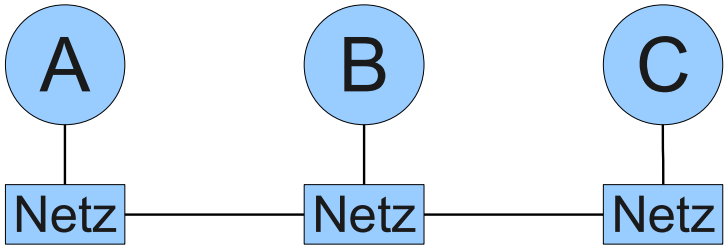
# Aufbau eines virtuellen privaten Netzes mit Peer-to-Peer-Technologie

Wolfgang Ginolas

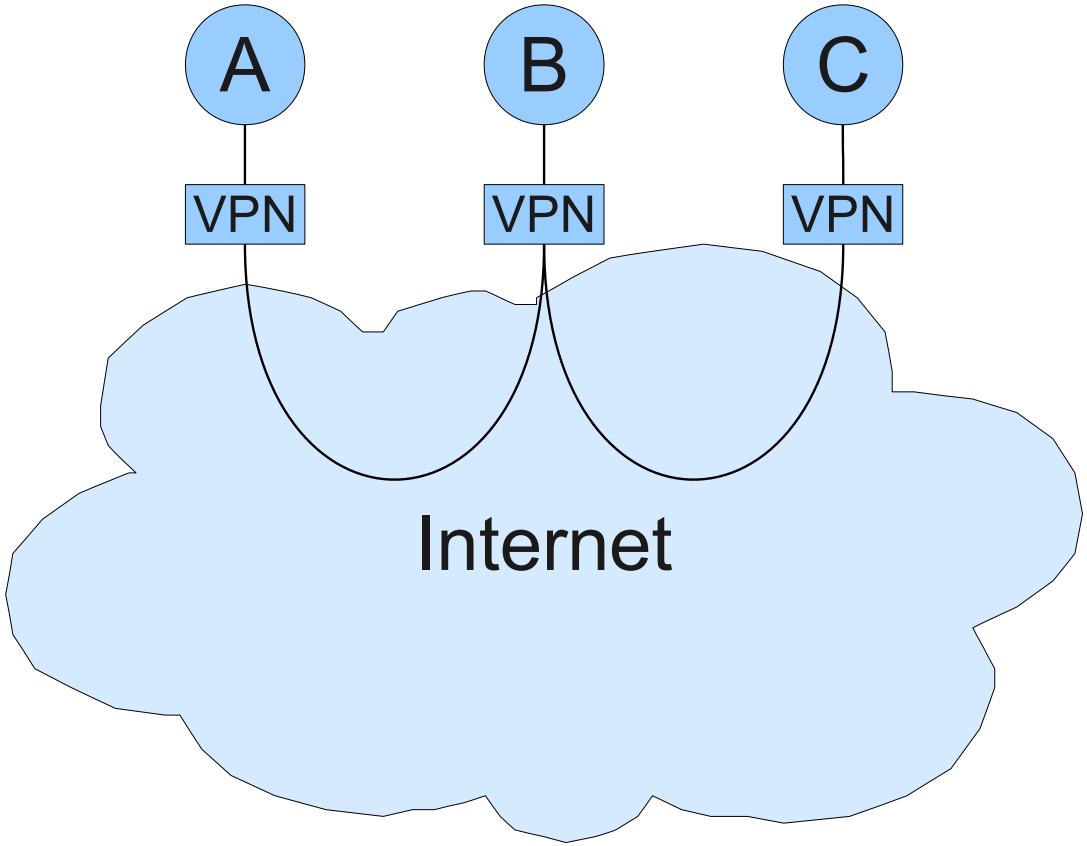
Fachhochschule Wedel

21. September 2009

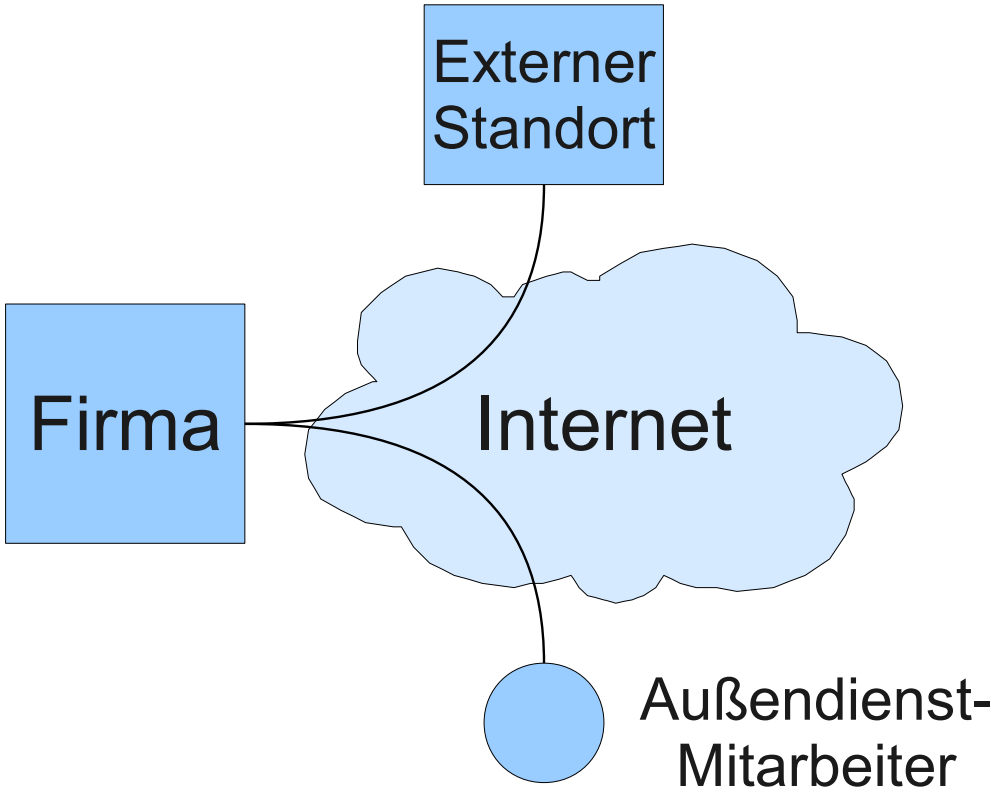
# Virtuelles Privates Netzwerk



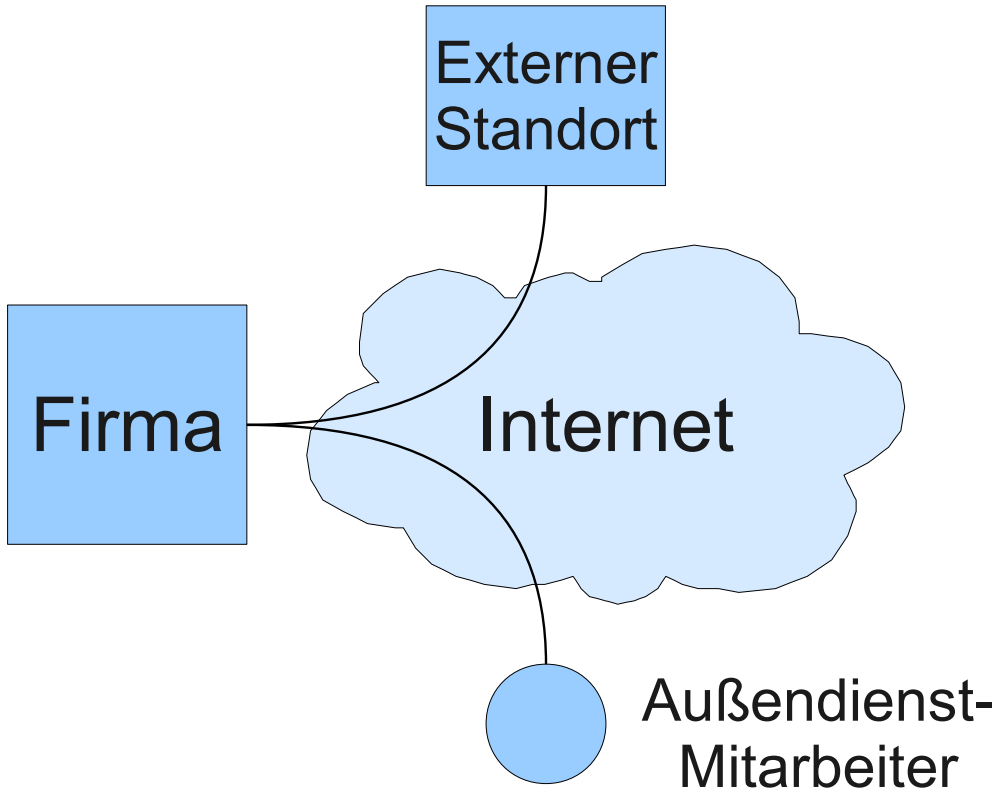
# Virtuelles Privates Netzwerk



# VPN - Firma

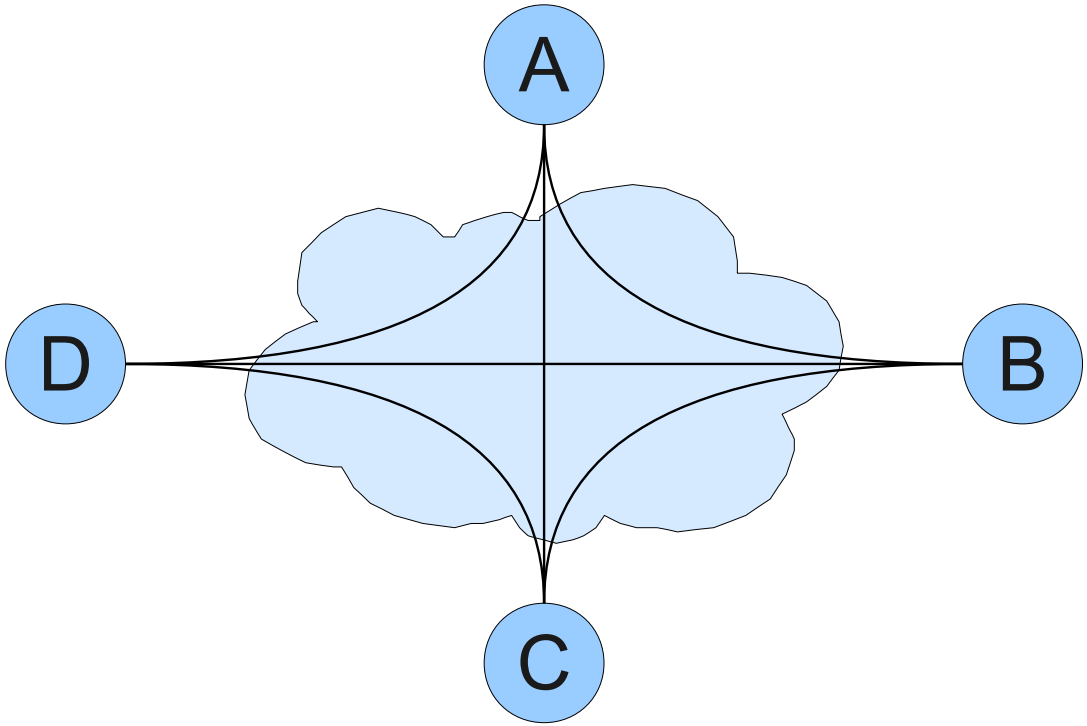

Externer
Standort
Firma
Internet
Außendienst-
Mitarbeiter

# VPN - Firma

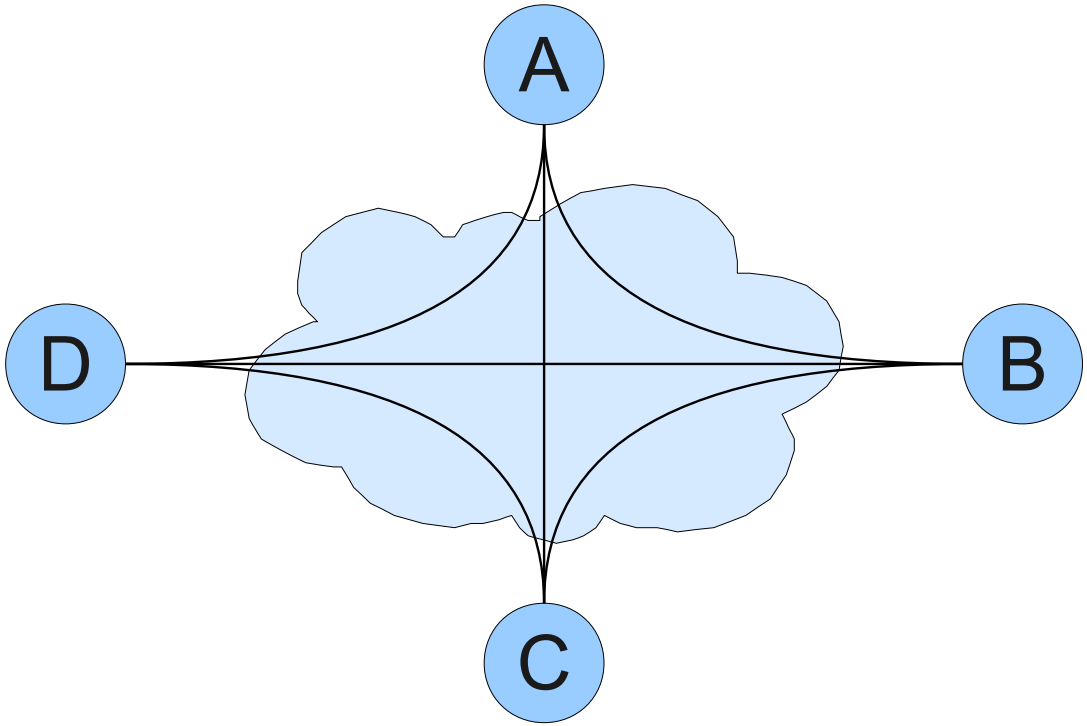



- Server
- Administrator

# VPN - Privatpersonen



# VPN - Privatpersonen




- Kein Server
- Kein Administrator

# Ziele dieser Arbeit

- Benutzerfreundlichkeit
- Sicherheit

# Ziele dieser Arbeit

- Benutzerfreundlichkeit
  - Konfiguration einfach und verständlich
  - Server aufsetzen ist nicht nötig
  - Grafische Oberfläche
- Sicherheit

# Ziele dieser Arbeit

- Benutzerfreundlichkeit
