CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

System- und Netzwerk-administration

CloudCommand GmbH chr.schumacher@gmx.tm

Übertragungs-technik

Netzwerkinfrastruktur

Netzwerkinfrastruktur beschreibt die technische Gestaltung eines Netzwerks, damit alle Geräte miteinander kommunizieren können. Die Netzwerkinfrastruktur stellt die Grundlage für ein funktionierenden Netzwerk dar und ermöglicht den Datenverkehr zwischen sämtlichen netzwerkfähigen Geräten und Servern.

Die Netzwerkinfrastruktur besteht in der Regel aus einer Mischung von Hardware, Software und Netzwerkdiensten.

- Hardware: Server, PC, Router, Switches, Firewall, Modems, ...
- Software: Überwachungs- und Verwaltungstools und Betriebssysteme.
- Netzwerkdienste: Netzwerkprotokolle wie z.B. DNS, TCP, DHCP.

Netzwerkinfrastruktur

- In professionellen Unternehmensnetzwerken involvierte Gerät und alle Server sind über Netzwerkkabel an einen Switch und über diesen teilweise an einige weitere Switches angeschlossen, sodass am Ende jedes Endgerät mit jedem anderen Endgerät eine direkte Verbindung aufbauen kann.
- Wichtige Komponenten eines Netzwerks sind die Netzwerkkabel, Server, Rechner, Drucker, Switches, Router und Access Points
- Netzwerke, die vollkommen auf WLAN ausgerichtet sind, finden – im Unternehmensumfeld – bisher weniger Einsatz als kabelgebundene Netzwerke, aber dies ändert sich zunehmend.

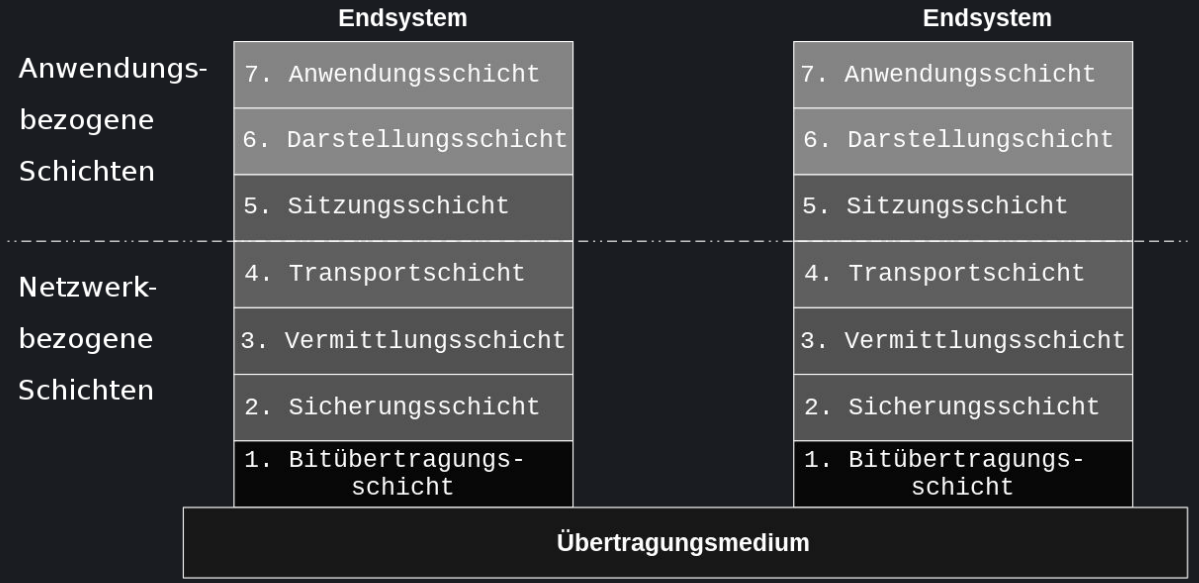
→ Warum?

Netzwerkinfrastruktur

Netzwerkinfrastruktur Management:

- Überwachung der Netzwerkinfrastruktur
- Konfigurations-/Assetmanagement
- Performance Management
- Störungsmanagement
- Sicherheitsmanagement

OSI-Layer zur Orientierung



Netzwerkkabel

Twisted-Pair Kabel:

- Twisted-Pair-Kabel ist das Kabel, dass am häufigsten in lokalen Netzen verwendet wird.
- Ein Twisted-Pair-Kabel hat insgesamt acht Kupfer-Adern.
- verwendet in der Regel einen RJ-45 Stecker

Netzwerkkabel

Twisted-Pair Kabel:

