Troubleshooting Network Connections

[?] Where do you start when troubleshooting network connectivity?

Establish Scope

- IPv4

    - `ping`
    - `traceroute`

        - `yum install traceroute`

    - `tracepath`

- IPv6

    - `ping6`
    - `traceroute6`

        - `yum install traceroute`

    - `tracepath6`

[?] Where do we go if the problem is on our end?

- Configuration Files

    - RedHat based distros

        - `/etc/sysconfig/network-scripts/ifcfg-eth0`
        - `/etc/sysconfig/network`

    - Debian based distros

        - `/etc/network/interfaces`

    - Check name resolution servers/order

        - `/etc/resolv.conf`
        - `order hosts,bind,nis`
        - `order bind,hosts,nis`

    - Check local name resolution

        - `/etc/hosts`

- Verifying Settings

    - `ip`

        - Replacement for `ifconfig`
        - `ip addr`

            - Lists interface addresses
            - Netmasks and CIDR

        - `ip link`

            - Displays current link status

- `ip -s link` provides statistics

- `ip route`

  - Displays the routing table

[?] What if our settings don't match the running configuration?

- Reset Networking

  - `service network restart`
  - `systemctl restart network.service`

[?] Can we see if traffic is actually coming in and out?

- ss - Display network connections

  - `ss -atp` (All sessions)
  - `ss -tp` (Active sessions)
  - `ss --route` displays routing table
  - `ss --program` attempts to display software using ports

- Packet Capture

  - `tcpdump`
  - Displays packets passing through an interface
  - `tcpdump -i eth0 > data.txt`
  - `tail -f ./data.txt`

[?] Is there anything we can do if we think a firewall is blocking us?

- netcat

  - `nc`
  - Tests connections to hosts
  - `nc itpro.tv 80`
  - `GET`
  - `netstat -an | grep itpro.tv`