Packet Tracer: Explorar una implementación de NetFlow

Objetivos

Parte 1: Observar registros de flujos de NetFlow - Un sentido

Parte 2: Observar registros de NetFlow correspondientes a una sesión que ingresa y sale del colector

Aspectos básicos/Situación

En esta actividad utilizará Packet Tracer para crear tráfico de red y observará los registros de flujos de NetFlow correspondientes en un colector de NetFlow. Packet Tracer ofrece una simulación básica de la funcionalidad de NetFlow. No sustituye a aprender NetFlow en un equipo físico. Puede haber algunas diferencias entre los registros de flujos de NetFlow generados por Packet Tracer y los registros creados por un equipo de red con todas las funciones.

Instrucciones

Parte 1: Observar registros de flujos de NetFlow - Un sentido

Paso 1: Abra el colector de NetFlow.

a. En el colector de NetFlow, haga clic en la pestaña **Escritorio**. Haga clic en el ícono de **Colector de NetFlow**.

b. Haga clic en el botón de **Encender** para activar el colector según sea necesario. Posicione y cambie el tamaño de la ventana para poder verla desde la ventana de la topología de Packet Tracer.

Paso 2: Haga ping al gateway predeterminado desde PC-1.

a. Haga clic en **PC**-1.

b. Abra la pestaña de **Escritorio** y haga clic en el ícono de **Command Prompt**.

c. Introduzca el comando **ping** para probar la conectividad al gateway predeterminado en 10.0.0.1.

```
C:\> ping 10.0.0.1
```

d. Después de una breve demora, en la pantalla del Colector de NetFlow se verá un gráfico circular.

Nota: Es posible que no se envíe el primer conjunto de pings al Colector de NetFlow porque el proceso de ARP primero debe resolver direcciones IP y MAC. Si no aparece un gráfico circular después de 30 segundos, repitan el ping al gateway predeterminado.

e. Haga clic en el gráfico circular o en la entrada de las referencias para mostrar los detalles del registro del flujo.

f. El registro del flujo tendrá entradas similares a las de la siguiente tabla. Sus marcas de hora serán diferentes.

Entrada	Valor	Explicación
Traffic contribution	100 % (1/1)	Esta es la proporción de todo el tráfico representado por este flujo.
IPV4 SOURCE ADDRESS	10.0.0.10	Esta es la dirección IP de origen de los paquetes del flujo.

Entrada	Valor	Explicación
IPV4 DESTINATION ADDRESS	10.0.0.1	Esta es la dirección IP de destino de los paquetes del flujo.
TRNS SOURCE PORT	0	Este es el puerto de origen de la capa de transporte. El valor es 0 porque se trata de un flujo ICMP.
TRNS DESTINATION PORT	0	Este es el puerto de destino de la capa de transporte. El valor es 0 porque se trata de un flujo ICMP.
IP PROTOCOL	1	Esto identifica al servicio de la Capa 4; suele ser 1 para ICMP, 6 para TCP y 17 para UDP.
timestamp first	00:47:49.593	Esta es la marca de hora correspondiente al comienzo del flujo.
timestamp last	00:47:52.598	Esta es la marca de hora correspondiente al último paquete del flujo.
tcp flags	0x00	Este es el valor del marcador de TCP. En este caso, no participa ninguna sesión de TCP porque el protocolo es ICMP.
counter bytes	512	Esta es la cantidad de bytes en el flujo.
counter packets	4	Esta es la cantidad de paquetes en el flujo.
interface input	Gig0/0	Esta es a interfaz del exportador de flujos que recogió el flujo en el sentido de entrada (ingreso a la interfaz del dispositivo de monitoreo).
interface output	Null	Esta es a interfaz del exportador de flujos que recogió el flujo en el sentido de salida (egreso de la interfaz del dispositivo de monitoreo). El valor es "Null" porque se trataba de un ping a la interfaz de entrada.

En este caso, el flujo representa al ping de ICMP desde el host 10.0.0.10 hacia 10.0.0.1. Había cuatro paquetes de ping en el flujo. Los paquetes ingresan a la interfaz G0/0 del exportador.

Nota: En esta actividad, el router perimetral se ha configurado como exportador de flujos de NetFlow. La interfaz LAN está configurada para monitorear los flujos que ingresan a ella desde la red LAN. La interfaz serial se ha configurado para recolectar flujos que ingresan a ella desde Internet. Esto se ha hecho para simplificar esta actividad.