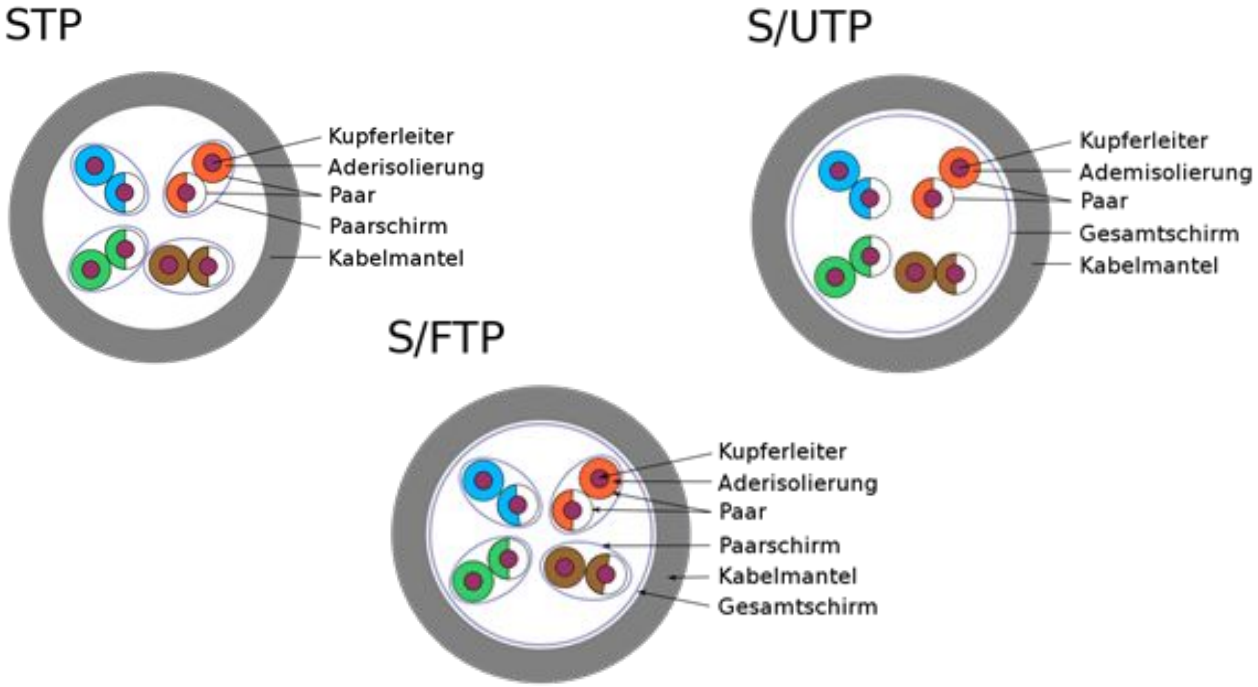
- Diese acht Drähte werden in vier Paare gruppiert: blau, Orange, grün und braun.
- Jedes Paar der Drähte ist über die gesamte Länge des Kabels verdreht.
- Durch die Verdrehung der Adern sollen Interferenzen vermieden werden.

Netzwerkkabel

STP, S/FTP, S/UTP

- Shielded-Twisted-Pair (STP) Kabel haben eine Aluminium-Schirm im Inneren des Kunststoff-Mantels, der die Draht Paare umgibt.
- Shielded-Foiled-Twisted-Pair (S/FTP) haben einen doppelten Schirm. Eine Folie um jedes Paar und eine Drahtgeflecht um alle Paare.
- Screened Unshielded Twisted Pair (S/UTP) haben nur ein Drahtgeflecht um alle Paare herum.

Netzwerkkabel



Netzwerkkabel

Dämpfung bei Twisted-Pair-Kabeln

- Max. Kabellänge bei Twisted-Pair-Kabel 100 m
- Längere Strecken, nur über Repeater, Hub oder Switch
- Andernfalls ist Glasfaserkabel die Lösung, weil sie viel weiter als Twisted–pair Kabel verlegt werden kann.

Netzwerkkabel

Kategorien von Twisted-Pair-Kabeln

- Twisted-Pair-Kabel werden nach der Frequenz, mit der sie Signale übertragen und ihrer Datentransferrate oder Geschwindigkeit kategorisiert.

