Linux tcpdump????

```
tcpdump -i ethX icmp and icmp[icmptype]=icmp-echo
```

查看 tcpdump 可以監聽的接口列表:

```
tcpdump -D
```

在接口 eth0 上監聽:

```
tcpdump -i eth0
```

監聽任何可用的接口 (不能在混雜模式下完成。需要 Linux 內核 2.2 或更高版本)：

```
tcpdump -i any
```

捕獲數據包時要詳細:

```
tcpdump -v
```

捕獲數據包時更詳細:

```
tcpdump -vv
```

捕獲數據包時要非常詳細:

```
tcpdump -vvv
```

詳細並以十六進制和 ASCII 格式打印每個數據包的數據，不包括鏈路級標頭:

```
tcpdump -v -X
```

詳細並以十六進制和 ASCII 格式打印每個數據包的數據，還包括鏈路級標頭:

```
tcpdump -v -XX
```

捕獲數據包時不那麼冗長（比默認設置）：

```
tcpdump -q
```

將捕獲限制為 100 個數據包:

```
tcpdump -c 100
```

將數據包捕獲記錄到名為 capture.cap 的文件中:

```
tcpdump -w capture.cap
```

將數據包捕獲記錄到一個名為 capture.cap 的文件中，但會在屏幕上顯示實時捕獲了多少數據包:

```
tcpdump -v -w capture.cap
```

顯示一個名為 capture.cap 的文件的數據包:

```
tcpdump -r capture.cap
```

使用名為 capture.cap 的文件的最大詳細信息顯示數據包:

```
tcpdump -vvv -r capture.cap
```

捕獲數據包時顯示 IP 地址和端口號，而不是域名和服務名稱（注意：在某些系統上，您需要指定 -nn 來顯示端口號）：

```
tcpdump -n
```

捕獲目標主機為 192.168.1.1 的任何數據包。顯示 IP 地址和端口號:

```
tcpdump -n dst host 192.168.1.1
```

捕獲源主機為 192.168.1.1 的任何數據包。顯示 IP 地址和端口號:

```
tcpdump -n src host 192.168.1.1
```

捕獲源或目標主機為 192.168.1.1 的任何數據包。顯示 IP 地址和端口號:

```
tcpdump -n host 192.168.1.1
```

捕獲目標網絡為 192.168.1.0/24 的任何數據包。顯示 IP 地址和端口號:

```
tcpdump -n dst net 192.168.1.0/24
```

捕獲源網絡為 192.168.1.0/24 的任何數據包。顯示 IP 地址和端口號:

```
tcpdump -n src net 192.168.1.0/24
```

捕獲源或目標網絡為 192.168.1.0/24 的任何數據包。顯示 IP 地址和端口號:

```
tcpdump -n net 192.168.1.0/24
```

捕獲目標端口為 23 的任何數據包。顯示 IP 地址和端口號:

```
tcpdump -n dst port 23
```

捕獲目標端口介於 1 和 1023 (含) 之間的任何數據包。顯示 IP 地址和端口號:

```
tcpdump -n dst portrange 1-1023
```

僅捕獲目標端口介於 1 和 1023 (含) 之間的 TCP 數據包。顯示 IP 地址和端口號:

```
tcpdump -n tcp dst portrange 1-1023
```

僅捕獲目標端口介於 1 和 1023 (含) 之間的 UDP 數據包。顯示 IP 地址和端口號:

```
tcpdump -n udp dst portrange 1-1023
```

捕獲目標 IP 為 192.168.1.1 和目標端口為 23 的任何數據包。顯示 IP 地址和端口號:

```
tcpdump -n “dst host 192.168.1.1 and dst port 23”
```

捕獲目標 IP 為 192.168.1.1 和目標端口為 80 或 443 的任何數據包。顯示 IP 地址和端口號:

```
tcpdump -n “dst host 192.168.1.1 and (dst port 80 and dst port 443)”
```

捕獲任何 ICMP 數據包:

```
tcpdump -v icmp
```

捕獲任何ARP數據包:

```
tcpdump -v arp
```

捕獲ICMP或ARP數據包:

```
tcpdump -v “icmp or arp”
```

捕獲任何廣播或多播的數據包:

```
tcpdump -n “broadcast or multicast”
```

為每個數據包捕獲500字節的數據，而不是默認的68字節:

```
tcpdump -s 500
```

捕獲數據包內的所有數據字節:

```
tcpdump -s 0
```

Revision #1
Created 3 August 2025 04:47:00 by Jason
Updated 3 August 2025 04:47:26 by Jason