

# Lernunterlagen Cloud Engineering

## Geschichte des Computers

- Netzwerk: Zusammenschluss von mehreren Computern, die Daten austauschen und zusammenarbeiten
  - difference engine
  - analytical engine (punch cards) -> very advanced calculated
  - Algorithm: A series of steps that solve specific problems
  - Cryptography: The art of writing and solving codes
  - bis 1950s - punch cards
  - -> magnetic tape -> magnetizing data onto a tape
  - ENIAC - erster riesen Computer
  - Compilers: Möglichkeit, menschliche Sprache mithilfe einer Programmiersprache in Computercode zu übersetzen
  - zuerst in Militär und Unis
  - 1970s erster apple computer (für zuhause) -> Apple II huge success
  - 1980s IBM führte einen PC ein -> Microsoft Disk Operating System
  - später: Microsoft Windows, bevorzugtes Betriebssystem in Unternehmen, weil es auf jeder kompatiblen Hardware läuft
  - arcades in 70er und 80er beliebter -> Video-Games
  - Atari Video Computer System
  - Stallman -> Entwicklung eines kostenlosen, Unix-ähnlichen Betriebssystems -> GNU
  - GNU = Open-Source (Code = quelloffen), sodass ihn alle ändern und weitergeben konnten
  - GNU war kein vollständiges Betriebssystem, aber Grundlage für Linux = größtes Open-Source-Betriebssystem
  - mozilla firefox = open source browser
  - Anfang 90er: PDAs -> Personal Digital Assistants -> Vorläufer von Handys
- 
- Computer: Gerät, das Berechnungen durchführt, um Daten zu verarbeiten und zu speichern
  - je höher die Rechenleistung, desto größer die Möglichkeiten
  - 0en und 1en berechnen.  $0+1$  oder  $1+1$  ist einfach, aber was, wenn es milliarden Rechnungen davon sind
  - -> Binary system: The communication that a computer uses, also known as a base-2 numeral system
  - funktioniert wie Buchstaben: unterschiedliche Anordnungen = unterschiedliche Bedeutung
  - computing: we group binary into 8 numbers/bits
  - bit = binary digit (also 0 oder 1)
  - $2^8$  Zahlen waren ausreichend viele Werte für die benötigten Berechnungen
  - 8-Bit-Gruppierung wurde Branchenstandart
  - Byte: Gruppe aus 8 Bits
  - each byte can store one character, and we can have 256 possible values thanks to the base-2 system
  - ein byte kann zb ein buchstabe sein

## Digitale Logik

- character encoding: Assigns our binary values to characters, so that we as humans can read them -> wie ein Wörterbuch, welches Zeichen gehört zu welchem binären Code
- ASCII = ältester Standard für die Zeichencodierung
- war irgendwann nicht genug, da mehr Zeichen nötig als 256
- UTF-8 -> der heute gängigste Zeichencodierungsstandard
- z.B. Emojis, die nicht mit einem Byte möglich sind (da nur ein Zeichen in einem Byte gespeichert werden kann)
- mit UTF-8 kann ein Zeichen in mehr als einem Byte gespeichert werden
- basiert auf einem Unicode-Standard -> hilft, Zeichencodierung einheitlich darzustellen
- wie werden Farben dargestellt? -> RGB (red green blue)
- RGB-Modell verwendet 3 Zeichen -> jedes Zeichen steht für ein Farbton, der die Farbe des Pixels auf dem Bildschirm verändert
- mit Nullen und Einsen in nur acht Kombinationen wird alles dargestellt, was wir am Computer sehen, vom einfachen Buchstaben bis zu Videos

### Binärsystem

- vorstellbar wie Lichter -> 0 = aus, 1 = an (punch cards)
- Elektrizität über Transistoren -> elektrische Spannung = 1, keine Spannung = 0
- Transistoren reichen nicht aus (Beispiel Raum mit 2 Lichtschaltern, es muss möglich sein, das Licht mit beiden Schaltern ein und aus zu schalten, je nach Zustand des Lichtes)
- -> Logic Gates (Logikgatter): Allow our transistors to do more complex tasks, like decide where to send electrical signals depending on logical conditions
- Schaltkreise

### Im Binärsystem zählen

- mit Dezimalsystem können wir ermitteln, welche Bits unser Computer verwenden kann
- jede existierende Zahl kann mit Bits dargestellt werden
- Dezimalsystem -> 0-9
- Binärsystem -> 0 und 1
- die größtmögliche Dezimalzahl eines Bits ist 255 (da die 0 mitzählt)

## Computerschichtenarchitektur

### Abstraktion

- > we take a relatively complex system and simplify it for our use
- bsp: bei einem Auto verwenden wir Lenkrad und Pedale zur Steuerung, ohne zu wissen, wie das Innere funktioniert
- wir benutzen Maus, Tastatur, Touchscreen für Computer
- error-meldung ist auch schon eine Abstraktion

### Computerarchitektur

- 4 main layers (als IT Support muss man wissen, wie die layers miteinander interagieren)
  - Hardware

- Betriebssystem
  - Software
  - User
- 
- Hardware = physisch
  - Betriebssystem = wie kommuniziert Hardware mit dem System
  - Software = wie interagieren wir Menschen mit unserem Computer
  - User = Mensch, der mit Computer kommuniziert

## **Zusammenfassung:**

**Abstraktion:** Die Vereinfachung eines relativ komplexen Systems für unsere Nutzung

**Algorithmus:** Eine Reihe von Schritten zur Lösung bestimmter Probleme

**ASCII:** Der älteste verwendete Zeichencodierungsstandard. Er repräsentiert das englische Alphabet, Ziffern und Satzzeichen.

**Binärsystem:** Die von einem Computer verwendete Kommunikation wird als Binärsystem bezeichnet, auch als „Base 2-Zahlensystem“ bekannt

**Byte:** Eine Folge aus 8 Bit

**Zeichencodierung:** Wird verwendet, um Zeichen Binärwerte zuzuweisen, damit sie visuell lesbar sind

**Computer:** Ein Gerät, das Berechnungen durchführt, um Daten zu speichern und zu verarbeiten

**Kryptografie:** Die übergeordnete Disziplin, die das Codieren und Verbergen von Nachrichten vor Dritten umfasst

**Base 10-System in Dezimalform:** Im Dezimalsystem gibt es zehn mögliche Zahlen, die Sie verwenden können – von null bis neun

**Digitale Spaltung:** Die wachsende Kompetenzlücke zwischen Menschen mit und ohne digitale Kompetenzen

**Informationstechnik:** Der Einsatz von digitaler Technologie wie Computern und dem Internet zum Speichern und Verarbeiten von Daten in nützliche Informationen

**Linux-Betriebssystem:** Linux ist eines der größten Open-Source-Betriebssysteme, das in der Unternehmensinfrastruktur und im Verbraucherbereich häufig verwendet wird

**Logikgatter:** Ermöglicht Transistoren die Ausführung komplexer Aufgaben wie etwa festlegen, wohin elektrische Signale je nach logischen Bedingungen gesendet werden sollen

**Open Source:** Software, bei der Entwickler anderen Entwicklern das Recht einräumen, ihre Software kostenlos freizugeben, zu ändern und zu verteilen

**PDA (Personal Digital Assistant):** Ein tragbarer kompakter Computer

**Lochkarten:** Sequenz aus Karten mit Löchern, die automatisch Berechnungen vornehmen, statt diese manuell einzugeben

**RGB-Modell:** Das RGB-Modell (Rot Grün Blau) ist das Basismodell für die Darstellung von Farben

**UTF-8:** Der heute am häufigsten verwendete Codierungsstandard

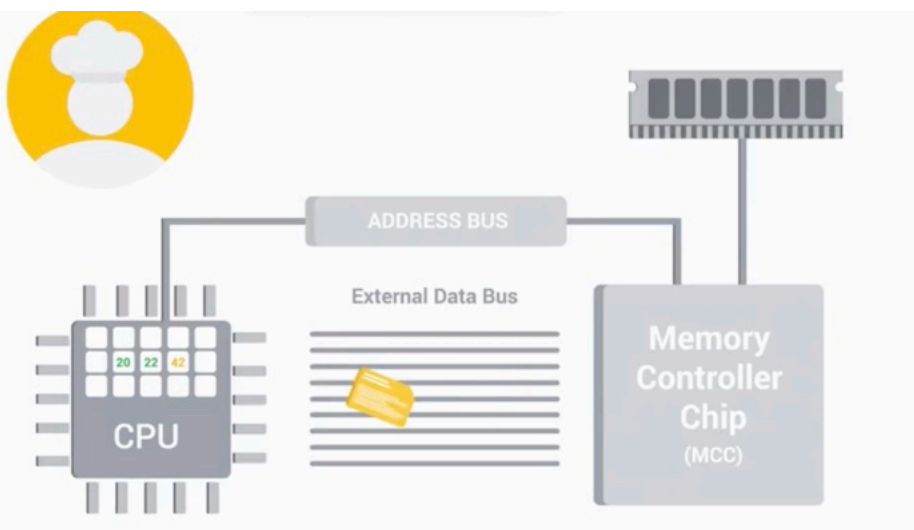
## Computerhardware

- Ports: Anschlüsse, um die Funktionalität des Computers zu erweitern
- innen:
- CPU oder zentrale Verarbeitungseinheit (durch Kühlkörper abgedeckt)
- -> Gehirn eines Computers, führt alle Berechnungen und Datenverarbeitung aus
- kommuniziert sehr viel mit RAM (Random Access Memory) -> short term memory -> wenn man zb Text in einen Chat eingibt wird es vorübergehend im RAM gespeichert
- hard drive: Langzeitspeicherung -> hold all of our data, which includes all of our music, pictures, applications
- Motherboard (größter Teil): body or circulatory system of the computer that connects all the pieces together
- power control (wandelt strom in energie für computer um)

## Programme, CPU und Speicherplatz

- Programs: instructions that tell the computer what to do (bsp. wie Rezepte)
- CPU ist wie der Koch, der die von uns gesendeten Rezepte zu Mahlzeiten verarbeitet
- die CPU kann schneller Kochen, als sie lesen kann -> Rezepte werden ins RAM zwischengespeichert (short term)

- auf das RAM kann die CPU schneller zugreifen, als auf die Festplatte
- wir können der CPU einzelne Rezepte geben, statt das ganze Kochbuch vorzulesen
- man gibt der CPU nicht direkt das komplette Rezept, sondern Schritt für Schritt über den RAM
- die Rezepte können nur im binären System übermittelt werden
- External data bus (EDB) / externer Datenbus: mehrere Leitungen, die Bestandteile des Computers verbinden, etwa wie die Adern in unserem Körper
- EDB Größen: 8 Bit, 16 Bit, 32 Bit oder 64 Bit
- je mehr Leitungen, desto mehr Daten können gesendet werden
- CPU hat Register
- Register dienen zum Speichern von Informationen, z.B. Zahl 1 in Register A, zu der Zahl 2 in Register B addiert wird -> Ergebnis wird in Register C gespeichert
- Register = Arbeitsfläche des Kochs
- dort übersetzt der Koch (CPU) sein Binärformat in Aufgaben (z.B. 10010011 = Salz hinzugeben)
- **Programme werden zum Lesen von der CPU in den RAM kopiert und kann dort in jedem Bereich gleich schnell abgerufen werden**
- Daten aus RAM werden nicht über EDB gesendet, dazu sind die Datenmengen zu groß
- -> deshalb gibt es den **MCC** -> Speicher Controller
- **MCC = Brücke zw. RAM & CPU**
- **RAM hat unzählige Informationen in random Anordnung, wenn CPU also z.B. Schritt 3 vom Rezept will, sucht der MCC diesen Schritt heraus und sendet ihn über den EDB an den CPU**



- der MCC ist über den address bus mit dem CPU verbunden -> der address bus sendet die Location der gesuchten Datei, sendet diese aber nicht. Der EDB sendet die Datei dann an den CPU

- **Cache** = noch schnellerer Weg als RAM, um CPU Daten zuzuführen
- Daten, die wir oft benutzen werden in Caches gespeichert
- Verbirdlichung: RAM ist wie ein Kühlschrank, den man erst öffnen muss. Cache ist wie unsere Hosentasche
- -> kürzlich oder häufig abgerufene Daten im Cache
- Cache-Stufen im CPU: L1, L2, L3
- Der L1-Cache ist die schnellste und kleinste der drei CPU-Cache-Ebenen. L1 enthält die derzeit von der CPU verwendeten Daten
- CPU weiss durch Taktgeber, wann Rechenzyklen beginnen und enden, also: wann beginnt ein neuer Rechenauftrag und wann endet er
- **Taktgeber** sind wie das Ticken einer Uhr -> mit jedem Tick führt die CPU einen Betriebszyklus durch
- das Senden einer Spannung an den Taktgeber wird als **Taktzyklus** bezeichnet -> wenn für einen Befehl viele Daten verarbeitet werden müssen, müssen viele Taktzyklen ausgeführt werden
- Computer mit 3,4 GHz -> Höchstanzahl an Taktzyklen, die in einem bestimmten Zeitraum verarbeitet werden kann
- wird dieser Wert überschritten -> übertakten (over clocking)
- Wenn Sie gerne Spiele spielen und sich bessere Grafik und weniger Latenz wünschen, können Sie Ihre CPU übertakten, wenn Sie ein Spiel spielen. Es gibt jedoch auch Nachteile, beispielsweise kann die CPU überhitzen.

## CPU

- Funktionen wie Addieren, Subtrahieren und Kopieren von Daten sind alles Befehle, die die CPU ausführen kann
- Jedes Programm auf dem Computer ist zwar hochkomplex, kann jedoch in sehr kleine und einfache Befehle aufgeteilt werden, die im Befehlssatz stehen
- Befehlssätze sind in die CPU hartcodiert
- Verschiedene CPU-Hersteller können verschiedene Befehlssätze verwenden
- -> ähnlich wie bei Autos und Motoren: unterschiedliche Hersteller = unterschiedliche Motoren, aber gleiche Funktion
- gängige Hersteller: wie **Intel, AMD, Qualcomm**
- CPU-Hersteller verwenden unterschiedliche Produktnamen, um ihre Prozesse zu differenzieren: Intel Core i7, AMD Athlon, Snapdragon 810, Apple A8 ect.
- Auswahl CPU: muss mit Motherboard kompatibel sein -> richtige Sockel und Kontaktpunkte

- zwei Arten von CPU-Sockeln: Land Grid Array, auch LGA, und Pin Grid Array, auch PGA
- CPU überhitzt schnell, deshalb benötigt sie einen Kühler, der die Wärme von der CPU aufnimmt und über einen Lüfter oder ein anderes Medium ableitet

## RAM

- beim Ausschalten des Computers werden alle Daten aus dem RAM gelöscht
- Computer bestehen aus Programmen
- Um ein Programm auszuführen, müssen wir eine Kopie im RAM erstellen, damit es die CPU verarbeiten kann (Programm zuvor auf Massenspeicher, also Festplatte ect)
- z.B. 16 GB RAM = 16GB Programme, die gleichzeitig ausgeführt werden können
- Texteingabe z.B. in RAM gespeichert (bei Stromausfall ist es dann weg)
- es gibt unterschiedliche RAM Arten, in Computern meist DRAM (Dynamic Random Access Memory)
- Wenn eine Eins oder Null an den DRAM gesendet wird, wird jedes Bit in einem Mikrocondensator gespeichert
- Diese Halbleiter werden in Chips auf dem RAM eingesetzt, die unsere Daten speichern
- Es gibt verschiedene Speichermodule, auf die die DRAM-Chips gesetzt werden können
- Die moderneren DIMM-Module – DIMM steht für Dual Inline Memory Module – haben Kontakte verschiedener Größen
- Ein RAM wird für gewöhnlich nicht aufgrund der Anzahl vorhandener DRAM-Chips gekauft, sondern aufgrund der Kapazität, zum Beispiel ein RAM-Modul mit acht GB
- Nach dem DRAM bauten RAM-Hersteller den SDRAM, das steht für „synchrones DRAM“ -> Der SDRAM ist mit der Taktgeschwindigkeit des Systems synchronisiert, was eine schnellere Verarbeitung ermöglicht
- In heutigen Systemen wird eine andere Art RAM verwendet: Double Data Rate SDRAM oder DDR-SDRAM
- Die aktuellste Version DDR4 ist der schnellste Kurzzeitspeicher, den es momentan für Computer gibt
- **Ein schnellerer RAM bedeutet schnellere Programme und mehr Programme gleichzeitig**

## Motherboards

- Grundeigenschaften: Chipsatz -> 2 Chips ->
- Northbridge (verbindet zb RAM oder Grafikkarten)
- Southbridge (für Input-Output-Controller zuständig -> Festplatte, USB ect.)
- **Der Chipsatz ist eine wichtige Komponente unserer Hauptplatine -> dadurch wird der Datenfluss zwischen unserer CPU, dem RAM und Peripheriegeräten (externe Geräte wie Bildschirm ect.) gesteuert**
- neben dem Chipsatz: Erweiterungssteckplätze (expansion slots)
- Über Erweiterungssteckplätze können wir die Funktionalität eines Computers erweitern
- Um die Grafikkarte aufzuwerten, können wir einfach eine neue kaufen und diese über einen Erweiterungssteckplatz auf der Hauptplatine installieren
- es gibt unterschiedliche Formfaktoren: z.B. ATX (groß), ITX (kleiner) + Unterformen von den beiden

## physischer Speicher: Festplatten

- Die kleinste Einheit eines Datenspeichers ist ein Bit. Ein Bit kann eine Binärzahl speichern. Also eine Eins oder eine Null. Die nächstgrößere Einheit ist das Byte. Es besteht aus 8 Bit. Ein Byte kann für einen Buchstaben, eine Zahl oder ein Symbol stehen
- zwei grundlegende Festplattentypen genutzt: Hard Disc Drives (HDD) und Solid State Drives (SSD)
- Bei HDDs kommt es häufiger zu Beschädigungen, da sie viele bewegliche Teile nutzen
- Es gibt sogar hybride SSD/HDD-Festplatten (mit Vorteilen von beiden)
- Schnittstellen: SATA-Kabel für HDD, NVMe Express für SSD (wegen Übertragungsgeschwindigkeit)

## Netzteile

- Es gibt zwei Arten von Strom: **Gleichstrom**, der in eine Richtung fließt, und **Wechselstrom**, der ständig seine Richtung ändert
- Unsere Computer nutzen Gleichstrom -> wir müssen irgendwie den Wechselstrom unseres Energieversorgers in etwas Verwertbares umwandeln -> Hier kommt unser Netzteil ins Spiel.
- Watt ist die Menge an Volt und Ampere, die das Gerät benötigt
- Netzteil mit zu niedriger Wattzahl kann Computer nicht ausreichend versorgen
- zu großes Netzteil ist nicht schlimm, da sie nur so viel Strom zieht, wie benötigt
- üblich: 500W Netzteil für Computer (bei viel Rendering ect. größeres Netzteil)
- Die Größe des Formfaktors und die in die Motherboards integrierten Komponenten sind der Ausgangspunkt für die erforderlichen Mindestwattleistungen der Netzteile
- Die internen Hardwarekomponenten eines Computers benötigen zum Betrieb unterschiedliche Eingangsspannungen
- Spannungsregler im Motherboard des Computers steuern, wie viel Strom an die verschiedenen internen Komponenten des Computers geliefert wird
- Bei der Auswahl eines Netzteils für Ihren Computer sollten Sie Folgendes beachten:
  - Die für das Land, in dem der Computer verwendet wird, übliche Eingangsspannung von Steckdosen
  - Die Anzahl und den Stromverbrauch der internen Komponenten des Computers
  - Die technischen Spezifikationen und Anforderungen für das Motherboard-Modell und den Formfaktor

## Mobilgeräte

- Mobilgeräte sind auch Computer: Sie haben CPUs, RAM, Speicher, Stromsysteme und Peripherie
- Die Teile von Mobilgeräten sind normalerweise fest verbaut
- Ein System auf einem Chip packt die CPU, den RAM und manchmal sogar den Speicher auf einen einzigen Chip. Das SOC ist nicht nur klein, es hat auch einen geringeren Akkuverbrauch als separate Komponenten



