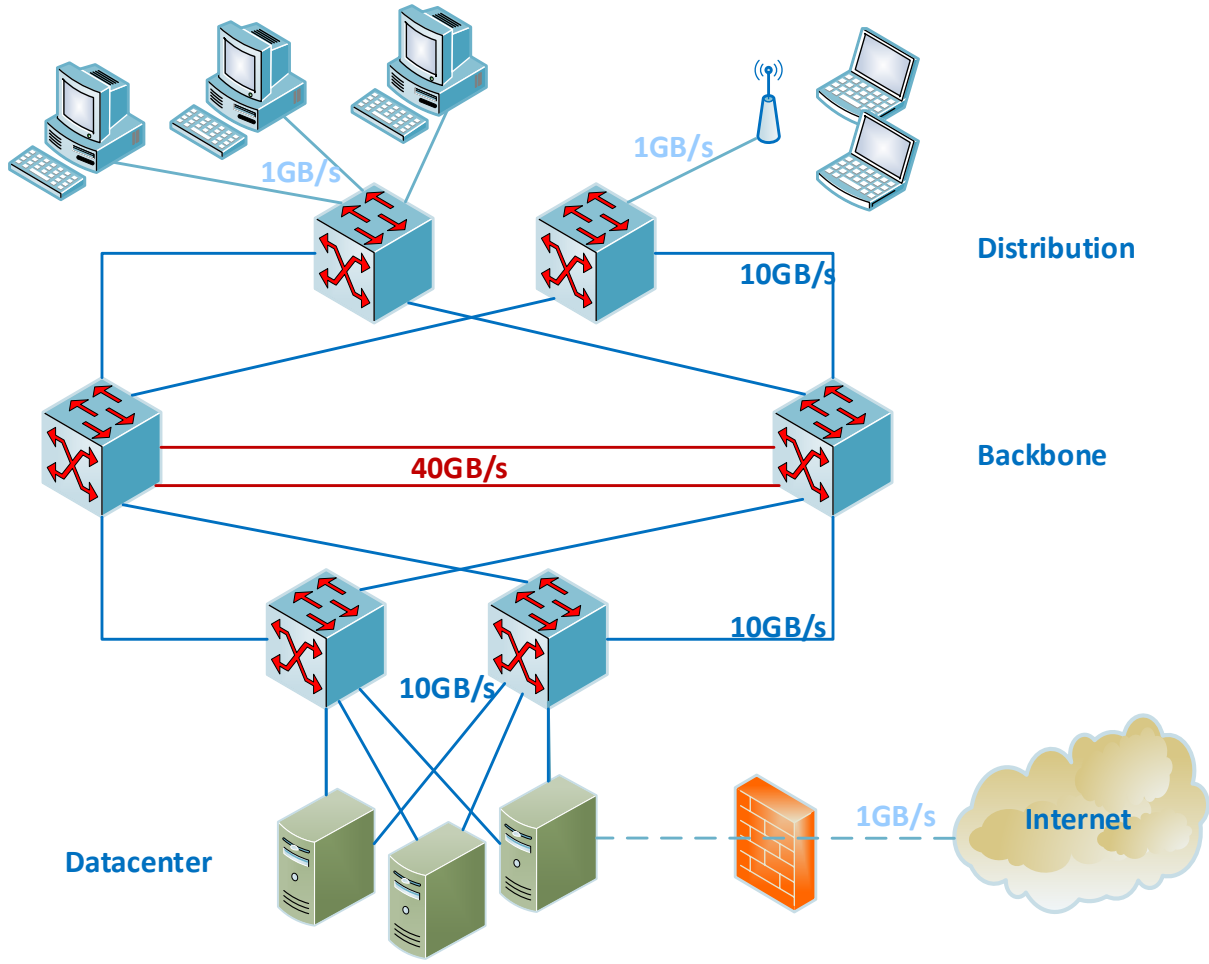
Grundlagen Netzwerksicherheit

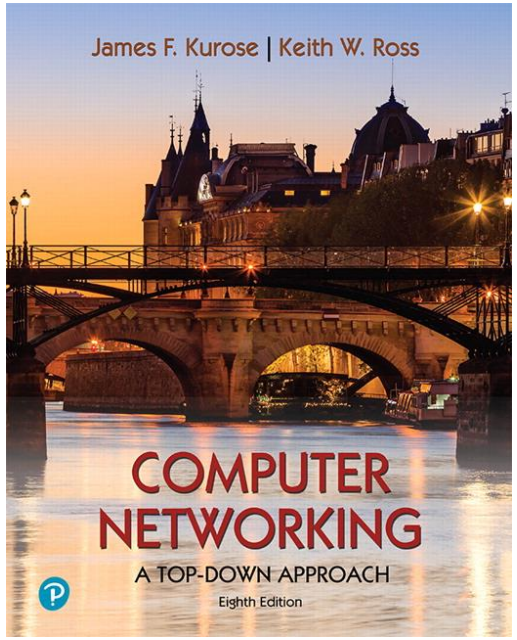
Prof. Dr.-Ing. Jürgen Schneider

Inhaltsübersicht

1. Management von sicheren lokalen Netzwerken
2. Netzwerksegmentierung mit Firewalls und IPS-Systemen
3. Netzwerkbasierte Authentifizierung und Autorisierung (NAC, EAP, RADIUS)
4. Sicherer Nachrichtentransport (IPsec, MACsec)

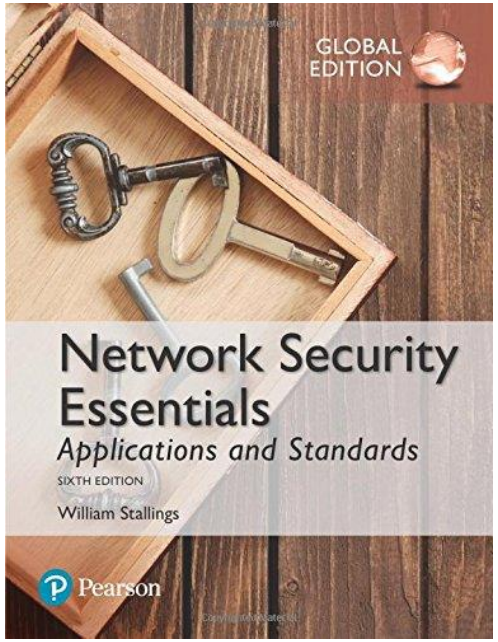


Meine Literaturempfehlung



Computer Networking: A Top-Down-Approach

8th. Edition
Jim Kurose, Keith Ross
Pearson, 2021.



Network Security Essentials

6th. Edition
Global Edition
William Stallings
Pearson 2017.

Kapitel 1: Management von sicheren Netzwerken

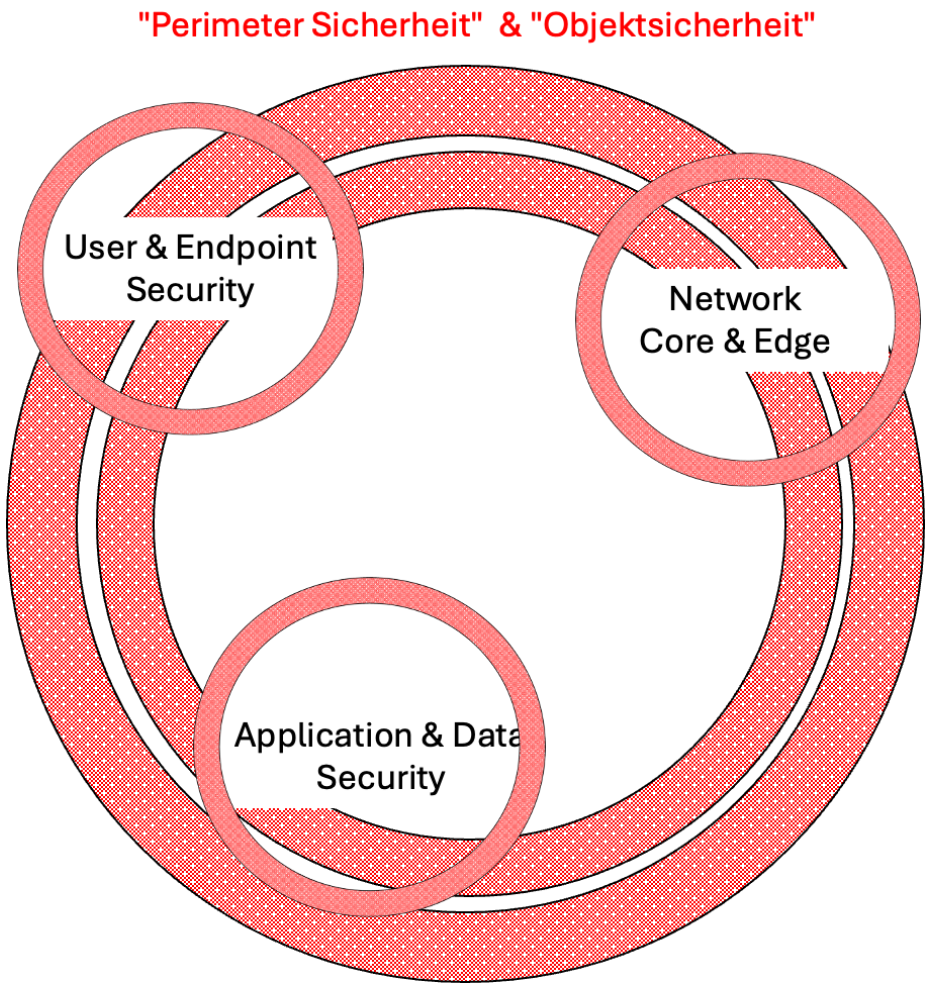
Lernziele:

Die folgenden Themen verstehen und einem Dritten erklären können

- Kernziele und Kerndienste in Netzwerken
- Funktionsweise und Ziel virtueller Netzwerke
- Methoden für ein sicheres Layer-2 Netzwerk
- Methoden für ein sicheres Layer-3 Netzwerk

Überblick:

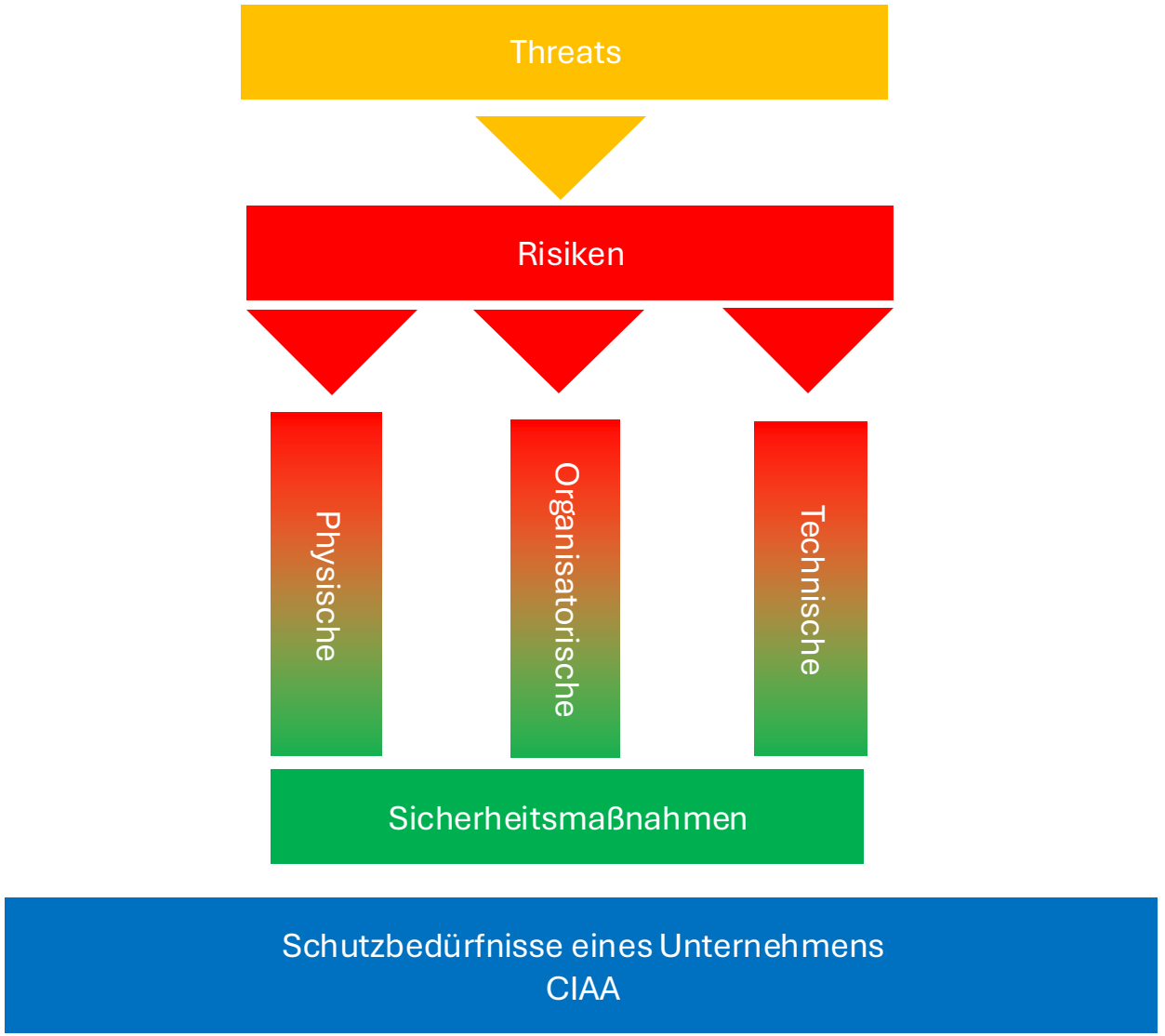
1.1 Kernziele und Kerndienste für sichere Netzwerke



IT-Security

Die Gesamtheit der in einem Unternehmen ergriffenen Sicherheitsmaßnahmen zur Abwehr der Schadensauswirkungen eines möglichen Cyber-Angriffes fasst man unter dem Begriff IT-Security (Angriffssicherheit) zusammen.

- Die Sicherheitsmaßnahmen gewährleisten die Schutzbedürfnisse eines Unternehmens.
- Die Schutzbedürfnisse sind:
  - Vertraulichkeit der Daten (Confidentiality C)
  - Integrität der Daten und Systeme (Integrity I)
  - Verfügbarkeit der Daten und Systeme (Availibility A)
  - Rechenschaftspflicht von Transaktionen (Accountability A)
- Die Sicherheitsmaßnahmen können in physische, organisatorische und technische Maßnahmen unterteilt werden.



Traditionelle Datenverarbeitung

Bei der traditionellen Datenverarbeitung werden die Daten fast ausschließlich innerhalb eines Unternehmensnetzwerkes (Campus) verarbeitet und konsumiert.
Die Daten werden im Unternehmensnetzwerk (im eigenen Rechenzentrum) erzeugt und dort zentral in Speichersystemen gespeichert.

- Finanzdaten

  Gewinn- und Verlustrechnungen, Bilanzen und Kapitalflussrechnungen.

  Daten geben Einblick in die finanzielle Situation des Unternehmens.

- Geistiges Eigentum

  Über neue Produkte kann ein Unter-nehmen einen wirtschaftlichen Vorteil gegenüber seinen Wettbewerbern erzielen.

  Dieses geistige Eigentum sollte als Geschäftsge-heimnis behandelt werden.

- Personenbezogene Mitarbeiterdaten

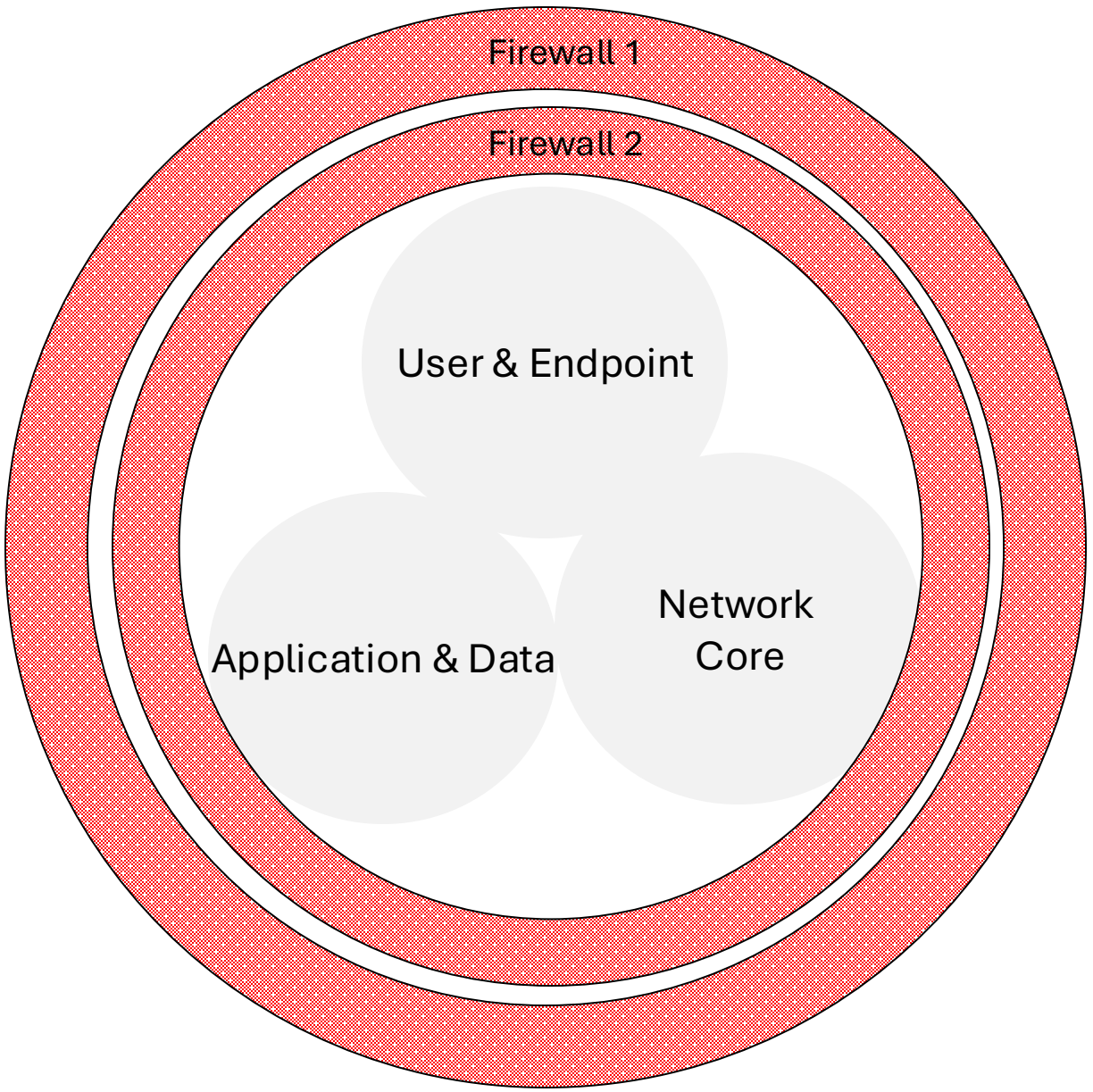
  Bewerbungsunterlagen, Gehaltsabrechnungen, Ziele- und Mitarbeitervereinbarungen und alle Informationen, die für Personalentscheidungen verwendet werden

- Kunden- und Lieferantendaten

  Kontakte, Angebotsschreiben, Aufträge, Projektstatus, Rechnungen, Qualität von gelieferten Waren und Dienstleistungen, ...

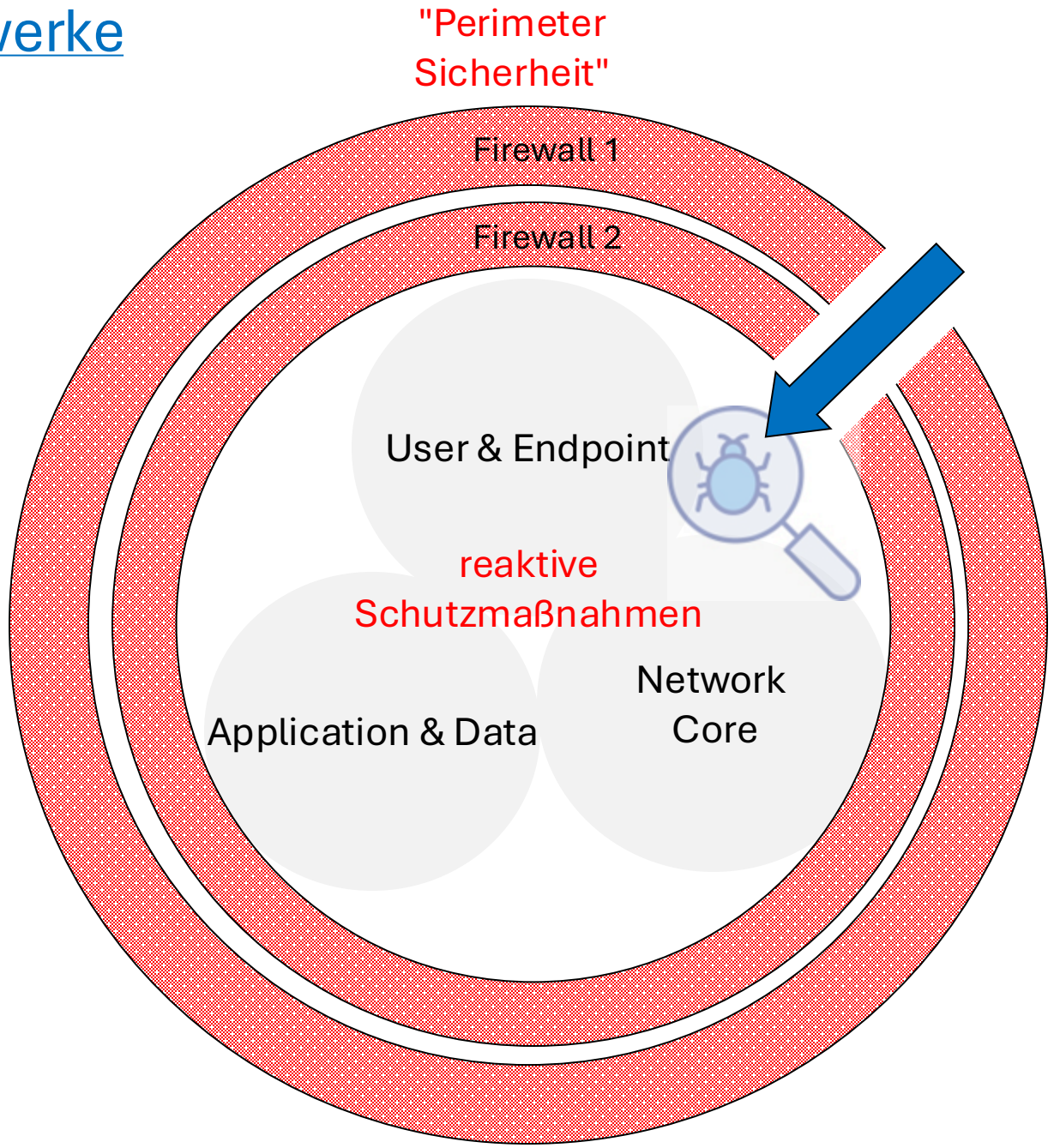
Traditionelles Sicherheitsmodell für Netzwerke

- Da die Prozesse und Daten im eigenen Unternehmensnetzwerk verarbeitet werden, kann durch die Absicherung des Netzwerk-Perimeters eine hohe Sicherheit erlangt werden.
- Klassische Schutzmaßnahmen sind eine "doppelwandige" Firewall-Infrastruktur, bestehend aus zwei Firewalls bekannter aber unterschiedlicher Hersteller.
  - Allen Systemen innerhalb des Perimeters wird vertraut.
  - Allen Systemen außerhalb des Perimeters wird nicht vertraut.
  - Der Datenverkehr innerhalb des Unternehmensnetzwerkes wird als vertrauenswürdig erachtet, sodass keine besonderen Schutzmaßnahmen getroffen wurden.
  - Problem: Internationalisierung der Firmen führt zu firmeninternen VPNs, zu Standorten (in China) mit unterschiedlichem Sicherheitsverständnis.



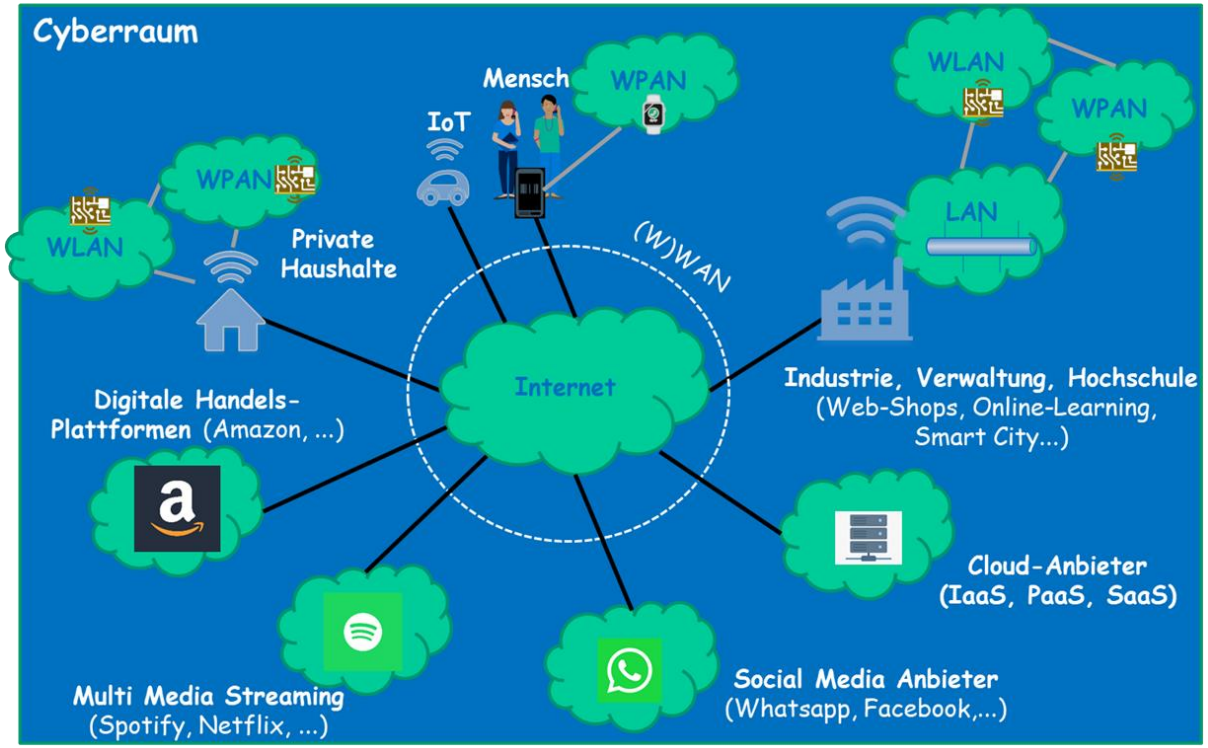
Traditionelles Sicherheitsmodell für Netzwerke

- Durch die Interaktion der internen Endgeräte mit Systemen im Internet (klassisch: E-Mail, Web-Server), also nicht vertrauenswürdigen Systemen, wurde das Schutzkonzept durch reaktive Schutzmaßnahmen ergänzt
  - Antivirus-Scanner
  - Secure-E-Mail-Gateway
- Um eine permanente Überwachung des Perimeters und der Schutzmaßnahmen zu ermöglichen, wurden sogenannte IT-Leitstände (IT-Operation Center) eingeführt.
- Die IT-Leitstände wurden mit Überwachungssystemen (detektive Maßnahmen) ausgestattet, die eine Erkennung von Incidents schnell ermöglichen sollen.



Gesellschaftlicher Trend: Digitalisierung und zunehmende Vernetzung

- Um die Produktions- und Betriebskosten einer Organisation zu senken aber auch um attraktive Produkte zu gestalten, ist eine zunehmende Digitalisierung von Prozessen und Produkten einhergehend mit einer zunehmenden Vernetzung von Organisationen und Verteilung von Information zwingend notwendig:
  - Vernetzung zwischen Behörden, Unternehmen, Privathaushalten
  - Vernetzung zwischen internen Systemen mit externen Systemen (z.B.: Produkten mit Sensoren).
  - Vernetzung von internen Produktionsanlagen (ICT) mit externen Dienstleistern
  - Nutzung von internen IT-Systemen und externen Cloud-Ressourcen.
  - Verteilung von personenbezogenen Daten über verschiedene Organisationen: Personalakte - Arbeitgeber, Gesundheitsdaten – Krankenkasse, Fitnessdaten – App-Hersteller, Lebensläufe - Berufsnetzwerke, Private Interessen – Social Media, ...).

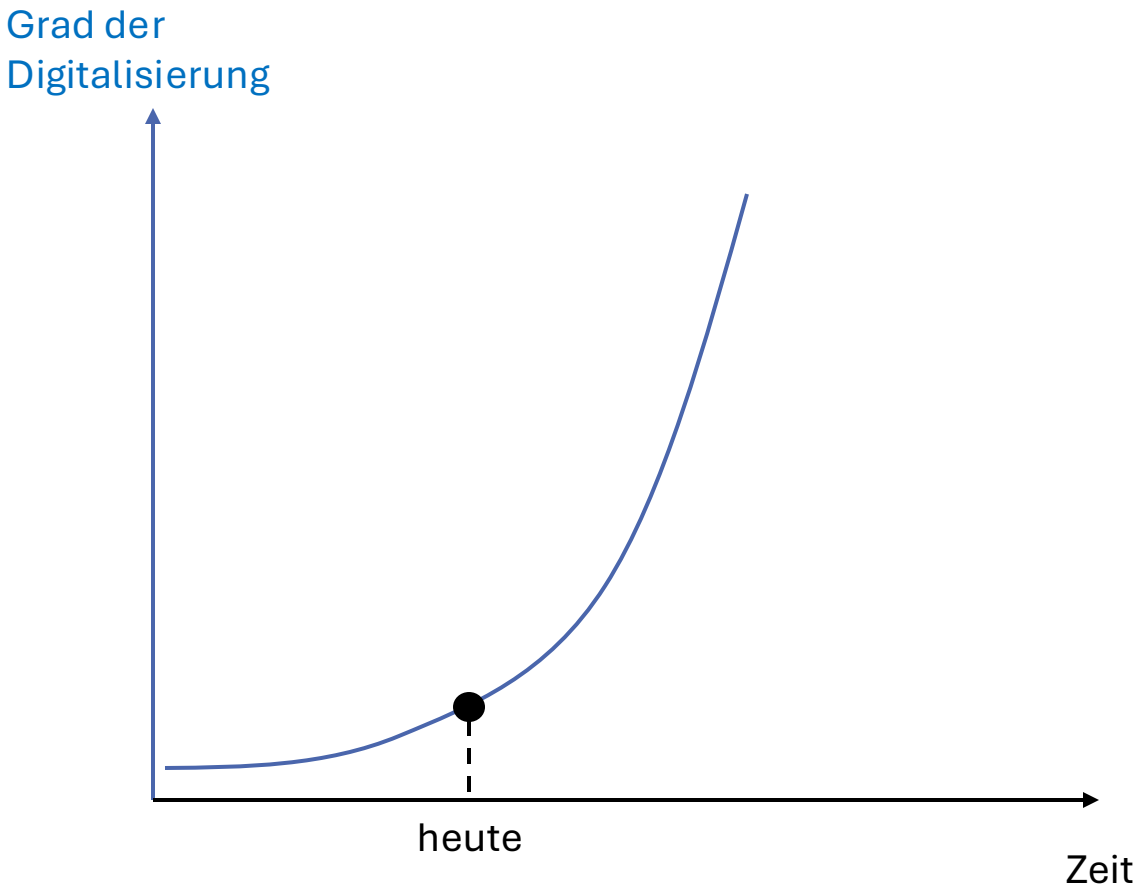


Verschwinden der Netzwerkgrenzen zwischen „Innen“ (sicheres Netzwerk) und „Außen“ (unsicheres Netzwerk).

Digitalisierung und neue Technologien

Erfolgsfaktoren der Digitalisierung

- Moderne Kommunikationsinfrastrukturen:
  - Funknetze 5G, WiFi-7
  - Smarte, mobile und leistungsfähige Endgeräte
  - Mobilen Sensoren in Produkten (Auto, Ski, Handy, ...)
  - Glasfaser-Hochgeschwindigkeitsnetzwerke
  - Leistungsfähigkeit zentraler IT-Systeme:
  - Cloud-Computing & Hyperscaler
  - Edge-Computing
- Echtzeitorientierte Integration von IT-Prozessen und IT-Systemen unternehmensübergreifend
- Moderne Benutzerschnittstellen (Sprache, Gestik ...)
- Einsatz von KI (ML ...) in Prozessen



"Wir sind erst am Anfang der Digitalisierung."

Big Data im Cyberraum

Big Data bezeichnet primär die Verarbeitung von großen, komplexen, zum großen Teil unstrukturierten (z.B.: Textdokumente, Bilder, ...) oder schwach strukturierten (z.B.: HTML, XML, JSON, ...) und sich schnell ändernden Daten.
Die Daten werden verteilt im Cyberraum verarbeitet und gespeichert.

