Actividad de laboratorio: Solución de problemas del tráfico LAN mediante SPAN

Topología

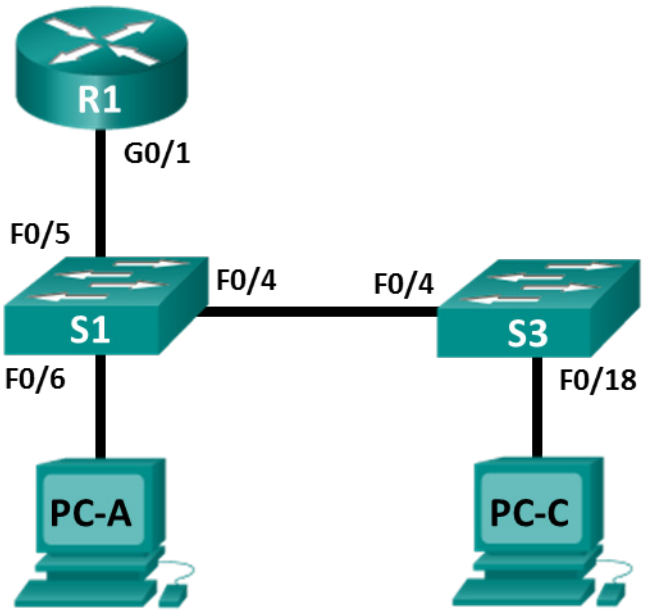


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	N/D
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.3	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.254	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Armar la red y verificar la conectividad

Parte 2: Configurar SPAN local y capturar el tráfico copiado con Wireshark

Aspectos básicos/situación

Como administrador de la red, decide analizar la red de área local interna en busca de tráfico de red sospechoso y de posibles ataques de DoS o de reconocimiento. Para hacerlo, configurará replicación de puertos en todos los puertos de switch activos y replicará/copiará todo el tráfico a un puerto de switch designado en el que una PC con Wireshark en ejecución pueda analizar el tráfico capturado. El objetivo es identificar el origen del tráfico sospechoso. Para configurar la duplicación de puertos, usará la función del

analizador de puertos conmutados (SPAN) en el switch de Cisco. Es común encontrar un dispositivo que ejecute un detector de paquetes o sistema de detección de intrusiones (IDS) conectado al puerto duplicado.

Nota: Los routers que se usan en las actividades prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con Cisco IOS versión 15.4(3) (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: Asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

Recursos necesarios

- 1 router (Cisco 1941 con Cisco IOS versión 15.4(3), imagen universal o equivalente)
- 2 switches (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
- 2 PC (Windows con un programa de emulación de terminal, como Tera Term o PuTTY, Wireshark y Zenmap)
- Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Parte 1: Armar la red y verificar la conectividad

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

Paso 1: Realizar el cableado de red como se muestra en la topología

Conecte los dispositivos como se muestra en la topología y realice el cableado necesario.

Paso 2: Configurar los hosts de las PC

Paso 3: Inicializar y vuelva a cargar los routers y los switches según sea necesario

Paso 4: configurar los parámetros básicos para el router.

a. Desactive la búsqueda de DNS.

b. Configure el nombre del dispositivo como se muestra en la topología.

c. Configure una dirección IP para el router, como se indica en la tabla de asignación de direcciones.

d. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

e. Asigne **cisco** como contraseña de la consola y vty, habilite el inicio de sesión.

f. Defina las líneas vty en **transport input telnet**.

g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.

h. Copie la configuración en ejecución en la configuración de inicio

Paso 5: Configurar los parámetros básicos para cada switch

a. Desactive la búsqueda de DNS.

b. Configure el nombre del dispositivo como se muestra en la topología.

c. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

d. Configure las direcciones IP para los switches como se indica en la tabla de direccionamiento.

e. Configure el gateway predeterminado en cada switch.

f. Asigne **cisco** como contraseña de la consola y vty, y habilite el inicio de sesión.

g. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.

h. Copie la configuración en ejecución en la configuración de inicio

Paso 6: Verifique la conectividad.

a. Desde PC-A, debería poder enviar un comando ping a la interfaz en R1, S1, S3 y PC-C. ¿Todos los comandos ping produjeron un resultado correcto?

