Watching and Manipulating Your Network Traffic

tcpdump - your binoculars

```
$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
14:59:39.168508 IP a204-2-177-16.deploy.akamaitechnologies.com.www > josiah-
desktop.local.34594: . 884145450:884146898(1448) ack 1384394675 win 6266 <nop,nop,timestamp
612468726 176413364>
14:59:39.168526 IP josiah-desktop.local.34594 > a204-2-177-
16.deploy.akamaitechnologies.com.www: . ack 1448 win 1267 <nop,nop,timestamp 176413372
612468726>
14:59:39.170034 IP a204-2-177-16.deploy.akamaitechnologies.com.www > josiah-
desktop.local.34594: . 1448:2896(1448) ack 1 win 6266 <nop,nop,timestamp 612468726 176413364>
14:59:39.170052 IP josiah-desktop.local.34594 > a204-2-177-
16.deploy.akamaitechnologies.com.www: . ack 2896 win 1313 <nop,nop,timestamp 176413372
612468726>
...
14:59:39.284334 IP ec2-174-129-15-1.compute-1.amazonaws.com.www > josiah-desktop.local.50615: P
3587518292:3587518498(206) ack 329762849 win 66 <nop,nop,timestamp 1308615091 176412617>
14:59:39.284367 IP josiah-desktop.local.50615 > ec2-174-129-15-1.compute-1.amazonaws.com.www: .
ack 206 win 108 <nop,nop,timestamp 176413401 1308615091>
14:59:39.284374 IP ec2-174-129-15-1.compute-1.amazonaws.com.www > josiah-desktop.local.50615: F
206:206(0) ack 1 win 66 <nop,nop,timestamp 1308615091 176412617>
14:59:39.284580 IP josiah-desktop.local.50615 > ec2-174-129-15-1.compute-1.amazonaws.com.www: F
1:1(0) ack 207 win 108 <nop,nop,timestamp 176413401 1308615091>
```

A packet as seen by tcpdump

14:59:39.284374 IP ec2-174-129-15-1.compute-1.amazonaws.com.www > josiah-desktop.local.50615:F 206:206(0) ack 1 win 66 <nop,nop,timestamp 1308615091 176412617>

19:56:05.497478 arp who-has 192.168.1.16 tell 192.168.1.1

19:57:33.302510 IP 192.168.1.42.53708 > 192.168.1.24.snmp: GetRequest(38) E:hp.2.3.9.4.2.1.4.1.5.2.39.0

19:58:30.954951 IP 192.168.1.25.54733 > resolver1.opendns.com.domain: 23503+ PTR? 24.1.168.192.in-addr.arpa. (43)
19:58:30.990415 IP resolver1.opendns.com.domain > 192.168.1.25.54733: 23503 NXDomain 0/0/0 (43)

20:01:50.159642 IP 192.168.1.25.ntp > time7.apple.com.ntp: NTPv4, Client, length 48

20:09:37.686346 IP 192.168.1.25.63770 > 192.168.1.255.netbios-ns: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST

tcpdump examples

- `tcpdump`
- `tcpdump -i eth1`
- `tcpdump -c 25 > dump_to_file`
- `tcpdump host adam and not src eve`
- `tcpdump -n host adam or eve and port 80 and vlan 1`
- `tcpdump -F filename host adam`

If all else fails, pipe it to grep

```
$ tcpdump | grep www
```

iproute2 - your swiss army knife

- Replaces ifconfig, route, iptunnel and others
- Sudo apt-get install iproute
- Setup nics and virtual nics
- Configure routing tables
- Setup multiple routing tables
- Set rules that restrict traffic flow
- Set rules that enable traffic flow
- Setup simple point-to-point tunnels
- Configure ARP table

Iproute - managing interfaces

- ip addr add 10.10.20.254/24 dev eth0
- ip addr add 10.20.0.254/24 label eth0:1 dev eth0
- ip address del

iproute - Routes

ip route add default dev eth1 via 66.77.88.99

ip route add 10.0.0.0/24 dev eth1:1

ip route delete (ip r d)

ip route change (ip r c)

ip route show (ip r s)

iproute - the routing table

```
$ ip route sh table main

10.0.0.0 dev eth0  scope link

10.11.12.0/24 dev eth0  proto kernel  scope link  src 10.11.12.13

192.168.1.0/24 dev eth0  proto kernel  scope link  src 192.168.1.159
metric 1

169.254.0.0/16 dev eth0  scope link  metric 1000
default via 192.168.1.254 dev eth0
```

iproute Rules!

```
ip rule add from unknown type  unreachable priority 3000

ip rule add from enemy type blackhole priority 3001

ip rule add fwmark 1 table hide-the-good-stuff \
  priority 3002

ip rule add from 10.10.20.0/24 to 192.168.0.0/24 \
  type unreachable priority 3003
```

iproute - Tunnels

ip addr add 10.0.0.1/30 label eth1:1 dev eth1

ip tunnel add my_tunnel mode ipip local 10.0.0.1 /
remote 66.77.88.1 ttl 64 dev eth1

ip address add dev my_tunnel 10.0.0.1 peer 10.0.0.2/32

iproute - neighbours

```
$ ip neigh sh
192.168.1.5 dev eth0  FAILED
192.168.1.4 dev eth0 lladdr 00:1e:c9:dd:d8:b8 REACHABLE
192.168.1.254 dev eth0 lladdr 00:50:da:21:8c:11 REACHABLE
192.168.1.3 dev eth0  FAILED
192.168.1.2 dev eth0 lladdr 00:11:2f:11:08:3e STALE
```

Thank You!

http://josiahritchie.com/cposc09

Josiah Ritchie
josiah@fim.org
http://josiahritchie.com
@josiahritchie
facebook.com/josiah.ritchie