Inhalt

Protokolle und Modelle

Protokolle: Regeln, die festlegen, wie Geräte miteinander kommunizieren

Netzwerkprotokolle

- **Netzwerkkommunikationsprotokolle**: Ermöglichen die Kommunikation von zwei oder mehreren Geräten über ein oder mehrere Netzwerke (IP, TCP, http)
- **Netzwerksicherheitsprotokolle**: Sichern Daten – Authentifizierung, Datenintegrität und Verschlüsselung (SSH, SSL, TSL)
- **Routingprotokolle**: Ermöglicht Routern Informationen über Routen auszutauschen und zu vergleichen (OSPF, BGP)
- **Diensterkennungsprotokolle**: Erkennung von Geräten oder Diensten (DHCP, DNS)

Referenzmodelle

- Netzwerk ist komplex
    - Aufteilung in mehrere Schichten um es überschaubarer zu machen
- Vorteile:
    - Wettbewerb wird gefördert: Produkte von verschiedenen Herstellern sind miteinander kompatibel
    - Veränderungen auf einer Schicht wirken sich nicht auf die anderen aus

OSI-Modell

Nr	Schicht	Aufgabe
7	**Anwendung**	Kommunikation zwischen Prozessen
6	**Darstellung**	Gemeinsame Darstellung der Daten, die zwischen Anwendungsschicht-Diensten übertragen werden
5	**Sitzung**	Bereitstellung der Daten für die Darstellungsschicht; Dialogsteuerung und Verwaltung des Datenaustauschs
4	**Transport**	Dienste für Segmentierung, Transfer und Zusammenfügen der Daten zwischen End-Geräten
3	**Vermittlung**	Dienste für Austausch einzelner Datenblöcke über das Netzwerk zwischen Endgeräten
2	**Sicherung**	Methoden für den Austausch von Daten-Frames zwischen Geräten über gemeinsames Medium
1	**Bitübertragung**	Beschreiben mechanische, elektrische, funktionale und prozedurale Mittel zum Aktivieren, Verwaltend und Deaktivieren physikalischer Verbindungen zur Bitübertragung zwischen Netzwerk-Geräten

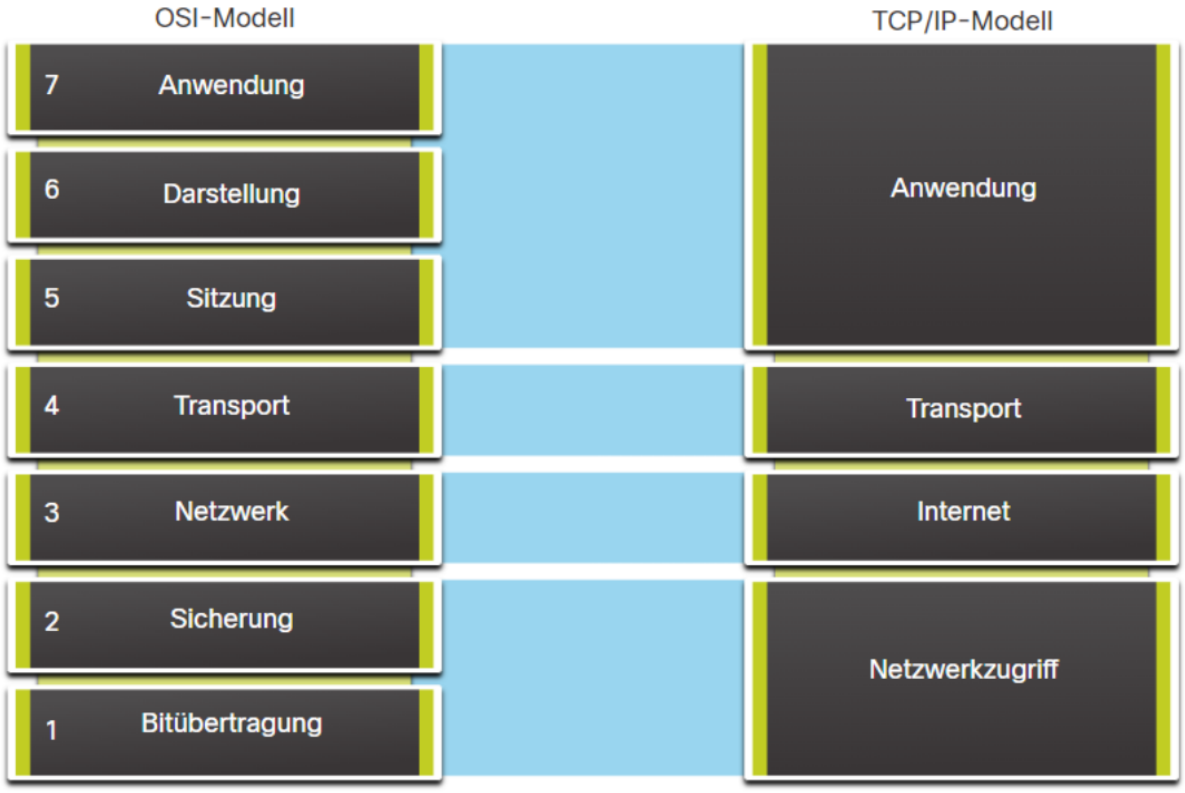
Merksatz: Alle deutschen Studenten trinken verschiedene sorten Bier

TCP/IP-Modell

Nr	Schicht	Aufgabe
4	**Anwendung**	Präsentiert Daten; Übernimmt Kodierung und Dialogsteuerung
3	**Transport**	Kommunikation zwischen Geräten über Netzwerke
2	**Internet**	Bestimmt Pfad durch Netzwerke
1	**Netzwerkzugriff**	Steuert Geräte und Medien, aus denen das Netzwerk besteht

Merksatz: Andy Tanzt irgendwie nicht (lebt er noch?)

Gegenüberstellung: OSI- & TCP/IP-Modell



- TCP fasst die **Anwendungsschicht** zusammen, die bei OSI aus **Anwendung**, **Darstellung** und **Sitzung** besteht
- TCP fasst die **Netzwerkzugriffsschicht** zusammen, die bei OSI aus **Sicherung** und **Bitübertragung** besteht
- OSI wird eher verwendet, wenn es um die niedrigeren Schichten geht o Trennung der physikalischen Schicht von der Sicherungsschicht

VLSM – Variable Length Subnet Mask

- Immer große Netzte zuerst, da sonst Lücken entstehen können
- Anzahl der nutzbaren Adressen ist n-2
  - Eine Adresse für die Netzadresse
  - Eine Adresse für den Broadcast

ANDing

- Berechnen der Netzadresse aus
  - IP-Adresse
  - Subnetzmaske
- Durch ANDing lässt sich feststellen, ob zwei IP-Adressen im selben Subnetz sind

```
11000000.10101000.00000001.01100100   (IP-Adresse)
AND
11111111.11111111.11111111.00000000   (Subnetzmaske)
--------------------------------
11000000.10101000.00000001.00000000   (Netzwerkteil)
```

MAC-Adresstabelle & Forwarding

Mac-Addresstabelle (CAM-Tabelle)

Eine Tabelle im Switch, die MAC-Adressen den physischen Ports zuordnet

Lernprozess

Der Switch prüft die **Quell-MAC** eines eingehenden Frames. Ist sie unbekannt, wird sie mit dem zugehörigen Port in die Tabelle eingetragen.

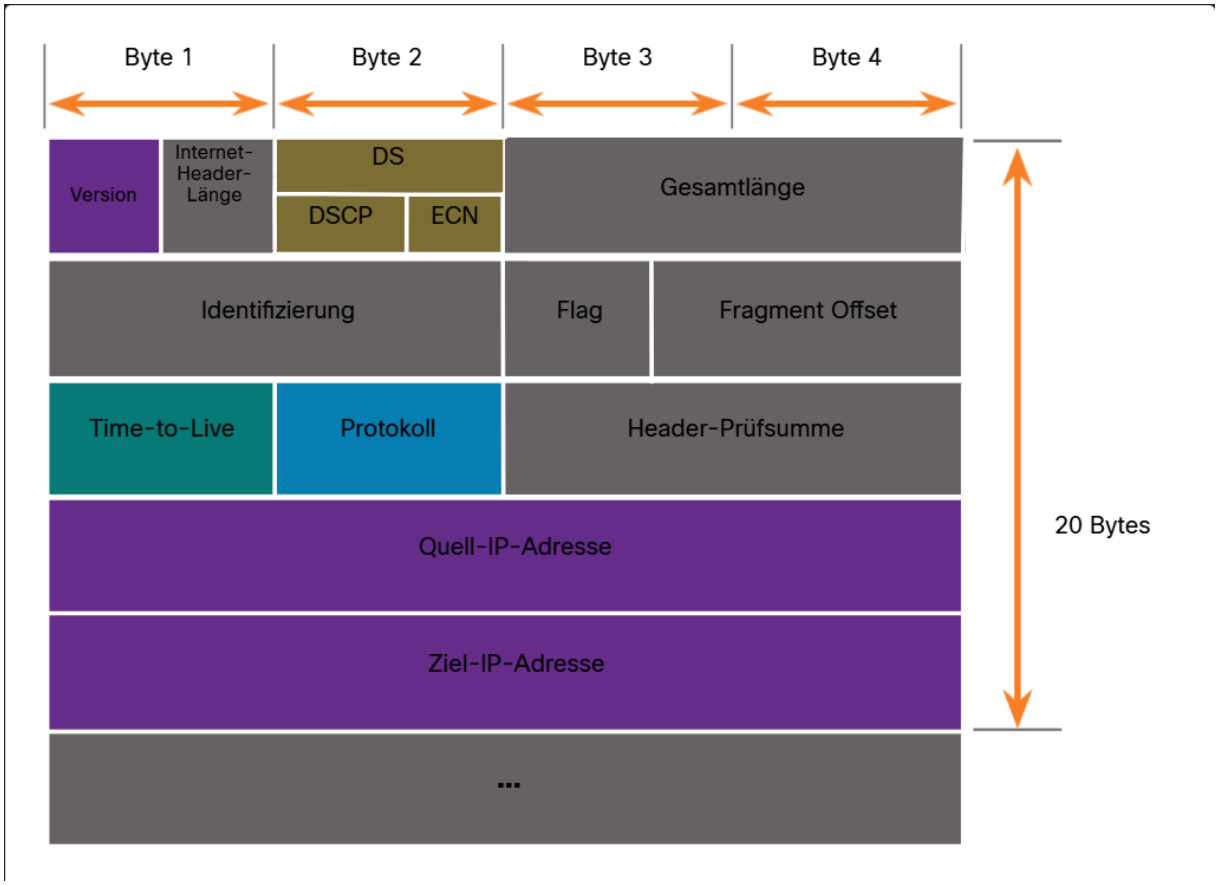
Forwarding

- Der Switch prüft die **Ziel-MAC**:
  - **Eintrag vorhanden:** Frame wird gezielt an diesen Port weitergeleitet (Unicast).
  - **Eintrag nicht vorhanden / Broadcast:** Der Switch flutet den Frame an alle Ports außer dem Eingangsport (Unknown Unicast Flooding). (Nicht das gleiche wie Broadcast)

IPv4

IPv4 Header

- Version
- Gesamtlänge
- Flags
- Fragment Offsets
- Time-To-Live
- Protokoll
- Prüfsumme für Header
- Quell-IP-Adresse
- Ziel-IP-Adresse



ARP

- Address Resolution Protocol
- Löst eine bekannte IPv4-Adresse in eine MAC-Adresse auf, damit die Daten im lokalen Netz adressiert werden können
- Wird Per Broadcast gesendet per FF:FF:FF:FF:FF:FF oder 255.255.255.255
- Es werden alle gefragt bis entweder einer die Adresse hat oder das Gerät selbst antwortet

