Notizen zu CompTIA Network+

ISO-OSI-Schichtmodell:

OSI-Schicht		Ebene	Beispiel-Protokolle und Verfahren	Einheiten	Hardware
7	Application	Application	HTTP, FTP, SMTP	Data	Gateways (Protokoll-Umwandler)
6	Presentation		ASCII, MP3, Encryption		
5	Session		NetBIOS		
4	Transport	Network	TCP, UDP	Segment	
3	Network		IP, ICMP, IGMP	Packet	Router, Layer-3-Switch
2	Data Link		Ethernet, Frame Relay, ARP	Frames	Switch, Bridge
1	Physical			Bits	Repeater, Hub

Strukturierte Verkabelung (Universelle Gebäudeverkabelung):
- Standards: ISO/IEC 11801:2002 und TIA/EIA 568
- Europa-Norm: EN 50173-1 für "Anwendungsneutrale Kommunikationskabelanlagen

Primärbereich:
- Anbindung des Standortes an andere Standorte oder das Internet
- Verbindung zwischen einzelnen Gebäuden
- fast ausschließlich Glasfaser-Spezifikationen (LWL) im Einsatz

Sekundärbereich:
- vertikale Gebäudeverkabelung (Steigbereich zwischen Gebäudeverteiler und Stockwerkverteiler)
- LWL oder S/STP, S/FTP (auf jeden Fall TwistedPair)

Tertiärbereich:
- horizontale Stockwerk-Verkabelung ("Etagenverkabelung")
- zwischen Patchpanel und Einzelsteckdosen

Netzwerk-Hardware:

Hubs/Repeater:
- einfache Layer-1 Signalweitergabe ohne eigene Logik (aber ggf. inkl. Aufarbeitung/Verstärkung)
- physisch: Stern-Topologie; logisch: Bus-Topologie

Bridges:
- Bridges arbeiten - wie Switches - auf dem Data Link Layer (Layer-2)
- schirmen **Kollisionsdomänen** (auf MAC-Adressen basierend) voneinander ab, wenn die Ziel-MAC-Adresse in der gleichen Kollisionsdomäne wie die Quell-MAC-Adresse liegt.
- bei unbekannten MAC-Adressen leitet die Bridge die Frames der Quell-MAC-Adresse an alle Ports an, an der die Kollisionsdomäne des Absenders nicht anliegt und speichert den Absender am

entsprechenden "Quell"-Port
- je kleiner die **Kollisionsdomänen** sind, desto besser funktioniert die Kommunikation!

Switches:
- MAC-Adresstabelle für jeden Port, d.h. jedes Endgerät ist eine "Kollisionsdomäne"
- ein Switch ist eine "Multi-Port-Bridge", ggf. mit weiteren Zusatzfunktionen

Medienkonverter:
- vermitteln zwischen verschiedenen Layer-1-Anschlüssen, z.B. SFP-Ports 100BaseTX <=> T=TwistedPair/RJ45, TwistedPair/RJ45 1000BaseSX <=> GBICs Short Range Fiber, TwistedPair/RJ45 1000BaseLX <=> SFP Long Range Fiber)
- bieten für das Medium die entsprechenden Spezifikationen (Stecker-Form, Signaleinspeisung)
- typische Medienkonverter: GBIC (Gigabit Interface Converter) - älter, SFP (Small Form-Factor Pluggable) - aktuell

Modem (Modulation - Demodulation):
- Wählmodem
- Telefon-Modem (POTS !)
- Faxmodem (POTS-Modem inkl. Faxprotokoll)
- DSL-Modem
- Kabelmodem
- Funk-Modem, SAT-Modem

Multiplexer/Demultiplexer:
- fasst mehrere Signale zusammen und überträgt sie simultan über ein Medium (z.B. Glasfaser, Funk...) - OSI-Layer 1 (Physical Layer)
- ermöglichen die Unterscheidung verschiedener Eingangssignale
- verschiedene Multiplexing-Verfahren: z.B. Wellenlängen-Multiplexing, Zeit-Multiplexing, Frequenz-Multiplexing
- auch bei WDM (Wavelength Division Multiplexing): DWDM (Dense WDM) - momentan leistungsfähigste Übertragung bis 160 GB pro Farbfrequenz-Kanal, CWDM (Coarse WDM) - weniger Kanäle, geringere Bandbreite (8 Farben/ 8 Kanäle, deutlich geringere Datenübertragungsrate)
- Multiplexer sind wie Drehschalter - jedes Signal kann isoliert betrachtet werden

