[Howto] How to use tcpdump in network debugging?

Tcpdump is a tool to dump traffic on a network.This data can be dumped to file or viewed normally.

Examples

List of network interfaces

```
user@localhost:~$ sudo tcpdump -D
1.eth0
2.any (Pseudo-device that captures on all interfaces)
3.lo
```

Capture all traffic path in eth0 then write it to file named "tcpdumpfile" and set the each file size to be around 3M without trying to resolve IP/Port name

```
[user@localhost ~]# sudo tcpdump -nnxX -i eth0 -w tcpdumpfile -C 3
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
82 packets captured
166 packets received by filter
0 packets dropped by kernel
```

To print all packets arriving from or departing to 10.0.2.2

```
[user@localhost ~]# sudo tcpdump -nnvvv -i eth0 host 10.0.2.2
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
07:14:13.748986 IP (tos 0×0, ttl 64, id 0, offset 0, flags [DF], proto: ICMP (1), length: 84) 10.0.2.15 > 10.0.2.2: ICMP echo request, i
07:14:13.749484 IP (tos 0×0, ttl 255, id 6544, offset 0, flags [DF], proto: ICMP (1), length: 84) 10.0.2.2 > 10.0.2.15: ICMP echo reply
```

capture all traffic dst to http port and coming form my loop back interface

```
[user@localhost ~]# sudo tcpdump -vvv -i lo dst port http
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes
07:18:39.937891 IP (tos 0×0, ttl 55, id 52591, offset 0, flags [none], proto: TCP (6), length: 44) localhost.36901 > 10.0.2.15.http: S,
07:18:40.937973 IP (tos 0×0, ttl 39, id 62265, offset 0, flags [none], proto: TCP (6), length: 44) localhost.36902 > 10.0.2.15.http: S,
```

capture all Address Resolution Protocol (ARP) packets

```
[user@localhost ~]# sudo tcpdump -nnevvv -c 3 arp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
07:23:47.914195 08:00:27:ed:89:bd > ff:ff:ff:ff:ff:ff, ethertype ARP (0×0806), length 42: arp who-has 10.0.2.3 tell 10.0.2.15
07:23:47.914514 52:54:00:12:35:03 > 08:00:27:ed:89:bd, ethertype ARP (0×0806), length 60: arp reply 10.0.2.3 is-at 52:54:00:12:35:03
07:23:54.698897 08:00:27:ed:89:bd > ff:ff:ff:ff:ff:ff, ethertype ARP (0×0806), length 42: arp who-has 10.0.2.2 tell 10.0.2.15
3 packets captured
7 packets received by filter
0 packets dropped by kernel
```

Try to capture icmp traffic AND to or from the host 10.0.2.2

```
[user@localhost ~]# sudo tcpdump -nn icmp host 10.0.2.2
tcpdump: ‘icmp’ modifier applied to host
[user@localhost ~]#
```