- Web Tracking

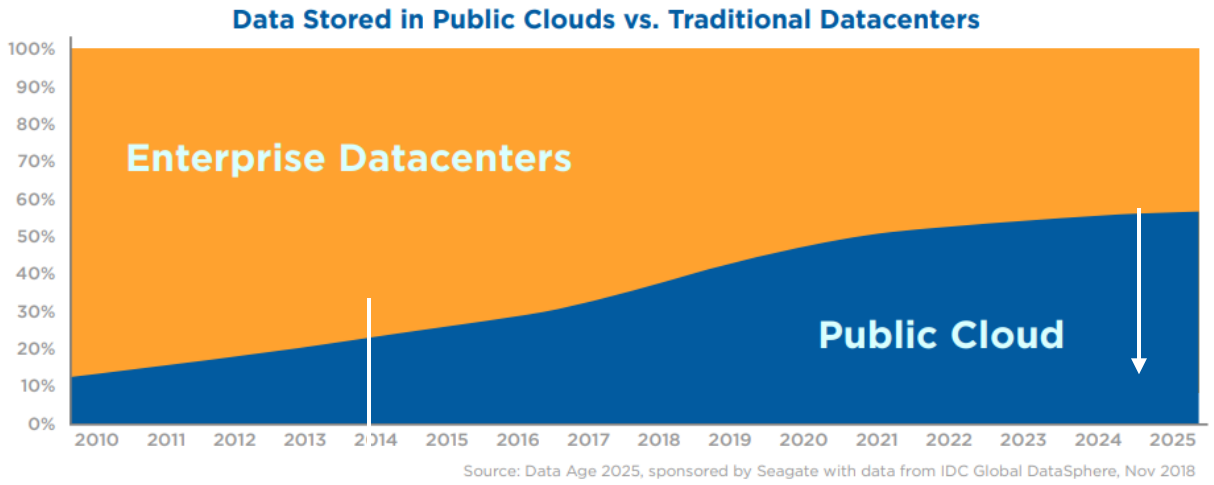
  Vermessung des Benutzerverhaltens (personenbezogene Daten) bei dem Einsatz von Software (APP, Web-Seiten, Plattformen,...) auf mobilen/stationären Geräten.

- Service Tracking

  Vermessen von Dienstleistungen (Lieferzeiten, Verfügbarkeitszeiten, Bearbeitungszeiten, Antwortzeiten, ...).

- Sensor Tracking (IoT)

  Vermessen von Produkten, Maschinen oder Menschen über Sensoren, um Informationen über die Nutzung und Qualität eines Produktes oder um Informationen von Vitalparameter eines Menschen zu sammeln. Diese Informationen spiegeln das Verhalten von Produkten bzw. Kunden wider.



Daten- und Prozessstandorte

Die Verarbeitung der Daten erfolgt im Cyberraum an 3 unterschiedlichen Datenstandorten stattfinden

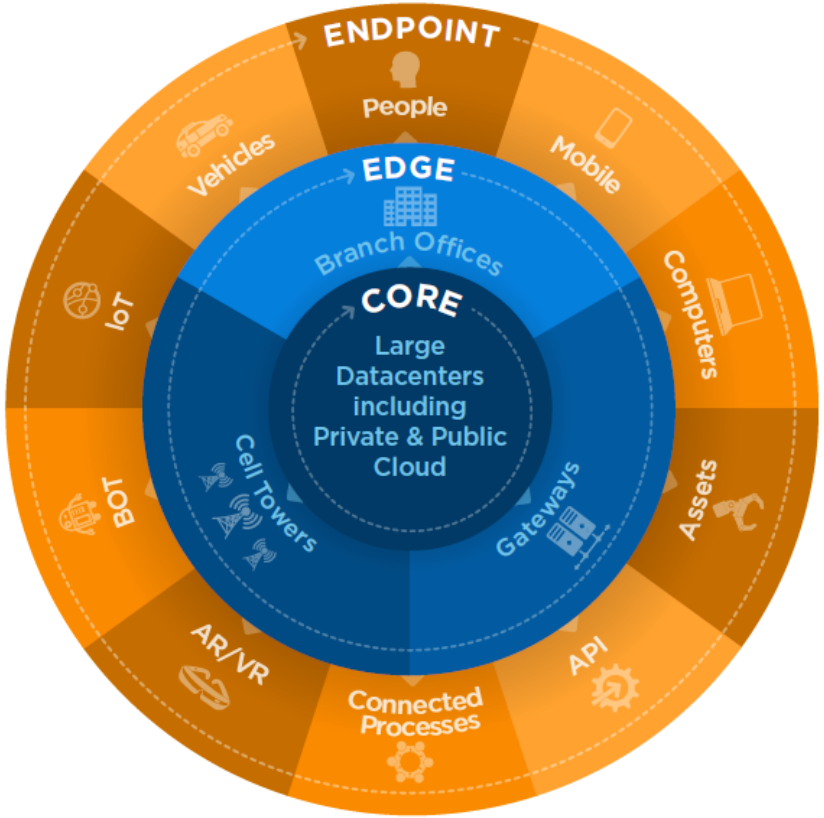
- Network Core (privat oder public):

  Speichern und Verarbeiten von Daten in unternehmenseigenen Rechenzentren oder in Rechenzentren von Cloud-Anbietern.

- Network Edge (privat oder public):

  Dezentrales Speichern und Verarbeiten von Daten durch gehärtete Server und Network-Appliances am Übergang (Edge) zum Internet, um schnellere Reaktionszeiten zu ermöglichen

  - Campus-Serverräume, Edge-Gateway-Server im Feld bei Kunden oder externen Dienstleistern
  - Mobilfunkmasten und verteilte kleinere Rechenzentren
  - Cloud-Rechenzentren



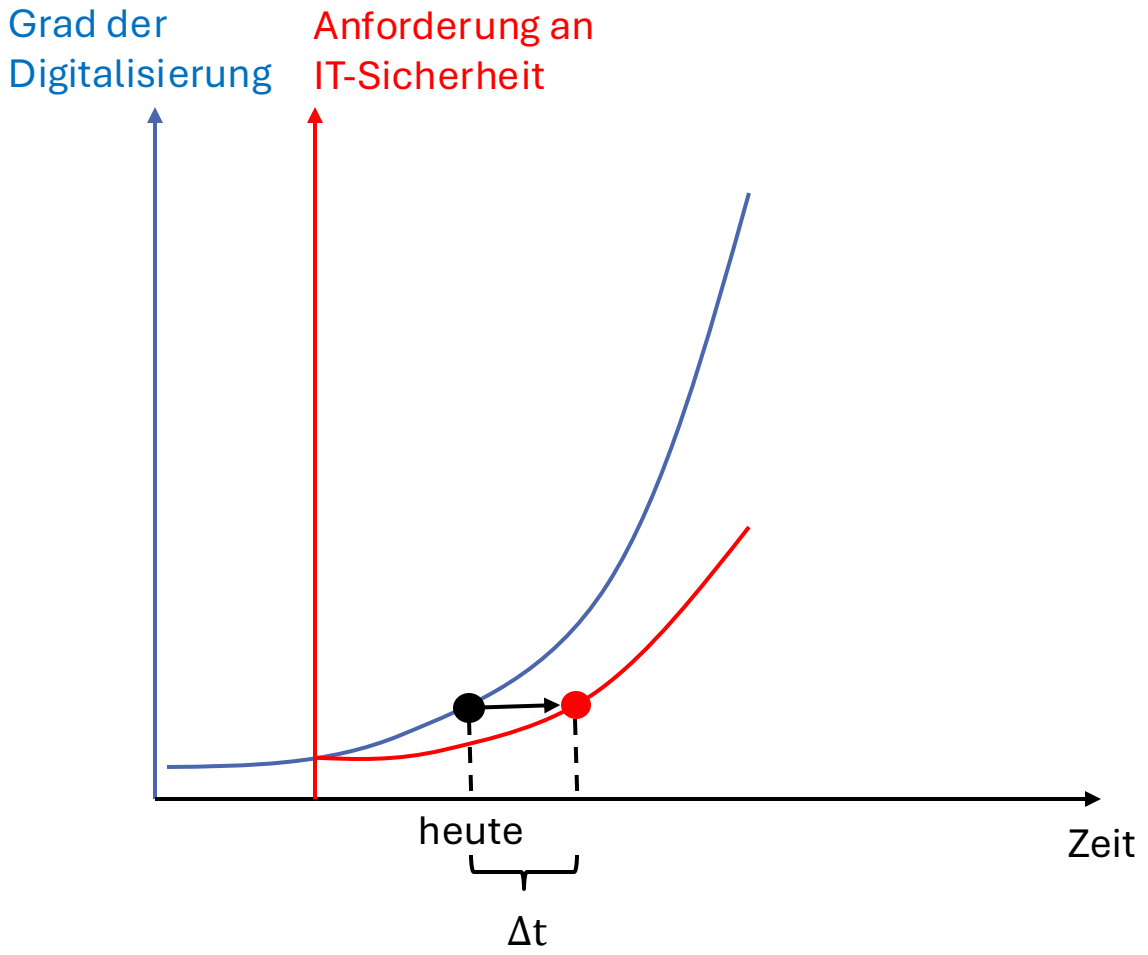
Source: IDC's Data Age 2025 study, sponsored by Seagate

- Endpunkte (privat oder public):

  Alle Endgeräte unabhängig von deren Standort wie PCs, Smart Phones, Wearables, Industriesensoren oder vernetzte Autos.

Digitalisierung und Cybersicherheit

- **Herausforderungen der Digitalisierung an die Cyber-Sicherheit**
  - Verbesserung der Softwarequalität- mehr Schutz vor Malware: Secure SDLC
  - Netzwerkauthentifizierung mit digitalen Zertifikaten und MFA-Authentifizierung mit FIDO2.
  - Verschlüsselter Nachrichtentransport (E-Mails, IPSec, TLS ...).
  - Sichere Architekturen für Netzwerke und Applikationen (Komponenten, Trusted Computing Plattform,, ...).
  - „Stand der Technik“-Sicherheitskomponenten für unterschiedliche Schutz-Szenarien.
  - Verfügbare (Redundanz) und sichere Hardware und Systeme ("Härtung").
  - Quantenkryptographie
  - Sichere KI

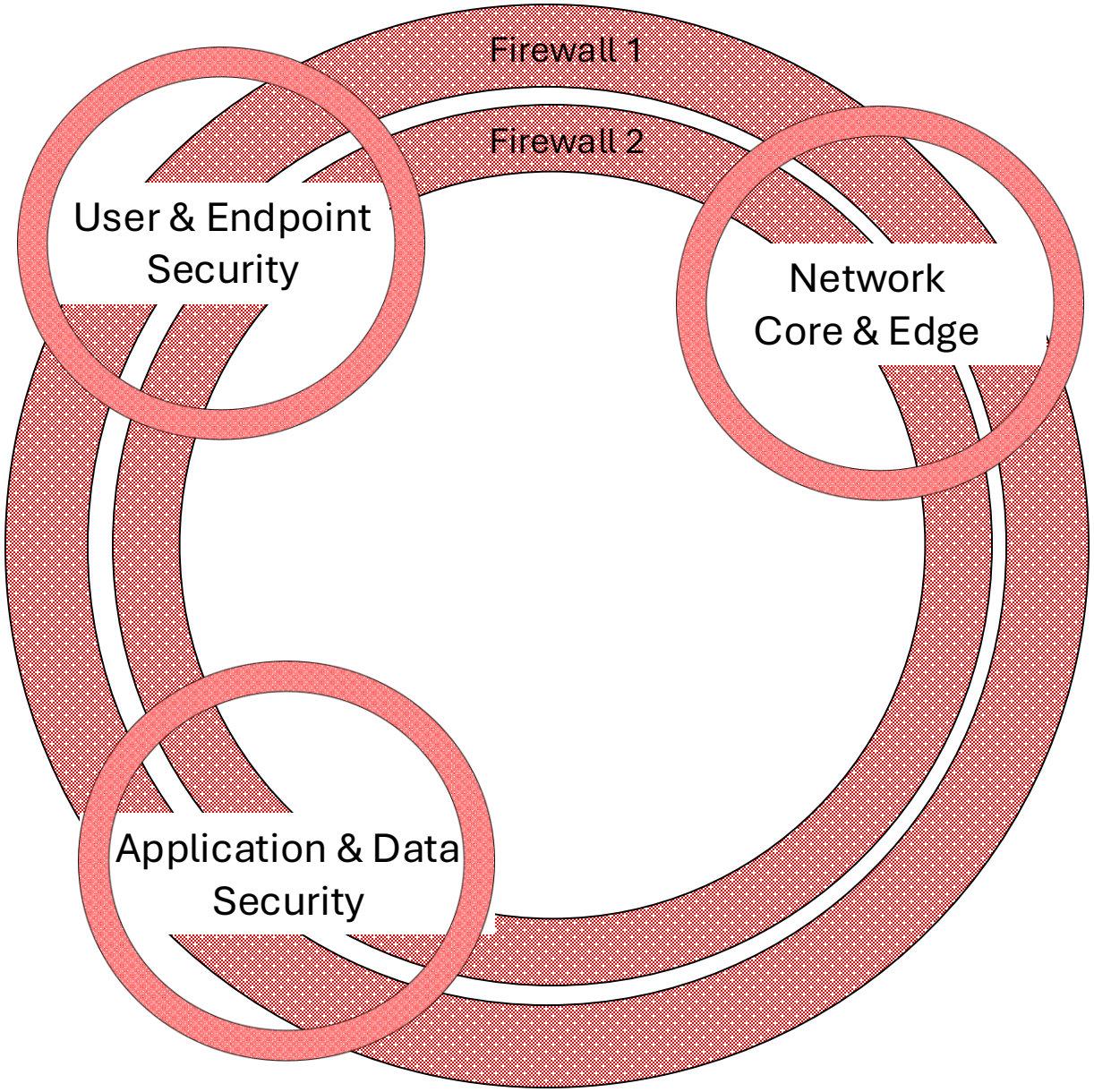


"Sicherheitsmaßnahmen laufen den Anforderungen hinterher."

Verbessertes Sicherheitsmodell: Zero-Trust

"Perimeter Sicherheit" & "Objektsicherheit"

- Da Daten außerhalb und innerhalb des Unternehmens-netzwerkes verarbeitet werden und die Endgeräte sich ebenfalls außerhalb und innerhalb des Unternehmens befinden können ist ein Ansatz, der nur auf die Sicherheit des internen Unternetzwerkes setzt nicht mehr aus-reichend.
- Ansatz: Zero-Trust-Sicherheitsmodell
  - Wie bisher - Perimeter-Sicherheit
  - Jedes konsumierte IT-Asset wird als extern und nicht vertrauenswürdig behandelt.
  - Jedes IT-Asset überprüft die Authentizität und die Berechtigung eines Zugriffs ("Access-Control") und besitzt geeignete Schutzmaßnahmen, um sich zu schützen.



Defense-in-Depth

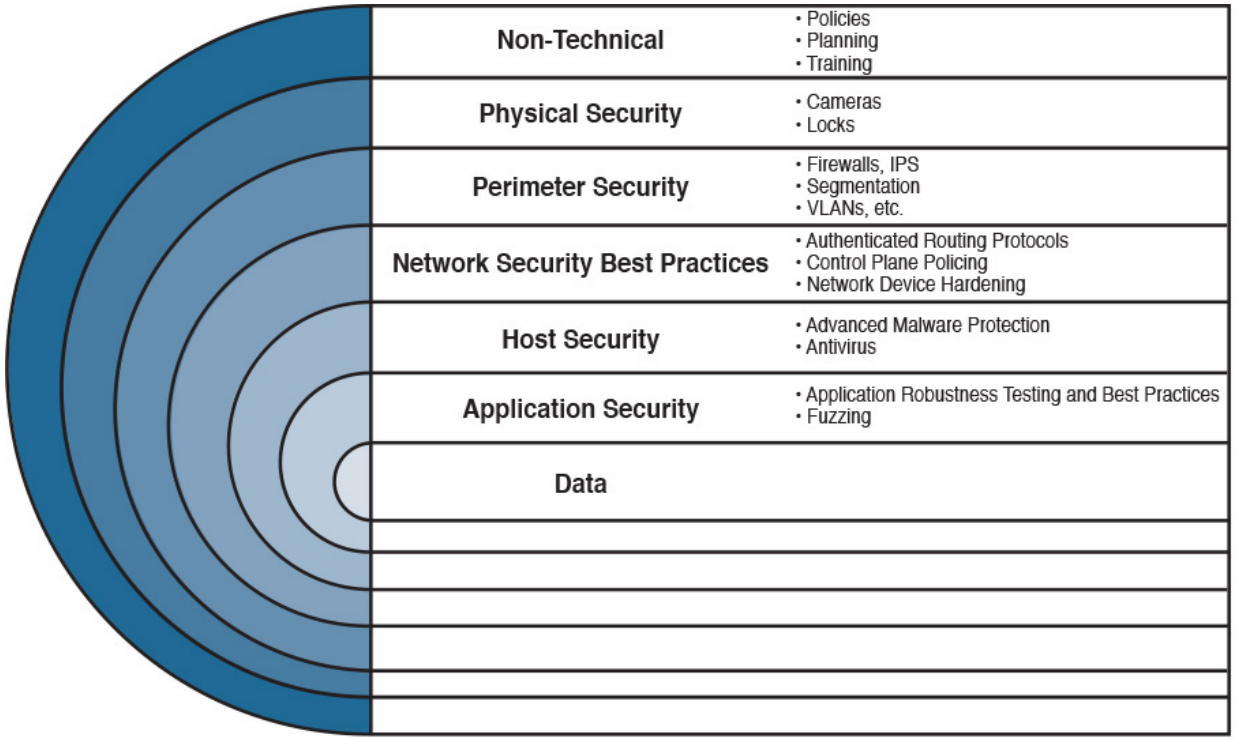
- Um eine Zero-Trust-Strategie für ein IT-Assets wirksam umzusetzen, reicht es nicht aus sich nur auf eine Sicherheitsmaßnahme zu verlassen.
- Idee: Mehrschichtige Verteidigungsmechanismen mit unterschiedlichen strategischen Wirkungen sind nötig.
  - Präventive Maßnahmen: Maßnahmen, die die Durchführung eines Angriffes erschweren oder verhindern.

    Beispiel: Zeitnahes Einspielen von Sicherheitspatchen
  - Detektierende Maßnahmen: Maßnahmen die zeitnah einen Cyber-Angriff erkennen.

    Beispiel: Logging aller Transaktionen und Anzeige in einem Leitstand.
  - Reaktive Maßnahmen: Maßnahmen die einen stattfinden Angriff eindämmen bzw. blockieren

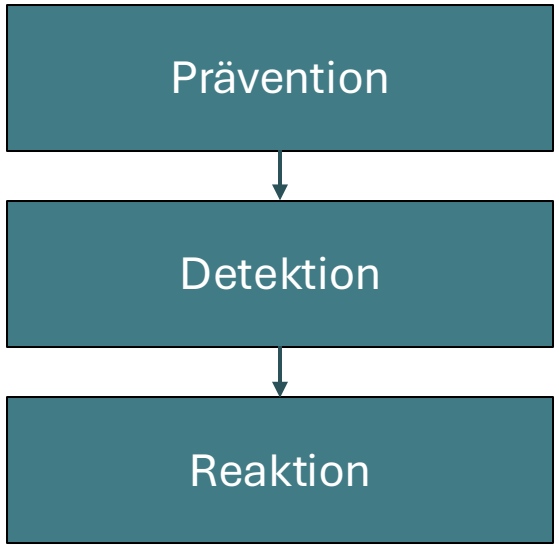
    Beispiel: Blockieren eines Netzwerkpaketes an einer FW.

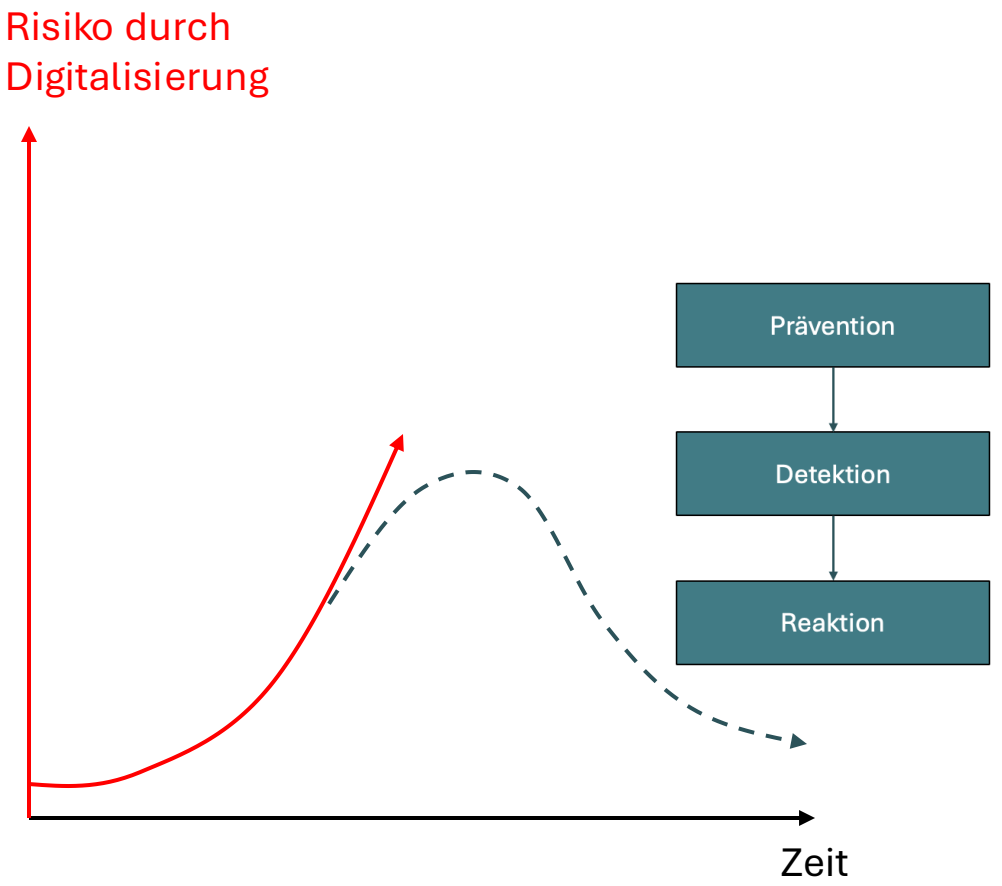
Security Principle: "Defense in Depth" ist ein Sicherheitsprinzip, das mehrere Ebenen von Sicherheitsmaßnahmen zum Schutz von Netzwerken einsetzt. Ziel ist die Schaffung eines mehrschichtigen Verteidigungssystems, das sicherstellt, dass bei einer Verletzung einer Ebene weitere Ebenen verbleiben, um einen Sicherheitsvorfall zu verhindern oder abzumildern.



Strategien zum Umgang mit Risiken

- Diese mehrschichtige Strategie hilft die vielfältigen Risiken der Digitalisierung zu reduzieren und zu beherrschen.



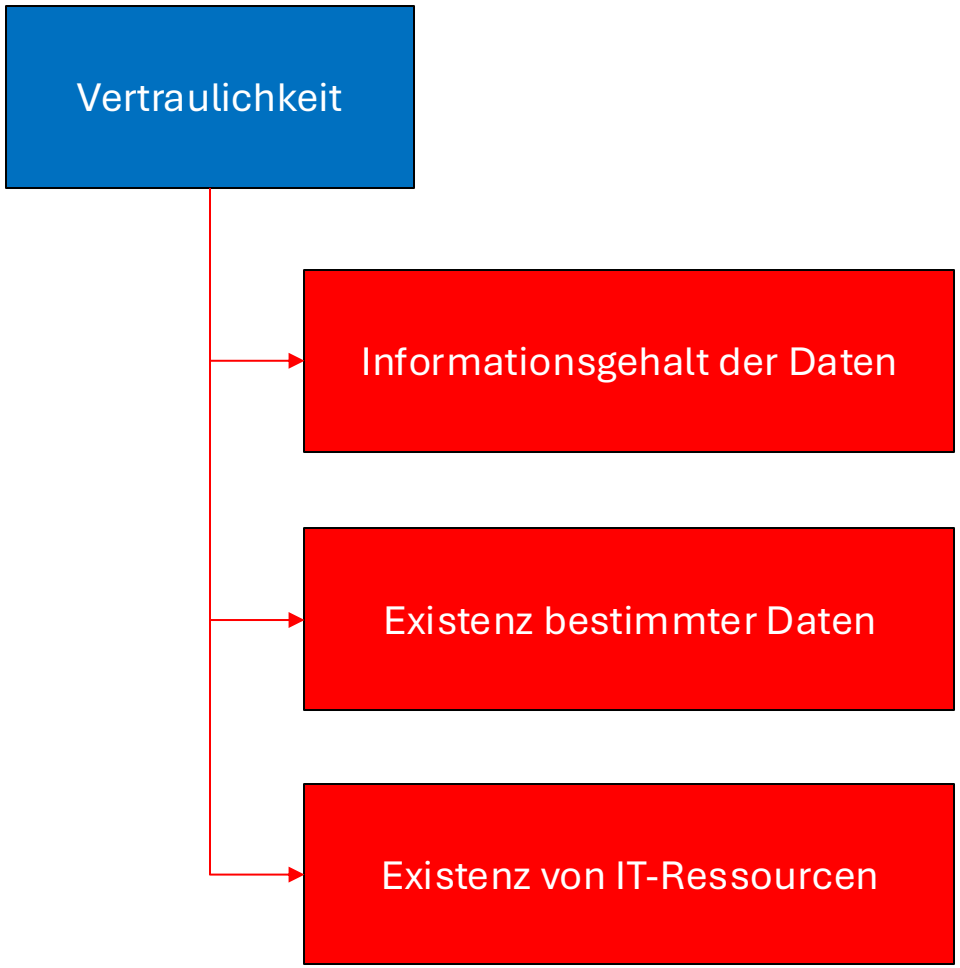


Vertraulichkeit (Confidentially)

Unter Vertraulichkeit versteht man

- das Verheimlichen von Informationen,
- das Verheimlichen der Existenz bestimmter Daten und
- das Verheimlichen der Existenz von Applikationen

- Vertraulichkeit muss durch präventive Maßnahmen durchgesetzt werden.
  - Verschüsselung von statischen Daten.
  - Verschlüsselung von dynamischen Daten.
- Präventive Systeme die Vertraulichkeit erzielen sind:
  - Kryptografische Protokolle (Verschlüsselung)
  - Segmentierung von Netzwerken durch FW, ….
  - Härtung von Systemen
  - Authentifizierung und Autorisierung von Zugriffen auf ein System.



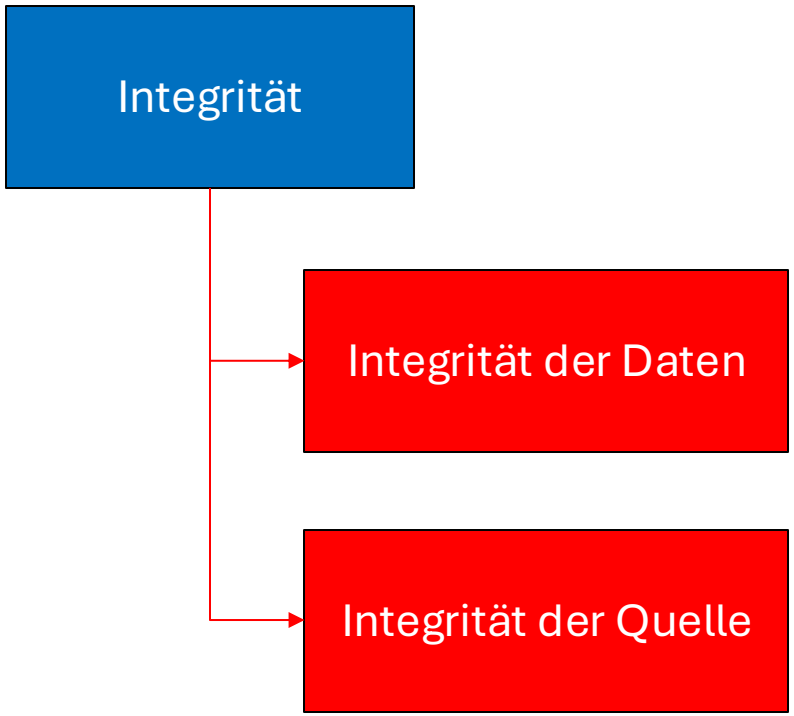
P: Verheimlichen durch Netzsegmentierung.
P: Verheimlichen durch Verschlüsseln.
P: Verheimlichen durch Anonymisierung.

Integrität (Integrity)

Unter Integrität versteht man das Verhindern von unzulässiger oder unbefugter Änderung

- von Daten oder Prozessen (Information, Verfügbarkeit)
- der Quelle von Daten (des Absenders)

- Präventionsmechanismen zielen darauf ab, die Integrität der Daten aufrechtzuerhalten, indem sie alle unbefugten Versuche, die Daten zu ändern, verhindern: Hash-Werte, White-Listing, Access-Control, digitale Zertifikate
- Detektionsmechanismen melden, dass die Integrität der Daten nicht mehr vertrauenswürdig ist. Dabei können Systemereignisse (Benutzer- oder Systemaktionen) oder (häufiger) die Daten selbst analysiert werden, um Verletzungen zu erkennen (Hash-Werte).
- Reaktive Mechanismen sind beispielsweise das Einspielen eines Backups.



P: Schützen vor Veränderung (RBAC, Least Privilege).

P: Schützen des Datenverkehrs durch Hash–Werte

D: Logging von Veränderung.

R: Wiederherstellen (Backup/Recovery).

Isolation von Systemen

- Eine Analyse von APT (Advanced Persistence Threats) zeigt, das diese über Anwendungsdomänen hinweg (horizontal) verlaufen.
  - Beispielsweise ermöglich ein gehackter Webserver Zugriff auf das lokale Netzwerk.
- Diese Erkenntnis führt zu einem wichtigen Security Principle nämlich dem "Least Common Mechanism"-Prinzip.

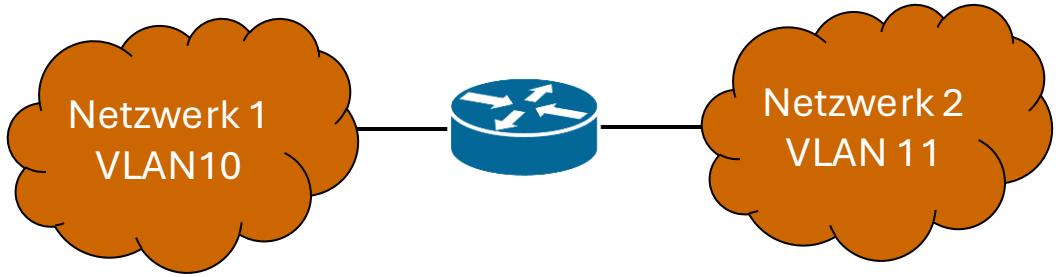
  Least Common Mechanism (Isolation): Zugriffskanäle auf Ressourcen sollten nicht zwischen unterschiedlichen IT-Assets (User, Devices,...) geteilt ("shared") werden.

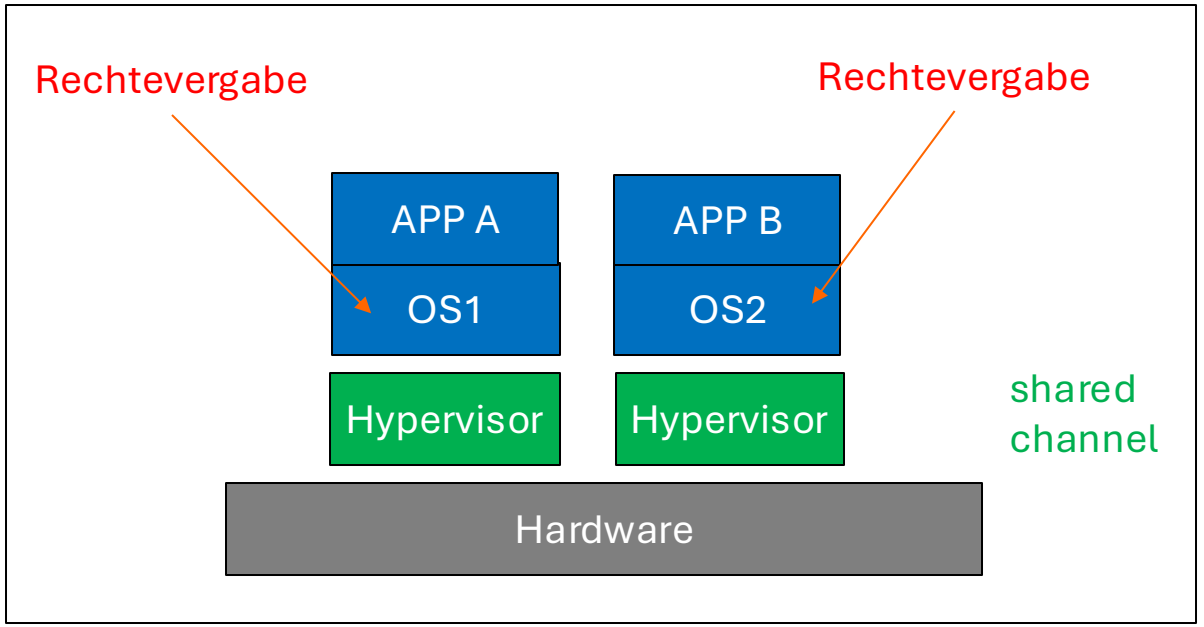
- Die gemeinsame Nutzung von Ressourcen stellt einen geteilten Kanal (shared channel) dar, über den Informationen unberechtigt gelesen, verändert oder sogar blockiert werden kann.
- Gemeinsame Ressource werden auch als covert channels oder side channels bezeichnet.
- Isolation (Segmentierung) ist ein Prinzip, das in drei Kontexten gilt.