Netzwerkkabel

EIA/TIA 568	ISO/IEC 11801	Anwendung / Bandbreite
Cat. 1	-	Telefon- und Modemleitungen
-	-	Telefon- und Modemleitungen
Cat. 2	-	Terminal-Systeme, ISDN
Cat. 3	-	10Base-T, 100Base-T4, ISDN, analoges Telefon
Cat. 4	-	Token Ring (16 MBit)
Cat. 5	Cat. 5	100Base-TX, SONET, SOH

Netzwerkkabel

EIA/TIA 568	ISO/IEC 11801	Anwendung / Bandbreite
Cat. 5e	Cat. 5e	1000Base-T
Cat. 6	Cat. 6	10GBase-T (bis 55 Meter), 155-MBit-ATM, 622-MBit-ATM
Cat. 6A	Cat. 6_A	10GBase-T
-	Cat. 7	10GBase-T
-	Cat. 7_A	10GBase-T
Cat. 8	Cat. 8.1/8.2	40GBase-T und 100GBase-T (bis 30 Meter)

Netzwerkkabel

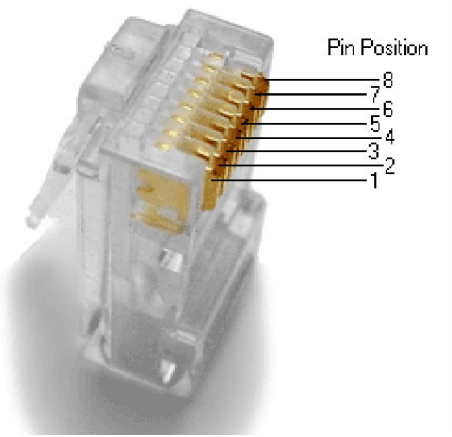
Flammwidriges Kabel (plenum-rated)

- Plenum-rated oder Raucharme Kabel sind Kabel für die Verwendung in Innenwänden oder durch abgehängte Decken, wo sie im Falle eines Brandes nicht durch Sprinkleranlagen geschützt sind.
- Plenum-rated Kabel haben eine Teflon-Beschichtung die sie unempfindlicher gegen Feuer macht.
- Sie werden verwendet, da Standard-Twisted-Pair-Kabel eine PVC-Ummantelung haben, die im Brandfall tödliche Gase freisetzen können.

RJ45-Stecker

Definiert in der EIA/TIA 568

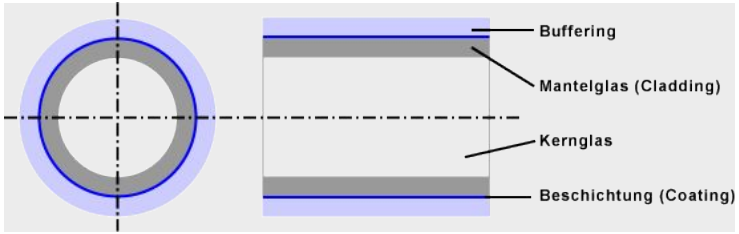
- 2 verschiedene Ausprägungen sind möglich: A und B



		EIA TIA 568 B	EIA TIA 568 A
Signal	**Pin**	**Farbe**	**Farbe**
TX+	1	weiß/grün	weiß/orange
TX-	2	grün	orange
RX+	3	weiß/orange	weiß/grün
	4	blau	blau
	5	weiß/blau	weiß/blau
RX-	6	orange	grün
	7	weiß/braun	weiß/braun
	8	braun	braun

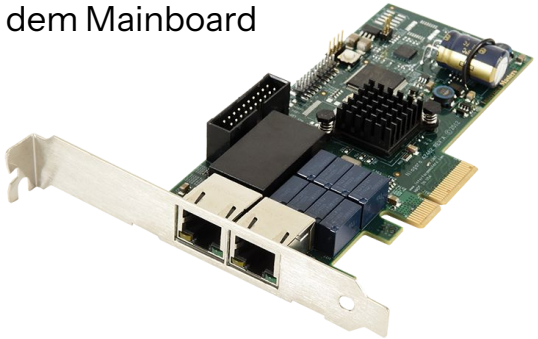
Glasfaser / LWL / FC

- LWL-Kabel überträgt Licht (Photonen) anstelle von Strom, und dieses Licht wird durch Glas oder Kunststoff übertragen.
- Es wird unterschieden zwischen
  - Single-Mode-Glasfaser und
  - Multi-Mode-Glasfaser
- SM erreicht Reichweiten bis zu 10km, bei MM sind es bis zu 2km
- LWL erreicht Übertragungsgeschwindigkeiten bis zu 100 Gbit/s



Netzwerkkarte

- Ein Netzwerkadapter / Netzwerkkarte / NIC (Network Interface Card) ist das Gerät, welches es dem Computer ermöglicht Daten zu senden und zu empfangen.
- Ein Adapter kann kabelgebunden oder drahtlos mit dem Netzwerk verbinden.
- Der RJ45-Port ist die häufigste Art eines Netzwerkkarten Anschlusses.
- als Steckkarte oder direkt als Chipsatz auf dem Mainboard



Netzwerkkarte

- Jede Netzwerkkarte ist mit einer weltweit eindeutigen Hardware-Adresse versehen.
- Bei Ethernet und WiFi Adaptern ist das die „Media Access Control“-Adresse, kurz MAC Adresse.
- Die MAC-Adresse wird üblicherweise im Hexadezimalsystem, kurz HEX, dargestellt und umfasst 48 Bit.
- Die ersten 24 Bit identifizieren den Hersteller der Karte und die zweiten 24 Bit die Adresse der eigentlichen Karte.
- 00-07-E9-1A-00-A0 oder 00:07:E9:1A:00:A0

Zusammenschluss von Netzwerkkarten (NIC-Teaming)

Leistungsoptimierung (Bonding):

- Hierbei werden mehrere Schnittstellen zusammengefasst, um den Netzwerkdurchsatz zu erhöhen.