Router:
- unterteilt Netzwerke in logische Segmente (**Broadcast-Domänen**)
- Router arbeiten auf OSI-Layer 3 (Network Layer)
- Router entscheiden anhand der IP-Adressen über die Weiterleitung
- dienen als Kopplungselemente zwischen z.B. dem lokalen Netzwerk und dem Internet
- können ebenso auch Netzwerk-Segmente innerhalb eines Standortes unterteilen
- begrenzt ebenso auf OSI-Layer 2 (Data Link Layer) **Kollisionsdomänen**
- d.h. Router begrenzen den Broadcast sowohl auf **Kollisionsdomänen** (Layer 2 Broadcast: FF:FF:FF:FF:FF:FF) als auch auf **Broadcast-Domänen** (Layer 3 Broadcast: 255.255.255.255)

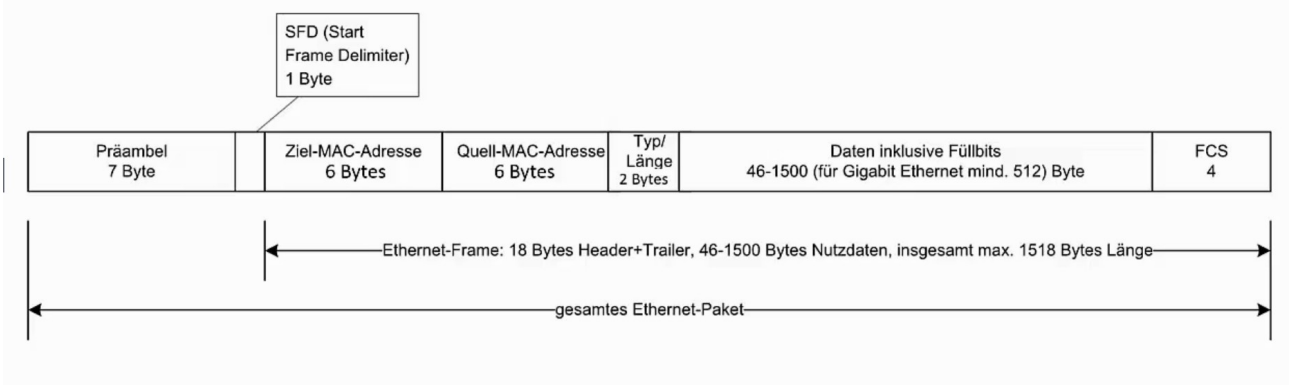
Ethernet und Switching:

802.3: CSMA/CD
- weitere LAN-Technologien der IEEE-Arbeitsgruppe 802: 802.4 - Token Bus, 802.5 - Token Ring
- basiert auf einer logischen Bus-Topologie

- kein zentraler Steuerungsmechanismus
- es wird kein Token ("Daten-Körbchen") verwendet
- steht für Carrier Sense Multiple Access with Collision Detection: alle Knoten lauschen auf einem geteilten Medium (Bus); Knoten senden, wenn gerade kein Betrieb ist; Knoten bemerken, wenn eine Kollision auftritt und sehen ein Jam-Signal aus; Knoten warten Zufallszeit (Backoff Time) ab, um anschließend erneut zu senden
- deswegen: CSMA/CD ist umso performanter, je weniger Hosts/Knoten im Segment vorhanden sind (!!!)
- ist nicht der einzige Ansatz von Ethernet (!!!)