Auswahlprozess

1. Vorbereitung
    - **Ziel-IP:** IP von PC2
    - **Quell-IP:** IP von PC1
    - **Quell-MAC:** MAC von PC1 (08-15-47-11-20-01)
    - **Ziel-MAC: Unbekannt** (Hier stockt der Prozess!)
2. ARP-Cache Check
    - **Was ist der ARP-Cache?** Eine temporäre Tabelle im Arbeitsspeicher des Hosts, die IP-Adressen den zugehörigen MAC-Adressen zuordnet
    - **Was findet das Protokoll hier?** Da es die "erste Verbindung" ist, findet PC1 **keinen Eintrag** für die Ziel-IP. Das Paket kann noch nicht gekapselt werden
3. ARP-Request
    - **Spezieller Name: ARP-Request** (Broadcast)
    - **Ziel-MAC:** FF-FF-FF-FF-FF-FF (Broadcast-Adresse)
    - **Inhalt:** "Wer hat die IP von PC2? Bitte antworte an PC1."
    - **Wer bekommt das Paket? Alle** Geräte im lokalen Subnetz (da es ein Broadcast ist)
    - **Was passiert mit dem Datenpaket?** Das ursprüngliche Datenpaket von PC1 wird solange gepuffert (wartet), bis die MAC bekannt ist
4. ARP-Replay
    - **Verhalten der anderen:** Alle Geräte, die nicht die gesuchte IP haben, verwerfen das Paket einfach
    - **Verhalten von PC2:** PC2 erkennt seine IP, trägt PC1 in seinen eigenen ARP-Cache ein und erstellt ein Antwort-Paket
    - **Name des Pakets: ARP-Reply** (Unicast)
    - **Ziel-MAC:** MAC von PC1 (08-15-47-11-20-01)
    - **Inhalt:** "Ich bin PC2, hier ist meine MAC: 08-15-47-11-20-02."
5. Abschluss
    - **Aktion von PC1:** Er empfängt die Antwort und speichert die MAC von PC2 in seinem **ARP-Cache**
    - **Das Datenpaket: Jetzt kann PC1 den fertigen Frame senden:**
        - **Ziel-MAC: 08-15-47-11-20-02 (MAC von PC2)**
        - **Quell-MAC: 08-15-47-11-20-01 (MAC von PC1)**
        - **Inhalt: Die eigentlichen Nutzdaten (z. B. ein HTTP-Request oder Ping)**
6. Besonderheit (Reden nach Außen)
    a. PC1 stellt fest, dass die Ziel-IP außerhalb seines Subnetzes liegt
    b. ARP wird nun **nicht** für die Ziel-IP ausgeführt, sondern für das **Standard-Gateway** (Router-Port G01)
    c. PC1 sendet das Paket an die MAC des Routers (08-15-47-11-20-65), damit dieser es weiterleitet

IPv6

Aufbau einer IPv6-Adresse

- 128-Bit lang
- Darstellung erfolgt hexadezimal
- Blöcke werden durch Doppelpunkte getrennt
- **Der Trenner (/64):** In der Regel wird die Adresse exakt in der Mitte geteilt. Die ersten 64 Bit bilden das **Netzwerkpräfix** (Netzwerkanteil), die letzten 64 Bit bilden die **Interface-ID** (Hostanteil). `/64` ist das Standard-Subnetz für lokale Netzwerke (notwendig z.B. für SLAAC).

Wichtige Adressbereiche

- `::/0` **(Standardroute / "allow all"):** Repräsentiert alle möglichen IPv6-Adressen. Es ist das IPv6-Äquivalent zur IPv4-Standardroute `0.0.0.0/0`. Wird im Routing (Default-Route) oder in ACLs verwendet, um den restlichen Traffic abzufangen oder durchzulassen.
- `::1` **(Localhost / Loopback):** Das ist die Loopback-Adresse des eigenen Geräts. Es ist das exakte Äquivalent zur `127.0.0.1` unter IPv4 und wird genutzt, um die lokale TCP/IP-Konfiguration zu testen.

DNS: Domain Name System

- „Adressbuch des Internets“
- IP-Adressen schwer zu merken
  => Domain-Namen wurden entwickelt
- Außerdem leichter wartbar, da beim Benutzen eines Domain-Namen dem Nutzer nicht auffällt, wenn sich die IP-Adresse hinter dem Namen ändert
- **FQDN:** Fully Qualified Domain Name z.B. shenjas-pc.fritz.box
- **NSLOOKUP:** Dienstprogramm zur “manuellen” Abfrage von Domain-Namen, z.B. für Debug

Schritte

1. Nutzer gibt Domain-Namen ein
2. Client sendet entsprechende DNS-Abfrage an DNS-Server
3. DNS-Server gleicht FQDN mit IP-Adresse ab
4. DNS-Server antwortet mit IP-Adresse des FQDN
5. Client verwendet die IP-Adresse für die tatsächliche Kommunikation mit dem Server

Ressourcendatensätze

Art	Bedeutung
A	IPv4 Adresse
NS	Autoritativer Nameserver
AAAA	IPv6 Adresse
MX	Mail-Exchange

DNS-Server-Vorgang

- Server erhält DNS-Abfrage
    - Server kann mit eigenen Datensätzen auflösen
        - Fertig
    - Server hat keinen passenden Datensatz
    - Gibt die Abfrage an den nächsten DNS-Server weiter
    - Sobald der Datensatz von einem anderen Server aufgelöst wurde, sendet der DNS-Server die entsprechende Auflösung und speichert diese für einen definierten Zeitraum in den eigenen Datensätzen, um eine weiter Abfrage schneller auflösen zu können

Hierarchie

- Namensstruktur wird in kleinere und dadurch überschaubarere Zonen unterteilt
- Jeder DNS-Server bedient nur eine dieser Zonen
    - Leitet Abfragen außerhalb seiner Zone an zuständige DNS-Server weiter
    - Eine Zone enthält die DNS-Einträge (Records)
- DNS ist dadurch Skalierbar

Abfolge

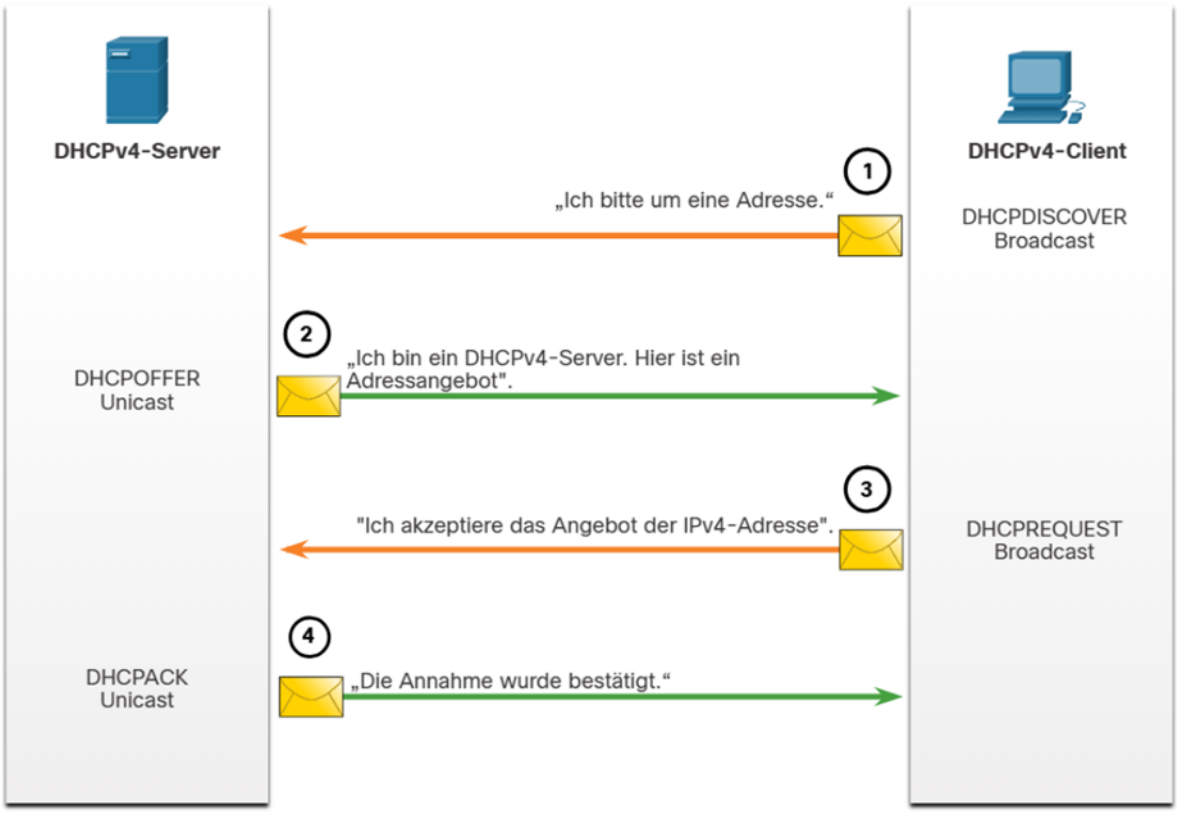
1. Root-Level-Domain
2. Top-Level-Domain (TLD): .net / .de / .com …
3. Second-Level-Domain: tinquiz.de / shenjasmom.to

DHCP: Dynamic Host Configuration Protocol

- Automatisierte Zuweisung von Netzwerkeinstellungen wie IP-Adresse, Subnetzmaske, Gateway und DNS-Server
- Gegenstück ist die statische Adressierung
- DHCP-Netzwerkgeräte fordern beim Verbinden zum Netzwerk DHCP-Daten an
- Die DHCP-Daten haben eine definierte Gültigkeitsdauer (Lease-Dauer)
    - Nach Ablauf werden die Daten neu angefordert

Schritte

1. **Discover** (Broadcast): Client sendet DHCP-Discover beim Booten bzw. beim Herstellen einer Verbindung in einem Netzwerk
2. **Offer:** Ein DHCP-Server, der den Discover-Broadcast erhalten hat, antwortet mit einem DHCP-Offer, in dem die Netzwerkdaten über eine bestimmte Lease-Dauer enthalten sind
3. **Request**: Da ggf. mehrere DHCP-Server auf den Discover ein Offer senden muss der Client ein Offer wählen und es mit einem entsprechenden Request bestätigen
4. **ACK**
    a. Wenn die angebotene Adresse aus dem Offer am Server noch verfügbar ist, antwortet dieser mit einer entsprechenden Bestätigung
    b. Ist die angebotene Adresse nicht mehr verfügbar antwortet der Server mit einer negativen Bestätigung (**NAK**). Das DHCP-Verfahren beginnt am Client mit einem **Discover** von vorne.