Lastenausgleich (Load Balancing):

- Dieser kann statisch oder dynamisch definiert werden, z.B. auf Basis von IP-Adressen oder TCP-Paketen.

Fehlertoleranz (Fault Tolerance):

- **statisch:** Ein Adapter arbeitet als primäre Verbindung, der andere als sekundäre, die nur zum Einsatz kommt, wenn die primäre Verbindung ausfällt.
- **dynamisch:** die Adapter verwalten sich selber und können sich im Fehlerfall gegenseitig vertreten.

Koppelelemente

Medienkonverter

- Verbinden Netzwerksegmente unterschiedlicher Medien miteinander.
- Es gibt auch Switches, welche ein Konverter Modul beinhalten können.
  - GBIC (Gigabit Interface Converter)
  - SFP Modul (Small Form-Factor Pluggable)

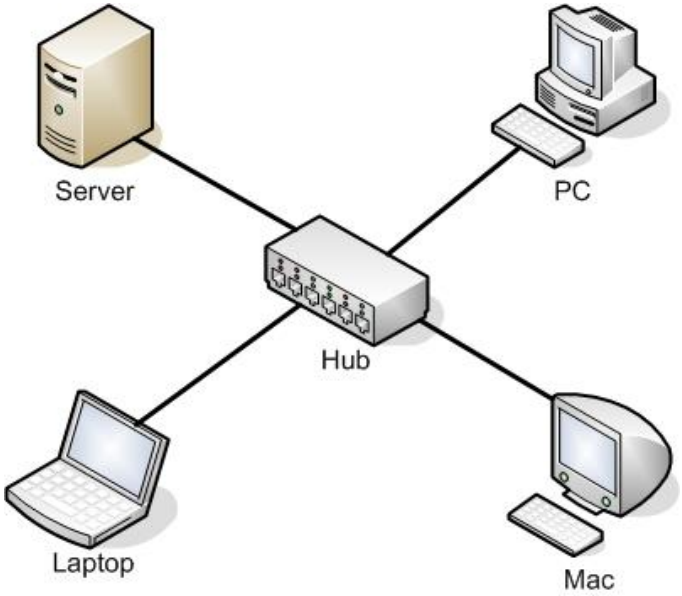
Repeater

- Erweitern das WLAN um die Reichweite zu erhöhen und das Signal zu verstärken.
- Arbeiten im Regelfall auf der elektronischen Ebene und besitzen keine „echte" Intelligenz.
- Verstärkt und regeneriert Signale auf elektrischer Ebene.
- Arbeiten auf OSI-Layer 1 und kümmern sich einzig um die Signalaufbereitung.

Hub

- Ein Hub war das grundlegendste der zentralen Verbindungsgeräte.
- Es verbindet jedes der Netzwerkcomputer miteinander, mittels TP-Leitungen.
- Jeder Host sendet Daten zuerst an den Hub, wo sie an alle anderen im Netz ausgestrahlt werden.
- Es gibt passive Hubs (nur Signalweiterleitung)
- Es gibt aktive Hubs (mit Signal Regeneration)
    - Ein (aktiver) Hub ist lediglich ein Repeater mit mehreren Anschlüssen

