IT-Systemengineering & -Operations

Netzwerke im Rechenzentrum

Vers. 1.0

Markus Waldmann

Lucerne University of
Applied Sciences and Arts

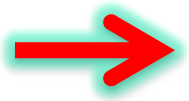
HOCHSCHULE
LUZERN

INFORMATIK

Lernziele

- Sie können die Anforderungen an ein RZ-Netzwerk definieren und erklären.
- Sie sind fähig die kritischen Punkte eines RZ-Netzwerks zu adressieren und vorbeugende Massnahmen vorzuschlagen.
- Sie kennen die grundlegenden Topologien im RZ-Netzwerk.
- Sie kennen die wichtigsten Begriffe im RZ-Netzwerkbereich.

Inhaltsübersicht



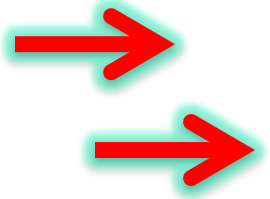
- Einführungsübung
- Technologie
  - Topologie
    - Provider – Grenze – DMZ – Netzwerk
  - Services
  - Produkte
  - Technikbegriffe
- Management
- Kosten

Einführungsübung

- Lösen sie die Einführungsaufgabe gemäss der separaten Übungsbeschreibung im ILIAS.

- Präsentation der Ergebnisse um _____ Uhr im Klassenverband

Inhaltsübersicht



- Einführungsübung
- Technologie
  - Topologie
    - Provider – Grenze – DMZ – Netzwerk
  - Services
  - Produkte
  - Technikbegriffe
- Management
- Kosten

Topologie

- Provider
  - Angebot, Speed, Technik
- Grenze
  - Router, Firewall, IDP, Redundanz
- DMZ
  - Web-Services, Authentifizierung, Dienste
- Lokales Netzwerk (LAN)
  - Topologien, Speed, Trennungen, Services

Provider

- Angebot nicht einfach zu überblicken
- Übersicht Beispiel: https://www.providerliste.ch/
- Globale, regionale, lokale Angebote
- Gemischte und Bundle-Angebote
  (Zugang, Hosting, Housing, Services, …)

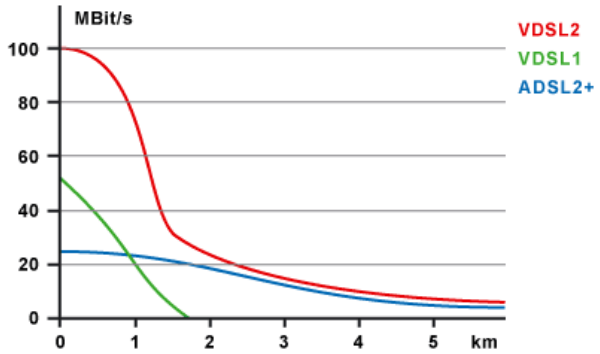
Provider Technik und Speed

- Kupferkabel (längenabhängige Leistung)
  - ADSL mit 2 – ca 16 Mbit/s

    "Asymmetric Digital Subscriber Line ", Uplink typ. 10% vom Downstream
  - VDSL mit 20 – ca. 100 Mbit/s

    "Very High Speed Digital Subscriber Line ", Uplink typisch 10% vom Down
  - SDSL mit 20 – 200 Mbit/s

    "Symmetric Digital Subscriber Line", Up- = Downstream



Quelle: http://www.elektronik-kompendium.de/sites/kom/0305237.htm

- Antennenkabel
  - Parallel zum TV Signal, 2 – 500 Mbit/s
- Glasfaser
  - Mit 10 Mbit/s – 10 Gbit/s

OTO-Dose der neuen FTTH Anschlüsse

- Richtfunk
  - Abgelegene, unerschlossene Gebiete, bis 20 Mbit/s

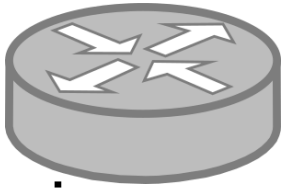
Zwischenübung

Jeder für sich oder in 2er Teams:

- Welche Anschlussmöglichkeiten/Preise haben sie bei sich zu Hause/im Betrieb bei den folgenden Anbietern:

Anbieter	**VDSL** **Ja/Nein/Speed**	**Kosten**	**SDSL** **Ja/Nein/Speed**	**Kosten**	**GLAS** **Ja/Nein/Speed**	**Kosten**
Swisscom						
Fiber7						
UPC						
WWZ						
…						

Grenze: Router



- oft in Firewall oder in Layer3-Switches integriert
- Arbeitet mit IP-Paketen, Umsetzung von öffentlichen in private Adressen (NAT/PAT)
- Anbindung von verschiedenen Netzen oder mehreren Providern (Netzwerksegmente, Speed, Topologie)
- optimale Weiterleitungen bei redundanten Leitungen oder Start von Fallback Szenarien
- Aufrechterhaltung von QOS durch spezifische Weiterleitungen (auf Grund von Pakettypen/Protokoll)
- Kann auch VPN-Endpunkt sein (Authentifizierung)
- Anpassung an unterschiedliche Netzwerktechniken (Ethernet, xDSL, PPPoE, ISDN, ATM, FDDI, …)

Grenze: Firewall

- **"A firewall is not an end-all and be-all. It has to work in tandem with endpoint management and threat analysis."**
  - ***Chris Rodriguez**, senior industry analyst, Frost & Sullivan*

- Sicherheitsbaustein, Teil des Sicherheitskonzepts
- Übernimmt meist auch Routing-Funktionen
- Regelbasierte Sperrung oder Weiterleitung von Netzwerkpaketen
  - Paketfilter, Stateful Inspection, Proxy- und Content-Filter
- VPN-Endpunkt mit Authentifizierung (lokal, Radius, AD)
- Kann auf allen OSI-Schichten arbeiten