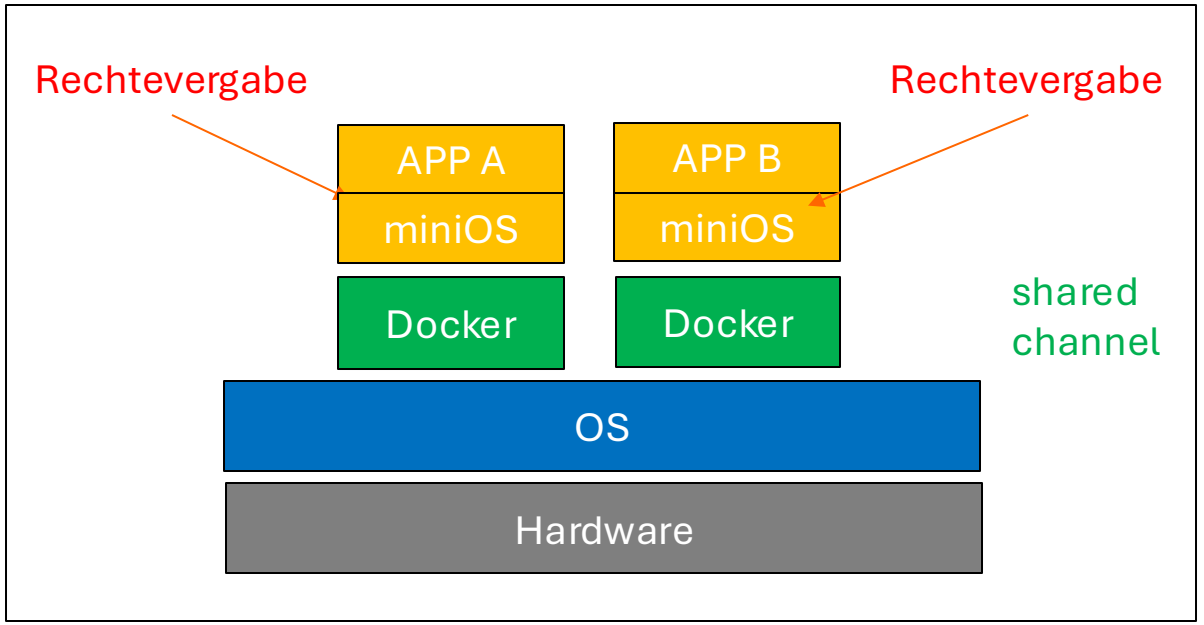
1. Öffentlich zugängliche Systeme müssen von kritischen Ressourcen (Daten, Prozesse usw.) isoliert werden, um die Offenlegung oder Manipulation zu verhindern.
2. Reduktion der Anzahl der Systeme und Benutzer, die Zugriff auf sensitive Daten und kritische Systeme erhalten sollen.
3. Prozesse und Daten mit unterschiedlichen Sicherheits-anforderungen sollten voneinander isoliert werden.

Isolation von Systemen

- Maßnahmen:
  - Die Trennung kann durch die physische Isolation also getrennte Netzwerke oder getrennte Betriebssysteme erfolgen. Die Kommunikation untereinander erfolgt über eine Sicherheit-Appliance (Router, Firewall, IPS, Hypervisor, TPC).
  - Die Trennung kann logisch erfolgen durch die Einrichtung virtueller Netzwerke (VLAN), oder beispielsweise durch den Einsatz von Port-Isolation auf Switchen, die es einem infizierten PC nicht ermöglich, die PCs seiner Kollegen ebenfalls zu infizieren.



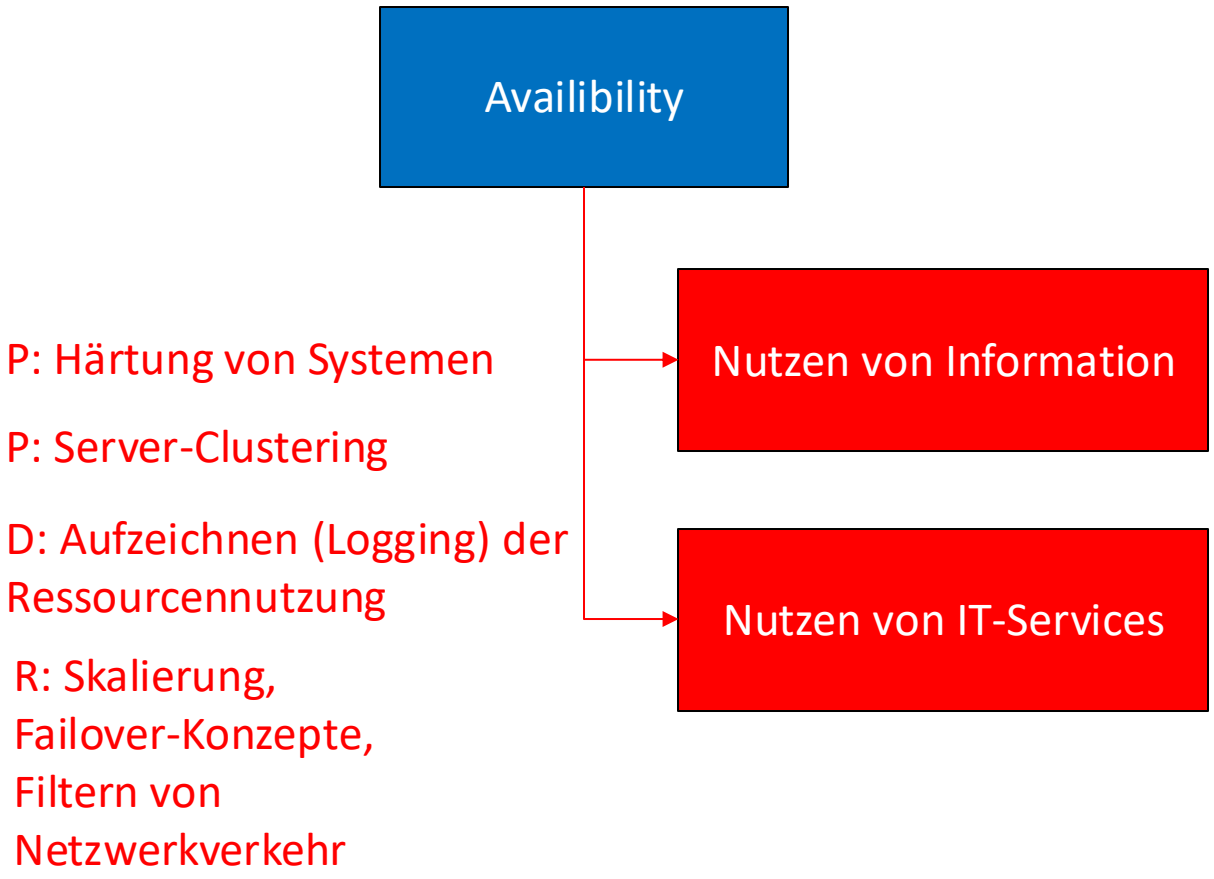




Verfügbarkeit (Availability)

Unter Verfügbarkeit versteht man die Fähigkeit, Informationen oder Services zu nutzen innerhalb eines definierten Zeitfensters (z.B.: Mo-Fr von 7.00 -18:00).

- Verfügbarkeit beinhaltet die präventive Planung eines zuverlässigen und sicheren Systemdesigns.
- Die Entwicklung eines zuverlässiges Systemdesign wird oftmals unter dem Begriff Safety zusammengefasst.
  Beispiele: Clustering, Load-Balancing, Redundanz im Netzwerk, ...
- Bei der Entwicklung eines sicheren Systemdesigns berücksichtigt man präventive Maßnahmen (SecSDLC, Härtung, Fail-Safe-Default,...), detektierende Maßnahmen (normaler vs. anormaler Netzwerktraffik, CPU-Nutzung, NetIO, DiskIO, ...) und reaktive Maßnahmen (DDos – Mitigation, TCP-Port-/IP-Address-Blocking, ...).



Minimize the Attack Surface

Security Principle :

Minimize the Attack Surface: Je kleiner die Angriffsfläche, desto sicherer ein Netzwerk (oder eine Anwendung).

- Die Größe der Angriffsfläche wird durch die Anzahl an möglichen Netzwerkzugänge (IP-Source und TCP-Port Destination) und die Anzahl der möglichen Schnittstellen APIs einer Applikation bestimmt.
- Das Risiko R für eine Applikation ist dann das Produkt aus

$$R = \text{Größe der Angriffsfläche x Wahrscheinlichkeit für einen Angriff pro Schnittstelle}$$

- Die Wahrscheinlichkeit eine Schnittstelle auszunutzen ist immer größer als Null.

- Beobachtungen im IT-Betrieb:
  - Angriffsflächen neigen dazu, zu wachsen, wenn sie nicht bewusst/gezielt reduziert werden.
  - Es besteht erheblicher fachlicher Druck, neue Einstiegspunkte in Netzwerke oder Applikationen zu generieren in Form von neuer Konnektivität, neuen Funktionen, neuen APIs, ...
  - z.B.: Firewall wird zum Schweizer Käse !
- Die Reduzierung der Angriffsfläche von bestehendem Code kann einen erheblichen Ressourceneinsatz erfordern (ggf. komplettes Re-Design).
  - Ansatz: Secure Software Development Lifecycle (Secure SDLC). Sicherheit wird von Anfang an bei der Entwicklung einer Software berücksichtigt: Requirement, Design, Coding, Testing, Integration, Betrieb

Minimize the Attack Surface: Härtung

- Das Minimieren der Attack Surface eines Systems wird auch als Härtung des Systems bezeichnet.
- Beispiel für Härtung von Systemen
  - Reduktion der Anzahl der offenen Netzwerk-Ports in einer FW oder auf einem System.
  - Reduktion der Anzahl an installierten Softwarekomponenten auf einem System.
  - Entfernen nicht mehr benötigte Dienste auf einem System (Risiko: veraltete Dienste die nicht mehr gepatched werden)
  - Reduktion der Anzahl der standardmäßig ausgeführten Dienste reduzieren. Selten benötigte Dienste nur bei Bedarf starten.
  - Reduktion der Privilegien von Diensten auf einem System (Dienst-Account mit minimalen Rechten anstatt Admin-Account)
  - Reduktion der Anzahl an Konten mit Adminrechten.
  - Reduktion der Anzahl an Hardwareschnittstellen (USB, AUX, ...) Softwareschnittstellen auf einem System.
  - Reduktion der Anzahl an Third-Party-Treibern auf einem System
  - Secure-Boot von Systemen mit zertifizierten Treibern.
  - Verwenden von Mikrokernels mit einer geringen Anzahl an Code-Zeilen (20.000) als Trusted Computing Base (TCB) für ein Betriebssystem.
  - Remote-Administration eines Systems nur über sichere Protokolle (ssh, https).
  - Schutz von Dateien & Verzeichnissen durch die konsequente Vergabe von Zugriffsrechten (RBAC).
  - Schutz von Funktionen in Applikationen durch die konsequente Vergabe von Zugriffsrechten (RBAC).

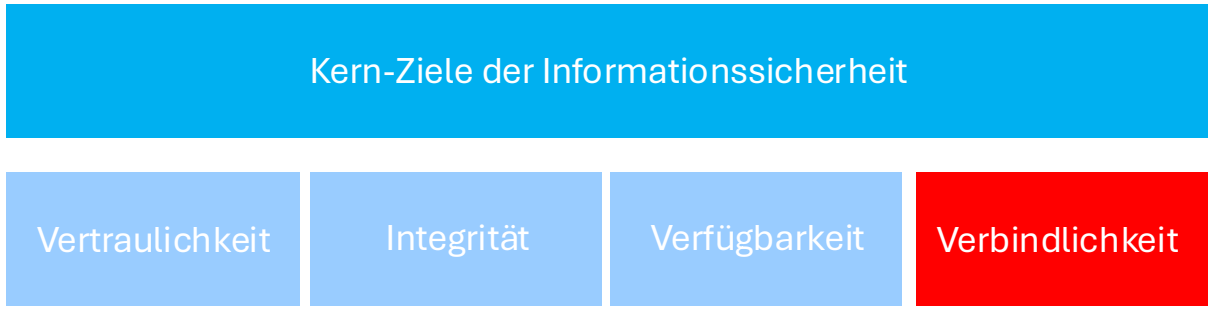
Verbindlichkeit (Non-repudiation)

- Die 3 Schutzziele werden durch ein weiteres Schutzziel "Verbindlichkeit" ergänzt.

Unter Verbindlichkeit (Non-Repudiation) versteht man, dass es möglich sein muss, Handlungen eindeutig dem zuzuordnen, der sie ausgeführt hat.

- Die elementaren Schutzziele für ein Unternehmens-netzwerk lassen sich wie folgt zusammenfassen :
  - Vertraulichkeit (**C**onfidentiality) von Daten und Diensten
  - Integrität (**I**ntegrity) von Daten und Diensten
  - Verfügbarkeit (**A**vailability) von Daten und Diensten
  - Verbindlichkeit oder Unbestreitbarkeit (**N**on-Repudiation oder Accountability) von Transaktionen und Transaktionsteilnehmern

CIAA-Kernziele



P: Digitale Signaturen und CA/PKI

P: Authentifizierung und Autorisierung für jeden Zugriff

P: Verschlüsselung und Integritätssicherung des Datenverkehrs

D: Aufzeichnen aller Benutzertransaktionen in zentralem Logfile

D: Analyse (Korrelation) der aufgezeichneten Logdaten auf Anomalien

R: Sperren von Diensten

Safety

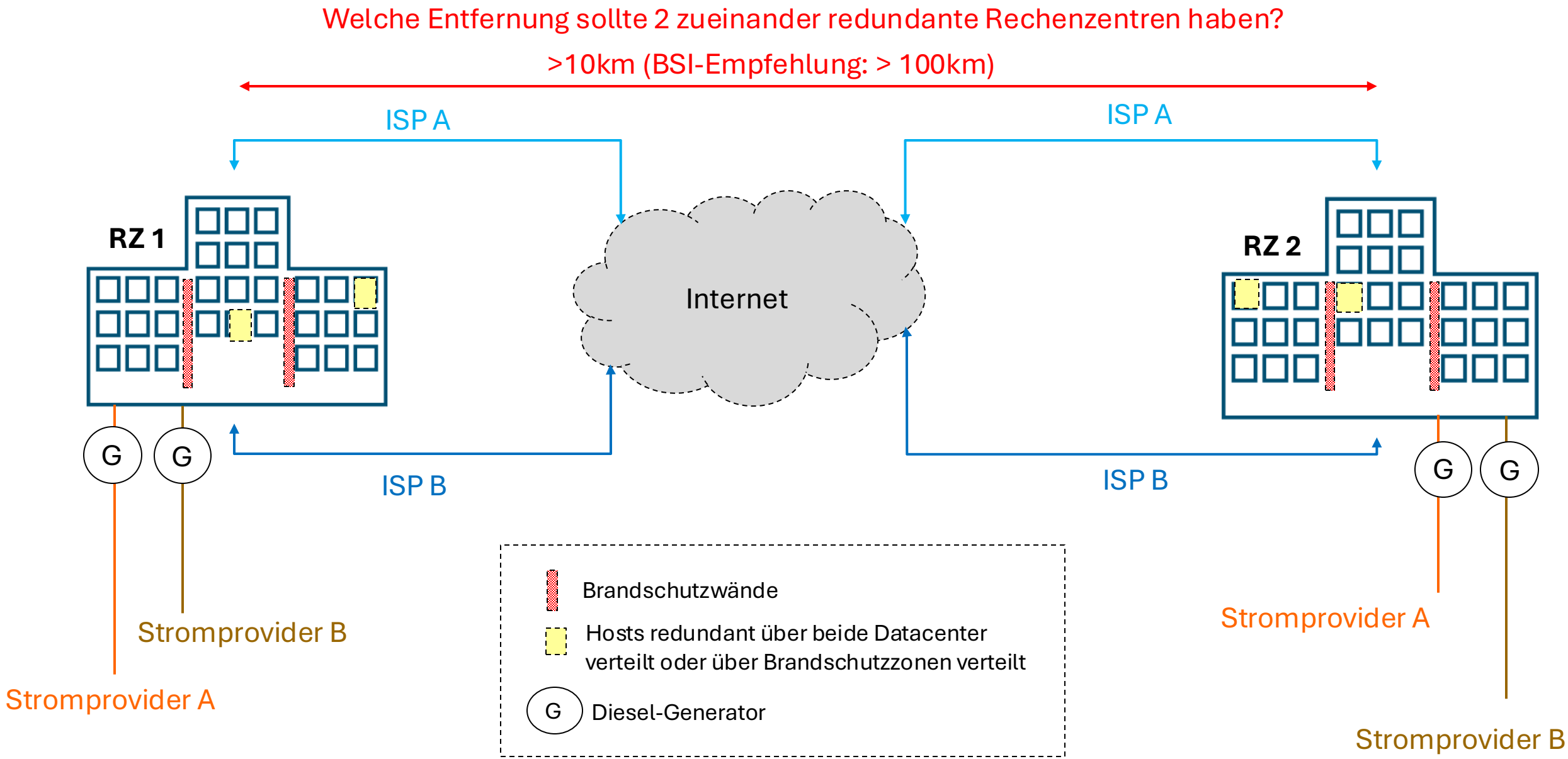
Unter Safety (Betriebssicherheit) versteht man die Gesamtheit aller Maßnahmen zur Minderung der Schadensauswirkung von unvorsehbaren Ereignissen und zur Vermeidung oder Milderung von Betriebsfehlern.

Beispiele für unvorhersehbare Ereignisse sind

- Naturkatastrophen wie z.B.: Feuer, Überschwemmungen, Wirbelstürme oder Pandemien
- Technische Fehler wie z.B. Ausfall der Klimatisierung im Rechenzentrum, Ausfall von Serverhardware, Ausfall der Stromversorgung, Ausfall der Anbindung an das Internet.
- Menschliche Fehler wie z.B. Fehlbedienung beispielsweise ein versehentlicher Reboot eines Servers oder falsche Konfiguration eines Routers, Drücken des Not-Aus-Schalter in RZ, ...,

- Proaktive Maßnahmen: Redundante Auslegung von Rechenzentren und Hardwarekomponenten. Redundante Anbindung ans Internet und an die Stromversorgung über 2 Leitungen und 2 verschiedene Provider. Redundante Verkabelung im Netzwerk. Schulung und Zertifizierung von Mitarbeiter.
- Detektierende Maßnahmen: Maßnahmen, um einen Ausfall schnell zu erkennen z.B.: Monitoring der Strom-, Kühl-Infrastruktur, Monitoring der Temperatur,...
- Reaktive Maßnahmen: Gaslöschanlagen zur Brandbekämpfung, Umschalten der Systeme in ein Backup-RZ, Incident-Response-Management zur strukturierten schnellen Problem-Behebung.

Beispiel: Safety – Georedundanz von Rechenzentren



Privacy – Datenschutz

Unter Privacy versteht man die Gesamtheit aller Maßnahmen zur Verhinderung der unautorisierten Verarbeitung bzw. dem unautorisierten Zugriff auf personenbezogene Daten.

Personenbezogene Daten sind immer dann vorhanden, wenn sie persönliche oder sachliche Informationen über eine natürliche Person verarbeiten. Dazu muss die Person nicht namentlich benannt werden. Es genügt, wenn diese bestimmbar wird:

- IP-/MAC-Adresse Adresse ihres Notebooks
- Geräte-ID ihres Smart-Phones
- GPS-Daten, Zuordnung Handy Mobilfunkmast
- E-Mail-Adresse
- Telefonnummer
- Active-Directory-Account
- Cookie
- ...

- Proaktive Maßnahmen:
  - Anwender: Whitelisting von datensparsamen Apps, Analyse der Datenschutzerklärungen des jeweiligen Anbieters, ...
  - Unternehmen: Verschlüsselung und Pseudonymisierung von personenbezogenen Daten, Authentifizierung und Autorisierung, Backup von Daten, ...
- Detektierende Maßnahmen:
  - Anwender: Adware-Blocker, Privacy-Blocker, ...
  - Unternehmen: Monitoring von Datenzugriffen, Monitoring von Datenflüssen
- Reaktive Maßnahmen:
  - Meldung von Datenschutzverletzungen
  - IPS-Systeme, Firewall, ...
  - Restore von Daten

Complete Mediation and AAA

Security Principle : "Complete Mediation"

Die Kernziele der IS sind in einem Unternehmensnetzwerk nur erfüllbar, wenn gewährleistet ist, das bei jedem Zugriff auf eine IT-Ressource (Software, Hardware, Daten, Gebäude), eine Zugriffskontrolle (Access Control) erfolgt.

- Die Access Control setzt sich aus den folgenden 2 Sicherheitsdienste zusammen:
  - Authentication (Authentifizierung) der behaupteten Identität (z.B.: Benutzername, MAC-Adresse) einer zugreifenden Person/eines zugreifenden Geräts.
  - Authorization (Autorisierung) also zuweisen von Rechten
- Um nachzuweisen das eine bestimmte Aktion von einer bestimmten Person durchgeführt wurde, benötigt man noch einen Accountability (Auditing)-Dienst, der jeder Aktion aufzeichnet.

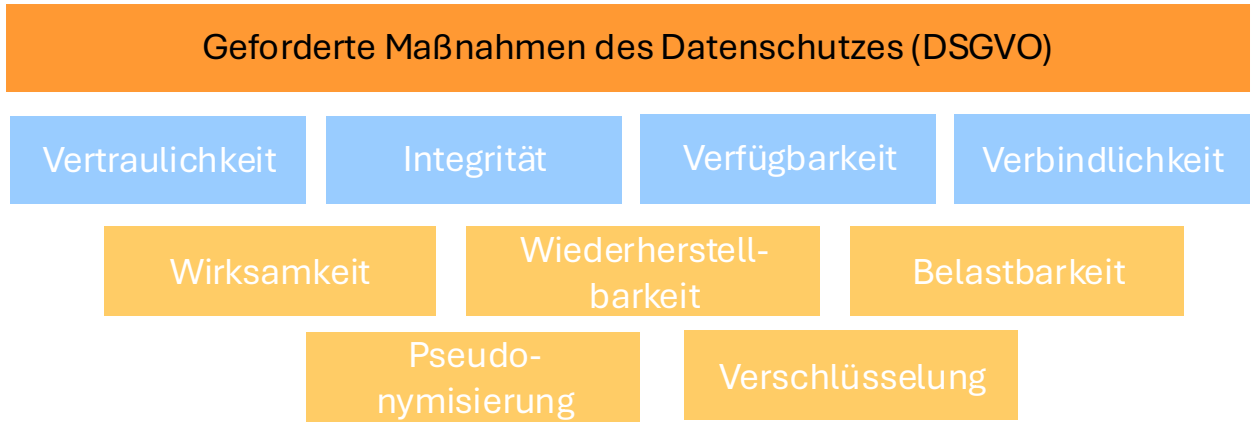
- IT-Systeme, die diese Sicherheitsmaßnahmen bereitstellen, werden auch als Triple-A-Systeme bezeichnet.

A + A + A

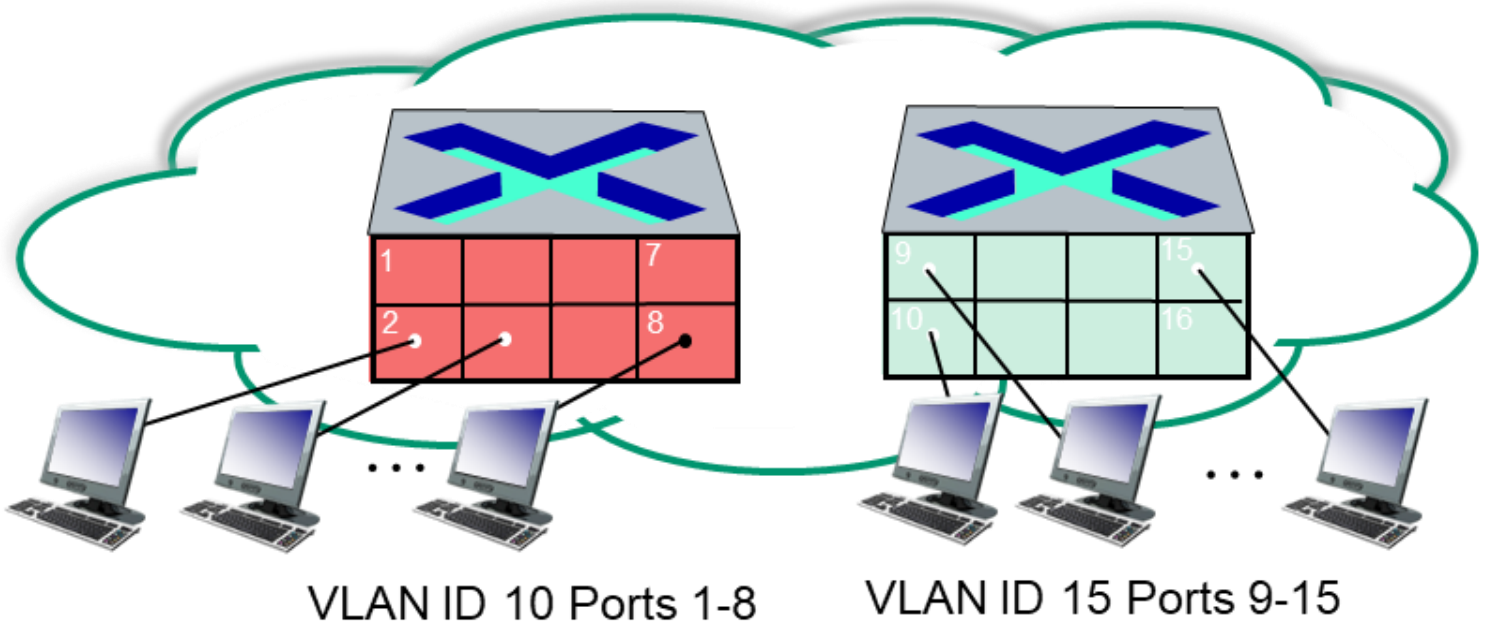
Generell sollten alle IT-Systeme die Triple-A-Services selbst besitzen oder diese von vorhandenen zentralen Triple-A-Systemen beziehen.

EU-Datenschutzverordnung und TOM

- Die EU-Datenschutzgrundverordnung (EU-DSGVO) verlangt von Unternehmen die personenbezogenen Daten verarbeiten, die Dokumentation und die Umsetzung von Technisch Organisatorischen Maßnahmen (TOM).
- Für die TOM-Maßnahmen werden zusätzlich zu den Kernzielen der IS, die folgenden Maßnahmen zum Schutz der personenbezogenen Daten (Art. 32 DSGVO) gefordert:
  (1) Pseudonymisierung der personenbezogenen Daten
  (2) Verschlüsselung der personenbezogenen Daten
  (3) Belastbarkeit der Systeme (z.B.: Performancetest)
  (4) Wiederherstellbarkeit pers. Daten (z.B.: Restore-Übung)
  (5) Nachweis der Wirksamkeit der umgesetzten Sicherheitsmaßnahmen (z.B.: PenTest, interne Tests)

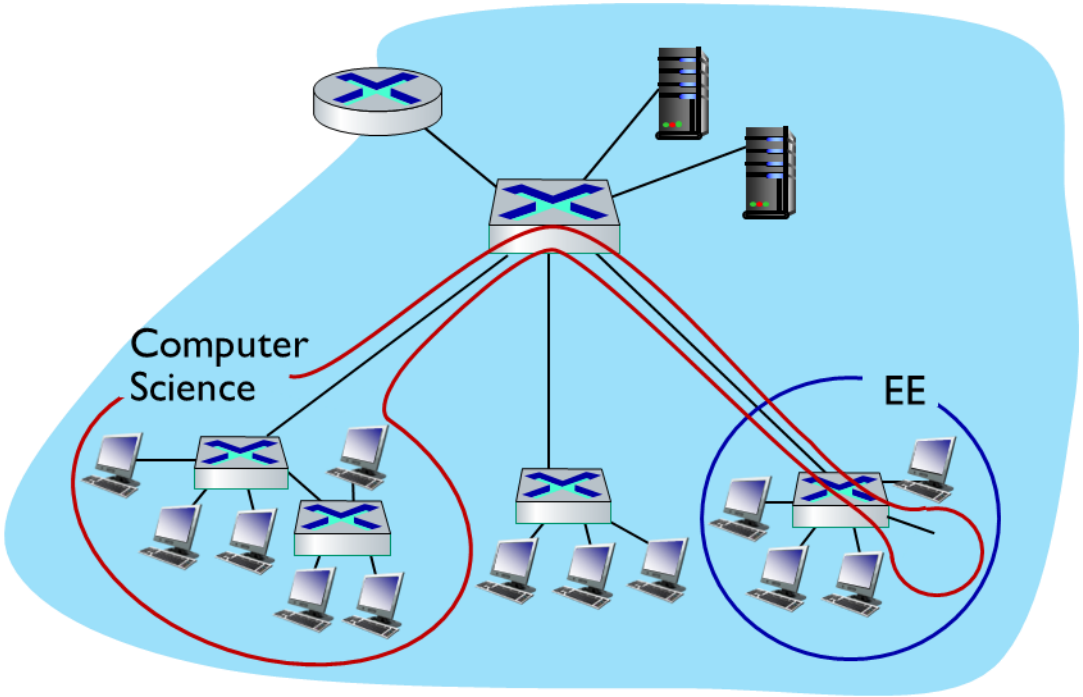


1.2 Segmentierung von LAN mittels Virtuellen Netzwerken



Virtual LANs (VLANs): Motivation

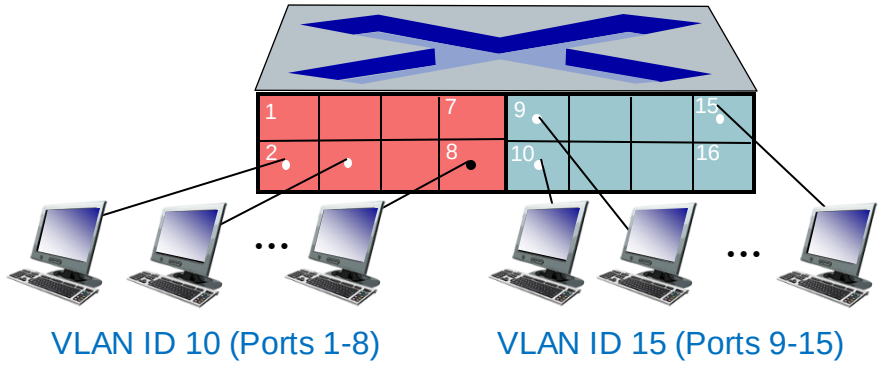
- Warum Virtual LANs (VLANs)?
- Fehlende Verkehrsisolation:
  - In Stern-Stern-Topologie verbundene Switche bilden bezüglich Broadcast-/Multicast-Verkehr eine switch-übergreifende Broadcast-Domäne (ARP-Request, Flooding, ...)
  - Um den Datenverkehr von Arbeitsgruppen oder Systemen mit unterschiedlichen Sicherheitsanforderungen) zu trennen, wird ohne VLANs ein eigener physikalischer Switch benötigt, was hohe Kosten und hohe Managementaufwände erzeugt.
- Ineffiziente Verwendung von Switches:
  - Physikalische Switche sind sehr leistungsfähig und können eine große Anzahl an Geräten bedienen.

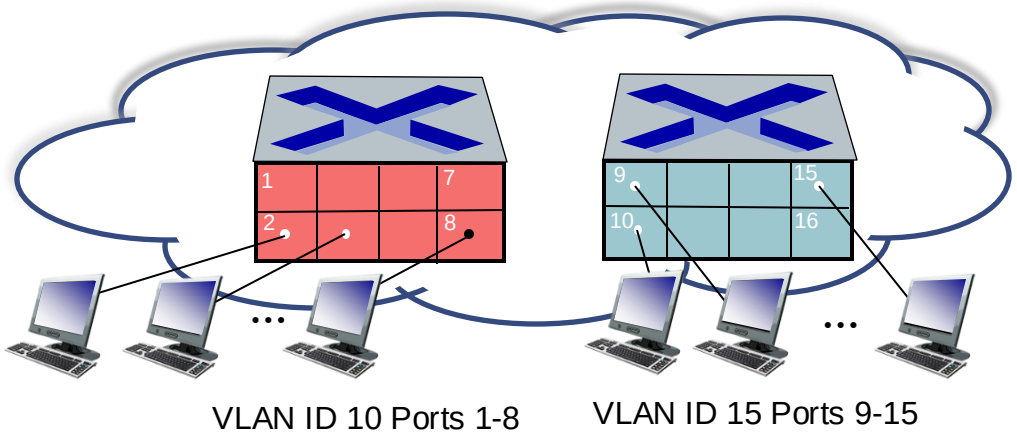


- Verbindungsmanagement: Wenn ein Teil einer Arbeitsgruppe das Büro wechselt, muss ggf. die physische Verkabelung geändert werden, um die Mitarbeiter mit "ihrem Abteilungs-Switch" zu verbinden.

Port-Based VLANs

- Switche können per Software so konfiguriert werden, das Sie mehrere Subnetze über eine einzige physikalische Switch-Hardware anbieten.
- Port-based VLAN: Ports eines Switches erhalten per Software eine sogenannte VLAN ID.
- Jede VLAN ID stellt ein eigenes Subnetz dar.
- Beispiel: siehe Bild
  - Die Ports 1 – 8 werden dem VLAN 10, die Port 9 – 15 werden dem VLAN 15 zugeordnet.
  - Isolierung des Netzwerkverkehrs: Eingehende Frames von Port 1 – 8 können nur auf die Ausgangsports Ports 1 – 8 weitergeleitet, analog für die Ports 9 -15
  - Broadcast-Verkehr in VLAN10 erreicht nicht die Ports des VLAN 15.
  - Switch verhält sich wie zwei getrennte physikalische Switche.



