

Atividade 8.1 – Portas TCP e UDP

Uma determinada aplicação utiliza a porta TCP 500, enquanto outra aplicação utiliza a porta UDP 500. Dado que ambas as aplicações estão sendo executadas na mesma estação, como o sistema operacional é capaz de diferenciar os dados que devem ser repassados para cada uma destas portas?

R:

Embora os números sejam iguais, os números das portas utilizadas pelo UDP são independentes das utilizadas pelo TCP.

Assim o SO primeiro diferencia o protocolo e depois identifica a porta de destino.

Atividade 8.2 – Campo com tamanho do cabeçalho

Avaliando os formatos dos datagramas UDP e segmentos TCP, podemos perceber que o TCP adota um campo que indica o tamanho do cabeçalho. Por que o protocolo UDP não adota um campo com a mesma funcionalidade?

R:

O cabeçalho do TCP é maior e contém mais campos, alguns opcionais, o que faz variar o tamanho do cabeçalho, dessa forma a necessidade de especificar o tamanho. Já o cabeçalho UDP tem tamanho fixo.

Atividade 8.3 – Portas, conexões e endpoints

Diferentemente do protocolo UDP, que usa apenas a porta de destino para demultiplexar os datagramas recebidos, o protocolo TCP utiliza a identificação da conexão, ou seja, um par de endpoints. Por que o TCP não pode utilizar apenas a porta de destino?

R:

Pois no protocolo TCP uma única porta pode participar de várias conexões, assim só o número da porta não seria capaz de distinguir a conexão, por isso o uso de um identificador de conexões.

Atividade 8.4 – Portas UDP

Em sistemas Linux, o comando netstat, ativado com a opção -u, permite a visualização das portas UDP em uso. A Figura 8.26 mostra um exemplo de uso do comando netstat. A opção -a sinaliza que todas as portas UDP ativas devem ser listadas. A opção -n indica que os endereços IP e as portas não devem ser traduzidos para os respectivos nomes.

Para cada porta, o comando netstat mostra: o protocolo adotado (Proto); o número de bytes na fila de recepção (Recv-Q); o número de bytes na fila de transmissão

(Send-Q); o endereço IP e a porta UDP local (Local Address); o endereço IP e a porta UDP remota (Foreign Address). O endereço IP local 0.0.0.0 indica que os datagramas UDP serão aceitos quando encapsulados em datagramas IP que são endereçados a qualquer endereço IP da estação. Por outro lado, o endereço IP remoto 0.0.0.0 indica que os datagramas UDP serão aceitos de qualquer endereço IP remoto.

1. Execute o comando netstat e identifique as portas UDP ativas na sua estação. Em estações Windows, o comando deve ser `c:\netstat -p UDP -an`.

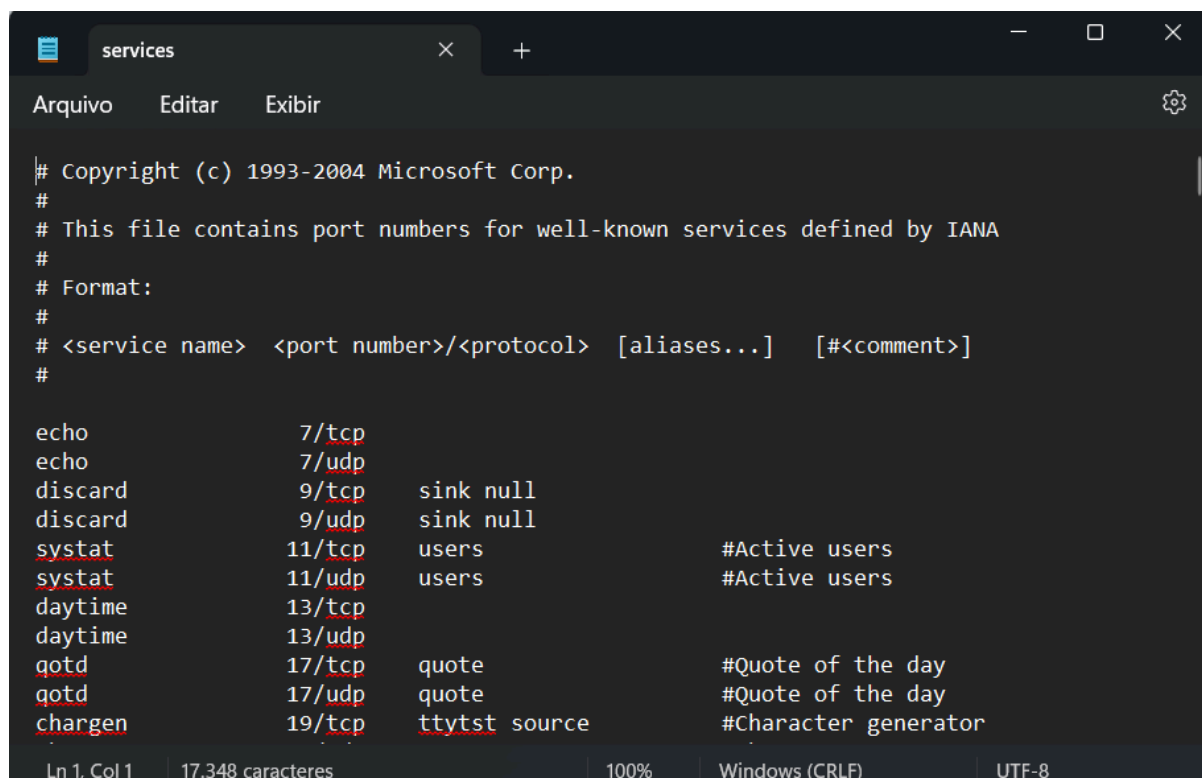
```
C:\Users\elder>netstat -p UDP -an

Conexões ativas

Proto Endereço local      Endereço externo      Estado
UDP    0.0.0.0:123          *:*
UDP    0.0.0.0:5050         *:*
UDP    0.0.0.0:5353         *:*
UDP    0.0.0.0:5355         *:*
UDP    0.0.0.0:53305        *:*
UDP    0.0.0.0:60913        *:*
UDP    0.0.0.0:61482        *:*
UDP    0.0.0.0:63456        *:*
UDP    127.0.0.1:1900        *:*
UDP    127.0.0.1:57099      *:*
UDP    127.0.0.1:60627      127.0.0.1:60627
UDP    127.0.0.1:63783      127.0.0.1:63783
UDP    192.168.18.99:137     *:*
UDP    192.168.18.99:138     *:*
UDP    192.168.18.99:1900    *:*
UDP    192.168.18.99:57098   *:*
UDP    192.168.56.1:137      *:*
UDP    192.168.56.1:138      *:*
UDP    192.168.56.1:1900     *:*
UDP    192.168.56.1:57097    *:*
```

```
C:\Users\elder>|
```