# Peripheriegeräte

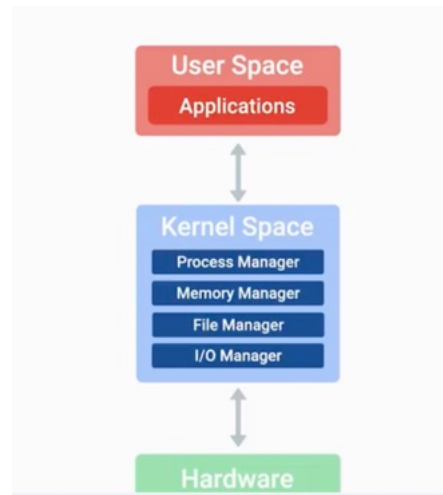
- **MB steht für Megabyte und ist eine Einheit für Datenspeicher - Mbit/s steht für Megabit pro Sekunde und gibt die Geschwindigkeit der Datenübertragung an**
- Wenn Sie ein USB 2.0-Gerät an einen USB 3.0-Port anschließen, erhalten Sie keine 3.0-Geschwindigkeit, aber Sie können den Port verwenden -> abwärtskompatibel
- USB 2.0-Ports: schwarz, USB 3.0-Ports: blau, USB 3.1-Ports: blaugrün

## BIOS

- Wenn man eine Taste auf der Tastatur drückt, dann wird nur ein Byte an die CPU gesendet
- die CPU hat keine Ahnung, was das ist, ihr fehlen Anweisungen dazu, wie sie damit umgehen soll
- Auch diese Geräte verwenden Programme, um der CPU zu sagen, was sie tun soll -> „Dienstprogramme“ oder „Treiber“
- Treiber enthalten die Anweisungen, die unsere CPU benötigt, um externe Geräte wie Tastaturen, Webcams oder Drucker zu verstehen
- Die CPU weiß nicht: Da ist ein Gerät, mit dem ich sprechen kann
- sie muss eine Verbindung zum sogenannten BIOS (Basic Input Output Services) aufbauen
- Die BIOS-Software ist dafür zuständig, die Rechner-Hardware zu initialisieren -> Sie bringt unser Betriebssystem zum Laufen
- BIOS wird nicht auf Laufwerk gespeichert, sondern das Motherboard hat einen extra Nur-Lese-Speicher, auch **ROM-Chip** genannt
- Anders als RAM ist ROM nichtflüchtig -> Daten werden beim Ausschalten des Rechners nicht gelöscht
- UEFI - Das Unified Extensible Firmware Interface startet Computer, ebenso wie das traditionelle BIOS, ist aber moderner und bietet eine bessere Kompatibilität
- Weiter unterstützt es neuere Hardware
- Die meiste aktuelle Hardware kommt mit eingebautem UEFI
- Irgendwann wird UEFI das verbreitetere BIOS werden
- BIOS und UEFI kurz gesagt: Starthelfer der Computers (überprüft alles, lädt Treiber ect. -> POST, der Power-On Self-Test)
- Kommt es zu diesem Zeitpunkt zu einem Problem, so kann das nicht auf dem Bildschirm angezeigt werden, da Elemente wie der Grafiktreiber noch nicht geladen wurden
- Aber Rechner können meist schon Signaltöne ausgeben
- Das ist fast sowas wie ein Morsecode zur Identifizierung des Problems
- Die Hersteller nutzen unterschiedliche Pieptöne
- Startet der Computer erfolgreich, hört man oft nur einen Piep
- Hört man zwei Pieptöne, liegt eventuell ein POST-Fehler vor
- CMOS-Chip: speichert Grundlagendaten zum Hochfahren des Computers (Datum, Uhrzeit und wie er starten soll)
- für Änderungen muss man in die BIOS-Einstellungen (meist ein Tastenbefehl beim Booten)
- typische IT-Aufgabe: Re-Imaging
- Der Ausdruck bezieht sich auf ein Disk Image -> Kopie des Betriebssystems
- Der Prozess des Re-Imaging beinhaltet das Löschen und die erneute Installation eines Betriebssystems -> über USB-Stick, CD-ROM, oder via Netzwerk zugänglichen Server

# Betriebssystem (operating System)

- Ein Betriebssystem ist das Gesamtpaket zur Verwaltung der Ressourcen der Computer und lässt uns damit interagieren
- Ein Betriebssystem hat 2 Hauptbestandteile: den Kernel und den Benutzerbereich
- Der Kernel ist das Kernstück eines Betriebssystems -> kommuniziert direkt mit unserer Hardware und verwaltet die Ressourcen des Systems
- Als Benutzer interagieren wir nicht direkt mit dem Kernel -> Wir interagieren dafür mit dem zweiten Teil des Betriebssystems, dem Benutzerbereich

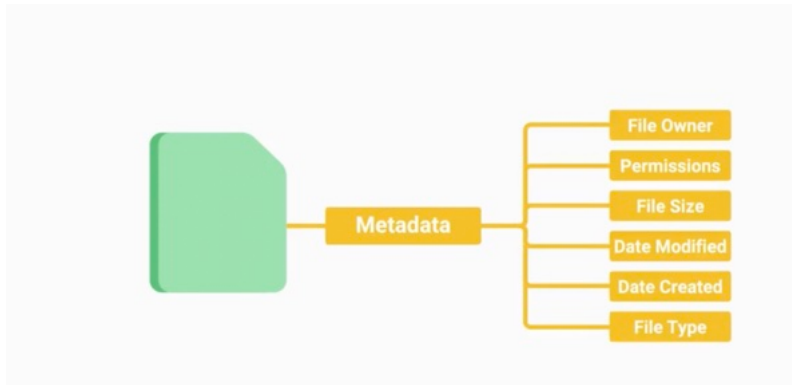


- Windows, Mac & Linux
- Einige gängige Linux-Distributionen sind Ubuntu, Debian und Red Hat
- Mobiltelefone -> Chrome OS & Android OS haben Linux-Kernel unter der Haube
- Der Prozess-Scheduler ist der Teil des Kernels, der dieses Multitasking möglich macht
- I/O-Verwaltung ist alles, wodurch wir Daten eingeben oder Daten ausgeben können

## Dateien und Dateisysteme

- 3 Hauptkomponenten zur Verwaltung von Dateien: die Dateidaten, die Metadaten und das Dateisystem
- Dateisystem: unterschiedliche, welche die große Dateimengen unterstützen oder kleinere, unterschiedlich schnell und sicher
- Für Windows wird hauptsächlich das Dateisystem **NTFS** genutzt
- Funktionen: Verschlüsselung, schnellere Zugriffsgeschwindigkeit, Sicherheit & mehr
- Unter Linux nutzen verschiedene Distributionen unterschiedliche Arten von Dateisystemen
- Standard für Dateisysteme unter Linux: **EXT4**
- Je nach Art des Dateisystems können Dateien nicht problemlos zwischen verschiedenen Dateisystemen verschoben werden
- Auf unsere Festplatte schreiben wir Daten in Form von Datenblöcken
- Wenn wir etwas auf die Festplatte schreiben, befindet sich dies nicht immer in einem Teil -> es kann in viele Teile zerlegt und auf verschiedene Teile der Festplatte geschrieben werden

- **Blockspeicherung** ermöglicht den **schnelleren Umgang** mit Daten, da Daten nicht in einem langen Stück gespeichert werden und der Zugriff darauf schneller ist. Dies dient ebenso der besseren Nutzung des Speicherplatzes



- Eine Dateierweiterung (file extension) ist das Anhängsel am Dateinamen, das uns sagt, um welchen Dateityp es sich in bestimmten Betriebssystemen handelt

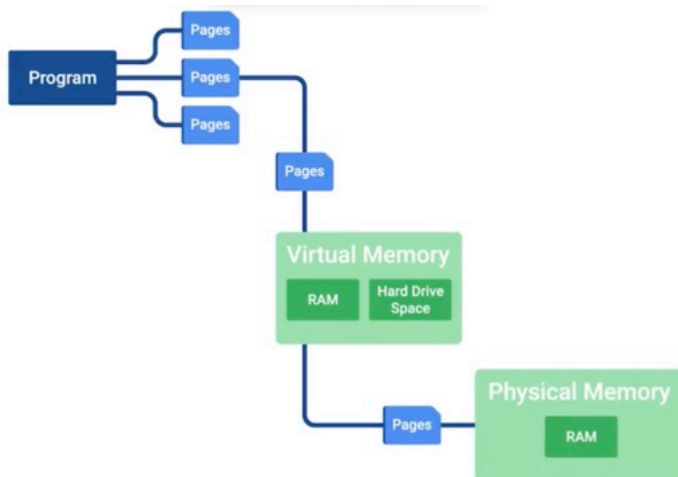
## Prozessverwaltung

- Ein Prozess ist ein Programm, das ausgeführt wird (z.B. Internet-Browser oder Texteditor)
- Ein Programm ist eine Anwendung, die wir ausführen können, wie Chrome
- Programm z.B.: Browser & die vielen Tabs im Browser = Prozesse
- Um Programme auszuführen, müssen wir ihnen Computerressourcen zuweisen, wie RAM und CPU
- endliche Menge an Ressourcen -> Der Kernel muss Ressourcen effizient verwalten, damit alle Programme, die wir nutzen möchten, ausgeführt werden
- CPU führt Prozesse nacheinander durch einen sogenannten Zeitschlitz aus -> ein sehr kurzes Zeitintervall, das einem Prozess zur Ausführung durch die CPU zugewiesen wird
- es wirkt also, als würde der Computer Prozesse gleichzeitig ausführen, tut dies aber eigentlich nacheinander unglaublich schnell
- Der Kernel legt Prozesse an, plant sie effizient zeitlich ein und bestimmt, wie Prozesse beendet werden
- Dies ist wichtig, da wir eine Möglichkeit benötigen, alle zuvor genutzten Ressourcen einzusammeln, die aktive Prozesse beansprucht hatten, und diese einem anderen Prozess zuzuweisen

## Speichermanagement und virtueller Speicher

- Wenn Prozesse laufen, benötigen sie Speicherplatz, damit der Computer sie schnell lesen und laden kann
- Im Vergleich zu Festplattenlaufwerken sind nur kleine Mengen Arbeitsspeicher vorhanden
- Um mehr Speicher zu bieten, als physisch vorhanden ist, nutzen wir sogenannten virtuellen Speicher

- Virtueller Speicher ist eine Kombination aus Festplattenspeicher und RAM, die wie Speicher agiert und von unseren Prozessen genutzt werden kann
- Wir nutzen nicht alle Funktionen unserer Anwendung auf einmal -> warum also alle auf einmal laden?
- Es ähnelt dem Nachkochen eines Rezepts aus einem Kochbuch: man muss nicht das ganze Buch lesen, nur um ein Rezept nachzukochen
- Sie brauchen nur die Seiten des Rezepts zu lesen, das Sie gerade nutzen
- Wenn wir unseren virtuellen Speicher auf unserer Festplatte speichern, nennen wir den zugewiesenen Speicherplatz **Swap-Speicher**



## I/O-Management

- I/O bedeutet nicht nur Übertragung von Daten zwischen uns und unseren Geräten, die Geräte müssen auch in der Lage sein, untereinander zu kommunizieren
- Kernel übernimmt die gesamte Kommunikation zwischen den Geräten
- Er findet ebenso die effizienteste Übertragungsmethode und versucht sein Bestes, dafür Sorge zu tragen, dass die Daten keine Fehler aufweisen
- Bei der Fehlersuche oder der Lösung eines Problems mit einem langsamen Rechner liegt meist ein Mangel an Hardware-Ressourcen vor
  - Wenn der RAM nicht ausreicht, können Sie nicht so viele Prozesse hochladen
  - Wenn Ihre CPU nicht ausreicht, können Sie Programme nicht schnell genug ausführen
  - Wenn zu viele Eingaben in das Gerät eingehen oder irgendwo zu viele Ausgaben erfolgen, werden auch andere Daten am Senden oder Empfangen gehindert

## Userspace (Benutzerbereich)

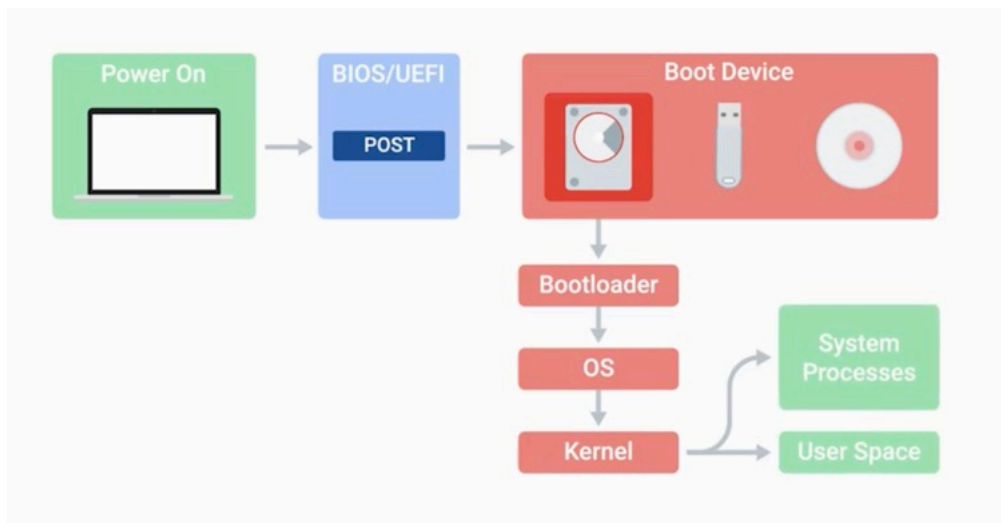
- Es gibt zwei Möglichkeiten, mit dem Betriebssystem zu interagieren: über eine **Shell** (Texteingabe) oder eine **grafische Benutzeroberfläche (GUI)**
- es gibt unterschiedliche Shells

- gebräuchlichste Shell: Bash oder Bourne-again shell in Linux
- Einige Tests können nur über Befehle durchgeführt werden

## Protokolle (Logs)

- Protokolle (Logs) sind Dateien, die Systemereignisse auf dem Computer erfassen, wie ein Tagebuch
- In allen Betriebssystemen werden Protokolle geführt

## Boot-Vorgang



## Virtual Machines

- Kopie einer realen Maschine
- -> Ich möchte keinen neuen Computer kaufen oder zwei separate Betriebssysteme auf der Festplatte haben -> Ich kann stattdessen eine Anwendung wie Virtual Box nutzen, um Linux zu installieren, und es ist vollständig von meiner Maschine isoliert
- Virtuelle Maschinen nutzen physische Ressourcen wie Datenspeicher, CPU und Speicherplatz, bieten aber zusätzlichen Nutzen, da gleichzeitig mehrere Betriebssysteme laufen
- einfacher zu warten und bereitzustellen
- Sie können zudem Ressourcen freigeben, die nicht mehr genutzt werden
- Wenn Sie Software nutzen möchten, die nur für ein bestimmtes Betriebssystem zur Verfügung steht, ist es leichter, eine neue virtuelle Maschine anzulegen, die Software zu nutzen und am Ende die virtuelle Maschine zu löschen

## Windows 10 installieren

- Zunächst müssen wir gewährleisten, dass unsere BIOS- oder UEFI-Boot-Reihenfolge auf Booten vom USB-Laufwerk eingestellt ist
- Je nachdem, was der Hersteller Ihres Computers nutzt, müssen Sie entweder „F12“ oder eine andere Taste zum Zugriff auf das BIOS drücken
- Nun werde ich gefragt, welche Art der Installation ich durchführen möchte -> Ich klicke hier einfach auf „Benutzerdefiniert“, da ich nur Windows installieren möchte -> Ich wähle nun das Laufwerk aus, auf dem ich es installieren möchte

## Linux installieren

- unterschiedliche Distributionen
- häufigste: Ubuntu
- Ordner erstellen über eine Shell:
- Terminal öffnen -> man sieht, dass sich der Computer gerade im Desktop befindet
- „echo \$SHELL“ (Bash nutzen)
- „touch my\_super\_cool\_File“
- Ordner erstellen dagegen: mkdir NAME

## Qwiklabs

- Qwiklabs ist eine Online-Lernumgebung, in der wir auf echte Szenarien treffen

## Grenzen des Internets

- Es gibt verschiedene Arten von IP-Adressen: Das aktuelle Protokoll Internet Protocol Version 4, oder IPV4
- Adresse, die aus 32 Bits besteht und in vier Gruppen eingeteilt sind
- Eine IPV4-Adresse sieht ungefähr so aus: 73.55.242.3
- Für eine Internetverbindung braucht ein Gerät eine IP-Adresse, doch es gibt weltweit schon mehr Geräte als IP-Adressen -> IPV6 setzt sich durch mit 128 Bits
- -> IPV6 Adressen gehen nicht so schnell aus
- andere Lösung: **NAT (Network Address Translation)** -> nutzt öffentliche Adresse und richtet viele unterschiedliche Adressen im eigenen Netzwerk ein

## Modul 5

### Software

- Die Hardware ist der physische Gegenstand, den Sie in die Hand nehmen können
- Die Software erteilt die immateriellen Anweisungen, die der Hardware sagen, was sie tun soll
- Coding: translate one language to another
- Scripting: Coding in a scripting language -> Skripts dienen hauptsächlich für die Ausführung einer einzelnen oder begrenzten Aufgabe
- Programmieren ist Codieren in einer Programmiersprache
- Programmiersprachen sind spezielle Sprachen, die Softwareentwickler verwenden, um Anweisungen zu schreiben, die Computer ausführen sollen
- es gibt Application Software (bestimmter Zweck wie Grafiksoftware o.ä.) und System Software (damit das System läuft)
- Firmware ist eine Software, die dauerhaft auf einer Computerkomponente gespeichert ist
- Assembly Language: Sie ermöglichte es, menschenlesbare Anweisungen in Code zu verwandeln, den Computer verstehen konnten -> anstatt Binärcode zu erzeugen, konnten Informatiker mit Computerbefehlen wie diesem programmieren
- doch die Assembly Language war kaum besser als Computercode
- Compiled Programming Language:
  - Es wurde ein Programm benötigt, das auf vielen Arten von CPUs laufen konnte -> der Beginn von kompilierten Programmiersprachen -> Eine kompilierte Programmiersprache verwendet menschenlesbare Anweisungen und schickt sie durch einen Compiler -> Der Compiler nimmt die menschlichen Anweisungen und übersetzt sie in Maschinenbefehle.
- später: Sprache, die interpretiert und nicht kompiliert wurde -> Interpretierte Sprachen werden nicht im Voraus kompiliert
- Eine Datei, deren Code in einer dieser Sprachen geschrieben ist, wird als Skript bezeichnet -> Das Skript wird von einem Interpreter ausgeführt, der den Code genau zur richtigen Zeit in CPU-Anweisungen umwandelt, um sie auszuführen

### Softwaremanagement

- gefährlich ist veraltete Software wegen der Sicherheit
- Software Bug ist ein Softwarefehler, der zu unerwarteten Ergebnissen führt
- -> Software beständig aktualisieren
- Linux: befehl: apt install git (sudo apt install git - wegen permission)
- dpkg bei linux um programm zu suchen (ob installiert ist) dpkg -s gimp
- sudo apt-get install -f

## Modul 4:

### Netzwerk-Grundlagen

- Das Internet ist die physische Verbindung von Computern und Kabeln rundum die Welt
- Das Web ist die Information, die im Internet ausgetauscht wird
- Die IT-Branche nennt Verwaltung, Installation und Planung von Netzwerken „networking“
- Das Internet besteht aus einem riesigen Netzwerk aus Satelliten, Mobilfunknetzwerken und Kabeln, die alle im Boden vergraben sind
- Wir verbinden uns nicht wirklich direkt mit dem Internet -> Computer, die **Server** genannt werden, verbinden sich direkt mit dem Internet
- auf Servern sind Internetseiten gespeichert, die wir verwenden (Netflix ect.)
- die Websites stellen Informationen bereit
- die Geräte die wir nutzen werden Clients genannt
- die Clients fordern die Inhalte der Websites an
- Clients verbinden sich nicht direkt mit dem Internet, sondern mit einem Netzwerk, das von einem Internetanbieter, **ISP**, verwaltet wird (Telekom, Vodafone, O2, 1&1 ect.)
- Internetanbieter haben bereits aufgebaute Netzwerke und installieren alle echten Kabel, die Millionen von Computern in ein Netzwerk integrieren
- sie verbinden sich auch mit anderen Netzwerken und Internetanbietern
- Diese Netzwerke sind mit den Netzwerken von Google, Reddit, von Universitäten, und im Grunde mit allen anderen Netzwerken der Welt verbunden -> Sie alle spannen ein enormes Computernetzwerk, das wir Internet nennen.
- Die Computer in einem Netzwerk haben einen Identifikator, der **IP-Adresse** heißt (wie straße und hausnummer zb). Eine IP-Adresse besteht aus Zahlen und Ziffern, z. B. 100.1.4.3
- Wenn wir eine Website besuchen wollen, gehen wir eigentlich zu ihrer IP-Adresse
- Geräte, die sich mit dem Internet verbinden können, haben noch einen weiteren Identifikator, der **MAC-Adresse** -> in Gerät eingebaut
- Beispiel: wie beim Versenden eines Briefes: IP-Adresse ist die Adresse des Empfängers und MAC-Adresse der Name des Empfängers
- Daten werden als Pakete durch ein Netzwerk gesendet (Einsen und Nullen)
- egal ob Mails, Bilder, Text ect.
- am Ende wieder zusammengesetzt
- Anfrage auf Google: meine IP Adresse sendet Daten in Paketen, die sich auf die suche nach Google Server machen. Dort angekommen, sieht Google woher die Daten kommen (meine IP-Adresse) und gibt die Information zurück, dass ich etwas auf google suchen kann