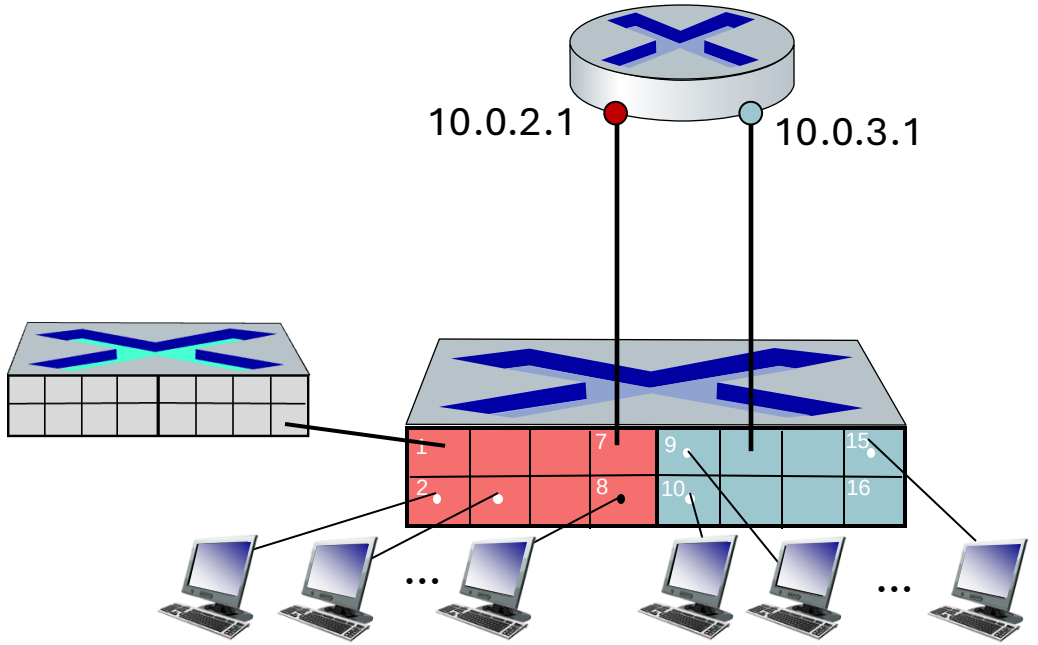


Konfiguration und Weiterleitung in VLANs

- Jeder Switch-Port kann einem anderen VLAN zugeordnet werden.
- Konfiguration für CISCO IOS

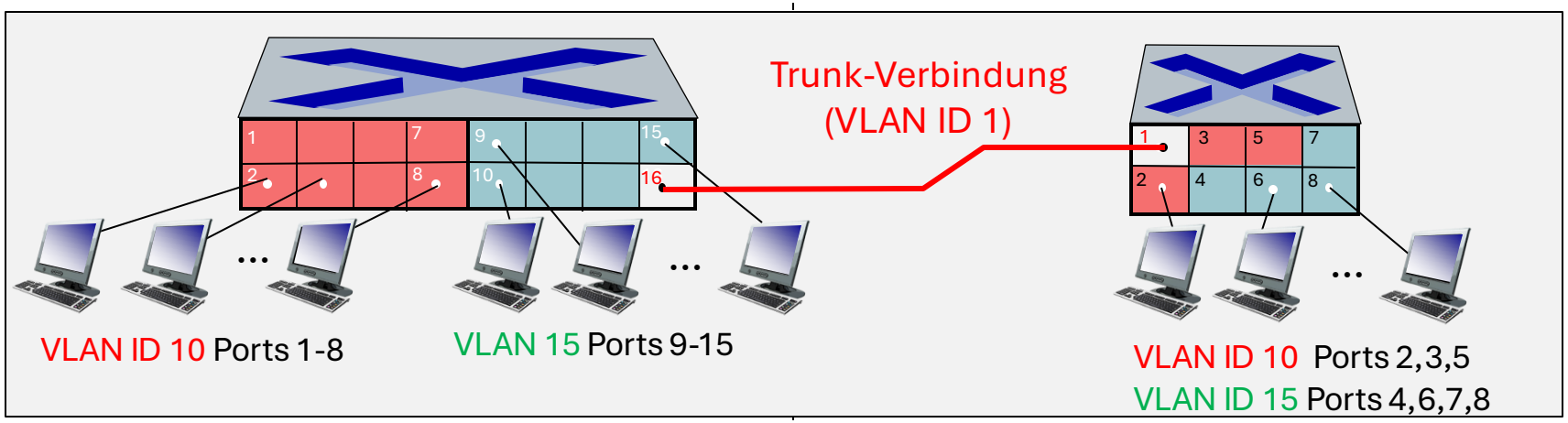
```
S1(config)# interface eth0/1 – 8
S1(config-if)# switchport access vlan 10

S1(config)# interface eth0/9 – 15
S1(config-if)# switchport access vlan 15
```

- Die Paketvermittlung zwischen VLANs kann nur über Layer-3 Routing erfolgen, wie bei physikalischen Switchen, die sich in separaten Subnetzen befinden.
- Den Hosts eines VLANs müssen IP-Adressen von unterschiedlichen Subnetzwerken zugeordnet werden.
- In der Praxis verkaufen Anbieter kombinierte Switche sogenannte L3-Switche: Router & Switch



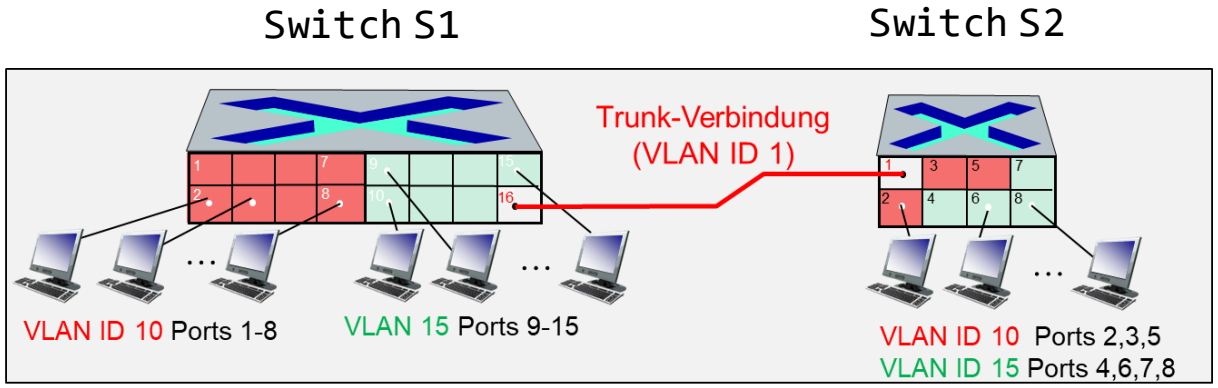
VLANs und mehrere Switche

- Wie können nun Daten auf Layer2 zwischen Hosts eines VLANs ausgetauscht werden, wenn dieses VLAN sich über mehrere Switche verteilt.
- VLAN Trunking: Auf jedem Switch wird ein spezieller Port als sogenannter Trunk Port definiert.
- Der Trunk-Port gehört zu allen VLANs.
- Frames, die innerhalb eines VLANs einen Empfänger adressieren, der mit einem anderen Switch mit derselben VLAN ID verbunden ist, können über die Trunk-Verbindung an diesen Switch weitergeleitet werden.
- Dazu wird der Ethernet-Header um ein sogenanntes VLAN-Tag erweitert.



VLAN Tagging

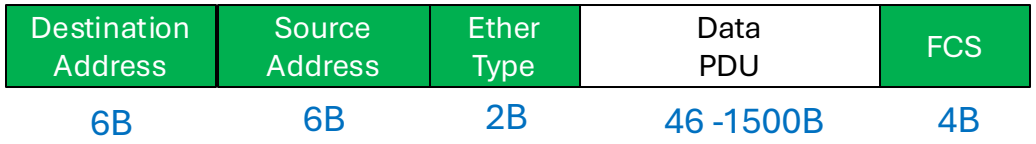
- VLAN Tagging: Erweiterung des Ethernet Frame Formates, um einen VLAN-Header der die VLAN ID enthält.
- Ein VLAN-Tagging kommt dann zum Einsatz, wenn ein Frame an einen Trunk-Port weitergeleitet wird.
- Das VLAN-Tag wird vom Switch auf der sendenden Seite eines VLAN-Trunks in einen Ethernet-Frame eingefügt (gekapselt), und vom Switch auf der empfangenden Seite des Trunks ausgewertet und entfernt.
- Ein Trunk-Port besitzt eine sogenannte native VLAN ID. Für dieses VLAN erfolgt kein VLAN-Tagging. Der Default-Wert beträgt 1 und sollte geändert werden.
- IEEE802.1Q - Standard definiert die Erweiterung des Ethernets Headers.



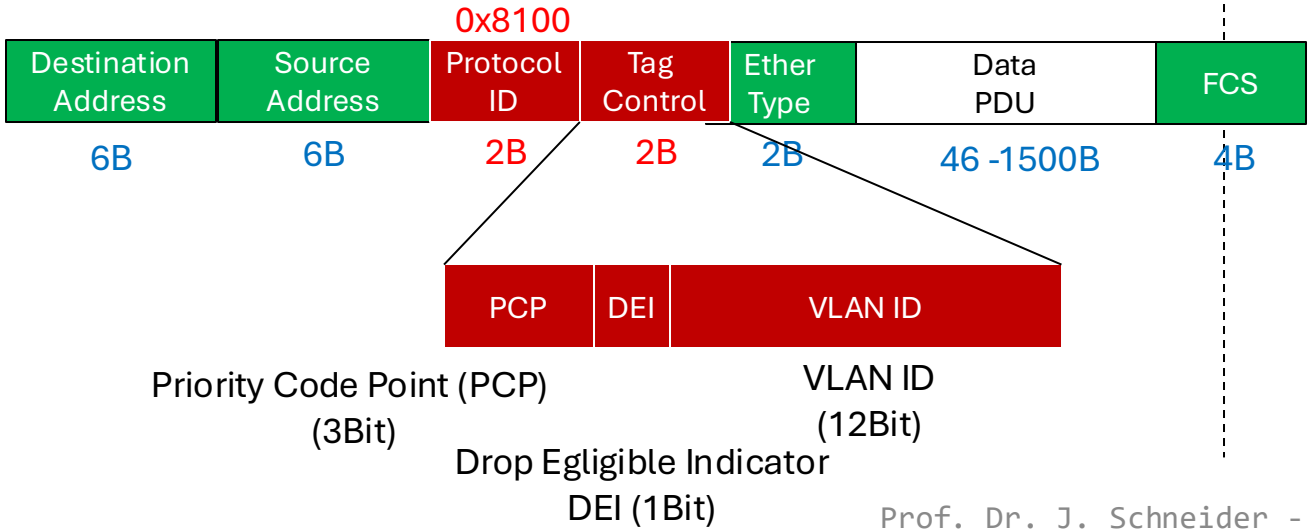

```
! Specify the interface for trunk port
S1(config)# interface eth0/16
! Set the interface as a trunk port
S1(config-if)# switchport mode trunk
! Set the encapsulation method to IEEE 802.1Q
S1(config-if)# switchport trunk encapsulation dot1q
!Set Native VLAN ID to 99
S1(config-if)# switchport trunk native vlan 99
```

802.1Q VLAN Tagging Frame Format

- Vor das Ethertype-Feld wird ein 4Byte großes Headerfeld eingeschoben
- Das Headerfeld besteht aus einer Protocol-ID und einer Tag Control Information.
- Das Protocol-ID-Datenfeld (2 Byte) wird bei 802.1Q-VLANs immer auf den Wert 0x8100 gesetzt.



IEEE 802.1Q-Frame "Dot1Q":



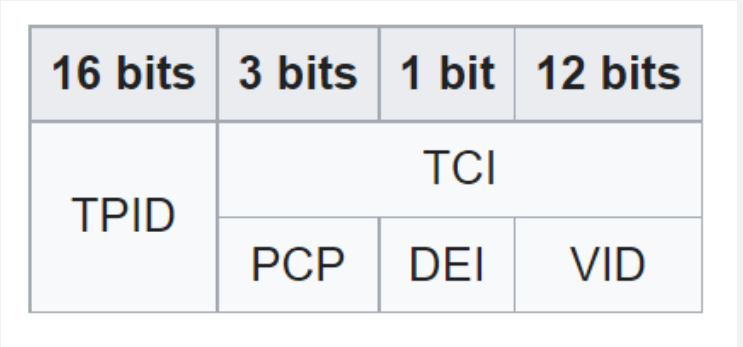
- Die darauf folgende Tag Control Information (2B) besteht aus dem
  - Priority Code Point (3Bit), das analog zur IP Precedence IPP) die Priorität des Ethernet-Frames in Form von 8 Service-Klassen regelt,
  - dem Drop Eligible Indicator (1Bit) das anzeigt ob ein Frame in Falle von Netzwerk Congestion gelöscht werden kann und
  - final die VLAN ID (12 Bit).

Aufgabe

a) Wieviel VLANs lassen sich generell definieren?

b) Welche Bedeutung hat die VLAN-ID=0x000 und welche Bedeutung hat die VLAN-ID=0xFFF?

c) Erklären Sie Einsatz des Drop Eligible Indicator (DEI).



a.) VLAN ID Feld: 12 Bit

→ $2^{12} = 4096$ Werte sind theoretisch möglich

praktisch nur 4094, da 0x000 (0), 0xFFF (4095) sind reservierte Werte

b.) VLANID=0x000 (0): indiziert dass das Frame keine VLANID enthält und nur die Prioritätssteuerung verwendet

→ Prioritäts-Tag

VLANID= 0xFFF (4095): reserved

c.) DEI= 1 : Frame darf bei einer Netzwerküberlast vom Switch gelöscht werden

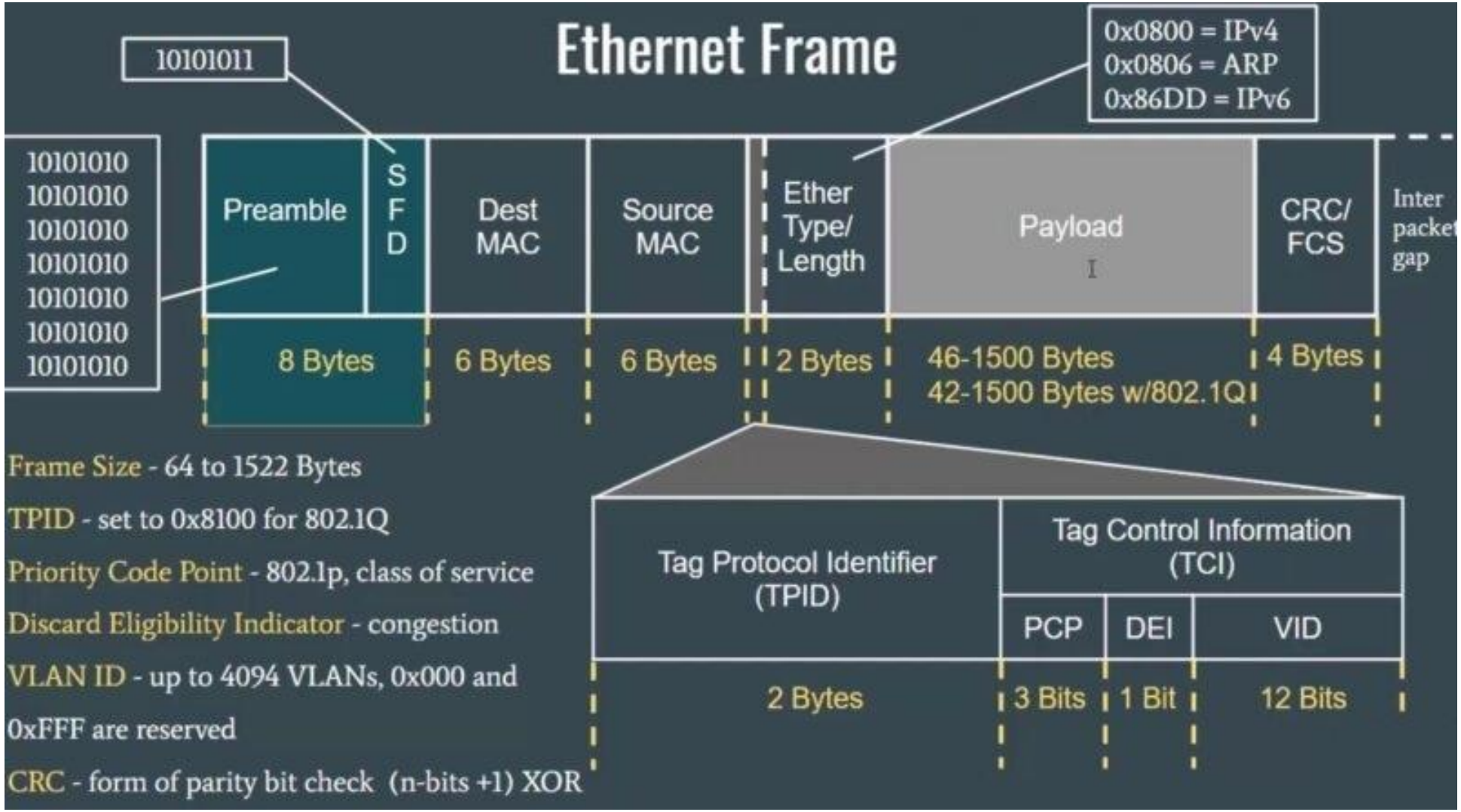
VLAN Port Typen

Access-Port: Ein Access-Port leitet Datenverkehr für ein bestimmtes VLAN weiter (Port-Based VLAN). Access-Ports werden häufig als ungetaggte Ports bezeichnet, da an einem Port jeweils nur ein VLAN vorhanden ist und Datenverkehr ohne Tags weitergeleitet werden. Nur demselben VLAN angehörende Ports können untereinander kommunizieren.

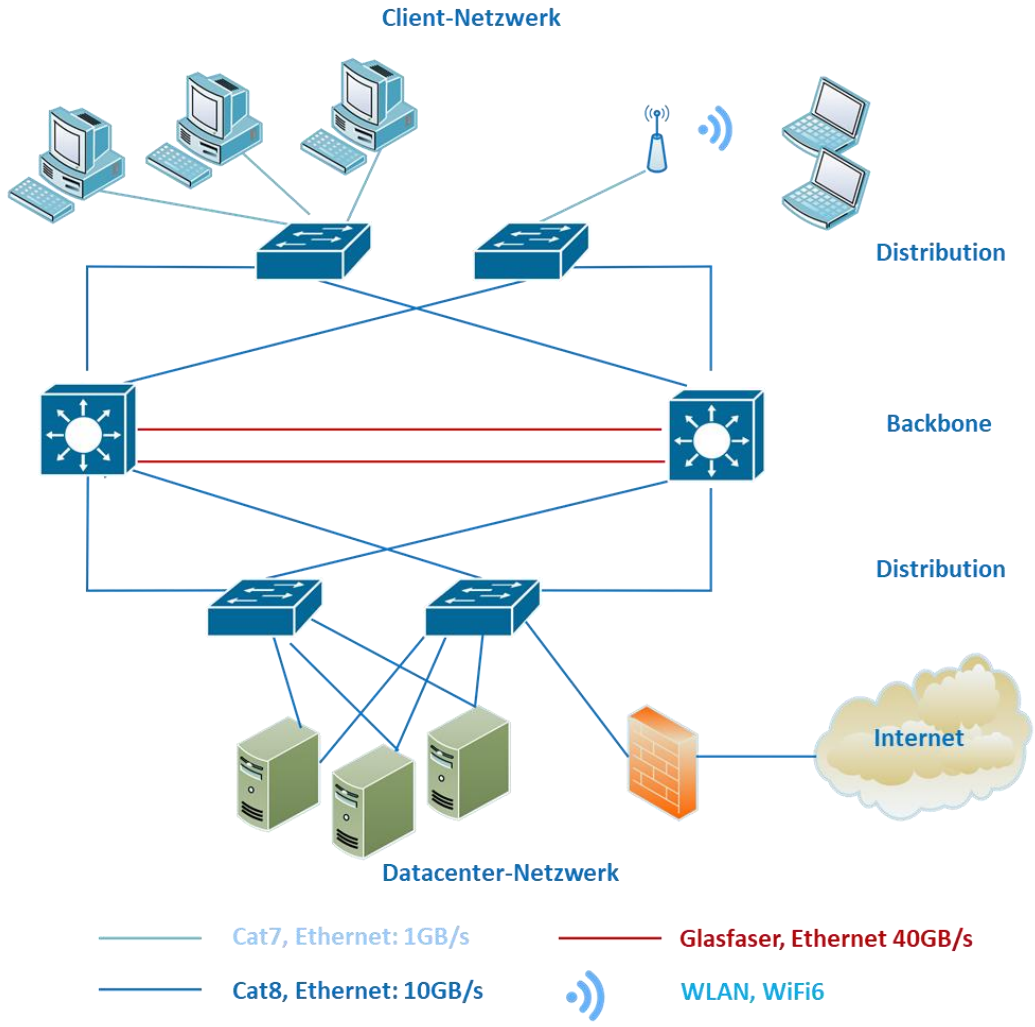
Trunk-Port: Ein Port auf einem Switch, der Datenverkehr für mehr als ein VLAN weiterleitet. Trunk-Ports werden häufig als getaggte Ports bezeichnet, da an einem Port mehr als ein VLAN vorhanden ist und der Datenverkehr für alle außer einem VLAN getaggt werden muss. Frames von einem Access-Port werden am Trunk-Port mit der VLAN-ID des Access-Ports getagged.

Natives VLAN: Das einzige VLAN an einem Trunk-Port, das kein Tag erhält und einem Trunk Port zugewiesen wird. Jeglicher Datenverkehr ohne Tag wird an das native VLAN gesendet. Aus diesem Grund muss sichergestellt sein, dass auf beiden Seiten eines Trunks dasselbe native VLAN vorhanden ist, da der Datenverkehr sonst nicht akzeptiert wird.

Ethernet Frame



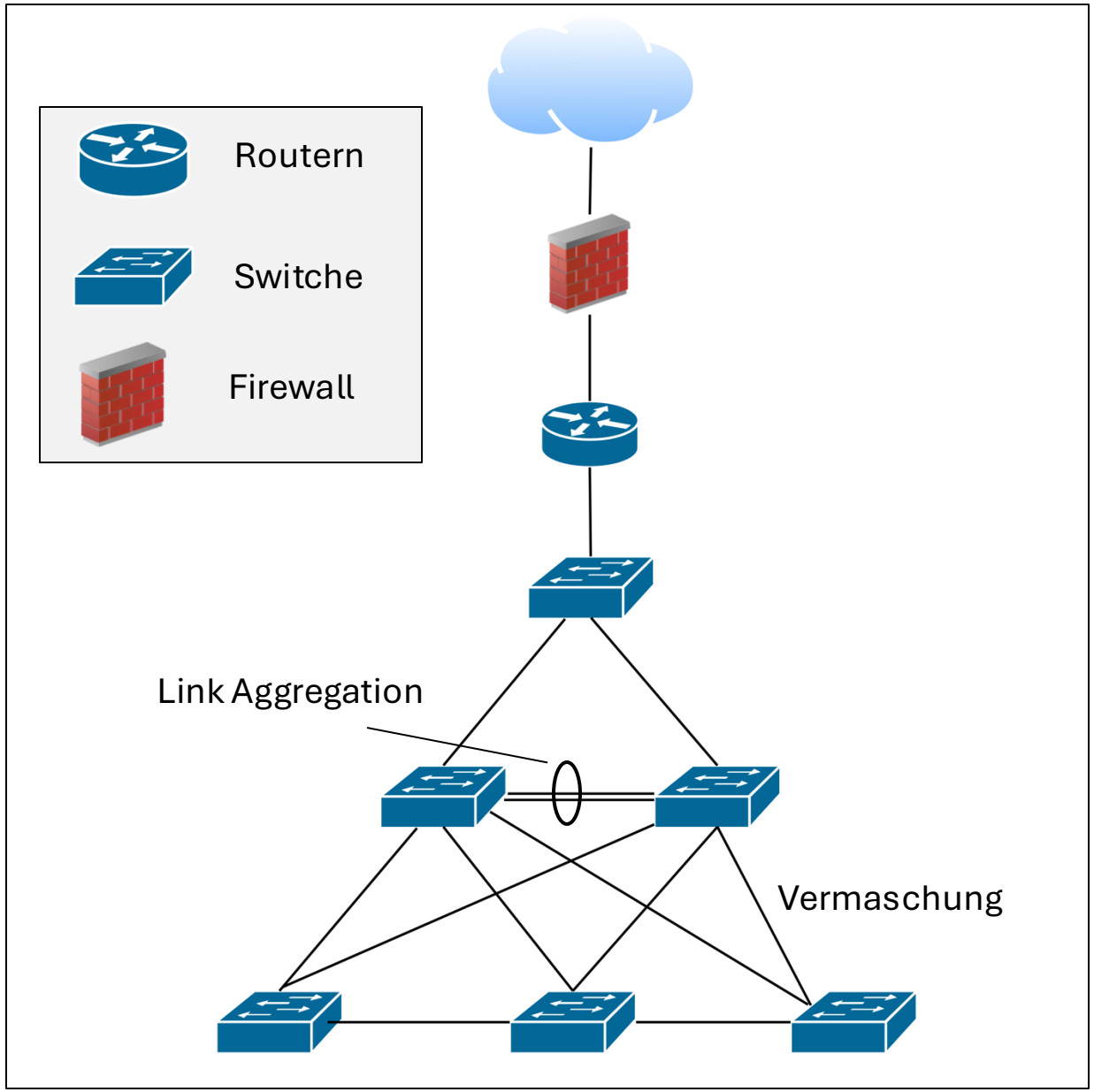
1.3 Sicherer Betrieb von Netzwerken



Sicherer Betrieb von Netzwerken

- Unternehmensnetzwerke bestehen aus 3 Kernkomponenten:
  - Switche (Layer 2)
  - Router (Layer 3) und
  - Firewalls (Layer3, Layer 4, Layer7)
- Die sichere Konfiguration und der sichere Betrieb dieser Netzwerkgeräte ist ein elementarer Baustein für die Sicherheit eines Netzwerkes.
- Jede Organisation muss über eine Netzwerkgeräte-Sicherheitsrichtlinie verfügen, die die Sicherheitsanforderungen an den Betrieb der Netzwerkgeräte definiert.
- Eine ergänzende Verfahrensanweisung (Betriebshandbuch) beschreibt die konkret umzusetzende Sicherheitskonfiguration für die Netzwerkgeräte.

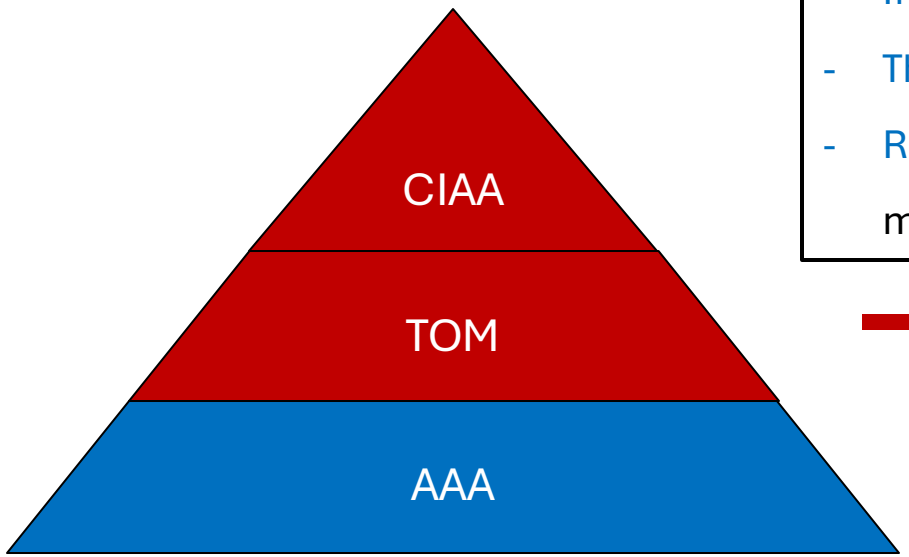
Vermaschtes LAN mit Switchen, Routern und Firewall



Information Security Management (ISMT)

Ableiten einer Sicherheits-Policy auf Basis von 3 Säulen

- Inventory: Welche Systeme befinden sich im Netzwerk?
- Threat-Analyse: Wie könnten diese angegriffen werden?
- Risiko-Analyse: Wie hoch ist das Risiko eines Angriffes und wie hoch ist der mögliche Schaden?



Unternehmens-Security-Policy

"Was ist erlaubt."

"Was ist nicht erlaubt."

Konkrete Maßnahmen

Compliance – Anforderungen:

- Gesetzliche Vorgaben
- Security-By-Design Prinzipien
- Best Practise Kataloge
- State of the Art Technology

Betriebshandbuch "Active Directory"

Betriebshandbuch "Netzwerk"

• • •

Betriebshandbuch "Mail-Infrastruktur"

Verschiedene Funktionsebenen eines Netzwerkgerätes

- Die drei Funktionsebenen eines Netzwerksgerätes, sind die Management Plane Ebene , die Control Plane Ebene und die Data Plane Ebene.
- Alle 3 Ebenen müssen geeignet geschützt werden, um einen sicheren Netzwerkbetrieb zu gewährleisten.
- Management-Plane – Die Verwaltungsebene managed die Netzwerkgeräte und sorgt für
  - eine sichere Konfiguration (z.B.: Fail-Safe-Default, NTP)
  - ein sicheres Monitoring (z.B.: Syslog & SIEM) und
  - einen sicheren Remote Zugang (z.B.: ssh) zu den Geräten.
- Data Plane – Die Datenebene leitet die erhaltenen Daten über ein Netzwerkgerät weiter. Die Datenebene wirkt als Vermittlungsstation.
  - Forwarding der Frames anhand Source-/Dest.-Adressen
  - Filtering der Frames anhand Source-/Dest.-Adressen (z.B. DHCP-Snooping), Port-Isolation, VLAN-Isolation
- Control Plane – Funktionen der Steuerungsebene bestehen aus den Protokollen und Prozessen, die für eine optimale Kommunikation zwischen den Netzwerkgeräten sorgen.

  Beispiele:
  - Routing-Protokolle (Border Gateway Protocol, OSPF) zum Aufbau einer IP-Route
  - Spanning Tree Protocol für ein vermaschtes LAN oder
  - ICMP zur Vermittlung oder Ermittlung von Status-Informationen aus dem Netzwerk.
  - DHCP-Snooping zum Filtern von erlaubten MAC-Adressen auf einem Port.

Im Folgenden werden ein paar ausgewählte Themen tiefer analysiert.

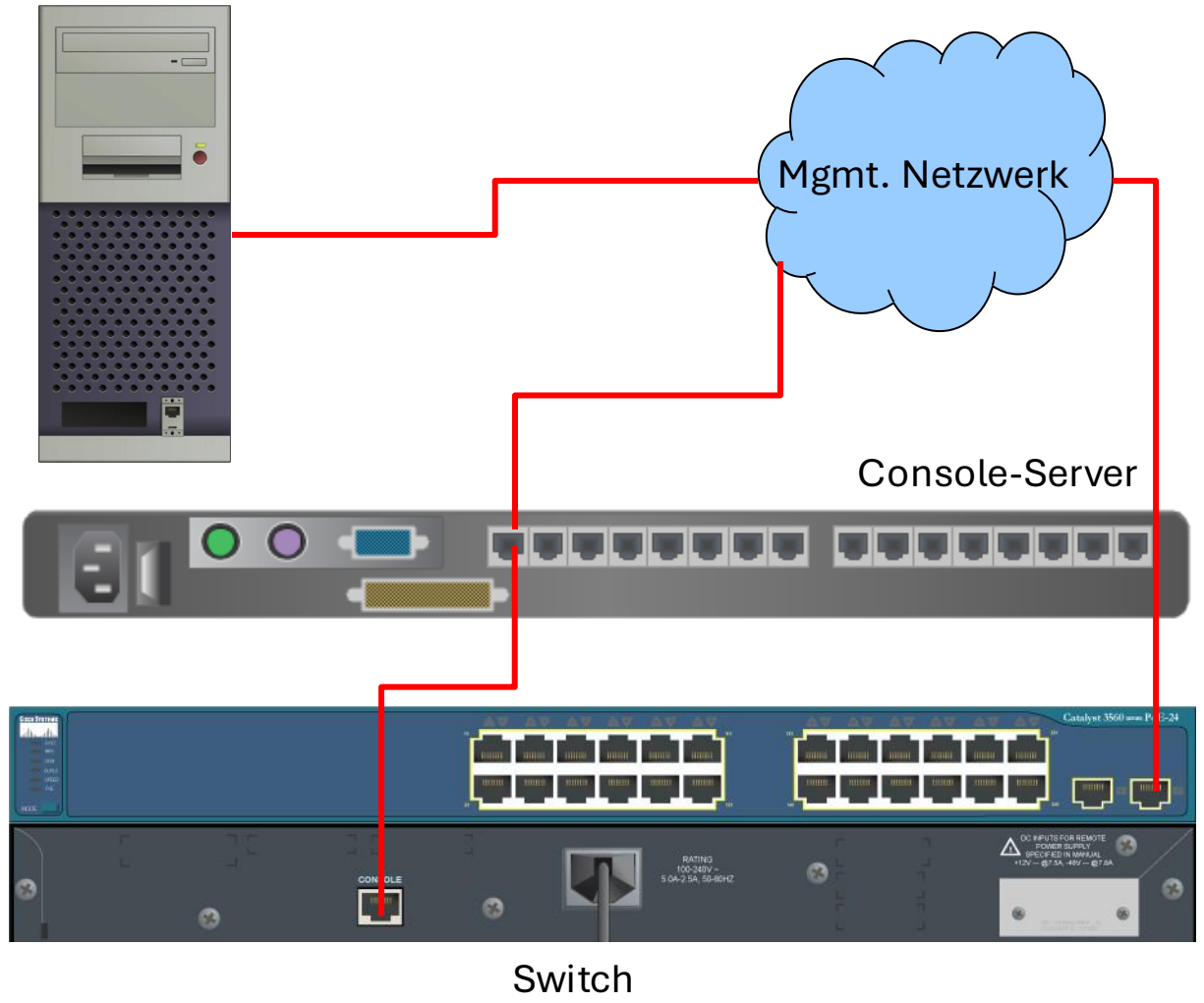
Secure Physical Access

- Netzwerkgeräte müssen generell in Räumen mit einem Zugangskontrollsystem (Rechenzentrum, Verteilerräume, Serverräume, ...) betrieben werden.
- Das Zugangskontrollsystem regelt den Personenkreis der physikalische Zugriff auf die Geräte erhalten soll und protokolliert wer und wann den geschützten Raum betreten hat.
- Der Zutritt in ein Rechenzentrum erfolgt über Personen-schleusen, die nur einzeln betreten werden können: "Vereinzelung"
- Um an die Personenschleuse zu gelangen, sollte mehrere Sicherheitszonen geschaffen werden:
  - Zugang zum Unternehmensgelände
  - Zugang zum RZ-Gebäude
  - Zugang zur RZ-Fläche (Vereinzelungsanlage)
- Weiterhin sollte die Personenschleuse sowie die einzelnen Serverreihen in einem Rechenzentrum mittels Kameras videoüberwacht werden.
- Die Videoüberwachung hilft bei der Aufklärung von Fehlbedienungen oder böswilligen Operationen durch interne und externe Akteure.
- In größeren Rechenzentren kann zusätzlich eine Trennung des administrativen Zugriffs über verschlossene Racks oder Metallkäfige erzielt werden.