Half-Duplex:
- Half-Duplex: Systeme können entweder senden oder empfangen, jedoch nicht beides gleichzeitig
- dadurch reduziert sich die Effektivität und die Wahrscheinlichkeit von Kollisionen erhöht sich
- Hubs können "von Natur aus" nur Half-Duplex
Full-Duplex:
- Full-Duplex: ermöglicht das gleichzeitige Senden und Empfangen - und damit die vollständige Eliminierung sämtlicher Kollisionen!
- die angeschlossenen Stationen/Knoten benötigen KEIN CSMA/CD mehr!
- effektive Übertragungsrate: bei 100Base-TX sind das 200 Mbit/s, da gleichzeitig 100Mbit/s gesendet und weitere 100 Mbit/s empfangen werden können
- bei 10Base-T und 100Base-TX mussten die Knoten das Half- oder Full-Duplex aushandeln, der heutige Standard 1000Base-T unterstützt ausschließlich Full-Duplex
- Ethernet: 10 Mbit/s-Standard, Fast-Ethernet: 100 Mbit/s-Standard, Gigabit-Ethernet: 1000 Mbit/s-Standard, 10-Gigabit-Ethernet: 10 Gbit/s-Standard

Der Ethernet-Frame:
direkt vergleichbar mit der MTU (Maximum Transmission Unit) = Maximallänge eines IP-Paketes



Die MAC-Adresstabelle:
- *# show mac address-table dynamic* zeigt auf Cisco-Systemen die dynamisch zugeordneten NIC-MAC-Adressen je Port
- *# show mac address-table aging-time* zeigt die globale Lease-Time der dynamischen Zuordnungen

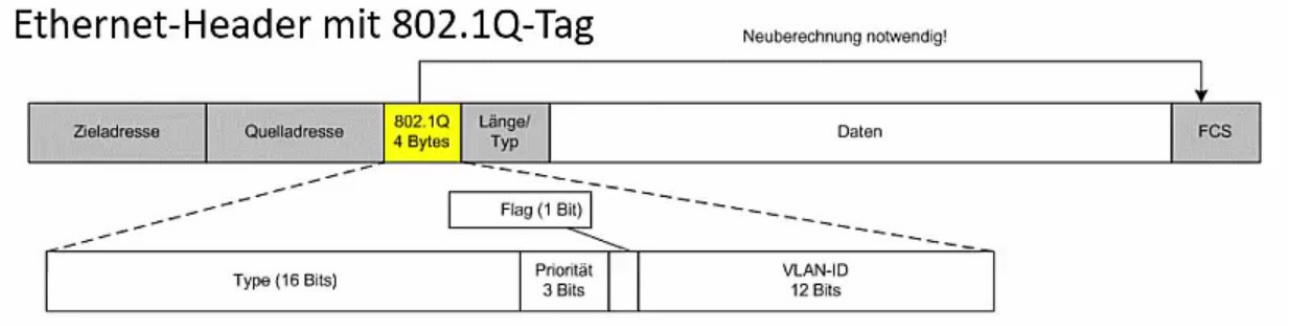
VLAN: Virtuelle LANs
- jedes VLAN entspricht einer Broadcast-Domäne
- jedes VLAN entspricht logisch einem virtuellen Switch (z.B. im physischen Switch)
- Schutzmechanismus: Separation durch Subnetze, Abschottung von Netzsegmenten!
- Optimierung der Bandbreite: Performance durch kleinere Broadcast-Domänen

- Flexibilität: Umzug von Knoten/Geräten in VLANs einfach
- Delegation: Administration durch verschiedene Admins möglich

Cisco:
- *# show vlan brief* (*# sh vl br*): Liste der konfigurierten VLANs inkl. Port-Zuordnung
- *# show interfaces status* (*# sh int status*): Liste aller Ports inkl. VLAN-Zuordnungen, Duplex-Mode, Speed, Type
- Konfigurationsmodus („global config mode“): *# configure terminal* (*# conf t*)
- anschl. Sub-Konfigurationsmodus z.B.: *# interface Gi0/1* (*# int g0/1*)
- anschl. Zuordnung zu VLAN 10: *# switchport access vlan 10; # end*