### Netzwerkhardware

- Ein Router verbindet viele verschiedene Geräte und hilft dabei, den Netzwerktraffic zu leiten
- Verschicken von Daten in ein anderes Netzwerk: Das Paket wird aus unserem Netzwerk zu dem des Internetanbieters geleitet -> Mithilfe von Netzwerkprotokollen kann es herausfinden, wo der Computer des Empfängers ist
- In diesem Prozess passiert unser Paket viele verschiedene Router, Switches und Hubs



- stellen Sie sich Switches als Poststelle in einem Gebäude vor: Router bringen Briefe zum Gebäude, aber einmal im Gebäude, nutzen wir die Poststelle, um herauszufinden, wo ein Brief hingehen soll
- Hubs verhalten sich wie firmenweite Memos: Weil sie nicht wissen, an wen das Memo gehen soll, schicken sie es an alle

## TCP/IP

- Netzwerkprotokolle = Regelwerke, die die Datenübertragung gestalten
- Sie haben Regeln, die dafür sorgen, dass unsere Pakete:
  - effizient weitergeleitet werden
  - nicht kaputt gehen
  - sicher sind
  - an das richtige Gerät gehen
  - entsprechend benannt sind
- viele unterschiedliche Protokolle, aber die wichtigsten sind Transmission Control Protocol und das Internet Protocol, kurz TCP/IP
- IP: Das Internet Protocol, oder IP, legt fest, wie unsere Pakete zu den richtigen PCs kommen
- -> hilft, Informationen zu leiten
- im TCP, ist festgelegt, wie Informationen zuverlässig von einem Netzwerk zu einem anderen gelangen
- -> TCP spielte eine wichtige Rolle bei der Einführung des Internets

## Das Internet

- Alle Websites können über das Web aufgerufen werden
- Websites sind im Grunde genommen Textdateien, die mit HTML formatiert sind -> Programmiersprache, die von Webbrowsern genutzt wird
- URL steht für „Uniform Resource Locator“ und ist nur eine Adresse im Web, so wie Ihre Adresse zu Hause
- www steht für world wide web, dann kommt der domain-name (jede Domain gibt es nur einmal und ist bei der ICANN eingetragen)
- die Endungen (com, de, org) sind standardisierte Endungen und geben nur einen Hinweis, um was es sich bei der Seite handeln könnte
- Wir sehen, dass die IP-Adresse 172.217.6.46 zur Homepage von Google führt, und dabei das wichtige Netzwerkprotokoll <i>Domain Name System</i>, oder **DNS**, nutzt
- Der Computer weiß nicht, was google.com ist -> Er weiß nur, wie er eine IP-Adresse erreichen kann -> Mit DNS kann er also die IP-Adresse von Google mit Google.com verknüpfen
- Wenn Sie also eine Website über ihre IP-Adresse aufrufen können, aber nicht über ihren Domain-Namen, dann ist die Wahrscheinlichkeit hoch, dass es ein Problem in der DNS-Konfiguration Ihres Netzwerkes gibt

**404 – Nicht gefunden:** Eine Fehlermeldung, die möglicherweise auf Websites angezeigt wird, die verschoben oder gelöscht wurden.

**Fehlermeldung:** Nützliche Hinweise, die Ihnen den Weg weisen können

**Berechtigung verweigert:** Eine Fehlermeldung beim Zugriff auf eine geschützte Datei

**Ursache:** Der Hauptgrund für eine Reihe von Problemen

**Fehlerbehebung:** Die Fähigkeit zur Diagnose und Behebung eines Problems

## **Begriffe und ihre Definitionen aus vorherigen Modulen**

A

**Abstraktion:** Die Vereinfachung eines relativ komplexen Systems für unsere Zwecke

**Adressbus:** Verbindet die CPU mit dem Speichercontroller und sendet den Speicherort der Daten, aber nicht die Daten selbst

**Algorithmus:** Eine Reihe von Schritten zur Lösung bestimmter Probleme

**Android:** Ein mobiles Betriebssystem, das auf Linux basiert

**Anwendung:** Ein Computerprogramm, das auf eine bestimmte Verwendung ausgelegt ist

**Anwendungssoftware:** Software, die für bestimmte Anforderungen entwickelt wurde, z. B. Text-, Browser- oder Grafiksoftware

**ARPANET:** Die erste Version des heutigen Internets wurde in den 1960er-Jahren durch das US-Regierungsprojekt DARPA geschaffen

**ASCII:** Der älteste verwendete Zeichencodierungsstandard. Er repräsentiert das englische Alphabet, Ziffern und Satzzeichen.

**Assemblersprache:** Eine Sprache, die es IT-Experten ermöglichte, menschenlesbare Anweisungen als maschinenlesbaren Code zu kompilieren

**ATA:** Die gängigste Schnittstelle, über die Festplatten eine Verbindung zum System herstellen

**ATX (Advanced Technology eXtended):** Der häufigste Formfaktor für Motherboards

**Automatisierung:** Der automatisierte Ablauf von Prozessen

B

**Abwärtskompatibel:** Wenn ältere Hardware mit neuerer Hardware kompatibel ist

**Binärsystem:** Die von einem Computer verwendete Kommunikation wird als Binärsystem bezeichnet, auch als „Base 2-Zahlensystem“ bekannt

**BIOS (Basic Input Output Services):** Software, die beim Initialisieren der Hardware auf dem Computer hilft und das Betriebssystem zum Laufen bringt

**BIOS/UEFI:** Low-Level-Software zum Initialisieren der Hardware des Computers, um sicherzustellen, dass alle Komponenten einsatzbereit sind

**Blockspeicher:** Ermöglicht eine schnellere Datenverarbeitung, da die Daten nicht einzeln, sondern in Blöcken gespeichert werden, sodass ein schnellerer Zugriff möglich ist

**Booten:** Einen Computer starten

**Bootloader:** Ein kleines Programm zum Laden des Betriebssystems

**BYOD (Bring Your Own Device, Nutzung eigener Geräte):** Bezeichnung dafür, dass Mitarbeiter ihre eigenen Geräte zum Arbeiten nutzen können

**Byte:** Eine Folge aus 8 Bit

C

**Cache:** Zugewiesener Speicherort für kürzlich oder häufig aufgerufene Daten; in mobilen Apps wird hier alles gespeichert, das mit der App geändert oder erstellt wurde

**Zeichencodierung:** Wird verwendet, um Zeichen Binärwerte zuzuweisen, damit sie von Menschen lesbar sind

**Ladezyklus:** Die vollständige Ladung und Entladung eines Akkus

**US-Gesetz zum Schutz der Privatsphäre von Kindern im Internet (Children's Online Privacy Protection Act, COPPA):** Regelt, welche Informationen Kindern unter 13 Jahren sehen dürfen

**ChromeOS:** Ein von Google entwickeltes Linux-basiertes Betriebssystem

**Clients:** Geräte, die Daten von einem Server empfangen

**Programmieren:** Übersetzen von Anweisungen in natürlicher Sprache in eine Programmiersprache

**Kompilierte Programmiersprache:** Eine Sprache, die menschenlesbare Anweisungen verwendet und diese dann an einen Compiler sendet

**Computer:** Ein Gerät, das Berechnungen durchführt, um Daten zu speichern und zu verarbeiten

**Urheberrecht:** Wird beim Erstellen von Originalwerken verwendet

**Chipsatz:** Entscheidet, wie Komponenten des Computers miteinander kommunizieren

**Taktzyklus:** Das Senden von elektrischer Spannung an den Taktgeber

**Taktgeschwindigkeit:** Die maximale Anzahl von Taktzyklen, die innerhalb eines bestimmten Zeitraums verarbeitet werden können

**Taktgeber:** Wenn Sie Daten senden oder empfangen, wird elektrische Spannung an diesen Taktgeber gesendet, um die CPU darüber zu informieren, dass die Berechnungen beginnen können

**Befehlszeile:** Eine Shell, die Befehle zur Interaktion mit dem Betriebssystem verwendet

**Computerdatei:** Von uns gespeicherte Daten und Dateien können beliebiger Art sein, wie etwa Textdokumente, Bilder oder Lieder

**CPU:** Zentrale Verarbeitungseinheit

**CPU-Sockel:** Ein CPU-Sockel besteht aus einer Reihe von Kontakten, die den Prozessor einer CPU mit dem Motherboard des PCs verbinden

**Kryptografie:** Die übergeordnete Disziplin, die das Codieren und Verbergen von Nachrichten vor Dritten umfasst

D

**DARPA:** Ein Projekt der US-Regierung in den 1960er-Jahren, durch das die früheste Version des heutigen Internets entstanden ist

**Datenblöcke:** Daten, die in viele Teile zerlegt und in verschiedene Bereiche der Festplatte geschrieben werden können

**Datengrößen:** Maßeinheiten, die sich auf Datengrößen beziehen, darunter Bit, Byte, Kilobyte, Kibibyte und Megabyte

**DDR SDRAM (Double Data Rate SDRAM):** Eine Art von RAM, die schneller ist, weniger Strom verbraucht und eine größere Kapazität als ältere SDRAM-Versionen hat

**Base 10-System in Dezimalform:** Im Dezimalsystem gibt es zehn mögliche Zahlen, die Sie verwenden können – von null bis neun

**Desktop:** Hauptbildschirm, auf dem wir Dateien, Ordner und Anwendungen aufrufen können

**Digitale Spaltung:** Die wachsende Kompetenzlücke zwischen Menschen mit und ohne digitale Kompetenzen

**DIMM:** Dual Inline Memory Module

**Displayport:** Port, der auch Audio und Video ausgibt

**Distributionen:** Gängige Linux-Distributionen sind Ubuntu, Debian und Red Hat

**Domainname:** Name einer Website; der Teil der URL nach www.

**Domain Name System (DNS):** Globaler und hochgradig verteilter Netzwerkdienst, der Buchstabenfolgen (z. B. den Namen einer Website) in eine IP-Adresse auflöst

**DRAM:** Dynamic Random-Access Memory

**Treiber:** Treiber enthalten die Anweisungen, die die CPU benötigt, um externe Geräte wie Tastaturen, Webcams und Drucker zu verstehen

**DVI:** DVI-Kabel geben in der Regel nur Video aus

E

**Elektrostatische Entladung:** Ein plötzlicher und kurzer Stromfluss zwischen zwei elektrisch aufgeladenen Objekten, der durch Kontakt, einen elektrischen Kurzschluss oder einen Spannungsdurchschlag verursacht wird

[Etcher.io:](https://etcher.io/)

Tool, mit dem Sie ein Installations-Image auf Ihr USB-Gerät laden und bootfähig machen können

**Ethernetkabel:** Hiermit können Sie ein Gerät mit dem Netzwerk verbinden

**.exe:** Dateiendung in Windows für eine ausführbare Datei

**Externer Datenbus (EDB):** Besteht aus mehreren Leitungen, die die Bestandteile eines Computers miteinander verbinden

F

**Auf Werkseinstellungen zurücksetzen:** Zurücksetzen des Geräts auf die Einstellungen, mit denen es ausgeliefert wurde

**Glasfaserkabel:** Glasfaserkabel enthalten einzelne optische Fasern, d. h. winzige Röhren aus Glas, die etwa die Breite eines menschlichen Haars aufweisen. Im Gegensatz zu Kupfer, das elektrische Spannung nutzt, verwenden Glasfaserkabel Lichtimpulse, um die Einsen und Nullen der zugrunde liegenden Daten darzustellen.

**Dateiendung:** Der angehängte Teil eines Dateinamens, aus dem hervorgeht, um welchen Dateityp es sich in bestimmten Betriebssystemen handelt

**Dateiverwaltung:** Ein Prozess zum Speichern von Daten mithilfe eines Programms

**Dateisystem:** Ein System zur Verwaltung von Dateien

**Firmware:** Software, die dauerhaft auf einer Computerkomponente gespeichert ist

**Finder:** Der Dateimanager für alle Macs

**Ordner/Verzeichnisse:** Zum Organisieren von Dateien

**Formfaktor:** Eine mathematische Methode, um Unregelmäßigkeiten in der Form eines Objekts durch das Verhältnis zwischen Volumen und Höhe auszugleichen

G

**GIT:** Ein Versionskontrollsystem, mit dem Änderungen an Dateien und Verzeichnissen nachverfolgt werden können

**Globalisierung:** Der Vorgang, der weltweite Verflechtungen und Kommunikation unter Behörden, Unternehmen und Organisationen ermöglicht

H

**Festplatte:** Speicherkomponente zum dauerhaften Speichern von Daten wie Musik, Bildern und Anwendungen

**Hardware:** Externe oder interne Geräte und Zubehör, mit denen Sie wichtige Funktionen ausführen können

**Hardware-Ressourcenmangel:** Bezieht sich auf den Mangel an Systemressourcen wie Arbeitsspeicher, Festplattenspeicher usw.

**HDD (Hard Disk Drive, Festplatte):** Festplatten bzw. HDDs nutzen eine rotierende Scheibe und einen mechanischen Arm, um Informationen zu lesen und zu schreiben

**HDMI:** Ein Kabeltyp, der sowohl Video- als auch Audiosignale ausgibt

**Kühlkörper:** Wird verwendet, um Wärme von der CPU abzuleiten

**HFS+/APFS:** HFS+ ist ein Journaling-System, das von Apple Inc. entwickelt wurde. APFS ist ein weiteres, aber verschlüsseltes Journaling-System von Apple

**Hostname:** Wird verwendet, um den Computer für die Kommunikation mit anderen Computern zu identifizieren

**Hubs:** Geräte, die als zentraler Ort fungieren, über den Daten geleitet werden

I

**Informationstechnik:** Der Einsatz von digitaler Technologie wie Computern und dem Internet zum Speichern und Verarbeiten von Daten in nützliche Informationen

**Eingabe-/Ausgabegerät:** Ein Gerät, das die Ein- und Ausgabe übernimmt, darunter Monitore, Tastaturen, Mäuse, Festplattenlaufwerke, Lautsprecher, Bluetooth-Headsets, Webcams und Netzwerkadapter

**Installations-Image:** Betriebssystem-Image, das zum Installieren eines Betriebssystems auf einem Gerät heruntergeladen werden kann

**Befehlssatz:** Eine Liste der Befehle, die die CPU ausführen kann

**Internet:** Ein weltweiter Verbund von Netzwerken

**Internet Corporation for Assigned Names and Numbers (ICANN):** Koordiniert die Vergabe von Websitenamen

**Internet der Dinge (IoT):** Mit dem Internet auf intelligente Weise verbundene Geräte, z. B. intelligente Thermostate, die die Klimaanlage ausschalten, wenn Sie das Haus verlassen, und wieder einschalten, wenn Sie zurückkommen

**Internet Protocol Version 4 (IPv4):** Eine Adresse mit 32 Bit, unterteilt in vier Gruppen

**Internet Protocol Version 6 (IPv6):** Eine Adresse mit 128 Bit, also viermal so viel wie IPv4

**Internetanbieter:** Ein Unternehmen, das Nutzern eine Internetverbindung zur Verfügung stellt

**Interpretersprache:** Eine Sprache, die nicht im Voraus kompiliert wird

**I/O-Management:** Der Prozess zum Übertragen von Daten in das System und aus dem System

**iOS:** Ein mobiles Betriebssystem, das von Apple Inc. entwickelt wurde

**IP-Adresse:** Das gängigste Protokoll, das in der Netzwerkschicht verwendet wird und beim Routing von Informationen hilft

**ITX (Information Technology eXtended):** Ein Formfaktor für Motherboards, der deutlich kleiner ist als ATX-Boards

K

**Kernel:** Der zentrale Bestandteil eines Betriebssystems, in dem Prozesse erstellt und effizient geplant werden und die Beendigung von Prozessen verwaltet wird

## L

**Land Grid Array (LGA):** Eine Art von CPU-Sockel, der aus dem Motherboard herausragt

**Lightning-Adapter:** Einer der Standardsteckertypen für Stromversorgung, Daten und Display an Mobilgeräten

**Linux-Betriebssystem:** Linux ist eines der größten Open-Source-Betriebssysteme mit häufiger Verwendung in der Unternehmensinfrastruktur und im Verbraucherbereich

**Logikgatter:** Ermöglicht Transistoren die Ausführung komplexer Aufgaben wie etwa festlegen, wohin elektrische Signale je nach logischen Bedingungen gesendet werden sollen

**Protokolle:** Dateien zur Erfassung von Systemereignissen auf dem Computer

## M

**MAC-Adresse:** Eine global eindeutige Kennung, die an eine einzelne Netzwerkschnittstelle angehängt ist. Es ist eine 48-Bit-Zahl, die normalerweise durch sechs Gruppierungen von zwei Hexadezimalzahlen dargestellt wird.

**Mac OS:** Betriebssystem von Apple

**Mbit/s:** Megabit pro Sekunde, eine Einheit für die Datenübertragungsrate

**Speichercontroller (Memory Controller Chip, MCC):** Eine Brücke zwischen CPU und RAM

**Arbeitsspeicherverwaltung:** Eine der Funktionen, die ein Kernel ausführt; optimiert die Arbeitsspeichernutzung und sorgt dafür, dass die Anwendungen genügend Arbeitsspeicher für die Ausführung haben

**Metadaten:** Enthalten alle notwendigen Informationen zu einer Datei: wer sie erstellt hat, wann sie zuletzt geändert wurde, wer darauf Zugriff hat und was der Dateityp ist

**Micro-DisplayPort:** Einer der Standardsteckertypen für Stromversorgung, Daten und Display auf Mobilgeräten

**Microsoft Terminal Services Client:** Ein Clientprogramm zum Erstellen von RDP-Verbindungen zu Remote-Computern

**Micro-HDMI:** Einer der Standardsteckertypen für Stromversorgung, Daten und Display auf Mobilgeräten

**Micro-USB:** Einer der Standardsteckertypen für Stromversorgung, Daten und Display auf Mobilgeräten

**Mini-HDMI:** Einer der Standardsteckertypen für Stromversorgung, Daten und Display auf Mobilgeräten

**Mini-USB:** Einer der Standardsteckertypen für Stromversorgung, Daten und Display auf Mobilgeräten

**Motherboard:** Sozusagen der Körper oder das Kreislaufsystem des Computers, das alle Teile miteinander verbindet

## N

**Netzwerk:** Verbindung von Computern untereinander

**Network Address Translation (NAT):** Mit diesem Tool können Organisationen eine öffentliche IP-Adresse und viele private IP-Adressen innerhalb des Netzwerks nutzen

**Vernetzung:** Netzwerke verwalten, erstellen und entwerfen

**Netzwerkprotokolle:** Regeln für die Übertragung von Daten in einem Netzwerk

**Netzwerkstack:** Hardware oder Software zur Bereitstellung der Infrastruktur eines Computers

**Northbridge:** Verbindet Dinge wie RAM und Grafikkarten miteinander

O

**Open SSH:** Das beliebteste Programm zur Verwendung von SSH in Linux

**Open Source:** Software, bei der Entwickler anderen Entwicklern das Recht einräumen, ihre Software kostenlos freizugeben, zu ändern und zu verteilen

**Betriebssystem:** Das komplette Paket, das die Ressourcen des Computers verwaltet und es uns ermöglicht, mit ihm zu interagieren

**Übertakten:** Erhöht die Rate der CPU-Taktzyklen, um mehr Aufgaben zu erledigen

P

**PC:** Ein Personal Computer, also ein Computer, der für den persönlichen Gebrauch gedacht ist

**PCI Express:** Peripheral Component Interconnect Express

**PDA (Personal Digital Assistant):** Ein tragbarer kompakter Computer

**Peripheriegeräte:** Externe Geräte, die an den Computer angeschlossen werden und zusätzliche Funktionen bieten, z. B. Maus, Tastatur und Monitor

**Pin Grid Array (PGA):** CPU-Sockel, in dem sich die Kontakte im Prozessor selbst befinden

**Plink (PuTTY Link):** Ein nach der Installation von PuTTY in die Befehlszeile integriertes Tool, das für SSH-Remote-Verbindungen verwendet wird

**Ports:** Verbindungspunkte, mit denen wir Geräte verbinden können, um die Funktionalität des Computers zu erweitern

**POST (Power-On Self Test):** Kann feststellen, welche Hardware sich auf dem Computer befindet

**PowerShell:** Eine Shell (Programm, das Textbefehle interpretiert) für Windows

**Netzteil:** Wandelt den Strom aus der Steckdose in ein Format um, das ein Computer nutzen kann

**Poweruser:** Ein Nutzer mit überdurchschnittlichen Computerkenntnissen

**Prozessverwaltung:** Die Fähigkeit, die vielen Programme in einem System zu verwalten – wann sie ausgeführt werden, in welcher Reihenfolge sie ausgeführt werden, wie viele Ressourcen sie verbrauchen, wie lange sie ausgeführt werden usw.

