Capturas de paquetes en la experiencia móvil conectada (CMX)

Contenido

Introducción

Este documento describe en cómo recoger a las capturas de paquetes del CLI del servidor móvil conectado 10.x de la experiencia (CMX). Estas capturas de paquetes pueden ayudar en resolver problemas varios escenarios (por ejemplo: Comunicación NMSP entre el regulador del Wireless LAN (WLC) y CMX servidor) para validar el flujo de la comunicación.

Requisitos

- Acceso del comando line interface(cli) al servidor CMX.
- La Computadora con Wireshark instaló para leer las capturas detalladamente.

Usando el TCPDUMP para las capturas

El TCPDUMP es un analizador de paquete que visualiza haber transmitido y los paquetes recibidos en el servidor CMX. Sirve como un análisis y herramienta de Troubleshooting para la red/los administradores de sistema. El paquete es incorporado al servidor CMX donde los datos sin procesar de los paquetes se pueden mirar.

El tcpdump corriente como usuario del “cmxadmin” fallaría con el error siguiente: (se requiere el acceso de la “raíz”)

```
In this example, tcpdump is attempted to be run as a 'cmxadmin' user.

[cmxadmin@laughter ~]$ tcpdump -i eth0 port 16113
tcpdump: eth0: You don't have permission to capture on that device (socket: Operation not
permitted)
```

Switch “para arraigar” al usuario después de abrir una sesión como usuario del “cmxadmin” al CLI sobre SSH o la consola.

```
[cmxadmin@laughter ~]$ su - root
Password:
[root@laughter ~]#
```

Usando la interfaz correcta

Anote la interfaz donde los paquetes serían capturados. Puede ser obtenida usando el “ifconfig-a”

```
In this example, 10.10.10.25 is the IP address of CMX server and 'eth0' is the interface it's
tied to on the server.
[cmxadmin@laughter ~]$ ifconfig -a eth0 Link encap:Ethernet HWaddr 00:50:56:A1:38:BB inet
addr:10.10.10.25 Bcast:10.10.10.255 Mask:255.255.255.0 inet6 addr:
2003:a04::250:56ff:fea1:38bb/64 Scope:Global inet6 addr: fe80::250:56ff:fea1:38bb/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:32593118 errors:0 dropped:0
overruns:0 frame:0 TX packets:3907086 errors:0 dropped:0 overruns:0 carrier:0 collisions:0
txqueuelen:1000 RX bytes:3423603633 (3.1 GiB) TX bytes:603320575 (575.3 MiB) lo Link encap:Local
Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING
MTU:65536 Metric:1 RX packets:1136948442 errors:0 dropped:0 overruns:0 frame:0 TX
packets:1136948442 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX
bytes:246702302162 (229.7 GiB) TX bytes:246702302162 (229.7 GiB) [cmxadmin@laughter ~]$
```

Captura de los paquetes

```
This example captures and displays all packets that are sourced from port - 16113 and enter the
CMX server on the eth0 interface.

[root@laughter ~]# tcpdump -i eth0 src port 16113 tcpdump: verbose output suppressed, use -v or
-vv for full protocol decode listening on eth0, link-type EN10MB (Ethernet), capture size 65535
bytes 09:50:29.530824 IP 172.18.254.249.16113 > laughter.cisco.com.40020: Flags [P.], seq
983381312:983382645, ack 2483597279, win 191, options [nop,nop,TS val 1792647414 ecr
1148435777], length 1333 09:50:31.507118 IP 172.18.254.249.16113 > laughter.cisco.com.40020:
Flags [.], seq 1333:2715, ack 1, win 191, options [nop,nop,TS val 1792647908 ecr 1148437650],
length 1382 09:50:31.507186 IP 172.18.254.249.16113 > laughter.cisco.com.40020: Flags [P.], seq
2715:2890, ack 1, win 191, options [nop,nop,TS val 1792647908 ecr 1148437650], length 175
09:50:33.483166 IP 172.18.254.249.16113 > laughter.cisco.com.40020: Flags [P.], seq 2890:4239,
ack 1, win 191, options [nop,nop,TS val 1792648402 ecr 1148439626], length 1349 09:50:35.459584
IP 172.18.254.249.16113 > laughter.cisco.com.40020: Flags [P.], seq 4239:5396, ack 1, win 191,
options [nop,nop,TS val 1792648896 ecr 1148441603], length 1157 ^C 5 packets captured 5 packets
received by filter 0 packets dropped by kernel [root@laughter ~]#
```

Para escribir la salida a un archivo

```
In this example, tcpdump would capture packets that are from 10.10.20.5 received on it's eth0
interface and write it to a file named TEST_NMSP_WLC.pcap.

[root@laughter cmxadmin]# tcpdump -i eth0 src 10.10.20.5 -w TEST_NMSP_WLC.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^C7 packets captured
7 packets received by filter
0 packets dropped by kernel
[root@laughter cmxadmin]#
```

El archivo está una vez listo, usted necesitará extraer el archivo .pcap del CMX a su ordenador para el análisis en una herramienta más cómoda tal como wireshark. Usted puede utilizar cualquier aplicación de SCP para hacer tan. Por ejemplo en Windows, la aplicación de WinSCP permitirá que usted conecte con el CMX usando las credenciales de SSH y usted puede después hojear el sistema de archivos y encontrar el archivo .pcap que usted acaba de crear. Para encontrar el trayecto actual, tipo “pwd” después de ejecutar el tcpdump para saber dónde el archivo fue guardado.

Para capturar el número específico de paquetes

Si un número específico de cuenta de paquetes se desea, usando - la opción c filtra exactamente para esa cuenta.

```
[root@laughter ~]# tcpdump -Z root -i eth0 -c 5 src 10.10.20.5 -w CMX_WLC_Capture.pcap tcpdump:
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes 5 packets captured 6
packets received by filter 0 packets dropped by kernel [root@laughter ~]#
```

Otras opciones de filtro

```
[root@laughter cmxadmin]# tcpdump -i eth0 dst 10.10.20.5 (filtered based on destination IP
address)
[root@laughter cmxadmin]# tcpdump -i eth0 src 10.10.20.4 (filtered based on Source IP address)

[root@laughter cmxadmin]# tcpdump -i eth0 port 80  (filtered for packets on port 80 in both
directions)
[root@laughter cmxadmin]# tcpdump -i eth0 port 443  (filtered for packets on port 443 in both
directions)
```

Las capturas escritas a los archivos serían guardadas en el directorio actual en el servidor y se pueden copiar hacia fuera para el estudio detallado usando Wireshark.