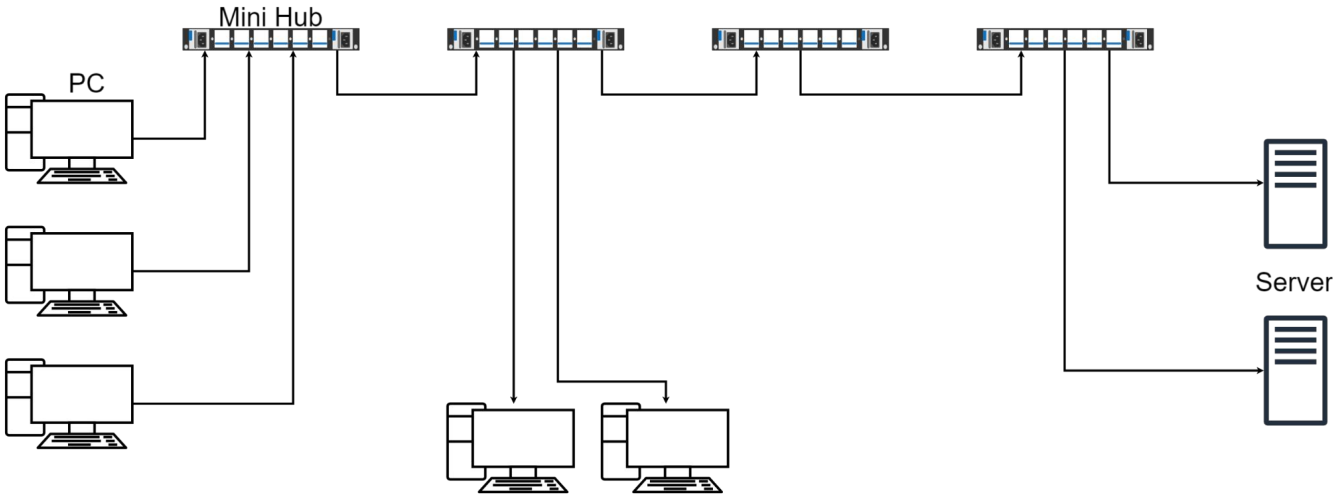
Hub



5-4-3-Regel

- Die 5-4-3-Regel besagt, dass innerhalb einer Kollisionsdomäne maximal 5 Segmente mittels 4 Repeatern (oder Hubs) verbunden werden können, aber nur an 3 dieser Segmente dürfen sich Endgeräte (Stationen) befinden.
- Eine Kollisionsdomäne ist ein Netzsegment in einem Netz. Alle Stationen, die auf einer gemeinsamen Schicht 1 (Physical Layer, Bitübertragungsschicht) entweder direkt oder mit Repeatern oder Repeater Hubs miteinander verbunden sind, befinden sich in einer gemeinsamen Kollisionsdomäne.
- Heutige Netzwerkarchitekturen basieren auf einer Mikrosegmentierung, die an einem Switchport nur noch eine Station anbindet und folglich keine Konkurrenzsituation mehr erzeugt.

5-4-3-Regel



Bridge

- Eine Bridge ist ein Layer 2 Gerät zur Teilung eines Netzwerkes.
- Bridges leiten Frames zwischen zwei Segmenten weiter.
- Bridges erlangen diese Fähigkeit durch das Lernen von MAC-Adressen der angeschlossenen Stationen. Dazu bauen Bridges eine Forwarding-Tabelle auf.
- Bridges reduzieren die Größe der Kollisionsdomäne.

Switches

- OSI-Layer 2
- Filterung basiert mittels Adresstabelle, auf MAC Adressen Ebene (hier SAT genannt, Source Address Table)
- eine Kollisionsdomäne pro Port
- Switches bauen eine virtuelle Verbindung zwischen zwei Geräten auf, über die explizit kommuniziert wird
    - Dadurch erreichen sie eine **Mikrosegmentierung**.
- Ein Switch ermöglicht mehrere simultane Kommunikationspfade.

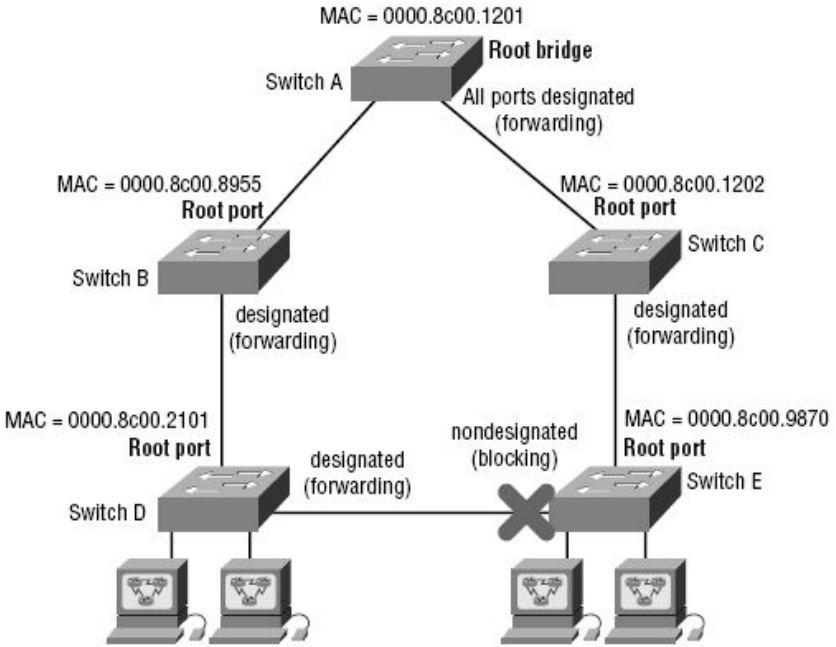
Store and Forward Switch

- leitet den vollständigen Rahmen weiter, berechnet CRC und prüft die Länge
- kann Priorisierungsschemata nutzen und Filter verwenden.
- Ziel-Port wird nicht mit fehlerhaften Frames belastet.

