Ethernet

Netzwerkgrundlagen (NWG2)

Markus Zeilinger[1]

[1]FH Oberösterreich
Department Sichere Informationssysteme

Sommersemester 2023

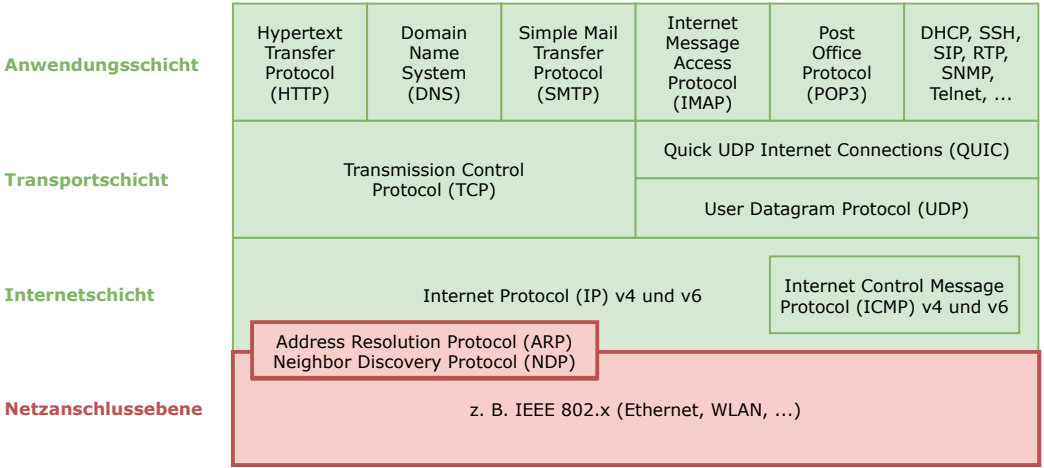
FH OBERÖSTERREICH
UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

Wichtiger Hinweis

Alle Materialien, die im Rahmen dieser LVA durch den LVA-Leiter zur Verfügung gestellt werden, wie zum Beispiel Foliensätze, Audio-Aufnahmen, Übungszettel, Musterlösungen, ... dürfen ohne explizite Genehmigung durch den LVA-Leiter NICHT weitergegeben werden!

Inhalt

Netzanschlussebene in der TCP/IP Protokollfamilie



Aufgaben der Netzanschlussebene

Übertragung von Daten an direkt angeschlossene Netzwerke
(umfasst OSI Schichten 1 und 2, keine genauer Spezifikation in TCP/IP)
frei von unerkannten Übertragungsfehlern.

- Kernaufgaben der Netzanschlussebene
  - Kapselung von IP Paketen in Frames,
  - Zuordnung von IP Adressen zu Hardware-Adressen (z. B. MAC Adressen im Ethernet) und
  - Fehlererkennung/-korrektur.
- Technologien (sehr umfangreich!): IEEE 802.3 Ethernet, IEEE 802.11 WLAN, IEEE 802.15.4 WPAN (u. a. Basis für Zigbee und Thread), ITU G.9959 (u. a. Basis für Z-Wave), Point-to-Point Protocol (PPP, u.a. Datenübertragung über Wählleitungen bei DSL), ...

Ethernet ("Äthernet")

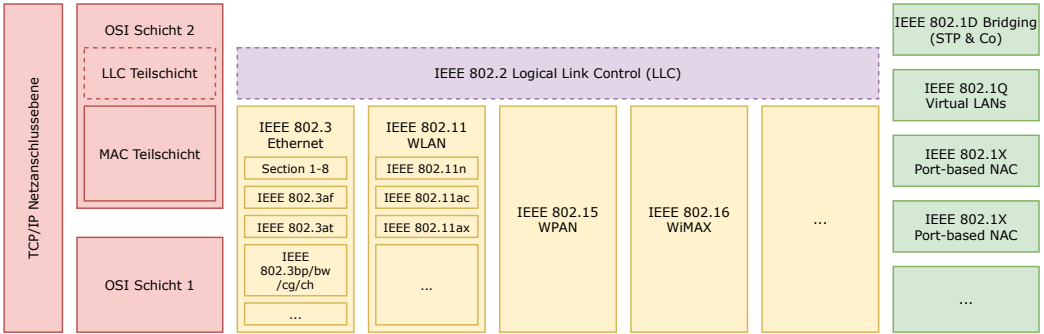
- Ursprünglich von Robert Metcalfe (Gewinner Turing Award 2022!) am Xerox Palo Alto Research Center (PARC) entwickelt.
- Schicht 1+2 Technologie (Netzzugangstechnologie) für verdrahtete LANs.
- Seit 1980 Standardisierung über die IEEE 802 Gruppe.
- Erfolgsfaktoren für Ethernet: einfach, robust, kostengünstiger als vergleichbare Technologien (z. B. IEEE 802.5 Token Ring) (v. a. wegen frühem Fokus auf Twisted Pair Kabel).
- Heute: Im LAN Bereich die alles beherrschende Technologie.
  - Starke Konvergenz in Richtung Ethernet: Metro Ethernet bzw. Carrier Ethernet (MAN, WAN), Ethernet in the first mile (EFM), Industrial Ethernet, Automotive Ethernet, Speichernetze, ...

- Old School Ethernet: Zusammenschluss von Systemen an einem gemeinsamen Netzwerk (Bustopologie auf Basis Koaxial Kabel) in Form eines Shared Mediums.
  - Shared (geteiltes) Medium + Bustopologie
  - → Half-Duplex Kommunikation (→ NWA Intro)
  - → Medienzugriffssteuerung mittels CSMA/CD (Carrier Sense Multiple Access with Collision Detection).
- Modernes Ethernet (Full-Switched Ethernet): Stern-/Baum-Topologien im Full-Duplex Betrieb realisiert durch Switches → keine Medienzugriffssteuerung notwendig.

