IP-Adressorganisation und Ausfallsicherheit

IP-Adressvergabe

Problem außerhalb Lab:

- öffentliche IP Adressen werden nur von RIRs (Regional Internet Registry) vergeben
- IPv4: schlechte verfügbar und teuer aufgrund Adressknappheit
- IPv6: auf dem Campus noch nicht verfügbar

IP-Adressvergabe

Problem im Lab:

- Einsatz von Subnetting oder VLAN?
- dynamische / statische Vergabe bzw. Mischform?
- wie Kommunikation nach außen?
- genaue Umsetzung?, nur IPv4 oder auch IPv6?

IP-Adressvergabe außerhalb Lab

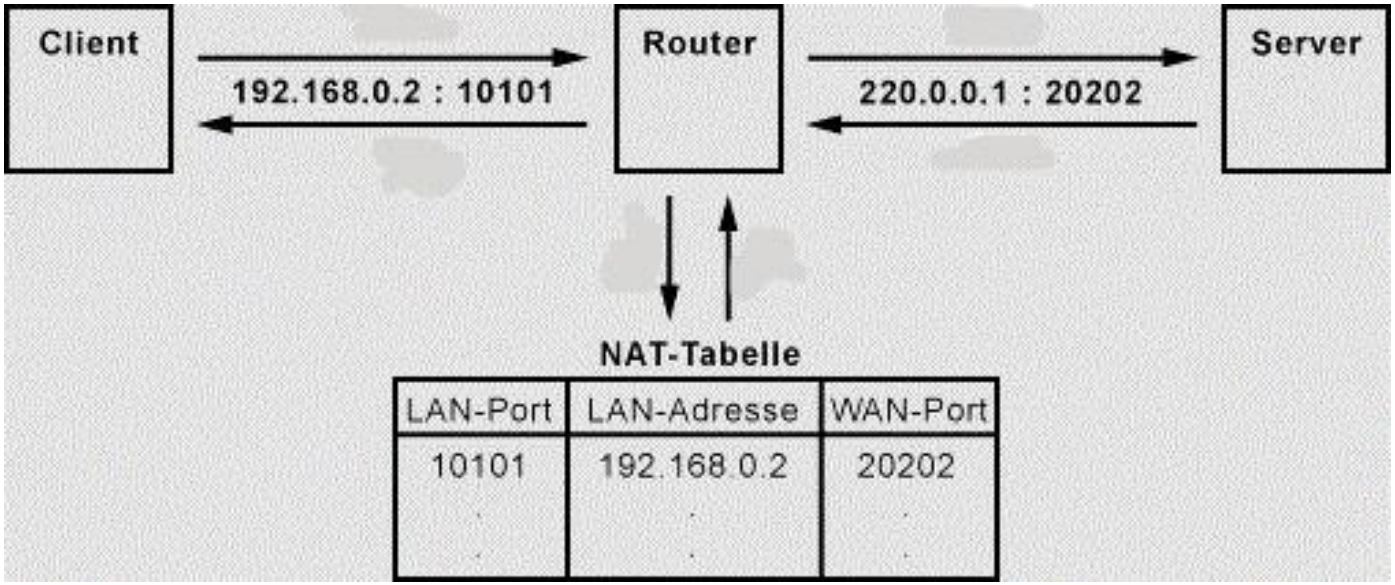
Mögliche Lösungen:

- **Proxy Server**
  Vermittler, der selbst nur eine öffentliche IP Adresse hat und mit privaten Netz verbunden ist

- **NAT-Router**
  ähnlich dem Proxy, aber weniger Funktionen

NAT (Network Adress Translation)

- Router mit einer öffentlichen IP ins Internet und einer privaten IP Adresse
- ermöglicht mehreren Hosts in privatem Netzwerk die Internetkommunikation über nur eine öffentliche IP-Adresse



Zuordnung von Datenpaketen zu Hosts über Port-Mapping oder mithilfe anderer Verbindungsinfos