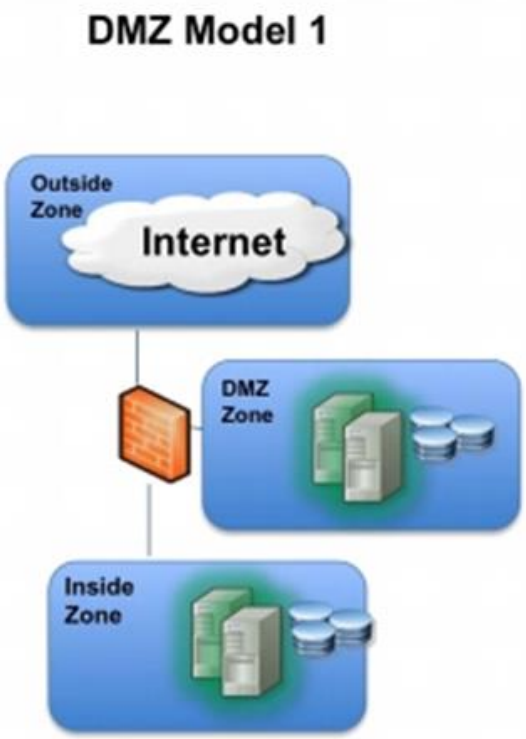
Grenze: IDP

- Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS): IDS+IPS=IDP
- Eindringversuche erkennen (Mustererkennung, DOS, Fakes, Portscan, IP-Spoofing, …)
- Rechenintensive Funktion, oft separates Device
- >= 1 Gbit/s Netzwerke sind heute an der Leistungsgrenze: Pakete müssen ev. verworfen werden, lückenhafte Überprüfung

DMZ

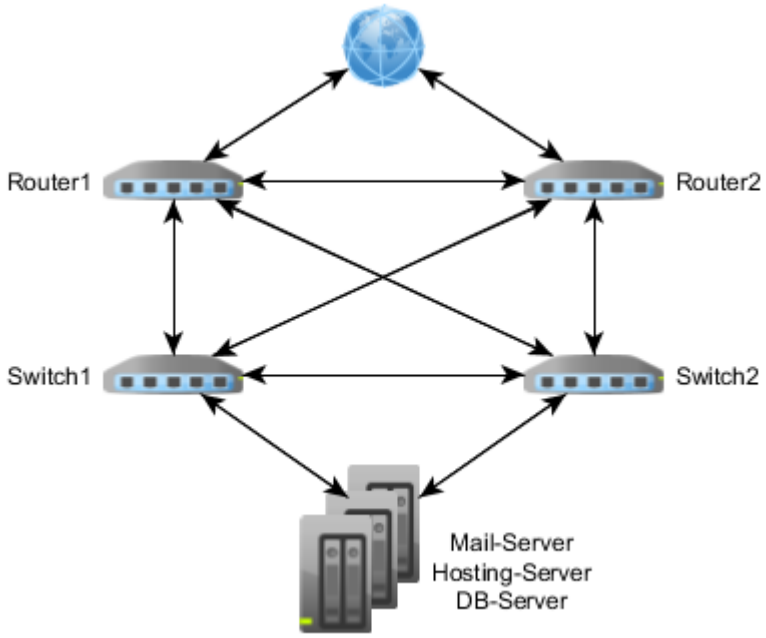
- Demilitarized Zone
- Geschützter Bereich, in welchen bestimmte Zugriffe erlaubt werden (WWW, Mail, FTP, …)
- 1 oder 2 Firewalls
- Bei 2 Schritten (DMZ Model 2) können verschiedene Hersteller und Gerätetypen verwendet werden

=> <u>höhere Sicherheit vor Hackern</u>



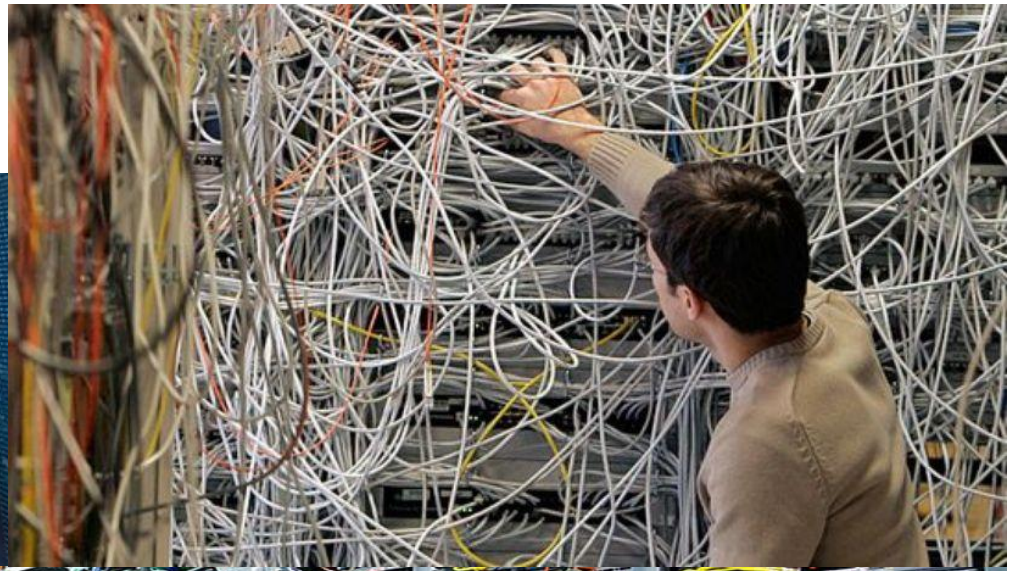
Netzwerk / Redundanz

- 1 Provider / 2 Zugänge
- 2 Provider / je 1 Zugang
- Ausfallüberwachung nötig (Router verbunden)
- Getrennte Wege/Trasse (2 Hauseinführungen)
- Ev. Verschiedene Medien
- Loadbalancing möglich