  - Konfiguration einfach und verständlich
  - Server aufsetzen ist nicht nötig
  - Grafische Oberfläche
- Sicherheit
  - Zugang nur für autorisierte Personen
  - Vertrauen darf nicht erzwungen werden
    - In Implementierung
    - In fremden Server

# Ziele dieser Arbeit

- Benutzerfreundlichkeit
  - Konfiguration einfach und verständlich
  - Server aufsetzen ist nicht nötig
  - Grafische Oberfläche
- Sicherheit
  - Zugang nur für autorisierte Personen
  - Vertrauen darf nicht erzwungen werden
    - In Implementierung
    - In fremden Server
- Also:

# Ziele dieser Arbeit

- Benutzerfreundlichkeit
  - Konfiguration einfach und verständlich
  - Server aufsetzen ist nicht nötig
  - Grafische Oberfläche
- Sicherheit
  - Zugang nur für autorisierte Personen
  - Vertrauen darf nicht erzwungen werden
    - In Implementierung
    - In fremden Server
- Also:
  - Quelloffen

# Ziele dieser Arbeit

- Benutzerfreundlichkeit
  - Konfiguration einfach und verständlich
  - Server aufsetzen ist nicht nötig
  - Grafische Oberfläche
- Sicherheit
  - Zugang nur für autorisierte Personen
  - Vertrauen darf nicht erzwungen werden
    - In Implementierung
    - In fremden Server
- Also:
  - Quelloffen
  - (Möglichst) Dezentral

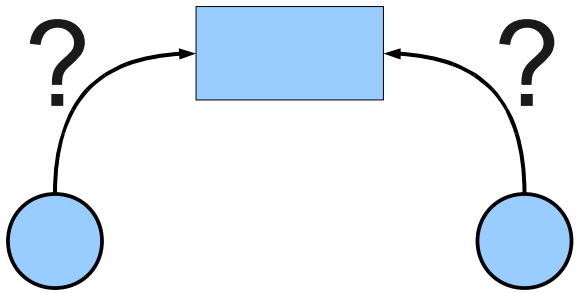
# Probleme durch dezentrale Topologie

# Probleme durch dezentrale Topologie

- Knoten finden

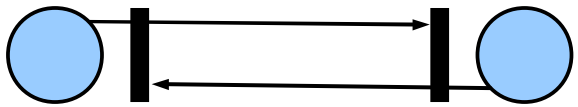
# Probleme durch dezentrale Topologie

- Knoten finden
  - Bootstrap-Server



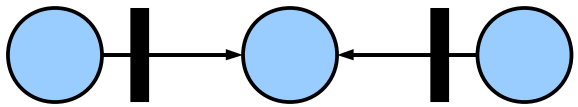
# Probleme durch dezentrale Topologie

- Knoten finden
  - Bootstrap-Server
- NAT umgehen



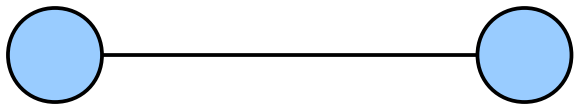
# Probleme durch dezentrale Topologie

- Knoten finden
  - Bootstrap-Server
- NAT umgehen
  - Routen



# Probleme durch dezentrale Topologie

- Knoten finden
  - Bootstrap-Server
- NAT umgehen
  - Routen
- Zugangsberechtigung prüfen



