Inhalt

NAT IPv4 (Network Address Translation)

- **Problem**: Nicht ausreichend IPv4 Adressen verfügbar
- Private IPv4-Adressen werden nicht ins Internet geroutet
- **Lösung**: Wechsel zu IPv6 / Translation

Vorteile

- Erhält öffentliche IPv4 Adressen
- **Datenschutz**: Kein direkter Rückschluss von extern durch die öffentliche IP-Adresse auf den Ursprungs-Client
- Keine Änderung an internen Clients notwendig beim ISP-Wechsel

Nachteile

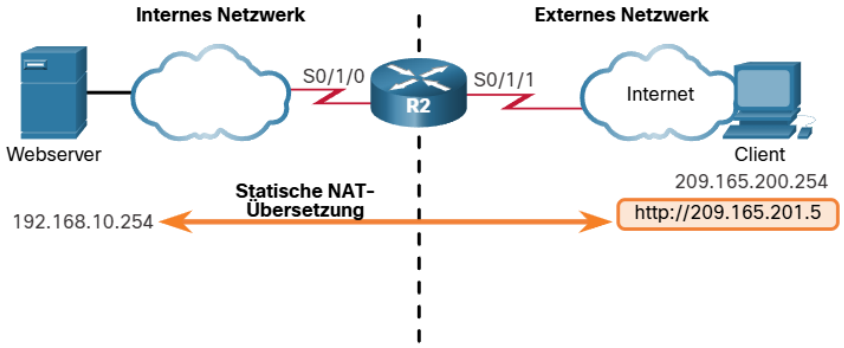
- Zusätzliche Verzögerung durch NAT/PAT (Kritisch bei Echtzeitprotokollen -> VoIP)
- End-to-End-Adressierung geht verloren (Manche Anwendungen kommen nicht mit NAT klar)
- Fehlersuche durch Adressänderung erschwert

Begriffe

- **NAT-Pool**: Menge an öffentlichen IP-Adressen an einem Router
- **Interne Adresse**: Adresse des Geräts, die mit NAT übersetzt wird
- **Externe Adresse**: Adresse des Zielgeräts
- **Lokale Adresse**: Im internen Netzwerk verwendet (Gibt Perspektive an)
- **Globale Adresse**: Im externen Netzwerk verwendet (Gibt Perspektive an)
- **Intern Lokal**: Adresse der Quelle aus Perspektive des internen Netzwerks
- **Intern Global**: Adresse der Quelle aus der Perspektive des externen Netzwerks
- **Extern Global**: Adresse des Ziels aus der Perspektive des externen Netzwerks
- **Extern Lokal**: Adresse des Ziels aus der Perspektive des internen Netzwerks
- **Beispiel**: PC sendet Daten an Öffentlichen Webserver
    - Interne Lokale wird am NAT-Router zur internen globalen Adresse
        - Private IP-Adresse (RFC1918) -> Öffentliche IP-Adresse aus NAT-Pool
    - Externe globale Adresse (also Ziel-IP) ändert sich in der Regel nicht, da das Ziel meistens öffentlich ist. Extern global und extern lokal sind dann identisch
    - Aus Sicht des öffentlichen Zielservers ist die Quell-IP die Interne globale Adresse (also öffentliche IP aus NAT-Pool)