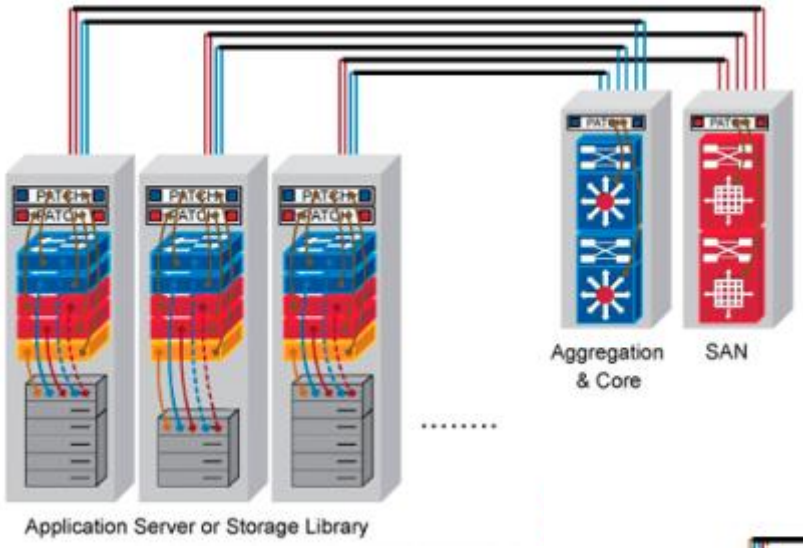


RZ LAN Topologie

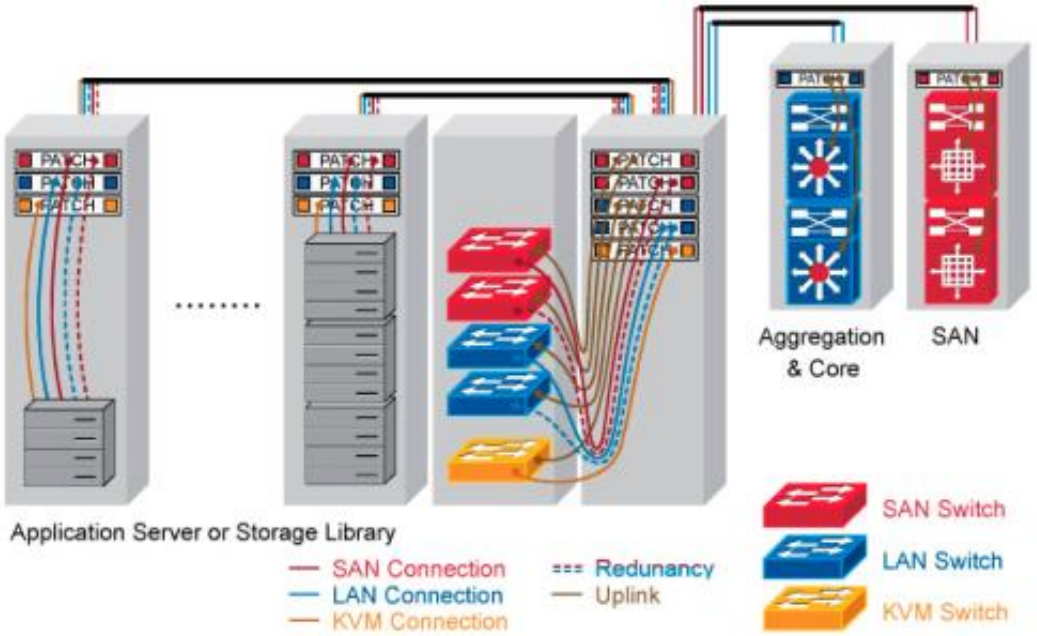
- Was darf es sein?



LAN Strukturen – Physikalisch



- TOR
  Top Of Rack: jedes Rack hat eigene Switches
- EOR
  End Of Row: Racks nur über Patchpanels verbunden



- Div. Vor- und Nachteile
  - Platz
  - Erweiterbarkeit
  - Anz. Geräte
  - Freie Ports
  - …

