

Actividad de laboratorio: Implementar SPAN local

Topología

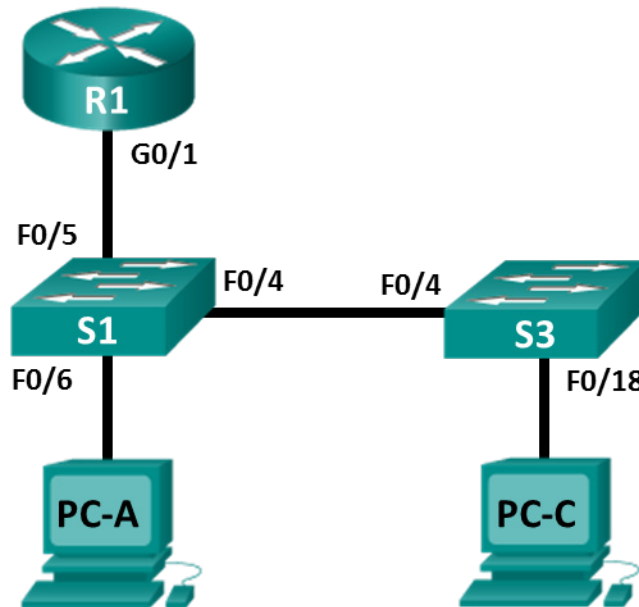


Tabla de asignación de direcciones

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 el administrador de la red, quiere analizar el tráfico que ingresa y sale de la red local. Para hacerlo, configurará replicación de puertos en el puerto de switch conectado al router y replicará todo el tráfico a otro puerto de switch. El objetivo es enviar todo el tráfico replicado a un sistema de detección de intrusiones (IDS) para su análisis. En esta implementación inicial, enviará todo el tráfico replicado a una PC que capturará el tráfico para analizarlo con un programa de monitoreo de puertos. Para configurar la duplicación de puertos, usará la función del analizador de puertos conmutados (SPAN) en el switch de Cisco. SPAN es un tipo de replicación de puertos que envía copias de una trama que ingresa a un puerto, y sale por otro puerto en el

Actividad de laboratorio: Implementar SPAN local

mismo switch. 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)
- 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

- Desactive la búsqueda de DNS.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- Configure las direcciones IP para los switches como se indica en la tabla de direccionamiento.
- Configure el gateway predeterminado en cada switch.
- Asigne **cisco** como contraseña de la consola y vty, y habilite el inicio de sesión.
- Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.
- Copie la configuración en ejecución en la configuración de inicio

Paso 6: Verifique la conectividad.

- 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.
- 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).

El puerto de origen de SPAN tendrá que configurarse en el puerto que se conecte al router en el puerto de switch F0/5 de S1. De esta manera, se monitoreará todo el tráfico que ingrese o salga de la LAN. El puerto de destino de SPAN se configurará en el puerto de switch F0/6 de S1 que está conectado a la PC-A que está ejecutando Wireshark.

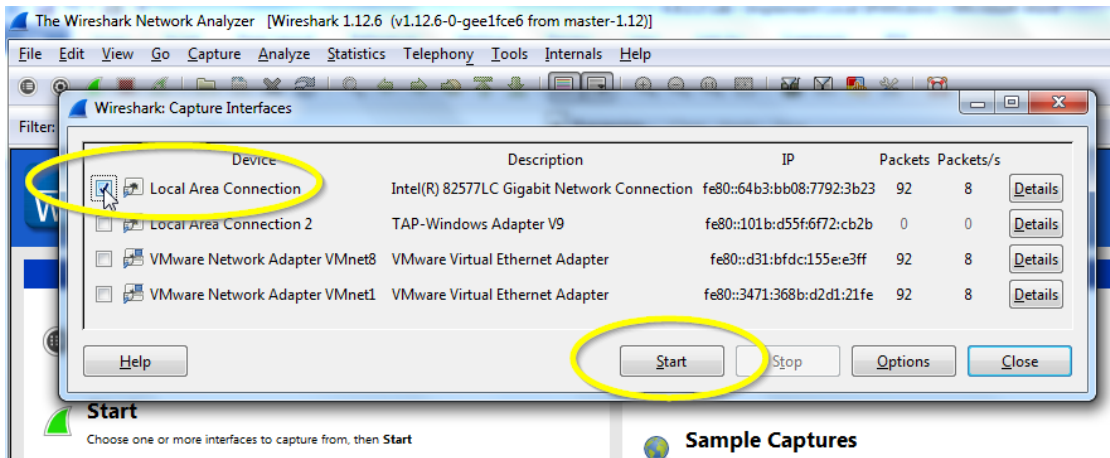
Paso 1: Configurar SPAN en S1.

