente rejeitado pelos servidores.

TELNET (cont.)

- telnet
  - **set localecho** <enter>
  - **open unerj.br 25**
  - **HELO** unerj.br <enter>
  - **MAIL FROM:** email@unerj.br <enter>
  - **RCPT TO:** EMAIL@unerj <enter>
  - **DATA** <enter>
    <digite o conteúdo do email>
    Para encerrar: digitar "**.**" (ponto) em nova linha.
  - **QUIT** <enter>

Programas

- **3D Traceroute** (Windows)
  - Várias ferramentas em uma:
    - traceroute, ping, netstat e etc...
  - http://www.hlembke.de/prod/3dtraceroute/
- **Enhanced Ping** (Windows)
  - Ping e traceroute gráficos
  - http://www.itoolpad.com/products/eping/