- Ethernet ist verbindungslos und unzuverlässig.
- Framing = Ethernet teilt den endlosen Bitstrom der Bitübertragungsschicht in Frames bzw. packt die PDUs der Netzwerkschicht in Frames ein.
- Fehlererkennung über ein CRC (Cyclic Redundancy Check) Verfahren (keine Fehlerkorrektur).
- Weiterführende Features (u. a.):
  - Virtual LANs: Logische Netzwerkorganisation unabhängig von der physischen Netzwerkinfrastruktur.
  - Power over Ethernet: Stromversorgung von Endgeräten über Twisted Pair Kabel.
  - Spanning Tree Protocol (STP): Ethernets mit physischer Leitungsredundanz (zwecks Ausfallssicherheit).

IEEE 802 Projekt

- IEEE 802 = Standards im LAN/MAN Bereich (http://www.ieee802.org/).



- Aktuelle Fassung: IEEE 802.3-2022

Jahr	Variante	Std/Erweiterung	Datenrate max.	K [1]	TP [1]	F [1]
1985	Ethernet	IEEE 802.3	10 Mbps	X	X	
1995	Fast Ethernet	IEEE 802.3u	100 Mbps		X	X
1998	Gigabit Ethernet	IEEE 802.3z/ab/ah	1 Gbps		X	X
2002	10 Gigabit Ethernet	IEEE 802.3ae/ak/an/ap/aq	10 Gbps		X	X
2010	40/100 Gigabit Ethernet	IEEE 802.3ba/bg	40/100 Gbps			X
2016	25/40 Gigabit Ethernet	IEEE 802.3bq	25/40 Gbps		X	X
2016	2.5/5 Gigabit Ethernet	IEEE 802.3bz	2.5/5 Gbps		X	
2017	200/400 Gigabit Ethernet	IEEE 802.3bs	200/400 Gbps			X

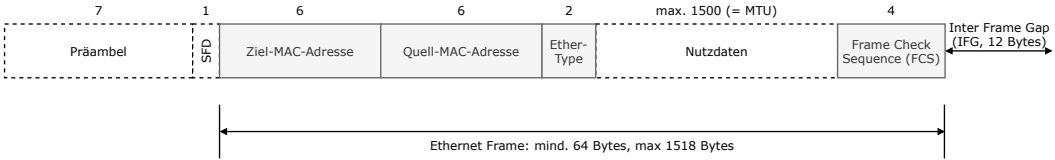
[1] K ... Koaxialkabel, TP ... Twisted Pair Kabel, F ... Fiber/Glasfaser (→ Kabel & Co)

- Benennungsschema Ethernet-Varianten: `X[G]BASE-Y`
- X ... maximal mögliche Datenrate (`10`, `100`, `1000` Mbps, `2.5G`, `5G`, `10G`, `25G`, `40G`, `100G`, `200G`, `400G` Gbps)
- Y ... nicht einheitlich genutzt
  - ... Medium: `-T` (Twisted Pair), `-S` (short, Multi-Mode Fiber, MMF), `-L` (long, Single-Mode Fiber, SMF), `-2/5` Koaxialkabel, ...
  - ... Codierung: `X`, `R` (PCS Kodierung)
  - ... Anzahl virtueller Kanäle oder Distanzen: `1`, `2`, `4`, `10`, ...

- Beispiel 1: `100BASE-TX`
  - Fast Ethernet, 100 Mbps Datenrate (`100`), Twisted Pair Kabel (`T`), PCS Kodierung (`X`), 100 m Distanz
- Beispiel 2: `100BASE-SX`
  - Fast Ethernet, 100 Mbps Datenrate (`100`), Multi-Mode Glasfaser, kurze Wellenlänge 850 nm (`S`), PCS Codierung (`X`), 550 m Distanz
- Beispiel 3: `1000BASE-T`
  - Gigabit Ethernet, 1 Gbps Datenrate (`1000`), Twisted Pair Kabel (`T`) (mind. Cat5e), 100 m Distanz
- Beispiel 4: `10GBASE-T`
  - 10 Gigabit Ethernet, 10 Gbps Datenrate (`10G`), Twisted Pair Kabel (`T`) (mind. Cat6a/7), 100 m Distanz

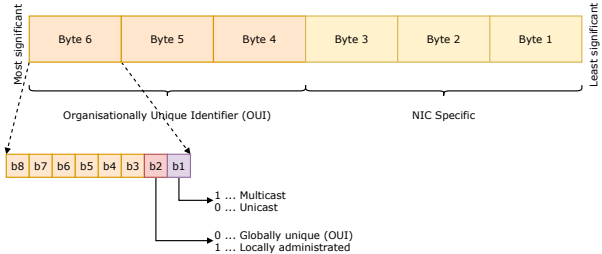
- Beispiel 5: `10GBASE-LR`
  - 10 Gigabit Ethernet, 10 Gbps Datenrate (`10G`), Single-Mode Faser, lange Wellenlänge 1310 nm (`L`), PCS Kodierung (`R`), 10 km Distanz
- Beispiel 6: `100GBASE-ER4`
  - 100 Gigabit Ethernet, 100 Gbps Datenrate (`100G`), Single-Mode Faser, 4 Farben/Wellenlängen (`E 4`), PCS Kodierung (`R`), 40 km Distanz
- Beispiel 7: `40GBASE-T`
  - 40 Gigabit Ethernet, 40 Gbps Datenrate (`40G`), Twisted Pair Kabel (`T`) (mind. Cat8), 30 m Distanz