Proxy Server

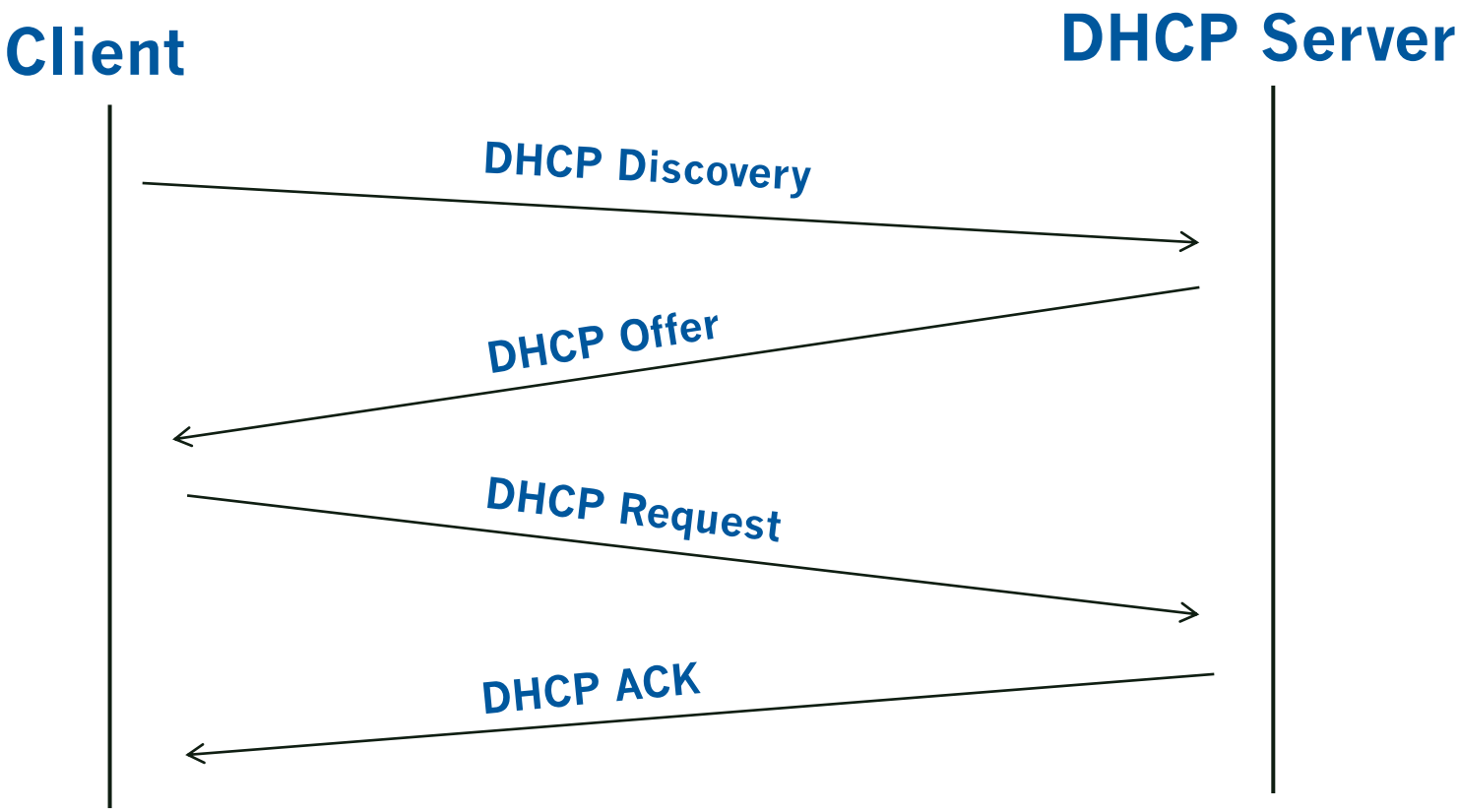
- ähnliche Logik wie NAT, besitzt also auch eine öffentliche und private IP Adresse
- kann auf bestimmte Kommunikationsprotokolle beschränkt werden
- NAT reicht Datenpakete nur durch, Proxy baut zu beiden Partnern jeweils eigenständige Verbindung auf
- => aktiver Eingriff in Kommunikation

IP-Adressvergabe im Lab

DHCP (Dynamic Host Configuration Protocol)

- komplett manuelle Zuweisung von IP Adressen => hoher Arbeitsaufwand, benötigt häufige Wartung durch Administrator
- => Automatische Zuordnung von IP Adressen in einem Netz
- Addressraum kann kleiner als Summe von Endgeräten sein, falls nicht alle Geräte gleichzeitig gebraucht werden

