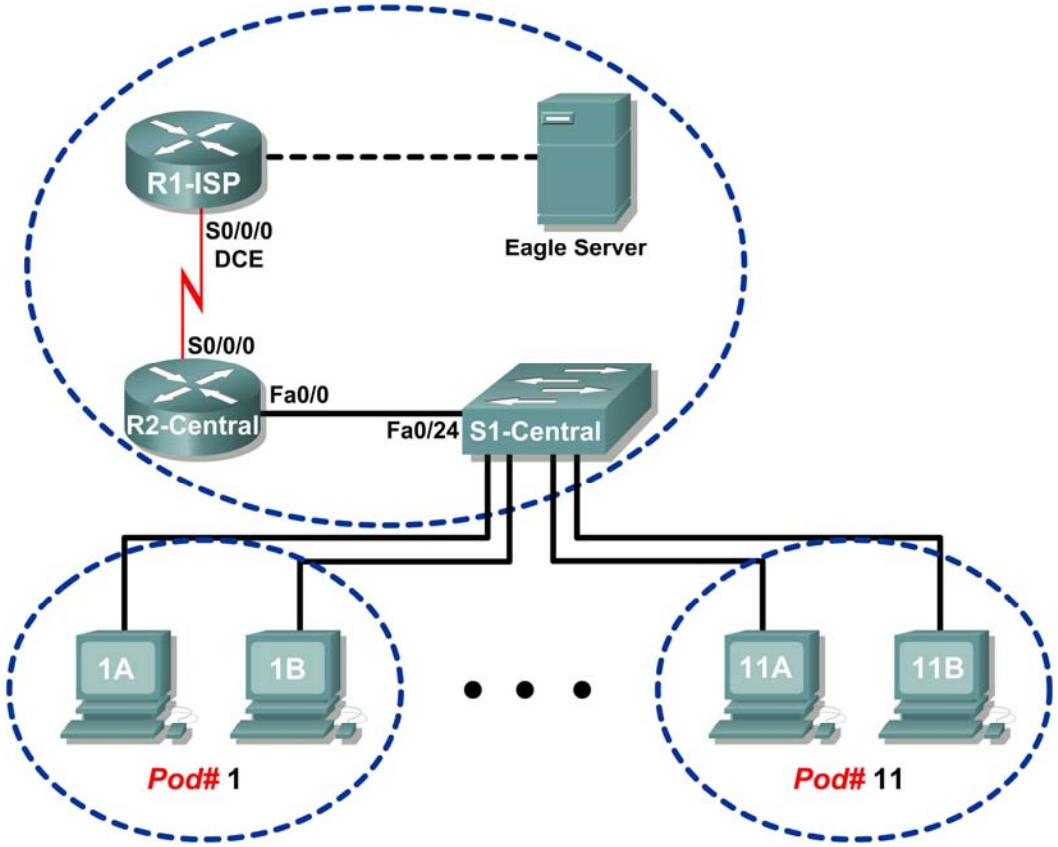
# Laboratório 4.5.1: Observando TCP e UDP usando Netstat

## Diagrama de Topologia




## Tabela de Endereçamento

| Dispositivo | Interface | Endereço IP | Máscara de Sub-Rede | Gateway Padrão |
|---|---|---|---|---|
| **R1-ISP** | **S0/0/0** | **10.10.10.6** | **255.255.255.252** | *N/A* |
| | **Fa0/0** | **192.168.254.253** | **255.255.255.0** | *N/A* |
| **R2-Central** | **S0/0/0** | **10.10.10.5** | **255.255.255.252** | **N/A** |
| | **Fa0/0** | **172.16.255.254** | **255.255.0.0** | *N/A* |
| **Eagle Server** | *N/A* | **192.168.254.254** | **255.255.255.0** | **192.168.254.253** |
| | *N/A* | **172.31.24.254** | **255.255.255.0** | *N/A* |
| **host***Pod#***A** | *N/A* | **172.16.***Pod#***.1** | **255.255.0.0** | **172.16.255.254** |
| **host***Pod#***B** | *N/A* | **172.16.***Pod#***.2** | **255.255.0.0** | **172.16.255.254** |
| **S1-Central** | *N/A* | **172.16.254.1** | **255.255.0.0** | **172.16.255.254** |

## Objetivos

- Explique parâmetros e saídas do comando **netstat** comum.
- Usar **netstat** para examinar informação de protocolo em um computador.