Para ver el tráfico que coincide con una sesión bidireccional completa, el exportador de NetFlow tendría que configurarse para recoger flujos que ingresan y salen de la red.

Paso 3: Crear tráfico adicional

a. Haga clic en **PC-2 > Desktop**.

b. Abra un símbolo del sistema y haga **ping** al gateway predeterminado: 10.0.0.1.

¿Qué esperan ver en los registros de flujo del colector de NetFlow? ¿Cambiarán las estadísticas correspondientes al registro de flujo ya existente, o aparecerá un flujo nuevo en el gráfico circular?

c. Regrese a PC-1 y repita el ping al gateway.

¿Cómo se representará este tráfico? ¿Cómo un segmento nuevo en el gráfico circular, o modificará los valores del registro de flujo ya existente?

d. Emita pings desde PC-3 y PC-4 a la dirección del gateway predeterminado.

¿Qué debería suceder en la pantalla del colector de flujos?

Parte 2: Observar registros de NetFlow correspondientes a una sesión que ingresa y sale del colector

El exportador de NetFlow se ha configurado para recoger los flujos que salen de la red LAN e ingresan al router desde Internet.

Paso 1: Acceder al servidor web por dirección IP

Antes de continuar, apaguen y enciendan el Colector de NetFlow para borrar los flujos.

a. Haga clic en **Colector de NetFlow > Ficha Física.**

b. Haga clic en el botón de encendido rojo para apagar el servidor. Luego, vuelva a hacerle clic para encenderlo nuevamente. (**Nota**: Es posible que tenga que desplazarse o alejarse).

c. En el colector de NetFlow, haga clic en la pestaña **Escritorio.**

d. Haga clic en el ícono del Colector de Netflow. Haga clic en el botón de opción “Activado” para activar el colector. Cierre la ventana del Colector de NetFlow.

e. Antes de acceder a un servidor web desde PC-1, prediga cuántos flujos habrá en el gráfico circular. Explique su respuesta.

Basándose en lo que sabe sobre protocolos de red y NetFlow, prediga los valores correspondientes a las solicitudes de páginas web que salen de la red LAN.

Campo de registro	Valor	Pautas
Dirección IP de origen		N/D
Dirección IP de destino		N/D
Puerto de origen	1025–5000 (MS Windows de manera predeterminada, que es lo que utiliza PT.	Se trata de un valor aproximado que se crea dinámicamente.
Puerto de destino		N/D
Interfaz de entrada		N/D
Interfaz de salida		N/D

Prediga los valores correspondientes a la respuesta de la página web que ingresa al router del exportador de NetFlow desde Internet.

Campo de registro	Valor	Pautas
Dirección IP de origen		N/D
Dirección IP de destino		N/D
Puerto de origen		N/D
Puerto de destino	1025-5000	Este es cualquier valor asignado aleatoriamente desde el rango de puertos efímeros.
Interfaz de entrada		N/D
Interfaz de salida		N/D

f. Haga clic en **PC-1 > Escritorio**. Si es necesario, cierre la ventana del Símbolo del sistema. Haga clic en el ícono del navegador web.

g. En el navegador web de PC-1, introduzca 192.0.2.100 y haga clic en **Go** (Ir). Aparecerá la página web del Sitio web de ejemplo.

h. Después de una breve demora, aparecerá un gráfico circular nuevo en el colector de NetFlow. Verá al menos dos segmentos circulares correspondientes a la solicitud y a la respuesta HTTP. Podría ver un tercer segmento si se excedió el tiempo de espera del caché de ARP correspondiente a PC-1.

i. Haga clic en el segmento circular de HTTP para mostrar el registro y verificar sus predicciones.

j. Haga clic en el enlace a la página de Copyrights.

¿Qué ocurrió? Explique. (Pista: compare el número de puerto en el host correspondiente a los flujos).

Paso 2: Acceder al servidor web por dirección IP

a. Apague y encienda el Colector de NetFlow para borrar los flujos.

b. Active el servicio del Colector de NetFlow.

c. Antes de acceder al servidor web por su dirección URL.

¿Qué espera ver en la pantalla del colector de NetFlow?

d. En PC-1, introduzca **www.example.com** en el campo de la URL y presione **Go** (Ir).

e. Después de que los flujos aparezcan en la pantalla, inspeccione cada registro de los flujos. ¿Qué valores ve para el campo del protocolo IP del registro del flujo? ¿Qué significan estos valores?