Inhalt

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
- **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

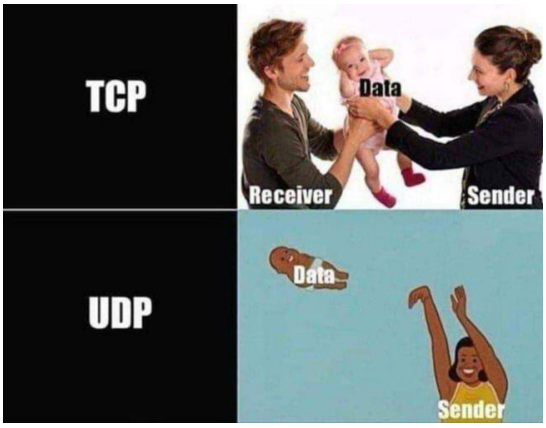
- Automatisierte Zuweisung von Netzwerkeinstellungen wie IP-Adresse, Subnetzmaske, Gateway und DNS-Server
- Gegenstück ist die statische Adressierung
- DHCP-Netzwerkgeräte fordern beim Verbinden zum Netzwerk DHCP-Daten an
- Die DHCP-Daten haben eine definierte Gültigkeitsdauer (Lease-Dauer)
    - Nach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

OSI Layer 4: Transportschicht

- Verantwortlich für Kommunikation zwischen Anwendungen auf verschiedenen Hosts
- Verwaltet alle Konversationen zwischen Hosts
- Segmentiert Daten und setzt Daten zusammen für den Transportweg
- Fügt Header-Daten hinzu, damit der Empfänger die Daten richtig interpretiert
- Ziel-Anwendung wird über Port-Nummer identifiziert



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

Anwendung

- 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

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 kleine 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

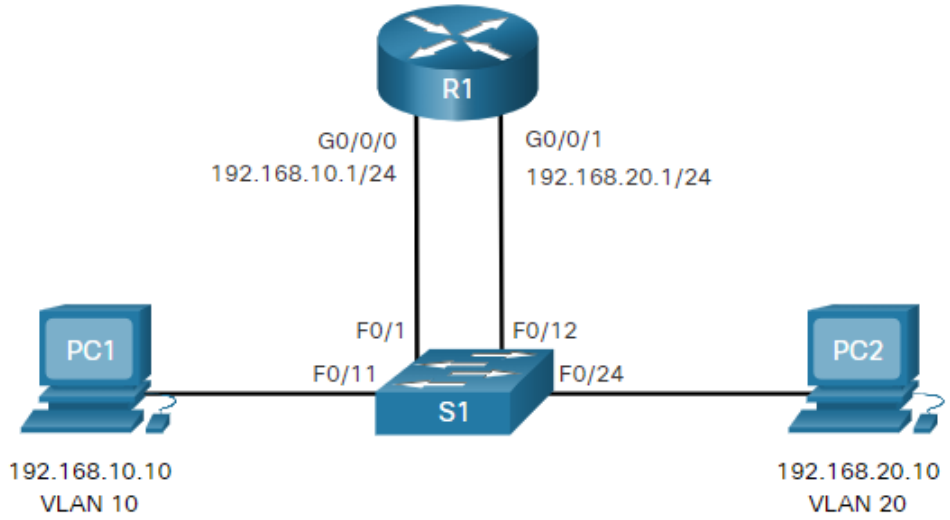
VLAN-Trunk (IEEE 802.1Q)