## Contexto

**netstat** é uma abreviatura para o utilitário de estatística de rede, disponível nos computadores Windows e Unix / Linux. Passar parâmetros opcionais com o comando alterará informações de saída. O **netstat** exibe conexões de rede de entrada e saída (TCP e UDP), informações da tabela de roteamento do computador e estatísticas de interface.

## Cenário

Neste laboratório, o aluno examinará o comando **netstat** em um computador e ajustará as opções de saída do **netstat** para analisar e entender e o status do protocolo da Camada de Transporte TCP/IP.

### Tarefa 1: Explique parâmetros e saídas do comando netstat comum

Abra uma janela do terminal clicando em Iniciar | Executar. Digite **cmd** e pressione **OK**.

Para exibir informações de ajuda sobre o comando **netstat**, use as opções **/?**, como exibido:

```
C:\> netstat /? <ENTER>
```

Use a saída do comando **netstat** /? como referência para preencher a opção adequada que melhor se adeque à descrição:

| Opção | Descrição |
|---|---|
| | Exibir todas as conexões e portas de monitoramento. |
| | Exibir endereços e números de porta em forma numérica. |
| | Re-exibir estatísticas a cada cinco segundos. Pressione CTRL+C para parar a re-exibição das estatísticas. |
| | Mostra conexões para o protocolo especificadas por proto; proto pode qualquer um dos seguintes: TCP, UDP, TCPv6 ou UDPv6. Se usado com a opção –s exibi estatística por protocolo, proto pode ser qualquer um dos seguintes: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP ou UDPv6. |
| | Re-exibir todas as conexões e portas de monitoria a cada 30 segundos. |
| | Exibir somente conexões abertas. Esse é um problema complicado. |

Quando as estatísticas **netstat** são exibidas para conexões TCP, o estado TCP é exibido. Durante o tempo de uma conexão TCP, a conexão passa por uma série de estados. A tabela a seguir é um resumo

de estados TCP, compilados do RFC 793, Transmission Control Protocol, setembro de 1981, conforme informado pelo **netstat**:

| Estado | Descrição da Conexão |
|---|---|
| OUVIR | A conexão local está esperando uma solicitação de conexão de qualquer dispositivo remoto. |
| ESTABELECIDO | A conexão está aberta e dados podem ser trocados através da conexão. Este é o estado normal para a fase de transferência de dados da conexão. |
| TEMPO-ESPERA | A conexão local está esperando um período padrão de tempo após enviar uma solicitação de término de conexão antes de fechar a conexão. Esta é uma condição normal e irá normalmente durar entre 30 - 120 segundos. |
| FECHAR-ESPERA | A conexão está fechada, mas está esperando uma solicitação de término do usuário local. |
| SYN-ENVIADO | A conexão local está esperando uma resposta após enviar uma solicitação de conexão. A conexão deve passar por uma rápida transição por este estado. |
| SYN_RECEBIDO | A conexão local está esperando uma confirmação da solicitação de confirmação de conexão. A conexão deve passar por uma rápida transição por este estado. Múltiplas conexões no estado SYN_RECEBIDO podem indicar um ataque TCP SYN. |

Endereços IP exibidos pelo **netstat** entram em várias categorias:

| Endereço IP | Descrição |
|---|---|
| 127.0.0.1 | Este endereço se refere ao host local, ou a este computador. |
| 0.0.0.0 | Um endereço global, significando "QUALQUER". |
| Endereço Remoto | O endereço do dispositivo remoto que tem uma conexão com este computador. |

## Tarefa 2: Usando netstat para Examinar Informações de Protocolo em um Computador

### Passo 1: Usar netstat para visualizar conexões existentes.

Da janela do terminal na Tarefa 1, acima, emita o comando **netstat –a**:

```
C:\> netstat –a <ENTER>
```

Uma tabela será exibida listando o protocolo (TCP e UDP), o endereço Local, o endereço Externo e informações de Estado. Endereços e protocolos que podem ser traduzidos em nomes são exibidos.