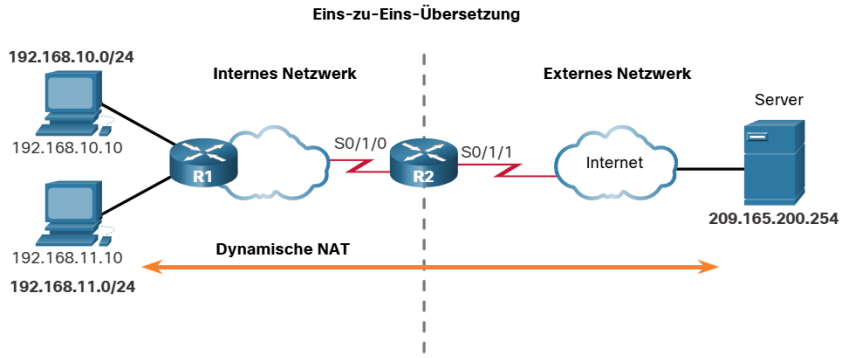
Arten von NAT

Statisches NAT



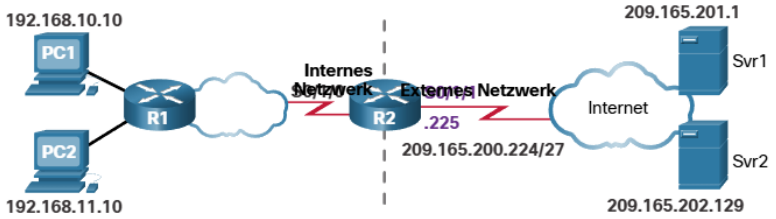
- 1:1 Übersetzung der privaten in öffentliche Adressen
- Für das Internet haben die einzelnen Geräte öffentliche IP-Adressen
- Manuell konfiguriert und zugeordnet
- Hilfreich, wenn Geräte von der gleichen öffentlichen IP erreichbar bleiben müssen (Webserver)
- Benötigt ausreichend öffentliche IP-Adressen
- Nur so viele parallele Sitzungen möglich wie öffentliche IP-Adressen verfügbar sind

Dynamisches NAT



- 1:1 Übersetzung der privaten in öffentliche Adressen
- Öffentliche IP-Adressen aus dem NAT-Pool werden bei einer Anfrage nach dem First-Come-First-Serve-Prinzip vergeben
- Nur so viele parallele Sitzungen möglich wie öffentliche IP-Adressen verfügbar sind

Port Address Translation (PAT)



NAT-Tabelle			
Interne lokale Adresse	**Interne globale Adresse**	**Externe globale Adresse**	**Externe lokale Adresse**
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.11.10:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

- N:1/M Übersetzung
  - Beliebig viele private Adressen zu einer oder mehreren öffentlichen Adressen
- Kommunikation eines internen Clients mit einem Webserver:
  - Client sendet Paket an Webserver und wählt einen Quell-Port
  - Router prüft, ob der Quell-Port schon in Verwendung ist
    - Wenn nicht wir der Port übernommen
    - Wenn bereits in Verwendung wird der nächste verfügbare Port verwendet
  - Router setzt interne globale Adresse + Quell-Port
  - Webserver antwortet auf diese IP-Adresse und setzt Quell-Port als Ziel-Port
  - Router kann das Paket vom Webserver eindeutig dem Client zuordnen.
    - Je nachdem, ob der Router den Port anpassen musste, stellt er den Ausgangs-Port wieder her
    - Zusätzliche Sicherheit: PAT prüft zusätzlich, ob die Daten vom Webserver überhaupt zuvor angefordert wurden
- Wenn alle Ports einer IP-Adresse aus dem NAT-Pool ausgeschöpft sind, wird mit der nächsten weiter gemacht, bis keine IP-Adressen und Ports mehr verfügbar sind
- Pakete ohne Schicht-4-Segment (Ohne Portnummer) erhalten vom Router eine Abfrage-ID um Anfrage und Antwort zuordnen zu können

CLI

Befehl	**Verwendung**
show ip nat translations [verbose]	Ausgabe aller konfigurierten / dynamischen Übersetzungen. Ggf. inklusive aktueller Externen Adressen „verbose“ gibt zusätzliche Informationen an (Zeit)
clear ip nat translations	Löschte alle dynamischen Übersetzungseinträge
show ip nat statistics	Zeigt Verwendete Interfaces, aktive Übersetzungen, Konfiguration, Anzahl der Adressen im Pool, Anzahl der zugewiesenen Adressen

RFC1918: Address Allocation for Private Internets

Klasse	**Bereich**	**Prefix**
A	10.0.0.0-10.255.255.255	10.0.0.0/8
B	172.16.0.0-172.31.255.255	172.16.0.0/12
C	192.168.0.0-192.168.255.255	192.168.0.0/16

Wide Area Network (WAN)