Cutting Through Switch

- leitet den Rahmen an den Output Port weiter, sobald die MAC-Zieladresse erkannt wird
- erzeugt eine geringstmögliche Latenzzeit
- Fehlerhafte Frames werden weitergeleitet und belasten unnötig den Weg vom Port bis zum Empfänger.
- Viele Switches können zwischen cut-through und store and forward wechseln.

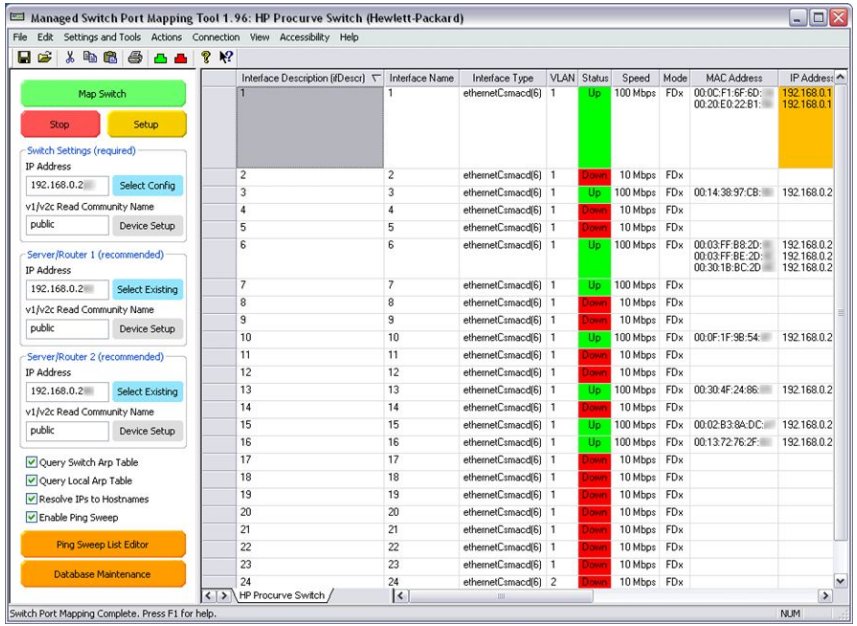
STP (Spanning Tree Protocol)