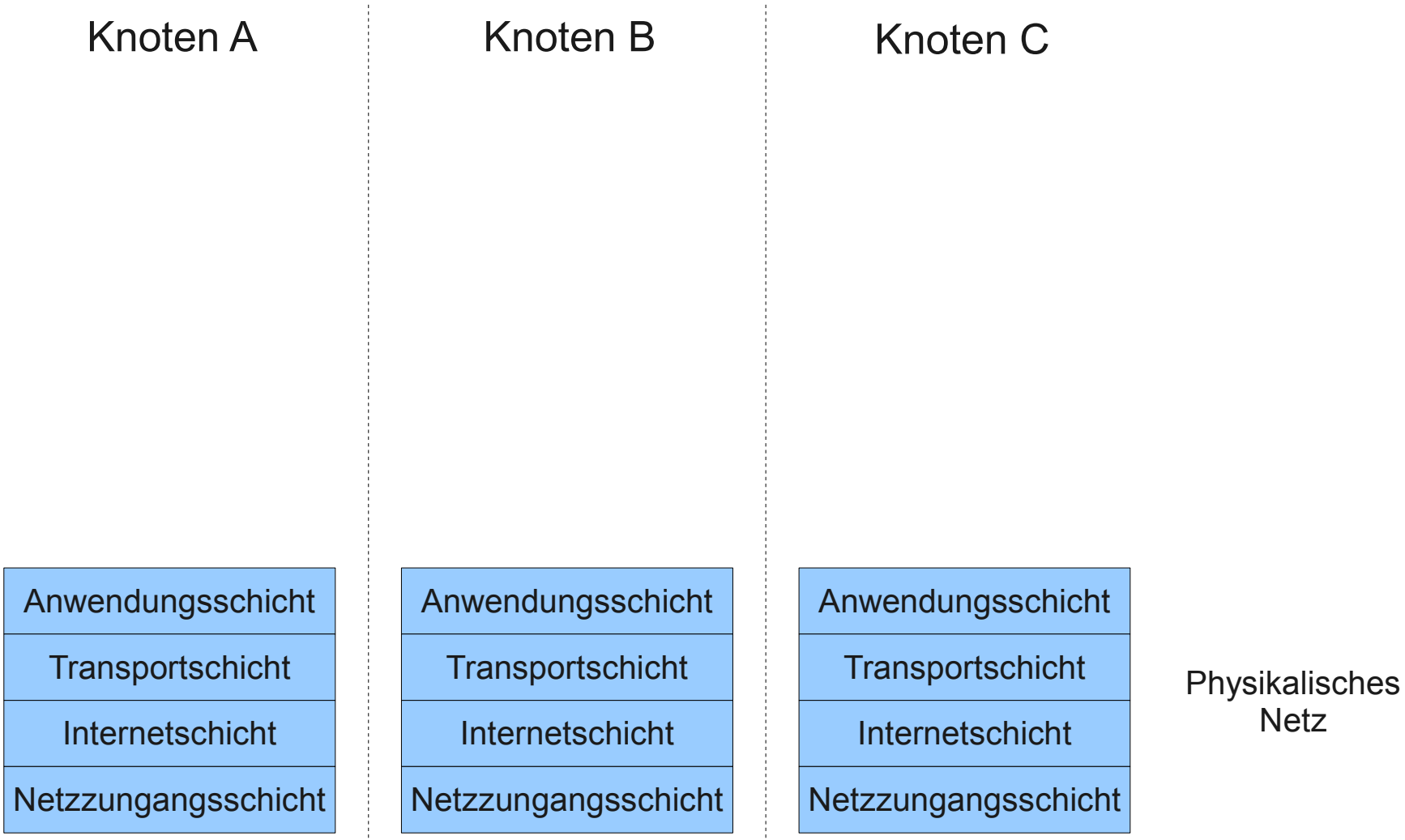
# Schichten

Knoten A

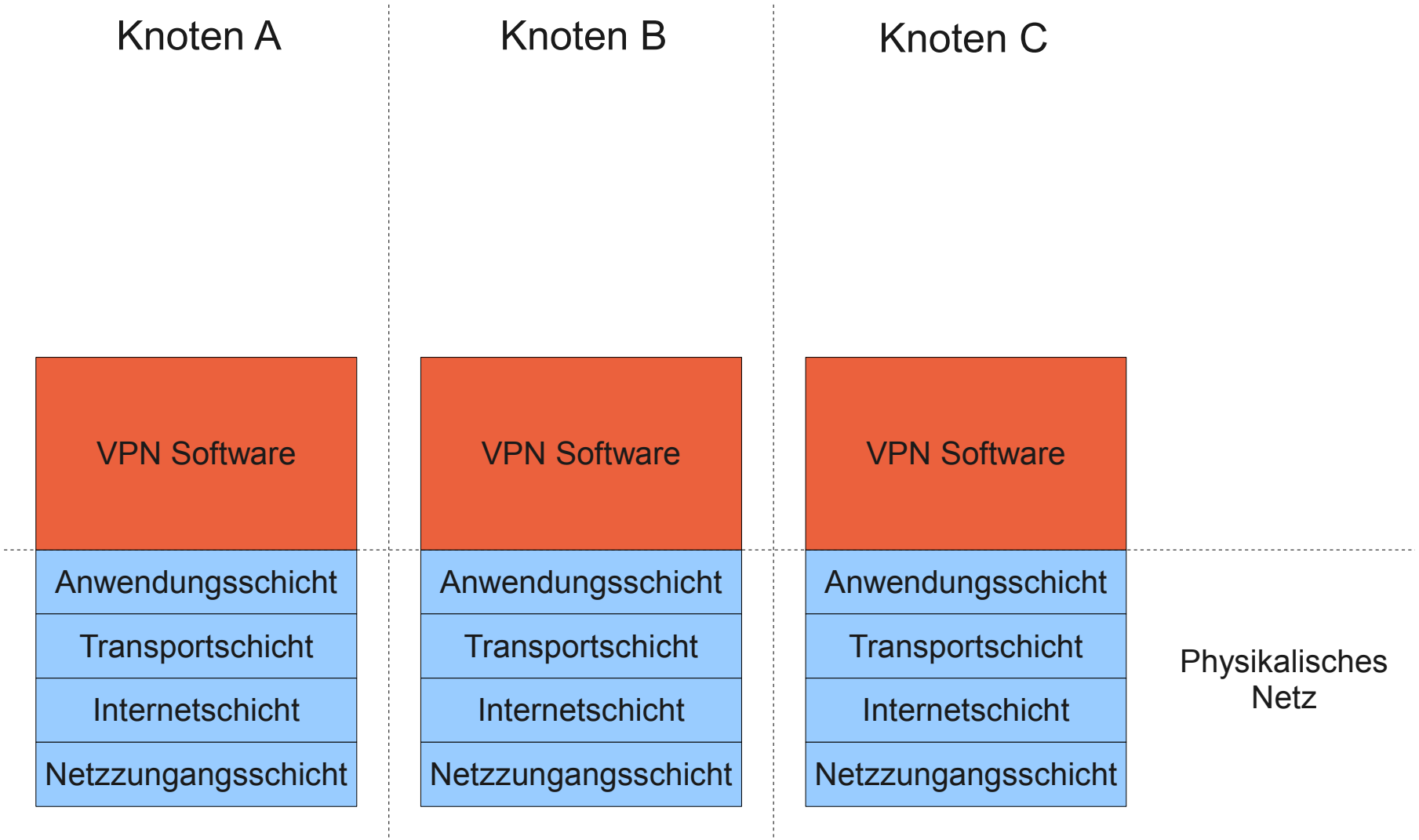
Knoten B

Knoten C

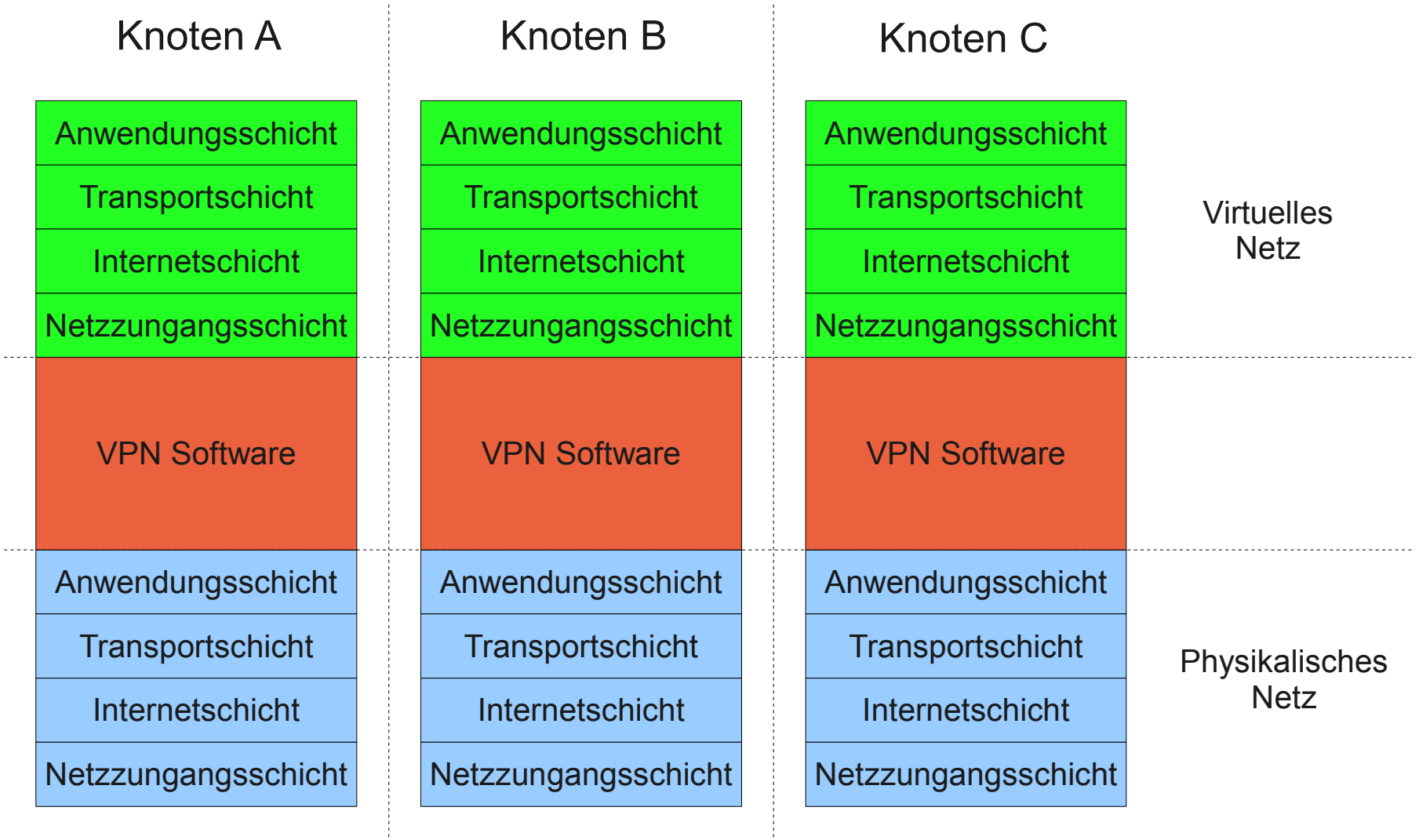
# Schichten


Knoten A
Knoten B
Knoten C
Anwendungsschicht
Transportschicht
Internetschicht
Netzzugangsschicht
Anwendungsschicht
Transportschicht
Internetschicht
Netzzugangsschicht
Anwendungsschicht
Transportschicht
Internetschicht
Netzzugangsschicht
Physikalisches Netz