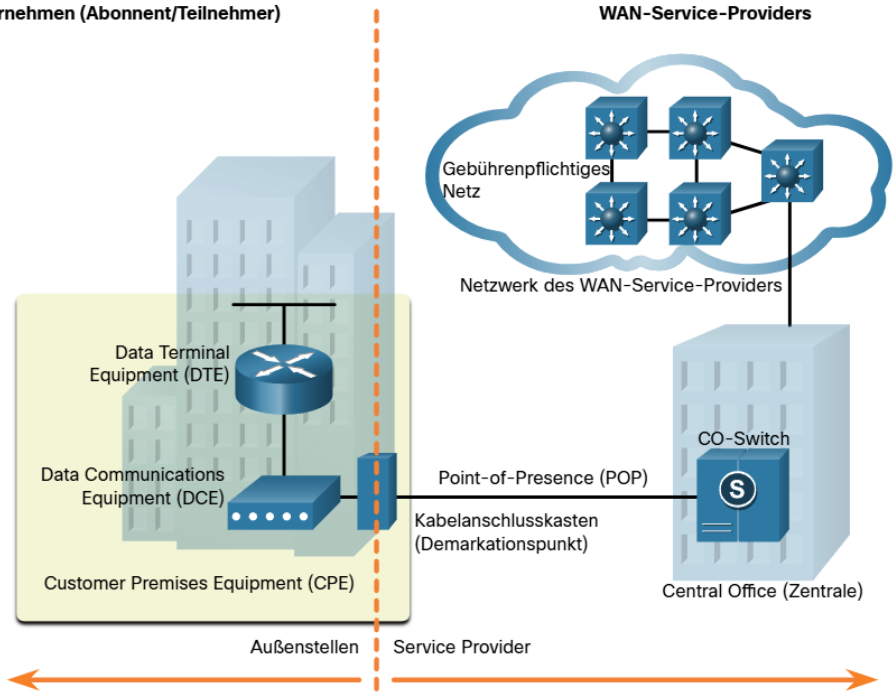
- **WAN**: Kommunikationsnetz, dass sich über einen großen geografischen Bereich erstreckt
- Notwendig um Remote-LANs mit dem eignen LAN zu vernetzen

Local Area Networks (LANs)	Wide Area Networks (WANs)
LANs stellen Netzwerk-Dienste innerhalb eines kleinen geografischen Bereichs zur Verfügung (d.h. Heim-, Büro-, Gebäude- oder Campus-Netzwerke).	WANs bieten Netzwerk-Dienste über große geografische Bereiche hinweg an (d.h. in und auch zwischen Städten, Ländern und Kontinenten.)
LANs werden verwendet, um lokale Computer, Peripheriegeräte und andere Geräte miteinander zu verbinden.	WANs dienen dazu, Remote-Benutzer, Netzwerke und Standorte miteinander zu verbinden.
Ein LAN befindet sich im Besitz eines Unternehmens oder eines Privatanwenders und wird von diesem verwaltet.	WANs werden von Internet-Service-, Telefon-, Kabel- und Satellitenanbietern betrieben und verwaltet.
Abgesehen von den Kosten für die Netzwerkinfrastruktur fallen keine Gebühren für die Nutzung eines LAN an.	WAN-Dienste hingegen werden gegen eine Gebühr bereitgestellt.
LANs ermöglichen hohe Übertragungsgeschwindigkeiten über kabelgebundene Ethernet- und Wi-Fi- Dienste.	WAN-Anbieter ermöglichen niedrige bis hohe Übertragungsgeschwindigkeiten über große Entfernungen mit komplexen physischen Netzwerken.

WANs im OSI-Modell

- Auf Layer 1 (Bitübertragunsschicht / Physical Layer) und 2 (Sicherungsschicht / Datalink Layer)
- **Layer 1**:
    - Elektronische, Mechanische Übertragung von Bits
    - Provider verwenden meistens Glasfaser für hohe Bandbreite und lange Strecken
        - Protokoll-Standards:
            - SDH: Synchronous Digial Hierachy
            - SONET: Synchronous Optical Networking
            - DWDM: Dense Wavelength Division Multiplexing
- **Layer 2**:
    - Definition der Framekapselung
    - Protokolle:
        - Breitband (DSL & Kabel)
        - Wireless
        - Ethernet-WAN
        - Multiprotocol Label Switching (MPLS)
        - Point-to-Point Protocol
        - High-Level Data Link Control

Begriffe

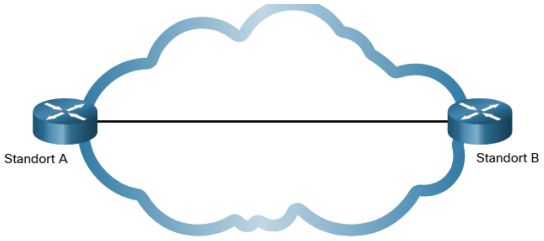


- **Data Terminal Equipment (DTE):** Verbindet Teilnehmer-LANs mit dem WAN-Kommunikationsgerät
- **Data Communications Equipment (DCE) (Datenleitungs-Endgerät):** Kommunikation mit dem Provider
- **Customer Premises Equipment (CPE):** Fasst DTEs und DCEs am Firmenstandort zusammen
- **Point-of-Presence (POP):** Punkt, an dem sich Teilnehmer- und Providernetz verbinden
- **Demarkationspunkt**: Offizieller Trennungspunkt zwischen CPE und Geräten vom Provider
- **Local Loop (letzte Meile):** Kupfer/Glasleitung, die CPE mit CO verbindet
- **Central Office (CO, Zentrale):** Einrichtung des Providers, die CPE mit Provider-Netz verbindet
- **Gebührenpflichtiges Netz:** Infrastruktur des Providernetzes
- **Backhaul Netzwerk:** Verbindet mehrere Zugangskonten des Providernetzes
- **Backbone-Netzwerk:** Großes Netzwerk; Hohe Kapazität; Verbindung von Prodivernetzen