**Programmierung:** Coding in einer Programmiersprache



**Programmiersprache:** Software, mit der Softwareentwickler Anleitungen schreiben, die von Computern ausgeführt werden

**Programme:** Grundlegende Anweisungen, die dem Computer mitteilen, was er tun soll

**Lochkarten:** Sequenz aus Karten mit Löchern, die automatisch Berechnungen vornehmen, statt diese manuell einzugeben

Q

**Qwiklabs:** Eine Onlineplattform für Schulungen in Cloud-Diensten

R

**RAM:** Random-Access Memory

**Register:** Ein zugänglicher Speicherort zum Aufbewahren der Daten, mit denen die CPU arbeitet

**Neuaufspielen eines Images:** Der Prozess, bei dem ein Betriebssystem auf die Werkseinstellungen zurückgesetzt und mit einem Speicherabbild (die Kopie eines Betriebssystems) neu installiert wird

**Remote-Verbindung:** Möglichkeit, eine autorisierte Person per Fernzugriff mit einem Computer oder Netzwerk zu verbinden; ermöglicht die Verwaltung mehrerer Computer von überall in der Welt

**Remote Desktop Protocol (RDP):** Ein von Microsoft entwickeltes sicheres Netzwerkkommunikationsprotokoll, mit dem Nutzer eine Remoteverbindung zu einem anderen Gerät herstellen können

**Rücksendeschein (Return Merchandise Authorization, RMA):** Der Vorgang für den Erhalt zurückgegebener Merchandise-Artikel und die Autorisierung einer Erstattung

**RGB-Modell:** Das RGB-Modell (Rot Grün Blau) ist das Basismodell für die Darstellung von Farben

**ROM-Chip (Read Only Memory, Nur-Lese-Speicher):** Ein schreibgeschützter Speicherchip, in dem das BIOS gespeichert wird

**Router:** Ein Gerät, das Daten zwischen unabhängigen Netzwerken weiterleiten kann

**U/min:** Umdrehungen pro Minute

S

**Sichere Betriebstemperatur:** Der Temperaturbereich, in dem Akkus betrieben werden müssen, um Schäden zu verhindern

**SATA:** Das beliebteste serielle ATA-Laufwerk, das für die Datenübertragung ein einzelnes Kabel verwendet

**Skalierbarkeit:** Das Maß der Fähigkeit eines Systems, Leistung und Kosten als Reaktion auf unterschiedliche Lasten bei den Anforderungen der Systemverarbeitung zu erhöhen oder zu senken

**Script:** Wird von einem Interpreter ausgeführt, der den Code genau zur richtigen Zeit in CPU-Anweisungen umwandelt, um sie auszuführen

**Scripting:** Programmieren in einer Scriptsprache

**SDRAM:** Synchroner DRAM; eine Art von RAM, mit dem die Taktgeschwindigkeit der Systeme synchronisiert wird, um eine schnellere Verarbeitung von Daten zu ermöglichen

**Server-Logs:** Textdateien, die aufgezeichnete Informationen zu Aktivitäten enthalten, die in einem bestimmten Zeitraum auf einem bestimmten Webserver ausgeführt wurden

**Server:** Geräte, die Daten an andere Geräte senden, die diese Daten anfordern (auch als Client bezeichnet)

**Shell:** Ein Programm, das Textbefehle interpretiert und zur Ausführung an das Betriebssystem sendet

**SoC (System-on-Chip):** Packt CPU, RAM und manchmal auch Speicher auf einen einzelnen Chip

**Software:** Immaterielle Anweisungen, die der Hardware vorgeben, was zu tun ist

**Softwarefehler:** Ein Fehler in der Software, der unerwartete Ergebnisse verursacht

**Softwareverwaltung:** Ein allgemeiner Begriff, der sich auf jede Art von Software bezieht, die dazu dient, ein Projekt oder eine Aufgabe zu verwalten oder dabei zu helfen

**Southbridge:** Verwaltet die E/A-Controller (Eingabe/Ausgabe), z. B. Festplatten und USB-Geräte, die Daten ein- und ausgeben

**SSD:** Solid State Drive

**SSH (Secure Shell):** Ein Protokoll, das von anderen Programmen für den sicheren Zugriff auf einen Computer über einen anderen Computer implementiert wird

**SSH-Authentifizierungsschlüssel:** Sicheres Authentifizierungsverfahren, das den Zugriff auf einen Computer über andere Geräte ermöglicht

**SSH-Client:** Ein Programm, das auf Ihrem Gerät installiert sein muss, damit eine SSH-Verbindung zu einem anderen Gerät hergestellt werden kann

**SSH-Server:** Auf einem Computer installierte Software, mit der dieses Gerät eine SSH-Verbindung akzeptieren kann

**Standardisierung:** Eine systematische Methode zur Benennung von Hosts

**Abstandhalter:** Wird verwendet, um das Motherboard anzuheben und am Gehäuse zu fixieren

**Auslagerungsbereich:** Zugewiesener Speicherplatz, unter dem der virtuelle Arbeitsspeicher auf der Festplatte gespeichert wird, wenn der physische Speicherplatz vollständig belegt ist

**Switches:** Geräte zur Unterstützung der Datenübertragung

**System:** Ein System bezieht sich auf eine Gruppe von Hardware- und Softwarekomponenten, die zusammen die Programme oder Prozesse auf dem Computer steuern

**Systemeinstellungen:** Einstellungen wie Bildschirmauflösung, Nutzerkonten, Netzwerk, Geräte usw.

**Systemsoftware:** Software, die dazu dient, die zentralen Abläufe des Systems zu steuern, z. B. Betriebssystemtools und Dienstprogramme

D

**Taskleiste:** Bietet schnellen Zugriff auf Optionen und Informationen wie Netzwerkverbindung, Datum, Systembenachrichtigungen, Ton usw.

**Terminal:** Eine textbasierte Schnittstelle zum Computer

**Wärmeleitpaste:** Eine Substanz, die dazu dient, die Verbindung zwischen CPU und Kühlkörper zu verbessern, damit die Wärme vom einen zum anderen abgeleitet wird

**Zeitschlitz:** Ein sehr kurzes Zeitintervall, das einem Prozess für die CPU-Ausführung zugewiesen wird

**Transfer Control Protocol (TCP):** Ein Protokoll zur zuverlässigen Übermittlung von Informationen von einem Netzwerk an ein anderes

**USB-C-Anschluss:** Ein USB-Stecker, durch den viele Verbindungen von Peripheriegeräten ersetzt werden sollen

U

**Ubuntu:** Die beliebteste Linux-Distribution für Verbraucher

**UEFI:** United Extensible Firmware Interface

**Uniform Resource Locator (URL):** Eine Webadresse, die einer Privatadresse ähnelt

**USB (Universal Serial Bus):** Ein Verbindungsstandard für den Anschluss von Peripheriegeräten an Geräte wie Computer

**USB-C-Adapter:** Einer der Standardsteckertypen für Stromversorgung, Daten und Display auf Mobilgeräten

**Nutzername:** Eine eindeutige Kennzeichnung für ein Nutzerkonto

**Userspace:** Der Aspekt eines Betriebssystems, mit dem Nutzer direkt interagieren, z. B. Programme wie Texteditoren, Musikplayer, Systemeinstellungen, Benutzeroberflächen usw.

**UTF-8:** Der heute am häufigsten verwendete Codierungsstandard

V

**Virtual Box:** Eine Anwendung, mit der Sie Linux installieren und vollständig von Ihrem Computer isoliert ausführen können

**Virtuelle Maschine (VM):** Eine Anwendung, die physische Ressourcen wie Arbeitsspeicher, CPU und Speicher nutzt und außerdem den Vorteil bietet, dass mehrere Betriebssysteme gleichzeitig ausgeführt werden können

**Virtueller Arbeitsspeicher:** Kombination aus Festplattenspeicher und RAM, die als Arbeitsspeicher dient und von Prozessen verwendet werden kann

**VPN (Virtuelles privates Netzwerk):** Sichere Methode, ein Gerät über das Internet mit einem privaten Netzwerk zu verbinden

W

**WannaCry-Angriff:** Ein Cyberangriff, der in Europa initiiert wurde und Tausende von Computern weltweit infizierte

**Drahtlose Netzwerke (WLAN):** Netzwerke, zu denen Sie über Funkschnittstellen und Antennen eine Verbindung herstellen

**World Wide Web (WWW):** Das Informationssystem, mit dem Dokumente und andere Webressourcen über das Internet aufgerufen werden können

# Kurs 2

## TCP/IP-Fünf-Schichten-Netzwerkmodell

#	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc...	Messages	n/a
4	Transport	TCP/UDP	Segment	Port #'s
3	Network	IP	Packet / Datagram	IP Address
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address
1	Physical	n/a	Bits	n/a

- physical layer: represents the physical devices that interconnect computers
- -> Spezifikationen für die Netzkabel und Steckertypen, die Geräte miteinander verbinden sowie Spezifikationen, die die Signalübertragung beschreiben
- data link layer (network interface): -> Protokolle
- Verkabelung, Steckertypen und Signale
- legt fest, wie die Signale interpretiert werden, damit Netzwerkgeräte kommunizieren können
- bekanntestes Protokoll auf der data link Schicht -> 'Ethernet'
- Ethernet beschreibt nicht nur Eigenschaften der Bitübertragungsschicht, es definiert auch ein Protokoll, das Daten zu Netzwerk- oder Verbindungsknoten bewegt
- network layer (internet layer): allows different networks to communicate with each other through devices known as router
- internetwork: a collection of networks connected together through routers (most famous: Internet)
- IP (Internet Protocol) ist das Herzstück des Internets und für die meisten kleineren Netzwerke
- Netzwerksoftware -> Client und Server -> Client-Anwendungen stellen Anfrage nach Daten und Server-Software beantwortet Anfrage über das Netzwerk
- überträgt Datenschicht zw. zwei einzelnen Knoten
- transport layer: legt fest, welche Clients und welche Server die Daten letztendlich erhalten sollen
- Bsp: bei Ihnen können E-Mail-Programme und Webbrowser laufen. Sowohl die Client-Anwendung auf Ihrem Computer als auch Ihr E-Mail- und Web-Server können gleichzeitig auf demselben Server laufen. Trotzdem werden E-Mails an Ihre E-Mail-Anwendung gesendet und Internetseiten an Ihren Webbrowser
- wichtig: die Netzwerkschicht, hier: IP, dafür sorgt, dass Daten von einem zum anderen Knoten gelangen. Wichtig ist außerdem, dass TCP und UDP dafür sorgen, dass Daten zur richtigen Anwendung auf diesen Knoten geleitet werden
- application layer: unzählige Protokolle, die anwendungsspezifisch sind
- Protokolle, die es erlauben, im Internet zu surfen oder auch E-Mails zu empfangen, gehören zu den gängigsten



Physical



Data Link



Network



Transport



Application

- Hub ist ein physical layer device (verbindet geräte, aber sendet daten an alle gleichzeitig)
- switch ist ein data layer device —> kann die Inhalte der Ethernet-Protokoll Daten untersuchen, die im Netzwerk gesendet werden, dann festlegen, für welches Gerät die Daten bestimmt sind, und die Daten entsprechend weiterleiten
- Router verbindet Netzwerk mit dem Internet (ist aber gleichzeitig auch ein switch, da er die lokalen Geräte über Kabel oder WLAN verbindet)
- Router = network layer device
- Der Router leitet den Traffic an den ISP, also den 'Internet Service Provider', weiter
- Sobald der Traffic beim ISP ankommt, übernehmen weitaus ausgefeiltere Router —>

### Core-Router

- Router tauschen Daten über das Protokoll BGP aus („Border Gateway Protocol“)
- zeigt dem Router den besten Weg, um Traffic weiterzuleiten
- Wenn Sie einen Webbrowser öffnen und eine Seite im Internet laden, hat der Traffic zwischen Computer und Webserver eine Reise über dutzende Router zurückgelegt
- alle Netzwerkgeräte ermöglichen es Computern, miteinander zu kommunizieren (Knoten)
- **Server**: stellt Daten für etwas bereit, das Daten anfordert
- -> **Client** erhält die Daten
- meist sind die Knoten (nodes) beides, aber eben primär Client oder primär Server

- Kabel: Mittels **Modulation** kann die Spannung der Ladung über das Kabel variiert werden
- Im Falle von Computernetzwerken wird diese Art der Modulation eher als Leitungscodierung bezeichnet
- Dadurch können Geräte an jedem Ende der Verbindung verstehen, dass die elektrische Ladung in einem bestimmten Zustand Eins bedeutet und in einem anderen Null -> 10 Mrd. Einsen und Nullen pro Sekunde über ein einzelnes Kabel
- duplex communication -> Informationen in beide Richtungen möglich

## Ethernet und MAC-Adressen

- Mit CSMA/CD wird bestimmt, wann die Kommunikationskanäle frei sind und wann das Gerät Daten übermitteln kann
- MAC-Adressen:
  - Die ersten 3 Oktette der Adresse heißen OUI -> Hardwarehersteller erhalten diese vom IEEE
  - Die letzten drei Oktette der Adresse kann der Hersteller nach Belieben vergeben, wobei jede Adresse aber nur einmal vergeben werden darf
  - Beim Ethernet wird mit MAC-Adressen sichergestellt, dass die gesendeten Daten eine Adresse für die Maschine haben, die die Übertragung sendete, und eine für die, für die sie gedacht war.
- Eine Unicast-Übertragung ist immer nur für eine Empfängeradresse bestimmt

Begriff	Empfänger	Beispiel
Unicast	Ein einzelnes Gerät	Laptop → Drucker
Multicast	Bestimmte Gruppe von Geräten	Live-Video-Stream an Abonnenten
Broadcast	Alle Geräte im Netzwerk	DHCP-Anfrage „Wer ist hier?“

### Unicast vs. Multicast vs. Broadcast

**Unicast:** Paket an die feste MAC-Adresse eines *einzelnen* Geräts.

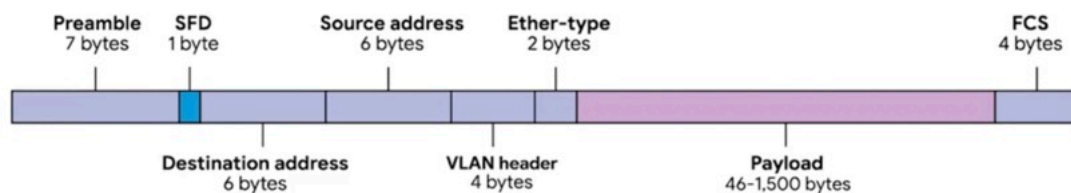
**Multicast:** Paket an eine spezielle Multicast-MAC-Adresse, die eine **Gruppe** von Geräten repräsentiert. Dein Gerät sagt: „Ich möchte die Pakete dieser Gruppe empfangen.“

**Broadcast:** Paket an die Adresse **FF:FF:FF:FF:FF:FF**, das *alle* Geräte im lokalen Netzwerk erhalten.

- Datenpaket: ist ein allumfassender Begriff, der alle Binärdatensätze bezeichnet, die über Netzwerkverbindungen gesendet werden
- an keine Ebene oder Technologie gebunden

## Ethernet-Frame

- Ethernet-Frame: stark strukturierte Sammlung von Informationen, angeordnet in einer bestimmten Reihenfolge



- Preamble (Präambel):
  - 8 Byte bzw. 64 Bit lang und kann in zwei Abschnitte aufgeteilt sein ->
  - die ersten 7 Byte: Reihe alternierender Einsen und Nullen -> fungieren teilweise als Puffer zwischen den Frames und können von Schnittstellen genutzt werden, um interne Uhren zu synchronisieren, die die Geschwindigkeit regulieren, mit der sie Daten senden
  - letzter Teil des Preambles -> zeigt einem Empfangsgerät, dass die Präambel jetzt zu Ende ist und der tatsächliche Frame-Inhalt folgt
- Destination address -> MAC-Adresse des Empfängers
- Source address -> MAC-Adresse des Senders
- Ether-type: beschreibt das Protokoll der Frame-Inhalte
- statt Ethertype-field kann auch VLAN header vorhanden sein, dann folgt das Ether-type-field darauf
- VLAN = virtual LAN
  - Diese Technik erlaubt es, dass auf derselben physischen Ausstattung mehrere logische LANs betrieben werden
  - Jedes Frame mit VLAN-Tag wird nur aus einem Switch gesendet, der so konfiguriert ist, dass er genau diesen Tag weiterleitet
  - -> physisches Netzwerk, das wie mehrere LANs funktioniert
  - VLANs werden meist genutzt, um verschiedene Arten von Traffic zu trennen -> bei Firmen operieren evtl. alle IP-Telefone in einem VLAN und alle Computer in einem anderen
- Payload: die eigentlichen Daten, die transportiert werden -> alle Daten der höheren Ebenen, wie der IP-, Transport- und Anwendungsebene, die tatsächlich übermittelt werden
- frame check sequence: Eine zyklische Redundanzprüfung, kurz CRC, ist ein wichtiges Datenintegritätskonzept und wird in der Informatik überall genutzt
  - Führen Sie für 1 Datensatz eine CRC durch, sollte jedes Mal dieselbe Prüfsummenzahl rauskommen -> Empfänger-Netzwerkschnittstelle weiß, ob sie fehlerfreie Daten empfangen hat
  - ist der Frame fehlerhaft, muss eine höhere Ebene entscheiden, ob die Datei nochmals gesendet wird -> Ethernet meldet nur die Datenintegrität, stellt jedoch keine Daten wieder her

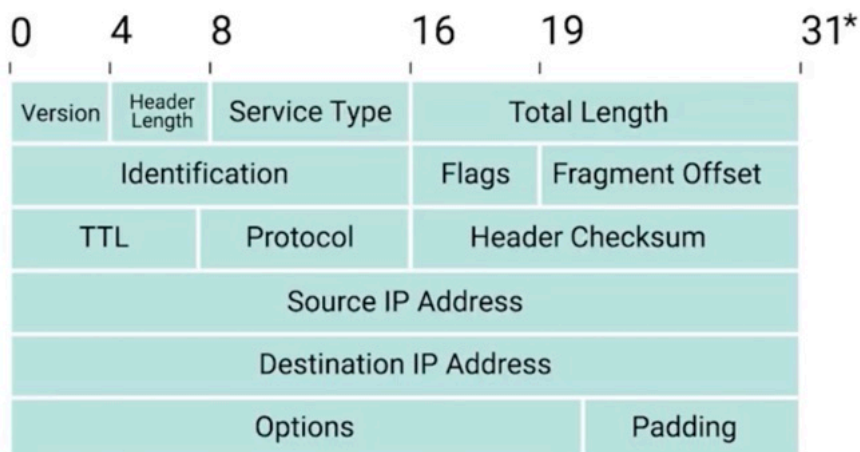
## IPV4-Adressen

- IP-Adressen sind Nummern mit einer Länge von 32 Bits, bestehend aus vier Oktetten
- IP-Adressen gehören zu Netzwerken, nicht zu den Geräten, die an diese angeschlossen sind
- Ihr Laptop hat immer dieselbe MAC-Adresse, egal wo Sie ihn benutzen, aber ihm wird in einem Internet-Café eine andere IP-Adresse zugeordnet als bei Ihnen zuhause
- -> Dynamic Host Configuration Protocol
- Eine auf diese Weise zugewiesene IP-Adresse wird dynamische IP-Adresse genannt
- Gegenteil: statische IP-Adresse -> muss auf einem Knoten manuell konfiguriert werden
- statische IP-Adressen -> auf Servern und Netzwerkgeräten verwendet
- dynamische IP-Adressen -> für Clients reserviert

## IPv4-Datagramm und Datenkapselung

- Unter dem IP-Protokoll wird ein Paket gewöhnlich als IP-Datagramm bezeichnet
- Genau wie Ethernet-Frames sind IP-Datagramme eine hochstrukturierte Reihe von Feldern, die genau definiert sind

### IP Datagram Header

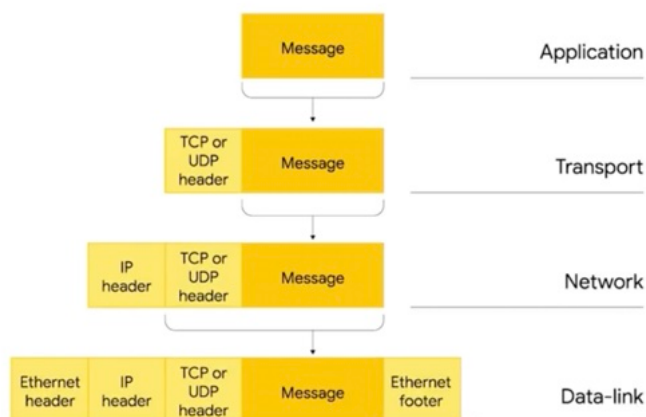


\*32 bits total including 0.

