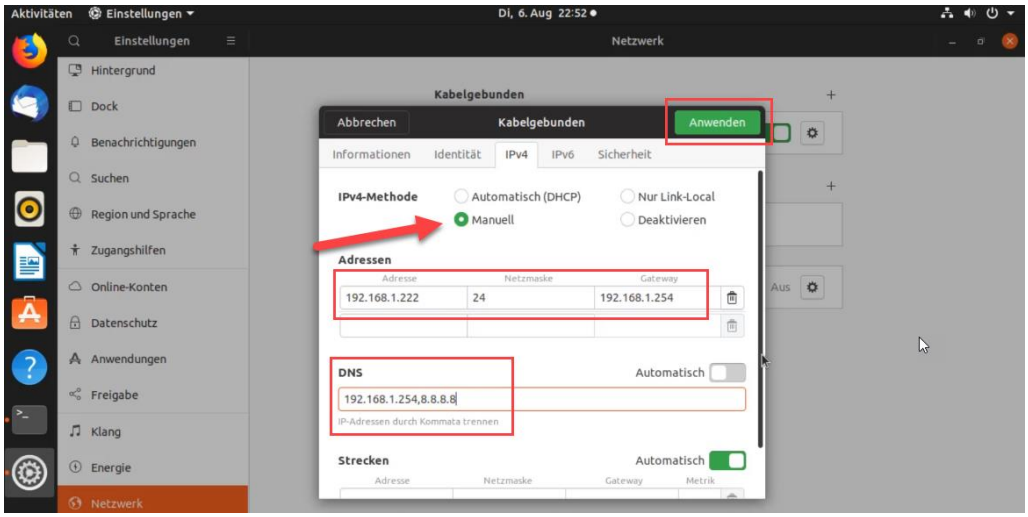
Zusammenfassung Tag 26

Grundlegende Netzwerkeinstellungen abfragen

- Die Netzwerkkonfiguration kann sowohl über die GUI via NetworkManager als auch in der Kommandozeile vorgenommen werden
- Der NetworkManager wurde zunächst für WLAN-Umgebungen konzipiert, unterstützt mittlerweile aber alle Arten von Netzwerken
- Im Paket `iproute2` wird insbesondere das Programm `ip` mitgeliefert, das für alle Aspekte der IP-Konfiguration genutzt werden kann
- Jedes Linux-System hat eine Loopback-Schnittstelle (lo, 127.0.0.1/8 bzw. ::1/128), die zur systeminternen Kommunikation genutzt wird.
- Mit dem Tool `ss` lassen sich Kommunikationsverbindungen und Portbindungen anzeigen
- Die älteren Tools, wie `ifconfig`, `netstat` u.a. befinden sich im Paket `net-tools`, das mittlerweile oft separat installiert werden muss
- `/etc/resolv.conf` enthält traditionell die Nameserver-Einträge (DNS)
- Mittlerweile übernimmt das der Dienst systemd-resolved
- Der NetworkManager hat auch ein CLI-Frontend namens `nm-cli`

Grundlegende Netzwerk-Konfiguration mit dem NetworkManager

- Mit Hilfe der GUI geschieht die Konfiguration über die LAN-Einstellungen und das dortige IPv4-Register
- Dort finden wir die IPv4-Konfigurationsmethode, das Eingabefeld einer statischen IP-Adresse mit zugehöriger Netzmaske und das Default-Gateway
- Zudem kann hier ein DNS-Server angegeben werden



- Änderungen werden hier erst nach einer Re-Initialisierung wirksam, daher das Interface deaktivieren und danach wieder aktivieren
- Auch die IPv6-Konfiguration kann über die GUI vorgenommen werden

