Práctica de laboratorio 4.5.1: Observación de TCP y UDP a utilizando de Netstat

Diagrama de topología

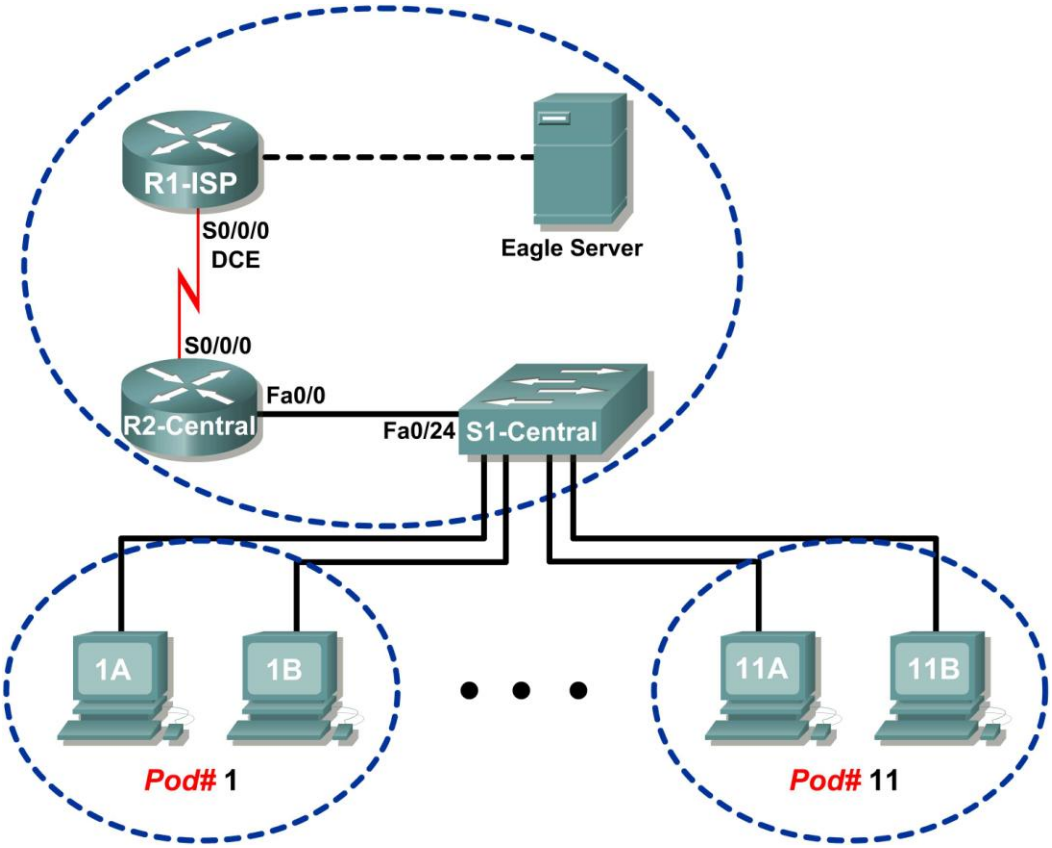

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	*No aplicable*
	Fa0/0	192.168.254.253	255.255.255.0	*No aplicable*
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	*No aplicable*
	Fa0/0	172.16.255.254	255.255.0.0	*No aplicable*
Eagle Server	*No aplicable*	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	*No aplicable*
host*Pod#***A**	*No aplicable*	172.16.*Pod#.*1	255.255.0.0	172.16.255.254
host*Pod#***B**	*No aplicable*	172.16.*Pod#.*2	255.255.0.0	172.16.255.254
S1-Central	*No aplicable*	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

- Explicar parámetros y resultados de comandos **netstat** comunes.
- Utilizar **netstat** para examinar la información del protocolo en un equipo host del módulo.