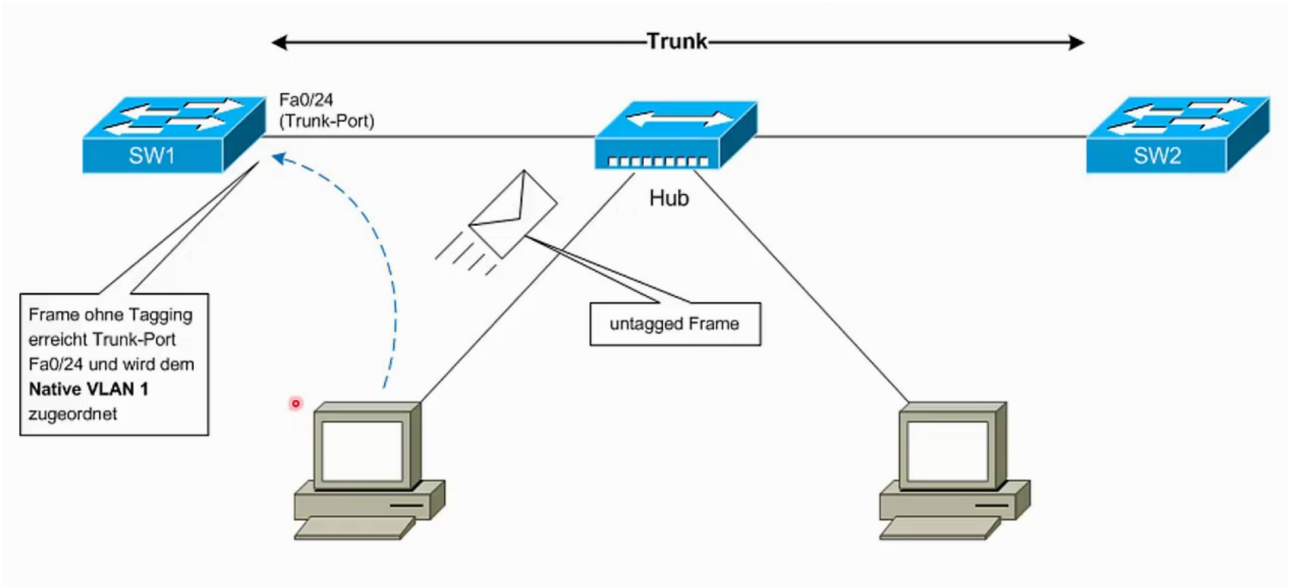
VLAN-Trunking und Tagging:

- zwischen Switchen z.B. auf verschiedenen Etagen können VLAN-Informationen im Uplink übertragen werden (Technologie: *IEEE 802.1Q – „VLAN-Tagging“*):



- die Uplink-Ports (Ports zur Verbindung zwischen den Switchen) werden als *tagged ports* bezeichnet, die Ports für Endgeräte sind *untagged ports* (die VLAN-Informationen sind hier bereits entfernt)
- bei Cisco wird dieses Verfahren als *Trunking* bezeichnet und der Uplink *Trunk* genannt

Native-VLAN:
- Endgeräte verwerfen Frames mit 802.1Q-Tags
- Fallback-Mechanismus: Frames ohne Tagging werden vom Switch dem Native-VLAN zugeordnet, um zugestellt werden zu können



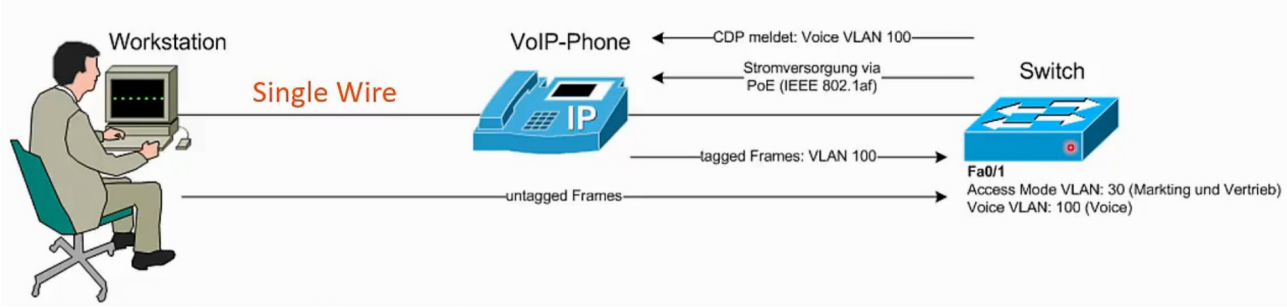
(Dieser Aufbau ist tunlichst zu vermeiden! Zwischen Trunk-Ports sollte nur ein Uplink-Kabel sein!)