http://www.datacentre.matrixgn.com/data%20centre%20topologies.htm

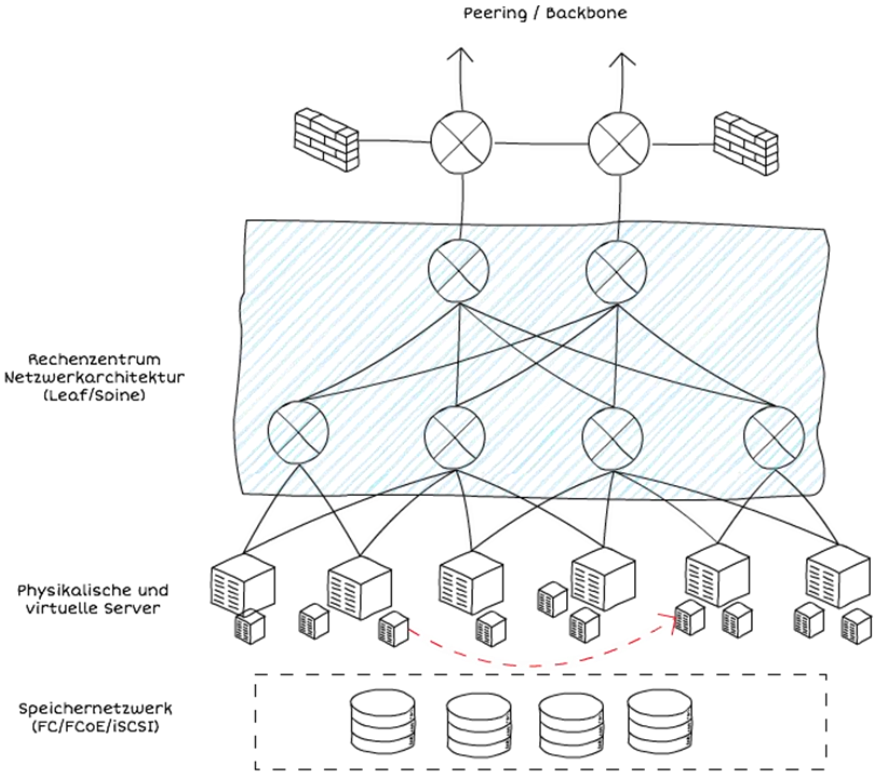
Fragen

- Welche Vor- und Nachteile sehen sie in den beiden Architekturen der letzten Folie?
  - Platzbedarf
  - Erweiterbarkeit
  - Anz. Geräte
  - Freie Ports
  - Verbindungen
  - …

LAN Strukturen - einfach

Ein einzelner Switch wird nicht reichen, es braucht verschiedene Ebenen:

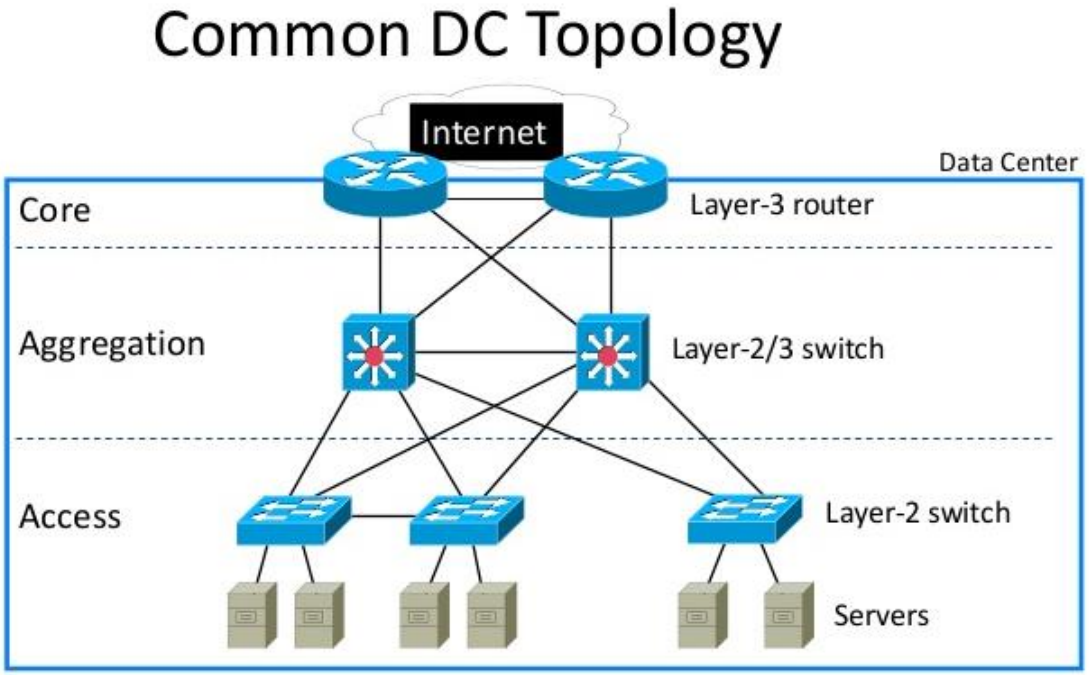
- Peering / Peripherie
  - Anschluss nach aussen
- Backbone / Spine / Core
  - Rückgrat, zentrales Netz
- Leaf
  - Anschlüsse für Server



RZ Topologie

Funktionsstufen:

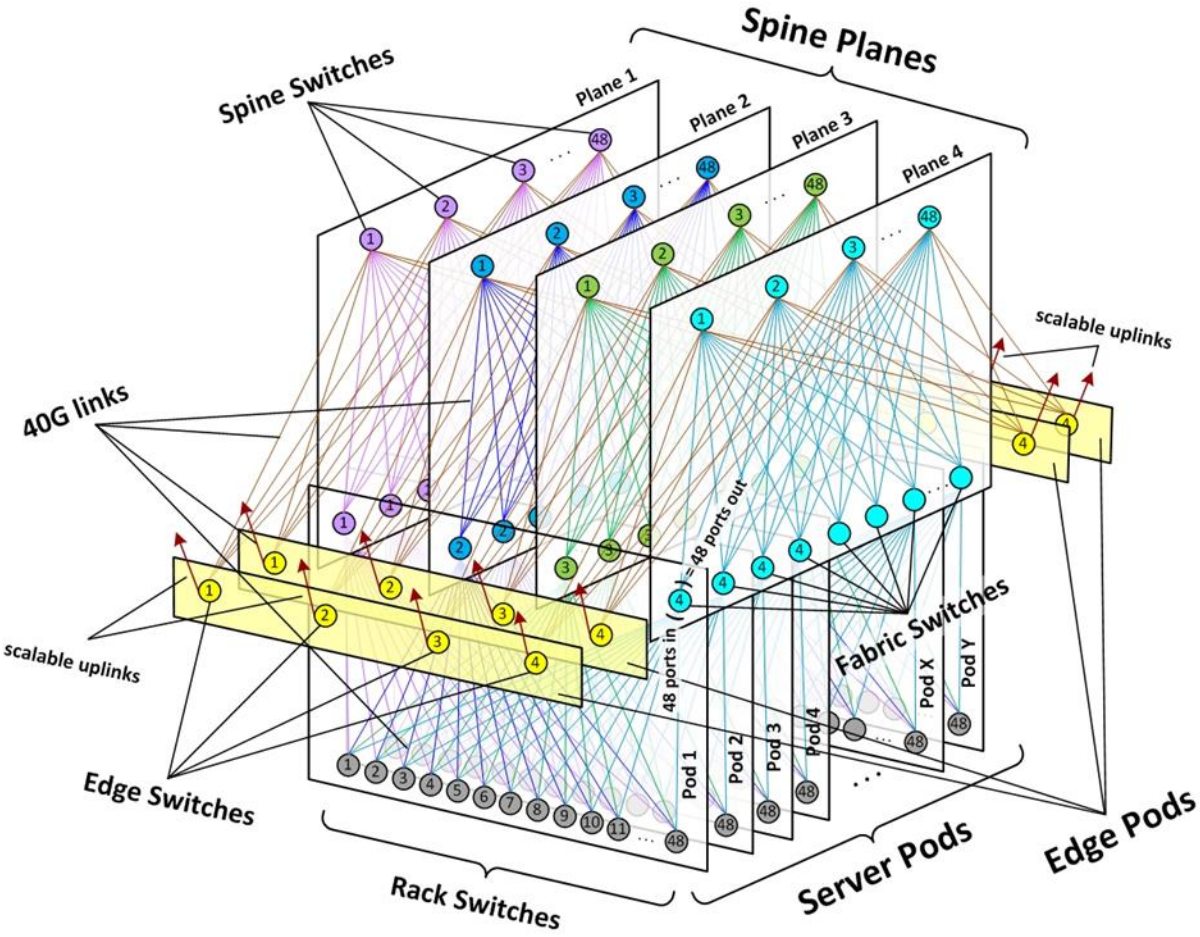
- Core
  - Zentrale Verbindungen
  - Auch RZ zu RZ
- Aggregation
  - Direkte Verbindungen von Serverfarmen
- Access
  - Zugangspunkt für physikalische Server und Komponenten