Información básica

netstat es la abreviatura de la utilidad de estadísticas de red que se encuentra disponible tanto en computadoras Windows como en computadoras Unix / Linux. El paso de parámetros opcionales con el comando cambiará la información de resultado. **netstat** muestra conexiones de red entrantes y salientes (TCP y UDP), información de tabla de enrutamiento del equipo host y estadísticas de la interfaz.

Escenario

En esta práctica de laboratorio el estudiante examinará el comando **netstat** en un equipo host del módulo y ajustará las opciones de resultado de **netstat** para analizar y entender el estado del protocolo de la capa de Transporte TCP/IP.

Tarea 1: Explicar parámetros y resultados de comandos netstat comunes.

Abra una ventana terminal haciendo clic en Inicio | Ejecutar. Escriba **cmd** y presione **Aceptar**.

Para mostrar información de ayuda sobre el comando **netstat**, utilice las opciones **/?**, como se muestra:

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

Utilice el comando de salida **netstat** /? como referencia para completar la opción que mejor se ajuste a la descripción:

Opción	Descripción
	Muestra todas las conexiones y puertos que escuchan.
	Muestra direcciones y números de puerto en forma numérica.
	Vuelve a mostrar estadísticas cada cinco segundos. Presione CONTROL+C para detener la nueva visualización de las estadísticas.
	Muestra conexiones para el protocolo especificadas por protocolo. El protocolo puede ser cualquiera de los siguientes: TCP, UDP, TCPv6, o UDPv6. Si se usa con la opción –s para mostrar estadísticas por protocolo, el protocolo puede ser cualquiera de los siguientes: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, o UDPv6.
	Vuelve a mostrar todas las conexiones y puertos que escuchan cada 30 segundos.
	Muestra sólo las conexiones abiertas. Éste es un problema complicado.

Cuando se muestran estadísticas **netstat** para conexiones TCP, también se muestra el estado TCP. Durante la conexión TCP, la conexión atraviesa por una serie de estados. La siguiente tabla es un resumen de los estados TCP desde RFC 793, Transmission Control Protocol, septiembre de 1981, tal como lo informó **netstat**:

Estado	Descripción de la conexión
ESCUCHAR	La conexión local está a la espera de un pedido de conexión de parte de cualquier dispositivo remoto.
ESTABLECIDA	La conexión está abierta y se pueden intercambiar datos a través de la conexión. Éste es el estado normal para la fase de transferencia de datos de la conexión.
TIEMPO-ESPERA	La conexión local está esperando un período de tiempo predeterminado después de enviar un pedido de finalización de conexión antes de cerrar la conexión. Ésta es una condición normal y generalmente dura entre 30 y 120 segundos.
CERRAR-ESPERAR	La conexión se cerró pero sigue esperando un pedido de finalización por parte del usuario local.
SYN-ENVIADA	La conexión local espera una respuesta después de enviar un pedido de conexión. La conexión debe transitar rápidamente por este estado.
SYN_RECIBIDA	La conexión local espera un acuse de recibo que confirme su pedido de conexión. La conexión debe transitar rápidamente por este estado. Conexiones múltiples en el estado SYN_RECIBIDO pueden indicar un ataque TCP SYN.

Las direcciones IP mostradas por **netstat** entran en varias categorías:

Dirección IP	Descripción
127.0.0.1	Esta dirección se refiere al host local o a este equipo.
0.0.0.0	Una dirección global, lo que significa "CUALQUIERA".
Dirección remota	La dirección del dispositivo remoto que tiene una conexión con este equipo.

Tarea 2: Utilizar netstat para examinar la información del protocolo en un equipo host del módulo.

Paso 1: Utilice netstat para ver conexiones existentes.

Desde la ventana Terminal en Tarea 1, arriba, ejecute el comando **netstat –a:**

```
C:\> netstat –a <INTRO>
```

Se mostrará una tabla que lista el protocolo (TCP y UDP), dirección local, dirección remota e información sobre el estado. Allí también figuran las direcciones y los protocolos que se pueden traducir a nombres.