Cisco-Praxis Trunk / Uplink:
- *CDP* - Cisco Discovery Protocoll: *# show cdp neighbor*
- *# conf t => # int g0/21 => # switchport mode ? => # switchport mode trunk => # end*
- falls noch festgelegt werden muss, welches Tagging-Protokoll verwendet werden soll (z.B. bei Fehler 'Command rejected: An interface whose trunk encapsulation is „Auto" can not be configured to „trunk" mode'): *# switchport trunk encapsulation ? => # switchport trunk encapsulation dot1q*
- überprüfen: *# show interface trunk* (802.1q encapsulation)
- **beachten:** Citrix *Native-VLAN* umstellen von (default) 1 auf z.B. 10

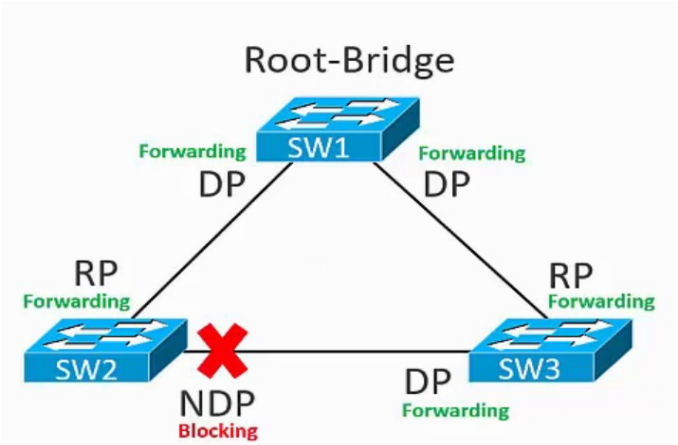
Power over Ethernet und das Voice-VLAN:

- im Switch konfiguriert: Voice VLAN 100 (Voice), Access Mode VLAN 30 (Marketing, Vertrieb)
- bei Cisco: VoIP-Phone meldet sich beim Switch, CDP (Cisco Discovery Protocol) meldet dem VoIP-Phone das passende VLAN: Voice VLAN 100
- VoIP-Phone: Stromversorgung via PoE (IEEE 802.1af)
- „Mini-Switch" im VoIP sended und empfängt tagged frames: VLAN 100
- bei über VoIP-Phone per Ethernet angeschlossenen PC leitet der „Mini-Switch" die VLAN 30-frames untagged weiter zum PC

Konfiguration bei Cisco, z.B. am Port *Fa0/1*:
SW1(config-ig)# switchport access vlan 30
SW1(config-ig)# switchport voice vlan 100



Das Spanning Tree Protocol (STP)
von Frau Radia Perlman, Oracle



- bei redundant verbundenen Switches
- durch redundante Wege können duplizierte Frames, MAC-Address-Flapping und Broadcast-Stürme (mit unendlicher TTL) entstehen
- Einsatz von STP (IEEE 802.1D) sorgt für eindeutigen Pfad in einer redundanten Switch-Struktur:
- zwischen den Switches werden Informationen über *Bridge Paket Data Units (BPDUs)* ausgetauscht (es gab damals noch keine Switches, nur Bridges – der Name ist geblieben!)
- jeder Uplink-Port (= Trunk-Port) wechselt entweder in den Zustand *Forwarding* oder *Blocking* (bzw. *Discarding* beim **Rapid Spanning Tree Protocol**) nach folgendem komplexen **STP-Algorithmus** (nur Grundstruktur)**:**
- Wahl der *Root-Bridge* (niedrigste Bridge-ID: Priorität+MAC)

- Ermittlung der *Root-Ports*: bester Weg zur *Root-Bridge*
- Ermittlung des *Designated Ports* für jedes Segment (*Forwarding*)
- Ermittlung der schlechteren, redundanten Wege: *Non-Designated Ports* (*Blocking*)
- Weiterentwicklung: **RSTP** (Rapid Spanning Tree Protocol: IEEE 802.1w) schnellere Konvergenz bei Abbruch einer Verbindung, *Root-Ports*, *Designated* und *Non-designated Ports* werden wesentlich schneller als bei STP erneut zugewiesen („das Netzwerk repariert sich selbst“ - (ca. 50sek. bei STP > ca. 1sek. bei RSTP)