Si los pings no se realizan correctamente, solucione los problemas de las configuraciones básicas del dispositivo antes de continuar.

b. Desde PC-C, debería poder enviar un comando ping a la interfaz en R1, S1, S3 y PC-A. ¿Todos los comandos ping produjeron un resultado correcto?

Si los pings no se realizan correctamente, solucione los problemas de las configuraciones básicas del dispositivo antes de continuar.

Parte 2: Configurar el SPAN local y capturar el tráfico copiado con Wireshark

Para configurar SPAN local tiene que configurar al menos un puerto de origen que llamará puerto monitoreado y un único puerto de destino también llamado puerto monitoreado para que se envíe el tráfico copiado o replicado. Los puertos de origen de SPAN se pueden configurar para que monitoreen el tráfico a su ingreso o egreso, o en ambas direcciones (opción predeterminada).

Paso 1: Configure SPAN en S1.

a. Localice los puertos de switch que están activos en S1.

```
S1# show ip interface brief
```

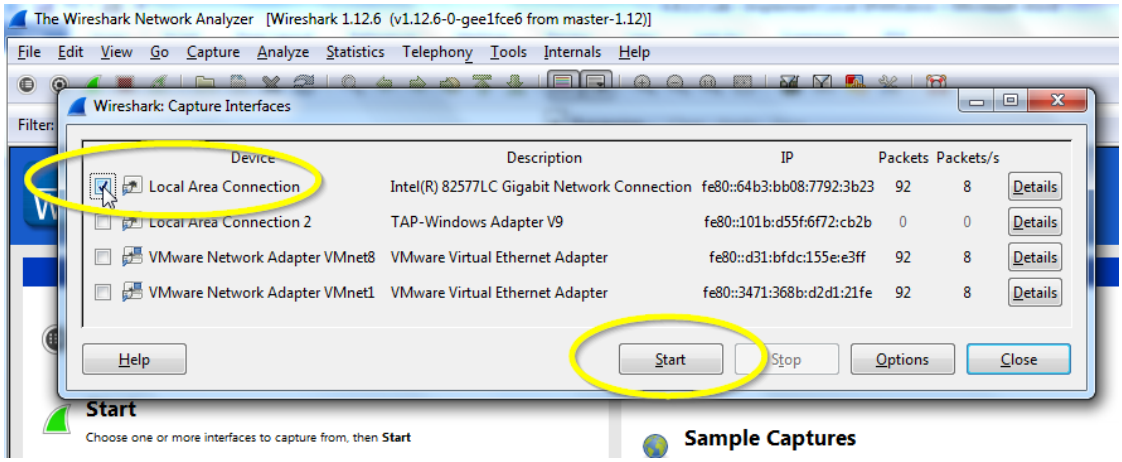
¿Qué puertos de switch están activos en forma física, y cuáles en forma lógica?

b. En S1, F0/6 se conecta a PC-A, que se utilizará para analizar el tráfico con Wireshark. F0/6 será el puerto de monitoreo de destino de SPAN para los paquetes duplicados. F0/4 y F0/5 serán los puertos de monitoreo de origen para los paquetes interceptados. Puede configurar múltiples puertos de monitoreo de origen pero solo uno de destino.

```
S1(config)# monitor session 1 source interface f0/4 - 5
S1(config)# monitor session 1 destination interface f0/6
```


Paso 2: Comience una captura de Wireshark en PC-A.