Switch

- Enterprise Switche besitzen typischerweise 24/48-Ports.
- Die Ports können als Access- oder Trunk-Ports konfiguriert werden.
- Klassische Bandbreiten der Ports
  - Client-Bereich: 1GBit
  - Server-Bereich: 10/40GBit
- Console-Port ist typischerweise ein Ethernet-Port (RJ45)
- Console-Port in Rechenzentren sind über einen Console-Server erreichbar.
- Zusätzlich kann per vty über einen Management-Port oder über ein separates VLAN auf den Switch zur Konfiguration zugegriffen werden.

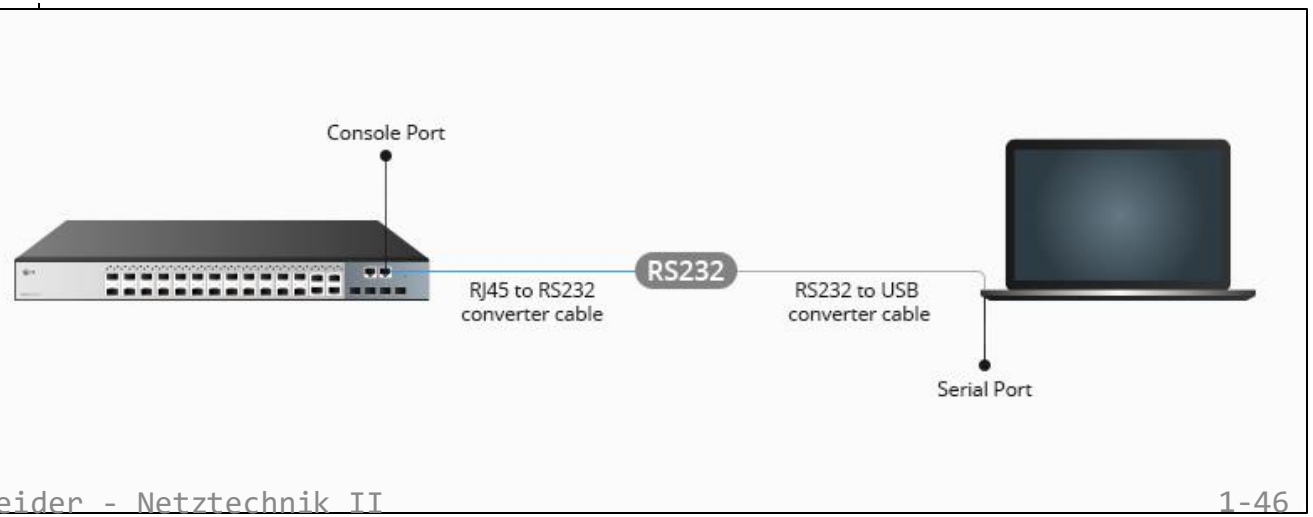
```
#MGMT-Schnittstelle 192.168.1.10
$ssh admin@192.168.1.10
```



Sichern des Console Zugriffs

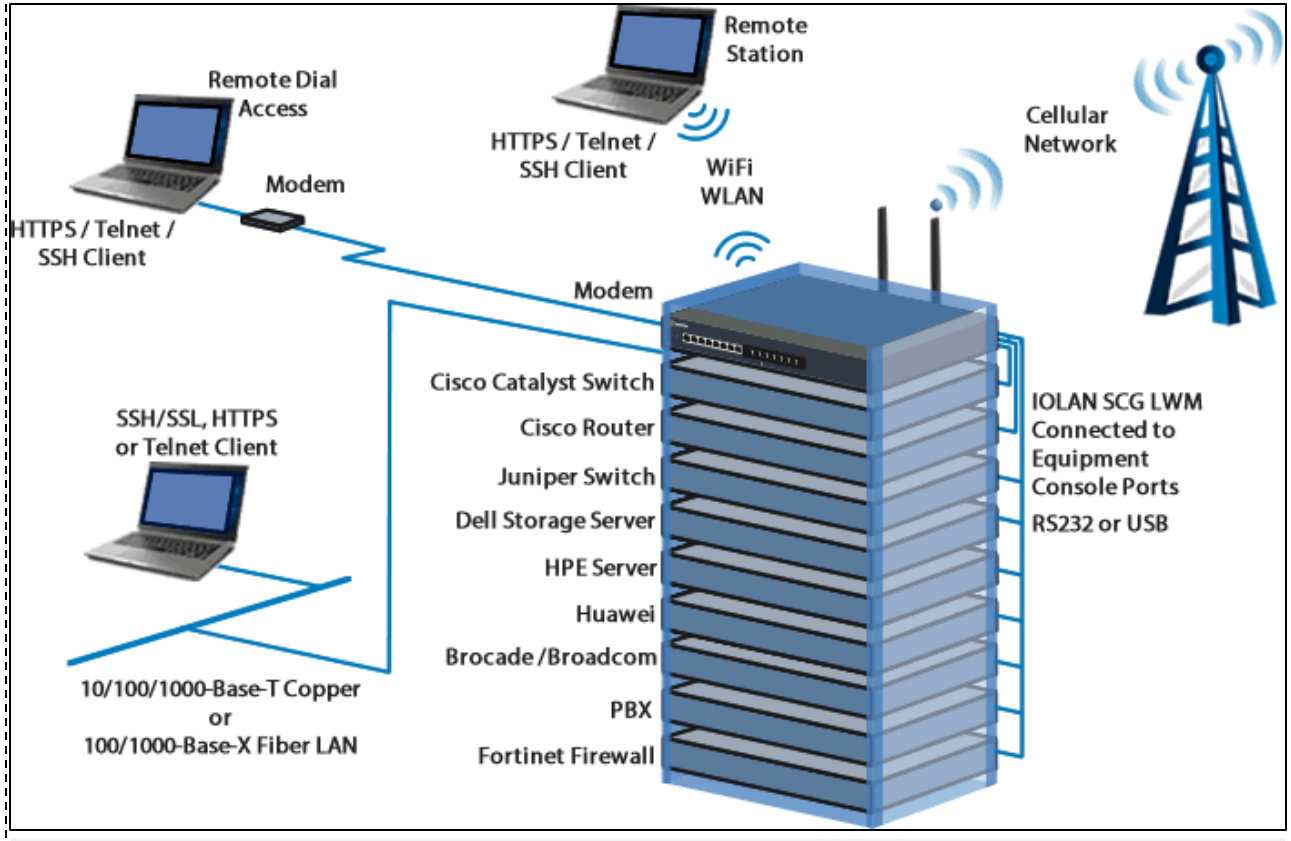
- Erhält ein Hacker Zugriff auf den Console Port eines Netzwerkgerätes, kann dieser das Passwort für einen Switch, Router oder Firewall ändern, indem dieser den Boot-Prozess des Gerätes unterbricht und in den Recovery-Mode wechselt.
- Bei CISCO-Geräten kann dies mit der Option "no service password-recovery" verhindert werden.
- Der Console-Zugriffspunkt sollte generell nur für die initiale Konfiguration oder für die Behebung von Fehlern, bei denen
  ein Remote-Zugriff nicht mehr möglich ist verwendet werden.
- Ansonsten sollte eine benutzerbezogene Anmeldung verwendet werden.

```
!Wechsel in den Privileged Exec Mode
S1#enable
!Wechsel in den Global Configuration Mode
S1#configure terminal
!Password Recovery not allowed
S1(conf)#no service password-recovery
//Exit Configuration Mode in Privileged Exec Mode
S1(conf)#exit
//Save to NVRAM
S1#write memory
```



Out-of-Band- Management-Lösung (OOBM)

- Ein Konsolenserver (Console Server) gewährleistet einen sicheren Remote-Zugriff auf den Console-Port einer Vielzahl von Geräten (Netzwerkgeräte, Server, ...).
- Der Konsolenserver stellt unterschiedliche Schnittstellen (Ethernet, RS232, USB) zur direkten Anbindung der Konsole eines Gerätes über eine dedizierte Leitung zur Verfügung.
- Der Administrator kann auf den Konsolenserver über LAN oder WLAN zugreifen.
  - Der Zugriff erfolgt über die IP-Adresse des Konsolen-servers unter Verwendung von TCP-Port-Forwarding.
  - Jedem angeschlossenen Gerät wird ein spezieller TCP-Port zugewiesen.
- Der Konsole Server sollte sich in einem separaten Manage-ment-Netzwerk befinden, das getrennt vom Unternehmens-LAN ist und nur für Administratoren zugänglich ist.

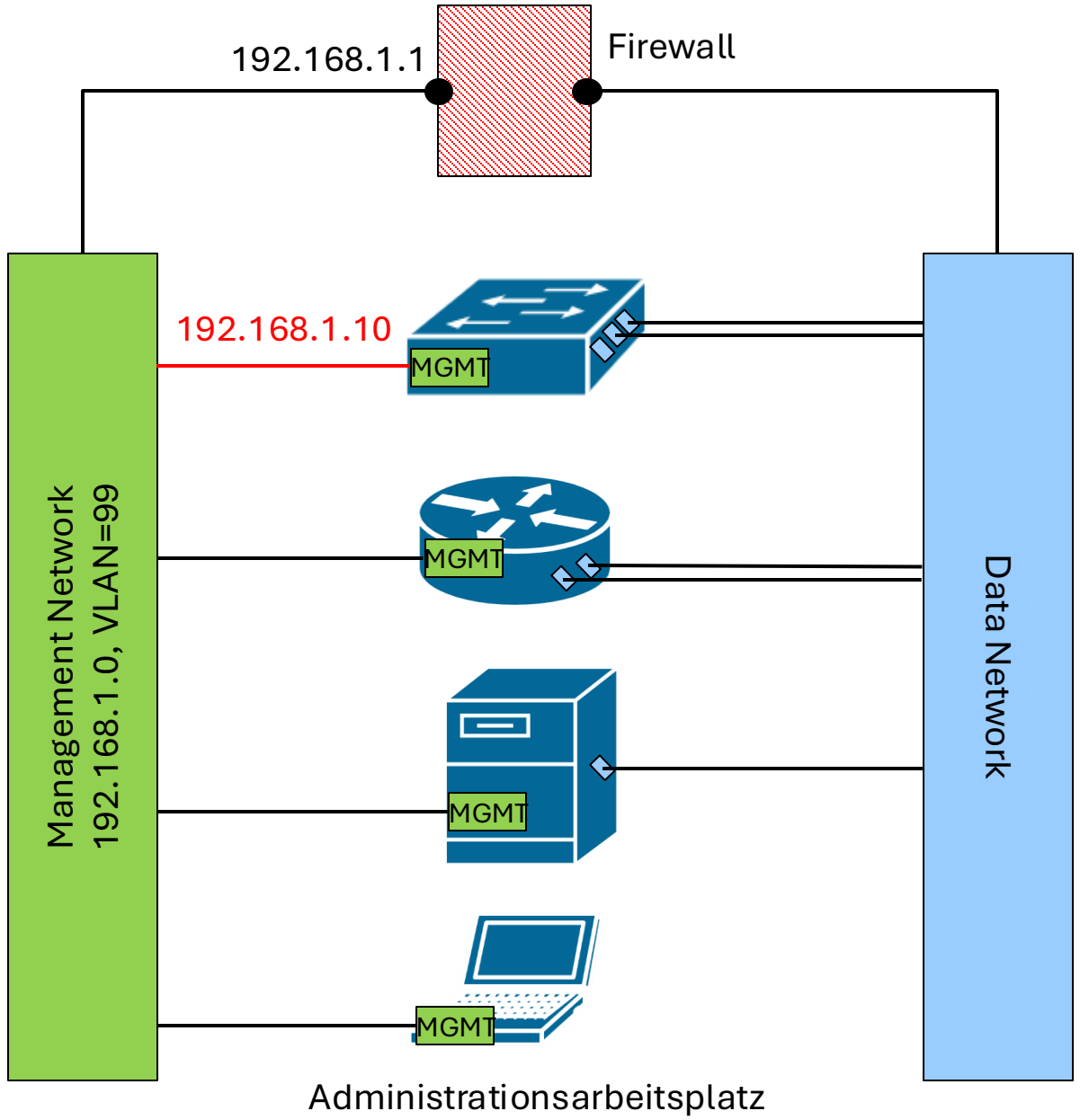



```
#Console-Server mit IP 192.168.56.44 und Benutzer admin
#Zugriff auf Cisco Catalyst: Port 7001
$ssh -l admin 192.168.56.44  -p 7001
#Zugriff auf Cisco Router: Port 7002
$ssh -l admin 192.168.56.44  -p 7002
```

Management Network per phys. Interface

- Für die direkte Remote Administration von Netzwerkgeräten oder Servern sollte ebenfalls das separierte Management-Netzwerk verwendet werden.
- Netzwerkgeräte und Server besitzen dafür spezielle Management-Interfaces.
- Beispiel: Konfiguration eines Mgmt.-Interfaces auf einem Switch

```
!Mgmt.-Interface
S1(config)#interface mgmt0
S1(config-if)#ip address 192.168.1.10 255.255.255.0
S1(config-if)# #no shutdown
S1(config-if)# #ip default-gateway 192.168.1.1
S1(config-if)# #end
S1#write memory
```



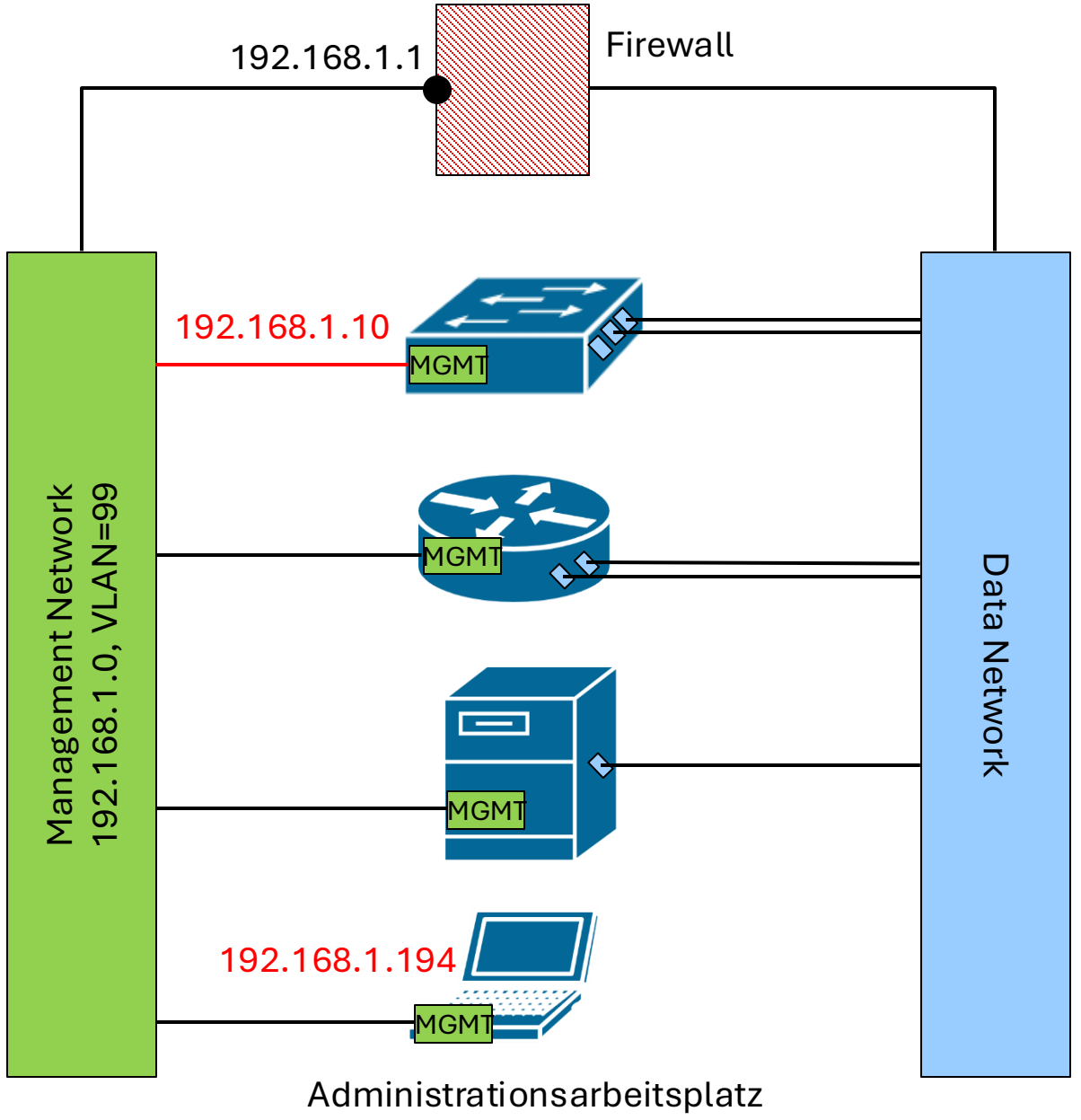
Standard Access Control Listen

- Um den Zugriff auf die Management-Schnittstelle für bestimmte IP-Adressen (Subnetze) einzuschränken, können sogenannte Access Control List (ACL) verwenden.
- Die ACL filtert den eingehenden IP-Datenverkehr analog zu einer Paket-Firewall (siehe hinten).

  Bei der Nummer 10 handelt es sich um eine Nummer für eine sogenannte Standard-ACL (Nummer 1– 99) die als Input nur die Source-IP-Adresse(n) erhält

```
!Only host with IP 192.168.1.194 is allowed
S1(conf)#access-list 10 permit 192.168.194 log
!All hosts with IP in range (.194 -.254) are allowed
S1(conf)#access-list 10 permit 192.168.1.193 0.0.0.63 log
S1(conf)#access-list 10 deny any log

S1(conf)#interface mgmt0
S1(conf-if)#ip access-group 10 in
S1(conf-if)#exit
```

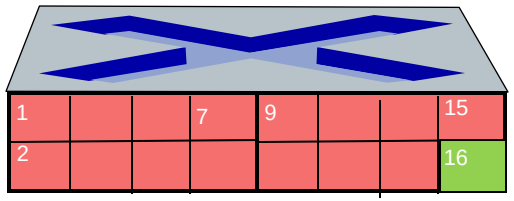
ingress-Netzwerkverkehr



Port Isolation

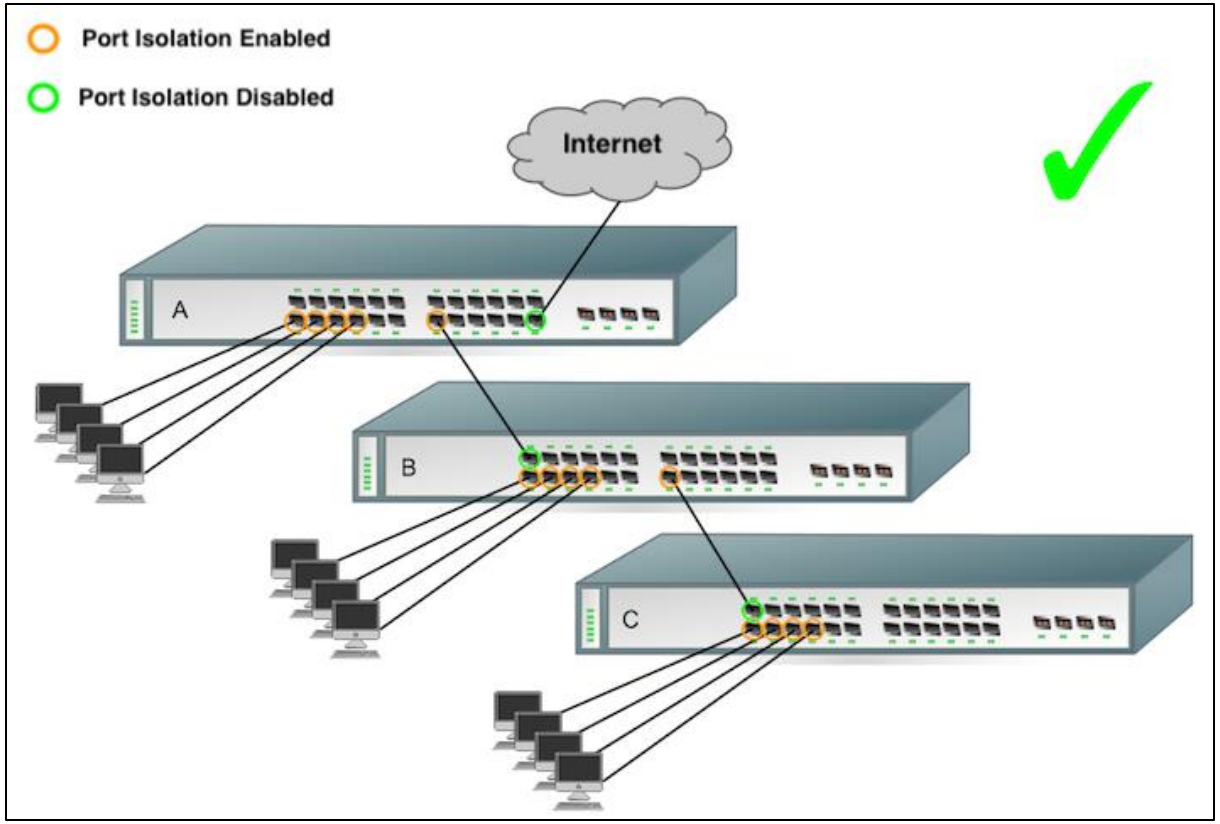
- Um die Sicherheit in LAN-Netzwerken zu erhöhen, kann die sogenannte Port-Isolation verwendet werden.
- Hosts, die an einen Switch angebunden sind können dann untereinander nicht kommunizieren.
- Die Außenkommunikation wird über einen Uplink ermöglicht.
- Die Port-Isolation sorgt für eine Firewall-ähnliche Barriere zwischen den Ports eines Switches, sodass jeglicher Unicast-, Broadcast- oder Multicast-Datenverkehr zwischen diesen Ports blockiert wird
- Einsatzszenario:
  - Typischerweise kommunizieren Clients (PCs) in einem Unternehmensnetzwerk nicht untereinander sondern über Server miteinander.
  - Dadurch wird die Sicherheit in einem LAN deutlich erhöht, da von einem gehackten Client nicht auf einen benachbarten Client zugegriffen werden kann.
- Konfiguration: Zu isolierende Ports werden in den "Protected State" gesetzt.
- Beispiel: Die 15 Ports Fast0/1 - Fast0/15 sollen untereinander nicht kommunizieren können. Der Port Fast0/16 wird als Uplink-Port verwendet.

```
S1(config)# interface Fast0/1 - 15
S1(config-if)# switchport protected
S1(config-if)# end
```



Port Isolation: Architektur in einem Unternehmensnetzwerk

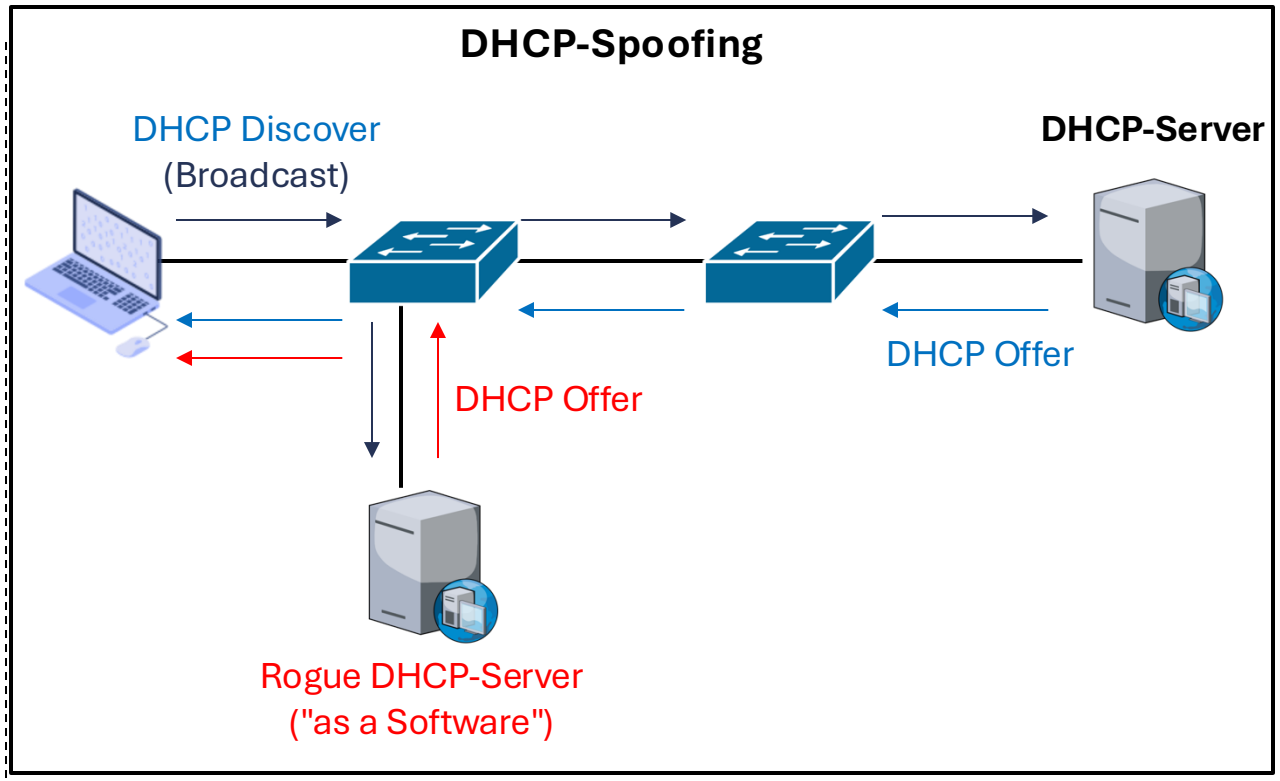
- Beispielarchitektur für ein Unternehmensnetzwerk:
  - Clients die mit "isolierten Ports" verbunden sind, können untereinander nicht kommunizieren.
  - Der Uplink von Switch C zu Switch B und von Switch B zu Switch A ist "nicht isoliert", der zugeordnete Port auf dem "höheren" Switch ist isoliert.
    Daten können dabei von unten (nicht isoliert) nach oben (isoliert) und umgekehrt fließen.
  - Der Uplink vom Switch A in das Internet ist "nicht isoliert". Die Frames aller Switches können somit mit dem Internet kommunizieren.
  - Daten vom Internet gelangen über einen "nicht isolierten" Port zu Switch A und können über einen "isolierten Port" nach unten fließen usw.

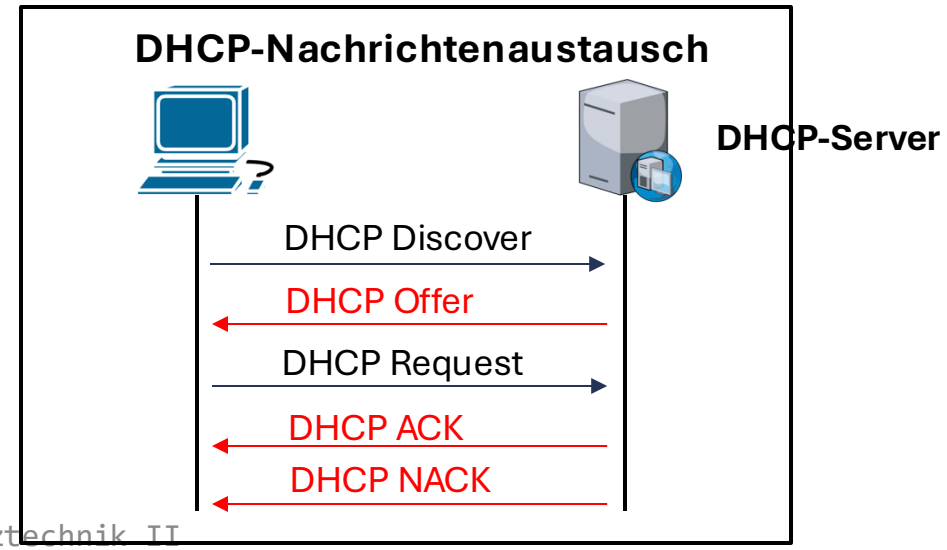


- Erlaubte Datenflüsse:
  - "nicht isoliert" → "isoliert"
  - "isoliert" → "nicht isoliert"

DHCP Spoofing

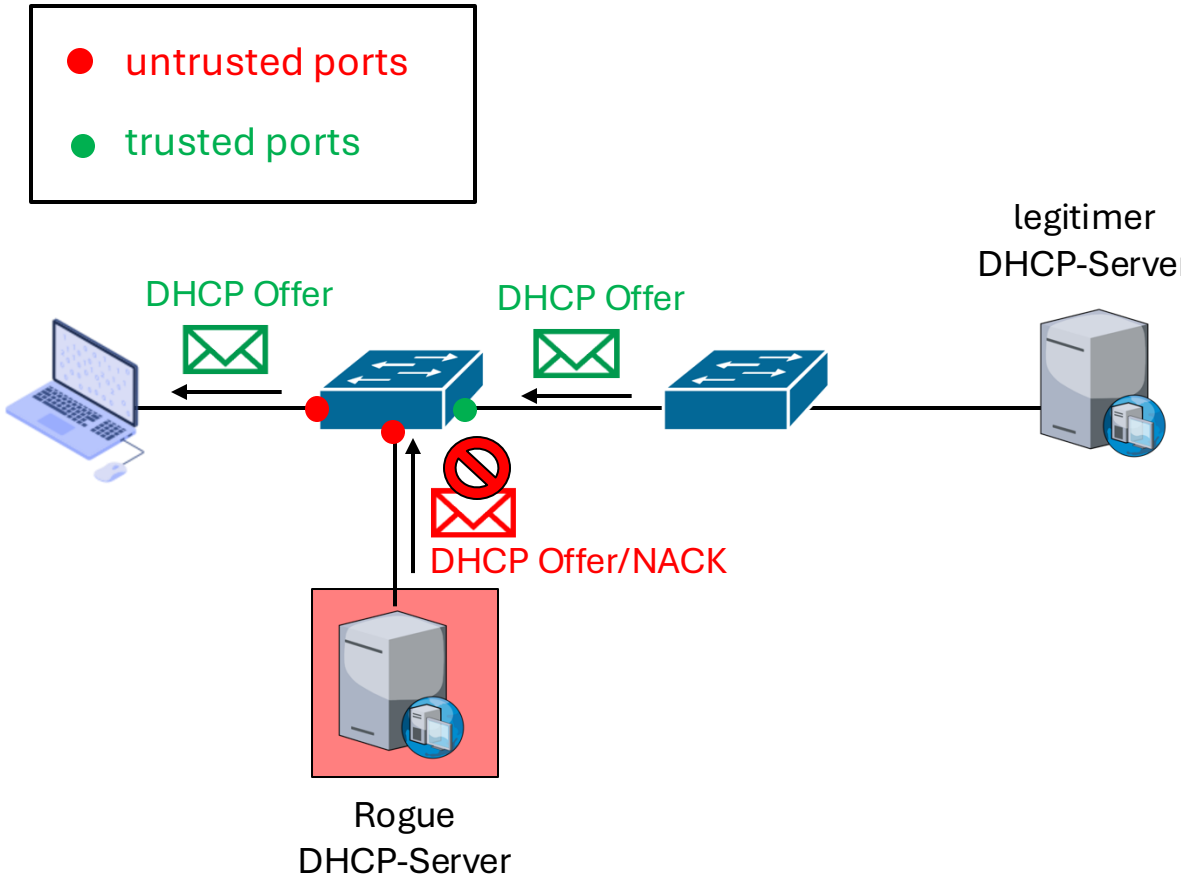
- Beim DHCP-Spoofing versucht ein Angreifer Antworten eines zulässigen DHCP-Servers zu fälschen.
- Der Rogue DHCP-Server antwortet auf eine DHCP-Anfrage (DHCP Discover) eines Clients schneller als der unternehmenseigene DHCP-Server.
  - Die Rogue-Antwort DHCP Offer übermittelt dann den Angreifer Server als Default-Gateway und als DNS-Server.
  - Als Default-Gateway-Server empfängt dann der Angreifer die Pakete der Clients und kann sie somit lesen oder verfälschen (Man-in-the-Middle-Angriff).
  - Als Default-DNS-Server kann er angefragte Zieladressen beliebig fälschen, sodass der Verkehr an ihn weitergeleitet wird (DNS Spoofing).
  - Mittels DHCP NACK konnte ein Rogue Server einen legitimen DCHP Request eines Clients ablehnen und so Verbindungsprobleme im Netzwerk erzeugen.





DHCP Snooping

- Mittels DHCP-Snooping wird festgelegt, welche Switch-Ports eingehende DHCP-Nachrichten (DHCP-OFFER , DHCP-ACK, DHCP-NACK) akzeptieren und als legitim betrachten.
  - Diese Switch-Ports werden als vertrauenswürdig (trusted) konfiguriert und sind mit legitimen DHCP-Servern oder stellen einen Uplink zu Switches/Routern, dar, an die ein legitimer DHCP-Server angebunden ist.
  - Nicht vertrauenswürdige Ports (untrusted ports) sind mit Endgeräten verbunden, worunter sich möglicherweise das Endgerät eines Hackers befindet. Auf diesen Ports werden eingehende DHCP-Nachrichten blockiert.
- Es ermöglicht somit nur autorisierten DHCP-Servern, auf DHCP-Anforderungen zu antworten.