Lease Verlängerung

Funktioniert nur innerhalb eines Lease Zeitraums

Schritte

1. DHCP-Request (Unicast): Eine direkte Anforderung an den DHCP-Server von dem das aktuelle Lease ist. Erhält der Client in einem bestimmten Zeitabstand keine Antwort sendet er das Request als Broadcast um andere verfügbare DHCP-Server zu erreichen.
2. DHCP-Ack (Unicast): Der Server bestätigt die Verlängerung

DHCPv6

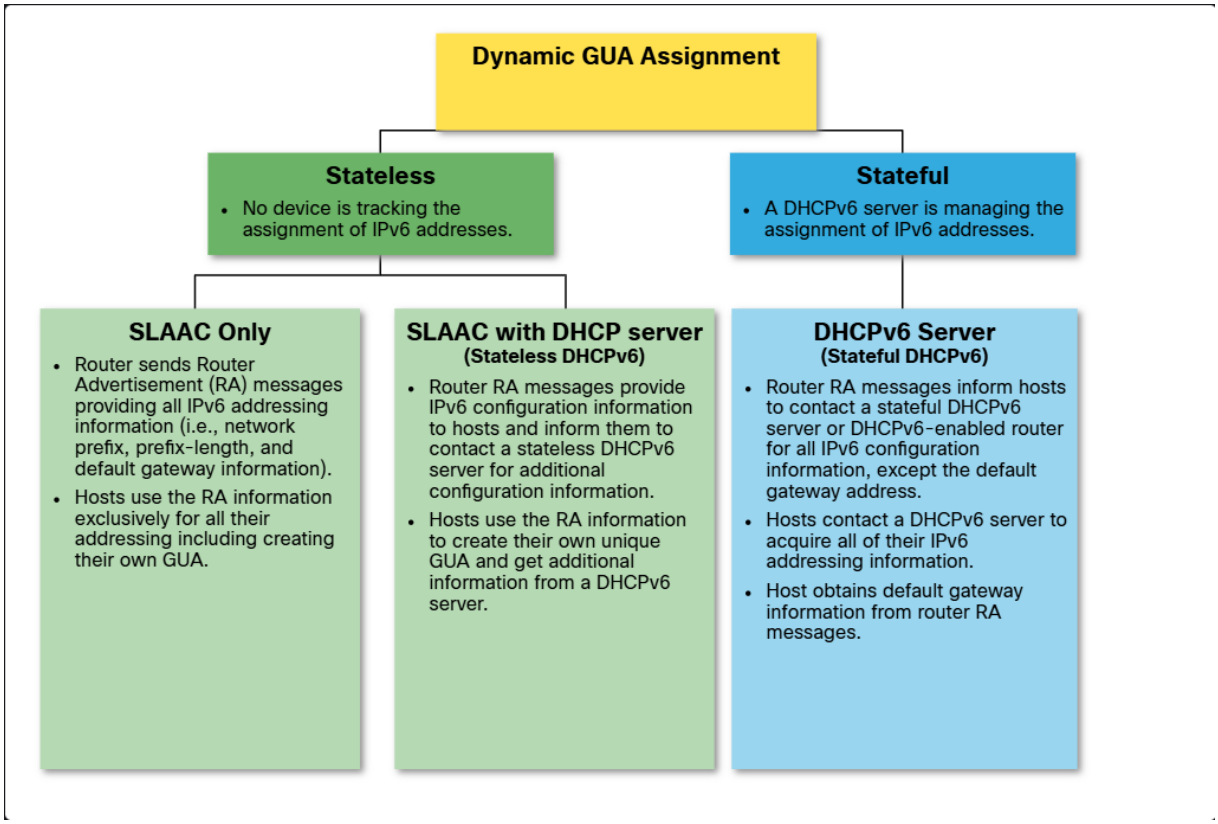
- A flag: Das ist der Address Autoconfigure Flag
- O flag: Das ist der Other Flag bedeutet der Server hat noch Informationen
- M flag: Das ist der Managed Flag bedeutet der Server gibt die Addresse vor

SLAAC

Der Client generiert seine eigene Adresse mithilfe von Router Advertisement (RA) Nachrichten, ohne einen DHCP-Server zu benötigen und wird eingeleitet mit einem A Flag only Nachricht.

DHCPv6

- Stateless DHCPv6
  - Beginnt mit einer Antwort vom Server mit einer A und O Flag Antwort
  - Der Client gibt sich selbst die Adresse, aber Server hat zusätzliche Informationen über den Client wie z.B. DNS
- Stateful DHCPv6
  - Beginnt mit einer M Flag Antwort
  - Der Client erhält seine IPv6 Adresse von dem DHCPv6 Server



TCP: Transmission Control Protocol

- Stellt sicher, dass die Daten beim Ziel ankommen
- Teilt Daten in Segmente auf
- Zuverlässig
- Verbindungsorientiert

Grundlegende Operationen

- Nummerierung und Nachverfolgung von Datensegmenten
- Bestätigung empfangener Daten
- Erneute Übertragung, wenn keine Bestätigung erfolgt
- Sequenzieren von Daten, die ggf. in falscher Reihenfolge angekommen sind
- Effiziente Datenrate, die der Empfänger verarbeiten kann

Anwendungen

- SMTP/IMAP
- http/HTTPS

Aufbau
Header (20 Byte) enthält folgende Daten:

- Quellport
- Zielport
- Sequenznummer: Für den Wiederzusammenbau
- Bestätigungsnummer: Anzeige, dass Daten erhalten wurden und auf das Nächste Segment gewartet wird
- Länge des Headers
- Reserviert
- Steuer-Bit: Erläutert Zweck und Funktion des Segments
- Fenstergröße
- Prüfsumme
- Dringlichkeit
- Optionen

Drei-Wege-Handshake

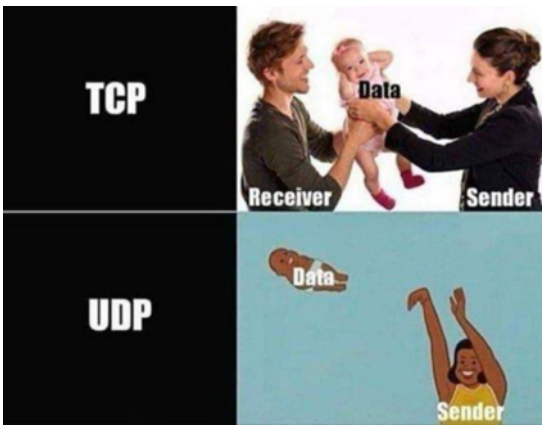
1. **SYN**: Initiierende Client fordert eine Kommunikationssitzung an
2. **ACK**, **SYN**: Der Server bestätigt die Kommunikationssitzung und fordert ebenfalls eine an
3. **ACK**: Der initiierende Client bestätigt die Kommunikationssitzung

Beenden von Sitzungen

1. **FIN**: Client sendet Segment mit FIN-Flag wenn keine Daten mehr übertragen werden müssen
2. **ACK**: Server bestätigt Ende der Sitzung
3. **FIN**: Server sendet FIN um die Sitzung zu beenden
4. **ACK**: Client bestätigt Ende der Sitzung

UDP: User Datagram Protocol

- Unzuverlässig
- Schnellere Verarbeitung
- Teilt Daten in Datagramme auf
- Verbindungslos
- Keine Bestätigung empfangener Daten



Anwendung

- VOIP
- DNS

ICMP (Ping + Tracert)

- Internet Control Message Protocol
- **Zweck**: Fehlermeldungen und Diagnoseinformationen zur IP-Paketübertragung
- Wichtige Nachrichten:
    - **Echo Request / Reply**: Wird vom Befehl ping genutzt, um Erreichbarkeit zu prüfen
    - **Destination Unreachable**: Meldung, wenn ein Ziel oder Dienst nicht erreichbar ist
    - **Time Exceeded:** Wenn die TTL eines Pakets auf 0 sinkt (genutzt von traceroute)

VLAN

- Logische Segmentierung von Netzwerken
- Verhält sich wie eigenes physikalisches Netzwerk (LAN)
- VLAN schafft logische Broadcast-Domäne

VLAN vs. Subnet

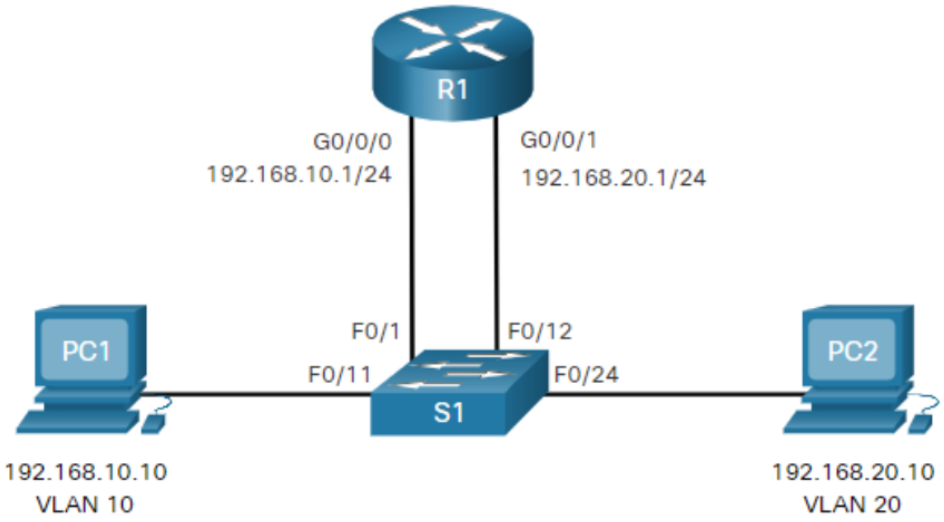
- VLANs trennen auf logischer Ebene auf OSI-Layer 2 Netzwerke voneinander
- Subnetting ermöglicht es auf OSI-Layer 3 ein großes Netz in mehrere kleinen Subnetze aufzuteilen
- Damit Clients im selben VLAN miteinander kommunizieren können müssen sie ebenfalls im selben Subnetz sein (ohne Router)

Vorteile

- **Kleine Broadcast-Domänen**: Segmentierung reduziert die Anzahl der Clients in einer großen Broadcast-Domäne
- **Erhöhte Sicherheit**: Nur Clients im selben VLAN können miteinander kommunizieren
- **Reduzierte Kosten**: VLANs verwenden die vorhandene Bandbreite effizienter
- **Mehr Leistung**: Kleine Broadcast-Domänen reduzieren unnötigen Datenverkehr
- **Einfaches Management**: VLANs fassen Geräte / Benutzer zusammen

Arten

- **Standard-VLAN**: Wenn kein VLAN konfiguriert ist liegt das VLAN 1 an
- **Daten-VLAN**: Trennung von benutzergeneriertem Datenverkehr
- **Natives-VLAN**: Zwischen Trunk-Ports (IEEE 802.1Q)
    - Untagged Frames werden an einem Trunk-Port in das Native-VLAN weitergeleitet



    - Frames mit einem Tag des Nativen-VLANs werden verworfen
- **Management-VLAN**: Netzwerkverwaltungsverkehr (SSH, SNMP usw.)
- **Sprach-VLAN**: VoIP benötigt ein priorisiertes VLAN

VLAN-Trunk (IEEE 802.1Q)

- Strecke zwischen zwei Switches über die mehrere unterschiedliche VLANs laufen
- VLANs auf einem Trunk-Port müssen getagged werden

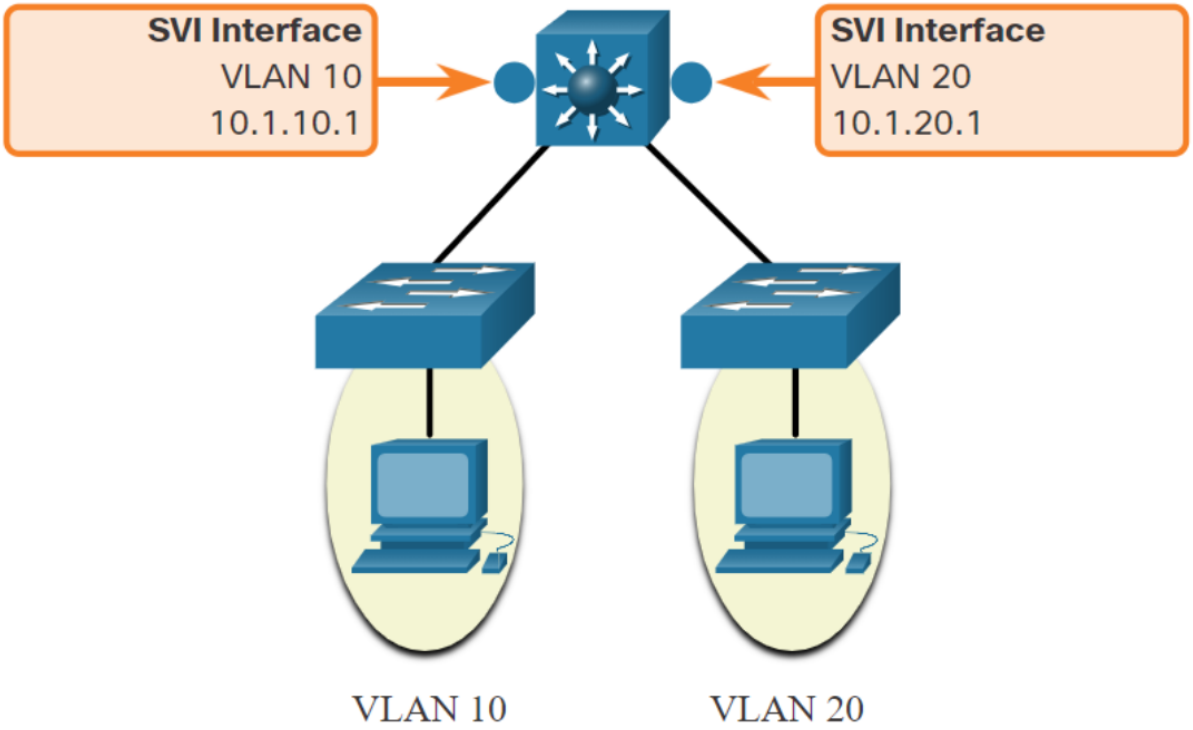
Inter-VLAN-Routing

Inter-VLAN-Routing ist der Prozess der Weiterleitung von Netzwerkverkehr von einem VLAN zu einem anderen VLAN