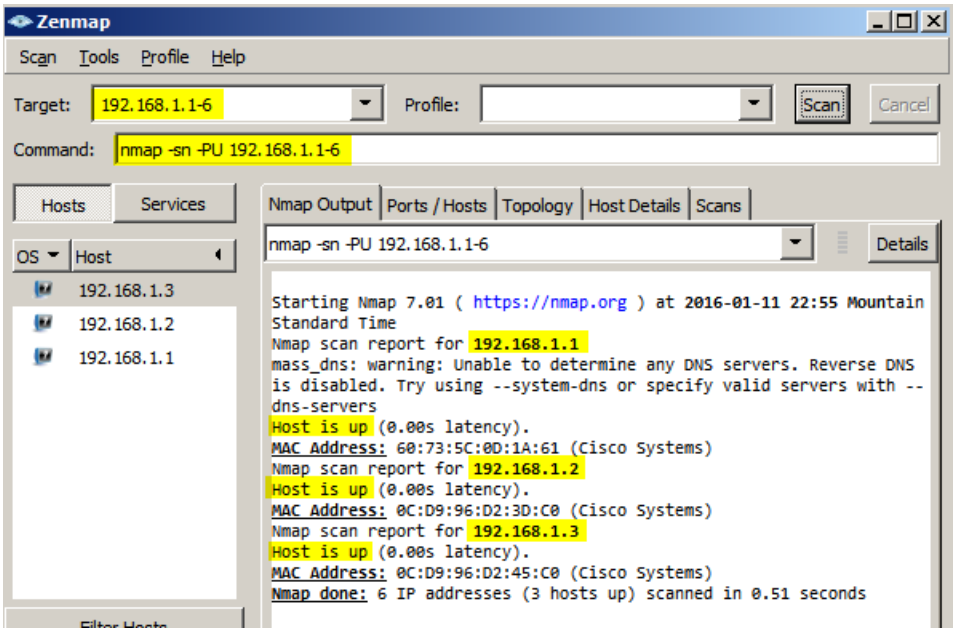
a. Abra Wireshark en PC-A, defina la interfaz de captura en la Conexión de área local y haga clic en Start (Comenzar).



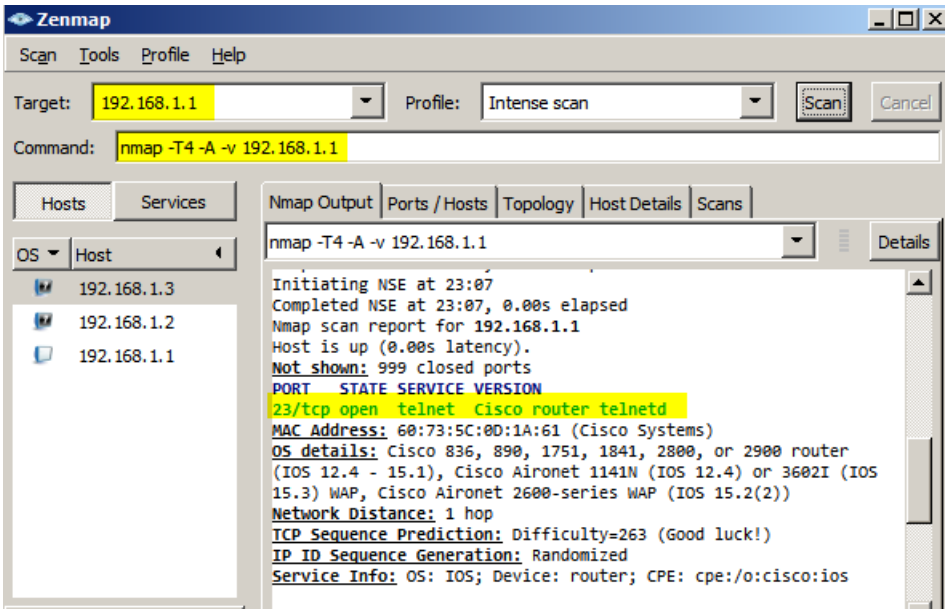
Paso 3: Desde PC-C, utilice NMAP para generar tráfico sospechoso.

a. De ser necesario, vaya a NMAP.org para descargar Zenmap. Desplácese hacia abajo en la página para encontrar la última versión estable para PC-C. Luego después de las instrucciones en la pantalla para instalar Zenmap con las configuraciones predeterminadas.

b. Abra Zenmap en PC-C y ejecute un escaneo de pings UDP para buscar hosts disponibles (*nmap –sn –PU 192.168.1-6*). En el resultado de la búsqueda se identifican 3 hosts en la red R1, S1 y S2, en 192.168.1.1, 192.168.1.2 y 192.168.1.3. Fíjese que Zenmap también ha identificado las direcciones MAC de los tres hosts como interfaces de Cisco Systems. Si se tratara de un ataque de reconocimiento de red real, el escaneo podría abarcar todo el rango de hosts de red, al igual que los puertos y la identificación del SO.