DHCP Snooping

- Zusätzlich liest der Switch den Inhalt (Payload) der DHCP-Nachrichten und speichert diesen in einer DHCP-Snooping Datenbank.
- Die folgenden Informationen werden gespeichert:
  - MAC-Adresse des DHCP-Clients
  - Zugewiesene IP-Adresse für den DHCP-Clients
  - Lease Time (Gültigkeitsdauer) der DHCP-Adresse
  - VLAN-ID des DHCP-Clients
  - Interface des Switches an dem der DHCP-Client angeschlossen ist.
  - Binding Type:

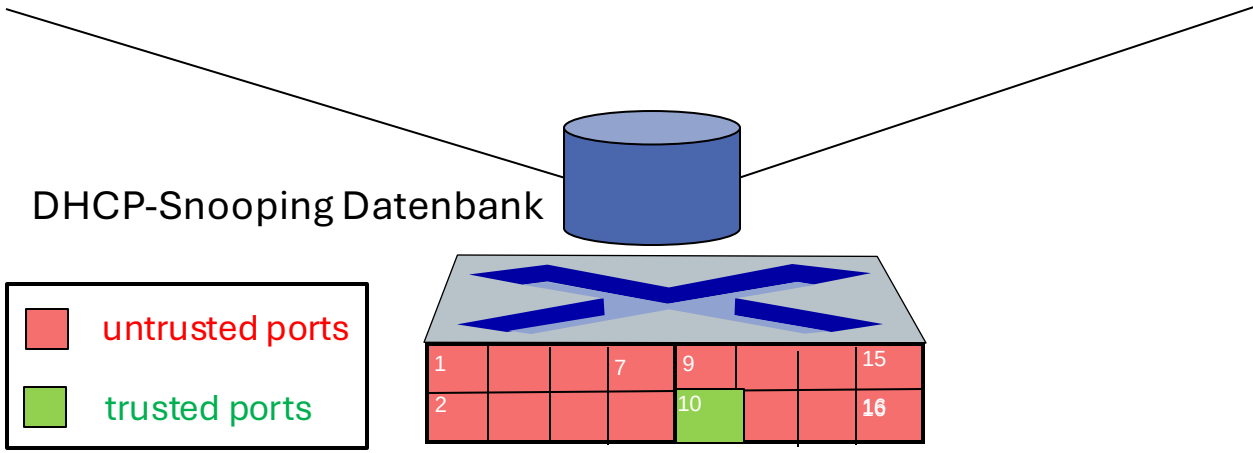
    dynamic: gelernt von DHCP-Nachrichten

    static: von einem Netzadmin hinzugefügt
- Der Switch ist somit in der Lage Spoofing-Angriffe (z.B. ARP-Spoofing, IP-Spoofing) pro Interface zu erkennen (siehe hinten).

```
!Manual Entry in snooping db
S1(config)# ip dhcp snooping binding 192.168.1.100 mac
00e0.4c68.8b4d vlan 10
!Anzeige DHCP Snooping DB Inhalt
S1# show ip dhcp snooping binding
```

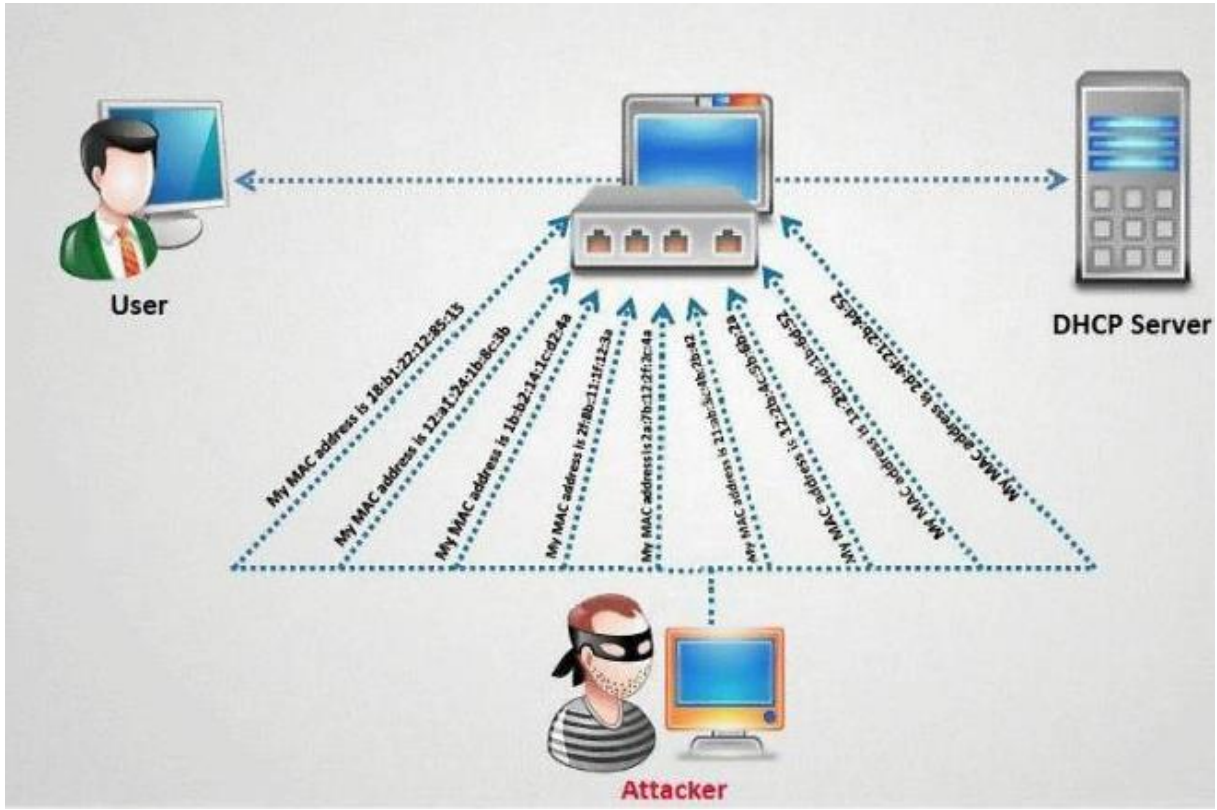
DHCP-Snooping Datenbank Eintrag

MAC-Address	IP-Address	Lease Time	VLAN	Inter-face	Binding Type
00:1a:2b:3c:4d:5e	192.168.1.10	3600s	10	Gig0/1	dynamic
00:e0:4c:68:8b:4d	192.168.1.100	-	10	Gig0/2	static



DHCP Starvation

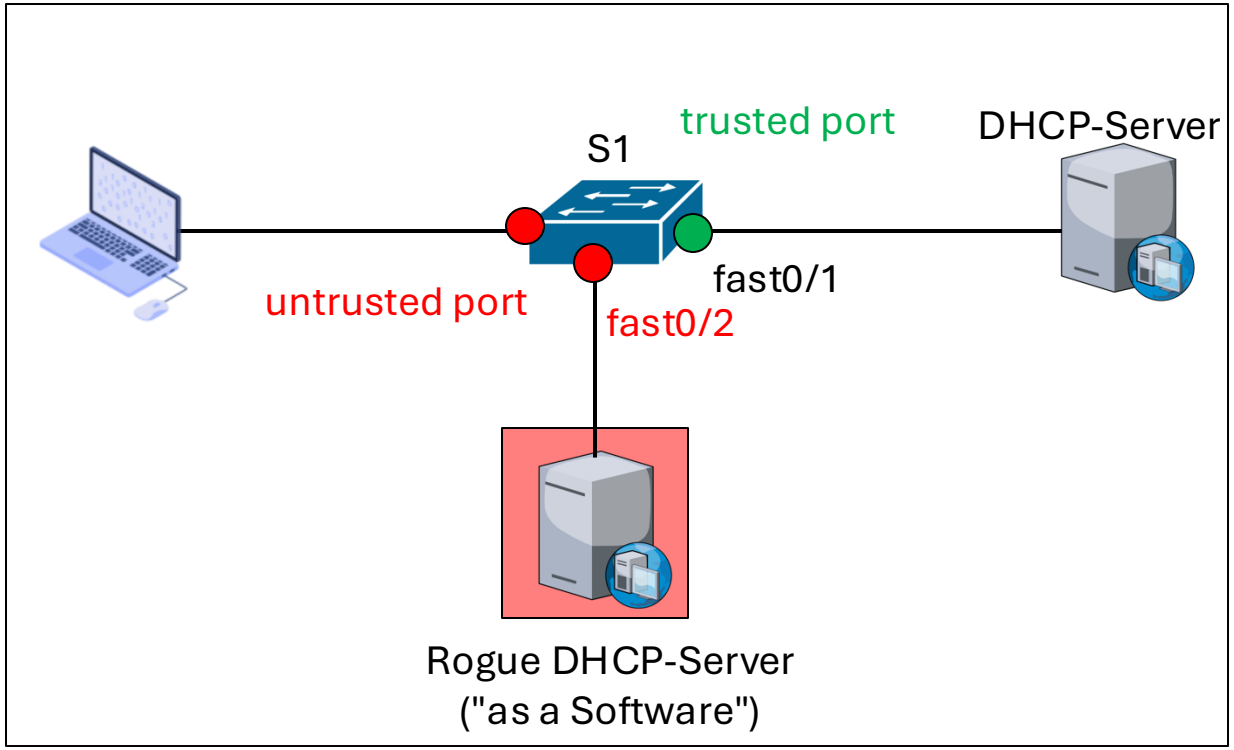
- Weiterhin kann die maximale Anzahl der DHCP-Anfragen pro Port eingegrenzt werden, um ein Aushungern des DHCP-Servers zu verhindern (DHCP Starvation).
- Beim DHCP-Starvation („Aushungern“) fordert ein Angreifer kontinuierlich neue IP-Adressen bei einem DHCP-Server an.
  - Dazu ändert er fortlaufend seine MAC-Adresse.
  - Hat der Angriff Erfolg werden alle verfügbaren IP-Adressen innerhalb des DHCP-Adresspools an den Hacker vergeben.
  - Möchte jetzt ein Anwender eine IP-Adresse beziehen, geht er leer aus und ist nicht arbeitsfähig.



Beispiel: DHCP Snooping und DHCP Starvation

- Beispiel: Im LAN soll für das VLAN 5 DHCP Snooping aktiviert werden. Für den Switch S1 soll weiterhin an den Port Fast 0/1 ein unternehmenseigener DHCP-Server angeschlossen werden. Weiterhin sind nur 10 DHCP-Anfragen pro Sekunde auf dem Interface erlaubt.

```
!Activate DHCP Snooping in vlan 5
S1(config)# ip dhcp snooping vlan 5
!Configure trusted interface
S1(config)# interface fast0/1
!Trusted Port für DHCP snooping
 S1(config-if)# ip dhcp snooping trust
!DHCP Starvation for untrusted access ports
S1(config)# interface fast0/2
! Max. 10 DHCP-Request pro Sekunde on fast0/2
 S1(config-if)# ip dhcp snooping limit rate 10
 S1(config-if)# exit
```



Address Resolution Protocol (ARP)

- Das Address Resolution Protocol (ARP) liefert die IP-zu-MAC-Zuordnung (IP-Adresse auf eine Ethernet-Adresse).

  IP-Adresse ↔ MAC-Adresse

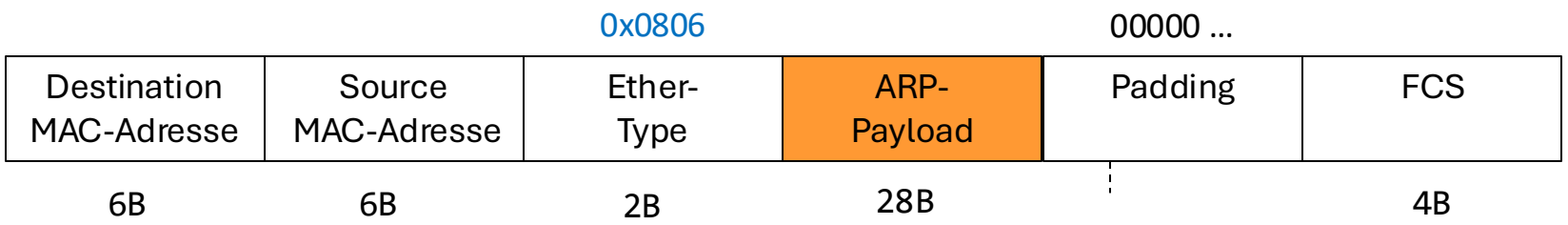
- ARP speichert die IP / MAC-Adressen-Zuordnung in einem lokalen Cache, dem sogenannten ARP-Cache.
- ARP-Nachrichten werden im Payload eines Ethernet-Frames (Ethernet, WLAN) transportiert.
- Da eine ARP-Message eine Größe von 28B hat wird das Ethernet-Frame mittels Padding (18B) auf die Mindestgröße von 64B erweitert. Das Padding besteht aus lauter Nullen.
- Der Ethertype für ARP ist 0x0806.

Anzeige des ARP-Cache

```
WINDOWS
C:\netsh interface ipv6 show neighbors
C:\arp –a

LINUX
$ip -4 neigh
```

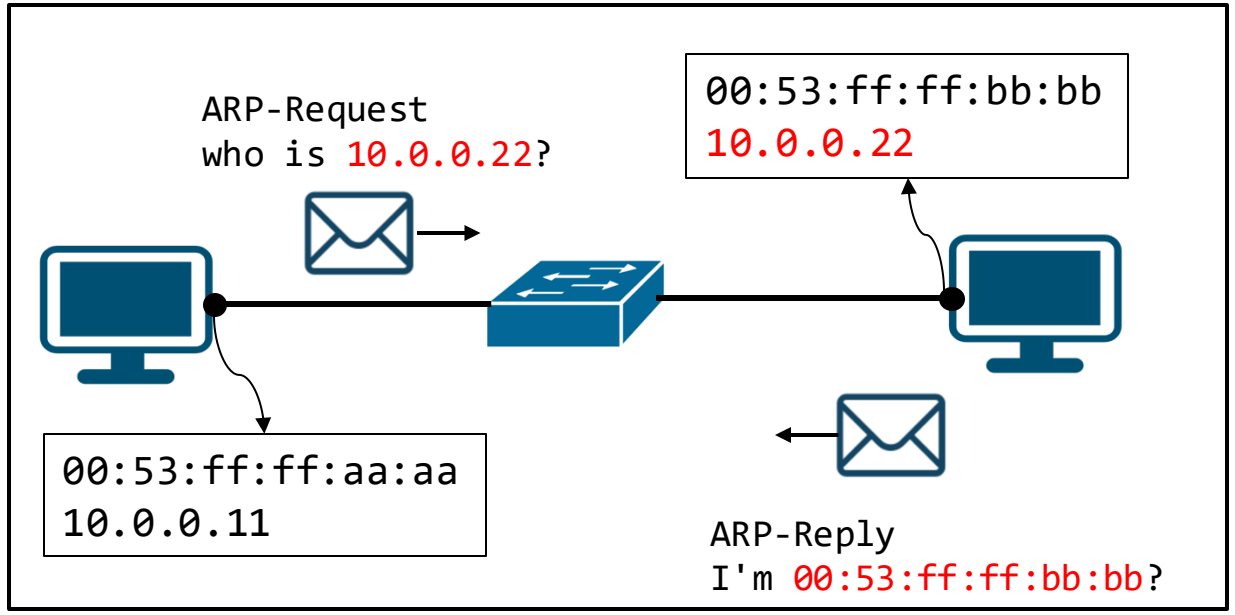
```
Schnittstelle: 192.168.178.77 --- 0xa
  Internetadresse      Physische Adresse     Typ
  192.168.178.1        44-4e-6d-c7-ab-85     dynamisch
  192.168.178.31       d2-ce-1e-98-e3-42     dynamisch
  192.168.178.43       00-17-88-a9-48-4a     dynamisch
  192.168.178.44       28-11-a5-f5-d6-c0     dynamisch
  192.168.178.72       5c-80-b6-0a-c8-32     dynamisch
  192.168.178.255      ff-ff-ff-ff-ff-ff     statisch
  224.0.0.22           01-00-5e-00-00-16     statisch
  224.0.0.251          01-00-5e-00-00-fb     statisch
  224.0.0.252          01-00-5e-00-00-fc     statisch
  239.255.255.250      01-00-5e-7f-ff-fa     statisch
  255.255.255.255      ff-ff-ff-ff-ff-ff     statisch
```

Roter Rahmen: Broadcast Adresse
Blauer Rahmen: Multicast Adressen



ARP Message Format

- ARP verwendet zwei Nachrichtentypen: ARP-Request und ARP-Response.
- Die nebenstehende Abbildung zeigt das Format einer ARP-Request-/-Response Nachricht.
- Beim ARP-Request ist die Destination MAC-Adresse gleich mit der lokalen Broadcast-Adresse (`ff:ff:ff:ff:ff:ff`).
- Beim ARP-Response ist die Destination gleich mit der MAC_Adresse des anfragenden Hosts.



Hardwaretyp (Ethernet) und Hardwaregröße (6Byte) geben eine Ethernet- Adresse an, die 6 Byte (48 Bit) groß ist.

Protokolltyp (IPv4) und Protokollgröße (4B) suchen eine IPv4-Adresse die 4 Byte (32 Bit) groß ist an.

Das Opcode-Feld definiert ob es sich um einen ARP Request (=1) oder einen ARP-Reply (=2) handelt..

ARP Payload

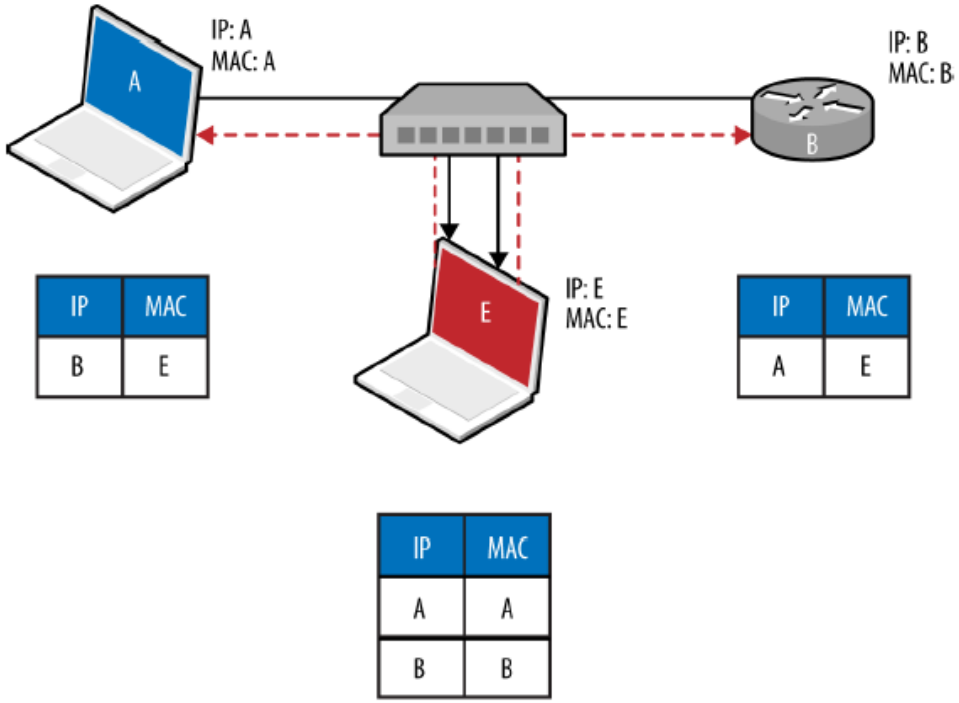
```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 00:53:ff:ff:aa:aa
    Sender IP address: 10.0.0.11
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 10.0.0.22
```

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 00:53:ff:ff:bb:bb
    Sender IP address: 10.0.0.22
    Target MAC address: 00:53:ff:ff:aa:aa
    Target IP address: 10.0.0.11
```

ARP-Spoofing, ARP-Poisoning

- Man-in-the-Middle (MITM) Angriff: Ziel eines Angreifers ist den ARP-Cache von 2 miteinander kommunizierenden Hosts so zu vergiften (poisoning), dass der Datenverkehr über den Host des Angreifers verläuft.
- Dazu verschickt er ARP-Nachrichten mit nachgeahmten (spoofing) MAC-Adressen, so dass die ARP-Caches auf den beteiligten Hosts jeweils auf den Angreifer-Host verweisen.
- Der Angreifer nutzt die Eigenschaft des ARP-Protokolls, sogenannte unaufgeforderte (gratuitous) ARP-Nachrichten per Ethernet-Broadcast zu versenden.
- Gratuitous ARP-Nachrichten werden beispielsweise versendet, wenn eine Netzwerkkarte (NIC) in einem Gerät geändert wurde und das Gerät neu startet.

"gratuitous": unaufgefordert

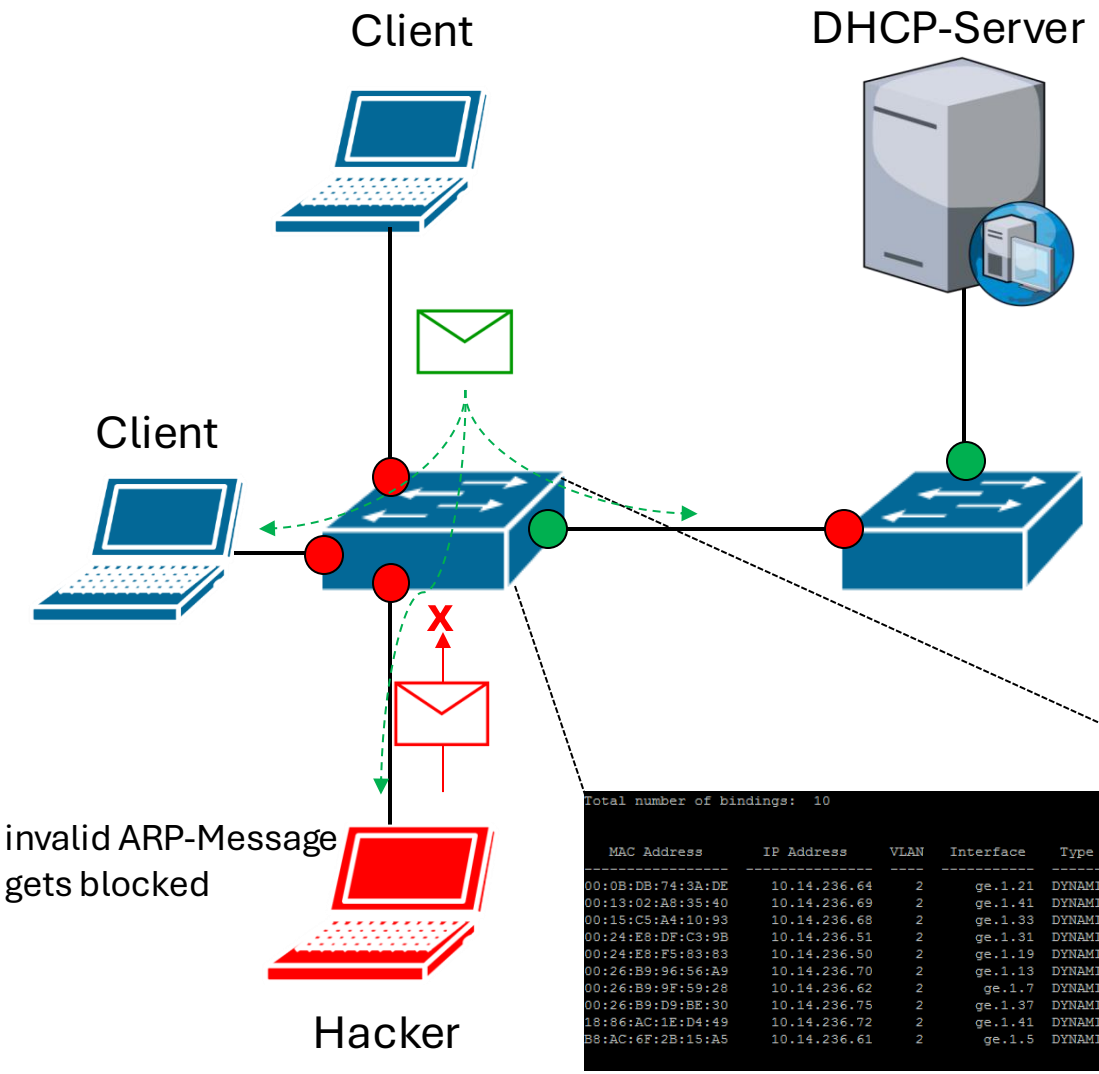


ARP E → A: (IP B, MAC E)

ARP E → B: (IP A, MAC E)

Dynamic ARP Inspection und

- Mittels Dynamic ARP Inspection (DAI) kann der Switch eingehende ARP-Frames auf Gültigkeit überprüfen.
  - Dazu überprüft der Switch ARP-Pakete von untrusted Ports und validiert die Kombination (IP,MAC-Adresse) im ARP-Payload anhand der DHCP-Snooping-Binding-Datenbank.
  - Wenn kein entsprechender (IP,MAC-Adresse) - Eintrag in der Snooping-Datenbank zu dem Switch-Interface vorhan-den ist, verwirft DAI das ARP-Paket und verhindert somit das ARP Poisoning der Caches.
- Weiterhin kann mittels DAI ein Flooding-Angriff (Denial of Service) verhindert werden, bei dem ein Angreifer versucht übermäßig viele ARP-Pakete sendet (z. B. bösartige oder fehlerhaft funktionierende Geräte), um so den Switch und das gesamte Netzwerk zu überlasten.



Total number of bindings: 10

MAC Address	IP Address	VLAN	Interface	Type	Lease (min)
00:0B:DB:74:3A:DE	10.14.236.64	2	ge.1.21	DYNAMIC	1425
00:13:02:A8:35:40	10.14.236.69	2	ge.1.41	DYNAMIC	802
00:15:C5:A4:10:93	10.14.236.68	2	ge.1.33	DYNAMIC	796
00:24:E8:DF:C3:9B	10.14.236.51	2	ge.1.31	DYNAMIC	490
00:24:E8:F5:83:83	10.14.236.50	2	ge.1.19	DYNAMIC	767
00:26:B9:96:56:A9	10.14.236.70	2	ge.1.13	DYNAMIC	971
00:26:B9:9F:59:28	10.14.236.62	2	ge.1.7	DYNAMIC	545
00:26:B9:D9:BE:30	10.14.236.75	2	ge.1.37	DYNAMIC	550
18:86:AC:1E:D4:49	10.14.236.72	2	ge.1.41	DYNAMIC	929
B8:AC:6F:2B:15:A5	10.14.236.61	2	ge.1.5	DYNAMIC	365

DHCP-Snooping-Binding-Datenbank

Konfiguration von Dynamic ARP Inspection

- Die ARP-Inspektion wird global auf dem Switch per VLAN konfiguriert.
- Die ARP-Inspektion kennt analog zu DHCP Snooping trusted und untrusted Ports.
- Auf Trusted Ports findet keine DAI-Prüfung statt. Trusted Ports müssen explizit per Port-Level definiert werden. Die restlichen Ports sind untrusted.
- Trusted DAI Ports sind Switch-to-Switch Ports oder Ports, an denen der DHCP-Server erreichbar ist (analog zu DHCP-Snooping)
- Um Flooding-Angriffe mittels ARP-Nachrichten zu verhindern, kann auf untrusted Port zusätzlich eine maximale Anzahl an ARP-Nachrichten pro Sekunde definiert werden. Wird diese Anzahl überschritten verwirft der Switch die das Limit überschreitenden ARP-Nachrichten und schreibt einen entsprochenen Log-Eintrag.

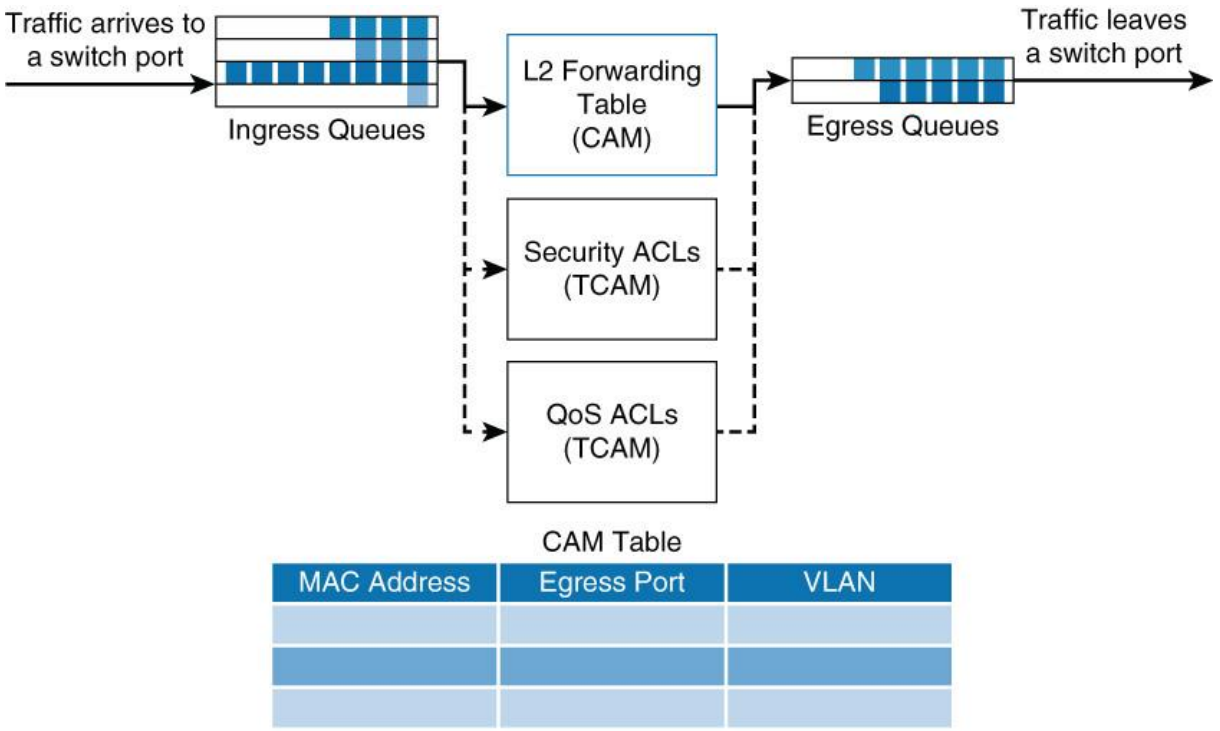
```
!Aktivieren von DAI für die vlans 5-9, 15
S1(config)# ip arp inspection vlan 5-9,15
!Definition von G0/1 als trusted DAI Ports
S1(config)# interface GigabitEthernet0/1
S1(config-if)# ip arp inspection trust
S1(config-if)# exit
! Aktivieren einer max. Anzahl an ARP-Nachrichten
! auf dem untrusted Port f0/18
S1(config)# interface FastEthernet0/18
S1(config-if)# ip arp inspection limit rate 20
```

Beispiel für eine Log-Nachricht

```
%SW_DAI-4-PACKET_RATE_EXCEEDED: 20 packets/sec
threshold exceeded on FastEthernet0/18
```

MAC-Address-Flooding

- Die MAC-Adresstabelle (Forwarding-Tabelle) eines Switches wird in dem CAM (Content Adressable Memory) gespeichert. Je nach Größe des Speichers kann eine unterschiedliche Anzahl an MAC-Adressen gelernt werden:
  - Kleine Switche: < 16.000
  - Mittlere Switche: < 128.000
  - Große Switche: < 256.000
- MAC-Address-Flooding ist eine Angriffsform, bei der ein Angreifer versucht den Switch mit nachgeahmten (spoofed) Source-MAC-Adressen über einen einzelnen Access-Ports zu überhäufen, mit dem Ziel einen Überlauf in der Forwarding-Tabelle zu generieren.
- In Folge dieses Überlaufs geht der Switch in einen „fail-open“ Modus über. Er arbeitet dann als HUB und flutet jedes neu empfangene Frame auf alle Interfaces.
- Der Angreifer kann alle Frames lesen.



MAC-Adresstabelle

Content Addressable Memory (CAM): Suche im Speicher erfolgt mit Hilfe eines Suchworts (z.B.: MAC_Adresse). Gespeicherte Suchwörter bestehen aus 0 und 1 Bit

Ternary CAM (TCAM): Gespeicherte Suchwörter enthalten ein "X" (don't care) Flag: 1:10, 0:01, X:00

Port-Security: MAC-Address-Flooding

- Mittels der Port-Security Funktion kann MAC-Adress-Flooding verhindert werden.
- Port-Security definiert pro Port eine maximale Anzahl an unterschiedlichen MAC-Adressen, die pro Port gelernt werden können (default: 1).
- Wird diese Anzahl überschritten kann mittels der violation-Anweisung
  - shutdown: das Interface deaktiviert und nach einem Recovery-Intervall wieder automatisch aktiviert werden.
  - restrict: die Frames mit noch nicht gelernter MAC-Adresse gelöscht und die Anzahl an Überschreitungen mittels eines "Violation Counter" in einem Log-File gespeichert werden.
- Achtung: Bei Virtualisierungshost können durchaus eine große Anzahl an MAC-Adressen pro Port für die unterschiedlichen virtuellen Maschinen auftreten (10 – 30.

- Beispiel: Das folgende Beispiel zeigt die Definition von Port-Security auf dem Interface f0/18 des Switches S1. Es sind maximal 10 unterschiedliche MAC-Adressen erlaubt.