Ethernet II Header nach IEEE 802.3 I



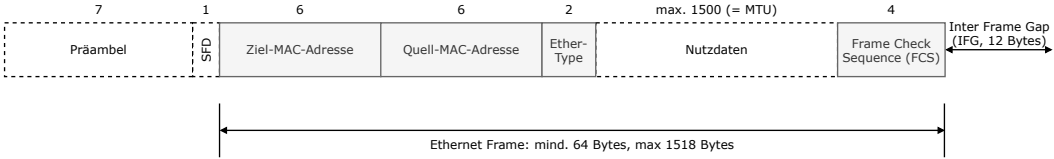
- Prämbel und Start Frame Delimiter (SFD) dienen zur Erkennung eines Frames und zur Synchronisation.
- Ziel- und Quell-MAC-Adresse
  - 48-Bit Hardware-Adresse des Senders und des Empfänger im direkt angeschlossenen Netzwerk (direkte Route).
  - Werden vom Hersteller eines Netzwerk Interfaces einprogammiert und sind aufgrund des Vergabeprozesses weltweit eindeutig (eindeutig sein müssen sie innerhalb eines LANs bzw. einer s. g. Broadcast Domain).
  - Schreibweise (hexadezimal): `00-24-D7-73-A3-34` (Windows), `00:24:D7:73:A3:34` (Linux), `0024.D773.A334` (Cisco) oder `0024D773A334`

Ethernet II Header nach IEEE 802.3 II



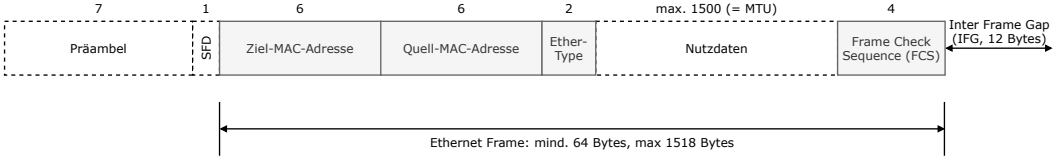
- Teilung in zwei Teile:
  - Organisationally Unique Identifier (OUI) = Kennzeichnung des Herstellers.
  - NIC Specific = fortlaufende Nummer für die NIC, vergeben durch den Hersteller.
- Verwaltung durch IEEE (Produkt z. B. MAC Address Block - Large [MA-L], Abfrage Registrierungen).
- Broadcast-MAC-Adresse: `ff:ff:ff:ff:ff:ff`

Ethernet II Header nach IEEE 802.3 II



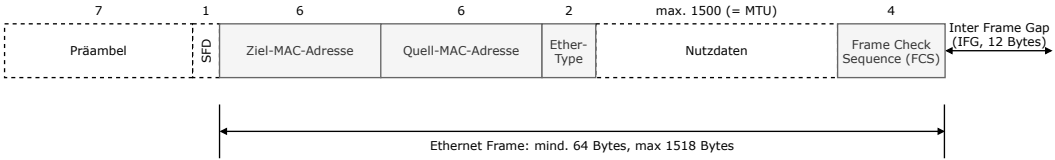
- EtherType
  - Codiert das im Frame enthalteten nächst höhere Protokoll und gibt damit die Interpretation der Nutzdaten im Ethernet Frame vor.
  - Verwaltung durch die IEEE, Abfrage Registrierungen.
  - Beispiele: 0x0800 (IPv4), 0x86DD (IPv6), 0x8100 (VLAN), 0x0806 (ARP, Address Resolution Protocol)

Ethernet II Header nach IEEE 802.3 III



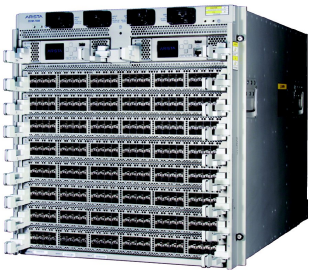
- Nutzdaten
  - Pro Ethernet Frame sind mind. 46 und max. 1500 Byte an Nutzdaten zulässig (ggf. Auffüllung durch ein 0-Padding).
  - Die Maximum Transmission Unit (MTU, = größtmögliche Dateneinheit, die ein Protokoll in sich transportieren kann) von Ethernet ist daher 1500 Bytes ($\rightarrow$ IP - Fragmentierung, TCP - Maximum Segment Size [MSS] Option).
  - Daneben gibt es s.g. Jumbo Frames (MTU 9000 Bytes, Verbesserung des Header-Nutzdaten-Verhältnisses) ab Gigabit Ethernet.

Ethernet II Header nach IEEE 802.3 III



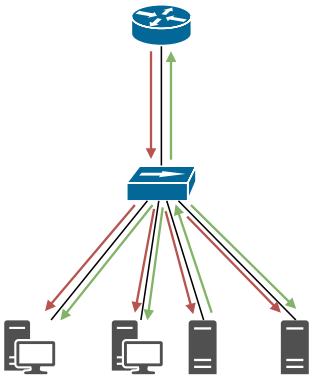
- Frame Check Sequence (FCS)
  - 32-Bit Prüfsumme zur Erkennung von Übertragungsfehlern (keine Fehlerkorrektur).
  - Verfahren: 32-Bit Cyclic Redundancy Check (CRC) basierend auf einer polynomialen Division.
  - CRC erkennt sehr zuverlässig Übertragungsfehler, ist aber nicht für Schutz vor absichtlicher Veränderung geeignet ($\rightarrow$ WEP in IEEE 802.11 WLAN).