Legacy-Inter-VLAN-Routing

- Router mit mehreren Ethernet-Schnittstellen
- Jede Schnittstelle ist mit einem Switchport in einem VLAN verbunden und stellt das Standardgateway des VLANs dar
- Bei vielen VLANs werden am Switch und am Router viele Ports benötigt
    - Schlecht Skalierbar

Router-on-a-Stick



- Weiterentwicklung des Legacy-Inter-VLAN-Routings
- Statt mehreren Ports zwischen Switch und Router wird ein einziger Trunk-Port verwendet

Layer 3 Switch

- Routing wird innerhalb des Layer-3-Switches von virtuellen Interfaces übernommen
- Routing ist dadurch schneller und benötigt keinen externen Router
- Layer-3-Switches sind teuer

Konsolenbefehle

VLAN erstellen

- Globaler Konfigmodus

1. VLAN erstellen: vlan <vlan-id>
2. VLAN-Namen vergeben: name <vlan-name>

VLAN löschen

- Globaler Konfigmodus

1. VLAN löschen: no vlan <vlan-id>

VLAN Portzuweisung

- Globaler Konfigmodus
1. Interface-Konfig: interface <inteface-id>
2. Accessmodus setzen: switchport mode access
3. Port zu VLAN zuweisen: switchport access vlan <vlan-id>
4. Interface aktivieren: no shutdown

VLAN Trunk konfigurieren

- Globaler Konfigmodus
1. Interface-Konfig: interface <interface-id>
2. Trunkmodus setzen: switchport mode trunk
3. Ggf. Natives VLAN ändern: switchport trunk native vlan <vlan-id>
4. Angeben welche VLANs erlaubt sind (komma separiert): switchport trunk allowed vlan <vlan-list>
5. Interface aktivieren: no shutdown

VLAN Trunk am Router konfigurieren

- Globaler Konfigmodus
1. Subinterface-Konfig (G0/0/1.10 -> 10 ist vlan-id): interface <interface-id>
2. Dot1Q aktivieren: encapsulation dot1Q <vlan-id>
3. IP-Adresse konfigurieren: ip add <ip> <subnetmask>
4. Subinterface verlassen: exit
5. Volle Interface-Konfig (G0/0/1): interface <interface-id>
6. Interface aktivieren: no shutdown

STP: Spanning-Tree-Protocol

Mit Hilfe von STP lassen sich Redundanzen im Netzwerk bilden. Ohne STP würden in diesen Topologien Schleifen auf Layer-2 entstehen, die das gesamte Netzwerk lahmlegen können.

Broadcast-Sturm

Wenn Schleifen existieren und STP nicht aktiviert ist, werden Broadcast-Pakete (z.B. ARP) von einem Client an jedem Switch an alle anderen Ports weitergeleitet. Bei Schleifen erhält ein Switch das gleiche Paket nach kurzer Zeit wieder und leitet es erneut an alle anderen Ports weiter. Die Anzahl der Pakete im Netz steigt somit schnell an und überlastet die Infrastruktur, wodurch andere Pakete vernachlässigt werden.

STP-Algorithmus

1. Root-Bridge auswählen

Es wird eine Root-Bridge ermittelt. Sie dient als Zentrum der STP-Topologie. Alle anderen Switches ermitteln den kostengünstigsten Pfad zur Root-Bridge.
Zur Ermittlung der Root-Bridge bildet jeder Switch eine **Bridge-ID**. Diese ID besteht ausfolgenden Elementen:

- **Priorität**
  - Kann in Schritten von 4096 gewählt werden
  - Bereich von 0 bis 61440
- **Erweiterte System-ID**
  - Entspricht der VLAN-ID
- **MAC-Adresse**
  - Entscheiden, wenn die Priorität und Erweiterte-System-ID bei zwei oder mehr Switches identisch sind

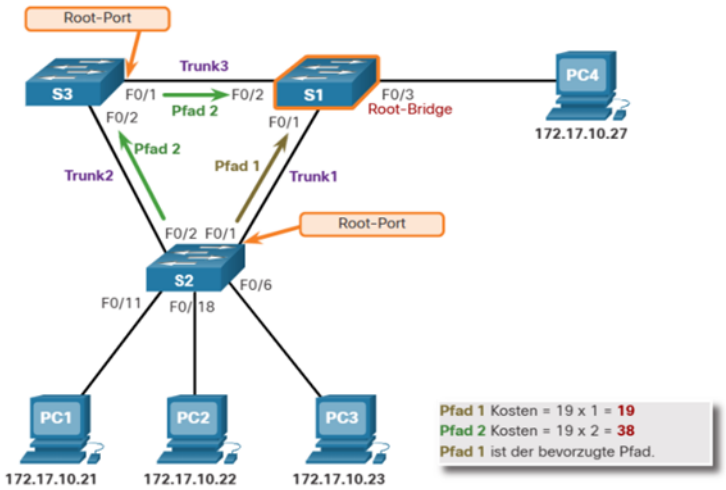
Der Switch mit der **niedrigsten BID** wird zur **Root-Bridge**

2. Pfadermittlung

Wenn eine Root-Bridge entschieden wurde, werden die kostengünstigsten Pfade von allen anderen Switches zur Root-Bridge ermittelt. Dabei ist die Geschwindigkeit der Strecken relevant.

3. Ermittlung der Prot-Zustände

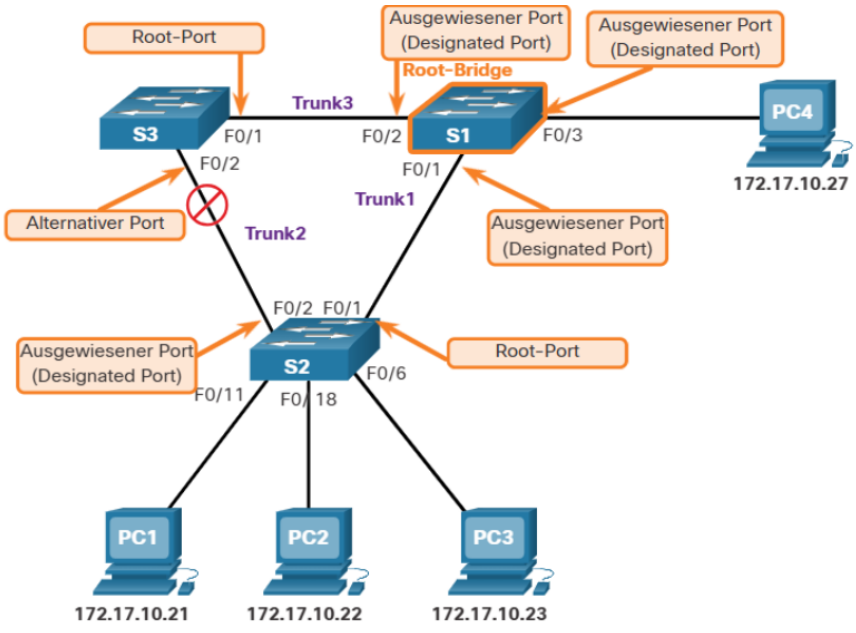
Jeder Switch, der nicht die Root-Bridge ist, wählt genau einen Root-Port aus. Der **Root-Port** ist der Port am Switch, der **der Root-Bridge am nächsten** ist.



Alle Ports **die gegenüber eines Root-Ports** liegen werden zu einem **Designated-Port**.

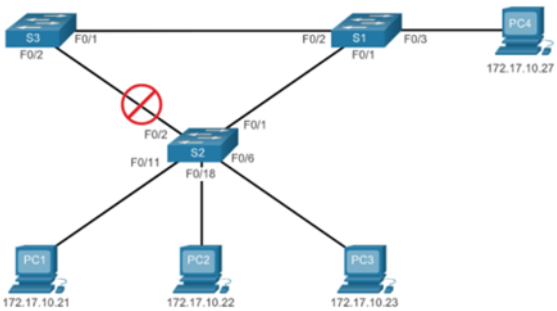
Bei einer Verbindung zwischen zwei Switches, bei denen keiner der beiden Ports ein Root-Port ist, wird der Switch Port am Switch mit **dem kostengünstigeren Pfad der Designated-Port**. Sind die Pfadkosten identisch entscheidet die **kleinere Bridge-ID.**

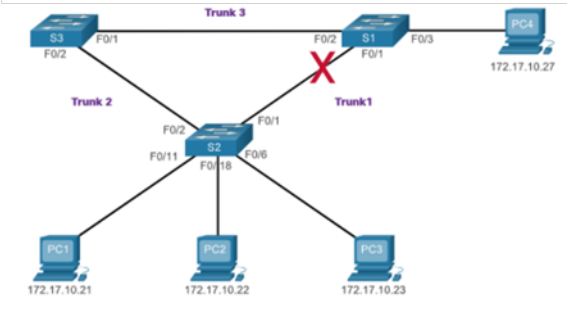
Alle anderen Ports zwischen Switches werden zu **Alternate-Ports/Blocked-Ports**. Über diese Leitungen wird die Kommunikation gesperrt und dadurch Schleifen verhindert.



4. Neuberechnung bei Topologie Änderung

Wenn ein Switch oder eine Leitung ausfällt wird die STP Topologie neuberechnet. Dabei werden zuvor geblockte Ports ggf. wieder freigegeben. Auch bei jedem topology change (neuer switch) wird root





neu ermittelt!

Etherchannel

Etherchannel aggregiert Verbindungen zwischen Geräten zu Bündeln. Dadurch können eine höhere Bandbreite, Ausfallsicherheit, Fehlertoleranz und Lastverteilung erreicht werden.

Es können nur Schnittstellen des gleichen Typs und maximal 8 separate Schnittstellen aggregiert werden.

Konfigurationsrichtlinien

- Schnittstellen müssen Etherchannel unterstützen
- Geschwindigkeit und Duplex-Modus müssen identisch sein
- Alle Schnittstellen müssen dieselben VLANs haben

Aushandlungsprotokolle

PAgP: Port Aggregation Protocol

- Cisco-Proprietär
- Verwaltet die Bildung des Etherchannels und falls aktiviert den erstellten Etherchannel
- Switch Zustände:
    - **On**: Erzwingt die Erstellung eines Channels ohne PAgP
    - **PAgP desirable**: Verhandelt aktiv die Bildung eines Etherchannels
    - **PAgP auto**: Ist bereit zur Verhandlung über PAgP aber initiiert nichts. Reagiert nur.

PAgP Modes

S1	S2	Channel-Einrichtung
Ein	Ein	Yes
Ein	Erwünscht/Auto	No
Erwünscht	Erwünscht	Yes
Erwünscht	Automatisch	Yes
Automatisch	Erwünscht	Yes
Automatisch	Automatisch	No

LACP: Port Aggregation Control Protocol

- Ideal für Multivendor-Umgebungen
- Ähnliche Switch Zustände wie PAgP:
    - **On**: Erzwingt die Erstellung eines Channels ohne LACP
    - **LACP active**: Verhandelt aktiv die Bildung eines Etherchannels
    - **LACP inactive**: Ist bereit zur Verhandlung über LACP aber initiiert nichts. Reagiert nur.