A opção –n força o netstat a exibir a saída em formato bruto. Da janela do terminal, emita o comando **netstat –an**:

```
C:\> netstat –an <ENTER>
```

Use a barra de rolagem vertical da janela para ir e voltar entre as saídas dos dois comandos. Compare as saídas, anotando como os números de portas conhecidos são alterados a nomes.

Escreva três conexões TCP e três UDP da saída **netstat –a**, e os números de porta traduzidos correspondentes da saída **netstat –an**. Se houver menos de três conexões que traduzem, anote isso na sua tabela.

| Conexão | Proto Endereço Local Endereço Externo Estado |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Consulte a seguinte saída **netstat**. Um novo engenheiro de rede suspeita que seu computador foi comprometido por um ataque externo contras as portas 1070 e 1071. Como você responderia?

```
C:\> netstat –n
Conexões Ativas
Proto  Endereço Local         Endereço Externo         Estado
TCP    127.0.0.1:1071         127.0.0.1:1070         ESTABELECIDO
TCP    127.0.0.1:1071         127.0.0.1:1070         ESTABELECIDO
C:\ >
```

_____

_____

**Passo 2: Estabelecer múltiplas conexões TCP concomitantes e registrar a saída netstat.**

Nesta tarefa, várias conexões simultâneas serão feitas com o Eagle Server. O comando **telnet** venerável será usado para acessar os serviços de rede do Eagle Server, fornecendo, assim, vários protocolos para examinar com o netstat.

Abra quatro adicionais janelas de terminais. Arrume as janelas para que todas fiquem visíveis. As quatro janelas de terminal que serão usadas para conexões telnet ao Eagle Server podem ser relativamente pequenas, aproximadamente ½ tela de largura por ¼ de altura da tela. As janelas de terminal que serão usadas para recolher informações de conexão devem ter ½ tela de largura por altura de tela cheia.

Vários serviços de rede no Eagle Server responderão a uma conexão telnet. Nós usaremos:

- Servidor de nome de domínio DNS-, porta 53
- Servidor FTP- FTP, porta 21
- Servidor de e-mail SMTP- SMTP, porta 25
- Servidor TELNET- Telnet, porta 23

Por que o telnet às portas UDP falharia?

_____

_____

Para fechar uma conexão telnet, pressione as teclas <CTRL> ] juntas. Isso trará o prompt telnet, Microsoft Telnet>. Digite **sair <ENTER>** para fechar a sessão.

Na primeira janela do terminal telnet, conecte-se ao Eagle Server na porta 53. Na segunda janela do terminal, conecte-se à porta 21. Na terceira janela do terminal, conecte-se à porta 25. Na quarta janela do terminal, conecte-se à porta 23. O comando para uma conexão telnet na porta 21 é exibido abaixo:

```
C:\>telnet eagle-server.example.com 53
```

Na grande janela do terminal, registre conexões estabelecidas com o Eagle Server. A saída deve parecer similar ao seguinte. Se a digitação estiver devagar, uma conexão poderá se fechar antes de todas as conexões terem sido feitas. Possivelmente, as conexões devem finalizar por inatividade.

```
Proto  Endereço Local         Endereço Externo         Estado
TCP    192.168.254.1:1688     192.168.254.254:21     ESTABELECIDO
TCP    192.168.254.1:1691     192.168.254.254:25     ESTABELECIDO
TCP    192.168.254.1:1693     192.168.254.254:53     ESTABELECIDO
TCP    192.168.254.1:1694     192.168.254.254:23     ESTABELECIDO
```

### Tarefa 3: Reflexão

O utilitário **netstat** exibe conexões de rede de entrada e saída (TCP e UDP), informações da tabela de roteamento do computador e estatísticas de interface.

### Tarefa 4: Desafio

Feche sessões Estabelecidas de maneira abrupta (feche a janela do terminal) e emita o comando **netstat –an**. Tente visualizar conexões em estágios diferentes de ESTABELECIDO.

### Tarefa 5: Limpeza

A menos que não solicitado pelo instrutor, desligue os computadores. Remova qualquer coisa que tenha sido trazida ao laboratório e deixe a sala pronta para a próxima aula.