[zu IEEE 802.1D => IEEE 802.1w:
Großbuchstaben – eigener Standard, Kleinbuchstaben – abgeleiteter, weiterentwickelter Standard]

Grundlagen Switch-Port Security:

ermöglicht die Kontrolle der Absender-MAC-Adressen eingehender Frames:
- die Anzahl maximal gleichzeitig kommunizierender MAC-Adressen
- welche MAC-Adressen über den Port kommunizieren dürfen
- welche Maßnahmen ergriffen werden, wenn eine Richtlinie verletzt wird (z.B. Port deaktivieren, Frame verwerfen)

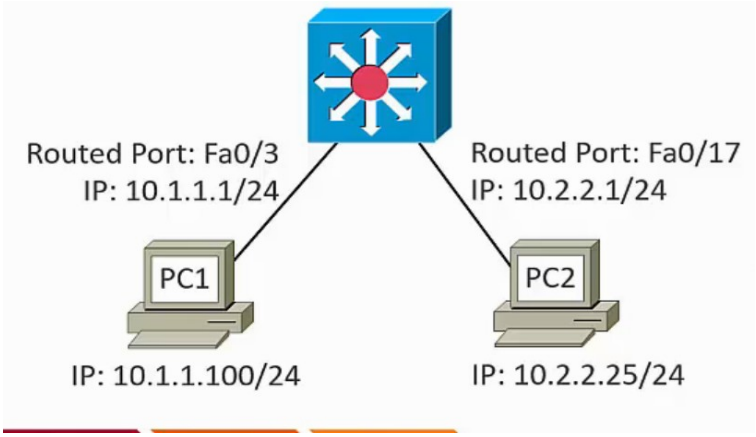
Konfiguration bei Cisco-Switches:
SW1# show int status
SW1# show run int gi0/13 (laufende Konfiguration des Ports GI0/13)
SW1# conf t (globaler Konfig-Modus)
SW1(config)# int g0/13 (Port anwählen)
SW1(config-if)# switchport mode access (damit Port-Security funktioniert)
SW1(config-if)# switchport port-security
SW1(config-if)# end
--------- Anzeige der Port-Security Konfiguration ---------
SW1# show port-security (alle Ports)
SW1# show port-security int g0/13 (detaillierte Ansicht für einen Port)
SW1# conf t
SW1(config)# int g0/13
SW1(config-if)# switchport port-security mac-address ?
SW1(config-if)# switchport port-security mac-address sticky (schreibt die erste(n) MAC-Adressen in die Konfiguration, Anzahl je nach vorher freigegebener Anzahl maximaler MAC-Adressen)
SW1(config-if)# end
SW1# show run int gi0/13 (Überprüfen der MAC-Adresseintragungen)
bei Regelverstoß:
SW1# show int status (zeigt *err-disabled* beim entsprechenden Port)
SW1# show port-security int g0/13 (detaillierte Ansicht für gesperrten Port)
SW1# conf t
SW1(config)# int g0/13
SW1(config-if)# switchport port-security maximum 2 (da noch im sticky-Mode kann automatisch eine weitere MAC-Adresse zur bisher einzigen erlaubten hinzu gefügt werden)
SW1(config-if)# no shutdown
SW1(config-if)# do show int status (*do* wegen aktivem Sub-Konfig-Modus) => Port noch disabled!
SW1(config-if)# shutdown
SW1(config-if)# no shutdown
SW1(config-if)# do sh run int g0/13 status => Port enabled (detail. Ansicht inkl. 2. MAC-Adresse)!

SW1(config-if)# switchport port-security violation ?
SW1(config-if)# switchport port-security violation restrict (ignoriert nicht erlaubte Frames; vorher: shutdown schließt Port, muss manuell wieder aktiviert werden!)
SW1(config-if)# end