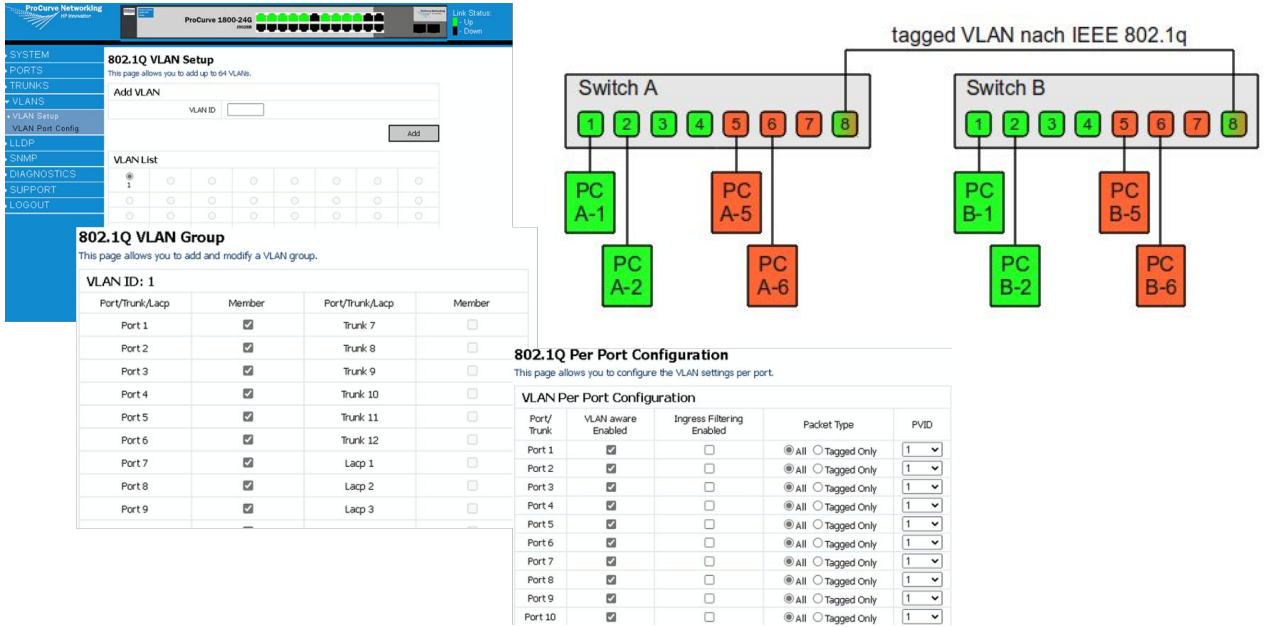
Managed Switch und Layer 3 Switch

- Ein Layer 3 Switch ist typischerweise ein Layer 2 Switch, der den Routingprozesses Layer 3 unterstützt.
- Die Layer 3 Headerinformation wird geprüft und das Paket auf der Basis der IP-Adresse weitergeleitet.
- Layer 3 Funktionalität bezieht sich ausschließlich auf IP.

Managed Switch und Layer 3 Switch

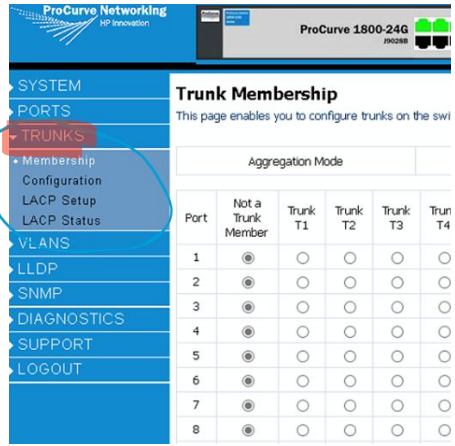


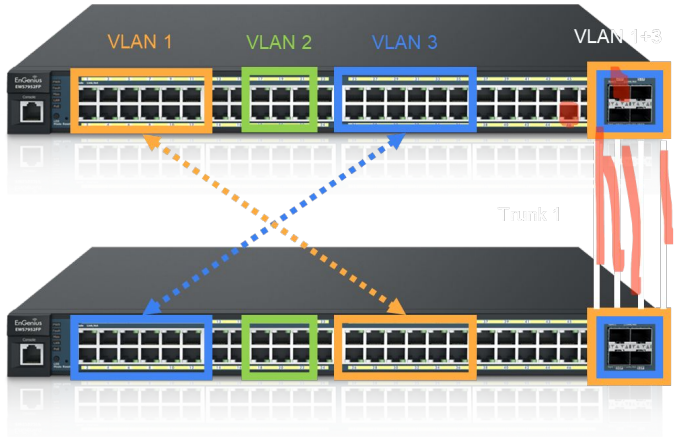
VLAN (Virtual LAN)



Trunk

- Bündelung mehrerer physikalischer Leitungen zu einer logischen Verbindung (vgl. NIC-Teaming)





Router

- Ein Router ist ein Layer 3 Gerät.
- Router nutzen Wege durch ein Netzwerk.
- Router leiten Pakete basierend auf Adressen der Schicht 3 weiter.
- Router nutzen Routingtabellen, um den Weg zum Ziel zu ermitteln.

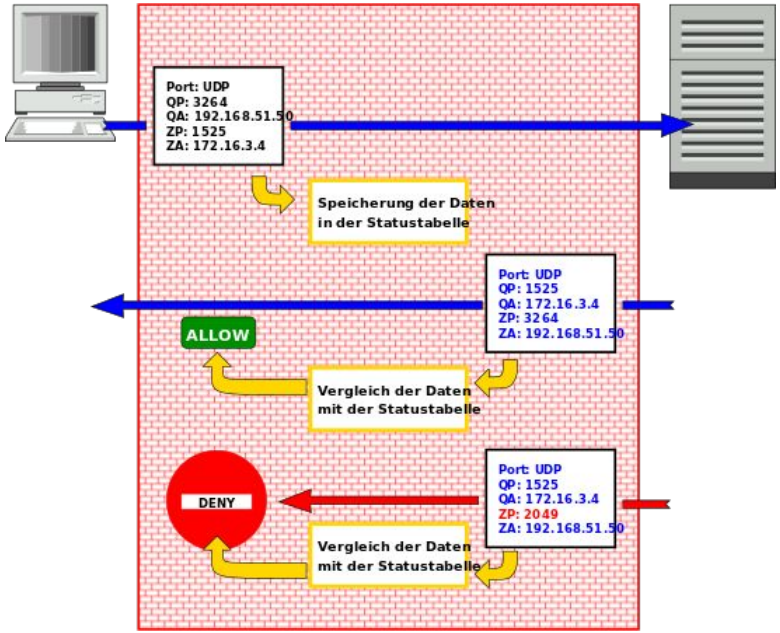
Firewall

- **Personal Firewall** (Desktop Firewall) oder **externe Firewall** (Netzwerk- oder Hardware-Firewall)
- Die externe Firewall arbeitet nicht auf dem zu schützenden System selbst, sondern auf einem separaten Gerät, welches Netzwerke oder Netzsegmente miteinander verbindet
- Genau genommen ist die Firewall nur als Hardware Firewall als Koppelelement zu betrachten.
    - Sie arbeitet von OSI Layer 4 bis 7.