```
S1(config)# interface f0/18
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 10
S1(config-if)# switchport port-security violation shutdown
```

- Definition des Switch-weiten Recovery Intervalls auf 300s bei einer Port-Security Violation

```
!Reset Error
S1(config)# errdisable recovery cause psecure-violation
!Recover after 300s
S1(config)# errdisable recovery interval 300
```

IP-Spoofing und IP Source Guard

- IP-Spoofing: Neben dem Nachahmen der MAC-Adresse kann ein Angreifer auch seine IP-Adresse fälschen.
- IP-Spoofing kann in Kombination mit anderen Techniken (z.B.: TCP-SYN-Flooding) für einen DoS-Angriff genutzt werden.
- IP Source Guard kann IP Spoofing mitigieren.
- IP Source Guard untersucht jedes eingehende Paket, das über einen untrusted DHCP-Snooping-Port empfangen wird.
- Dazu vergleicht IP Source Guard die im Paket gespeicherte Kombnation an Adressen:

```
(Source-IP-Adresse, Source-MAC-Adresse, VLAN-ID)
```

  mit den Einträgen in der sogenannten IP Source Binding Tabelle gespeichert sind.

- Diese Tabelle wird aus den Einträgen der DHCP-Snooping-Datenbank gefüllt und kann durch manuelle Einträge erweitert werden.
- Wenn die Einträge in dem eingehenden IP-Paket-Header nicht mit einem gültigen Eintrag in der IP Source Binding Tabelle übereinstimmt, verwirft der Switch das Paket.
- IP Source Guard muss pro Port aktiviert werden.

1. DHCP-Snooping muss aktiviert sein, um die IP-zu-MAC-Adresstabelle zu erstellen.
2. Wenn ein Client eine IP-Adresse über DHCP erhält, speichert der Switch diese Information.
3. IP Source Guard wird auf einen bestimmten Switch-Port (nicht vertrauenswürdiger Port) angewendet.
4. Wenn ein nicht autorisiertes Gerät versucht, Pakete mit einer IP-Adresse zu senden, die nicht an diesen Port gebunden ist (Spoofing), verwirft der Switch die Pakete.

Konfiguration IP Source Guard

- Beispiel: Aktivieren von IP Source Guard auf dem untrusted `Port f0/18` für Endgeräte

```
S1(config)#int f0/18
S1(config-if)# switchport mode access
!Activating IP Source Guard on Interface
S1(config-if)# ip verify source port-security
S1(config-if)# ip verify source port-security violation {protect |
                    restrict | shutdown}
```

  - protect: Verwirft Pakete mit ungültigen IP- oder MAC-Adresspaaren, generiert aber keine Protokolleinträge und schaltet den Port nicht ab.
  - restrict: Verwirft Pakete mit ungültigen (IP-Addr., MAC-Addr.)-Paaren und generiert Protokolleinträge.
  - shutdown: Schaltet den Port ab und versetzt ihn in einen fehlerdeaktivierten Zustand und generiert einen Protokolleintrag.

- Beispiel: Hinzufügen einer statischen IP-MAC-Bindung auf einem Switch für das VLAN 11 auf dem Interface g0/1, beispielsweise für einen Router oder Server mit statischer IP-Adresse:

  MAC-Addr.: 01:00:02:30:00:02

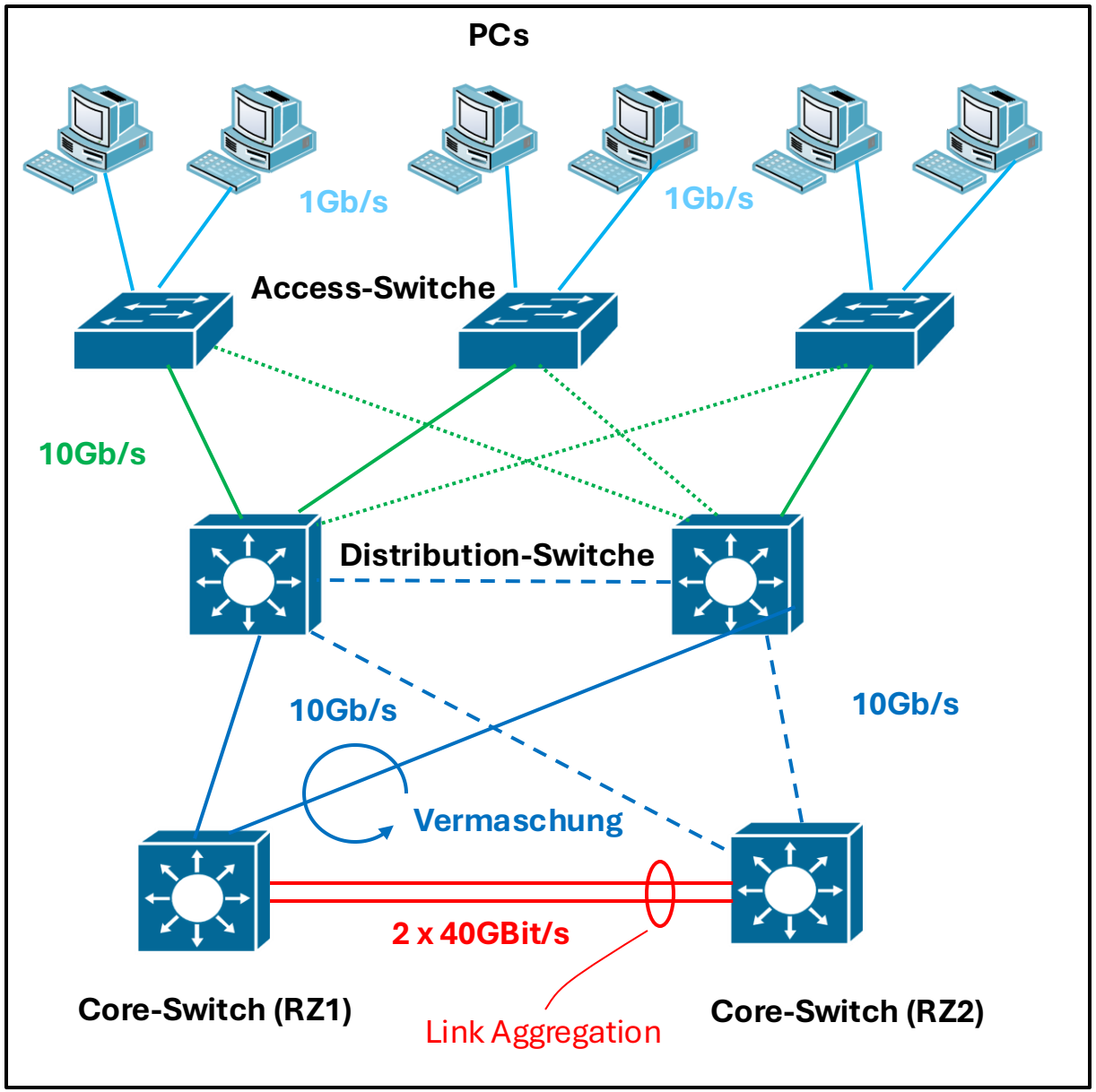
  IP-Addr.: 10.0.0.4

```
!Hinzufügen einer statischen Adresse zur
!IP Source Binding table
S1(config)# ip source binding 0100.0230.0002 vlan 11
                                10.0.0.4 interface g0/1
```

Safe Physical Operation mit Spanning Tree Protocol

- Um einen Single-Point-of-Failure im Backbone (Core-Tier) zu vermeiden, wird jeder Distribution-Switch mit beiden Core-Switchen verbunden.
- Pro Distributionsswitch entstehen somit mehrere Wege in den Backbone des Netzwerkes. Man spricht auch von einem vermaschten Netzwerk.
- Dadurch wird die Betriebssicherheit erhöht, da trotz des Ausfalls eines Core-Switches die betroffenen Endsysteme weiterarbeiten können.
- Physikalisch entsteht eine Schleife (engl. loop) zwischen den Core-Switchen und dem Distribution-Switch, diese muss logisch per Layer-2-Protokoll (STP) aufgehoben werden.
- Auch für die Access-Switch kann eine Vermaschung zu den Distribution-Switchen durchgeführt werden, umso einen Single-Point-of-Failure in der Distributionsschicht zu umgehen (gestrichelte grüne Linien).

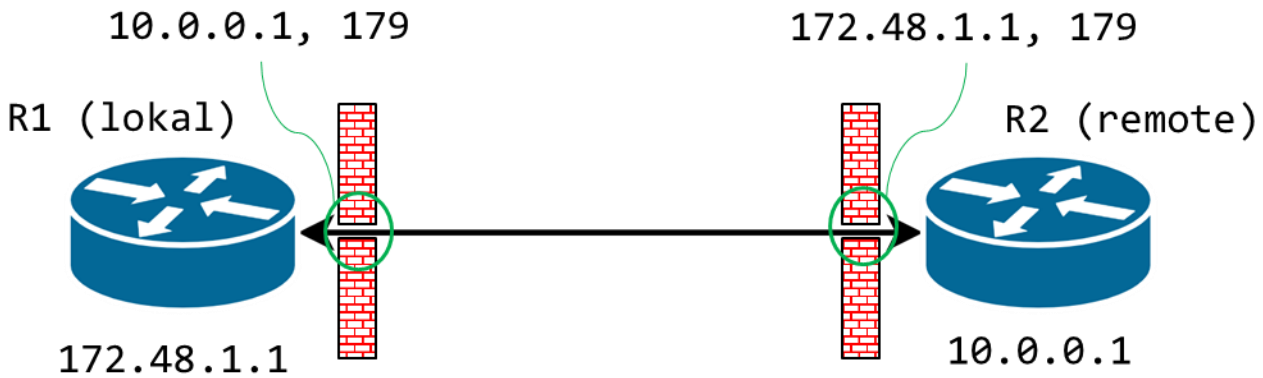
Das Drei-Ebenen-Netzwerkmodell



Allgemeine Richtlinien zur Härtung des administrativen Zugriffs

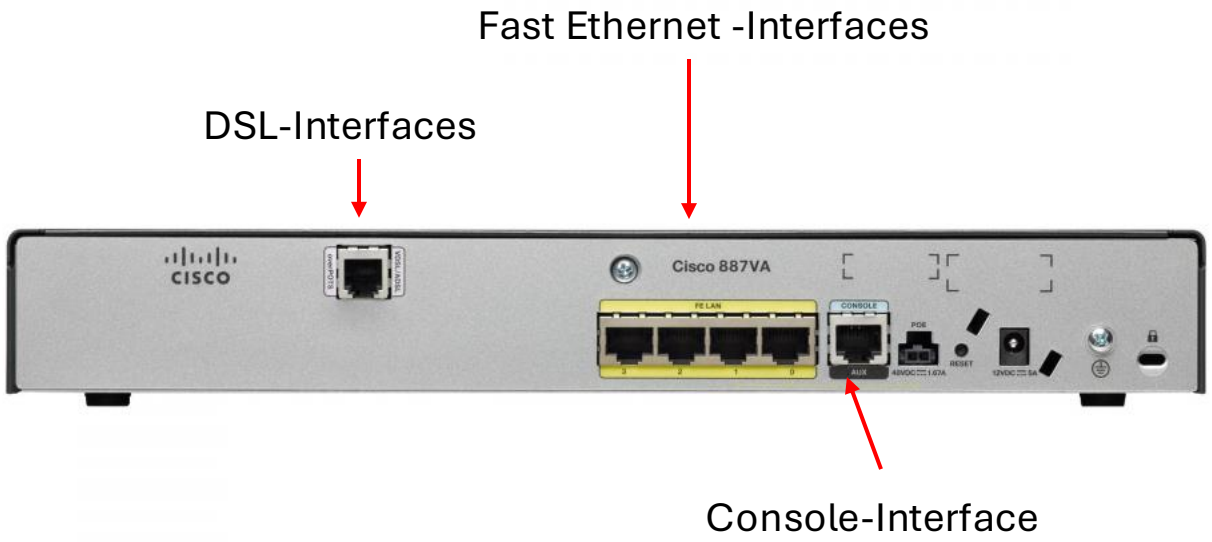
- Richtlinien zur Absicherung von Netzwerkgeräten
  - Der Console-Zugriffspunkt sollte nur für die initiale Konfiguration des Gerätes verwendet werden.
  - Jeder Zugriffspunkt sollte mit einem komplexen Passwort geschützt werden.
  - Passwörter sollten nur gehashed gespeichert werden.
  - Für jeden Netzwerk-Administrator einen eigenen Admin-Benutzer in einem zentralen Authentifizierungs-Server (AAA) angelegen.
  - Netzwerkbasierender Zugriff muss verschlüsselt und signiert werden.
  - Verwendung eines dedizierten Management Netzwerk für den administrativen Zugriff.
  - Vermeidung von Backdoor-Verbindungen: Trennung von Management- und Datennetzwerk durch die Verwendung von unterschiedlichen physikalischen Interfaces (separater Mgmt.-Port) und logischer Trennung mittels ACLs.
  - Nicht verwendete Switch-/Router-Ports sollte prinzipiell deaktiviert werden, um die Angriffsfläche zu verringern.
  - Nicht benötigte Services sollten deaktiviert und wenn möglich deinstalliert werden.
  - Aktivierung des Logging für Events und weiterleiten der Events zu einem zentralen Syslog-Server.
  - snmp v3 (Simple Network Management Protocol) für die Systemüberwachung von End- und Netzwerkgeräten.
  - Zeitsynchronisation der Uhren aller Netzwerkgeräte mittels ntp (Network Time Protocol).

1.4 Sicherer Betrieb von Netzwerken mit Routern



Router

- Router arbeiten auf dem Layer-3.
- Zentrale Funktion von Router ist die Weiterleitung von IP-Paketen auf einer optimalen (schnellsten) Route.
- Die Absicherung des Routers auf der Management-Ebene erfolgt analog zu Switchen:
  - Sicheres Passwort Management
  - Sichere Remote Administration per ssh
  - Authentification, Authorization und Accounting (AAA)
  - Zentrales Sys-Logging
  - SNMP-Überwachung des Routers
  - Schutz durch ACL (ACL)
  - NTP-Zeitserver für die Uhrensynchronisation im Netzwerk
  - Deaktivieren nicht benötigter Services und Ports



Standard versus Extended ACLs

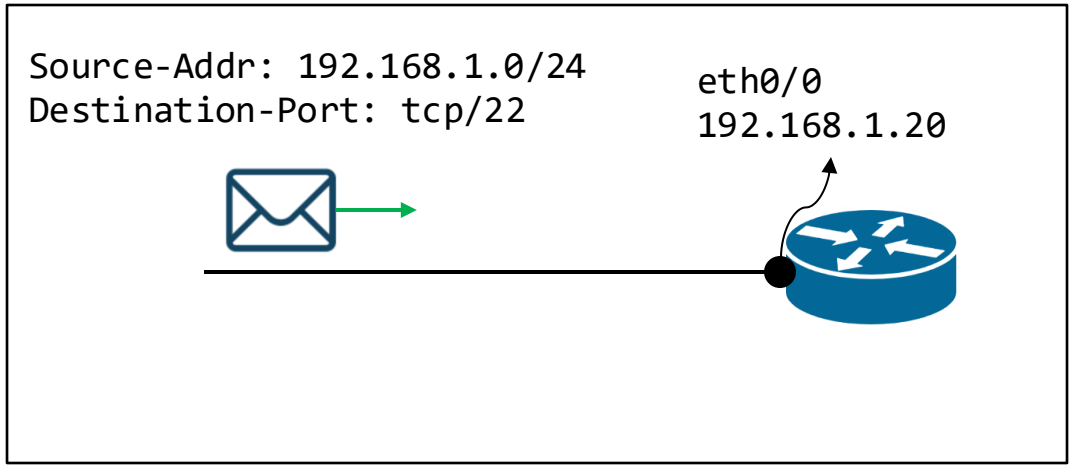
- Standard ACL
  - Überprüfen nur die IP-Source-Adresse eines Paketes
  - Erlaubt oder verweigert das IP-Paket unabhängig von den verwendeten Upper-Protokollen (TCP/UDP, HTTP, ...)
- Extended ACL
  - Überprüft die IP-Source- und IP-Destination-Adresse eines Paketes
  - Erlaubt oder verweigert das IP-Paket in Abhängigkeit vom Transportprotokoll (TCP/UDP) und dem Applikationsprotokoll (HTTP, SSH, ...).

ACL-Type	Number Range / Identifier
Number for Standard	1-99, 1300-1999
Number for Extended	100-199, 2000-2699
Name (Standard and Extended)	Name: "MYACCESSLIST"

Infrastructure ACLs

- Access Control Listen (ACL) eignen sich, um den erlaubten Datenfluss (Control-Plane) zwischen Netzwerken zu steuern.
- ACL-Listen werden einem Interface zugeordnet. Bei der Zuordnung wird definiert, ob die Regel auf eingehenden oder ausgehenden Datenverkehr angewandt werden soll.
- Beispiel: Definiere eine extended ACL die nur Maschinen aus dem Management-Netzwerk (192.168.1.0/24) einen SSH-Zugriff auf das loopback-Interface (`192.168.1.20`) eines Routers erlaubt:

- Eine permit-Zugriffsliste bewirkt für alle anderen Adressen und Ports implizit eine "access-list deny ip any any" Zugriffregel, sodass nur der explizit definierte permit-Verkehr erlaubt ist.




```
R1(config)# access-list 101 permit tcp 192.168.1.0 0.0.0.255 host 192.168.1.20 eq 22
```

Transport-Protokoll

Bitmaske

Port

eindeutige Nummer (100 – 199)

Source (IP-Subnetz)

Destination (1 Host, Port 22)

ACLs und Bitmasken

- Bitmasken werden mit IP-Adressen in ACLs verwendet, um festzulegen, welche Adressen von der ACL betroffen sind.
- Bitmaske als Filter:

  0: Adressbit muss übereinstimmen

  1: Adressbit muss nicht übereinstimmen, Wildcard
- Bestimmte Source Wildcard Kombinationen haben einen Namen erhalten
  - Jede IP-Adresse "111....1"

    any (source wildcard): 0.0.0.0 255.255.255.255
  - Genau eine IP-Adresse "000....0"

    host (source wildcard): 172.48.1.1 0.0.0.0

- Allgemeine Regeln für ACLs
- "first match"- Prinzip:
  - ACLs werden in der Reihenfolge abgearbeitet, in der sie eingegeben werden.
  - Je spezifischer die Information einer ACL, desto früher (vorne) in der Liste der ACLs sollte sie angesiedelt sein.
  - Nachträgliches Einfügen von ACLs ist nicht möglich (Ausnahme: Löschen einzelner Zeilen in Named Access Lists.)
- "implicit deny"-Prinzip:
  - Nicht explizit erlaubte Kommunikation ist verboten.
  - Security-Prinzip: "Default-is-Deny"

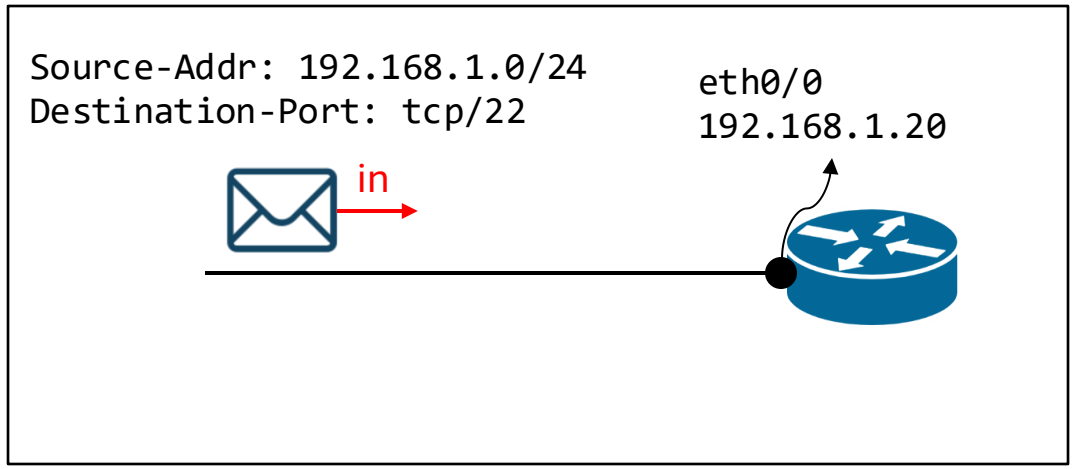
Port-Zuweisung von ACL

- Die Access-Listen müssen einem Router-Interface zugeordnet werden.
- Hierzu verwendet man sogenannte Access-Groups.

```
R1(config-if)#ip access-group {accesslistnumber | name}  {in | out}
```

- Die Access-Group spezifiziert die für das Interface anzuwendende ACL und definiert zusätzlich ob der eingehende Verkehr ("in") oder der ausgehende Verkehr ("out") gefiltert werden soll.
- Beispiel: Router-Interface eth0/0 erhält die IP-Adresse 172.48.1.1. Zusätzlich soll die ACL mit der Nummer 101 auf eingehenden Verkehr "in" angewendet werden. Die ACL soll eingehenden ssh-Verkehr erlauben.

```
R1(config)# access-list 101 permit tcp 192.168.1.0
0.0.0.255 host 192.168.1.20 eq 22
!Configure ACL on Interface
R1(config)# int eth0/0
R1(config-if)# ip address 192.168.1.20 255.255.255.0
R1(config-if)# ip access-group 101 in
```



Inbound ACL vs Outbound ACL

Inbound Access List ("in"): Eingehender Datenverkehr

Vor der Verarbeitung also dem Routing des Paketes wird zuerst die ACL geprüft.

Ist das Paket zulässig wird das Routing durchgeführt.

Outbound Access List ("out"): Ausgehenden Datenverkehr

Eingehendes Packet wird zuerst an das Ausgangsinterface geroutet.

Erst unmittelbar vor der Versendung des Paketes wird mittels der ACL geprüft, ob das

Paket überhaupt weitergesendet werden darf.

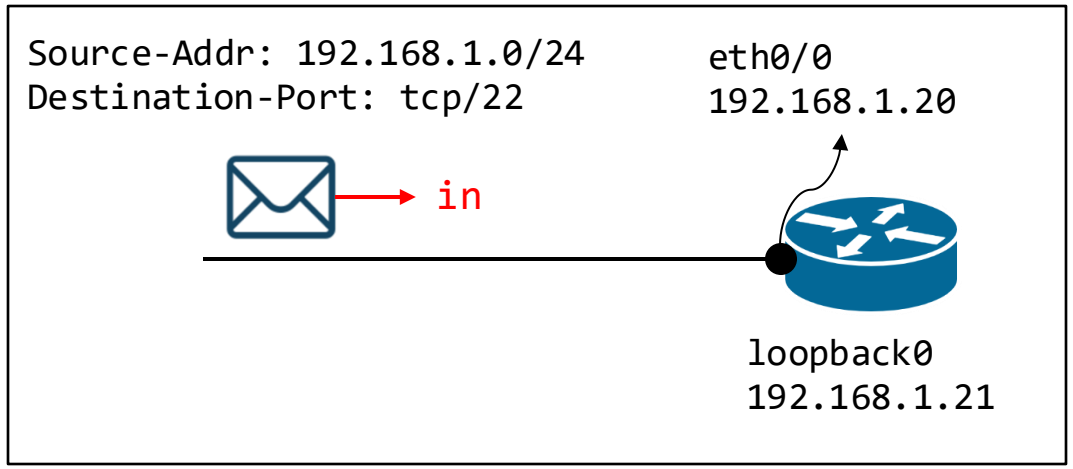
Beispiel: Extended ACL für Loopback-Adresse auf Router

- Auf einem Router kann eine sogenannte Loopback-Adresse konfiguriert werden. Eine Loopback-Adresse ist eine logische Schnittstelle, die immer "up" bleibt, solange der Router läuft.
- Sie ist unabhängig von dem Zustand einer phys. Schnitt-stelle und eignet sich von daher, um einen Management-Zugriff unabhängig vom Status eines Interfaces zu erhalten.
- Loopback-Adressen werden häufig als eindeutige Identifikatoren, der sogenannten Router-ID in Routing-Protokollen wie OSPF oder BGP verwendet.

```
!Activate ACL on Loopback-Interface
Router# configure terminal
Router(config)# hostname R1

!Configuration loopback Interface 0
R1(config)#interface Loopback 0
R1(config)# ip address 192.168.1.21 255.255.255.0
R1(config-if)# description Loopback for Management Access
R1(config-if)# exit
```

Beispiel: Extended ACL für Loopback-Adresse auf Router

- Um auf eine Loopback-Adresse nur bestimmte Zugriffs-typen (ssh, snmp, icmp) aus dem Management-Network (192.168.1.0) zuzulassen, können Sie eine extended ACL verwenden.



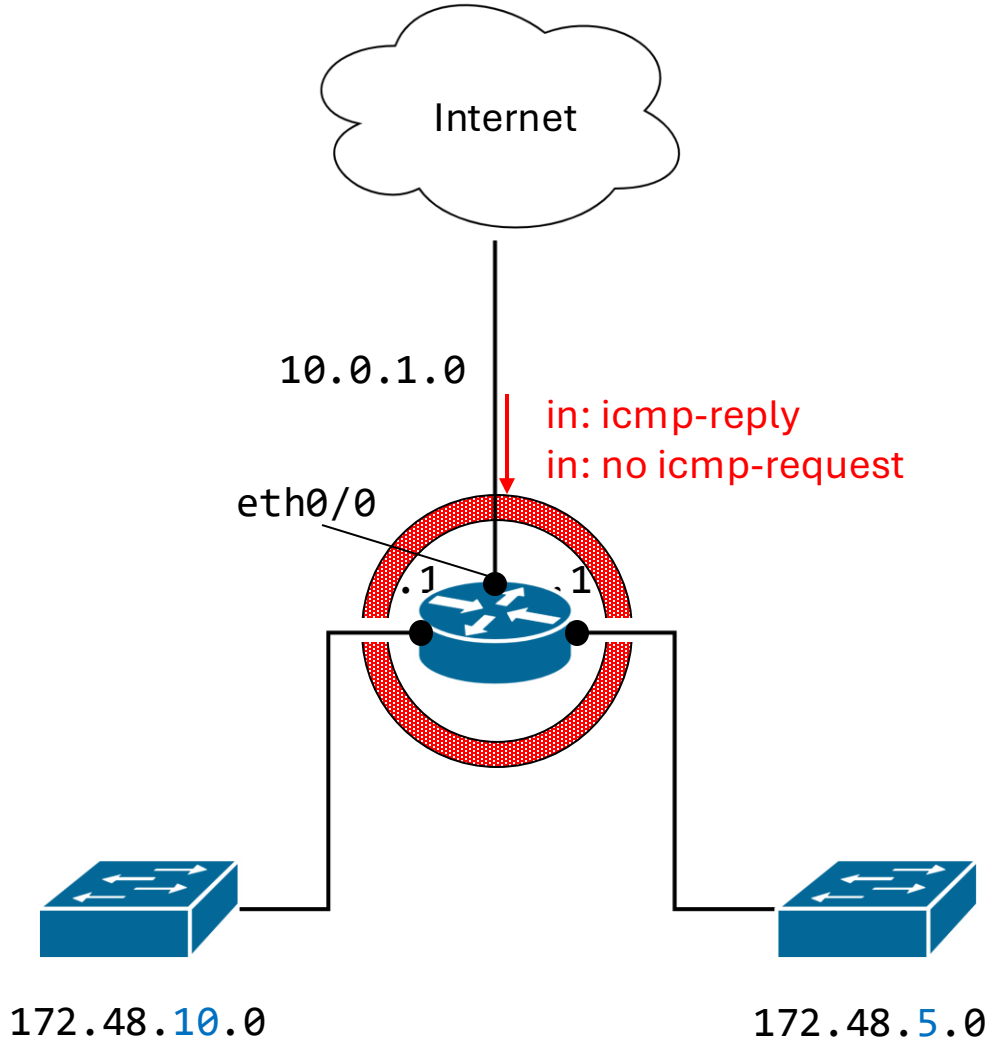

```
R1(config)# ip access-list extended MGMT_TRAFFIC
! Allow SSH from management network to loopback 0
R1(config)# permit tcp 192.168.1.0 0.0.0.255 host
192.168.1.21 eq 22 log
! Allow SNMP from management network
R1(config)# permit udp 192.168.1.0 0.0.0.255 host
192.168.1.21 eq 161 log
! Allow ICMP- Echo-Reply (ping) from management network
R1(config)# permit icmp 192.168.1.0 0.0.0.255 host
192.168.1.21 echo-reply log
!Deny all other traffic and log them to syslog
R1(config)# deny ip any host 192.168.1.21 log
R1(config)#exit
!Activate ACL on Loopback-Interface
R1(config)#  interface Loopback 0
R1(config-if)# ip access-group MGMT_TRAFFIC in
R1(config-if)# exit
```

Beispiel: ICMP-Verkehr am Edge-Interface

Szenario: Um ihr Netzwerk vor unerwünschten "Scan"-Versuche zu schützen aber selbst nach außen Scans starten zu können, implementieren Sie am Eingangs-Interface (eth0/0) ihres Edge-Routers die folgende ACL:

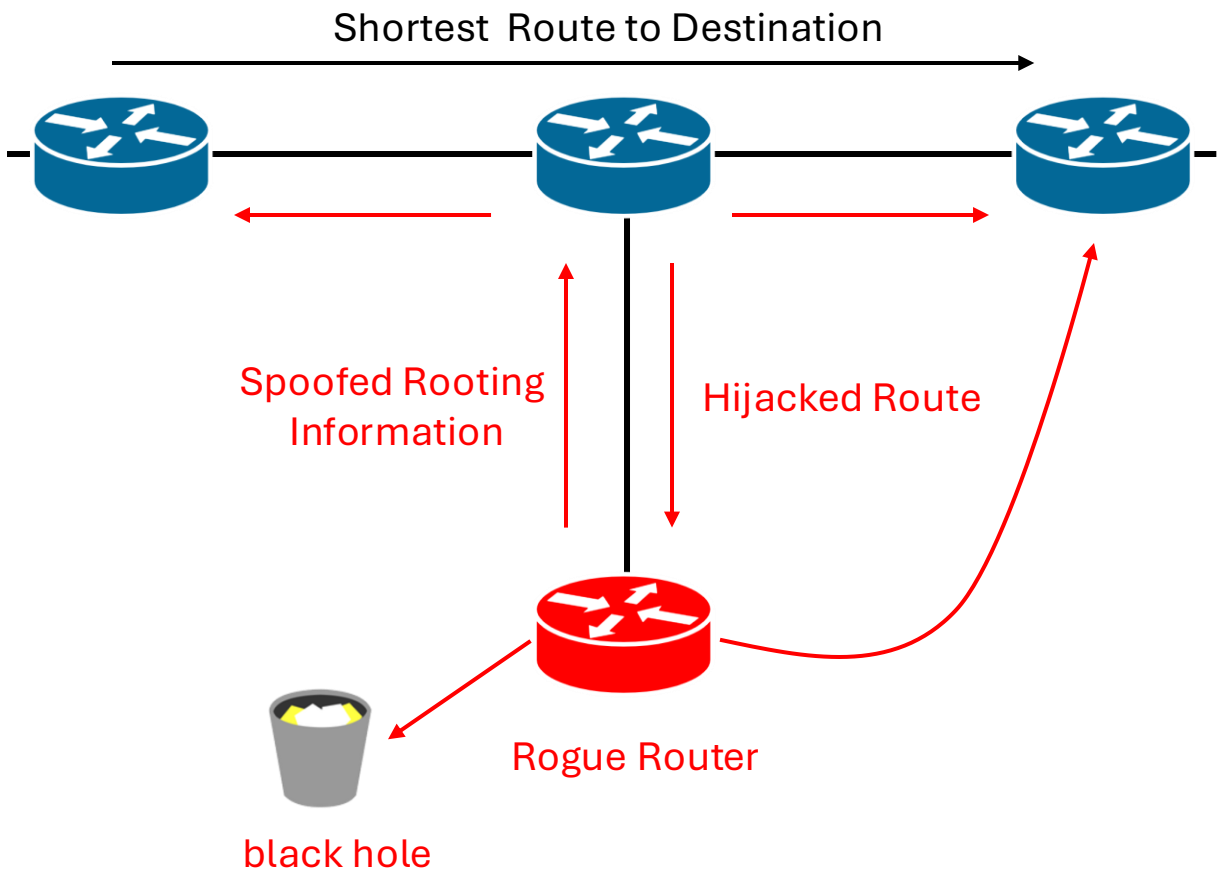
- Ingress-Verkehr aus dem Internet: ICMP-Echo-Request blockieren.
- Ingress-Verkehr aus dem Internet: ICMP-Echo-Reply durchgelassen werden.