Aktive Netzwerkkomponenten



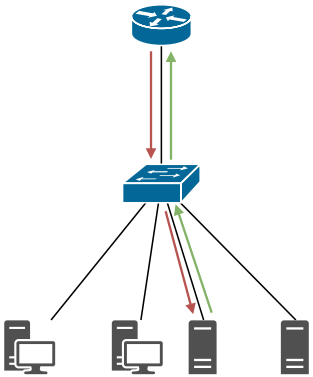
Repeater und Hub (Schicht-1)

- Zweck: Signalerneuerung zur Überbrückung von max. Distanzen (Signalverlust durch Dämpfung).
- Repeater hat 2, Hub 4/8/16/.. Interfaces (Hub = Multi-Port Repeater).
- Prinzip: Repeater/Hub leitet Daten an alle außer das eingehende Interface weiter (Flooding).
  - → jedes System sieht die Daten aller anderen.
  - → physisch Stern aber logisch Bus (→ Shared Medium, Medienzugriffssteuerung).
- Alle Systeme an einem Repeater/Hub befinden sich in der gleichen Kollisiondomäne.
- Hubs praktisch irrelevant, Repeater im WAN Bereich von Bedeutung.



Bridge und Switch (Schicht-2)

- Kollisionen beeinträchtigen die Übertragungsleistung im Netzwerk (im Ethernet ab 50 % Auslastung "spürbar").
- Lösung: Reduktion der Systeme in einer Kollisiondomäne auf (idealerweise) 2 mit Hilfe von Bridges bzw. Switches.
  - Bridge/Switch leitet Daten nur an das Interface, an das das Ziel der Kommunikation (auf Basis Ziel-MAC-Adresse) angeschlossen ist.
- Bridge vs. Switch
  - Bridge: Nur zwei Anschlüsse, kann versch. Schicht-2-Technologien (z. B. Ethernet und WLAN) verbinden.
  - Switch: 4/8/16/24/48/... Anschlüsse, verbindet Netze mit gleicher Schicht-2 aber ev. unterschiedlicher Schicht-1-Technologie (10/100/1000 Mbps, ...).



Full-Switched Ethernet

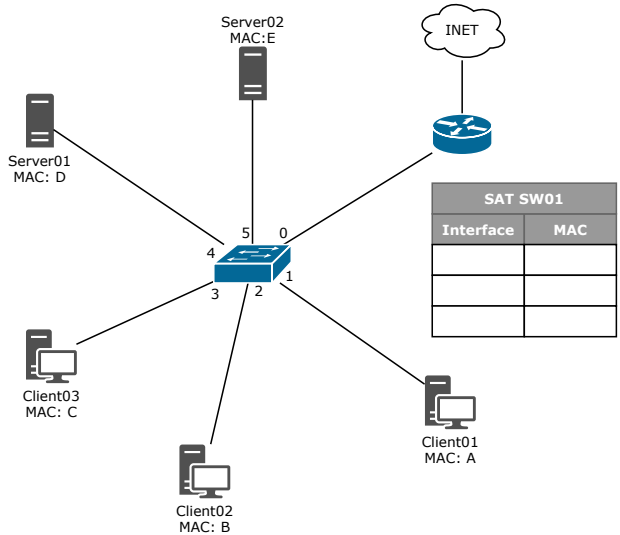
- Full Switched Ethernet: pro Switch Interface ist ein Systeme angeschlossen (1:1).
  - → gleichzeitiges Senden und Empfangen möglich (Full-Duplex).
  - → keine Kollisionen → keine Medienzugriffssteuerung notwendig.
- Vorgehen eines Switches beim Empfang eines Frames
  1. Learning: Prüfung, ob es zur Quell-MAC-Adresse einen Eintrag in der Source Address Table (SAT, auch: MAC [Address] Table) gibt. Wenn nicht, wird ein Eintrag angelegt (`<VLAN (opt.)>`, `<Switch-IF>`, `<Quell-MAC-Adresse>`).
  2. Forwarding: Prüfung, ob es zur Ziel-MAC-Adresse und zum VLAN (opt.) einen Eintrag in der SAT gibt. JA → Weiterleitung über das damit assoziierte Interface (`<Switch-IF>`), NEIN → Flooding.
- Die SAT ist speicher-begrenzt (typisch: 8k Einträge = Anzahl der möglichen Geräte im Ethernet), Einträge haben eine begrenzte Lebenszeit (typisch: 300 s).

Source Address Table (SAT) Beispiel

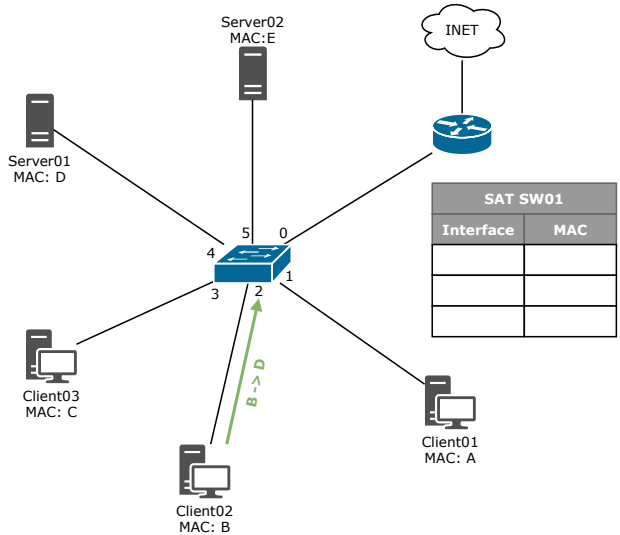
```
SW01#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
[...]
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
 100    009b.2fd4.3492    DYNAMIC     Gi0/1
 100    005c.3f3c.c8b4    DYNAMIC     Gi0/12
 100    00a1.be05.5c65    DYNAMIC     Gi0/5
 100    001e.2bcf.832d    DYNAMIC     Gi0/4
 100    0012.10df.ddd5    DYNAMIC     Gi0/22
 120    0017.c9b7.3de9    DYNAMIC     Gi0/1
 120    0012.4ed8.d008    DYNAMIC     Gi0/1
 120    0014.96c4.efde    DYNAMIC     Gi0/8
 300    0015.289a.bee0    DYNAMIC     Gi0/2
 300    001c.b9c0.91cb    DYNAMIC     Gi0/27
 430    0017.ce17.c579    DYNAMIC     Gi0/1
 430    001c.4871.dbb9    DYNAMIC     Gi0/21
 430    0019.8e0e.8560    DYNAMIC     Gi0/9
```