Grundlegende IP-Konfiguration auf der Kommandozeile

- Konfiguration auf der Kommandozeile ist distributionsabhängig
- Ubuntu und andere Debian-Derivate:
    - Datei `/etc/network/interfaces`
      Hier wurden früher die Interface-Parameter festgelegt. Heute in der Regel nur noch für das Loopback-Interface zuständig, da die anderen Interfaces vom Network-Manager verwaltet werden.
    - Datei `/etc/resolv.conf`
      Hier können DNS-Server eingetragen werden
    - Verzeichnis `/etc/netplan`
      Metaebene für die Netzwerk-Konfiguration namens `netplan`
    - Datei `01-network-manager-all.yaml` im Verzeichnis `/etc/netplan`
      In dieser Konfigurations-Datei steht, wer das Netzwerk verwaltet (i.d.R. NetworkManager)
    - Sollte die IP-Konfiguration auf der Kommandozeile angepasst werden, kann dies mit dem Tool `nmcli` durchgeführt werden. Die hier vorgenommenen Änderungen bleiben auch nach einem Neustart erhalten
- CentOS:
    - Setzt ab Version 7 auf den NetworkManager und das Tool `nmcli`
    - Verzeichnis `/etc/sysconfig/network-scripts`
      Hier befinden sich traditionell die Konfigurationsdateien für die vorhandenen Schnittstellen
    - Sollte die IP-Konfiguration auf der Kommandozeile angepasst werden, kann dies mit dem Tool `nmcli` durchgeführt werden. Diese Änderungen bleiben auch nach einem Neustart erhalten (analog zu Debian-Derivaten)

DNS mit dig & Co. Testen

- Linux implementiert mit dem Nameservice-Switch, kurz: `nsswitch`, ein Konzept, das die grundsätzliche Auflösung von Namen in numerische Werte regelt
  Konfigurationsdatei: `/etc/nsswitch.conf`
- Es gibt verschiedene Komponenten, wie `passwd`, `group`, `shadow`, `hosts` oder `protocols`, die eine Auflösung in numerische Werte benötigen
- Für die Benutzerverwaltung mittels `passwd`, `group`, etc. werden zunächst die entsprechenden Dateien zurate gezogen, also z.B. `/etc/passwd`, `/etc/group` oder `/etc/shadow`

- Wenn dort keine Auflösung erfolgen kann, wird ggf. ein systemd-Mechanismus gefragt. Wie dieser angesprochen wird, regeln Shared Libraries
- Bei Host-Namen wird zunächst die Datei `/etc/hosts` abgefragt
- Die Hosts-Datei wird in der Regel immer vor dem DNS-Mechanismus befragt, daher können hier gezielt Einträge vorgenommen werden, deren Namensauflösung frei wählbar sind
- Danach kommt mdns4_minimal, mDNS steht für Multicast DNS und ist ein spezieller, neuerer Dienst, der versucht, DNS-Namen per Multicast im lokalen Netz aufzulösen
- Der Befehl `getent` steht für Get Entity und ermöglicht das gezielte Auslesen eines Eintrags aus einer der administrativen Datenbankdateien, wie z.B. `passwd`, `hosts`, etc.
- Das Tool `nslookup` ist ein DNS-Clientprogramm. Es hat einen interaktiven Modus und kann DNS-Anfragen absetzen
- Das Tool `host` löst ebenfalls den Namen in IPv4- und IPv6-Adresse auf
- Mit `host -t` können wir den Abfragetyp ändern und nach Mailserver (mx) oder dem Nameserver (ns) fragen
- Die Ausgabe von `dig` enthält viele, zunächst kryptisch anmutende, Informationen und Werte. Diese entsprechen jedoch ziemlich genau den Datenfeldern der DNS-Pakete, die über das Netzwerk gehen, daher ist `dig` das leistungsstärkste Tool für DNS-Abfragen
- `dig` fragt per Default nur nach A-Einträgen, nicht aber nach AAAA
- `dig` nimmt nicht automatisch eine Reverse-Auflösung vor, dazu muss die Option `-x` gesetzt werden, z.B.: `dig @192.168.1.254 -x 8.8.8.8`

Den Hostnamen festlegen

- Der Hostname wird in verschiedenen Situationen verwendet und dient zur Identifikation des Hosts lokal und im Netzwerk
- Der Hostname wird im Prompt angezeigt und kann auf verschiedene Wege ausgegeben werden:
  Zum Beispiel mit `uname -n` oder `hostname`
- Der Hostname wird in der Datei `/etc/hostname` hinterlegt, der Befehl `hostname` greift hierauf zu
- Mit `hostname -f` kann der FQDN des Systems, also der vollständigen Hostnamen mit Domain und Toplevel-Domain angezeigt werden
- Mit `systemctl set-hostname "Name"` kann der Hostname konfiguriert werden, es gibt mittlerweile verschiedene Varianten:
  - Beim *Pretty Hostname* handelt es sich um eine erweiterte Form des Hostnames, wenn sonst eigentlich nicht erlaubte Zeichen verwendet werden
  - Der *Static Hostname* entfernt alle Sonderzeichen
  - Der *Transient Hostname* kann z.B. entstehen, wenn über eine dynamische Konfiguration ein Hostname übermittelt wird. Sobald ein statischer Hostname gesetzt ist, wird dieser jedoch bevorzugt