DHCP


Client
DHCP Server
DHCP Discovery
DHCP Offer
DHCP Request
DHCP ACK

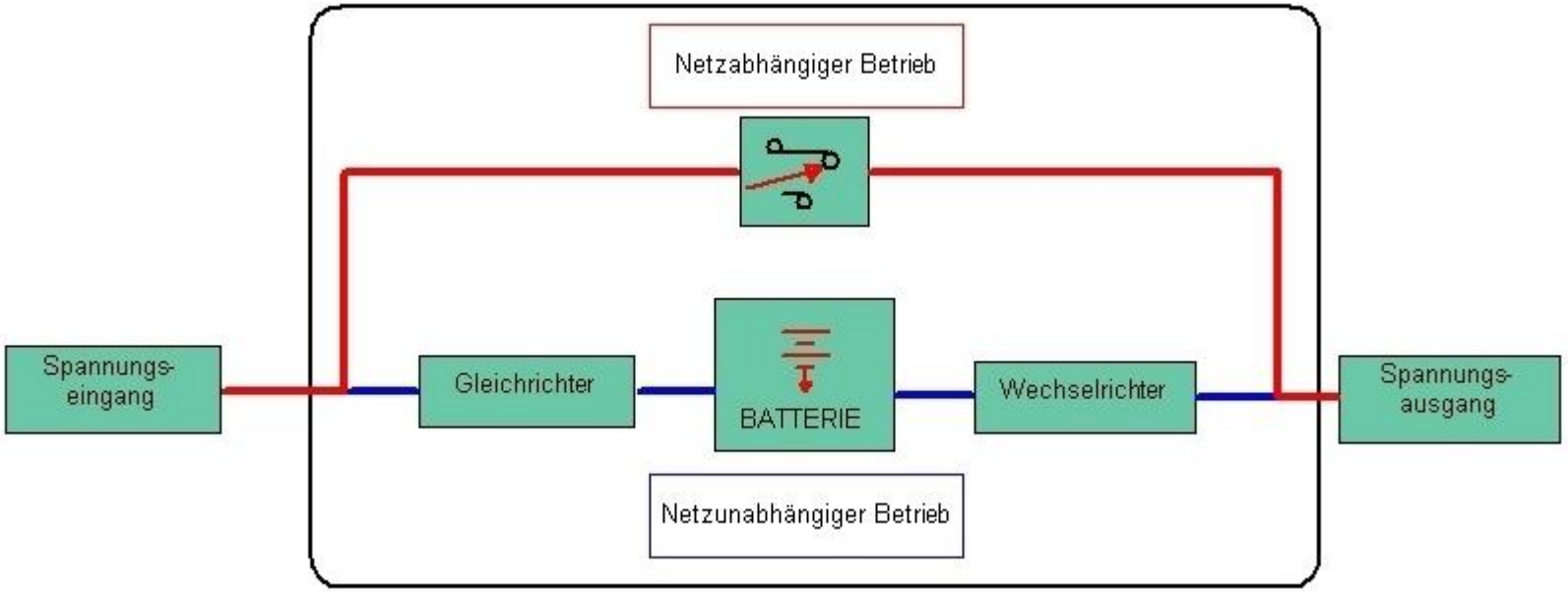
IP-Adressvergabe im Lab

- => dynamische Vergabe mittels DHCP für normale Endgeräte
- => Festlegung statischer IPs für Service-Geräte, z.B. VoIP + IPTV Server, Monitoring System etc.
- IPv6 vorerst nur innerhalb Lab-Netz
- Nutzung VLAN, statt Subnetting
- NAT für Internet⇔Lab
- Software: dnsmasq, iptables

Redundanz, Ausfallsicherheit

USV – Unterbrechungsfreie Stromversorgung

Zusätzliches Gerät das zwischen Stromversorgung von Servern und Stromnetz geschaltet wird -> reine Hardware-Lösung



Hauptaufgaben einer USV:

- Sicherstellung der Energieversorgung, bei Stromausfällen
- Schutz vor Spannungsstößen, Ausgleich von Spannungseinbrüchen
- Über- und Unterspannungschutz
- Ausgleich von Frequenzschwankungen
- Rausch- und Störungsunterdrückung
- Automatisches Herunterfahren nachgelagerter Komponenten

Arten von USVs

Online USV: Stromversorgung läuft dauerhaft über die Batterie der USV (oft trotzdem mit Bypass)

Vorteil:

- **dauerhafte Versorgung der Verbaucher**
- **galvanische Trennung**
- **meist „sauberste“ Ausgangskurve**

Nachteile:

- **teuer, nicht immer notwendig**
- **geringere Effizienz**

Arten von USVs

Offline USV: Stromversorgung läuft normal über Netz; im Störfall wird auf Batterie umgeschaltet

Vorteile:

- **günstiger, für Server ausreichend**
- **geringere Batteriebelastung**
- **höhere Effizienz**

Nachteile:

- **Umschaltzeit (~ 2 – 4 ms) vorhanden -> kurze Unterbrechung**
- **„weniger saubere“ Ausgangskurve**

Bonding / Link Aggregation

Prinzip: logische Bündelung von redundanter Hardware zur Erhöhung der Ausfallsicherheit oder Steigerung Datendurchsatz

Bei Ausfall einer Komponente ist Funktion immer noch sichergestellt

Bonding / Link Aggregation

Link Aggregation bei Linux über *Linux bonding driver* und *ifenslave* oder NetworkManager

Erzeugt eine logische NIC mit eigener MAC-Adresse, unter welcher physische Interfaces gebündelt werden

Voraussetzung: Unterstützung beider Endpunkte, alle physischen Links müssen Full-Duplex sein

Beispiel: 2 x 1Gbit/s => 1x ~2Gbit/s + Ausfallsicherheit

Redundanzkonzept für Lab

- Schutz der wichtigen Komponenten (Server, Storage) mit Offline- oder netzinteraktiver USV
- autom. Herunterfahrens der Komponenten, zusätzlich Benachrichtigung bei Ausfall, Problemen etc.
- Nutzung von Netzfilter und Überspannungsschutz an Endgeräten
- redundante Infrastruktur, z.B. mehrere Kabel zwischen zwei Endpunkten, redundante Switches, Anbindung mittels Link Aggregation