- Conéctelo con un cable de consola a S1 y configure los puertos de monitoreo de origen y destino en S1. Ahora, todo el tráfico que entre o salga de F0/5 se copiará y reenviará fuera de F0/6.

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

Paso 2: Comenzar 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: Establecer una conexión Telnet a R1 y cree tráfico ICMP en la LAN.

- a. Establezca una conexión Telnet de S1 a R1.

```
S1# Telnet 192.168.1.1
Trying 192.168.1.1 . . . Open

User Access Verification
```

```
Password:
R1>
```

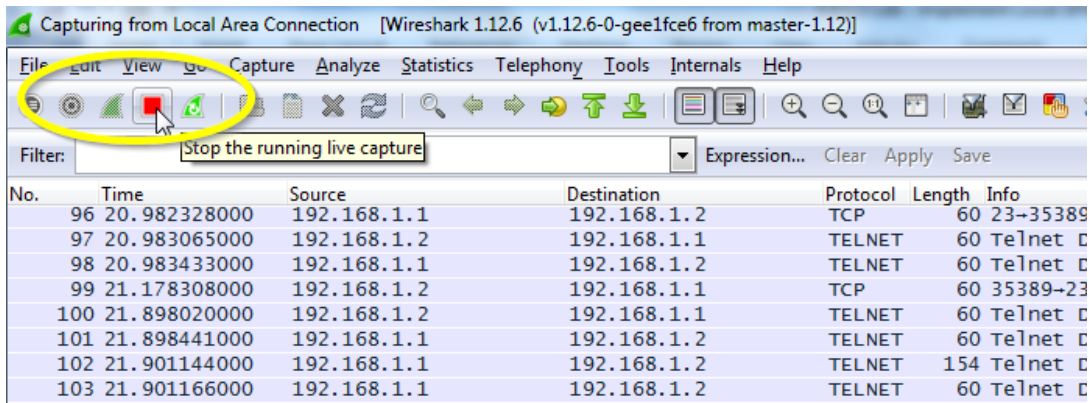
- b. En el modo con privilegios, emita un ping a PC-C, S1 y S3.

```
R1> enable
Password:
R1# ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1# ping 192.168.1.2
<Resultado omitido>
R1# ping 192.168.1.3
<Resultado omitido>
```

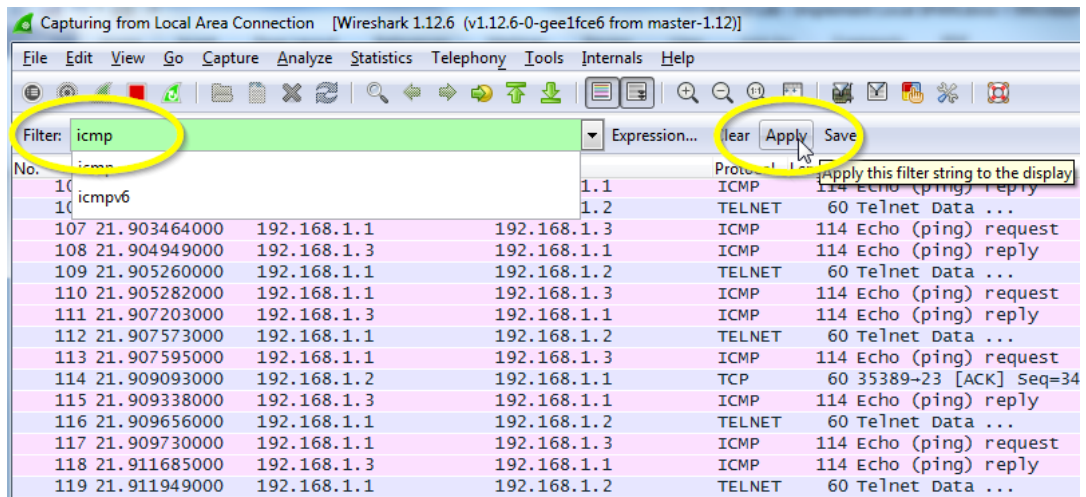
Actividad de laboratorio: Implementar SPAN local

Paso 4: Detener la captura de Wireshark en PC-A y filtrarla para encontrar ICMP.