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

Inter-VLAN-Routing

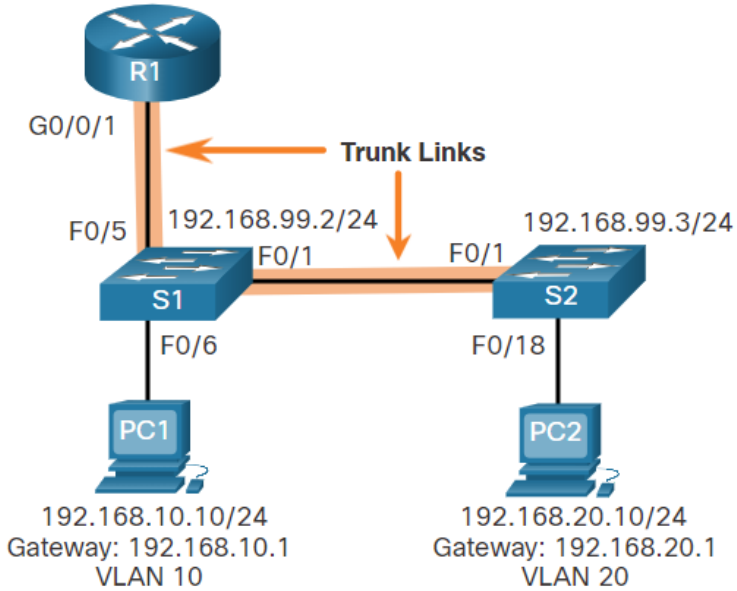
Inter-VLAN-Routing ist der Prozess der Weiterleitung von Netzwerkverkehr von einem VLAN zu einem anderen VLAN

Legacy-Inter-VLAN-Routing



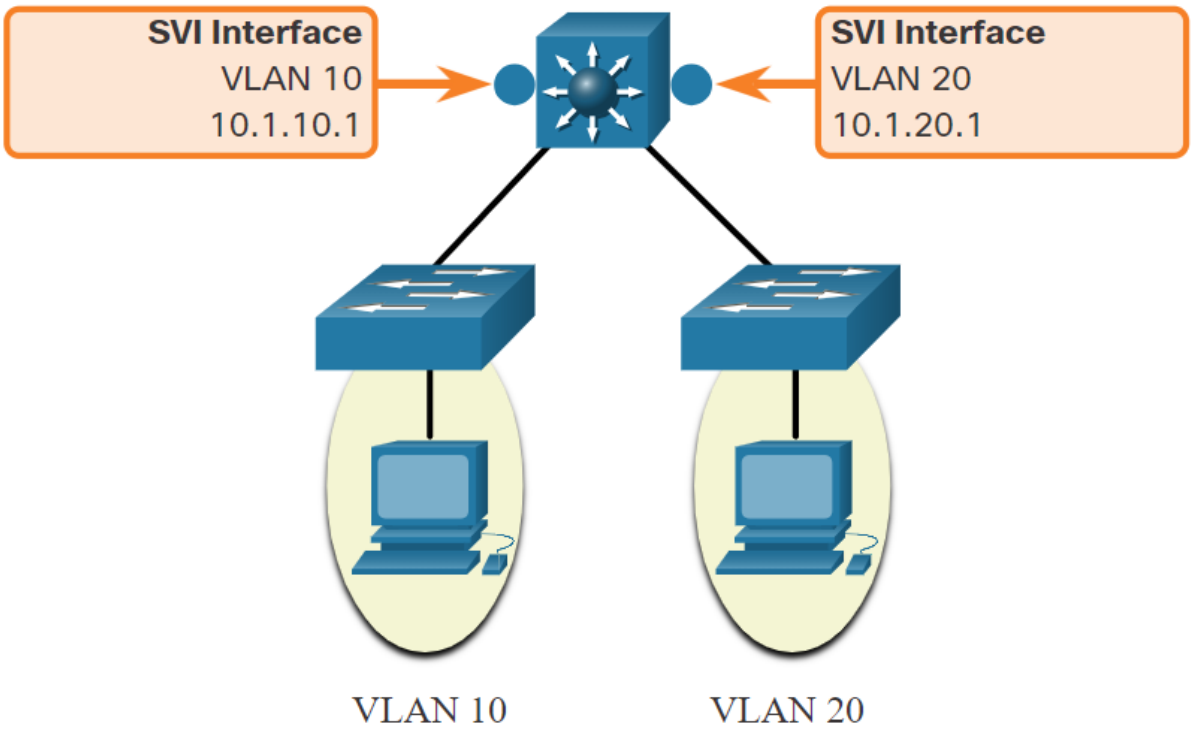
- Router mit mehreren Ethernet-Schnittstellen
- Jede Schnittstelle ist mit einem Switchport in einem VLAN verbunden und stellt das Standardgateway des VLANs dar
- Bei vielen VLANs werden am Switch und am Router viele Ports benötigt
    - Schlecht Skalierbar

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