2. No Linux, o arquivo `/etc/services` descreve a associação de portas TCP e UDP com os nomes dos respectivos serviços. No Windows, o arquivo `services` está localizado em `"C:\Windows\System32\drivers\etc"`. Identifique os nomes dos serviços UDP que estão ativos na sua estação.



```
# Copyright (c) 1993-2004 Microsoft Corp.
#
# This file contains port numbers for well-known services defined by IANA
#
# Format:
#
# <service name> <port number>/<protocol> [aliases...] [#<comment>]
#

echo                7/tcp
echo                7/udp
discard             9/tcp    sink null
discard             9/udp    sink null
systat              11/tcp    users          #Active users
systat              11/udp    users          #Active users
daytime             13/tcp
daytime             13/udp
qotd                17/tcp    quote         #Quote of the day
qotd                17/udp    quote         #Quote of the day
chargen             19/tcp    ttytst source #Character generator
```

Atividade 8.5 – Portas TCP

O comando `netstat`, ativado com a opção `-t`, permite identificar as conexões TCP ativas, como também as portas TCP que estão aguardando requisições de conexão. A Figura 8.27 mostra outro exemplo de uso do comando `netstat`. A opção `-a` sinaliza que todas as conexões e portas TCP devem ser listadas. A opção `-n` indica que os endereços IP e as portas não devem ser traduzidos para os respectivos nomes.

Para cada conexão, o comando `netstat` mostra: o protocolo adotado (Proto); o número de bytes no buffer de recepção (Recv-Q); o número de bytes no buffer de transmissão (Send-Q); o endpoint local (Local Address); o endpoint remoto (Foreign Address); e o estado da conexão. As portas que aguardam requisições de conexão possuem o estado `LISTEN` (mostrado apenas com a opção `-a`). Já as conexões ativas possuem o estado `ESTABLISHED`. No estado `LISTEN`, o endereço IP local `0.0.0.0` indica que as requisições de conexão serão aceitas quando encapsuladas em datagramas IP que são endereçados a qualquer endereço IP da estação. Por outro lado, o endereço IP remoto `0.0.0.0` indica que as requisições de conexão serão aceitas de qualquer endereço IP remoto.

1. Execute o comando `netstat` e identifique as conexões TCP ativas e as portas TCP que estão aguardando requisições de conexão. Em estações Windows, o comando deve ser `c:\netstat -p TCP -an`.

```
C:\Users\elder>netstat -p TCP -an
```

Conexões ativas

Proto	Endereço local	Endereço externo	Estado
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49670	0.0.0.0:0	LISTENING
TCP	0.0.0.0:50128	0.0.0.0:0	LISTENING
TCP	127.0.0.1:49175	127.0.0.1:49176	ESTABLISHED
TCP	127.0.0.1:49176	127.0.0.1:49175	ESTABLISHED
TCP	127.0.0.1:49177	127.0.0.1:49178	ESTABLISHED
TCP	127.0.0.1:49178	127.0.0.1:49177	ESTABLISHED
TCP	192.168.18.99:139	0.0.0.0:0	LISTENING
TCP	192.168.18.99:50333	172.202.248.67:443	ESTABLISHED
TCP	192.168.18.99:50563	34.107.243.93:443	ESTABLISHED
TCP	192.168.18.99:51217	34.120.208.123:443	TIME_WAIT
TCP	192.168.18.99:51221	52.104.130.25:443	TIME_WAIT
TCP	192.168.18.99:51223	20.50.201.204:443	TIME_WAIT
TCP	192.168.18.99:51226	52.104.130.25:443	ESTABLISHED
TCP	192.168.18.99:51227	2.17.166.24:443	ESTABLISHED
TCP	192.168.18.99:51228	204.79.197.203:443	ESTABLISHED
TCP	192.168.18.99:51230	204.79.197.203:443	TIME_WAIT
TCP	192.168.18.99:51232	51.104.15.252:443	TIME_WAIT
TCP	192.168.18.99:51233	20.50.201.204:443	ESTABLISHED
TCP	192.168.18.99:51241	204.79.197.222:443	ESTABLISHED
TCP	192.168.56.1:139	0.0.0.0:0	LISTENING

2. Identifique os nomes dos serviços TCP que estão ativos e aguardando conexões.