# Capturas de paquetes en Connected Mobile Experience (CMX)

## Contenido



## Introducción

Este documento describe cómo recopilar capturas de paquetes del servidor CLI de Connected Mobile Experience (CMX) 10.x. Estas capturas de paquetes pueden ayudar en la resolución de problemas en varios escenarios (por ejemplo: Comunicación NMSP entre el controlador de LAN inalámbrica (WLC) y el servidor CMX) para validar el flujo de comunicación.

## Requirements

- Acceso de la interfaz de línea de comandos (CLI) al servidor CMX.
- Ordenador con Wireshark instalado para leer las capturas en detalle.

## Uso de TCPDUMP para Capturas

TCPDUMP es un analizador de paquetes que muestra los paquetes transmitidos y recibidos en el servidor CMX. Sirve como herramienta de análisis y resolución de problemas para administradores de redes/sistemas. El paquete está integrado en el servidor CMX donde se pueden ver los datos sin procesar de los paquetes.

La ejecución de tcpdump como usuario 'cmxadmin' fallaría con el siguiente error: ('acceso raíz' es obligatorio)

```
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)
```

Cambie al usuario 'root' después de iniciar sesión como usuario 'cmxadmin' a la CLI sobre SSH o consola.

```
[cmxadmin@laughter ~]$ su - root
```

```
Password:
[root@laughter ~]#
```

## Uso de la interfaz correcta

Tenga en cuenta la interfaz donde se capturarían los paquetes. Se puede obtener mediante el comando '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 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 el resultado en 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]#
```

Una vez que el archivo esté listo, tendrá que extraer el archivo .pcap del CMX a su equipo para analizarlo en una herramienta más cómoda, como wireshark. Puede utilizar cualquier aplicación SCP para hacerlo. Por ejemplo, en Windows, la aplicación WinSCP le permitirá conectarse al CMX utilizando las credenciales SSH y, a continuación, podrá navegar por el sistema de archivos y encontrar el archivo .pcap que acaba de crear. Para buscar la ruta actual, escriba "pwd" después de ejecutar tcpdump para saber dónde se guardó el archivo.

## Para capturar un número específico de paquetes

Si se desea un número específico de conteo de paquetes, el uso de los filtros de la opción -c exactamente para ese conteo.

```
[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 filtrado

```
[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 en los archivos se guardarán en el directorio actual del servidor y se pueden copiar para una revisión detallada mediante Wireshark.