Configuración y captura de paquetes integrados en el software

Contenido

Introducción

Este documento describe la función de captura integrada en paquetes (EPC) en el software Cisco IOS®.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IOS Release 12.4(20)T o posterior
- Cisco IOS XE versión 15.2(4)S - 3.7.0 o posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cuando está habilitado, el router captura los paquetes enviados y recibidos. Los paquetes se almacenan dentro de un búfer en la DRAM y no persisten durante una recarga. Una vez que se capturan los datos, se pueden examinar en una vista de resumen o detallada en el router.

Además, los datos se pueden exportar como un archivo de captura de paquetes (PCAP) para permitir un examen más detallado. La herramienta se configura en modo exec y se considera un instrumento de personal temporario. Como resultado, la configuración de la herramienta no se almacena dentro de la configuración del router y no permanece en su lugar después de una recarga del sistema.

La herramienta Generador y analizador de configuración de captura de paquetes está disponible para que los clientes de Cisco puedan ayudar en la configuración, captura y extracción de capturas de paquetes.

Ejemplo de Configuración de Cisco IOS

Configuración básica de EPC

1. Defina un 'buffer de captura', que es un buffer temporal donde se almacenan los paquetes capturados.
2. Hay varias opciones que se pueden seleccionar cuando se define el búfer, como el tamaño, el tamaño máximo del paquete y el formato circular/lineal:

```
monitor capture buffer BUF size 2048 max-size 1518 linear
```

3. Se puede aplicar un filtro para limitar la captura al tráfico deseado. Defina una lista de control de acceso (ACL) en el modo de configuración y aplique el filtro al búfer:

```
ip access-list extended BUF-FILTER
    permit ip host 192.168.1.1 host 172.16.1.1
    permit ip host 172.16.1.1 host 192.168.1.1
```

```
monitor capture buffer BUF filter access-list BUF-FILTER
```

4. Defina un punto de captura que defina la ubicación en la que se produce la captura.

5. El punto de captura también define si la captura se produce para IPv4 o IPv6 y en qué ruta de switching (proceso frente a cef):

```
monitor capture point ip cef POINT fastEthernet 0 both
```

6. Adjuntar el búfer al punto de captura:

```
monitor capture point associate POINT BUF
```

7. Inicie la captura:

```
monitor capture point start POINT
```

8. La captura está ahora activa. Permitir la recopilación de los datos necesarios.
9. Detener la captura:

```
monitor capture point stop POINT
```

10. Examine el búfer en la unidad:

```
show monitor capture buffer BUF dump
```

> Nota: Esta salida sólo muestra el volcado hexadecimal de las capturas de paquetes. Para verlos en el humano legible hay dos maneras.

Exporte el búfer del router para un análisis más detallado:

```
monitor capture buffer BUF export tftp://10.1.1.1/BUF.pcap
```

El método anterior no siempre es práctico, ya que requería acceso T/FTP al router. En tales situaciones, tome una copia del volcado hexadecimal y utilice cualquier convertidor hex-pcap en línea para ver los archivos.

11. Una vez recopilados los datos necesarios, elimine el 'punto de captura' y el 'búfer de

captura':

```
no monitor capture point ip cef POINT fastEthernet 0 both
no monitor capture buffer BUF
```

Información de Configuración Adicional de Cisco IOS

- En las versiones anteriores a Cisco IOS Release 15.0(1)M, el tamaño del búfer estaba limitado a 512K.
- En las versiones anteriores a Cisco IOS Release 15.0(1)M, el tamaño del paquete capturado estaba limitado a 1024 bytes.
- El buffer de paquetes se almacena en la DRAM y no persiste durante las recargas.
- La configuración de captura no se almacena en la NVRAM y no se conserva durante las recargas.
- El punto de captura se puede definir para capturar en las trayectorias de conmutación de procesos o cef.
- El punto de captura se puede definir para capturar sólo en una interfaz o globalmente.
- Cuando el búfer de captura se exporta en formato PCAP, no se conserva la información L2 (como la encapsulación Ethernet).
- Consulte Prácticas recomendadas para comandos de búsqueda para obtener más información sobre los comandos utilizados en esta sección.