LAN Strukturen – High Perfomance

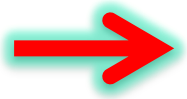
The Top:

- extremely high performance data center networking architecture example:
- Facebook's next generation DC network



https://code.facebook.com/posts/360346274145943/introducing-data-center-fabric-the-next-generation-facebook-data-center-network/

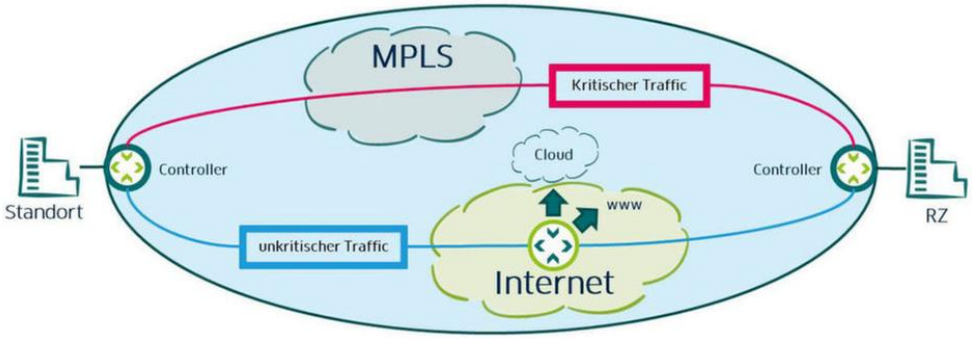
Inhaltsübersicht



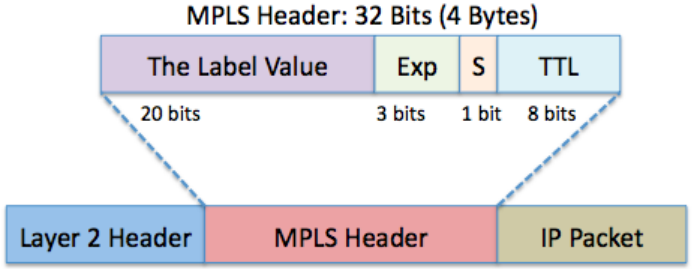
- Einführungsübung
- Technologie
  - Topologie
    - Provider – Grenze – DMZ – Netzwerk
  - Services
  - Produkte
  - Technikbegriffe
- Management
- Kosten

Services: MPLS

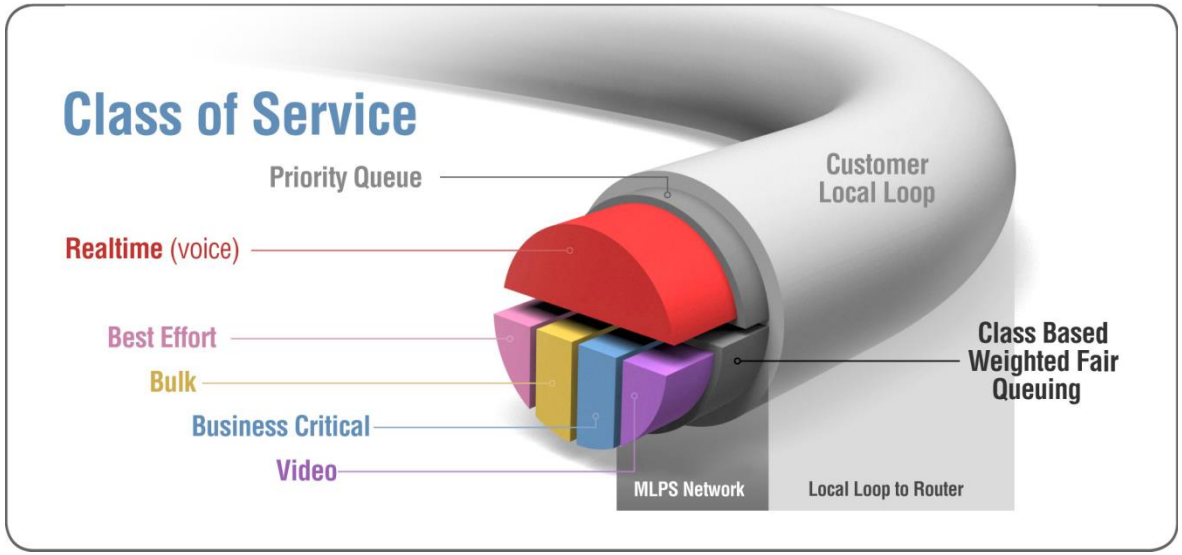
- MPLS (Multiprotocol Label Switching)
  - VPN-ähnliche Strukturen zur Verbindung von zusammengehörigen Netzwerken ohne Rücksicht auf IP Segmente
  - Paketvermittlung durch den Provider auf Grund von Labels in den Paketen