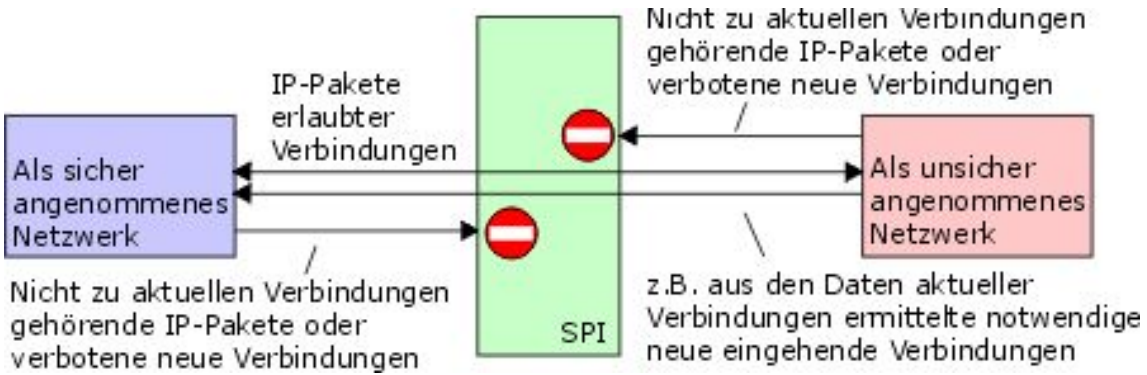
Firewall

- Die Firewall (Layer 4) erkennt keine Angriffe. Sie blockt und akzeptiert anhand von definierten Regeln.
  - Sie ist ein Sicherungssystem, das ein Netzwerk oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.
  - Die Firewall-Software überwacht den durch sie laufenden Datenverkehr, basierend auf Absender- oder Zieladresse und genutzten Diensten.

Firewall


Port: UDP
QP: 3264
QA: 192.168.51.50
ZP: 1525
ZA: 172.16.3.4
Speicherung der Daten
in der Statustabelle
Port: UDP
QP: 1525
QA: 172.16.3.4
ZP: 3264
ZA: 192.168.51.50
ALLOW
Vergleich der Daten
mit der Statustabelle
Port: UDP
QP: 1525
QA: 172.16.3.4
ZP: 2049
ZA: 192.168.51.50
DENY
Vergleich der Daten
mit der Statustabelle

SPI Firewall (Stateful Packet Inspection)



Proxy

- Eigentlich kein echtes Koppelelement, sondern eine Software, bzw. Funktion einer Firewall oder eines Routers
- Proxy bedeutet „Stellvertreter“, stellt die Anfrage stellvertretend für den Client
- Ein Verbindungselement zwischen einem lokalen Netzwerk und weiteren Netzwerken wie z.B. dem Internet
- reguliert den aus- und eingehenden Netzwerkverkehr (Content filtering)
- Kann Inhalte zwischenspeichern (Cache)

Was sollte ich auf jeden Fall behalten

OSI-Schicht		Einordnung	Kopplungselemente
4	Transport (Transport)	Ende-zu-Ende (Multihop)	Firewall, Gateway, Content-Switch, Proxy, Layer-4-7-Switch
3	Vermittlung-/Paket (Network)		Router, Layer-3-Switch
2	Sicherung (Data Link)	Punkt-zu-Punkt	Bridge, Layer-2-Switch, Wireless Access Point
1	Bitübertragung (Physical)		Netzwerkkabel, Repeater, Hub

Was sollte ich auf jeden Fall behalten

ISO/IEC 11801	Anwendung/Bandbreite
Cat. 5	100Base-TX, SONET, SOH
Cat. 5e	1000Base-T
Cat. 6	10GBase-T (bis 55 Meter), 155-MBit-ATM, 622-MBit-ATM

Was sollte ich auf jeden Fall behalten

- Die erste Hälfte identifiziert den Hersteller der Karte und die zweiten Hälfte die Adresse der eigentlichen Karte (zusammengesetzt MAC-Adresse, Media Access Control).
- Ein Virtual Local Area Network (VLAN) ist ein logisches Teilnetz (Netzsegment) innerhalb eines Switches bzw. eines gesamten physischen Netzes.
- Die Paket-Inspektion wertet Teile des Inhaltes der Pakete (also Teile der Anwendungsdaten) aus. Dabei werden die Daten nur analysiert und nicht verändert.
- Entsprechend der Regeln wird das Paket danach geblockt oder erlaubt.

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm