Práctica de laboratorio: Recopilación y análisis de datos de NetFlow

Topología

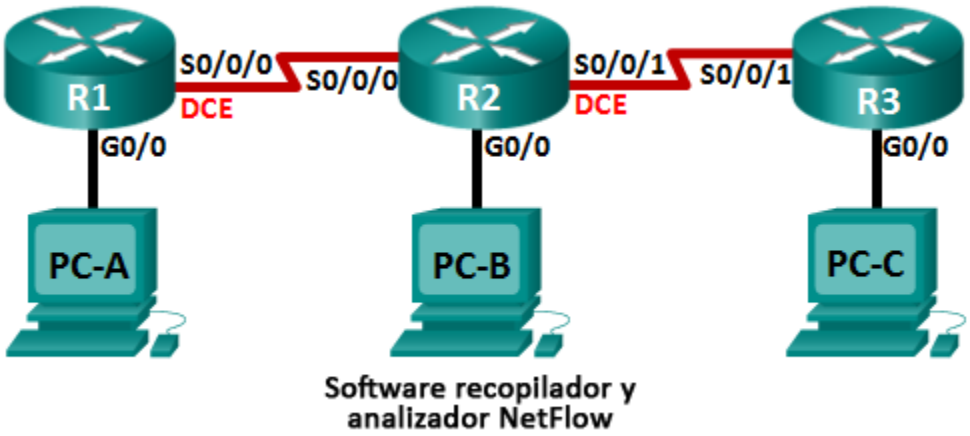

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Gateway predeterminado
R1	G0/0	192.168.1.1/24	N/A
	S0/0/0 (DCE)	192.168.12.1/30	N/A
R2	G0/0	192.168.2.1/24	N/A
	S0/0/0	192.168.12.2/30	N/A
	S0/0/1 (DCE)	192.168.23.1/30	N/A
R3	G0/0	192.168.3.1/24	N/A
	S0/0/1	192.168.23.2/30	N/A
PC-A	NIC	192.168.1.3	192.168.1.1
PC-B	NIC	192.168.2.3	192.168.2.1
PC-C	NIC	192.168.3.3	192.168.3.1

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: Configurar NetFlow en un router

Parte 3: Analizar NetFlow mediante la CLI

Parte 4: Explorar el software recopilador y analizador NetFlow

Información básica/situación

NetFlow es una tecnología del IOS de Cisco que proporciona estadísticas sobre los paquetes que fluyen a través de un switch multicapa o un router Cisco. NetFlow habilita el monitoreo de red y de seguridad, la planificación de la red, el análisis de tráfico y la contabilidad de IP. Es importante no confundir el propósito y los resultados de NetFlow con los del hardware y el software de captura de paquetes. La captura de paquetes registra toda la información posible que sale de un dispositivo de red o que ingresa a este para un análisis posterior, NetFlow identifica información estadística específica.

Flexible NetFlow es la tecnología de NetFlow más reciente y mejora el NetFlow original al agregar la capacidad de personalizar los parámetros de análisis de tráfico. Flexible Netflow usa el formato de exportación de la versión 9. A partir de la versión 15.1 del IOS de Cisco, se admiten muchos comandos útiles de Flexible NetFlow.

En esta práctica de laboratorio, configurará NetFlow para capturar paquetes entrantes y salientes. Utilizará comandos **show** para verificar que NetFlow funciona y recopila información estadística. También explorará las opciones disponibles para el software de recopilación y de análisis de NetFlow.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Pueden utilizarse otros routers y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, 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 que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los routers.

Paso 1: realizar el cableado de red tal como se muestra en la topología.

Paso 2: inicializar y volver a cargar los routers según sea necesario.

Paso 3: configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

b. Configure los nombres de los dispositivos como se muestra en la topología.

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

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

e. Cifre las contraseñas de texto no cifrado.

f. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.

g. Configure **logging synchronous** para la línea de consola.

h. Establezca la frecuencia de reloj para todas las interfaces seriales DCE en **128000**.

i. Configure las direcciones IP como se indica en la tabla de direccionamiento.

j. Configure OSPF con la ID de proceso 1 y anuncie todas las redes. Las interfaces Ethernet deben ser pasivas.

k. Cree una base de datos local en el R3 con el nombre de usuario **admin** y la contraseña **cisco** con el nivel de privilegio **15**.

l. En el R3, habilite el servicio HTTP y autentique los usuarios HTTP con la base de datos local.

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

Paso 4: configurar los equipos host.

Paso 5: Verificar la conectividad de extremo a extremo.

Todos los dispositivos deben poder hacer ping a los otros dispositivos en la topología. Resuelva los problemas según sea necesario hasta que se establezca la conectividad de extremo a extremo.

Nota: quizá sea necesario deshabilitar el firewall de las computadoras para que los pings entre estas se realicen correctamente.

Parte 2: Configurar NetFlow en un router

En la parte 2, configurará NetFlow en el router R2. NetFlow capturará todo el tráfico entrante y saliente en las interfaces seriales del R2 y exportará los datos al recopilador NetFlow, la PC-B. Se utilizará la versión 9 de Flexible NetFlow para realizar la exportación al recopilador NetFlow.

Paso 1: Configurar la captura de NetFlow.

Configure la captura de datos de NetFlow en ambas interfaces seriales. Capture datos de los paquetes entrantes y salientes.

```
R2(config)# interface s0/0/0
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
R2(config-if)# interface s0/0/1
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
```

Paso 2: Configure la exportación de datos de NetFlow.