http://www.ip-insider.de/hybride-netze-mpls-internet-vpn-sd-wan-co-a-549030/



http://blog.ine.com/2010/02/21/the-mpls-forwarding-plane/



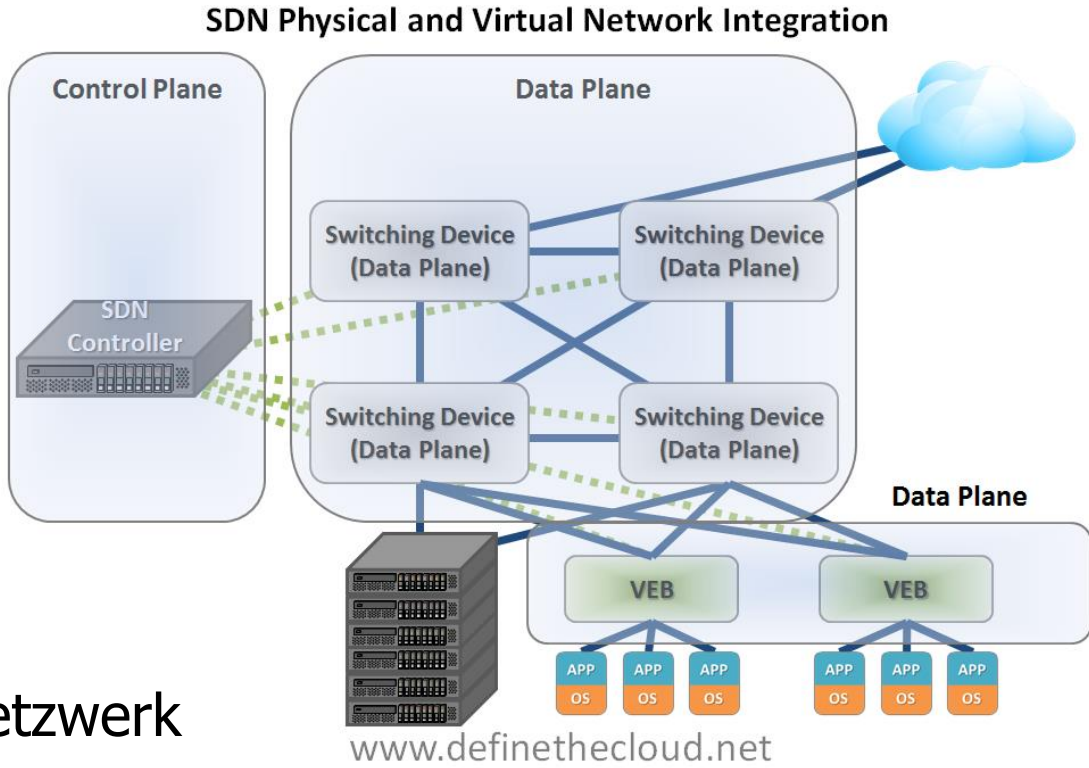
http://www.massivenetworks.net/index.cfm/ID/81/MPLS-AS-A-Service/

- QOS (quality of service)
  - Latenz, Jitter, Verlust, Durchsatz
- COS (class of service)
  - Reservierte «Bandbreiten»

SDN: Software Defined Networking

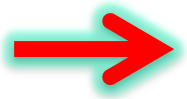
SDN:

- Zwei Ebenen:
  - Control-Plane
  - Data-Plane
- Netzwerke werden via Management SW erstellt
- Netze sind z.T. virtuell, sie werden auf einem Trägernetzwerk mit speziellen Protokollen/Suiten (z.B: Openflow) konfiguriert und verbunden



VEB: virtual Ethernet Bridge

Inhaltsübersicht



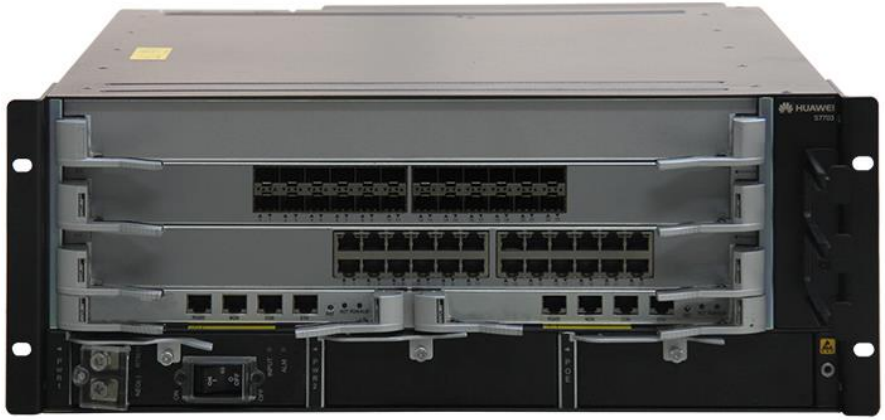
- Einführungsübung
- Technologie
  - Topologie
    - Provider – Grenze – DMZ – Netzwerk
  - Services
  - Produkte
  - Technikbegriffe
- Management
- Kosten