S1	S2	Channel-Einrichtung
Ein	Ein	Yes
Ein	Active/Passive	No
Active	Active	Yes
Active	Passive	Yes
Passive	Active	Yes
Passive	Passive	No

First-Hop-Redundancy Protokolle

In einem Netzwerk in dem Client einen einzelnen Router als Standardgateway hinterlegt haben, sind eben diese Clients vom externen Netz getrennt, sobald der Router ausfällt. Um das zu verhindern, werden First-Hop Redundancy-Protokolle verwendet.

Um einen Single-Point-of-Failure zu verhindern, bietet es sich an eine virtuelle IP-Adresse als Standardgateway zu verwenden, hinter der sich mehrere Router verbergen. Über die virtuelle IP-Adresse können Pakete nach extern weitergeleitet werden, auch wenn ein Router ausfällt.

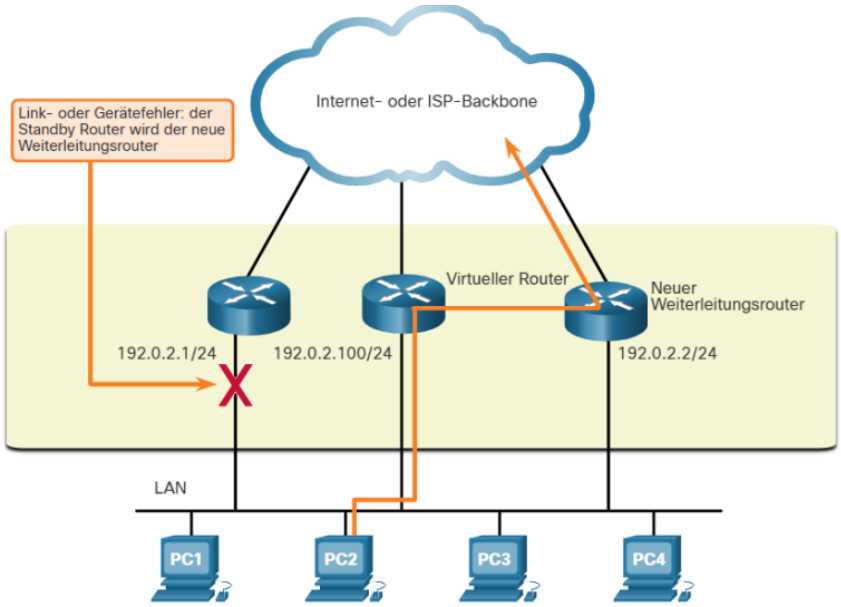
Verfügbare Protokole

HSRP: Hot Standby Router Protocol

- Cisco-Proprietär
- Überwacht und verwaltet aktive und Standby-Router

VRRP: Virtual Router Redundancy Protocol

- Ein Router wird Master, alle anderen werden Backup



GLBP: Gateway Load Balancing Protocol

- Cisco-Proprietär
- Wie HSRP/VRRP
- Zusätzlich Load Balancing

IRDP: ICMP Router Detection Protocol

- Altes Protokoll
- Erlaubt es Clients einen anderen Router zu finden, der eine Verbindung zu externen Netzen hat

HSRP: Hot Standby Router Protocol

- Bestimmt in einer Gruppe von Geräten den aktiven Router und die Standby-Router
- Aktiver Router:
    - leitet Pakete weiter
    - Standardmäßig der Router mit der höchsten IP
- Standby-Router: springt für aktiven Router im Falle eines Ausfalls ein
- HSRP-Priorität: Kann verwendet werden um den aktiven Router festzulegen
- Bestimmung des aktiven Routers
    - 1. Priorität: Standardmäßig 100; Zwischen 0 und 255; Höchste Prio gewinnt
    - 2. IP-Adresse: Höchste IP-Adresse gewinnt

HSRP-Präemotion

Wenn ein Router mit einer höheren Priorität online kommt kann dieser das Auswahlverfahren erneut erzwingen. Wenn Deaktiviert bleibt der aktuelle Router der aktive Router, auch wenn er ggf. eine niedrigere Priorität hat

Zustände

HSRP-Status	Beschreibung
Anf. Kosten	Dieser Zustand wird durch eine Konfigurationsänderung eingegeben oder wenn eine Schnittstelle verfügbar gemacht wird.
Lernen	Der Router hat die virtuelle IP-Adresse nicht ermittelt und hat noch keine Hello Nachricht vom aktiven Router empfangen. In diesem Zustand wird der Router warten, um vom aktiven Router Nachrichten zu empfangen.
Mithören	Der Router kennt die virtuelle IP-Adresse, aber der Router ist weder der aktiver Router noch der Standby-Router. Er hört auf Hello Nachrichten von anderen Routern.
Sprechen	Der Router sendet regelmäßige Hello Nachrichten und nimmt aktiv an der Auswahl des aktiven und/oder Standby-Routers teil.
Standby	Der Router ist ein Kandidat, der nächste aktive Router zu werden und sendet regelmäßige Hello Nachrichten.

Routing

- Den besten Pfad zum Weiterleiten eines Pakets anhand von Routing-Tabellen zu ermitteln
- **Next-Hop**: Bezeichnet den nächsten Router (oder das nächste Gerät) auf dem Weg zum Ziel, an den ein Paket weitergeleitet wird. Dieser Router muss direkt erreichbar sein

Routing Tabelle

- **show ip route**: Routing-Tabelle anzeigen lassen

Routing-Codes

- **L – Local**: Router-Adresse des Routers im direkt angeschlossenen Netz – Immer /32
- **C – Connected**: Netz, das direkt am Router angeschlossen ist
- **S – Static**: Statisch konfigurierte Route (Manuell konfiguriert)
- **O – OSPF**: Über OSPF (Open-Shortest-Path-First) gelernt
- **R – RIP**: Über RIP (Routing Information Protocol) gelernt
- **[X]* - Stern** an beliebigem Code: Markiert die Standardroute – z.B.: S*

Administrative Distanz

- Stellt Zuverlässigkeit der Route dar
- Je niedriger die Zahl, desto zuverlässiger
- Standard ADs:
    - Direkt verbunden: 0
    - Statisch: 1
    - OSPF: 110

Eintrag Aufbau

<Code> <Zielnetz> <Subnetzmaske> <Ausgangsport/NextHop/ Ausgangsport NextHop> <AdminDist>

Erstellen der Routing-Tabelle (14.1.6)

- **Direkt verbundene Netzwerke**: Netze, die auf aktiven Schnittstellen des Routers konfiguriert sind
- **Remote Netzwerke**: Netzwerke, die nicht direkt am Router anliegen
    - **Statische Routen**: Manuelles Bekanntmachen eines Netzes
    - **Dynamische Routing Protokolle (OSPF etc.): Wird zur Tabelle hinzugefügt, wenn Dyn. Routing-Protokolle etwas über entfernte Netze erfahren**
- **Standardroute**: Gibt Next-Hop-Router an, wenn keiner der Tabellen-Einträge passt. In der Hoffnung, dass der nächste Router das Zielnetz kennt.
    - Kann statisch konfiguriert oder dynamisch gelernt werden
    - Routeneintrag immer: 0.0.0.0/0

Statisches Routing

- **ip route <Eintrag ohne Code>:** Konfiguriert eine statische Route
- **Next-Hop-Route**: Ip route 0.0.0.0 0.0.0.0 172.168.0.2 (Zieladresse)
- **Direkt-verbundene Route**: Ip route 0.0.0.0 0.0.0.0 Fa0/2 (Ausgangsport)
- **Fully Qualified Route**: Ip route 0.0.0.0 0.0.0.0 Fa0/2 17216.0.2 (Ausgangsport und Zieladresse)

Floating Static Route

- Wird als Backup-Route für eine andere Route verwendet
- Lösung über Administrative Distanz -> Floating Static Route hat eine höhere AD als die primäre Route

Summary Static Route

- Mehrere Netze können zusammengefasst werden, indem man eine breitere Subnetzmaske wählt

Beispiel:

- 10.40.1.0/24
- 10.40.2.0/24
- 10.40.3.0/24
    - Kann unter **10.40.0.0/16** zusammengefasst werden
    - Alternativ auch enger als **10.40.0.0/22** -> umfasst 10.40.0.0 – 10.40.3.255

Dynamisches Routing

- Router tauschen Informationen über Remote-Netze miteinander aus
- Bei Topologie-Änderungen kann schnell ein neuer bester Pfad ermittelt werden
- Protokolle: OSPF, RIP

Packetweiterleitung

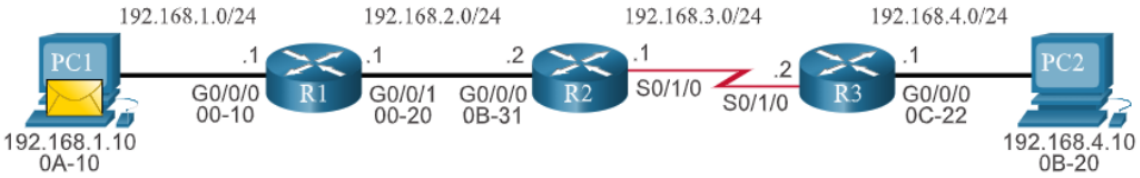
Entscheidungsprozess

1. Router erhält Paket
2. Router extrahiert die Ziel-IP-Adresse
3. Router vergleicht die Ziel-IP-Adresse mit seiner Routing-Tabelle auf die längste Übereinstimmung
    a. Router findet einen passenden Eintrag in der Routing Tabelle
        i. **Eintrag zeigt auf direkt verbundenes Netz**: Paket wird an Zielgerät geleitet (Ggf. ARP-Request notwendig)
        ii. **Eintrag zeigt auf remote Netz**: Paket wird an Next-Hop weitergeleitet
    b. Router findet keinen Eintrag in der Routing Tabelle
        i. **Es ist eine Standardroute konfiguriert**: Paket wird an Next-Hop weitergeleitet
        ii. **Es ist keine Standardroute konfiguriert**: Paket wird gelöscht

End-to-End-Weiterleitung

- Bei der Weiterleitung wird das Layer-3 Paket (IP) nicht verändert. Lediglich die Layer-2 (MAC) Informationen ändern sich ständig
- Falls keine Layer-2 Informationen am bearbeitenden Gerät vorliegen, muss erst ein ARP-Request durchgeführt werden
-

Beispiel



1. PC1 weiß, dass PC2 nicht im eigenen Netz ist -> Sendet Paket ans Standardgateway
    a. Quell-MAC: PC1
    b. Ziel-MAC: R1
2. R1 weiß, dass es kein direkt angebundenes Netzwerk ist. Er hat allerdings einen Routeneintrag in dem R2 als Next-Hop für das Netz angegeben wird
    a. Quell-MAC: R1
    b. Ziel-MAC: R2
3. R2 weiß, dass es kein direkt angebundenes Netzwerk ist. Er hat allerdings einen Routeneintrag in dem R3 als Next-Hop angegeben wird.
    a. Quell-MAC: /
    b. Ziel-MAC: 0x8F (Layer-2 Broadcast)
    c. R2 und R3 sind über eine serielle Schnittstelle miteinander verbunden -> R2 muss eine Layer-3 Broadcast-Adresse verwenden und keine Quell-Adresse angeben
4. R3 weiß, dass es ein direkt verbundenes Netzwerk ist. Er kann die MAC-Adresse des Endgeräts als Zieladresse hinterlegen
    a. Quell-MAC: R3
    b. Ziel-MAC: PC2
5. PC2 empfängt Paket auf seiner MAC-Adresse und erkennt, dass es sich um seine IP-Adresse handelt (die IP wurde nie geändert). Es muss also sein Paket sein

OSPF (Open Shortest Path First)

- **OSPFv2**: IPv4
- **OSPFv3**: IPv6
- V2 und V3 sind strikt getrennt

Ablösung für Distant Vector Routing

- **RIP** (Routing Information Protocol)
    - Hop-Anzahl als Angabe für die Effizienz einer Route
    - Schlecht skalierbar

Link-State Routing (OSPF)

- Netzwerk kann in verschiedene „**Areas**“ aufgeteilt werden
- Link kann sein …
    - **Interface** an einem Router
    - **Netzwerksegment**, dass zwei Router verbindet
    - **Endnetzwerk**, das nur mit einem Router verbunden ist
- Link-State beinhält…
    - Netzwerk-Prefix
    - Subnetz-Prefix
    - Kosten

OSPF-Komponenten

OSPF-Pakete (Link-State-Packets)

1. Hello Paket:
    - Nachbarschaft mit anderen OSPF-Routern herstellen und halten
    - Beinhält Parameter, die bei benachbarten Routern übereinstimmen müssen, damit sie benachbart sein können
    - Designated-Router und Backup-Designated-Router aushandeln
    - Dead-Intervall: Zeit bis ein Nachbar-Router als down definiert wird und einen Topology-Change auslöst
2. **Database-Description-Paket (DBD):**
    - Enthält abgekürzte Version der eigenen LSDB
    - LSDB muss überall gleich sein -> Empfänger gleicht DBD mit eigener LSDB ab
3. **Link-State-Request (LSR):** Nach mehr Informationen zu einem DBD fragen
4. **Link-State-Update (LSU):** Antwort auf LSR -> Bekanntmachen von Informationen durch LSAs
5. **Link-State-Acknowledgement (LSAck):** Empfänger bestätigt den Erhalt eines LSU-Pakets

Algorithmus

- Dijkstra Shortest-Path-First Algorithmus
- Errechnet die kumulativen Kosten um ein Ziel zu erreichen
- Erstellt SPF-Baum
    - Setzt jeden Router als Beginn des Baums
    - Errechnet dann den kürzesten Pfad zu jedem anderen Router
- Daraus entstehen die Routen für die Forwarding-Database

Datenstrukturen

- **Adjacency-Datenbank**
    - Benachbarte Router, zu denen es eine bidirektionale Verbindung gibt
    - Einzigartig pro Router
    - Show ip ospf neighbor
- **Link-State-Datenbank**
    - Alle anderen Router im Netzwerk
    - Stellt Topologie dar
    - Identisch bei jedem Router
    - Show ip ospf database
- **Forwarding-Datenbank**
    - Durch Algorithmus generierte Routen auf Basis der LSDB
    - Einzigartig pro Router
    - Show ip route

Ablauf: Link-State Operation

1. **Neighbor-Adjacency einrichten**
    - OSPF-Router müssen prüfen ob es weitere OSPF-Router in der „Nachbarschaft“ gibt
    - Senden „Hello“-Pakete aus allen OSPF-Schnittstellen
2. **Link-State-Advertisements (LSAs) austauschen**
    - Es werden Status und Kosten von jedem angebundenen Link an die Nachbarn ausgetauscht
    - Jeder Router sendet alle LSAs auch an alle anderen Router weiter, bis jeder Router alle LSAs hat
3. **Link-State Datenbank bauen**
    - Aus allen erhaltenen LSAs wird die LSDB gebaut
    - Daraus resultiert die Netzwerktopologie
4. **Ausführen des SPF-Algorithmus**
    - Es wird auf der Basis der LSDB der SPF-Baum erstellt
5. **Beste Route wählen**
    - Die besten Routen aus dem SPF-Baum zu jedem Netzwerk werden in die Routingtabelle aufgenommen, außer es gibt dort bereits eine Route zu diesem Netzwerk mit einer niedrigeren administrativen Distanz (z.B. statische Route)

Single- & Multi-Area

- **Single-Area**: Alle Router sind in derselben Area (Normalerweise: 0)
- **Multi-Area**:
    - Hierarchische Abtrennung von Areas
    - Alle Areas müssen mit dem Backbone (Area: 0) verbunden sein
    - Router zwischen Areas sind „Area Border Routers“ (ARBs)
    - Vorteile:
        - **Kleinere Routingtabellen**: Weniger Einträge, da Netzwerkadressen zusammengefasst werden können
        - **Reduzierter Berechnungsaufwand**: Neuberechnung der Datenbank nach Topology-Change nur für eigene Area
        - **Reduzierte Anzahl von Berechnungen**: LSA-Floods sind geringer, da weniger Router in derselben Area sind

Designated-Router (DR) Notwendigkeit

Probem

- Bei der Initialisierung oder bei Topology-Changes werden jedes Mal wieder LSAs von jedem Router versendet
- Netzwerk kann stark belastet werden
- Durch die Erstellung von Neighbor Ajacencies können viele Nachbarschaften entstehen => Unnötig
    - Bei 5 Routern im selben Netz -> 10 Nachbarschaften (20 R -> 190 N): n(n-1) /2

Lösung

- Es wird ein Designated Router erklärt (Zusätzlich auch ein Backup Designated Router (BDR) für den Fall des Ausfalls des DR)
    - Router mit der höchsten konfigurierten Interface-Priorität wird DR, zweithöchste wird BDR
    - Router die mit der Prio 0 konfiguriert wurden können nicht DR oder BDR werden
    - Wenn keine Prio konfiguriert ist (alle Router Prio 1) wird die Router-ID zur Entscheidung verwendet
    - Kommt ein neuer Router mit einer höheren ID hinzu wird die Wahl nicht wiederholt
- Alle anderen Router werden zu DROthers
- Alle Router senden nur noch an DR und BDR LSAs
- Der aktive DR verteilt dann an alle anderen Router das empfangene LSA
- Beim Ausfall des DR übernimmt der BDR und der DROther mit der höchsten Prio wird zum neuen BDR
- Neuer DR (alter BDR) bleibt DR, auch wenn ursprünglicher DR wieder da ist > solange bis entweder ausfall, oder neues Bestimmen (händisch)

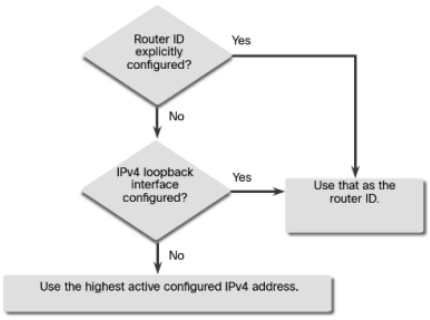
OSPF-Router-ID

- Elementarer Bestandteil von OSPF
- 32bit-Wert in Form einer IP-Adresse
- Jeder Router hat eine OSPF-Router-IDW
    - Verwendet die ID um…
        - Am Synchronisierungsprozess der OSPF Datenbanken teilzunehmen (Höchste ID beginnt)
        - Um den DR (Höchste ID) und BDR (Zweithöchste ID) zu bestimmen

Bestimmungsprozess

1. Ist die ID manuell festgelegt -> Manuelle ID verwenden
2. Loopback-IP ist konfiguriert -> Loopback-IP als ID verwenden
3. Höchste aktive konfigurierte IP-Adresse verwenden

- Wird die ID im Nachgang verändert muss OSPF neugestartet werden, da bereits mit der vorherigen ID Nachbarschaften bekanntgemacht wurden



Wildcard-Maske

- **Berechnung**: /32-Subnetzmaske – Konfigurierte Subnetzmaske = Wildcard-Maske
    - Umkehrung der Subnetzmaske
- Notwendig bei der Netzwerkkonfiguration für OSPF an einem Router

Punkt-zu-Punkt OSPF-Netzwerke

- Mehrere Router im selben Netzwerk
- DR und BDR werden gewählt um Netzlast zu reduzieren
- Wenig Overhead, da LSAs nur zwischen zwei Routern ausgetauscht werden müssen
- Einfacher Aufbau

Multiaccess OSPF-Netzwerke

- Mehrere Router im selben Netzwerk
- DR und BDR werden gewählt um Netzlast zu reduzieren

Single-Area OSPF Netze anpassen

Kosten:

- Kosten einer Route sind abhängig von der Bandbreite der Schnittstelle
    - Je höher die Bandbreite, desto niedriger die Kosten
- Kosten für 100M, 1G und 10G sind gleich, da sie immer auf 1 gerundet werden
    - Um bessere Leitungen zu priorisieren müssen die Kosten manuell konfiguriert werden
    - => Kosten für 100M und 1G sollten höher sein als für 10G
- **Berechnung**: Referenzbandbreite / Bandbreite = Kosten
- Kosten für eine Route werden aus der Summe der verwendeten Leitungen berechnet

Default-Route

- Wird verwendet um Traffic in andere Netze weiterzuleiten (z.B. Internet)
- **Autonomous-System-Boundary-Router (ASBR):** Router der zwischen einem OSPF- und einem Nicht-OSPF-Netz hängt
- Route muss am ASBR angelegt werden (ip route 0.0.0.0/0 next-hop)
- ASBR muss als Quelle der Route festgelegt werden für OSPF (default-information originate)

Access Control Lists (ACLs)

- Liste aus Access Control Entries
- Access Control Entries: Filter für Netzwerkverkehr (deny/allow)
- Jedes Paket wird mit den auf dem Interface festgelegten ACEs abgeglichen (**Layer 3 & 4**)
- Fördern Sicherheit und/oder Performance
- Können auf eingehenden (**inbound**) und ausgehenden (**outbound**) Verkehr konfiguriert werden
    - Inbound spart dem Router das heraussuchen der passenden Route
- Ablauf:
    - Jedes Paket durchläuft die ACL und damit jeden darin enthaltenen ACE nacheinander
    - Sobald ein ACE mit der Quell-IP übereinstimmt wird die ACE Aktion ausgeführt
    - Gibt es keinen Treffer wird das Paket verworfen, da am Ende jeder ACL ein implizites Deny-All existiert
- Bei der Erstellung von ACEs werden ebenfalls Wildcard-Masken verwendet (siehe OSPF)
    - 0.0.0.0 kann durch „host“ ersetzt werden
    - 255.255.255.255 kann durch „any“ ersetzt werden

Standard-ACLs

- Filter nur anhand der Quell-IP-Adresse
- Typischerweise am Ziel angewandt
- Können auch mittels „access-class“ auf Terminal-Schnittstellen gelegt werden um den Zugriff auf Geräte zu limitieren

Konfiguration

- Beispiele in grün

Nummerierte Standard ACL

access-list *access-list-number* {deny | permit | remark *text*} *source* [*source-wildcard*]
access-list 10 permit 192.168.20.0 0.0.0.255
access-list 10 permit host 192.168.20.1

Benannte Standard ACL

ip access-list standard *access-list-name*
ip access-list standard PERMIT-ACCESS
permit *source* [*source-wildcard*]
permit 192.168.20.0 0.0.0.255
permit host 192.168.10.10

Bearbeiten

Ip access-list standard {access-list-name | access-list-number}
Ip access-list standard PERMIT-ACCESS
Ip access-list standard 10
No sequence-number
No 10
Sequence-number {deny | permit | remark text} source [source-wildcard]
10 permit host 192.168.20.21

Extended-ACLs

- Filter anhand…
    - Quell-IP-Adresse
    - Ziel-IP-Adresse
    - TCP/UDP-Ports
    - Protokoll
- Typischerweise an der Quelle angewandt
    - Bandbreite einsparen
- Kann stateful arbeiten: TCP-Replies zulassen aber TCP-Requests nicht (established)

Konfiguration

- Beispiele in grün

Nummerierte Extended-ACL

access-list *access-list-number* {deny | permit | remark *text*} *protocol source source-wildcard* [*operator* {*port*}] *destination destination-wildcard* [*operator* {*port*}] [established]
access-list 10 permit tcp 192.168.10.0 0.0.0.255 any eq 443
access-list 20 permit tcp 192.168.10.0 0.0.0.255 192.168.0.0 0.0.255.255 eq www

Benannte Extended ACL

Ip access-list extended access-list-name

Ip access-list extended SURFING

{deny | permit | remark *text*} *protocol source source-wildcard* [*operator* {*port*}] *destination destination-wildcard* [*operator* {*port*}] [established]

Permit tcp 192.168.10.0 0.0.0.255 any eq 80

Permit tcp 192.168.10.0 0.0.0.255 any eq 443

Bearbeiten

Ip access-list extended {access-*list-name* | *access-list-number*}

Ip access-list extended SURFING

Ip access-list extended 10

No *sequence-number*

No 10

Sequence-number {deny | permit | remark *text*} *protocol source source-wildcard* [*operator* {*port*}] *destination destination-wildcard* [*operator* {*port*}] [established]

10 permit tcp 192.168.10.0 0.0.0.255 any eq www

Allgemeingültige Konfiguration

Anwenden auf Interface

Enable

Configure terminal

Interface g0/0/0

ip access-group {*access-list-number* | *access-list-name*} {in | out}

ip access-group 10 out

ip access-group PERMIT-ACCESS out

NAT IPv4 (Network Address Translation)

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

Vorteil

- 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

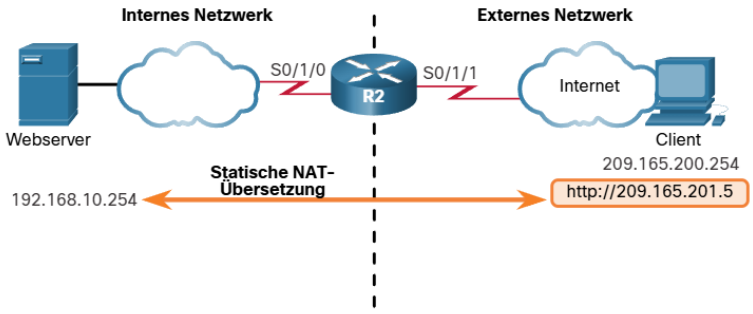
- Zusätzliche Verzögerung durch NAT/PAT (Kritisch bei Echtzeitprotokollen -> VoIP)
- End-to-End-Adressierung geht verloren (Manche Anwendungen kommen nicht mit NAT klar)
- Fehlersuche durch Adressänderung erschwert

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 Zielmeistens 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)

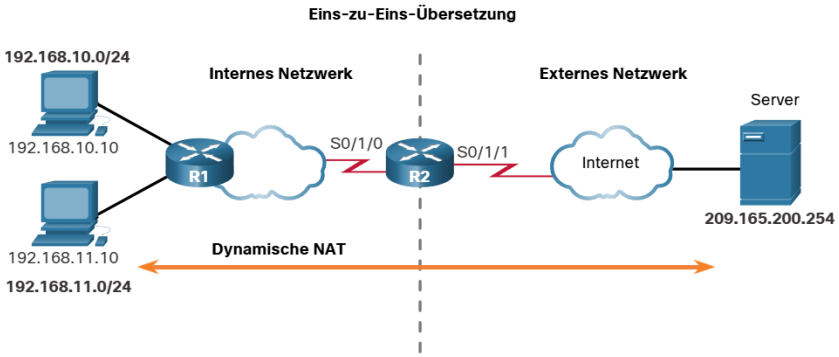
Arten von NAT

Statisches NAT



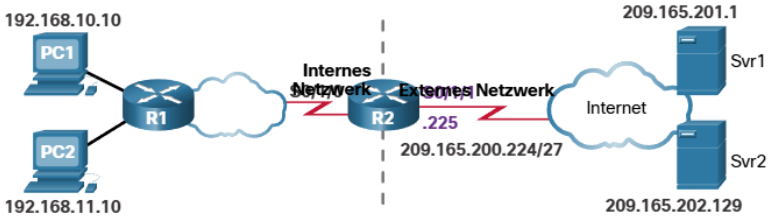
- 1:1 Übersetzung der privaten in öffentliche Adressen
- Für das Internet haben die einzelnen Geräte öffentliche IP-Adressen
- Manuell konfiguriert und zugeordnet
- Hilfreich, wenn Geräte von der gleichen öffentlichen IP erreichbar bleiben müssen (Webserver)
- Benötigt ausreichend öffentliche IP-Adressen
- 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)

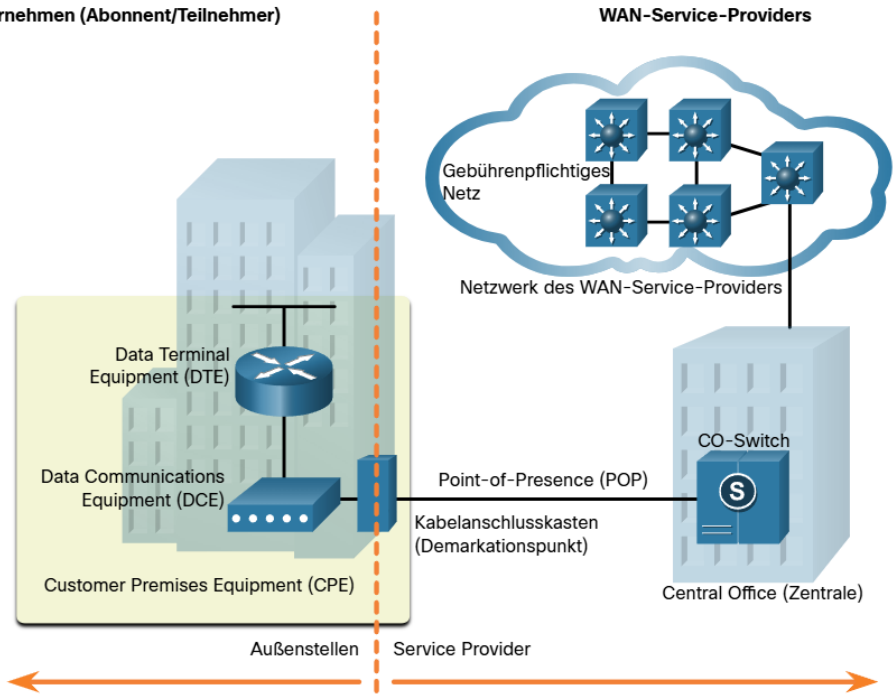
- **WAN**: Kommunikationsnetz, dass sich über einen großen geografischen Bereich erstreckt
- Notwendig um Remote-LANs mit dem eignen LAN zu vernetzen

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

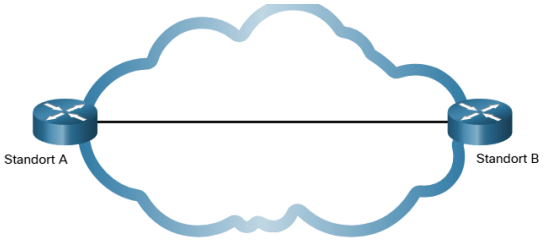


- **Data Terminal Equipment (DTE):** Verbindet Teilnehmer-LANs mit dem WAN-Kommunikationsgerät
- **Data Communications Equipment (DCE) (Datenleitungs-Endgerät):** Kommunikation mit dem Provider
- **Customer Premises Equipment (CPE):** Fasst DTEs und DCEs am Firmenstandort zusammen
- **Point-of-Presence (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

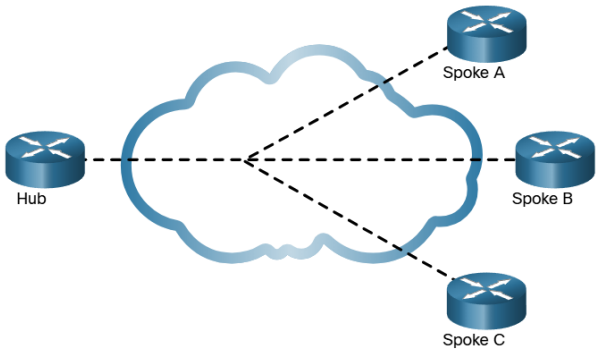
- Werden durch logische Topologien beschrieben

Punkt-zu-Punkt



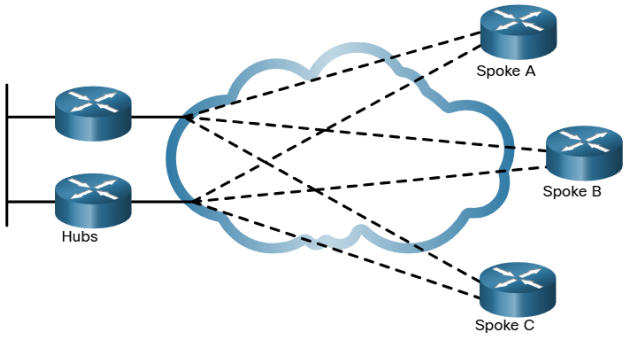
- Verbindung zwischen zwei Endpunkten
- Scheinbar eine physische Verbindung zwischen den Endpunkten
- Z.B. Standleitung (Teuer)

Hub-and-Spoke



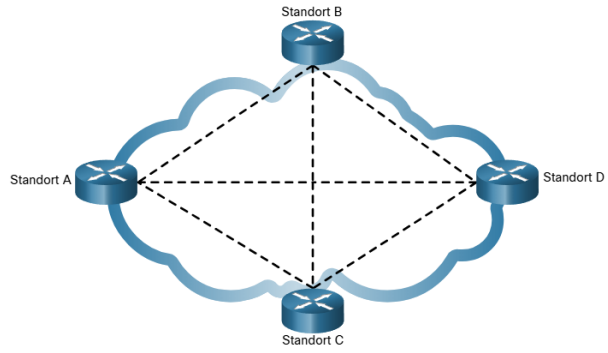
- Mehrere Spokes verwenden eine Schnittstelle des Hubs
  - Durch Subinterfaces oder virtuelle Verbindungen
- Spokes können nur über den Hub miteinander kommunizieren
- Hub ist Single-Point of Failure

Dual-Homed



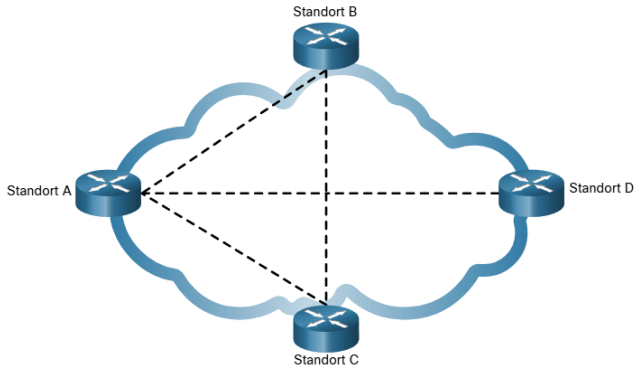
- Erweiterung von Hub-and-Spke
- Bietet Redundanz, Lastverteilung, dezentrale Datenverarbeitung
- Implementierung ist teurer (mehr Hardware nötig; komplexe Einrichtung)

Vollständig vermascht



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

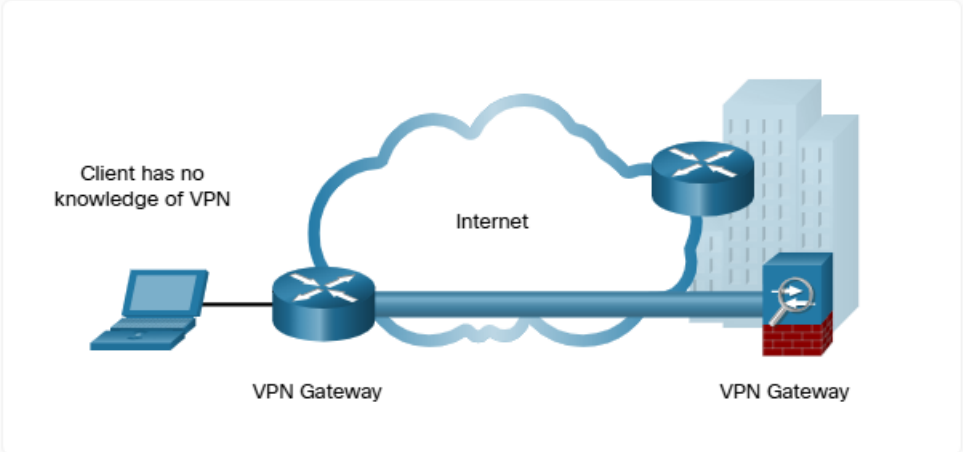
Teilweise vermascht



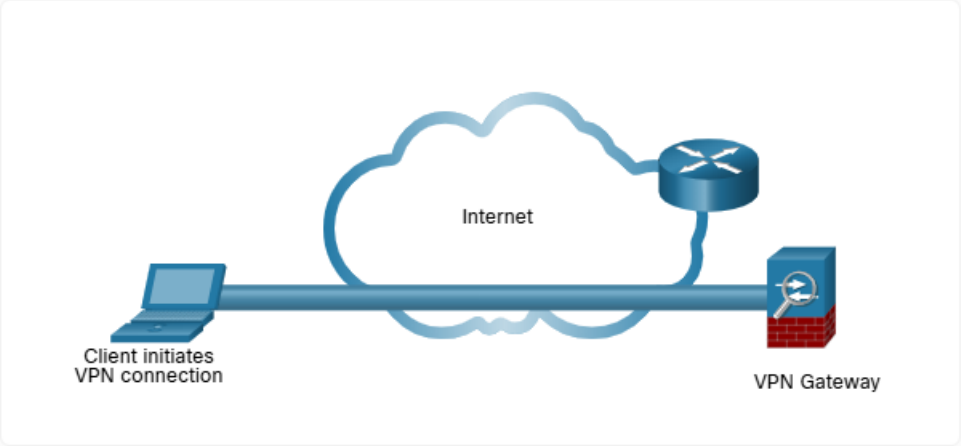
- Verbindet viele Standorte miteinander, aber nicht alle
- Schlechtere Fehlertoleranz als vollvermascht