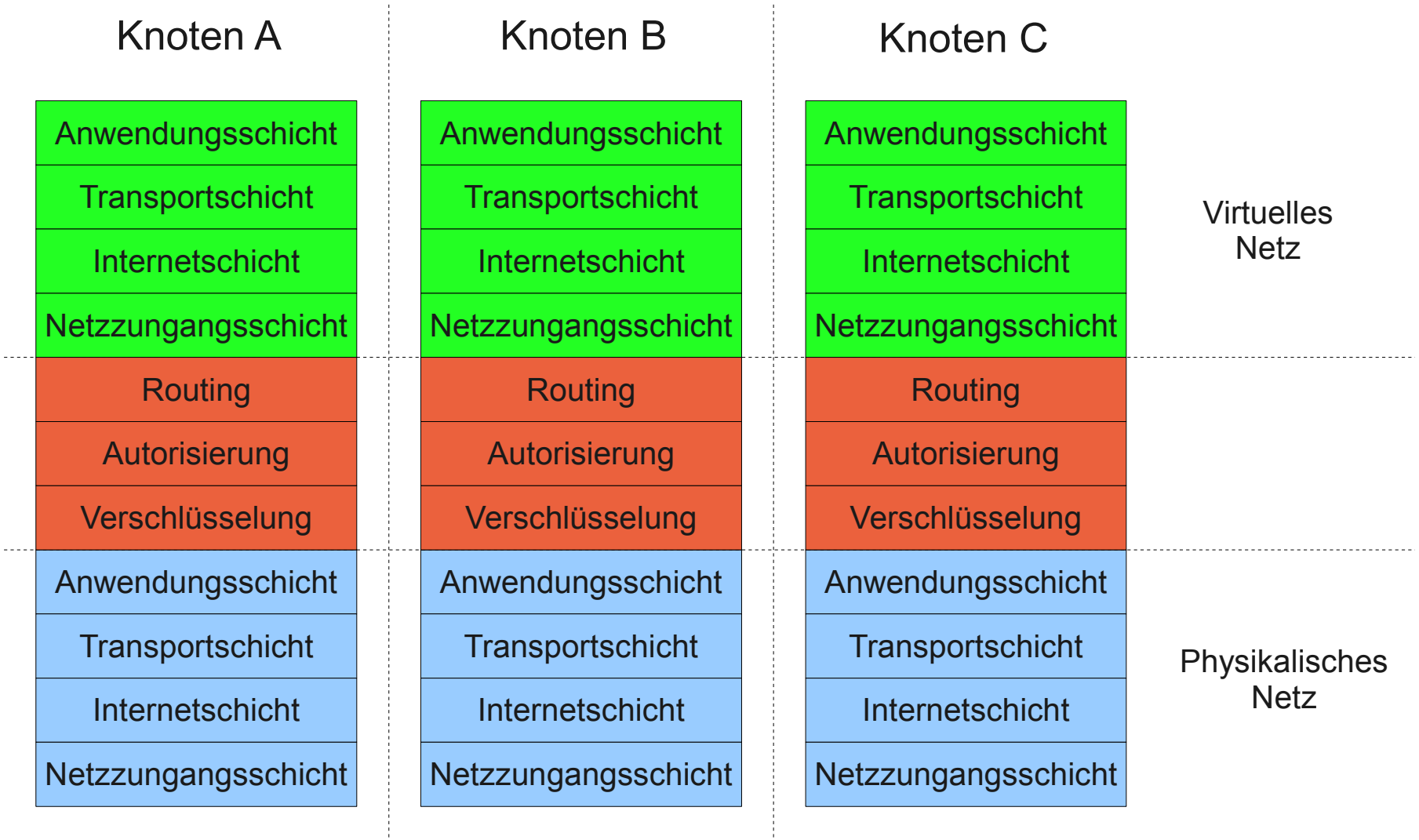
# Schichten


Knoten A
Knoten B
Knoten C
VPN Software
VPN Software
VPN Software
Anwendungsschicht
Transportschicht
Internetschicht
Netzzungangsschicht
Anwendungsschicht
Transportschicht
Internetschicht
Netzzungangsschicht
Anwendungsschicht
Transportschicht
Internetschicht
Netzzungangsschicht
Physikalisches Netz

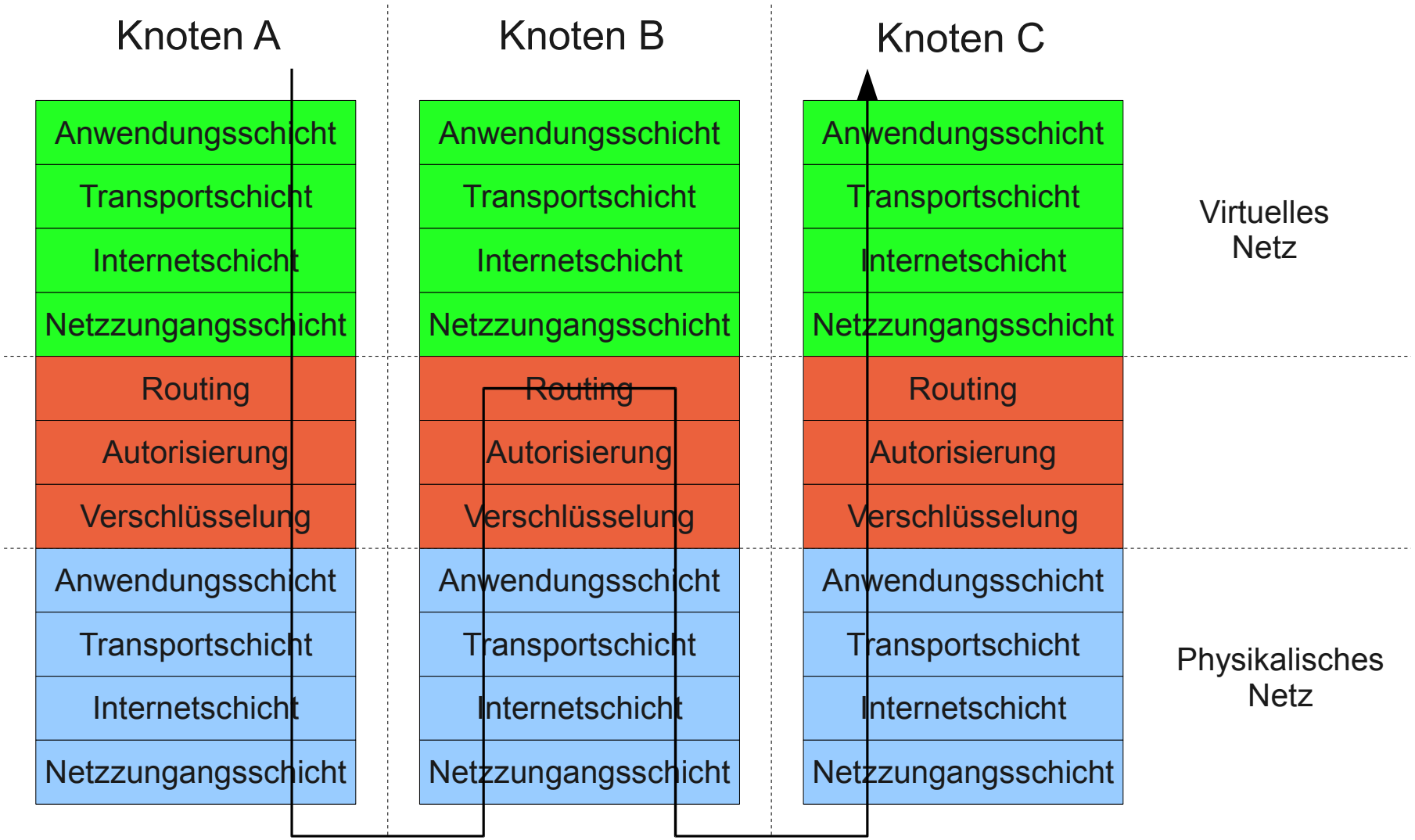
# Schichten


Knoten A
Knoten B
Knoten C
Anwendungsschicht
Transportschicht
Internetschicht
Netzzungangsschicht
VPN Software
Anwendungsschicht
Transportschicht
Internetschicht
Netzzungangsschicht
Virtuelles Netz
Anwendungsschicht
Transportschicht
Internetschicht
Netzzungangsschicht
Physikalisches Netz