```
#ip access-list extended ICMP_ACL
!Allow ICMP echo replies
#permit icmp any any echo-reply
!Deny incoming ICMP echo requests (pings) from any source
#deny icmp any any echo-request log
#interface Eth0/0
!Apply the ACL to incoming traffic
#ip access-group ICMP_ACL in
```



Route HiJacking

- Durch das Fälschen von Routing-Informationen kann sowohl die Netzwerkstabilität (DoS) als auch die Vertraulichkeit (Information Disclosure) von Daten verletzt werden.
- Netzwerkstabilität:
  - Löschen von Daten: Ein Angreifer leitet den Datenverkehr in ein schwarzes Loch (black hole: /dev/null) um.
  - Leitungsüberlastung: Backbone-Datenverkehr auf einer 10Gb-Transitverbindung wird über eine 1Gb-Verbindung geschickt, was zu einer Leitungsüberlastung führt.
- Vertraulichkeit
  - Angreifer leitet den Datenverkehr über seinen Rogue-Router um und kann so die Daten für eine spätere Analyse erfassen.



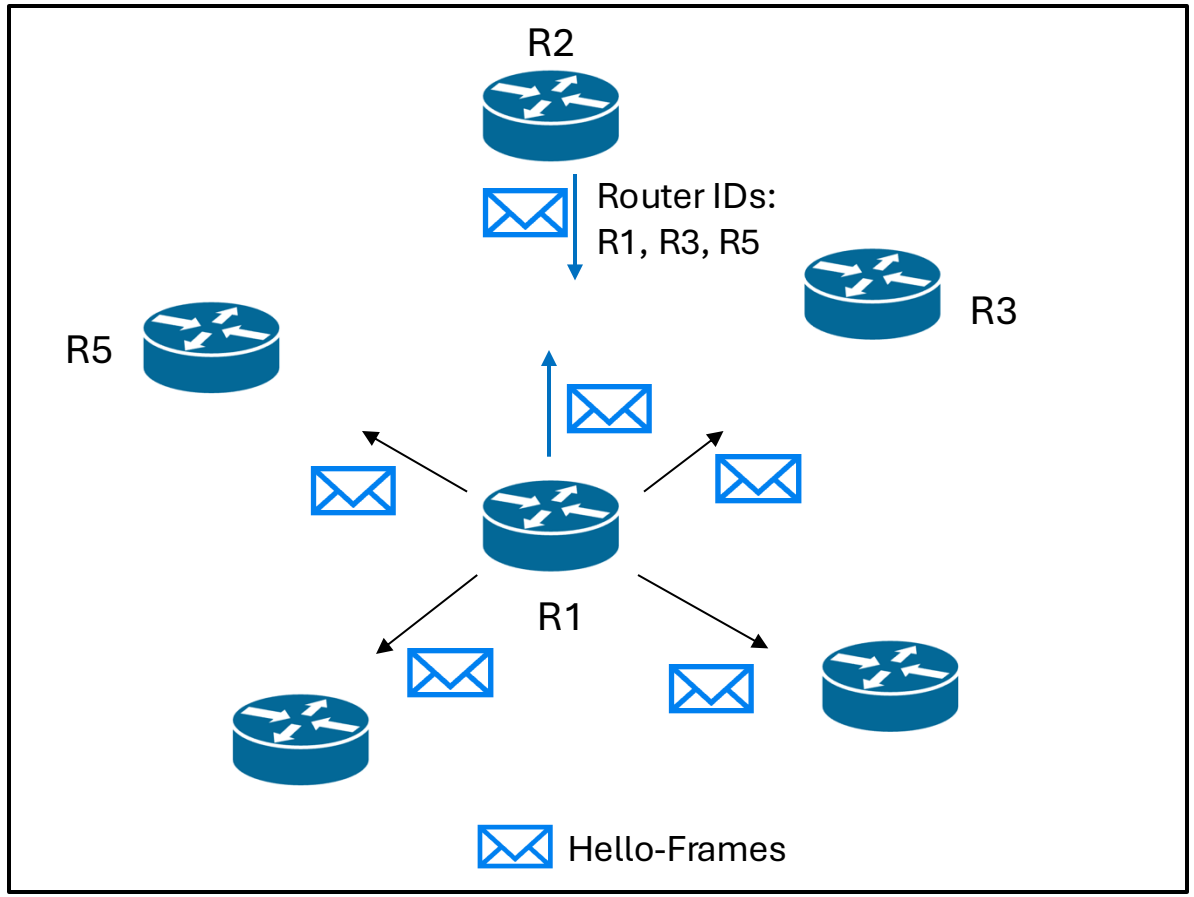
OSPF-Protokoll

- OSPF ist ein weit verbreitetes Routing-Protokoll für das Intra-Gateway-Routing.
- OSPF verwendet die folgenden Basiskonzepte
- Multicast- (224.0.0.5, 224.0.0.6) Pakete für die Verteilung Router-Topologie und Pflege der Router-Nachbarschaft
  - Hello-Nachrichten
  - Link-State-Advertisement (LSA)
  - Link-State-Acknowledgement (LSAck)
- Unicast-Pakete um die Retransmssion von LSA-Advertisments bei einem bestimmten Nachbarn anzufordern
  - Link-State-Request (LSR)
  - Link-State-Update (LSU)
  - Link-State-Acknowledgement (LSAck)

OSPF-Protokoll: Nachbarschaft

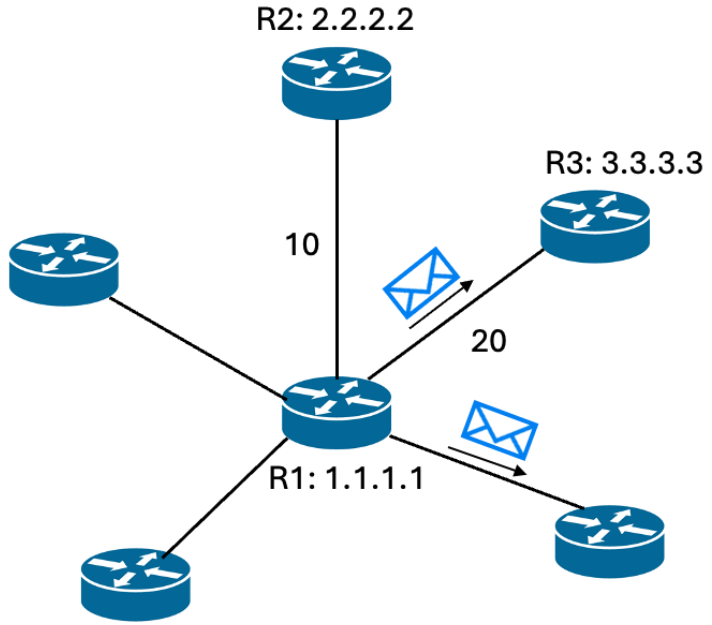
- Hello – Nachrichten:
  - Hello-Pakete sind Pakete, die ein OSPF-Prozess an seine OSPF-Nachbarn sendet. Sie dienen der Nachbarschafts-erkennung und der Aufrechterhaltung von Nachbar-schaftsbeziehungen
  - Die Hello-Pakete werden in einem konfigurierbaren Intervall (Default: 30s) gesendet.
  - Erkennung von Nachbarn: Wenn ein Router ein Hello-Paket von einem Nachbarn empfängt, trägt er die Router-ID des Nachbarn in sein nächstes Hello-Paket ein. Der Nachbar erkennt anhand dieser Liste, dass der Router seine Hello-Pakete empfangen hat. Dies fungiert als eine implizite Bestätigung.

- Aufrechterhaltung: Wenn ein Router innerhalb des soge-nannten Dead-Intervalls (4 x Hello-Intervall) kein Hello-Frame von einem Nachbarn erhält, erklärt er den Router als heruntergefahren



OSPF-Protokoll

- Link-State-Advertisements – Nachrichten (LSA):
  - LSA-Pakete enthalten die komplette Netzwerktopologie aus Sicht des einzelnen Routers (Links, IP-Adressen, Kosten zu seinen Nachbarn)
  - LSAs werden per OSPF Flooding an alle Router in einem Netzwerk weitergeleitet.
  - Trusted Neighbor: Jeder Router vertraut per se der von den Nachbarroutern erhaltenen LSA-Information.
    Beispiel: R2 vertraut der Info von R1 das Pfadkosten von R1 zu R3 20 betragen.
  - Fight-Back-Mechanism: Wenn ein Router eine LSA erhält, die eine falsche Routing-Information über den Router selbst enthält, sendet der Router sofort eine korrigierende LSA senden.
    Beispiel: R3 erkennt eine falsche Kosteninfo in der LSA von R1 und korrigiert diese.

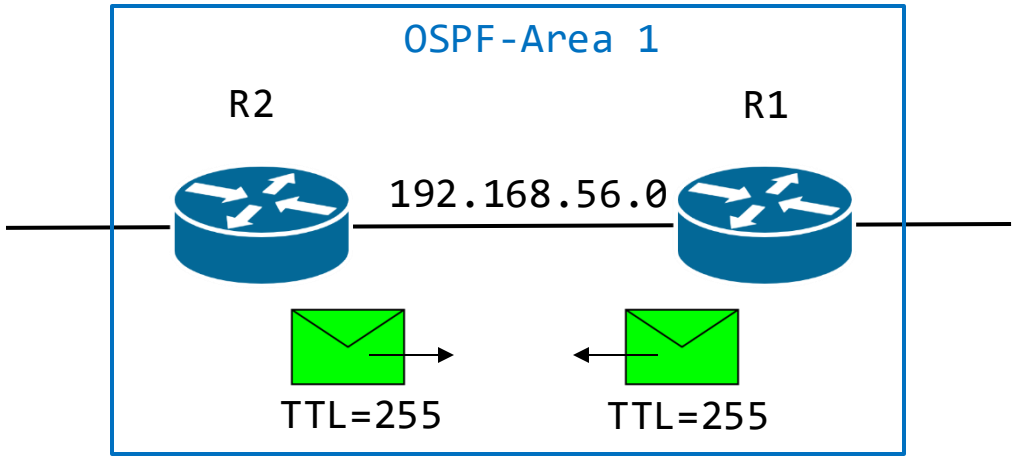



```
Router-LSA (Type 1) von Router R1:
Router ID: 1.1.1.1
Links:
  1. Link Type: Point-to-Point
       Link ID: 2.2.2.2 (R2 Router ID)
       Link Data: N/A (Point-to-point)
       Link Cost: 10
       Neighbors: 2.2.2.2 (Router R2)
  2. Link Type: Point-to-Point
       Link ID: 3.3.3.3 (R3 Router ID)
       Link Data: N/A (Point-to-point)
       Link Cost: 20
       Neighbors: 3.3.3.3 (Router R3)
```

OSPF TTL Security

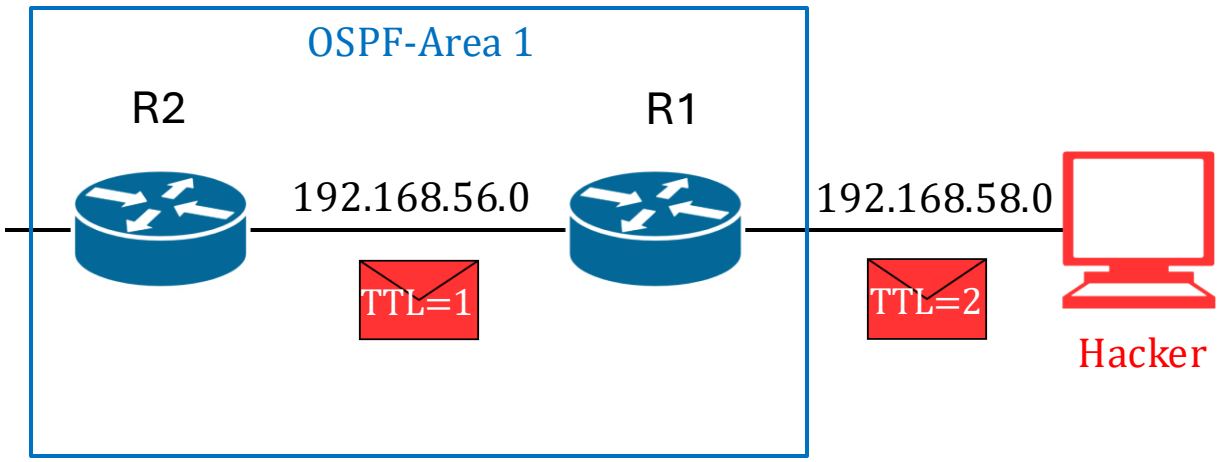
- OSPF versendet LSA-Nachrichten per Default mit einer TTL=1 (Nächster Router = Nachbar).
- Die OSPF-TTL-Sicherheitsprüfung ist ein Mechanismus, der OSPF vor Remote-Angriffen schützt. Wenn diese Funktion aktiviert wurde, sendet OSPF seine Pakete mit einer TTL von 255 und lehnt alle Pakete mit einer TTL ab, die kleiner als ein konfigurierter Schwellenwert (default: 254) ist.
- Das bedeutet das OSPF TTL Security standardmäßig nur Pakete mit einer TTL > 254 weitergeleitet. Da das Routing die TTL um eins verringert, bedeutet dies, dass nur OSPF-Pakete von direkt verbundenen Routern empfangen werden können.
- Beispiel: Konfiguration von zwei OSPF-Prozessen (10, 15) auf zwei benachbarten Router R1 und Router R2 die sich in derselben OSPF-Area 1 befinden. Beide werden mit TTL Security konfiguriert.

```
R1(config)#router ospf 10
R1(config-router)#network 192.168.56.0 0.0.0.255 area 1
R1(config-router)# ttl-security all-interfaces hops 254
R1(config-router)#exit
-----------------------------------------------
R2(config)#router ospf 15
R2(config-router)#network 192.168.56.0 0.0.0.255 area 1
R2(config-router)#ttl-security all-interfaces hops 254
R2(config-router)#exit
```

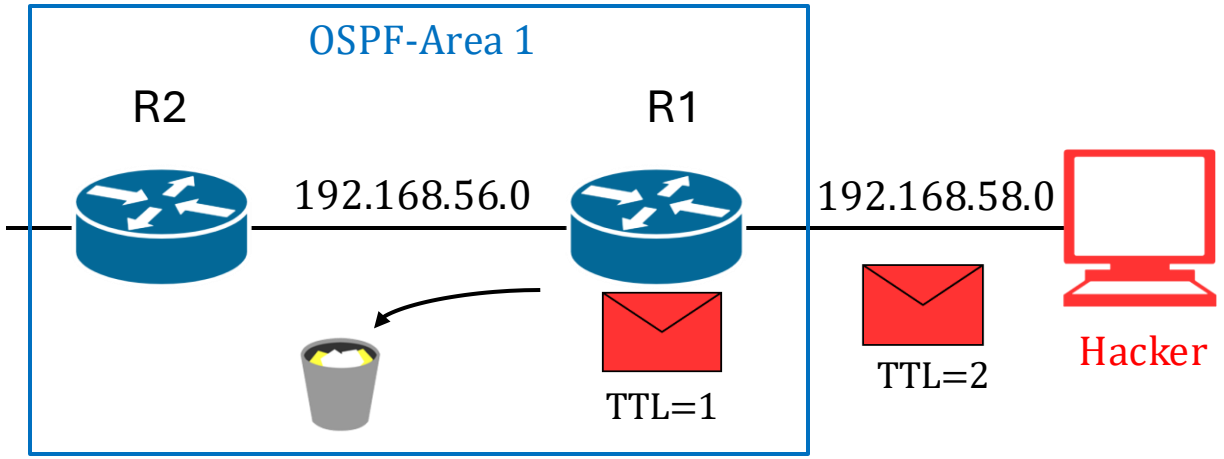


OSPF TTL Security

- Im nachfolgenden Diagramm sendet der Hacker eine Unicast Nachricht mit TTL=2 an Router R2 und verwendet die Source-Adresse von Router R1.
- Wenn R1 das Paket empfängt, verringert es die TTL um 1 und sendet es an R2.
  R2 empfängt das Paket denkt dass es von R1 stammt und verarbeitet die Information.



- Nach der Aktivierung von TTL-Security werden alle OSPF-Nachrichten mit dem Maximalwert TTL=255 verschickt.
- Empfängt R1 das vom Hacker gefälschte Paket, erkennt der Router an der TTL=2 das eine Fälschung vorliegt und verwirft der Router das Packet.



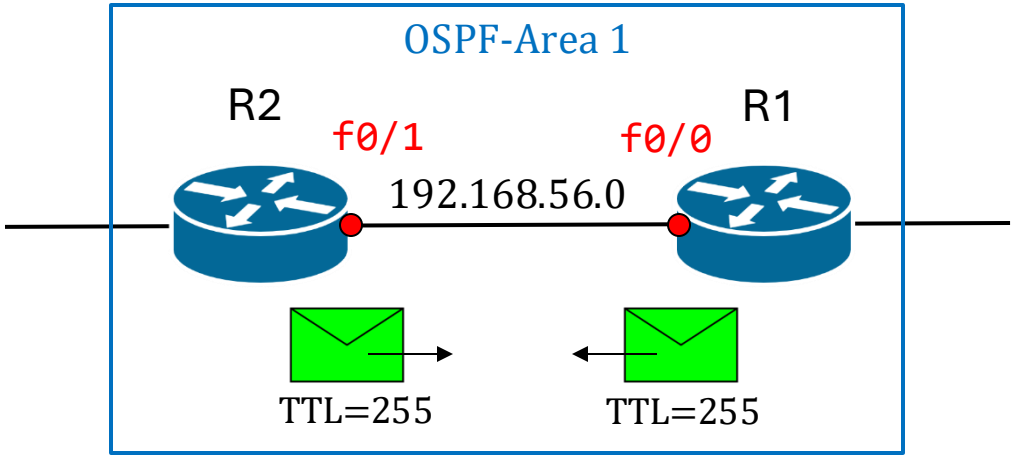
OSPF Authentification

- Per Default vertraut jeder Router den Nachrichten seiner benachbarten Router.
- OSPF unterstützt die Authentifizierung von ausgetauschten OSPF-Nachrichten zwischen 2 benachbarten Routern.
- OSPF unterstützt verschiedene Authentifzierungsverfahren
  - md5-Algorithmus: Berechnung eines HASH-Wertes für die OSPF-Nachricht mittels eines secrets und md5
  - HMAC-SHA-Algorithmus: Berechnung eines HASH-Wertes für die OSPF-Nachricht mittels secret key und SHA-Hashfunktion.

message-digist: "Nachrichtenzusammenfassung" in Form eines md5-Hash-Wertes.

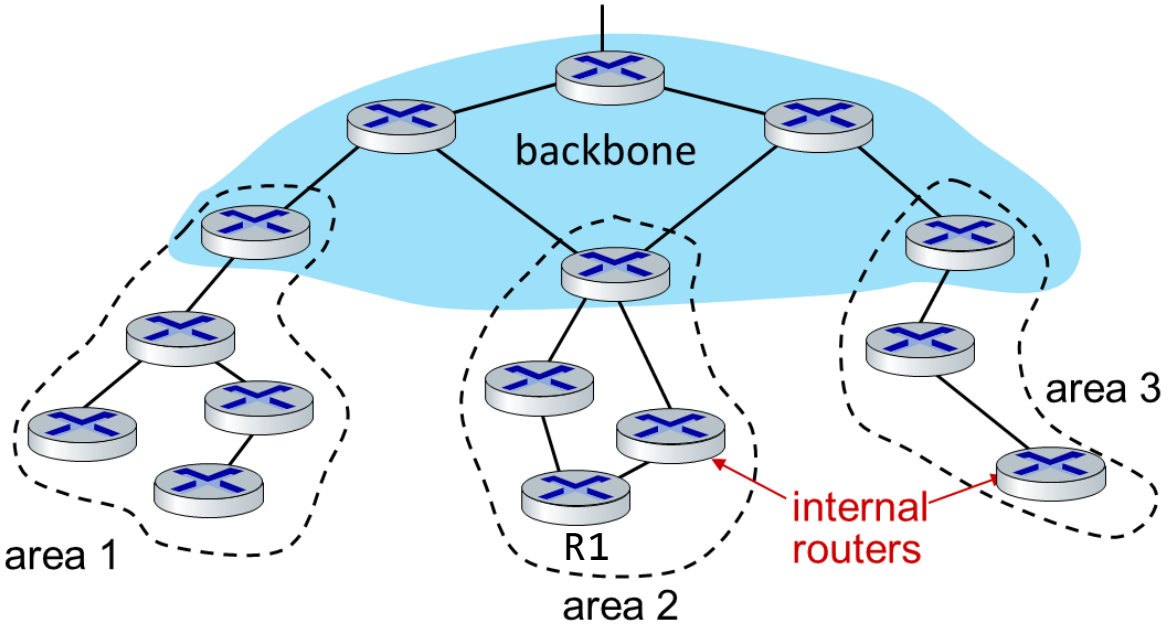
- Beispiel: Konfiguration zweier Router R1 und R2 mittels md5-Algorithmus mit einer key-id=1

```
R1(config)#interface f0/0
R1(config-if)#ip ospf message-digest-key 1 md5 <secret>
R1(config-if)#ip ospf authentication message-digest
-------------------------------------------------
R2(config)#interface f0/1
R2(config-if)#ip ospf message-digest-key 1 md5 <secret>
R2(config-if)#ip ospf authentication message-digest
```



OSPF Authentification für Areas

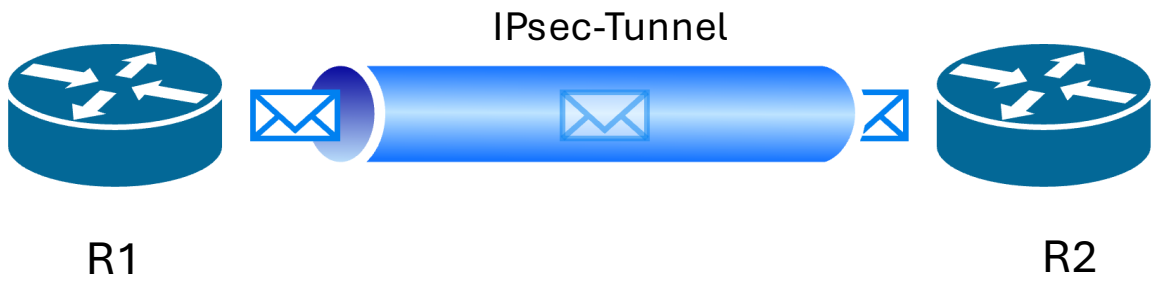
- OSPF Authentification sollte zusätzlich für die ganze OSPF-Area auf den teilnehmenden Routern konfiguriert werden.
- Dies erfolgt bei der Konfiguration des OSPF-Prozesses auf jedem Router.
- Beispiel: Aktivierung OSPF auf R1 mit Area2-Authentifizierung




```
!Define OSPF routing process with number 109
R1(config)# router ospf 109
!Define network interfaces to participate in area 2
R1(config-router)# network 172.10.0.0 0.0.255.255 area 2
!Define OSPF Authentification for area 2
R1(config-router) area 2 authentication message-digest

!Activate OSPF on interface f0/0
!Specify OSPF Authentification
R1(config)#interface f0/0
R1(config-if)#ip ospf message-digest-key 1 md5 <mypasswd>
R1(config-if)#ip ospf authentication message-digest
```

OSPF und IPsec: Verschlüsselung und Authentifizierung

- Durch die Verwendung des Protokolls IPSec (siehe hinten) kann Kommunikation zwischen OSPF-Routern verschlüsselt und gegenüber unerlaubter Veränderung geschützt werden.
  - Dazu wird zwischen 2 OSPF-Routern ein sogenannter IPsec-Tunnel aufgebaut.
  - Die OSPF-Nachrichten, wie z. B. Link-State Advertisements (LSAs) und Hello-Pakete werden in diesem Tunnel vertraulich und integer übertragen.

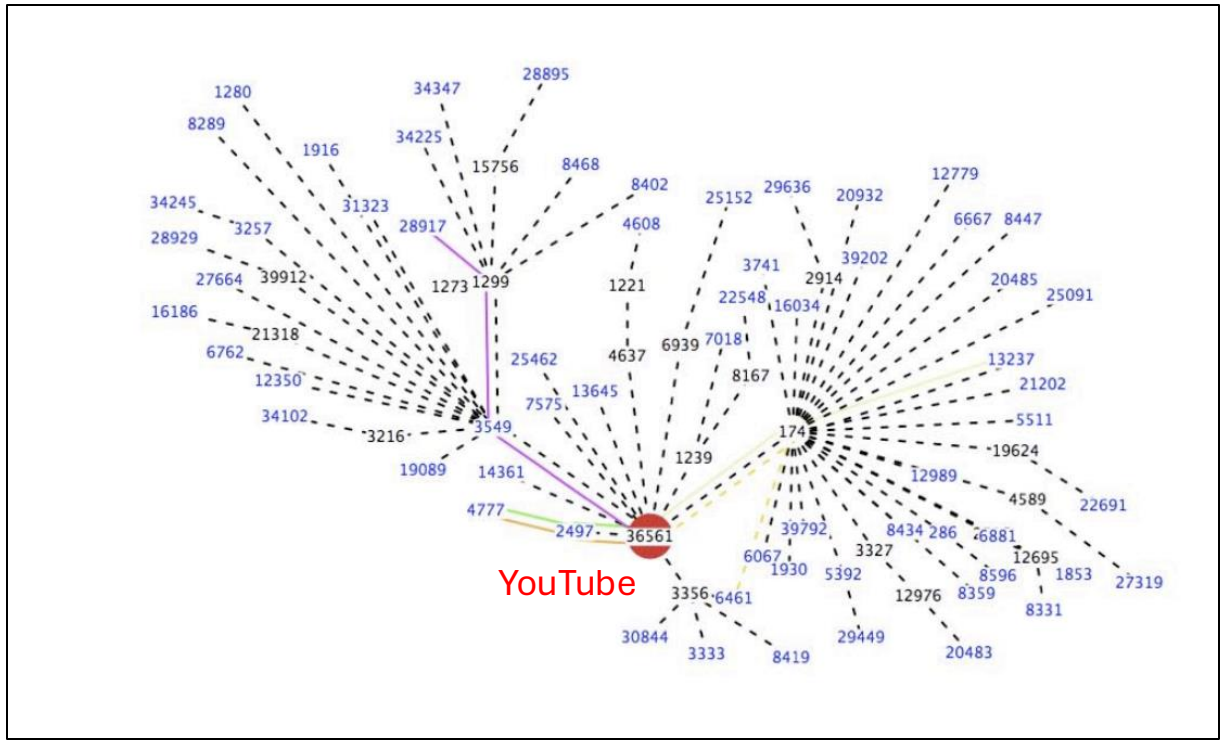


OSPF-Schutzmassnahmen

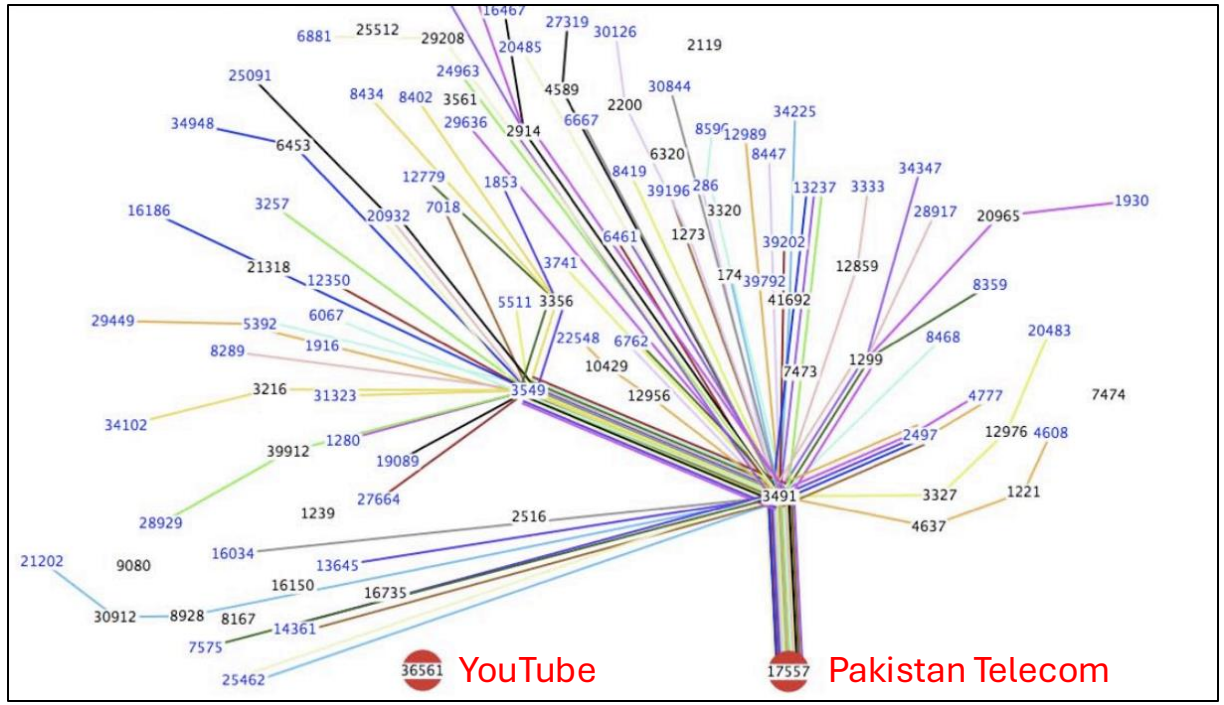
- Validierung der Sequenznummer in einer LSA und des Alters einer LSA:
  - Als Teil der OSPF-LSA-Validierung hat jedes LSA eine Sequenznummer und ein Alter.
  - Ein Rogue-Router kann ein LSA mit einer höheren Sequenznummer ankündigen, um es gültig erscheinen zu lassen, aber Router akzeptieren es nur, wenn die Sequenznummer korrekt und nicht veraltet ist.
  - Wenn das Rogue-LSA eine ungültige Sequenznummer hat (z. B. eine Nummer, die nicht in der richtigen Reihenfolge ist), wird der empfangende Router sie verwerfen.
- Rogue-LSA-Nachrichten
  - Empfängt ein Router mehrfach LSA-Information von einem Rogue-Router die falsch ist, kann der Router die OSPF-Nachbarschaftsbeziehung mit dem Rogue-Router beenden.

BGP-Hijacking

- YouTube besitzt ASN=36561 und besitzt den IP-Subnetzbereich 208.65.153.0/24.
- Subnetzbereich wird via BGP Advertisement vom YouTube Border Gate Router an alle ISPs verteilt:
  (208.65.153.0/24, 36561)



- Im Jahr 2008 hat die Pakistan Telecom ASN=17557 für ca. 2min den YouTube Subnetzbereich 208.65.153.0/24 als seinen eigenen IP-Adressbereich publiziert:
  (208.65.153.0/24, 17557)
- Ergebnis: Viele ISPs haben den weltweiten YouTube-Netzwerkverkehr an die Pakistan Telekom geschickt.

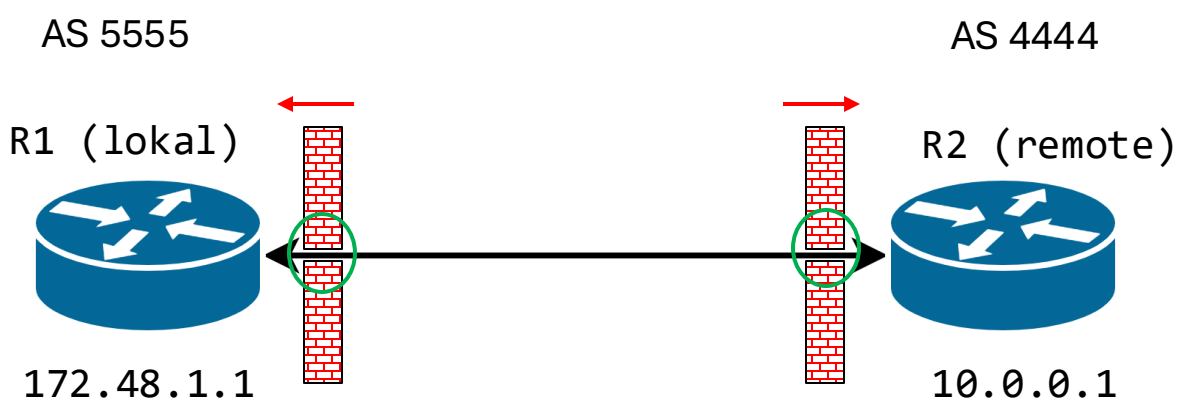


BGP: ACL-Listen

- Der (BGP-)Routing-Verkehr kann mittels ACLs kontrolliert werden.
- Soll ein lokales Router-Interface (172.48.1.1) nur BGP-Nachrichten (tcp/179) von einem bestimmten Remote BGP-Router (10.0.0.1) empfangen und umgekehrt, können Sie die folgende ACL definieren:

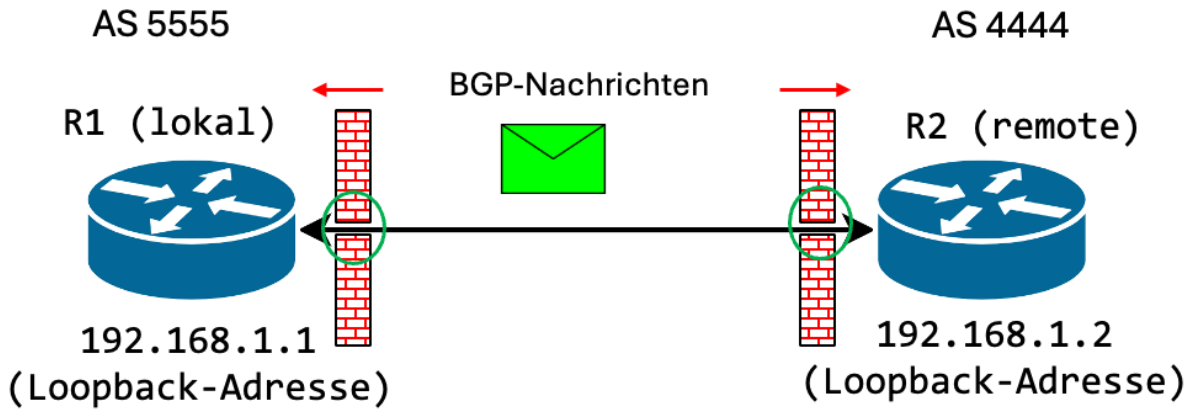
```
!BGP-Paket von 10.0.0.1 (BGP-Client) zu
! 172.148.1.1 (BGP-Server) erlaubt
R1(config)# access-list extended BGP_ACL
    permit tcp host 10.0.0.1 host 172.48.1.1 eq 179
!BGP-Paket von 172.48.1.1 (BGP-Client) zu
!10.0.0.1 (BGP-Server) erlaubt
R2(config)# access-list extended BGP_ACL
    permit tcp host 172.48.1.1 host 10.0.0.1 eq 179
```

```
!Configure BGP for Router R1 with AS5555
R1#router bgp 5555
!Define Router R2 as neighbor
R1#neighbor 10.0.0.1 remote-as 4444
!Apply ACL for incoming BGP messages
R1#neighbor 172.48.1.1 filter-list BGP_ACL in
```



BGP - Authentifizierung

- Der BGP-Nachrichtenverkehr zwischen 2 BGP-Peers kann ebenfalls mittels MD5 authentifiziert und per TTL-Security zusätzlich abgesichert werden.
- Analog zu OSPF kann auch IPsec zur Absicherung der Routing-Nachrichten zum Einsatz kommen.




```
R1# router bgp 5555
R1# bgp router-id 192.168.1.1
R1# neighbor 192.168.1.2 remote-as 4444
R1# neighbor 192.168.1.2 ttl-security hops 254
R1# neighbor 192.168.1.2 password <mysecretpasswd>
```

```
R2# router bgp 4444
R2# bgp router-id 192.168.1.2
R2# neighbor 192.168.1.1 remote-as 5555
R2# neighbor 192.168.1.1 ttl-security hops 254
R2# neighbor 192.168.1.1 password <mysecretpasswd>
```