

Packet Capture of Connected Mobile Experience (CMX)

Inhoud

[Inleiding](#)

[Vereisten](#)

[Het gebruik van TCPDUMP voor Capture](#)

[De juiste interface gebruiken](#)

[Packet opnemen](#)

[De uitvoer naar een bestand schrijven](#)

[Om een specifiek aantal pakketten op te nemen](#)

[Andere filteropties](#)

Inleiding

Dit document beschrijft hoe u pakketvastlegging kunt verzamelen op de CLI van Connected Mobile Experience (CMX) server met 10.x. Deze pakketvastlegging kan u helpen bij het oplossen van meerdere scenario's (bijvoorbeeld: NMSP Communications tussen Wireless LAN Controller (WLC) en CMX-server) om de communicatiestroom te valideren.

Vereisten

- Opdracht Line Interface (CLI) toegang tot de CMX-server.
- Computer met Wireshark geïnstalleerd om de opnamen in detail te lezen.

Het gebruik van TCPDUMP voor Capture

TCPDUMP is een pakketanalyzer die de verzonden en ontvangen pakketten op de CMX-server weergeeft. Het dient als analyse- en probleemoplossing voor netwerk-/systeembeheerders. Het pakket is ingebouwd in de CMX server waar de ruwe gegevens van de pakketten kunnen worden bekeken.

De volgende fout heeft betrekking op het uitvoeren van tcpdump als cmxadmin-gebruiker: ('root'-toegang is vereist)

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)
```

Schakelt over naar 'root'-gebruiker na inloggen als 'cmxadmin'-gebruiker naar de CLI via SSH of console.

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

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

De juiste interface gebruiken

Houd rekening met de interface waarin de pakketten worden opgenomen. Het kan verkregen worden met behulp van de "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:fe1:38bb/64  Scope:Global  
      inet6 addr: fe80::250:56ff:fe1:38bb/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 ~]$
```

Packet opnemen

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 ~]#
```

De uitvoer naar een bestand schrijven

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]#
```

Nadat het bestand klaar is, moet u het .pcap-bestand van de CMX naar uw computer ophalen voor analyse in een comfortabeler gereedschap zoals Wireshark. U kunt een SCP-toepassing gebruiken om dit te doen. In Windows bijvoorbeeld kunt u met de WinSCP-toepassing verbinding maken met de CMX met behulp van de SSH-referenties en u kunt vervolgens naar het bestandssysteem bladeren en het .pcap-bestand vinden dat u zojuist hebt gemaakt. Om het huidige pad te vinden typt u "pwd" na het uitvoeren van het tcpDump om te weten waar het bestand was opgeslagen.

Om een specifiek aantal pakketten op te nemen

Als een specifiek aantal pakketstellingen wordt gewenst, is het gebruik van de optie -c precies voor die telling filters vereist.

```
[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 ~]#
```

Andere filteropties

```
[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)
```

De Captures die naar bestanden zijn geschreven, worden opgeslagen in de huidige map op de server en kunnen worden gekopieerd voor een gedetailleerd review met Wireshark.