Configuración básica de exportación de tráfico IP

La exportación del tráfico IP es un método diferente para exportar paquetes IP que se reciben en interfaces WAN o LAN múltiples y simultáneas.

1. En el modo de configuración defina un perfil de exportación de tráfico IP.

```
Device(config)# ip traffic-export profile mypcap mode capture
```

2. Configure el tráfico bidireccional en el perfil.

```
Device(config-rite)# bidirectional
```

3. Salida

4. Especifique la interfaz para el tráfico exportado.

```
Device(config-if)# interface GigabitEthernet 0/1
```

5. Habilite la exportación de tráfico IP en la interfaz.

```
Device(config-if)# ip traffic-export apply mypcap size 10000000
```

6. Salida

7. Inicie la captura. La captura está ahora activa. Permitir la recopilación de los datos necesarios.

```
Device# traffic-export interface GigabitEthernet 0/1 start
```

8. Detenga la captura.

```
Device# traffic-export interface GigabitEthernet 0/1 stop
```

9. Exporte la captura a un servidor TFTP externo.

```
Device# traffic-export interface GigabitEthernet 0/1 copy tftp://<TFTP_Address>/mypcap.pcap
```

10. Una vez recopilados los datos necesarios, suprima el perfil.

```
Device(config)# no ip traffic-export profile mypcap
```

Desventajas de la exportación de tráfico IP

La exportación del tráfico IP tiene estas desventajas en comparación con el método EPC:

- La interfaz donde se exporta el tráfico capturado debe ser una interfaz Ethernet.
- Sin compatibilidad con IPv6.
- Sin información de capa 2, solo capa 3 y superior.

Ejemplo de Configuración de Cisco IOS-XE

La función Embedded Packet Capture se introdujo en Cisco IOS XE Release 3.7 - 15.2(4)S. La

configuración de la captura es diferente a la de Cisco IOS porque agrega más funciones.

Configuración básica de EPC

1. Defina la ubicación en la que tiene lugar la captura:

```
monitor capture CAP interface GigabitEthernet0/0/1 both
```

2. Asocie un filtro. El filtro se especifica en línea o se puede hacer referencia a una ACL o a un mapa de clase:

```
monitor capture CAP match ipv4 protocol tcp any any limit pps 1000000
```

3. Inicie la captura:

```
monitor capture CAP start
```

4. La captura está ahora activa. Permita que recopile los datos necesarios.

5. Detener la captura:

```
monitor capture CAP stop
```

6. Examine la captura en una vista de resumen:

```
show monitor capture CAP buffer brief
```

7. Examine la captura en una vista detallada:

```
show monitor capture CAP buffer detailed
```

8. Además, exporte la captura en formato PCAP para su posterior análisis:

```
monitor capture CAP export tftp://10.0.0.1/CAP.pcap
```

9. Una vez recopilados los datos necesarios, elimine la captura:

```
no monitor capture CAP
```

Additional Information

- La captura se realiza en interfaces físicas, subinterfaces e interfaces de túnel.
- Filtros basados en Network Based Application Recognition (NBAR) (que utilizan el **match protocol** bajo el mapa de clase) no se soportan actualmente.
- Consulte Prácticas recomendadas para comandos de búsqueda para obtener más información sobre los comandos utilizados en esta sección.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Para EPC que se ejecuta en Cisco IOS-XE®, este comando debug se utiliza para asegurarse de que EPC esté configurado correctamente:

```
debug epc provision
debug epc capture-point
```

Información Relacionada

- Captura de paquetes integrada: Cisco IOS-XE
- Captura de paquetes integrada: Cisco IOS
- Asistencia técnica y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).