VPN

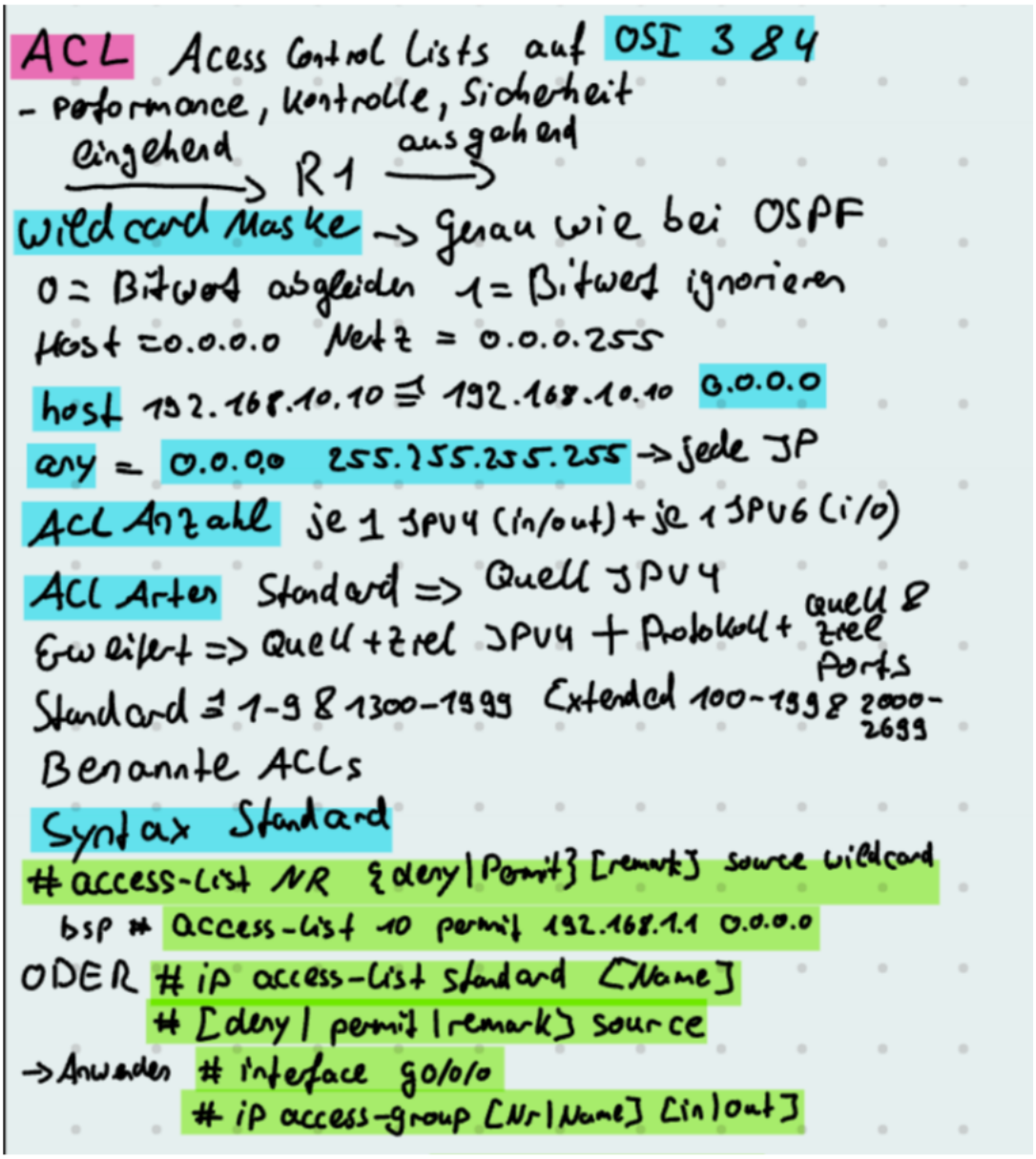
- Virtual Privat Network
- Benefits:
  - **Cost-Saving**: Da VPN-Router eine sehr hohe Bandbreite zueinander auf weißen ist es sehr kosten effizient dadurch eine hohe Bandbreite zu erreichen
  - **Security**: wegen der vorgeschrittenen Verschlüsslung von VPN-Tunneln weißt du dieser ein hohes Level an Sicherheit auf
  - **Scalability**: Es ist sehr einfach neue VPN-Clients und Router einem Bestehenden VPN-Netzwerk hinzuzufügen, dadurch ist das System sehr gut Skalierbar
  - **Compatibility**: Durch die hohe Standardisierung des VPN-Systems können viele Clients und Router in der gesamten Welt funktionieren zusammen.
- Types:
  - Site-to-Site VPN
    - Das ist eine Verbindung von 2 VPN Routern über das WAN zwischen z.B. zwei Standorten einer Firma

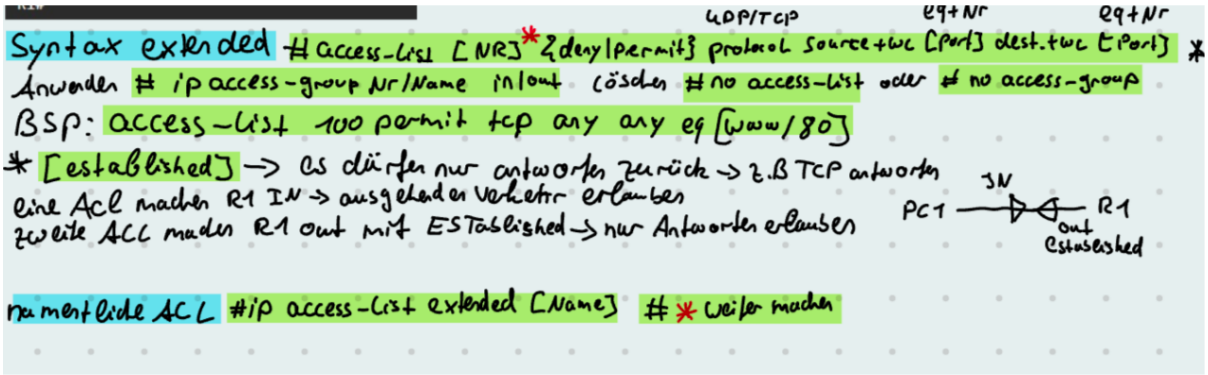


  - Remote-Access VPN
    - Verbindung zwischen einem Client (z.B. Laptop) und dem VPN-Router der Firma das ein VPN Tunnel entsteht so das z.B. aus dem Homeoffice geartbeite werden kann.



Shenjas Notes





DHCP

Ser — Client
Discover Broad →
← Offer uni
Request Broad →
← Ack uni

DHCPV6

A-Flag = Address Autoconfigure
O = other
M = Managed
Stateless | stateful
A A=0 | M
stateless SLAAC | DHCPV6
only DHCP

First Hop Redundancy Protokoll

→ Priority (Std. = 100)
→ IP-Adr
→ Höher gewinnt
VIP = Virtuelle IP ≙ Std.-gateway

Statisches NAT

Dynamisches NAT

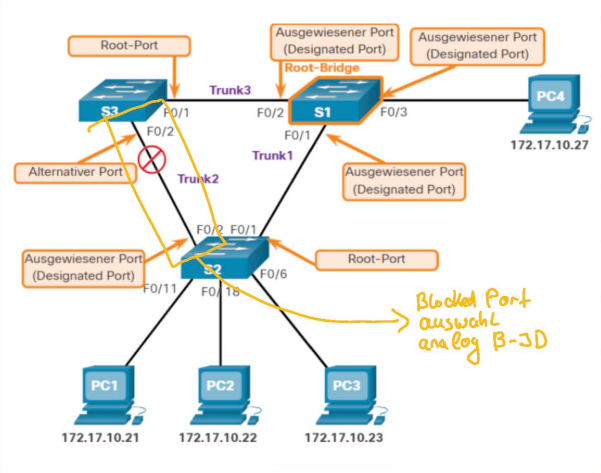
PAT

TCP

SYN →
← SYN ACK
ACK →

STP (Switch)

Kleinste Bridge-ID gewinnt
→ Root-Bridge
- Prio → 4096 Schritte
+ VLAN
+ MAC-Adresse



OSPF (Router)

- Adjacency database
  → Benachbarte Router
  → Einzigartig
- Link-State-DB
  → Topologie aller Router
  → Bei jedem gleich
- Forwarding DB ≙ Routing Tabelle
  → Router
  → Einzigartig

ABLAUF

Neighbour Adjacency ermitteln
→ Hello Pakete
Linkstate advertisements austauschen
LSA
Link-State-DB bauen
SPF-Algorithmus ausführen
Beste Route wählen → Forwarding DB

DR + BDR

- Höchste Prio gewinnt
  (0 wird ausgeschlossen)
  (1 ist Std)
- Router-ID
  1. manuelle ID
  2. Loopback IP
  3. höchste IP

→ STP

→ FHRP

ACL

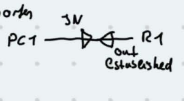
Access Control Lists auf OSI 3 & 4
- Performance, Kontrolle, Sicherheit

eingehend → R1 → ausgehend

Wildcard Maske → genau wie bei OSPF
0 = Bitwert abgleichen 1 = Bitwert ignorieren
Host = 0.0.0.0 Netz = 0.0.0.255
host 192.168.10.10 ≙ 192.168.10.10 0.0.0.0
any = 0.0.0.0 255.255.255.255 → jede IP
ACL Anzahl je 1 IPv4 (in/out) + je 1 IPv6 (i/o)
ACL Arten Standard => Quell IPv4
Erweitert => Quell+Ziel IPv4 + Protokoll + Quell & Ziel Ports
Standard ≙ 1-99 & 1300-1999 Extended 100-199 & 2000-2699
Benannte ACLs

Syntax Standard
access-list NR {deny|permit} [remark] source Wildcard
bsp # access-list 10 permit 192.168.1.1 0.0.0.0
ODER # ip access-list standard [Name]
[deny | permit | remark] source
→ Anwenden # interface g0/0/0
ip access-group [Nr|Name] [in|out]

Syntax extended # access-list [NR]* {deny|permit} protocol source+wc [Port] dest.+wc [Port] *
(UDP/TCP eq+Nr eq+Nr)
Anwenden # ip access-group Nr/Name in|out löschen # no access-list oder # no access-group
BSP: access-list 100 permit tcp any any eq [www/80]
* [established] → es dürfen nur antworten zurück → z.B. TCP antworten
eine ACL machen R1 IN → ausgehenden Verkehr erlauben
zweite ACL machen R1 out mit ESTablished → nur Antworten erlauben



momentliche ACL # ip access-list extended [Name] # * weiter machen