WAN-Topologien

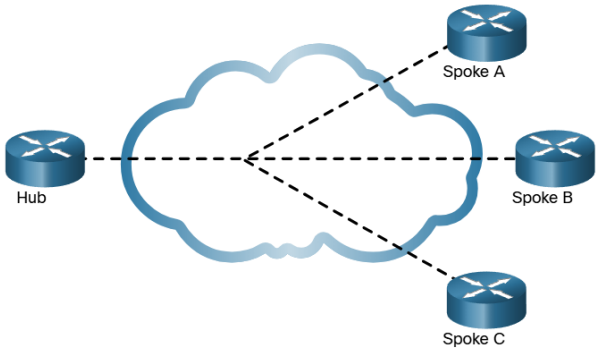
- Werden durch logische Topologien beschrieben

Punkt-zu-Punkt



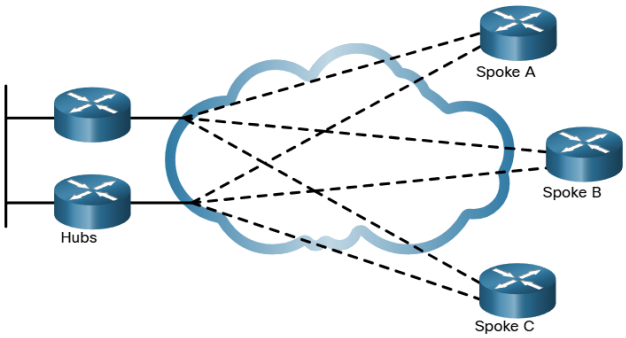
- Verbindung zwischen zwei Endpunkten
- Scheinbar eine physische Verbindung zwischen den Endpunkten
- Z.B. Standleitung (Teuer)

Hub-and-Spoke



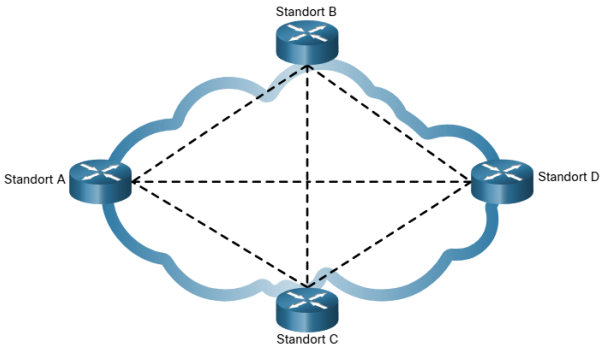
- Mehrere Spokes verwenden eine Schnittstelle des Hubs
    - Durch Subinterfaces oder virtuelle Verbindungen
- Spokes können nur über den Hub miteinander kommunizieren
- Hub ist Single-Point of Failure

Dual-Homed



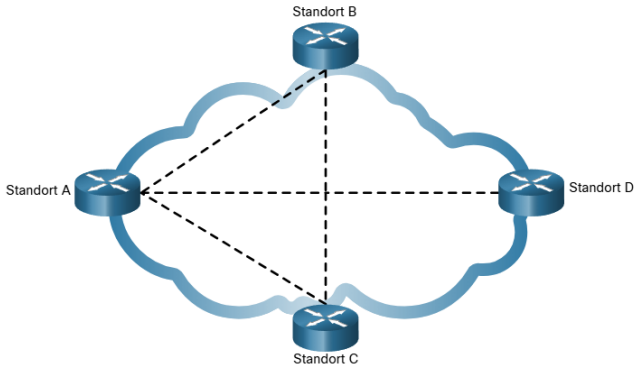
- Erweiterung von Hub-and-Spke
- Bietet Redundanz, Lastverteilung, dezentrale Datenverarbeitung
- Implementierung ist teurer (mehr Hardware nötig; komplexe Einrichtung)

Vollständig vermascht



- Mehrere virtuelle Verbindungen
- Alle Standorte miteinander vernetzt
- Hohe Fehlertoleranz

Teilweise vermascht



- Verbindet viele Standorte miteinander, aber nicht alle
- Schlechtere Fehlertoleranz als vollvermascht