Produkte

- Core Switches von CISCO

- Huawei Core Switch mit bis zu 100 GE

  S7700 Series Smart Routing Switches
- 10 – 50 k Franken

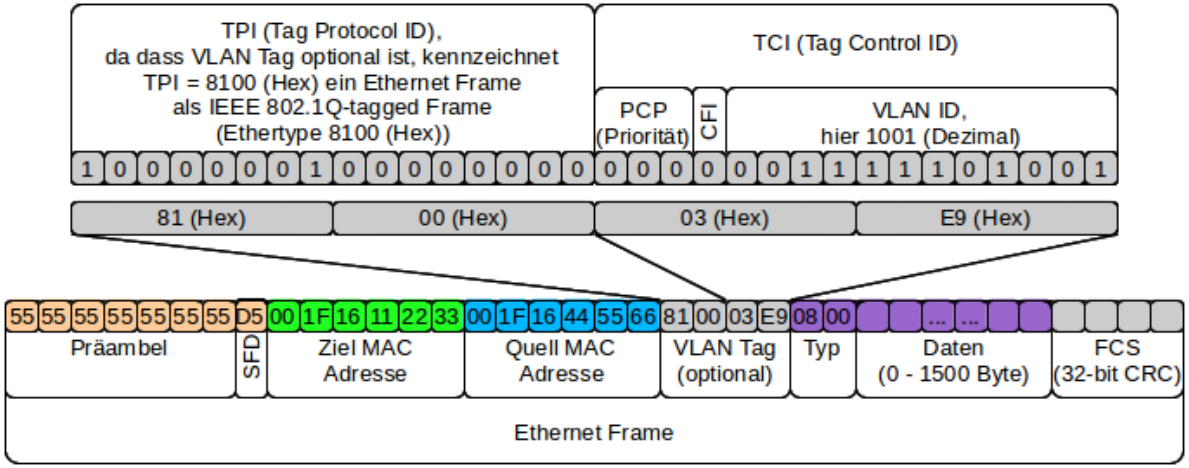


Inhaltsübersicht

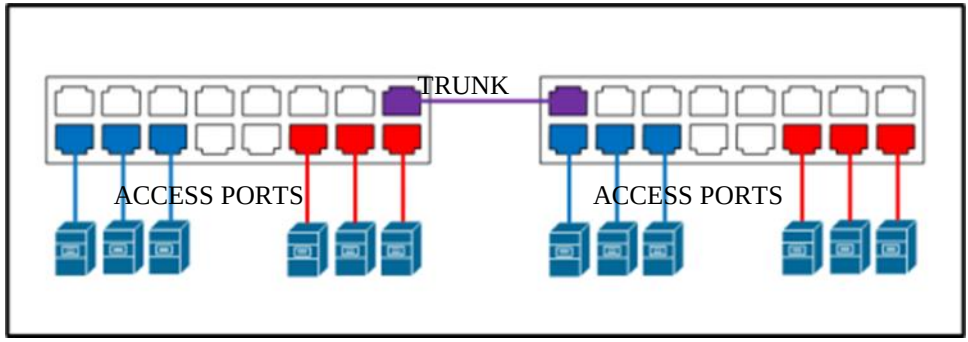
- Einführungsübung
- Technologie
  - Topologie
    - Provider – Grenze – DMZ – Netzwerk
  - Services
  - Produkte
  - Technikbegriffe
- Management
- Kosten

Technikbegriffe

- VLAN
  - Bildung von getrennten Netzen auf gemeinsamer Hardware
  - Virtual LAN
  - Tagged oder Untagged
  - Trunks (immer tagged) (mehrere VLANs)
  - Access Port (norm. 1 VLAN)



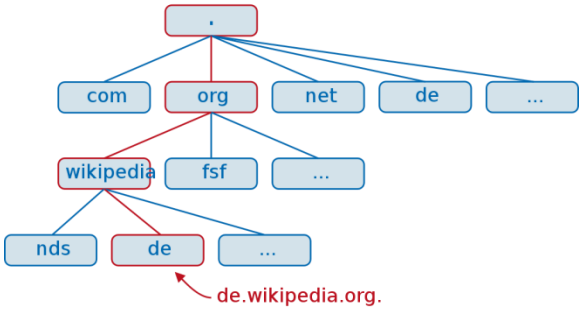
https://www.thomas-krenn.com/de/wikiDE/images/a/aa/Ethernet-Frame-VLAN-Tag.png



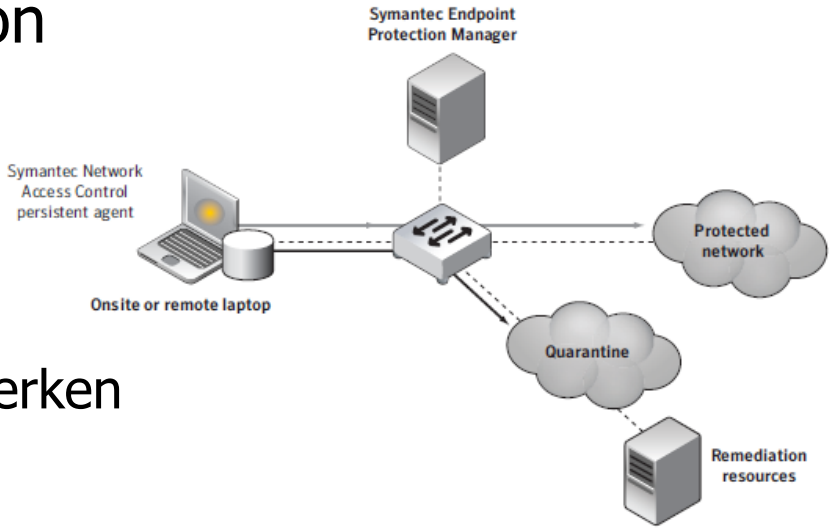
https://infrastructureadventures.files.wordpress.com/2010/11/vlans1.png