La opción –n obliga a netstat a mostrar el resultado en formato bruto. Desde la ventana Terminal, ejecute el comando **netstat –an:**

```
C:\> netstat –an <INTRO>
```

Utilice la barra de desplazamiento vertical de la ventana para desplazarse hacia atrás y adelante entre los resultados de los dos comandos. Compare los resultados, note cómo los números de puertos bien conocidos cambiaron por nombres.

Anote tres conexiones TCP y tres UDP del resultado de **`netstat –a`** y los números de puertos traducidos correspondientes del resultado de **`netstat –an`**. Si hay menos de tres conexiones que se traducen, anótelo en la tabla.

Conexión	Protocolo	Dirección Local	Dirección extranjera	Estado

Consulte el siguiente resultado **`netstat`**. Un ingeniero de red nuevo sospecha que su equipo host ha sufrido un ataque exterior a los puertos 1070 y 1071. ¿Cómo respondería?

```
C:\> netstat –n
Conexiones activas
Protocolo  Dirección Local        Dirección extranjera    Estado
TCP        127.0.0.1:1070         127.0.0.1:1071          ESTABLISHED
TCP        127.0.0.1:1071         127.0.0.1:1070          ESTABLISHED
C:\>
```

_____

_____

Paso 2: Establezca múltiples conexiones TCP simultáneas y grabe el resultado netstat.

En esta tarea, se realizarán varias conexiones simultáneas con Eagle Server. El comando **`telnet`** autorizado se utilizar para acceder a los servicios de red Eagle Server, además de proveer varios protocolos para examinar con `netstat`.

Abra cuatro ventanas terminales adicionales. Acomode las ventanas de manera tal que estén todas a la vista. Las cuatro ventanas terminales que se utilizarán para las conexiones telnet con Eagle Server pueden ser relativamente pequeñas, más o menos ½ pantalla de ancho por ¼ de pantalla de alto. Las ventanas terminales que se utilizarán para recolectar información de conexión deben ser de ½ pantalla de ancho por la pantalla entera de alto.

Responderán varios servicios de red de Eagle Server a una conexión telnet. Utilizaremos:

- DNS, servidor nombre de dominio, puerto 53
- FTP, servidor FTP, puerto 21
- SMTP, servidor de correo SMTP, puerto 25
- TELNET, servidor Telnet, puerto 23

¿Por qué fallarían los puertos telnet a UDP?

_____

_____

Para cerrar una conexión telnet, presione las teclas <CTRL>] juntas. Eso mostrar el indicador telnet, Microsoft Telnet>. Escriba **quit <INTRO>** para cerrar la sesión.

En la primera ventana terminal telnet, telnet a Eagle Server en puerto 53. En la segunda ventana terminal, telnet en puerto 21. En la tercera ventana terminal, telnet en puerto 25. En la cuarta ventana terminal, telnet en puerto 23. El comando para una conexión telnet en puerto 21 se muestra debajo:

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

En la ventana terminal más grande, registre las conexiones establecidas con Eagle Server. El resultado debe ser similar a lo siguiente. Si la escritura es lenta, puede que se haya cerrado una conexión antes de que se hayan establecido todas las conexiones. Finalmente, todas las conexiones deben finalizar con la inactividad.

```
Protocolo  Dirección Local        Dirección extranjera    Estado
TCP        192.168.254.1:1688     192.168.254.254:21      ESTABLISHED
TCP        192.168.254.1:1691     192.168.254.254:25      ESTABLISHED
TCP        192.168.254.1:1693     192.168.254.254:53      ESTABLISHED
TCP        192.168.254.1:1694     192.168.254.254:23      ESTABLISHED
```

Tarea 3: Reflexión

La utilidad **netstat** muestra conexiones de red entrantes y salientes (TCP y UDP), información de la tabla de enrutamiento del equipo host y estadísticas de la interfaz.

Tarea 4: Desafío

Cierre bruscamente las sesiones Establecidas (cierre la ventana terminal) y ejecute el comando **netstat –an**. Trate de ver las conexiones en etapas que no sean ESTABLECIDAS.

Tarea 5: Limpieza

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.