

# Acquisizioni pacchetti su Connected Mobile Experience (CMX)

## Sommario

[Introduzione](#)

[Requisiti](#)

[Utilizzo di TCP DUMP per le acquisizioni](#)

[Uso dell'interfaccia giusta](#)

[\\_Acquisizione dei pacchetti](#)

[Per scrivere l'output in un file](#)

[Per acquisire un numero specifico di pacchetti](#)

[Altre opzioni di filtro](#)

## Introduzione

Questo documento descrive come raccogliere le acquisizioni di pacchetti dalla CLI del server Connected Mobile Experience (CMX) 10.x. Queste acquisizioni di pacchetti possono essere utili nella risoluzione dei problemi in diversi scenari (ad esempio: Comunicazione NMSP tra Wireless LAN Controller (WLC) e server CMX) per convalidare il flusso di comunicazione.

## Requisiti

- Accesso CLI (Command Line Interface) al server CMX.
- Computer con Wireshark installato per leggere le clip in dettaglio.

## Utilizzo di TCP DUMP per le acquisizioni

TCP DUMP è un analizzatore di pacchetti che visualizza i pacchetti trasmessi e ricevuti sul server CMX. Funge da strumento di analisi e risoluzione dei problemi per gli amministratori di rete e di sistema. Il pacchetto è incorporato nel server CMX in cui è possibile esaminare i dati raw dei pacchetti.

L'esecuzione di tcpdump come utente 'cmxadmin' non riesce con il seguente errore: (è necessario l'accesso alla directory principale)

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)
```

Passare all'utente "root" dopo aver eseguito l'accesso come utente "cmxadmin" alla CLI su SSH o sulla console.

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

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

## Uso dell'interfaccia giusta

Prendere nota dell'interfaccia su cui i pacchetti verrebbero acquisiti. È possibile ottenerlo utilizzando il 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: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 ~]$
```

## Acquisizione dei pacchetti

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 ~]#
```

## Per scrivere l'output in un file

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]#
```

Quando il file è pronto, sarà necessario estrarre il file .pcap dal CMX al computer per l'analisi in uno strumento più comodo, ad esempio Wireshark. A tale scopo, è possibile utilizzare qualsiasi applicazione SCP. Ad esempio, in Windows, l'applicazione WinSCP consente di connettersi al CMX utilizzando le credenziali SSH. È quindi possibile esplorare il file system e individuare il file .pcap appena creato. Per trovare il percorso corrente, digitare "pwd" dopo aver eseguito tcpdump per sapere dove è stato salvato il file.

## Per acquisire un numero specifico di pacchetti

Se si desidera un numero specifico di pacchetti, usare i filtri dell'opzione -c esattamente per quel numero.

```
[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 ~]#
```

## Altre opzioni di 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)
```

Le clip scritte nei file vengono salvate nella directory corrente sul server e possono essere copiate per una revisione dettagliata utilizzando Wireshark.