Utilice el comando **ip flow-export destination** para identificar la dirección IP y el puerto UDP del recopilador NetFlow al cual el router debe exportar los datos de NetFlow. Se utilizará el número de puerto UDP 9996 para esta configuración.

```
R2(config)# ip flow-export destination 192.168.2.3 9996
```

Paso 3: Configure la versión de exportación de NetFlow.

Los routers Cisco que ejecutan el IOS 15.1 admiten las versiones de NetFlow 1, 5 y 9. La versión 9 es el formato de exportación de datos más versátil, pero no es compatible con las versiones anteriores. Utilice el comando **ip flow-export version** para establecer la versión de NetFlow.

```
R2(config)# ip flow-export version 9
```


Paso 4: Verificar la configuración de NetFlow

a. Emita el comando **show ip flow interface** para revisar la información de la interfaz de captura de NetFlow.

```
R2# show ip flow interface
Serial0/0/0
  ip flow ingress
  ip flow egress
Serial0/0/1
  ip flow ingress
  ip flow egress
```

b. Emita el comando **show ip flow export** para revisar la información de exportación de datos de NetFlow.

```
R2# show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  192.168.2.3 (9996)
  Version 9 flow records
  388 flows exported in 63 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

Parte 3: Analizar NetFlow mediante la CLI

En la parte 3, generará tráfico de datos entre el R1 y el R3 para observar la tecnología NetFlow.

Paso 1: Generar tráfico de datos entre el R1 y el R3.

a. Acceda mediante Telnet del R1 al R3 con la dirección IP 192.168.3.1. Introduzca la contraseña **cisco** para ingresar al modo EXEC del usuario. Introduzca la contraseña **class** para habilitar el modo EXEC global. Emita el comando **show run** para generar tráfico de Telnet. Mantenga activa la sesión de Telnet por ahora.

b. Desde el R3, emita el comando **ping 192.168.1.1 repeat 1000** para hacer ping a la interfaz G0/0 del R1. Esto generará tráfico ICMP a través del R2.

c. Desde la PC-A, acceda al R3 con la dirección IP 192.168.3.1. Inicie sesión como **admin** con la contraseña **cisco**. Mantenga el explorador abierto después de iniciar sesión en el R3.

Nota: asegúrese de que el bloqueador de elementos emergentes esté deshabilitado en el explorador.

Paso 2: Mostrar un resumen de las estadísticas de contabilidad de NetFlow.

En el R2, emita el comando **show ip cache flow** para mostrar los cambios en el resumen de datos de NetFlow, incluso la distribución del tamaño de paquetes, la información del flujo IP, los protocolos capturados y la actividad de interfaz. Observe que ahora se muestran los protocolos en los datos de resumen.

```
R2# show ip cache flow
IP packet size distribution (5727 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
```



```
   .000 .147 .018 .700 .000 .001 .001 .001 .001 .011 .009 .001 .002 .000 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .001 .097 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 114 added
  1546 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 112 added, 112 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics 00:07:35
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           4      0.0        27    43      0.2       5.0      15.7
TCP-WWW            104      0.2        14   275      3.4       2.1       1.5
ICMP                 4      0.0      1000   100      8.8      27.9      15.4

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Total:             112      0.2        50   146     12.5       3.1       2.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/0       192.168.12.1    Null          224.0.0.5       59 0000 0000    43
Se0/0/1       192.168.23.2    Null          224.0.0.5       59 0000 0000    40
```

Paso 3: Finalizar las sesiones de Telnet y del explorador.

a. Emita el comando **exit** en el R1 para desconectarse de la sesión de Telnet al R3.

b. Cierre la sesión del explorador en la PC-A.

Paso 4: Borrar las estadísticas de contabilidad de NetFlow.

a. En el R2, emita el comando **clear ip flow stats** para borrar las estadísticas de contabilidad de NetFlow.

```
R2# clear ip flow stats
```

b. Vuelva a emitir el comando **show ip cache flow** para verificar que se hayan restablecido las estadísticas de contabilidad de NetFlow. Observe que, aunque ya no genera más datos a través del R2, NetFlow captura datos. En el ejemplo que se muestra a continuación, la dirección de destino para este tráfico es la dirección de multidifusión 224.0.0.5, o los datos de LSA de OSPF.

```
R2# show ip cache flow
IP packet size distribution (124 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
```

```
IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 2 added
  1172 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  2 active, 1022 inactive, 2 added, 2 added to flow
  0 alloc failures, 0 force free
  1 chunk, 0 chunks added
  last clearing of statistics 00:09:48
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
IP-other             2      0.0       193    79      0.6    1794.8       5.7
Total:               2      0.0       193    79      0.6    1794.8       5.7


SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/0       192.168.12.1    Null          224.0.0.5       59 0000 0000    35

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/1       192.168.23.2    Null          224.0.0.5       59 0000 0000    33
```

Parte 4: Explorar el software recopilador y analizador NetFlow

El software recopilador y analizador NetFlow se puede conseguir de muchos proveedores. Algunas opciones de software se proporcionan como freeware, otras no. El siguiente URL proporciona una página web de resumen de algunas opciones de software de NetFlow freeware disponibles: http://www.cisco.com/en/US/prod/iosswrel/ps6537/ps6555/ps6601/networking_solutions_products_genericcontent0900aecd805ff72b.html.

Revise esta página web para conocer algunos de los productos de software recopilador y analizador NetFlow disponibles.

Reflexión

1. ¿Cuál es el propósito del software recopilador NetFlow?

2. ¿Cuál es el propósito del software analizador NetFlow?

3. ¿Cuáles son los siete campos fundamentales que usa NetFlow original para diferenciar flujos?

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 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 confeccionar 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 de ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.