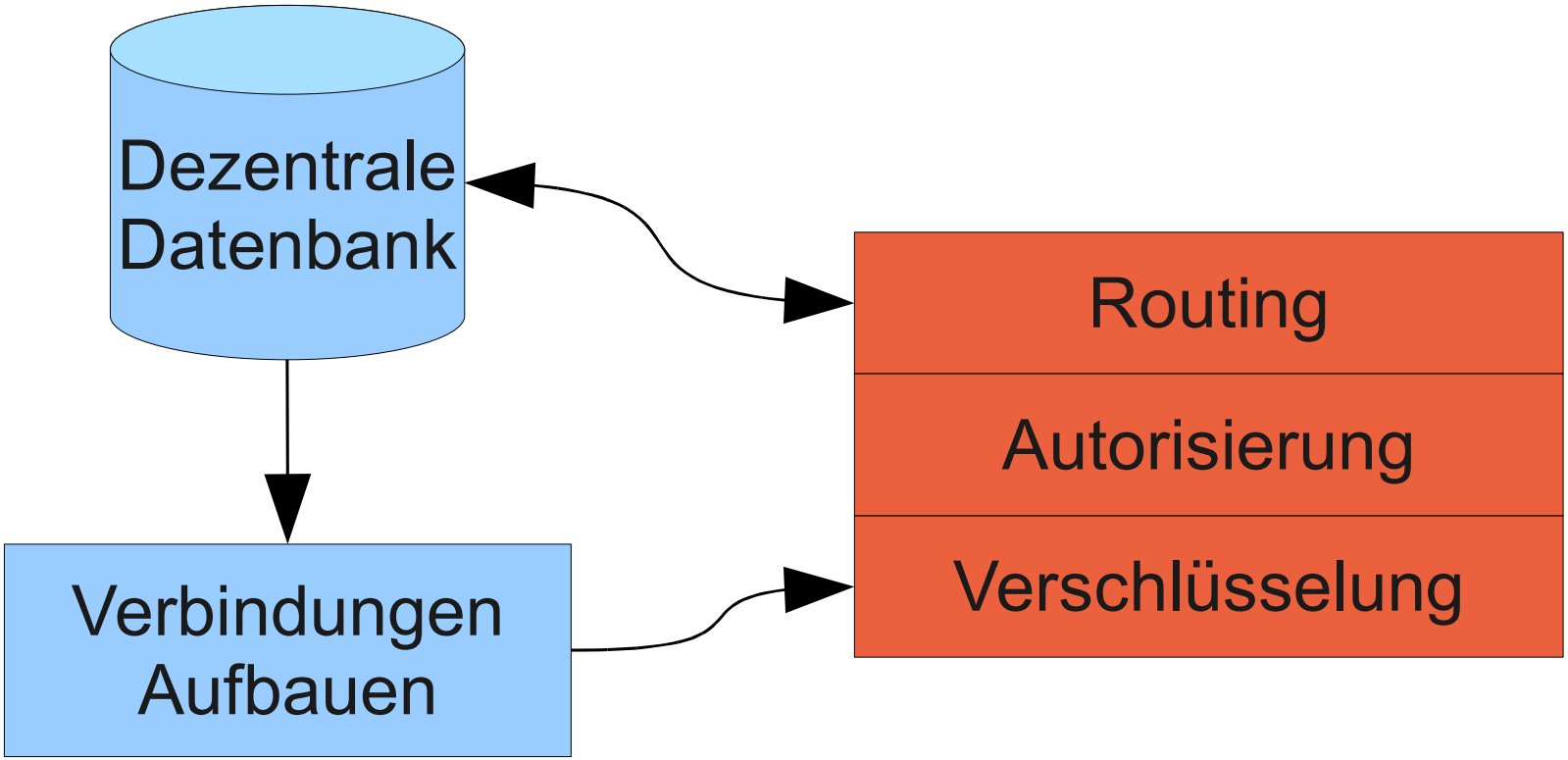
# Schichten


Knoten A
Knoten B
Knoten C
Anwendungsschicht
Transportschicht
Internetschicht
Netzzungangsschicht
Routing
Autorisierung
Verschlüsselung
Anwendungsschicht
Transportschicht
Internetschicht
Netzzungangsschicht
Virtuelles Netz
Physikalisches Netz

# Schichten


Knoten A
Knoten B
Knoten C
Anwendungsschicht
Transportschicht
Internetschicht
Netzzungangsschicht
Routing
Autorisierung
Verschlüsselung
Anwendungsschicht
Transportschicht
Internetschicht
Netzzungangsschicht
Virtuelles Netz
Physikalisches Netz

# Entwurf


Dezentrale Datenbank
Routing
Autorisierung
Verschlüsselung
Verbindungen Aufbauen

# Dezentrale Datenbank

# Dezentrale Datenbank

- Dezentrale Datenbank
  - Jeder Knoten kann Daten über sich veröffentlichen
  - Diese Daten werden verteilt und synchronisiert
    - $\Rightarrow$ Jeder Knoten hat eine aktuelle Kopie aller Daten

# Dezentrale Datenbank

- Dezentrale Datenbank
  - Jeder Knoten kann Daten über sich veröffentlichen
  - Diese Daten werden verteilt und synchronisiert
    - $\Rightarrow$ Jeder Knoten hat eine aktuelle Kopie aller Daten
- Jeder Knoten veröffentlicht:
  - Routinginformationen
    - Seine virtuelle MAC-Adresse
    - Liste der Nachbarn
  - Sonstiges
    - Seine virtuelle IP-Adresse
    - Seine physikalischen IP-Adressen
    - ...