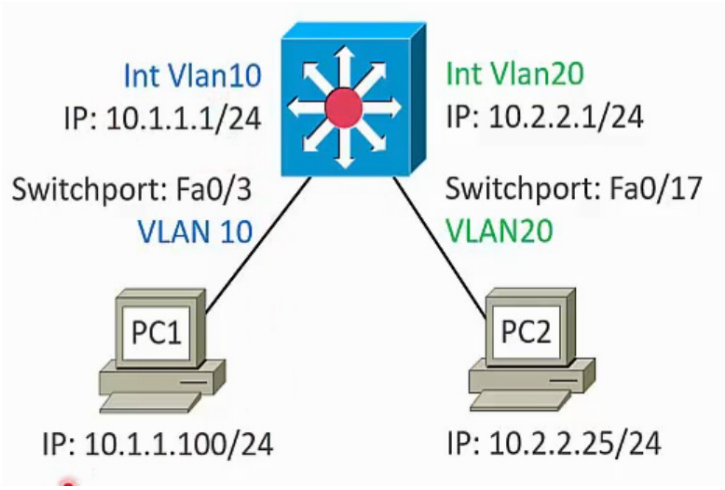
Multilayer-Switches:

- Standard-Switch: *Layer-2-Switch*, Weiterleitungsentscheidung nur nach MAC-Adressen und Ethernet-Informationen
- *Layer-3-Switch (Network Layer)*: Router in Switch-Form (Basis zusätzlich: IP und Switch kann bei Bedarf auch routen – *im LAN!*)
- Multilayer-Switches: mindestens *Layer-3-Switch*, ggf. auch Funktionen aus höheren Ebenen (z.B. Access Control Lists, QoS...)
- Vorteile: hohe Portdichte, flexibler und schneller als ein Router
- Nachteil: auf Ethernet begrenzt, nur in LAN-Strukturen einsetzbar

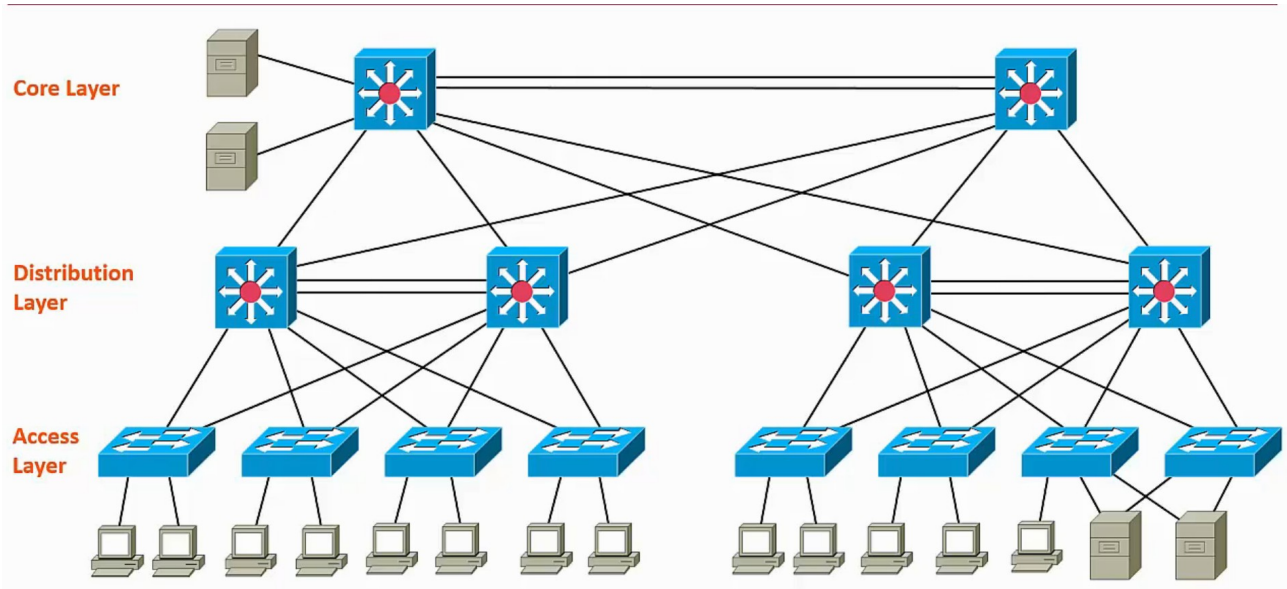
z.B.:



oder:



Best practice: Modernes Design einer Switch-Infrastruktur:



Quelle: https://www.udemy.com/course/computer-netzwerke-network (Eric Amberger)