- Der eigene Hostname wird zur Identifikation verwendet
- Auch wenn ein Eintrag in der Datei `/etc/hosts` erzeugt wurde, können andere Systeme im Netzwerk diesen Namen deswegen noch nicht auflösen. Dazu bedarf es z.B. DNS, wobei der Name unseres Systems dann in der Zonendatei des DNS-Servers als A oder AAAA-Eintrag vorhanden sein muss

Statische Routen

- Statische Routen werden auf Clients nur in Ausnahmefällen benötigt, eher in Server-Netzwerken und auf Routern erforderlich
- Statische Routen werden notwendig für Subnetze, die nicht über das Default-Gateway erreicht werden können
- Ein Routingeintrag bzw. eine Route beginnt mit dem Routing-Ziel und der Adresse des Routers, also des Gateways über das der Traffic geleitet werden soll
- Als normaler User dürfen keine Routen gesetzt werden
- Der Befehl `ip r` zeigt die vorhandenen Routen
- Beispiel: Der Befehl `route add –net 172.16.20.128 netmask 255.255.255.128 gw 192.168.1.1` fügt eine entsprechende Route dazu. Das ausgehende Interface wird automatisch hinzugefügt.
- Bespiel: Der Befehl `ip route add 172.16.20.128/25 via 192.168.1.1 dev enp0s3` dient äquivalent dazu
- Nach dem Neustart sind diese statischen Routen nicht mehr vorhanden
- Traditionell können entsprechende Skripts unter `/etc/network` bei Debian-Derivaten und `/etc/sysconfig/network-scripts` bei Red Hat-Derivaten hinterlegt werden, die beim Systemstart die statischen Routen einrichten
- Heutzutage wird dies i.d.R. mit `systemd` und `nmcli` erledigt:
  - In der GUI über das Dialogfenster „Strecken" (holprige Übersetzung für Routen)
  - Auf der Kommandozeile mit `nmcli` durch den Befehl `set ipv4.routes 10.10.10.0/24 192.168.1.1`

Netzwerk-Troubleshooting

- Systematische Prüfung der eigenen IP-Konfiguration (Adresse und Subnetzmaske), Erreichbarkeit des Gateways, die Einstellung der Default-Route und die Routing-Tabelle führen meist zu einer ersten guten Diagnose
- Eines der wichtigsten Tools ist `ping`. Es prüft die grundsätzliche Netzwerk-Konnektivität mit dem Ziel
- Bei `ping` wird IPv6 immer bevorzugt, wenn eine entsprechende IPv6-Adresse zurückgeliefert wird (wenn ein Hostname als Ziel angegeben wird)
- ping hat noch viele andere Optionen und Parameter
- Wird nur `ping` eingegeben, erscheint eine Kurzhilfe

- Ein weiterer wichtiger Befehl ist `traceroute`. Er muss ggf. dediziert nachinstalliert werden mit `apt install inetutils-traceroute` bzw. `yum install traceroute`
- Mit `traceroute` können wir eine Routenverfolgung durchführen, die jeden Hop, also Router, auf dem Weg zum Ziel darstellt
- Der Parameter`--resolve-hostnames` löst die Hostnames dabei auf
- Durch `traceroute` können z.B. Routing-Schleifen entdeckt werden
- Es kann sowohl bei `ping` als auch bei `traceroute` dazu kommen, dass Systeme nicht antworten, weil sie eine aktive Firewall haben, die eine Antwort verhindert.
- Auch Netzwerk-Firewalls oder entsprechend konfigurierte Router im Pfad blockieren häufig entsprechende Pakete
- Ob ein System im selben Subnetz aktiv ist und ggf. aufgrund einer Firewall nicht mit uns kommunizieren will, können wir ermitteln, indem wir nach dem Verbindungsversuch den ARP-Cache für IPv4 bzw. den Neighbor-Cache für IPv6 checken: `ip neigh` oder `ip n`
- Ein ähnliches Tool wie `traceroute` ist `tracepath`, es zeigt einige weitere statistische Informationen an, unter anderem die sogenannte Path MTU, kurz: PMTU