Linux Networking Commands

https://campus.barracuda.com/doc/48202759/

To help you find and solve networking problems, this article describes some Linux utilities and their commonly used options and parameters. Usage examples for the utilities are also provided. For more information on any of the following utilities, see their man pages.

ip

The ***ip*** tool is a TCP/IP interface configuration and routing utility. Use it to configure and view routing, devices, policy routing, and tunnels. You can also use it to configure network interfaces. To display all the options for this command, enter ***ip*** at the CLI.

ip a

Displays the list of used network interfaces (physical and virtual) with their assigned MAC addresses.

```
[root@winix:/]# ip a 1: lo: <loopback> mtu 16436 qdisc noqueue link/loopback
00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/24 brd 127.0.0.255
scope host lo:loop 2: tap0: mtu 1500 qdisc noqueue link/ether
fe:fd:00:00:00:00 brd ff:ff:ff:ff:ff:ff inet 127.0.1.1/24 brd 127.0.1.255
scope host tap0:fw 3: tap1: <broadcast> mtu 1500 qdisc noqueue link/ether
fe:fd:00:00:00:00 brd ff:ff:ff:ff:ff:ff inet 127.0.2.1/24 brd 127.0.2.255
scope host tap1:vpn inet 169.254.1.11/32 scope global tap1:aux1 4: tap2: mtu
1500 qdisc noqueue link/ether fe:fd:00:00:00:00 brd ff:ff:ff:ff:ff:ff inet
127.0.3.1/24 brd 127.0.3.255 scope host tap2:vpnpers inet 169.254.1.11/32
scope global tap2:aux2
```

ip r g <network address>

Displays information about the device that is bound to the specified IP address.

```
[root@winix:/]# ip r g 10.0.6.31 local 10.0.6.31 dev lo src 10.0.6.31 cache
<local> mtu 16436 advmss 16396
```

ip a a <IP> dev <device name>

Adds an IP address to the specified device.

> The IP address is removed again when the network or the Barracuda NextGen Firewall F-Series is restarted. A device route is only added if a netmask has been given with the IP address.

```
[root@winix:/]# ip a a 10.0.4.236 dev eth2
```

ip a d <IP> dev <device name>

Deletes an IP address from the specified device.

```
[root@winix:/]# ip a d 10.0.4.236 dev eth2
```

> If you use this command to remove a server or box IP address, the Control daemon will take action and reintroduce the deleted IP addresses.

tcpdump

To inspect packets, use the ***tcpdump*** utility. It is a sniffer tool that captures packets off a network interface and interprets them. It prints out the headers of packets on a network interface that match the Boolean expression. It understands all basic Internet protocols. It can also be used to save entire packets for later inspection.

OPTIONS

Use the following options to specify which network interfaces you want to inspect:

- ***-i [interface] | any***
  Specifies an interface name. To execute ***tcpdump*** on all available interfaces, use ***any*** . To combine multiple devices, use ***and/or*** .
- ***host <ip address>***
  Specifies a host IP address. To combine multiple hosts, use ***and/or*** .
- ***port <port number>***
  Specifies a queried port. To combine multiple ports, use ***and/or*** .

```
[root@winix:/]# tcpdump -i eth0 -nnn -s0 host 10.0.10.10 and host 10.0.10.11
and port 801 [root@winix:/]# tcpdump -v -vv -n -nn -s0 -i any host
192.168.10.1 and 212.72.195.42 and port 443 [root@winix:/]# tcpdump -v -vv -n
-nn -s0 -i any -w /tmp/dump.cap host 192.168.10.1 and 212.72.195.42 and port
443
```

fsck

If HDD/MEM tests are passing without errors, use the *fsck* utility with the following options to check and repair file systems:

fsck -A -y

These options solve most of the possible errors after a power outage because the utility checks all file systems and attempts to fix most detected file system corruption.

rpm

To check the kernel module architecture, use the *rpm* utility with the following options:

rpm -q --qf="%{arch}" kernel