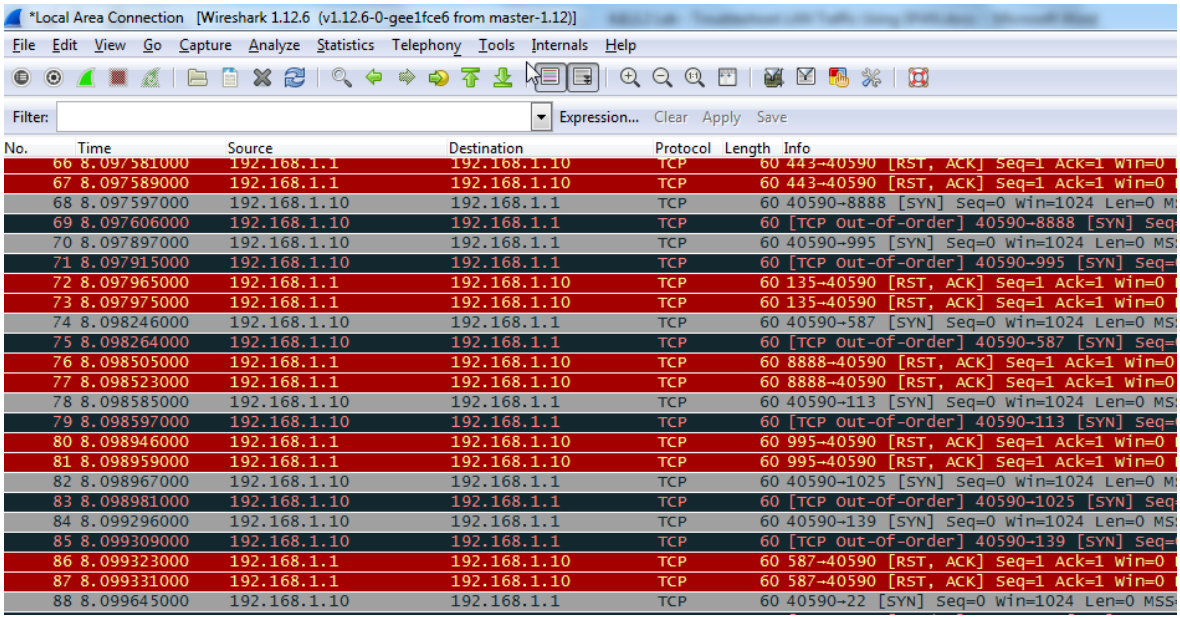


c. El atacante hipotético ahora puede ejecutar un escaneo intenso en R1 en 192.168.1.1 (nmap –T4 –A –v 192.168.1.1). En el resultado de la búsqueda se identifica un puerto 23/Telnet abierto.



Paso 4: En PC-A detenga la captura de Wireshark y examine los paquetes SPAN capturados.

a. Regrese a PC-A y detenga la captura de Wireshark. Tome nota de los patrones de tráfico no estándares entre PC-C en 192.168.1.10 y R1 en 192.168.1.1. Está plagado de segmentos Fuera de orden y de operaciones para restablecer la conexión (RST). Esta captura de paquetes identifica que PC-C está enviando tráfico sospechoso al router R1.



b. El atacante que está trabajando en PC-C y sabe que el router tiene un puerto abierto en el 23 podría intentar iniciar un ataque adicional de fuerza bruta o de DoS, como un ataque LAND. Un ataque LAND es un paquete SYN de TCP con la misma dirección IP y número de puerto de origen y destino. Si se utiliza Zenmap, el comando **nmap –sS 192.168.1.1 –S 192.168.1.1 –p23 –g23 –e eth0** es un ejemplo. Fíjese que el ataque LAND define tanto la dirección IP de origen como la destino en 192.168.1.1 y los números

de puerto de origen y de destino en el puerto abierto 23. Aunque R1 con IOS15 no es vulnerable a este tipo de ataque de DoS más antiguo, muchos sistemas y servidores anteriores siguen siéndolo. Este ataque detendrá el funcionamiento de los sistemas vulnerables, ya que los definirá en un bucle infinito.

Reflexión

En esta situación, ¿se utilizó SPAN para solucionar problemas e identificar el origen de la actividad sospechosa de la red? ¿En qué otras situaciones SPAN podría ser útil para solucionar problemas?

Tabla de resumen de interfaces de router

Resumen de interfaces de router				
Modelo de router	**Interfaz Ethernet 1**	**Interfaz Ethernet 2**	**Interfaz serial 1**	**Interfaz serial 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: Para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de hacer una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando de Cisco IOS para representar la interfaz.