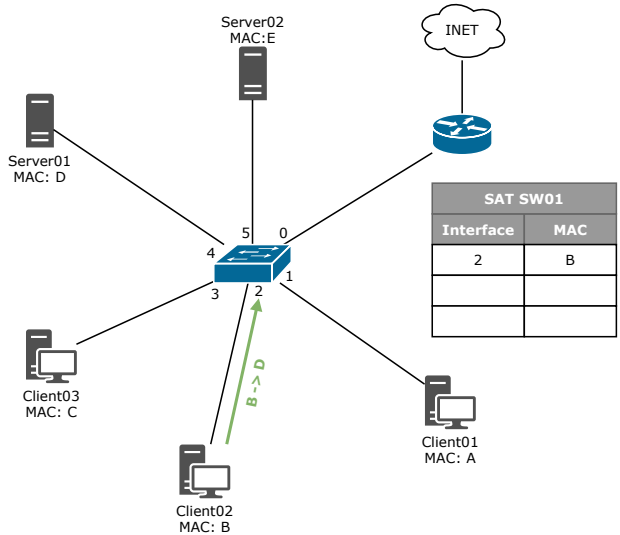
Switch Learning & Forwarding Beispiel I



Switch Learning & Forwarding Beispiel II

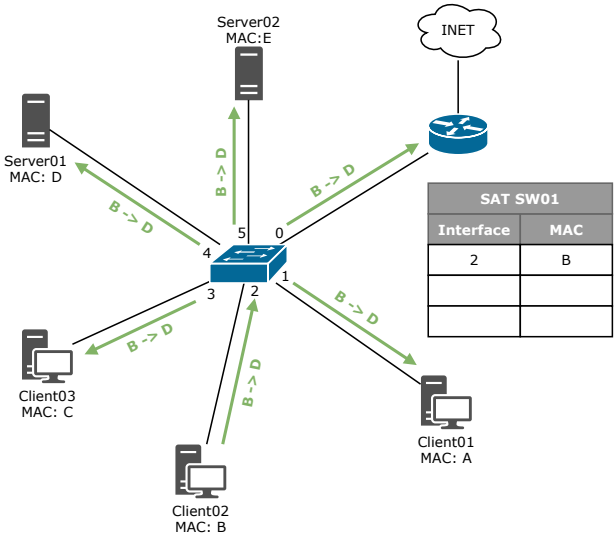


Switch Learning & Forwarding Beispiel III

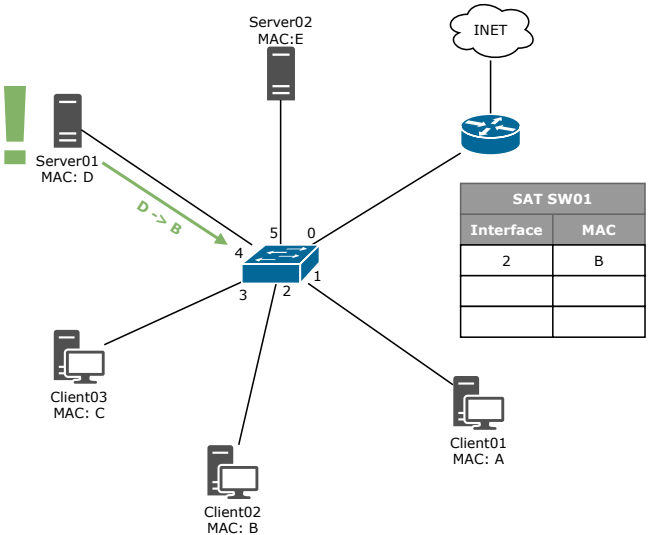


SAT SW01	
Interface	MAC
2	B

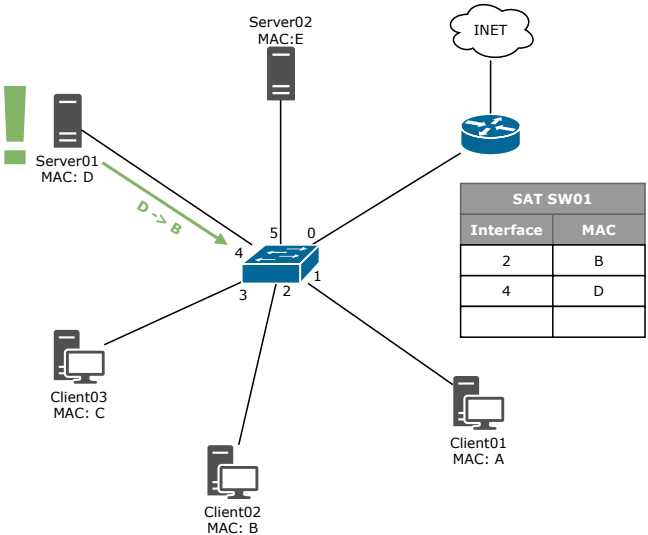
Switch Learning & Forwarding Beispiel IV



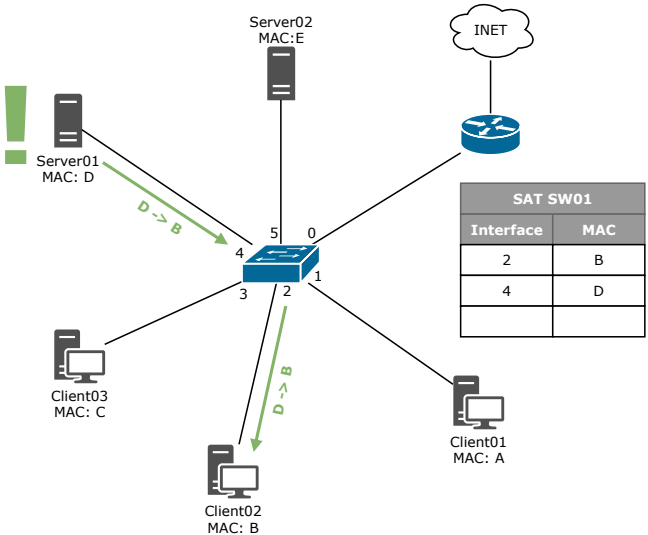
Switch Learning & Forwarding Beispiel V



Switch Learning & Forwarding Beispiel VI



Switch Learning & Forwarding Beispiel VII



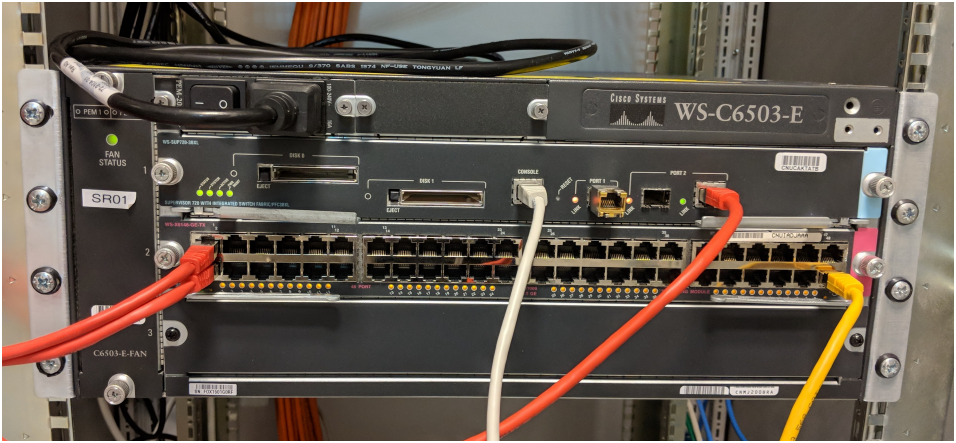
SAT SW01	
Interface	MAC
2	B
4	D

Switches Leistungskriterien

- Art der Interfaces (fix vs. modular[2], Twisted Pair vs. Fiber, ...).
- Anzahl der Interfaces (Anschlussdichte).
- Geschwindigkeit der Interfaces (10, 100, 1000 Mbps, 2.5, 5, 10, 25, 40, ... Gbps).
- Geschwindigkeit Switch Backplane/Fabric (ideal $>$ Anzahl Interfaces $\cdot$ max. Geschwindigkeit der Interfaces $\cdot$ 2 (Full-Duplex)).
- Modularität, Stackable.
- Konfigurierbarkeit (manageable, unmanageable).
- Features über L2 Switching hinaus (z. B. Port Security, IEEE 802.1X, Link Aggregation, VLANs, Layer 3 Routing [$\rightarrow$ Layer 3 Switches], ...).

[2] Small Form-Factor Pluggable: SFP, SFP+, QSFP, SFP28, QSFP+, QSFP28, QSFP28-DD