- a. Regrese a PC-A y detenga la captura de Wireshark en ejecución en PC-A.

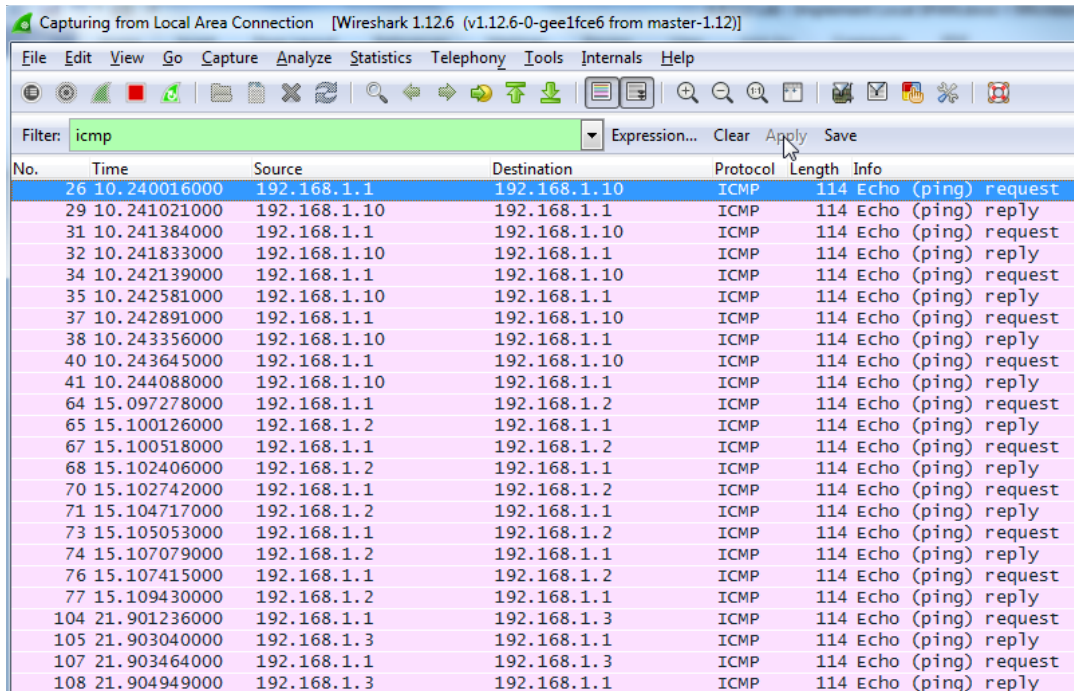


- b. Filtre la captura de Wireshark para encontrar paquetes ICMP.



- c. Busque paquetes ICMP en la captura de Wireshark filtrada.

Actividad de laboratorio: Implementar SPAN local



No.	Time	Source	Destination	Protocol	Length	Info
26	10.240016000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
29	10.241021000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
31	10.241384000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
32	10.241833000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
34	10.242139000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
35	10.242581000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
37	10.242891000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
38	10.243356000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
40	10.243645000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
41	10.244088000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
64	15.097278000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
65	15.100126000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
67	15.100518000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
68	15.102406000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
70	15.102742000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
71	15.104717000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
73	15.105053000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
74	15.107079000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
76	15.107415000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
77	15.109430000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
104	21.901236000	192.168.1.1	192.168.1.3	ICMP	114	Echo (ping) request
105	21.903040000	192.168.1.3	192.168.1.1	ICMP	114	Echo (ping) reply
107	21.903464000	192.168.1.1	192.168.1.3	ICMP	114	Echo (ping) request
108	21.904949000	192.168.1.3	192.168.1.1	ICMP	114	Echo (ping) reply

d. ¿Se copiaron y reenviaron satisfactoriamente de F0/6 a PC-A los pings de R1 a PC-C, S1 y S3?

e. ¿Se monitoreó y copió el tráfico en ambas direcciones? _____

Reflexión

En esta situación, en lugar de utilizar PC-A y un analizador de paquetes, ¿sería más apropiado emplear un IDS o un IPS?

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.