

# Procedure di acquisizione dei pacchetti Prime Infrastructure

## Sommario

[Introduzione](#)

[Usare il comando tcpdump](#)

[Copia i file catturati in una posizione esterna](#)

[Acquisisci pacchetti come utente root](#)

[Esempio di clip utente root](#)

## Introduzione

In questo documento viene descritto l'uso del comando `tcpdump` CLI per acquisire i pacchetti desiderati da un server Cisco Prime Infrastructure (IP).

## Usare il comando tcpdump

In questa sezione vengono forniti esempi che illustrano il modo in cui il comando `tcpdump` viene utilizzato.

```
nms-pi/admin# tech dumptcp ?  
<0-3> Gigabit Ethernet interface number
```

L'output del comando `show interface` restituisce informazioni precise sul nome e sul numero dell'interfaccia attualmente in uso.

```
nms-pi/admin# tech dumptcp 0 ?  
count Specify a max package count, default is continuous (no limit)  
<cr> Carriage return.
```

**Nota:** È possibile indicare il numero di pacchetti specifico nel comando precedente. Se non si indica un numero specifico di pacchetti, viene eseguita un'acquisizione continua senza limiti.

```
nms-pi/admin# tech dumptcp 0 | ?  
Output modifier commands:  
begin Begin with line that matches  
count Count the number of lines in the output  
end End with line that matches  
exclude Exclude lines that match  
include Include lines that match  
last Display last few lines of the output
```

```
nms-pi/admin# tech dumtcp 0 > test-capture.pcap
```

**Nota:** È più semplice salvare il file e quindi rivederlo. In questo esempio, il server salva il file nella radice della struttura di directory. Per visualizzare i file, immettere il comando **dir**.

## Copia i file catturati in una posizione esterna

Di seguito sono riportati due esempi che illustrano il modo in cui i file catturati vengono copiati in una posizione esterna al server:

- Nell'esempio, il file di acquisizione viene copiato su un server FTP con indirizzo IP **1.2.3.4**:

```
copy disk:/test-capture.pcap ftp://1.2.3.4/
```

- Nell'esempio, il file di acquisizione viene copiato su un server TFTP con un indirizzo IP **5.6.7.8**:

```
copy disk:/test-capture.pcap tftp://5.6.7.8/
```

## Acquisisci pacchetti come utente root

Se si desidera ottenere acquisizioni più granulari, accedere alla CLI come utente *root* dopo aver eseguito l'accesso come utente *amministratore*.

```
test$ ssh admin@12.13.14.15
Password:
nms-pi/admin#
nms-pi/admin# root
Enter root password :
Starting root bash shell ...
ade # su -
[root@nms-pi~]#
```

## Esempio di clip utente root

Di seguito sono riportati tre esempi di clip acquisite da un utente root:

- Nell'esempio, vengono acquisiti tutti i pacchetti destinati alla porta **162** sul server IP:

```
[root@nms-pi~]# tcpdump -i eth0 -s0 -n dst port 162
```

- Nell'esempio, tutti i pacchetti destinati alla porta **9991** vengono catturati e scritti in un file chiamato **test.pcap** nella directory **/localdisk/ftp/**:

```
[root@nms-pi~]# tcpdump -w /localdisk/ftp/test.pcap -s0 -n dst port 9991
```

- Nell'esempio, vengono acquisiti tutti i pacchetti con indirizzo IP di origine **1.1.1.1**:

```
[root@nms-pi~]# tcpdump -n src host 1.1.1.1
```