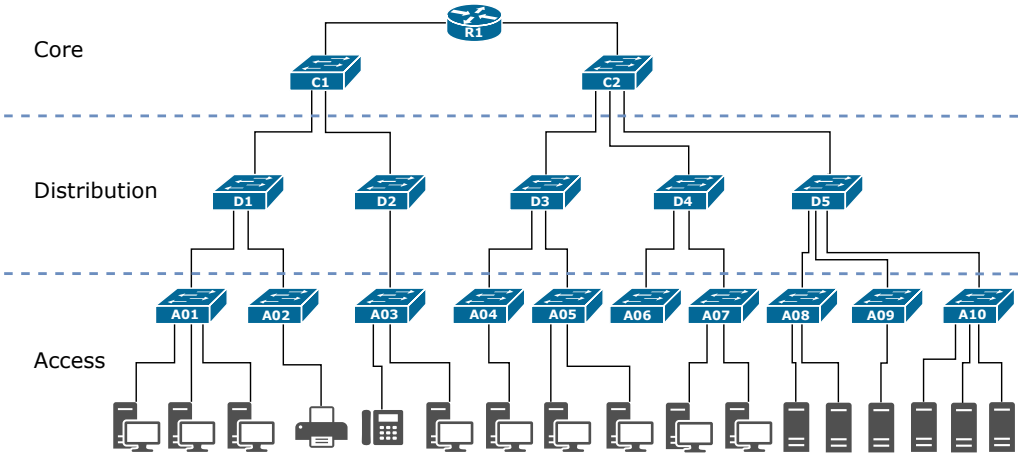
Beispiel Cisco WS-C6503



UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

Beispiel Cisco WS-C2960X-48TS-L

Switching Hierarchie



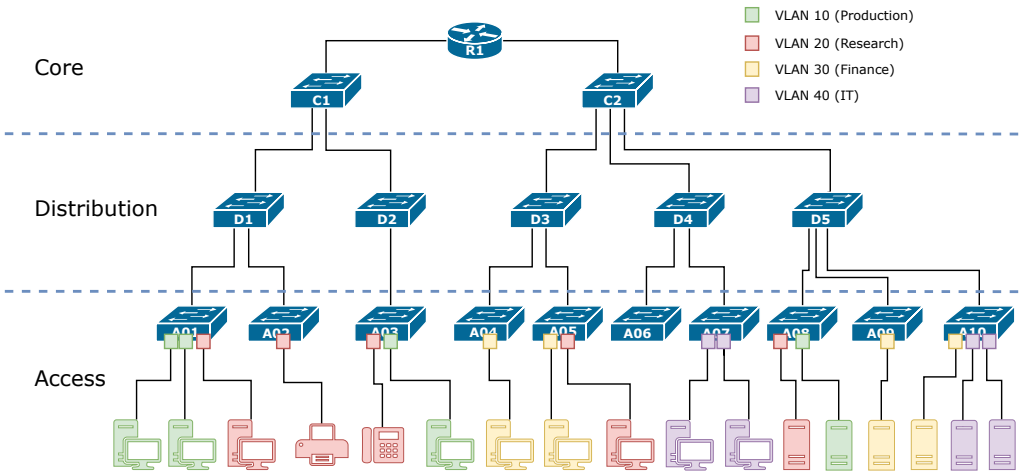
Virtual LANs (VLANs)

- VLAN = Virtual LAN = Menge von Ports an einem oder mehreren Switches.
- Kennzeichnung über eine ID (VLAN-ID, 12 Bit, theoretisch $2^{12} = 4096$ VLANs).
- Zweck: Aufteilung eines physischen Netzes (ein physischer Switch) in mehrere logische Netze (mehrere logische Switche).
- Vorteile:
  - Trennung der physischen Realisierung von der logischen Organisation (z. B. nach organisatorischen Gesichtspunkten) des Netzwerks.
  - Effizientere und flexiblere Nutzung von Switch-Ressourcen.
  - Verbesserung der Sicherheit durch Segmentierung von unterschiedlichen Netzbereichen (z.B. Trennung von Verwaltungsnetz und Labornetzen an der FH).
  - Bessere Performance durch Segmentierung in unterschiedliche Broadcast Domains.
- Static/Port-based VLANs und Tagged VLANs (IEEE 802.1Q).

Static/Port-based VLANs I

- Fixe (Statische) Zuordnung von Switch Interfaces in VLANs (nur ein VLAN pro Interface möglich).
  - Innerhalb von VLANs wird Datenverkehr geswitched (Schicht 2).
  - Zwischen VLANs muss der Datenverkehr geroutet werden (Schicht 3).
- Praktisch wird damit die gleiche Wirkung erzielt, wie wenn für jedes VLAN ein eigener, physischer Switch verwendet werden würde.

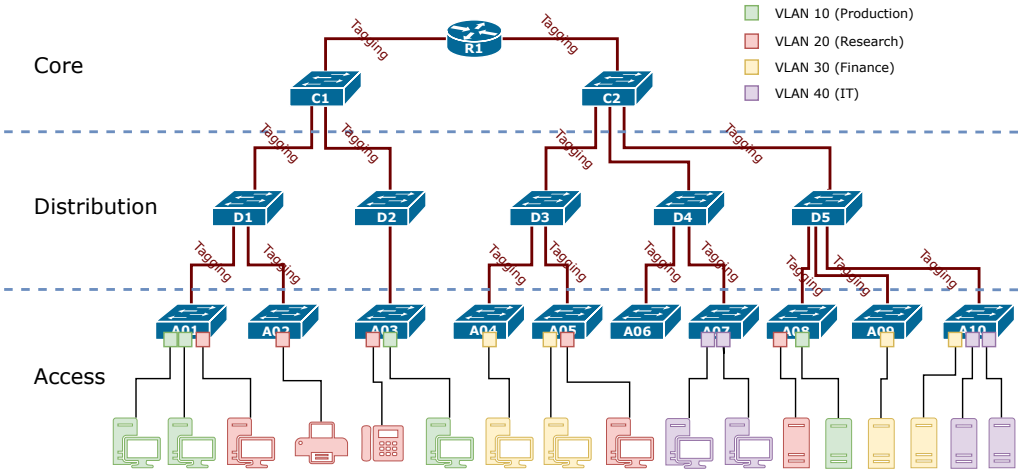
Static/Port-based VLANs II



Tagged VLANs I

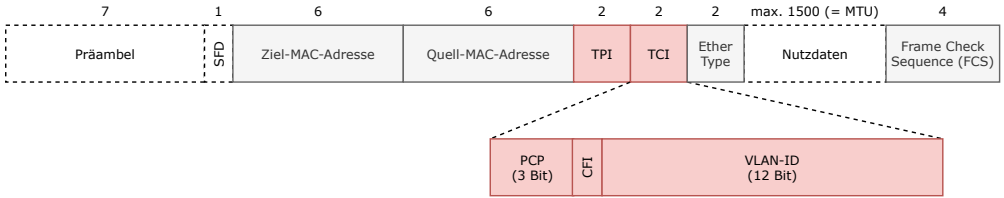
- Problem: Was tun, wenn ein Switch Interface zu mehreren VLANs gehören müsste?
  - z. B. Distribution Switch, der mehrere VLANs über mehrerer Access Switches verbinden soll.
- Lösung: Klassifizierung des Inter-Switch Datenverkehrs mittels eines Tags (Tagged VLAN).
  - Frames werden mit einem Tag (VLAN ID) entsprechend ihrer Zugehörigkeit zu einem VLAN versehen.
  - Getaggte Frames dürfen nur innerhalbt ihres VLANs weitergeleitet werden.
- Standard: IEEE 802.1Q (Begriffe Cisco: Trunking, VLAN Trunk)