- die ersten 4 Bits: zeigt an, welche **Version** des Internet-Protokolls verwendet wird
- **Header Length**: 4 Bits -> legt die gesamte Länge des Headers fest (20 Bytes ist die Mindestlänge eines IP-Headers)
- **Service Type**: Diese 8 Bits können verwendet werden, um Details zur Dienstgüte oder QoS-Technologie anzugeben -> Dienste, die es Routern ermöglichen, zu entscheiden, welches IP-Datagramm wichtiger sein könnte als andere
- **Total Length**: 16 Bit -> Es gibt die Gesamtlänge des IP-Datagramms an, an das es angehängt ist
- Das Identifikationsfeld ist eine 16-Bit-Nummer und wird zum Gruppieren von Nachrichten verwendet
- Die maximale Größe eines einzelnen Datagramms ist also die größte Zahl, die man mit 16 Bits darstellen kann: 65.535
- Wenn die Gesamtmenge an Daten, die gesendet werden muss, größer ist, als die Menge, die in ein Datagramm passt, muss die IP-Schicht diese Daten in viele individuelle Pakete aufspalten



- Wenn das passiert, wird das Identifikationsfeld (**Identification**) verwendet, so dass die Empfängerseite versteht, dass jedes Paket mit demselben Wert in diesem Feld, Teil der gleichen Übertragung ist
- **Flags-Feld** wird verwendet, um anzugeben, ob das Datagramm fragmentiert werden darf oder dass das Datagramm bereits fragmentiert wurde
- Fragmentierung ist der Prozess, bei dem ein einzelnes IP-Datagramm in mehrere aufgespalten wird.
- Die meisten Netzwerke arbeiten mit ähnlichen Einstellungen in Bezug auf die erlaubte Größe und das IP-Datagramm
- Die Konfiguration kann aber auch Unterschiede haben: Wenn ein Datagramm von einem Netz, das eine größere Datagramm-Größe erlaubt, in ein Netz mit kleinerer Größe wechselt, müsste das Datagramm in mehrere kleinere aufgespalten werden
- -> Das Feld **Fragmentation Offset** enthält Werte, die von der Empfängerseite verwendet werden, um alle Teile eines fragmentierten Pakets wieder in die richtige Reihenfolge zusammenzusetzen
- **TTL**: Dieses 8-Bit-Feld gibt an, wie viele Router-Sprünge ein Datagramm durchlaufen kann, bevor es verworfen wird -> damit es bei Fehlkonfiguration nicht zu einer Endlosschleife kommt
- **Protocol**: 8-Bit-Feld enthält Daten darüber, welches Protokoll für Transportschichten verwendet wird -> Die gängigsten Protokolle für Transportschichten sind **TCP und UDP**
- **Header Checksum**: Prüfsumme der Inhalte des gesamten Headers des IP-Datagramms
- Da das TTL-Feld bei jedem Router neu berechnet werden muss, den ein Datagramm passiert, ändert sich zwangsläufig auch das Prüfsummenfeld
- **Options** field: wird für das Einrichten spezieller Eigenschaften für Datagramme benutzt, die für Testzwecke verwendet werden
- Da das Optionen-Feld in Bezug auf die Länge sowohl optional als auch variabel ist, besteht das **Padding-Feld** aus einer Reihe von Nullen, die sicherstellen, dass der Header die korrekte Gesamtgröße hat
- Payload-Feld bei Ethernet-Frame = IP-Datagramm -> der Prozess wird **Kapselung** genannt

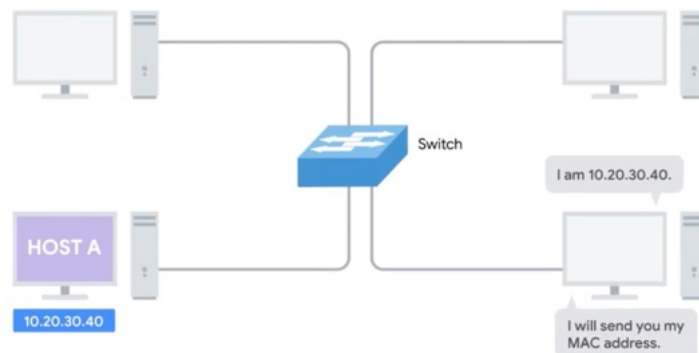


## IPv4-Adressklassen

- IP-Adressen können in zwei Abschnitte unterteilt werden: Die Netzwerk-ID und die Host-ID
- unterschiedliche Adressklassen (A,B,C,D,E) -> hängt mit Länge der Host ID zusammen

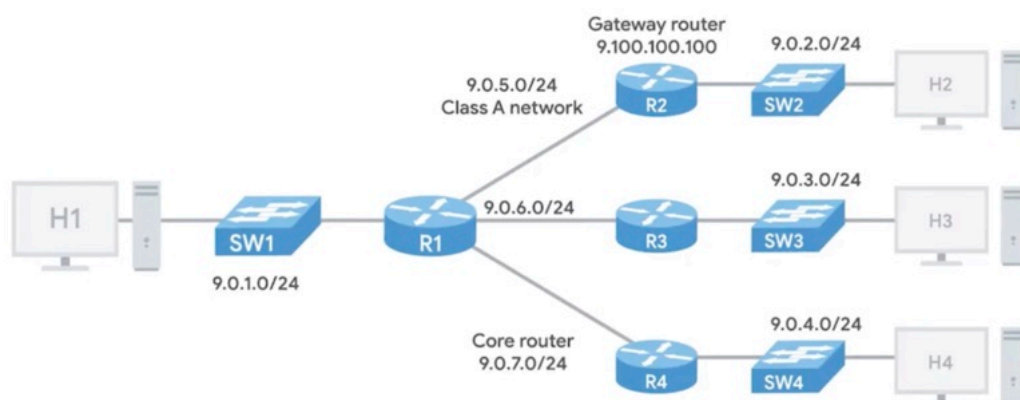
## Address Resolution Protocol (ARP)

- ARP verwendet man zur Ermittlung der Hardware-Adresse eines Knotens mit einer bestimmten IP-Adresse
- Sobald ein IP-Datagramm vollständig zusammengebaut ist, muss es in einem Ethernet-Rahmen gekapselt werden -> Dies bedeutet, dass das Sendergerät eine MAC-Zieladresse benötigt, um den Header des Ethernet-Frames zu vervollständigen
- Fast alle mit dem Netzwerk verbundenen Geräte behalten eine lokale ARP-Tabelle
- **ARP-Tabellen sind Listen mit IP-Adressen und den mit ihnen verbundenen MAC-Adressen**



- Jetzt weiß der sendende Computer, welche MAC-Adresse er in das Feld der Zieladresse der Hardware setzen muss -> Der Ethernet-Frame ist bereit für die Übertragung
- Er speichert diese IP-Adresse wahrscheinlich für eine Weile in seiner lokalen ARP-Tabelle, damit bei der nächsten Kommunikation kein ARP-Broadcast an die IP gesendet werden muss

## Subnetze



- Wenn wir mit der IP-Adresse 9.100.100.100 kommunizieren möchten, wissen die Core-Router im Internet, dass diese IP-Adresse zum Netzwerk 9.0.0.0 der Klasse A gehört
- Sie leiten die Nachricht dann an das **Gateway** weiter, das gemäß der Netzwerk-ID für das Netzwerk verantwortlich ist
- -> **Ein Gateway dient gezielt als Eintritts- und Austrittspunkt eines bestimmten Netzwerks**
- Im Gegensatz dazu können Core-Internetrouter nur mit anderen Core-Routern sprechen

- Wenn unser Datenpaket zum Gateway für Netzwerk 9.0.0.0 Klasse A gelangt, ist der Router dafür verantwortlich, diese Daten je nach der Host-ID zum richtigen System weiterzuleiten
- **Subnetting:** Mit Subnetzen können wir große Netzwerke in viele kleinere unterteilen -> Jedes einzelne Subnetz verfügt dabei über ein eigenes Gateway, das als Eintrittspunkt und Austrittspunkt für dieses Subnetz dient

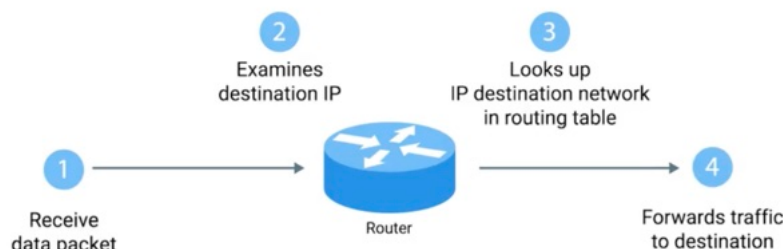
## CIDR

- 254 Hosts in einem Klasse-C-Netzwerk ist für viele Anwendungsfälle zu klein
- Aber die verfügbaren 65.534 Hosts in einem Klasse-B-Netzwerk sind oft viel zu viele
- -> viele Unternehmen hatten schließlich mehrere angrenzende Klasse-C-Netze, um ihre Bedürfnisse zu erfüllen -> das führte zu Routingtabellen mit etlichen Einträgen für etliche Klasse-C-Netze, die tatsächlich alle zum selben Ort geroutet wurden
- -> hier kommt **CIDR**, Classless Inter-Domain Routing, ins Spiel
- Demarkation Point: where one network ends and another one begins
- im vorherigen Modell bauten wir auf eine Netzwerk-ID, Subnetz-ID und Host-ID, um Datenpakete an die richtige Stelle zu liefern
- Bei CIDR werden die Netzwerk-ID und die Subnetz-ID vereint
- CIDR führt uns zu dieser Kurzschreibweise mit Schrägstrich, die wir vorher im Video über Subnetting gesehen haben -> Die Schreibweise mit Schrägstrich heißt auch **CIDR-Notation**

## Routing

- Router: Netzwerkgerät, das Datenverkehr je nach der Zieladresse des Pakets weiterleitet

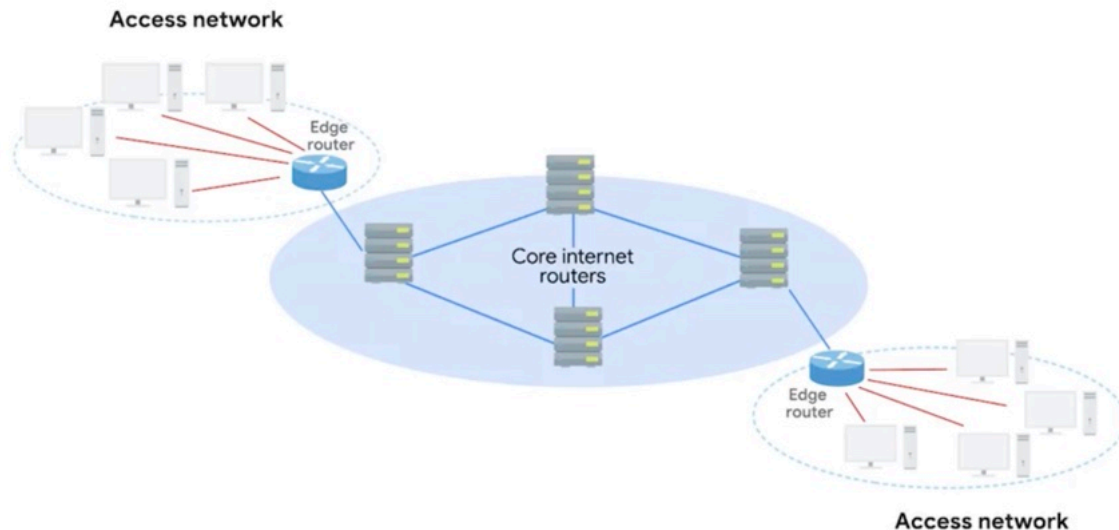
### Basic routing:



- -> Diese Schritte werden so oft wiederholt, bis das Datenpaket sein Ziel erreicht
- **Interior Gateway Protocols:** werden von Routern für den Informationsaustausch in einem einzelnen autonomen System verwendet (hier: einzelnes System = Netzbetreiber)
- **Exterior Gateway Protocols:** werden für den Informationsaustausch zwischen unabhängigen autonomen Systemen verwendet
- In der Informationstechnik werden Listen als Vektor bezeichnet
- Deshalb nennt man ein Protokoll, das nur eine Liste von Entfernungen an Netzwerke sendet, ein Distanzvektor-Protokoll
- Distanzvektor-Protokolle sind recht einfach, aber sie geben einem Router nicht viel Auskunft über den Zustand der Welt über ihre direkten Nachbarn hinaus
- -> Link-State-Protokolle haben einen komplexeren Ansatz an die Ermittlung des besten Wegs zu einem Netzwerk
- Link-State-Protokolle heißen so, weil jeder Router den Verbindungszustand jeder seiner Schnittstellen bekannt gibt
- Diese Schnittstellen können mit anderen Routern verbunden sein oder es können Direktverbindungen zu Netzwerken sein
- Link-State-Protokolle haben die Distanzvektor-Protokolle weitgehend überholt

## exterior-Gateway-Protokolle, autonome Systeme und die IANA

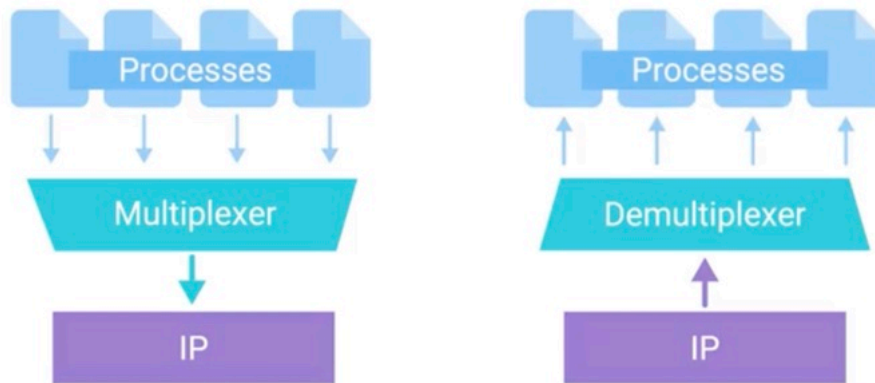
- Das Internet ist ein riesiges Netz autonomer Systeme
- Auf der höchsten Ebene brauchen Core-Internet-Router Informationen über autonome Systeme, um Traffic entsprechend weiterzuleiten
- Autonome Systeme sind bekannte und definierte Netzwerk-Kollektionen, wobei der Transport von Daten zum Edge-Router eines autonomen Systems das oberste Ziel von Core Internet-Routern ist



- Die **IANA** oder Internet Assigned Numbers Authority ist eine Nonprofit-Verwaltungsorganisation u. a. für die Zuteilung von IP-Adressen -> Das Internet könnte ohne eine zentrale Behörde für diese Dinge nicht funktionieren
- **ASNs** sind Nummern für individuelle, autonome Systeme
- Wie IP-Adressen sind ASNs 32-Bit-Zahlen -> Im Gegensatz zu IP-Adressen bezeichnet man sie jedoch mit einer Dezimalstelle anstatt lesbarer Bits
- IP-Adressen müssen in der Lage sein, eine Netzwerk-ID- und Host-ID-Portion für Nummern darzustellen -> Das ist einfacher, wenn die Nummer in vier Abschnitte mit 8 Bits aufgeteilt wird, insbesondere zur Zeit der Adressklassen
- Eine ASN muss nie angepasst werden, um mehr Netzwerke oder Hosts darzustellen -> Nur die Core Internet Routing-Tabellen müssen aktualisiert werden, um die ASN zu verstehen
- **RFC 1918** definierte drei IP-Adressbereiche, die nie von Core-Routern geroutet werden
- Das bedeutet, sie gehören niemandem und können von jedem verwendet werden
- Da sie von der Art und Weise, wie sich Traffic im Internet bewegt, getrennt sind, gibt es keine Obergrenze dafür, wie viele Personen diese Adressen in einem internen Netzwerk nutzen können
- Die drei grundlegenden Bereiche für nicht-routbaren Adressraum sind: 10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16
- Diese Bereiche können von jedem für interne Netzwerke verwendet werden
- Es sollte erwähnt werden, dass interne Gateway-Protokolle diese Adressbereiche routen, sodass sie innerhalb des autonomen Systems verwendet werden können, aber externe Gateway-Protokolle nicht

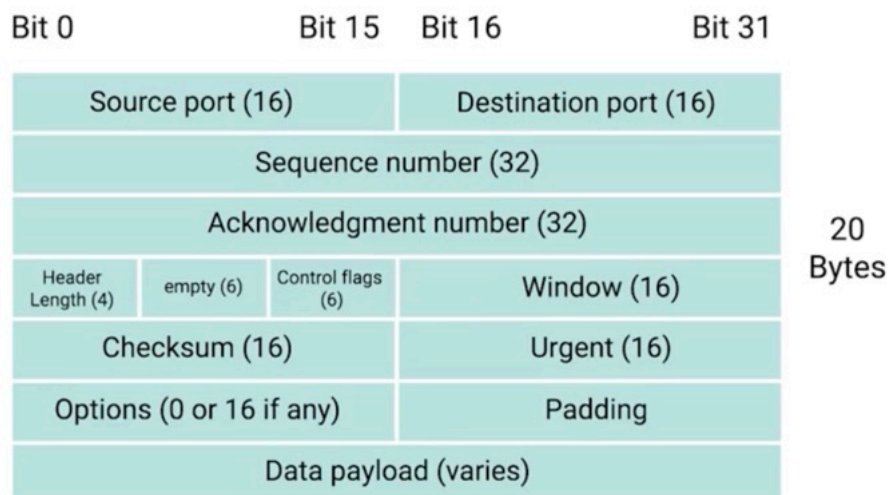
## Transportschicht

- Dank der Transportschicht kann der Traffic an spezifische Netzwerkanwendungen gesendet werden und die Anwendungsschicht ermöglicht es den Anwendungen, verständlich miteinander zu kommunizieren



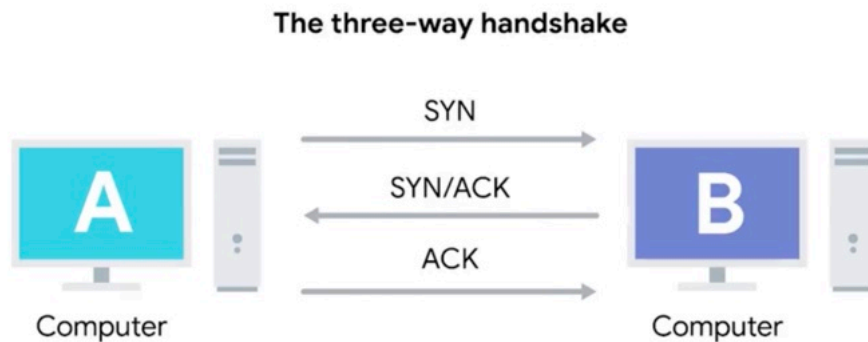
- Multiplexing in der Transportschicht bedeutet, dass die Knoten in einem Netzwerk Traffic zu zahlreichen Empfängerdiensten senden können
- Demultiplexing ist dasselbe auf der Empfängerseite
- Dabei wird Traffic für denselben Knoten genommen und an den entsprechenden Empfängerdienst geliefert
- Die Transportschicht managt das Multiplexing und Demultiplexing über Ports
- Ein **Port** ist eine 16-Bit-Zahl zum Weiterleiten von Traffic an spezifische Dienste, die auf einem vernetzten Computer laufen

## TCP-Frame




- **Quellport:** notwendig, sodass bei einer Antwort des Webserver der Computer, der die ursprüngliche Anfrage stellt, diese Daten an das anfragende Programm senden kann
- Auf diese Weise wird die Antwort bei Reaktion eines Webserver auf die Anfrage zur Ansicht einer Webseite von Ihrem Browser empfangen und nicht von Ihrem Textverarbeitungsprogramm
- **Sequenznummer:** 32-Bit-Zahl, die verwendet wird, um mitzuverfolgen, wo in einer TCP-Segmentsequenz es sich zu befinden hat
- Normalerweise ist ein Ethernet-Frame auf eine Größe von 1.518 Bytes limitiert, wir senden jedoch meist weit mehr Daten
- Auf der Transportebene teilt das TCP diese Daten in verschiedene Segmente auf
- Die Sequenznummer in einem Header wird dazu verwendet, um mitzuverfolgen, aus welchem Segment dieses bestimmte Segment stammt
- Die **Bestätigungsnummer** ist die Nummer des nächsten erwarteten Segments
- **Datenoffset-Feld:** ist eine 4-Bit-Zahl, die mitteilt, wie lang der TCP-Header für dieses Segment ist -> so weiß das Empfänger-Netzwerkgerät, wo die tatsächliche Datennutzlast beginnt
- Ein **TCP-Fenster** bezeichnet den Sequenznummernbereich, der gesendet werden kann, bevor eine Bestätigung erforderlich ist
- Das **TCP** ist ein Protokoll, das **stark auf Bestätigungen angewiesen** ist -> so wird sichergestellt, dass die gesamten erwarteten Daten empfangen werden und dass das Sendegerät keine Zeit mit dem Senden von Daten verschwendet, die nicht empfangen werden
- Urgent-Pointer-Feld wird in Verbindung mit einer der TCP-Steuerflags verwendet, um bestimmte Segmente hervorzuheben, die vielleicht wichtiger sind als andere
- Options-Felder: Manchmal wird es jedoch für kompliziertere Ablaufsteuerungsprotokolle verwendet
- **Padding-Feld** mit einer Reihe von Nullen, die dafür sorgt, dass der Datennutzlastabschnitt am entsprechenden Ort beginnt
- Als Protokoll stellt TCP Verbindungen her, mit denen lange Ketten von Datensegmenten gesendet werden können -> hebt sich von Protokollen wie IP und Ethernet ab, die einzelne Datenpakete senden
- **TCP Flags:**
  - Das zweite Flag ist **ACK**, also „acknowledged“ -> ein Wert von „1“ bedeutet, dass das Feld mit der Bestätigungsnummer geprüft werden sollte
  - Das dritte Flag ist **PSH**, kurz für „push“ -> so gibt das sendende Gerät an, dass das empfangende Gerät die aktuell zwischen- gespeicherten Daten schnellstmöglich an die Anwendung auf Empfangsseite weitergeben soll
  - Ein **Buffer** ist eine Computertechnik, bei der eine bestimmte Datenmenge an einem Ort aufbewahrt wird, bevor sie zu einem anderen Ort gesendet wird
  - Beim TCP werden so große Datenmengen effizienter versendet
  - Wenn eine bestimmte Datenmenge in einem Buffer aufbewahrt wird, kann TCP bedeutungsvollere Datenblöcke an das Programm senden, das darauf wartet -> In manchen Fällen senden Sie möglicherweise nur sehr wenige Informationen, auf die das wartende Programm sofort reagieren muss. Genau das macht das Push-Flag.
  - vierte Flag ist **RST**, kurz für „Reset“: Es bedeutet, dass eine der Seiten in einer TCP-Verbindung nach einer Reihe von fehlenden oder fehlerhaften Segmenten nicht wiederhergestellt werden konnte -> „hey, kannst du das nochmal senden“
  - Das fünfte Flag ist **SYN**, Abkürzung für „synchronize“: wird beim ersten Herstellen einer TCP-Verbindung verwendet -> damit kann der Empfänger das Feld für die Sequenznummer prüfen
  - sechste Flag, **FIN**, Abkürzung für „Finish“: Ein Wert von „1“ bedeutet, dass der sendende Computer keine weiteren Daten zum Senden hat und die Verbindung geschlossen werden kann

Mit einem **Handshake** prüfen zwei Geräte, dass sie dasselbe Protokoll haben und einander verstehen können:



- Nach dem Drei-Wege-Handshake wird die TCP-Verbindung hergestellt
- Jetzt kann Computer A alle gewünschten Daten an Computer B senden und umgekehrt
- Vier-Wege-Handshake: Der Computer, der die Verbindung schließen möchte, sendet ein FIN-Flag, was der andere Computer mit dem ACK-Flag bestätigt

### Was passiert bei TCP?

1. Dein PC (Client) sendet ein **SYN** → Will Verbindung aufbauen
2. Der Webserver (Server) antwortet mit **SYN-ACK**
3. Dein PC antwortet mit **ACK** → Verbindung steht 
4. Dein PC sendet jetzt ein **HTTP-GET-Request** (→ sagt dem Server: „Gib mir die Website!“)
5. Der Server antwortet mit den **HTML-Daten** → im Payload von TCP-Segmenten
6. Danach wird die Verbindung mit einem **4-Way-Handshake** beendet

## Socket-Zustände

- Ein Socket ist ein konkretes Software-Objekt, das einen Netzwerk-Endpoint darstellt und für eine mögliche TCP-Verbindung bereit ist
- Es ist die „praktische Umsetzung“ der Idee eines Kommunikationspunkts (IP + Port) in einem Computerprogramm
- Mit anderen Worten können Sie Traffic an jeden beliebigen Port senden, aber Sie erhalten nur eine Antwort, wenn ein Programm ein Socket auf dem Court geöffnet hat
- -> **Ein Port ist nur dann „offen“ und antwortet, wenn ein Programm aktiv einen Socket an diesem Port verwendet**
- **Ohne dieses „lauschende“ Programm bleibt der Port still, auch wenn Daten dorthin geschickt werden.**

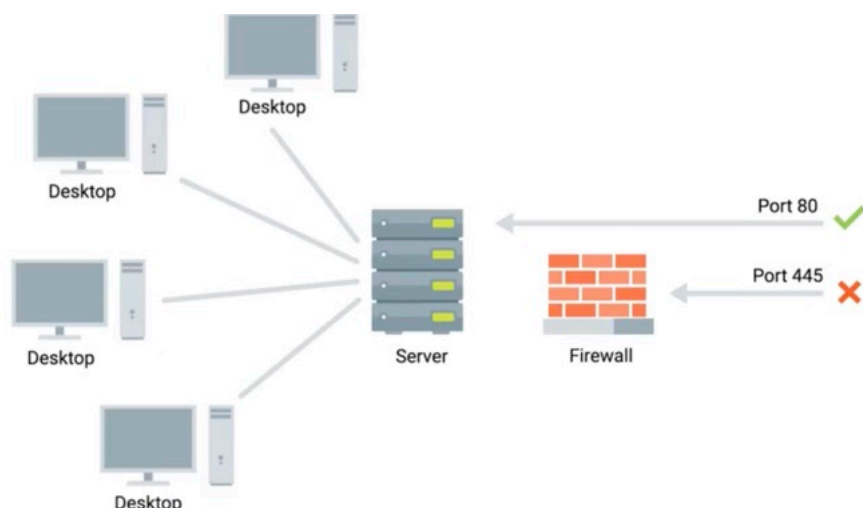


## - Zustände eines Sockets:

- LISTEN: Warten bedeutet, dass ein TCP-Socket bereit ist und auf eingehende Verbindungen wartet. Dies können Sie nur serverseitig sehen
  - SYN\_SENT bedeutet, dass eine synchrone Anfrage gesendet wurde, die Verbindung aber noch nicht hergestellt wurde. Dies können Sie nur clientseitig sehen
  - SYN\_RECEIVED bedeutet, dass ein Socket, der zuvor einen Listener-Status hatte, eine synchrone Anfrage erhalten und SYN\_ACK zurückgesendet hat. Das finale ACK vom Client wurde aber noch nicht empfangen (serverseitig)
  - ESTABLISHED bedeutet, dass die TCP-Verbindung funktioniert und beide Seiten sich gegenseitig Daten senden können -> auf Server- und Clientseite einer Verbindung
  - FIN\_WAIT gibt an, dass eine FIN gesendet wurde, aber das entsprechende ACK vom anderen Ende noch nicht eingegangen ist
  - CLOSE\_WAIT gibt an, dass die Verbindung auf der TCP-Schicht geschlossen wurde, aber dass die Anwendung, die den Socket geöffnet hat, ihren Hold für den Socket noch nicht freigegeben hat
  - CLOSED gibt an, dass die Verbindung vollständig beendet wurde und keine weitere Kommunikation möglich ist
- Als Protokoll ist TCP universell in seiner Anwendung -> jedes Gerät, das das TCP-Protokoll verwendet, muss dies genau gleich machen, damit die Kommunikation erfolgreich ist
  - die Beschreibung des Socket-Status auf Betriebssystemebene ist jedoch nicht ganz so universell
  - TCP = verbindungsorientiertes Protokoll: Bei diesem Protokoll wird eine Verbindung für eine korrekte Datenübertragung hergestellt
  - jedes gesendete Datensegment wird bestätigt -> sicher und zuverlässig
  - Wenn die Prüfsumme auf IP- oder Ethernet- Ebene nichts berechnet, werden diese Daten einfach verworfen -> das TCP entscheidet, wann diese Dateien noch einmal gesendet werden
  - Demgegenüber stehen verbindungslose Protokolle -> **UDP**
  - **UDP** sendet Segmente, ohne dass diese überprüft werden -> z.B. bei Videostreaming, damit nicht jedes Frame bestätigt werden muss

## Firewalls

- Firewalls funktionieren an vielen verschiedenen Ebenen im Netzwerk: es gibt Firewalls, die Traffic auf Anwendungsebene prüfen können, und Firewalls, die hauptsächlich IP-Adressbereiche sperren
- am häufigsten aber in der Transportschicht
- Diese Firewalls haben im Allgemeinen eine Konfiguration, mit der sie Traffic an bestimmte Ports verhindern, und Traffic an andere Ports zulassen





## Anwendungsebene

- Auf der Anwendungsschicht kommen zahlreiche Protokolle mit unterschiedlichen Funktionen zum Einsatz
- Webbrowser = Client und Webserver = Server
- am häufigsten genutzten Webserver sind **Microsoft IIS, Apache und NGINX**, die allerdings ebenfalls an das gleiche Protokoll gebunden sind
- So wird sichergestellt, dass unabhängig vom Browser mit jedem Server kommuniziert werden kann
- Für Webtraffic wird in der Anwendungsschicht das **HTTP-Protokoll** verwendet

## Zusammenarbeit der unterschiedlichen Schichten

### Computer 1:

- Erstellt einen **TCP-Segment** (für Port 80, z. B. mit SYN-Flag).
- Verpackt dieses in ein **IP-Paket** (mit Quell- und Ziel-IP).
- Verpackt das IP-Paket in ein **Ethernet-Frame** (mit Quell- und Ziel-MAC).
- Schickt das Ethernet-Frame an **Router A** (sein Gateway).

### Router A:

- Entfernt den alten **Ethernet-Frame**.
- Prüft das IP-Paket und erkennt, dass es weitergeleitet werden muss.
- Reduziert den TTL-Wert um 1 und berechnet eine neue Prüfsumme.
- Verpackt das IP-Paket in ein **neues Ethernet-Frame** (MAC-Adresse: Router B).
- Leitet es gemäß seiner **Routing-Tabelle** an **Router B** weiter.

### Router B:

- Entfernt ebenfalls den Ethernet-Frame.
- Erkennt, dass die Ziel-IP (**172.16.1.100**) in seinem eigenen Netzwerk liegt.
- Reduziert TTL wieder um 1, neue Prüfsumme.
- Verpackt das IP-Paket in ein neues Ethernet-Frame (MAC: Computer 2).
- Leitet es an **Computer 2** weiter.

### Computer 2:

- Entpackt das Ethernet-Frame und prüft die MAC-Adresse.
- Prüft das IP-Paket (Ziel-IP passt, Prüfsumme ok).

- Entpackt das TCP-Segment, prüft Port 80.
- Übergibt es an den Webserver (z. B. Apache), der auf Port 80 lauscht.
- Speichert die Sequenznummer (für den Verbindungsaufbau: SYN, SYN-ACK, ACK).

## Wichtig:

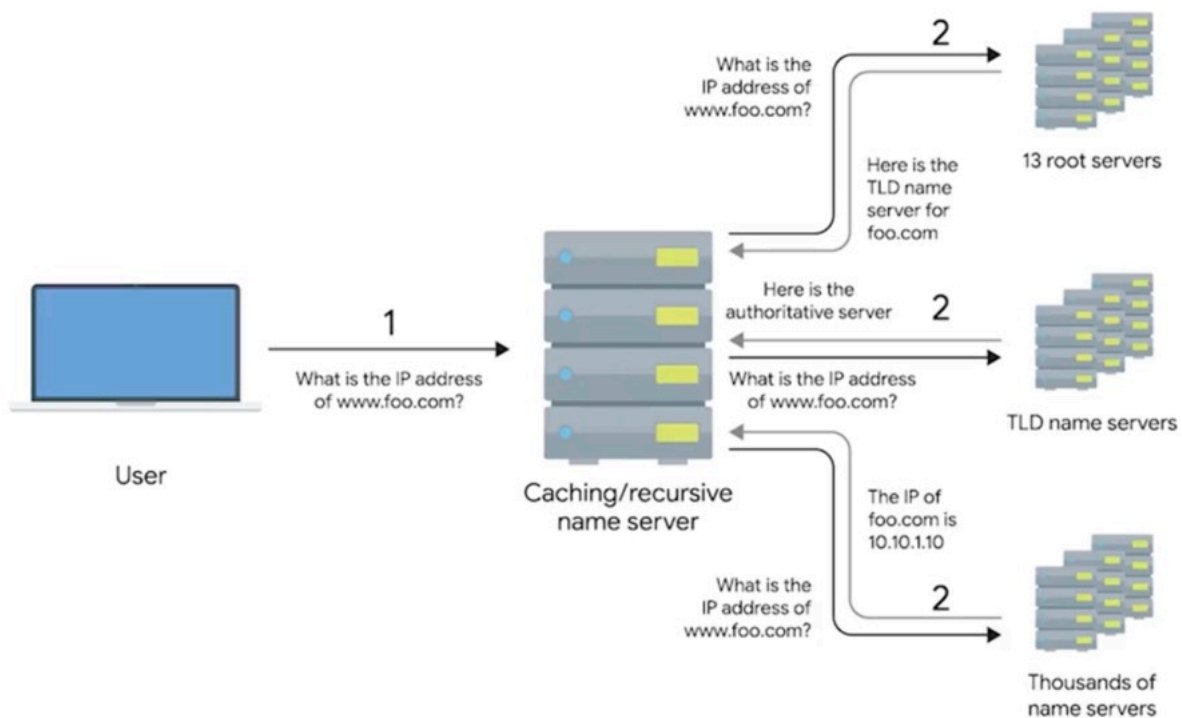
- Jeder **Router erstellt ein neues Ethernet-Frame** mit neuen MAC-Adressen (bei jedem „Hop“)
- Das **IP-Paket bleibt fast gleich**, außer TTL und Prüfsumme.
- Nur der **Zielcomputer entfernt die TCP-Kapselung**, da er als Empfänger vorgesehen ist.

Kurs 2, Modul 4

## Wofür brauchen wir DNS?

- DNS ist ein globaler und weit verbreiteter Netzwerkdienst, der Zeichenfolgen in IP-Adressen aufschlüsselt
- Ein Domainname ist lediglich der Begriff, für etwas, das über DNS aufgelöst werden kann
- DNS macht es Nutzern nicht nur leichter, sich eine Website zu merken, es ermöglicht ebenfalls administrative Änderungen hinter den Kulissen, ohne dass der Endnutzer sein Verhalten anpassen muss
- Aufgrund der globalen Struktur von DNS können Organisationen entscheiden, in welcher Region der Welt der Domainname zu welcher IP aufgelöst wird
- eine der wichtigsten Technologien, die Sie als IT-Supportmitarbeiter kennen sollten, um effektiv Netzwerkprobleme beheben zu können
- Dieser Prozess, bei dem über DNS ein Domainname in eine IP-Adresse umgewandelt wird, ist als **Namensauflösung (name resolution)** bekannt
- standardmäßige Netzwerkkonfiguration:
  - IP address
  - Subnet mask
  - Gateway for a host
  - DNS server
- Es gibt fünf Haupttypen von DNS-Servern:
  - **Caching-Nameserver**
  - **rekursive Nameserver**
  - **Root-Nameserver**
  - **TLD-Nameserver**
  - **autoritative Nameserver**
- ein einzelner DNS-Server kann viele dieser Funktionen gleichzeitig erfüllen kann
- **Caching- und rekursive Nameserver:** werden in der Regel von einem ISP oder dem lokalen Netzwerk bereitgestellt
- Sie haben die Aufgabe, Domainnamen-Lookups für eine bestimmte Zeit zu speichern
- es müssen zahlreiche Schritte ausgeführt werden, um einen Domainnamen vollständig qualifiziert aufzulösen -> um zu verhindern, dass dies bei jedem neuen TCP-Verbindungsaufbau geschieht, hat Ihr ISP oder Ihr lokales Netzwerk in der Regel einen Caching-Nameserver
- Die meisten Caching-Nameserver sind gleichzeitig rekursive Nameserver
- Rekursive Nameserver führen vollständige DNS-Auflösungsanfragen aus
- Alle Domainnamen im globalen DNS-System haben eine TTL (Time to Live)

- Vorgang bei rekursiver Auflösung:
- Der erste Schritt ist immer die Kontaktaufnahme mit einem Root-Nameserver
- Insgesamt gibt es 13 Root-Nameserver, die für die Weiterleitung von Anfragen an den entsprechenden TLD-Nameserver zuständig sind
- inzwischen sind sie meistens mittels Anycast über den ganzen Globus verteilt
- Dies ist ein Verfahren, mit dem der Traffic an verschiedene Ziele weitergeleitet wird, abhängig von Faktoren wie Standort, Überlastung oder Link-Zustand
- Root-Server: 13 Instanzen, die Root-Nameserver-Lookups als Dienstleistung anbieten
- die Root-Server antworten auf einen DNS-Lookup mit dem TLD-Nameserver, der abgefragt werden soll
- TLD steht für Top-Level-Domain und entspricht der obersten Ebene des hierarchischen DNS-Namensauflösungssystems
- Eine TLD ist der letzte Teil eines Domainnamens (z.B. „com“)
- Für jede existierende TLD gibt es einen TLD-Nameserver
- Doch ähnlich wie bei Root-Servern bedeutet dies nicht, dass es physisch nur einen dieser Server gibt -> höchstwahrscheinlich handelt es sich um eine globale Verteilung von Anycast-Servern, die für die einzelnen TLDs zuständig sind
- DNS ist ein gutes Beispiel für einen Dienst der Anwendungsschicht, der für die Transportschicht UDP anstelle von TCP verwendet
- In der Regel passen eine einzelne DNS-Anfrage und die Antwort in ein einziges UDP-Datagramm



- Der DNS-Resolver fragt einfach noch einmal nach, wenn er keine Antwort erhält

## Ressourceneintragstypen

- am häufigsten: **A-Eintrag (a record)** -> verknüpft bestimmte Domainnamen mit bestimmten IPv4-Adressen
- In seiner einfachsten Form ist ein einzelner A-Eintrag für einen einzigen Domainnamen konfiguriert
- Aber ein Domainname kann auch mehrere A-Einträge haben -> Lastverteilung per DNS (**round robin**)
- Bei der Lastverteilung wird eine Liste der Reihe nach durchgegangen, um damit den Traffic gleichmäßig auf die Listeneinträge zu verteilen
- **Quad A record**: -> IPv6-Adresse
- **CNAME record** -> ist auch sehr verbreitet -> leitet den Traffic von einer Domain zur anderen
- Richtet man einen CNAME ein, der von microsoft.com auf www.microsoft.com leitet, muss nur der A-Eintrag für www.microsoft.com geändert werden -> So erhalten Clients bei der Nachfrage nach beiden Domains die neue IP-Adresse
- **Mail exchange (MX)**: wird verwendet, um E-Mails an den richtigen Server zu senden
- Viele Firmen lassen ihre Webpräsenz und Mailserver auf unterschiedlichen Computern mit verschiedenen IPs laufen
- -> Darum wird der MX-Eintrag genutzt, um sicherzustellen, dass E-Mails an den Mailserver der Firma gehen, während andere Anfragen, wie Datenverkehr, zum Webserver gehen
- **SRV-Eintrag**: SRV steht für Service Record, Service-Eintrag, Er wird verwendet, um zu definieren, wo bestimmte Services zu finden sind
- **TXT-Einträge** oft verwendet, um zusätzliche Informationen für Email-as-a-service-Anbieter zu übermitteln

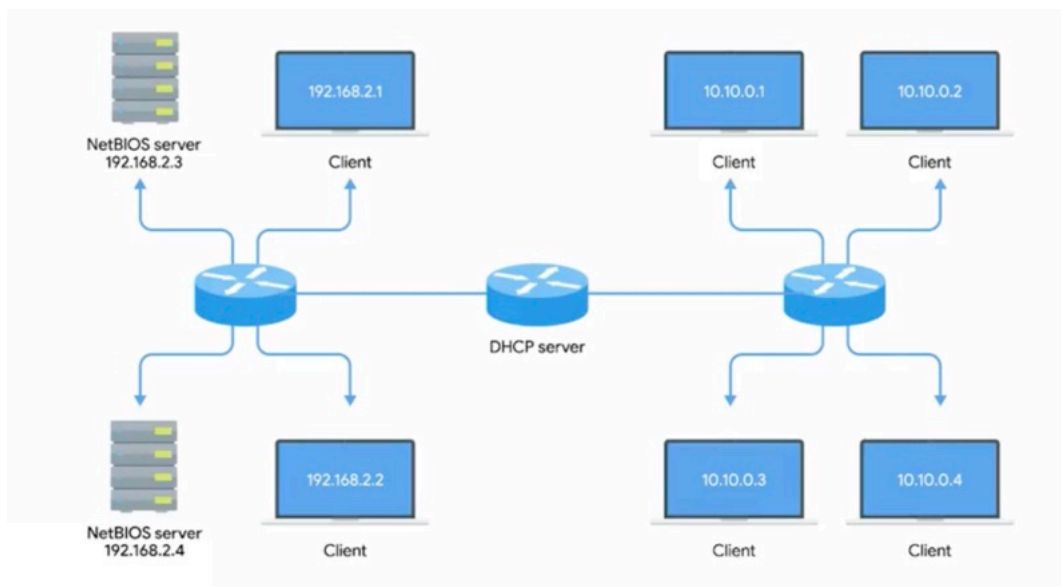
Typ	Zweck	Beispiel
A	Domain → IPv4-Adresse	example.com → 93.184.216.34
AAAA	Domain → IPv6-Adresse	example.com → 2001:db8::1
CNAME	Alias einer Domain zu anderer	blog.example.com → <a href="http://www.example.com">www.example.com</a>
MX	E-Mail-Zustellung	MX für example.com → mail.example.com
SRV	Dienst + Port angeben	_sip._tcp.example.com → voip.example.com:5060
TXT	Zusatzinfos (z. B. SPF, DKIM)	v=spf1 include:_spf.example.com ~all

## DNS-Zonen

- DNS-Zonen gibt es, um die Ebenen einer Domain besser managen zu können
- z.B. Firma in 3 unterschiedlichen Ländern mit je 200 Mitarbeitern -> braucht keine 600 A records sondern 4 autoritative Nameserver: einen für die main Domain und 3 für die Subdomains
- SOA-Eintrag gibt die Zone und den Namen des für die Zone zuständigen Nameservers an

# Einstieg in DHCP

- Auf jedem einzelnen Computer in einem modernen TCP/IP-basierten Netzwerk müssen jeweils mindestens vier Dinge speziell konfiguriert werden:
  - IP-Adresse
  - Subnetzmaske des lokalen Netzwerks
  - Standard-Gateway
  - Nameserver
- nur die IP-Adresse ist auf jedem Netzwerk-Knoten unterschiedlich
- **DHCP** (Dynamic Host Configuration) ist ein **Protokoll der Anwendungsschicht, das den Konfigurationsprozess von Hosts in einem Netzwerk automatisiert**
- Mit DHCP kann ein Computer eine Anfrage an einen DHCP-Server senden, wenn er sich mit dem Netzwerk verbindet, und die gesamte Netzwerkkonfiguration auf einmal erhalten
- DHCP erleichtert nicht nur die Arbeit beim Konfigurieren mehrerer Geräte in einem Netzwerk, sondern übernimmt auch die Aufgabe, jedem Rechner eine eigene IP zuzuordnen
- Jeder Computer in einem Netzwerk muss eine IP-Adresse haben, um kommunizieren zu können, aber kaum einer braucht eine allgemein bekannte IP
- Lediglich Server oder Netzwerkgeräte wie der Gateway-Router müssen eine statische und allgemein bekannte IP-Adresse haben



- Bei der **dynamischen Zuordnung** kann sich die IP eines Computers fast jedes Mal ändern, wenn dieser sich mit dem Netzwerk verbindet
- automatische Zuordnung: Unterschied -> hier soll der DHCP-Server speichern, welche IPs er welchen Geräten in der Vergangenheit zugewiesen hat
- Bei der **festen Zuordnung** wird eine manuelle Liste mit MAC-Adressen und den dazugehörigen IPs erstellt
- -> Das kann als **Sicherheitsmaßnahme** genutzt werden, denn es stellt sicher, dass nur Geräte mit MAC-Adressen, die für diesen bestimmten DHCP-Server konfiguriert sind, eine IP bekommen und im Netzwerk kommunizieren können
- Zusätzlich zur Vergabe von IP-Adressen und Standard-Gateways kann man DHCP auch nutzen, um zum Beispiel NTP-Server zu konfigurieren
- **NTP** steht für „Network Time Protocol“ und synchronisiert die Uhrzeit aller Computer in einem Netzwerk
- Wenn ein Client, der für die Nutzung von DHCP konfiguriert ist, nach den Spezifikationen für die Netzwerkkonfiguration fragt, heißt das **DHCP-Erkennung**

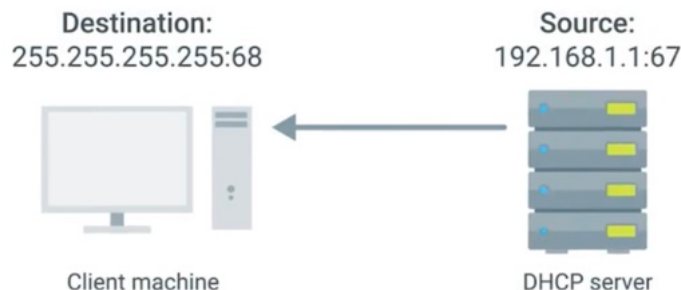
## DHCP-Lease

- 1. **Server-Erkennung:** Der DHCP-Client sendet eine Nachricht ans Netzwerk, die DHCP-Erkennungsnachricht genannt wird. Da der Computer noch keine IP zugewiesen bekommen hat und die IP des DHCP-Servers nicht kennt, erzeugt er eine extra erstellte Broadcast-Nachricht
- DHCP empfängt über UDP-Port 67 und DHCP-Erkennungsnachrichten werden immer über UDP-Port 68 gesendet

### DHCPDISCOVER



### DHCPOFFER



- **2.: DHCP-Angebot:** Als Nächstes geht der DHCP-Server seine eigene Konfiguration durch und entscheidet, ob und welche IP-Adresse er dem Client gibt. Das hängt davon ab, ob er für dynamische, automatische oder feste Zuordnung konfiguriert ist -> Antwort = DHCP-Angebot
- Broadcast Angebot wird vom richtigen Client erkannt, denn: Das DHCP-Angebot hat ein Feld, in dem die **MAC-Adresse dieses Clients** eingetragen ist -> Der Client verarbeitet das DHCP-Angebot dann, um herauszufinden, welche IP ihm angeboten wurde
- Meistens antwortet der DHCP-Client auf ein DHCP-Angebot mit einer:
- **3. DHCP-Anfrage**
- Diese Nachricht besagt im Grunde genommen: „Ja, ich möchte die IP haben, die du mir angeboten hast.“
- Da die IP noch nicht zugewiesen wurde, wird sie wieder von der IP 0.0.0.0 gesendet, und an die Broadcast-IP 255.255.255.255
- Der DHCP-Server empfängt die DHCP-Anfrage und antwortet darauf mit einer **DHCPACK**, einer: **4. DHCP-Empfangsbestätigung**
- Diese Nachricht wird auch wieder an die Broadcast-IP 255.255.255.255 und mit der tatsächlichen IP des DHCP-Servers als Quelle gesendet

- Der DHCP-Client erkennt wieder, dass die Nachricht an ihn gerichtet ist, weil seine MAC-Adresse in einem der Nachrichtfelder steht
- Der Protokollstapel des Client-Computers kann diese Konfigurationsdaten vom DHCP-Server nun nutzen, um seine eigene Konfiguration der Netzwerkschicht zu erstellen
- -> jetzt sollte der Computer, der als DHCP-Client dient, alle Informationen haben, die er braucht, um vollständig im Netzwerk agieren zu können.

## Die grundlegenden Prinzipien von NAT

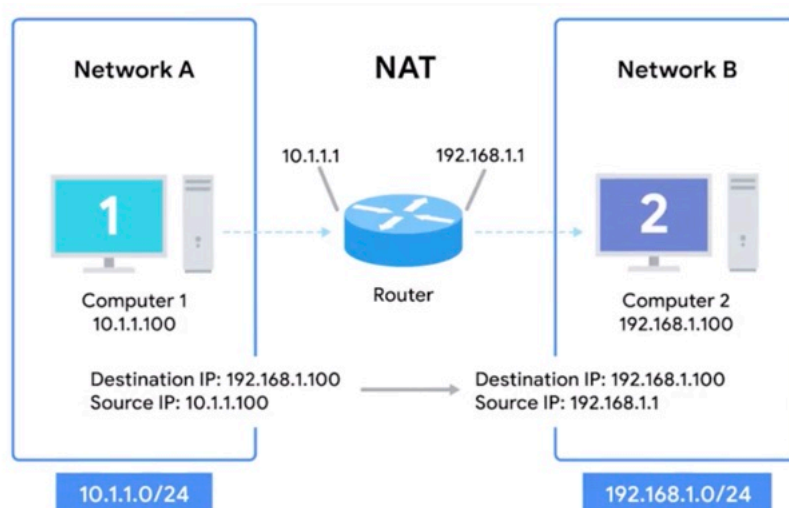
- Im Gegensatz zu Protokollen wie DNS und DHCP ist **Netzwerkadressübersetzung**, oder **NAT**, eine Methode und kein festgelegter Standard
- NAT nimmt eine IP-Adresse und übersetzt sie in eine andere
- NAT bietet die Möglichkeit, dass ein Gateway, meistens ein Router oder eine Firewall, die Quell-

### Beispiel zur Veranschaulichung:

Schritt	Aktion
1	Dein Laptop ( 192.168.1.10 ) will auf google.com zugreifen
2	Der Router ersetzt die Quell-IP mit seiner öffentlichen IP ( 93.184.216.34 )
3	Google antwortet an 93.184.216.34
4	Der Router sieht in seiner NAT-Tabelle nach, wer das ursprünglich angefragt hat
5	Der Router sendet die Antwort an 192.168.1.10 weiter

IP eines ausgehenden IP-Datagramms umschreibt und gleichzeitig die ursprüngliche IP zurückhält, um sie später wiederherzustellen

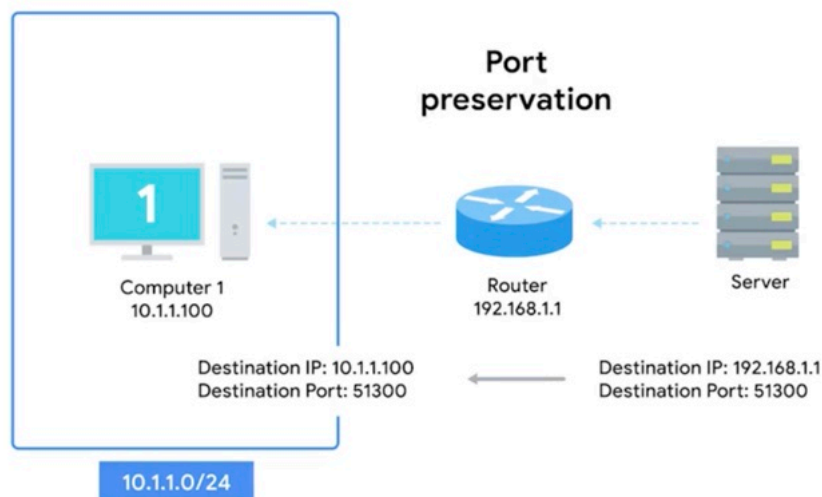
- NAT sorgt dafür, dass mehrere Geräte mit privaten IPs über eine gemeinsame öffentliche IP ins Internet gehen können -> dabei „versteckt“ es die internen IPs nach außen und ersetzt sie bei Bedarf wieder
- Normalerweise untersucht der Router den Inhalt des IP-Datagramms, verringert die TTL um eins, berechnet die Prüfsumme neu und versendet den Rest der Daten auf der Netzwerkschicht, ohne sie zu bearbeiten



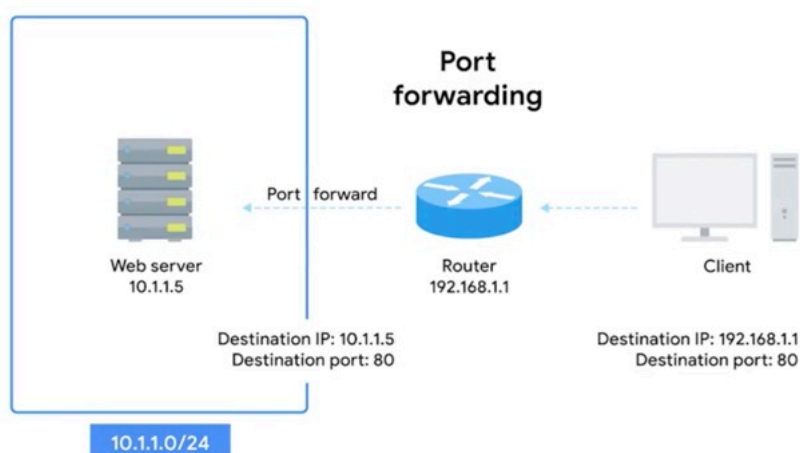
- Wenn aber NAT konfiguriert ist, schreibt der Router auch die Quell-IP um und ersetzt sie in diesem Fall mit der IP des Routers in Netzwerk B: 192.168.1.1
- bei einer Antwort fügt der Router wieder die richtige Quell IP ein
- In diesem Beispiel hält NAT die IP von Computer 1 vor Computer 2 geheim
- -> **IP-Masquerading** -> Sicherheitskonzept
- Außerhalb von Netzwerk A ist dessen gesamter Adressraum unsichtbar und vor Eingriffen geschützt -> diese Methode heißt "1:n NAT"

## NAT und die Transportschicht

- Es kann sein, dass hunderte von Antworten an dieselbe IP-Adresse gehen, und der Router mit dieser IP dann herausfinden muss, welche Antworten an welche Computer geleitet werden sollen
- -> das geht am besten mit **Port Preservation** -> eine Methode, bei der der Quellport, den ein Client wählt, der gleiche ist, den der Router benutzt

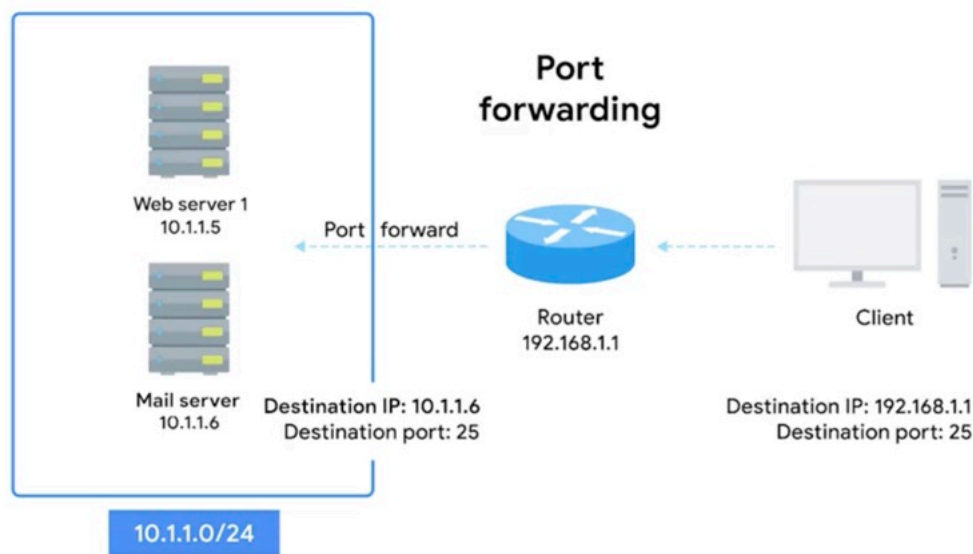


- Denken Sie daran, dass ausgehende Verbindungen einen Quellport zufällig aus den kurzlebigen Ports oder den Ports im Wertebereich 49.152 bis 65.535 auswählen
- Wenn die ausgehende Kommunikation beim Router ankommt, führt dieser eine Netzwerkadressübersetzung (NAT) durch und schreibt seine eigene IP in das Feld für die Senderadresse im IP-Datagramm
- Er lässt aber den Quellport im TCP-Datagramm stehen und speichert diese Daten in einer internen Tabelle ab
- Wenn die Kommunikation nun an Port 51.300 des Routers zurückgeht, weiß der Router, dass er an die IP 10.1.1.100 weiterleiten muss
- Ein weiteres wichtiges Konzept im Zusammenhang mit NAT und der Transportschicht ist die **Portweiterleitung**





- dabei können bestimmte Zielports so konfiguriert werden, dass sie immer zu bestimmten Knoten geleitet werden -> mit dieser Methode kann man ein vollständiges IP-Masquerading durchführen und trotzdem eingehende Anfragen beantworten
- Browser, die auf den Server zugreifen wollen, müssen nur die externe IP des Routers kennen, zum Beispiel 192.168.1.1. -> jede Kommunikation, die bei Port 80 der IP 192.168.1.1 ankommt, wird automatisch zur IP 10.1.1.5 weitergeleitet
- Die Quell-IP aller ausgehenden Antworten wird dann so umgeschrieben, dass sie der externen IP des Routers entspricht
- Stellen wir uns eine Firma vor, die einen Webserver und einen Mailserver betreibt:
  - beide Server müssen von außerhalb der Firma erreichbar sein, laufen aber auf zwei verschiedenen Servern mit unterschiedlichen IPs
  - Wir nehmen wieder an, dass der Webserver die IP 10.1.1.5 hat und der Mailserver die IP 10.1.1.6.
  - Wird die Portweiterleitung genutzt, kann die eingehende Kommunikation für beide



Dienste an **dieselbe externe IP und damit denselben DNS-Namen** gesendet werden, würde aber an komplett verschiedene interne Server gehen, weil sie jeweils an **unterschiedlichen Zielports** anliegen

## Virtuelle private Netzwerke (VPN)

- Für Firmen gibt es viele Gründe, ihr **Netzwerk sichern** zu wollen -> sie machen das mit Hilfe einiger der Technologien, die wir besprochen haben: **Firewalls, NAT, nicht routbare Adressräume** und so weiter
- Virtuelle private Netzwerke, kurz VPNs, sind eine Technologie, die es ermöglicht, ein privates oder lokales Netzwerk mit einem Host zu verbinden, der nicht im selben Netzwerk operiert
- VPNs sind Tunneling-Protokolle



- Die Angestellten im Homeoffice könnten einen VPN-Client nutzen, um einen VPN-Tunnel zum Netzwerk ihrer Firma herzustellen -> so erhält der Computer etwas, das man **virtuelle Schnittstelle** nennt, mit einer IP, die mit dem Adressraum des Netzwerkes übereinstimmt, mit dem sich der Computer über VPN verbunden hat
- indem der Computer über die virtuelle Schnittstelle Daten sendet, kann er auf die internen Inhalte des privaten Netzwerkes zugreifen, so als ob er direkt mit ihm verbunden wäre

## ◆ 1. Verpacken innerhalb der Verpackung

Stell dir vor, du willst ein Paket (Daten) ins Internet schicken.

- Normalerweise: Dein Gerät sendet ein normales Datenpaket (mit IP, Port, Nutzdaten, usw.).
- Mit VPN: Dieses Paket wird **komplett eingepackt in ein neues Paket** – so wie bei einer Matroschka-Puppe.
  - Es wird **verschlüsselt**.
  - Das neue, äußere Paket enthält nur die Infos, wie es zum VPN-Server kommt.

### 📌 Fachlich ausgedrückt:

- Das ursprüngliche Paket (mit Netzwerk-, Transport- und Anwendungsschicht) wird **in den Nutzdaten eines neuen Pakets versteckt**.
- Diese **inneren Schichten** sind verschlüsselt.
- Das äußere Paket hat die Infos, um es durch das Internet **bis zum VPN-Server** zu bringen.