# Routing

# Routing

- Voraussetzungen
  - Jeder Knoten kennt den kompletten Verbindungsgraphen
  - Es wird versucht, alle möglichen Verbindungen aufzubauen
  - Die Distanz zweier Knoten im Verbindungsgraphen ist meist $\leq 2$

# Routing

- Voraussetzungen
  - Jeder Knoten kennt den kompletten Verbindungsgraphen
  - Es wird versucht, alle möglichen Verbindungen aufzubauen
  - Die Distanz zweier Knoten im Verbindungsgraphen ist meist $\leq 2$
- Algorithmus
  1. Sende das Paket zu dem Nachbarn, der dem Ziel am nächsten ist
  2. Falls mehrere Möglichkeiten existieren:

     $\Rightarrow$ Wähle den Nachbarn, der zu mir die geringste Latenz hat

# Sicherheit

# Sicherheit

Ziel: Zugriff nur für autorisierte Personen

# Sicherheit

Ziel: Zugriff nur für autorisierte Personen

- Verschlüsselungsschicht
  - $\Rightarrow$ Abhören verhindern
- Autorisierungsschicht
  - $\Rightarrow$ Zugang kontrollieren

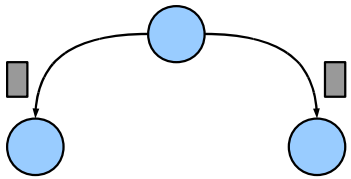
# Autorisierung

# Autorisierung

- Problem
  - Entscheidung, wer teilnehmen darf: Zentral
  - Überprüfung/Autorisierung: Dezentral

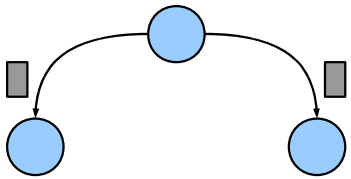
# Autorisierung

- Problem
  - Entscheidung, wer teilnehmen darf: Zentral
  - Überprüfung/Autorisierung: Dezentral
- Lösung
  - Es werden Zugangsberechtigungen verteilt
  - Knoten können sich mit diesen gegenseitig autorisieren



# Autorisierung

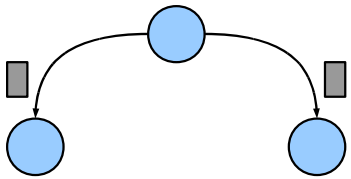
- Problem
  - Entscheidung, wer teilnehmen darf: Zentral
  - Überprüfung/Autorisierung: Dezentral
- Lösung
  - Es werden Zugangsberechtigungen verteilt
  - Knoten können sich mit diesen gegenseitig autorisieren
- Schlüssel
  - Ein Schlüsselpaar pro Netzwerk
    $\Rightarrow$ Zum Signieren der Zugangsberechtigungen
  - Ein Schlüsselpaar pro Zugangsberechtigung
    $\Rightarrow$ Zum Autorisieren



# Autorisierung

- Problem
  - Entscheidung, wer teilnehmen darf: Zentral
  - Überprüfung/Autorisierung: Dezentral

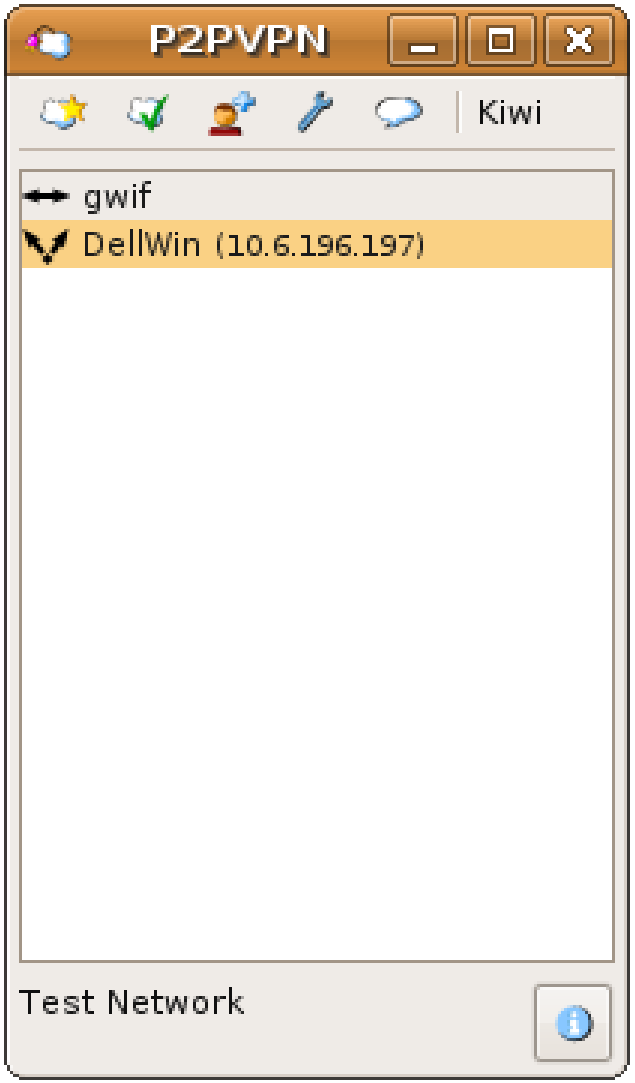
- Lösung
  - Es werden Zugangsberechtigungen verteilt
  - Knoten können sich mit diesen gegenseitig autorisieren



- Schlüssel
  - Ein Schlüsselpaar pro Netzwerk
    $\Rightarrow$ Zum Signieren der Zugangsberechtigungen
  - Ein Schlüsselpaar pro Zugangsberechtigung
    $\Rightarrow$ Zum Autorisieren
- Zusätzlich
  - Jeder Knoten hat eine Kennung, die er nicht ändern kann
  - Zugangsberechtigungen können ein Verfallsdatum haben
  - Der Netzwerkschlüssel kann weitergegeben werden

# Implementierung

- P2PVPN
  - Programmiersprache
    - Java
    - C für die Schnittstelle zum virtuellen Netz
  - Plattformen
    - Linux 32Bit
    - Windows 32Bit



# Erreichte Ziele

- Benutzerfreundlichkeit
- Sicherheit

# Erreichte Ziele

- Benutzerfreundlichkeit
  - Konfiguration weitgehend automatisch
  - Autorisierung verständlich
  - Knoten finden durch BitTorrent-Tracker
  - Grafische Oberfläche
- Sicherheit

# Erreichte Ziele

- Benutzerfreundlichkeit
  - Konfiguration weitgehend automatisch
  - Autorisierung verständlich
  - Knoten finden durch BitTorrent-Tracker
  - Grafische Oberfläche
- Sicherheit
  - Implementierung und Protokoll sind offen
  - Zugriff von außen nicht möglich
  - Knoten finden durch eigenen Server

# Erreichte Ziele

- Benutzerfreundlichkeit
  - Konfiguration weitgehend automatisch
  - Autorisierung verständlich
  - Knoten finden durch BitTorrent-Tracker
  - Grafische Oberfläche
- Sicherheit
  - Implementierung und Protokoll sind offen
  - Zugriff von außen nicht möglich
  - Knoten finden durch eigenen Server
- Rückmeldungen
  - Konstruktive Kritik
  - Mehr als 4000 Downloads