Tagged VLANs II



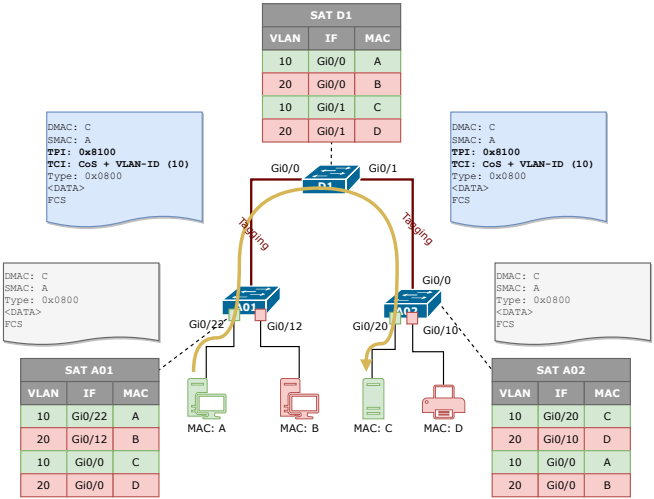
Tagged VLANs III

- Ethernet Frame Format mit IEEE 802.1Q Tagging:

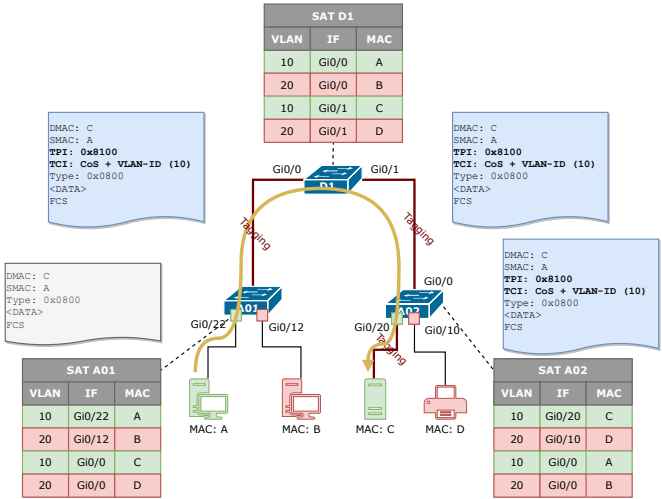


- Tag Protocol Identifier (TPI): 0x8100 für IEEE 802.1Q
- Priority Code Point (PCP): Priorisierungsmöglichkeit auf Basis IEEE 802.1p Class of Service
- VLAN-ID: 12 Bit (0 und FFF reserviert $\rightarrow$ 1 - 4094)

Tagged VLANs IV



Tagged VLANs V (Virtualisierungsserver)



Tagged VLANs VI

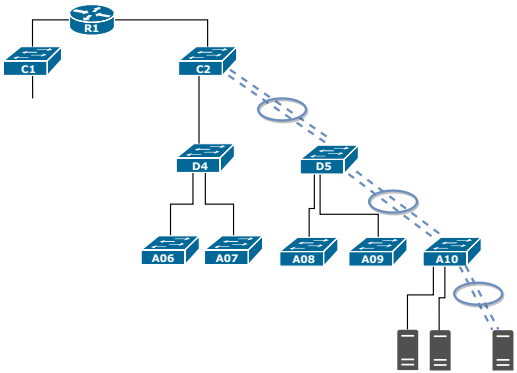
- Die Zuordnung eines Ports zu einem VLAN kann nicht nur statisch (konfiguriert durch den Administrator) sondern auch dynamisch erfolgen.
- Anwendung: Shared Office/Desk Szenarien
- Mögliche Kriterien:
  - MAC Adresse
  - Entity Authentication (Nutzer, System) (IEEE 802.1X)
  - Policy Compliance (Network Access Control [NAC] Systeme)

Power over Ethernet (PoE)

- Stromversorgung von leichtgewichtigen (= geringe Leistungsaufnahme) Endgeräten (z.B. Telefone, WLAN Access Points, Webcams, ...) über das Netzwerkkabel (Twisted Pair).
- Vorteil: Keine eigene Stromversorgung bei den Endgeräten notwendig (nur Datenkabel); einfachere Realisierung einer unterbrechungsfreien Stromversorgung (USV).
- IEEE 802.3af PoE: für (Fast) Ethernet, max. 175 mA Strom pro Ader, 15,4 W Leistungsaufnahme pro Switch Port ($\approx$ 13 W kommen wirklich an, tw. 30 W herstellerspezifisch erlaubt)
- IEEE 802.3at PoE+: für Gigabit Ethernet, max. 360 mA Strom pro Ader, 60 W Leistungsaufnahme pro Switch Port ($\approx$ 50 W kommen wirklich an).

Link Aggregation

- Standard: IEEE 802.1AX
- Bündelung mehrer physischer Interfaces zu einem logischen.
- Zweck: Erhöhung Datenraten, Ausfallssicherheit
- Auch für Endsysteme (z. B. Server) möglich.
- Herstellertechnologien (tw. $\neq$ IEEE 802.1AX), z. B.
  - Cisco: Etherchannel
  - Huawei: EtherTrunk
  - Linux: Bonding



UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA