Network troubleshooting

Last modified: 2014-06-09 15:49:42

A few opinionated checklists for network troubleshooting. RHEL/CentOS 7 is assumed.

General guidelines

A few best practices when setting up and troubleshooting network services

- **Automate** your tests or at least use a **checklist**
- Keep your checklist **up-to-date** as you learn new things
- Be **thorough**, don't skip steps (e.g checking the cables)
- Follow a **bottom-up** approach according to OSI or TCP/IP model layers
- **Error messages** usually give a clue of where to look. Google them.
- Work in **small steps** and verify every step.
- Don't assume. **Test**.
- Keep a **backup** copy of the original configuration, and the latest working version.
- Always **validate the syntax** of config files before applying them
- Know what **logs** to look at
- Open a separate terminal that shows the **logs in realtime** (`journalctl -f`)

Network configuration

1. Fysical/data link layer
    - Is the cable plugged in?
    - Check Ethernet port lights
    - Test Ethernet cable
2. Network layer: local settings
    - Check **IP address**: `ip address`
    - Is there a **default gateway**: `ip route`
    - Do we have **DNS servers**: `cat /etc/resolv.conf`
3. Network layer: remote
    - Ping default gateway (*)
    - Query DNS servers: `dig www.example.com @x.y.z.w`

(*) `Ping` doesn't always work, as some system administrators block ICMP traffic on their routers.

Network services

An example for `httpd`, can be applied to other services. Assume you just did `systemctl start httpd.service`, but you still can't see your website.

Don't forget to validate the network configuration of the server!

1. Validate configuration file

    - `apachectl configtest`

2. Is the service running?

    - `sudo netstat -tlnp` (options: `t` = tcp, `l` = listening, `n` = show port numbers, `p` = show process)
    - `sudo systemctl status httpd.service`

3. Check the log files for error messages: `journalctl -b -u httpd`
4. Test local connection (using client software), e.g.

    - `wget http://localhost/`
    - `curl http://localhost/`

5. Test remote connection, e.g.

    - use client software
    - `sudo nmap -sS -p 80` (perform a TCP SYN scan on port 80 using `nmap`)

6. Check firewall settings

    - `sudo iptables -L -n -v`
    - TODO: check configuration, fix (using `firewalld`)