Technikbegriffe

- DNS: Domain Name System
  - Zuordnung von IP Adr. zu DNS-Namen
- IPAM: IP Address Management
  - MS Service oder separate Verwaltungstools



- DHCP: Dynamic Host Configuration Protocol
  - Dynamische oder reservierte Zuweisung von IP-Adressen und weiteren Eigenschaften an einen TCP/IP-Client
- NAP: network access protection
- NAC: network access control
  - Qualifizierung des Clients anhand von verschiedenen Parametern (User, OS, Version, AntiVir, ...)
  - Zuordnung zu den erlaubten Netzwerken oder nur zur Quarantäne Zone



Inhaltsübersicht

- Einführungsübung
- Technologie
  - Topologie
    - Provider – Grenze – DMZ – Netzwerk
  - Services
  - Produkte
  - Technikbegriffe
- Management
- Kosten

Management

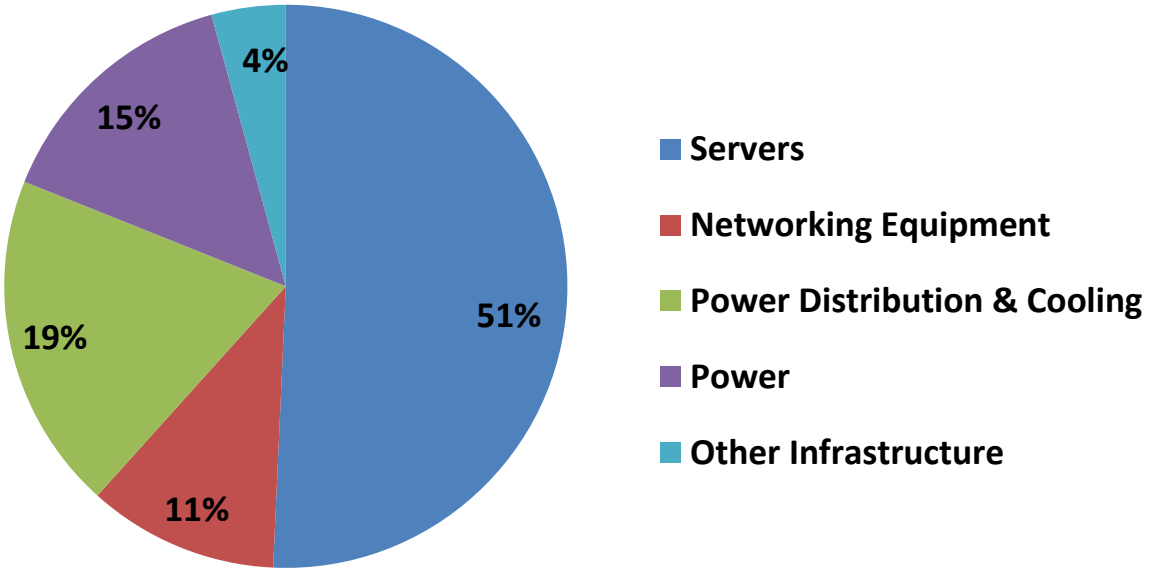
- Netzwerkmanagement
  - Verwaltung, Betriebstechnik und Überwachung von IT-Netzwerken und Telekommunikationsnetzen
  - OAM(&P): Operation, Administration, Maintenance (& Provisioning)
  - ISO: FCAPS Fault/Config/Accounting/Performance/Security Mgmt
- Systemmanagement
  - Monitoring aller Betriebsparameter und der Konfiguration: siehe ITIL
- Management Netzwerk
  - Vom restlichen Netzwerk getrenntes LAN, welches nur für das Management benutzt wird.
  - Beschränkter Zugriff (Stationen und Benutzer)
  - Oft nur via Jump-Host mit starkem Logging erreichbar

Inhaltsübersicht

- Einführungsübung
- Technologie
  - Topologie
    - Provider – Grenze – DMZ – Netzwerk
  - Services
  - Produkte
  - Technikbegriffe
- Management
- Kosten

Kostenverteilung

- Kostenverteilung in einem Rechenzentrum
  - Annahme: ca. 1000 Server
  - Basierend auf realistischen Annahmen



Basis: http://perspectives.mvdirona.com/2010/09/overall-data-center-costs/ (auf mittleres RZ redimensioniert)

Switch-Kosten

- How much will an enterprise have to pay for your core switch with the components to support 96 10 Gigabit Ethernet (10 GbE) ports in a chassis?
  - Cisco: Approximately $240,000 U.S. list.
    This includes a 6509-E switch chassis, Sup2T 9 Slots Bundle ($38,000), Six 6816 Line Cards ($32,000) and dual power supplies ($5,000). [Editor's note: The expected lifespan of this product is 10 to 15 years.]
  - HP: Approximately $146,994 U.S. list.
    This includes an HP 10504 switch chassis ($6,000), four HP 10504 960 Gbps Type D Fabric Modules ($8,999), HP 100500 Main Processing Unit ($9,000), dual HP 10500 2500 AC power supplies ($2,000), two HP 10500 48-port 10 GbE SFP+ SF Modules ($45,999).
  - Juniper: Approximately $145,000 U.S. list.
    This includes the EX8216 redundant chassis with 96 line-rate 10 GbE ports. As a 5:1 oversubscribed 10 Gigabit Ethernet switch, the average selling price would be approximately $75,000.
- http://searchnetworking.techtarget.com/feature/Campus-core-switch-comparison-How-Cisco-HP-Juniper-differentiate-their-switches
- Stand Dez. 2014

Links und Literatur

- Wikipedia RZ Portal

  https://de.wikipedia.org/wiki/Portal:Rechenzentrum

- Diverse Links direkt bei den Grafiken

Fragen