## ◆ 2. Ankunft am VPN-Server (Tunnel-Endpunkt)

Sobald das Paket den **VPN-Server** erreicht:

- Der VPN-Server **entschlüsselt** es.
- Das äußere VPN-Paket wird **entfernt (verworfen)**.
- Jetzt kommt das **ursprüngliche innere Paket** zum Vorschein (mit IP-Adresse, Zielport, Webadresse etc.).
- Der VPN-Server tut so, als wäre **er selbst der Absender** – und schickt das ursprüngliche Paket ins Internet weiter.

- Es ist wichtig zu wissen, dass VPN, genauso wie NAT, ein allgemeines technologisches Konzept ist und kein genau festgelegtes Protokoll
- Es gibt viele individuelle Anwendungsmöglichkeiten von VPN, und die jeweiligen Details können sehr unterschiedlich sein
- Das Wichtigste hier ist: **VPNs sind eine Technologie, die Tunnel herstellt und es ermöglicht, dass Computer oder Netzwerke sich so verhalten, als wären sie Teil eines Netzwerkes, mit dem sie nicht physisch verbunden sind**

## Proxy-Dienste

- Proxys befinden sich zwischen Clients und anderen Servern und sie bieten zusätzliche Vorteile:
  - Anonymität
  - Sicherheit
  - Filterung von Inhalten
  - eine verbesserte Leistung
  - und vieles mehr
- Das Konzept eines Proxys ist ein Konzept oder eine Abstraktion
- -> es bezieht sich nicht auf eine bestimmte Implementierung -> es gibt Proxys auf nahezu jeder Stufe unseres Netzwerkmodells
- Webproxys werden heute eher dafür eingesetzt, um den Zugriff auf Websites wie Twitter komplett zu unterbinden
- ein Unternehmen kann entscheiden, dass der Zugriff auf Twitter die Arbeitsproduktivität senkt -> verwendet man einen Webproxy, kann man jeden Webtraffic darüber lenken
- der Proxy kann die angeforderten Daten prüfen und die Anfrage zulassen oder blockieren, je nachdem, welche Webseite angefordert wird
- **Reverse-Proxy** (z.B. bei Websites mit sehr viel Datenverkehr):



- es wirkt als wären alle mit einem Server (z.B. der von Twitter) verbunden
- aber durch den großen Datenverkehr braucht es sehr viele Server
- -> der Reverse Proxy dient hier für das Front-End und kommuniziert aber mit freien Servern
- -> verteilt eingehende Anfragen an viele physische Server
- Dies dient zum Load Balancing wie beim DNS-Verfahren „Round Robin“
- Populäre Websites nutzen Reverse-Proxys auch oft zur Entschlüsselung
- Mehr als die Hälfte des Webtraffics ist heute verschlüsselt
- Das Ver- und Entschlüsseln von Daten kann jedoch sehr aufwändig sein
- Reverse-Proxys werden heute implementiert, um spezielle Verschlüsselungs- hardware einzusetzen
- Diese übernimmt dann die Ver- und Entschlüsselung -> die Server im Hintergrund dienen dann nur der Lieferung der Inhalte

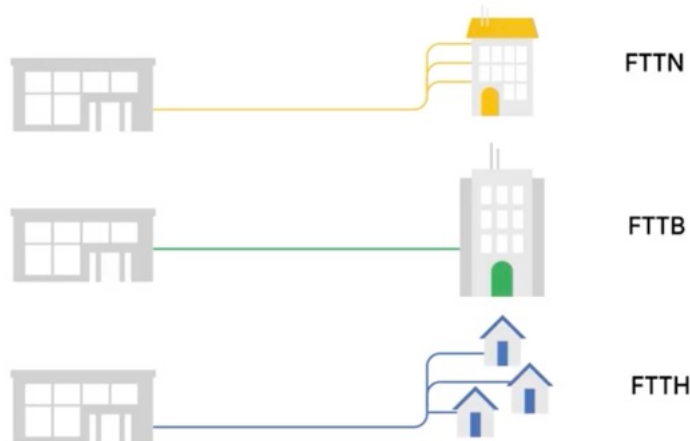
## Digital Subscriber Lines (DSL) und Breitbandkabel

- Es zeigte sich, dass Twisted-Pair-Kupfer wie in modernen Telefonleitungen viel mehr Daten übertragen kann als die Sprachtelefonie benötigt
- Über einen Frequenzbereich, der reguläre Telefonie nicht störte, konnte eine Technologie namens Digital Subscriber Line oder DSL viel mehr Daten übertragen als gewöhnliche Einwahltechnologien
- DSLAMs, Digital Subscriber Line Access Multiplexers -> genau wie Einwahlmodems stellen diese Geräte Datenverbindungen über Telefonleitungen her
- Anders als Einwahlverbindungen sind sie jedoch fortdauernd
- Das bedeutet, die Verbindung wird beim Einschalten des DSLAMs hergestellt und nicht unterbrochen, bis das DSLAM ausgeschaltet wird

- ADSL: Download schneller als Upload (die meisten Nutzer sind Clients, deshalb kostengünstiger und sinnvoller für üblichen Gebrauch)
- SDSL: Download und Upload gleich schnell
- es existieren noch viel mehr DSL-Varianten
- Ähnlich wie bei der Entwicklung von DSL stellten Kabelunternehmen schnell fest, dass die Koaxialkabel, mit denen Kabelfernsehen in die Häuser gebracht wird, viel mehr Daten übertragen können, als für das Fernsehen nötig ist
- Auf Frequenzen, die Fernsehübertragungen nicht stören, konnten kabelbasierte Technologien Internetzugang mit hoher Geschwindigkeit über dieselben Leitungen bereitstellen -> Breitband
- Heute versuchen die meisten Betreiber, ihre Netzwerke so weit zu aktualisieren, dass Endnutzer die geteilte Bandbreite nicht immer bemerken
- Es kommt jedoch immer noch häufig vor, dass Kabelinternet zu Zeiten besonders starker Nutzung langsamer wird, also wenn im selben Gebiet viele Menschen gleichzeitig Internet nutzen
- Cable Modem Termination System oder CMTS -> verbindet die vielen verschiedenen Kabelverbindungen mit dem Kernnetzwerk eines Internetanbieters

## Glasfaser

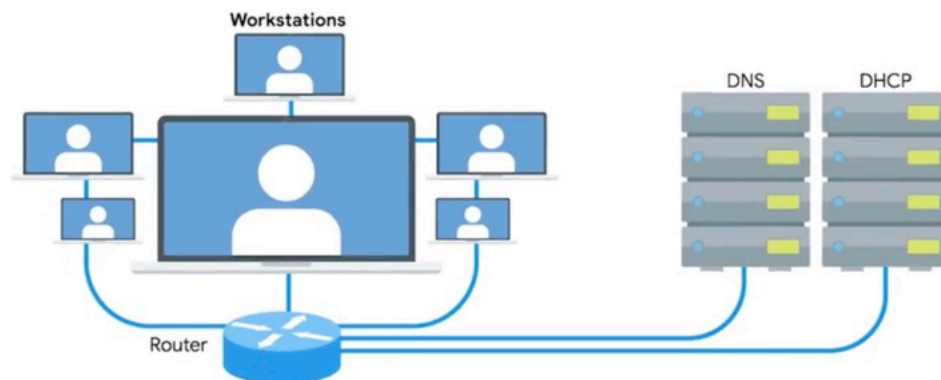
- Der Kern des Internets besteht seit Langem aus Glasfaser, wegen der Geschwindigkeit und weil Glasfaser viel weitere Übertragungen ohne Signalverschlechterung ermöglicht
- Übertragung mit Licht statt mit elektrischen Strömen



- FTTH und FTTB werden gemeinsam auch als FTTP bezeichnet, Fiber to the Premises – Glasfaser bis zum Grundstück
- Statt einem Modem ist der Abschlusspunkt Linientechnik für Glasfasertechnologien ein optischer Netzwerkabschluss oder **ONT** -> Der ONT wandelt Daten aus Protokollen, die das Glasfasernetzwerk verstehen kann, in Daten um, die Netzwerke mit Twisted-Pair-Kupferkabeln verstehen können

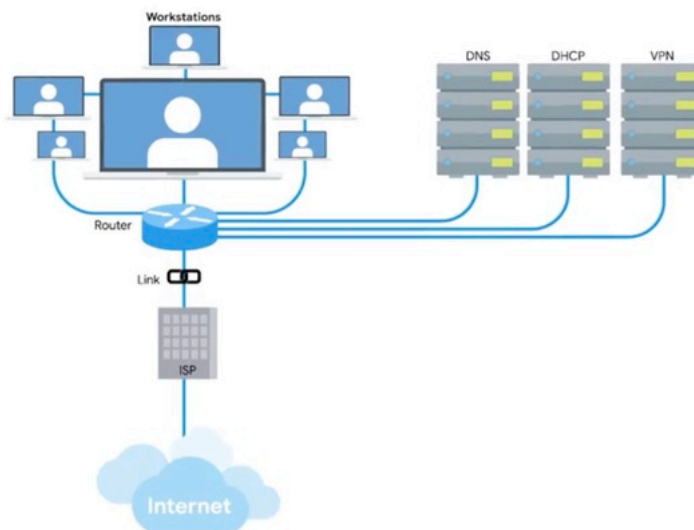
## Wide Area Network

- Beispiel kleines Unternehmen:



- Sie verwenden nicht routbaren Adressraum für die internen IPs, da IP-Adressen rar und teuer sind
- Sie richten einen Router für NAT ein
- Sie konfigurieren einen lokalen DNS-Server und einen DHCP-Server, um die Netzwerkkonfiguration zu erleichtern
- Und natürlich schließen Sie einen Vertrag mit einem Internetanbieter ab, damit das Büro eine Internetverbindung erhält und die Nutzer Internetzugriff haben

das Unternehmen wächst:



- Sie verwenden nicht routbaren Adressraum für die internen IPs, dort gibt es also genug Raum für Wachstum
- Vielleicht benötigen Vertriebsmitarbeiter unterwegs Ressourcen aus dem LAN -> Sie richten also einen VPN-Server ein und machen den VPN-Server mit Portweiterleitung zugänglich
- Jetzt können sich Mitarbeiter weltweit mit dem Büro-LAN verbinden

Das Unternehmen wächst noch weiter:

- Der CEO eröffnet ein neues Büro in einem anderen Teil des Landes
- Jetzt benötigt statt einiger Vertriebsmitarbeiter ein ganzes zweites Büro Fernzugriff auf Ihr Netzwerk
- Hier kommen **Wide Area Networks oder WAN-Technologien** ins Spiel
- Anders als ein LAN oder Local Area Network steht WAN für Wide Area Network
- Ein Wide Area Network wirkt wie ein einzelnes Netzwerk, erstreckt sich aber über mehrere Standorte
- Es ist in der Regel ein Internet-Link über den Internetanbieter nötig
- Der Anbieter sendet die Daten von einem Standort zum anderen
- Das WAN funktioniert, als wären alle Computer am selben Standort
- Stellen Sie sich ein Computernetzwerk auf einer Seite des Landes vor und ein weiteres auf der anderen: Jedes Netzwerk endet an einem Abschlusspunkt Linientechnik, an dem das Netzwerk des Internetanbieters übernimmt
- Der Bereich zwischen jedem Abschlusspunkt Linientechnik und dem Kernnetzwerk des Internetanbieters heißt Teilnehmeranschlussleitung
- Die Teilnehmeranschlussleitung könnte eine T-Carrier-Leitung oder eine Glasfaserverbindung zum Standort des Anbieters sein
- Hier befindet sich dann die Verbindung zum Anbieternetzwerk und dem gesamten Internet
- WANs verwenden Protokolle in der Sicherungsschicht, um Daten zwischen Standorten zu übertragen
- Dieselben Protokolle werden manchmal im Kern des Internets selbst eingesetzt statt dem uns bekannteren Ethernet
- Softwaredefiniertes WAN (SD-WAN): Software, die entwickelt wurde, um die individuellen Anforderungen cloudbasierter WAN-Umgebungen zu erfüllen -> günstiger
- Eine beliebte Alternative zu WAN-Technologien sind Point-to-Point-VPNs

## Cloud:

- Cloud: Für den Moment ist nur wichtig, dass Unternehmen ihre Infrastruktur mit der Cloud durch andere Unternehmen verwalten lassen können
- Nehmen wir E-Mails als Beispiel. Früher mussten Unternehmen eigene E-Mail-Server betreiben, wenn sie eine E-Mail-Präsenz wünschten
- Jetzt können sie einen E-Mail-Server von einem Anbieter für Cloud-Hosting hosten lassen
- Mit dieser Art Cloud-Lösung sind oft keine extrem schnellen Verbindungen zwischen Firmenstandorten mehr nötig
- -> Das macht die Kosten einer WAN-Technologie völlig unnötig
- Stattdessen können Unternehmen mit **Point-to-Point-VPNs** sicherstellen, dass ihre Standorte kommunizieren können
- Ein Point-to-Point-VPN oder Site-to-Site-VPN schafft einen **VPN-Tunnel zwischen zwei Standorten**
- Das funktioniert fast wie eine reguläre VPN-Konfiguration, bei der Nutzer vorgehen können, als wären sie direkt im verbundenen Netzwerk
- Nur, dass die VPN-Tunnel-Logik von Netzwerkgeräten auf beiden Seiten verwaltet wird, sodass Benutzer Verbindungen nicht selbst herstellen müssen

## Einstieg ins drahtlose Netzwerk

- Methode, ein Netzwerk ohne Kabel aufzubauen
- Die wichtigsten Spezifikationen für die drahtlose Kommunikation sind in der Norm IEEE 802.11 festgelegt
- Diese Spezifikationen werden auch die „802.11-Familie“ genannt und beschreiben das, was wir „WLAN“ nennen

- Drahtlose Netzwerkgeräte kommunizieren über Funkwellen miteinander. Verschiedene 802.11-Normen verwenden weitestgehend dieselben Protokolle, aber nutzen eventuell verschiedene Frequenzbänder
- Ein Frequenzband ist ein bestimmter Bereich des Funkspektrums, bei dem man sich darauf geeinigt hat, es für bestimmte Zwecke zu verwenden
- WLAN-Netzwerke verwenden einige verschiedene Frequenzbänder: meistens 2,4 und 5 Gigahertz
- 802.11 Frame:



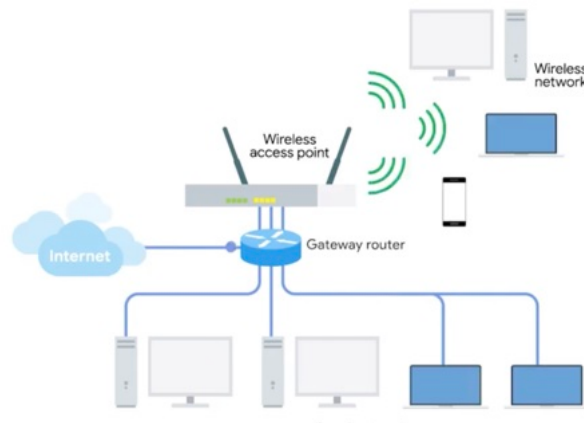
- **Frame-Control-Feld:** Dieses Feld ist 16 Bit lang und enthält einige untergeordnete Felder, die beschreiben, wie der Frame selbst verarbeitet werden soll -> Dazu gehört zum Beispiel die 802.11-Version, die verwendet wurde
- **Duration-Feld:** Das nächste Feld ist das Duration-Feld. Es gibt die Länge des gesamten Frames an -> So weiß der Empfänger, wie lange er der Übertragung zuhören muss
- Danach kommen **vier Adressfelder**
- -> wieso 4 statt 2 Adressfelder? :
  - Ein drahtloser Access Point ist ein Gerät, das den drahtlosen mit dem drahtgebundenen Teil eines Netzwerks verbindet
  - Wir haben also das übliche Quellen-Adressfeld mit der MAC-Adresse des Absenders
  - Wir haben aber auch das Zielgerät im Netzwerk sowie eine Empfänger- und eine Überträgeradresse
  - Die Empfängeradresse ist hierbei die MAC-Adresse des Access Points, der den Frame empfangen soll
  - Die Überträgeradresse ist die MAC-Adresse des Geräts, das gerade den Frame gesendet hat -> In vielen Situationen sind Ziel und Empfänger dasselbe Gerät
  - Oft sind auch die Quelle und der Überträger dasselbe Gerät
  - Doch bei manchen Architekturen von drahtlosen Netzwerken ist das eventuell nicht der Fall -> Manchmal geben Access Points einen Frame unter sich weiter
  - Da alle Adressen im 802.11-Frame MAC-Adressen sind, ist jedes Feld sechs Byte lang
  - **Sequence Control-Feld:** Das Sequence Control-Feld ist 16 Bit lang und enthält eine Nummer zum Verfolgen der Reihenfolge der Frames
  - Danach folgt die **Payload**, in der sich alle Daten der Protokolle weiter oben im Stack befinden
  - Zuletzt haben wir ein **Frame Check Sequence-Feld** -> enthält eine Checksumme für zyklische Redundanzprüfungen, genau wie auch beim Ethernet

## Konfiguration von drahtlosem Netzwerk

- Bei Ad-hoc-Netzwerken kommunizieren alle Knoten direkt miteinander
- Bei drahtlosen LANs (WLANs) dienen einer oder mehrere Zugriffspunkte als Brücke zwischen WLAN und kabelgebundenem Netzwerk
- Mesh-Netzwerke sind hybride Formen aus beiden Typen
- Ad-hoc-Netzwerke haben keine unterstützende Netzwerkinfrastruktur -> Jedes Gerät, das mit dem Netzwerk verbunden ist, kommuniziert mit allen anderen Geräten in Reichweite, und alle Knoten leiten Nachrichten weiter
- Ad-hoc-Netzwerke sind auch in Industrie- und Lagerumgebungen zu finden, wo einzelne Geräte miteinander kommunizieren müssen, aber nicht darüber hinaus
- Außerdem können Ad-hoc-Netzwerke im Katastrophenfall gute Dienste leisten



- Der gängigste Typ drahtloser Netzwerke in der Geschäftswelt sind drahtlose LANs, kurz WLANs
- WLANs bestehen aus einem oder mehreren Zugangspunkten, die als Brücke zwischen drahtlosem und kabelgebundenem Netzwerk dienen
- Das kabelgebundene Netzwerk ist ein normales LAN wie die, die wir bereits besprochen haben
- Das kabelgebundene LAN umfasst den ausgehenden Netzwerk-Link
- Um auf Ressourcen außerhalb des WLANs zugreifen zu können, kommunizieren drahtlose Geräte mit Zugangspunkten
- Diese leiten den Traffic anschließend an den Gateway-Router weiter, wo alles wie gewohnt abläuft



- Die meisten Mesh-Netzwerke bestehen ausschließlich aus drahtlosen Zugangspunkten, sind aber trotzdem mit einem kabelgebundenen Netzwerk verbunden

## WLAN-Kanäle

- Kanäle sind einzelne, kleinere Bereiche des gesamten Frequenzbands, das ein drahtloses Netzwerk nutzt
- Kanäle sind sehr wichtig, denn sie lösen ein altes Netzwerkproblem: Kollisionsdomänen
- Da je nach Land und Region andere Regelungsausschüsse entscheiden, welche Funkfrequenzen zu welchen Zwecken genutzt werden können, richtet sich die Zahl der verfügbaren Kanäle danach, wo in der Welt Sie sich befinden
- Bei 802.11b-Netzwerken wird Kanal 1 z. B. bei 2.412 MHz betrieben -> aber da die Kanalbreite 22 MHz beträgt, nutzt das Signal tatsächlich die Frequenzen von 2.401 bis 2.423 MHz
- Das liegt daran, dass Funkwellen ungenau sind und daher Puffer um die genauen Frequenzen einer spezifischen Übertragung benötigt wird
- Manche Kanäle überschneiden sich, andere liegen dagegen so weit auseinander, dass jede Störung ausgeschlossen ist
- Für ein 802.11b-Netzwerk heißt das, dass die Kanäle 1, 6 und 11 sich als einzige niemals überschneiden
- Drahtlose Netzwerkgeräte erkennen heute fast alle automatisch, welche Kanäle überlastet sind
- Manche Zugangspunkte analysieren die Kanäle nur beim Start, andere passen ihren Kanal nach Bedarf dynamisch an
- Achten Sie darauf, dass sich die Kanäle Ihrer Zugangspunkte und die Ihrer Nachbarn möglichst nicht überschneiden



## WLAN Sicherheit

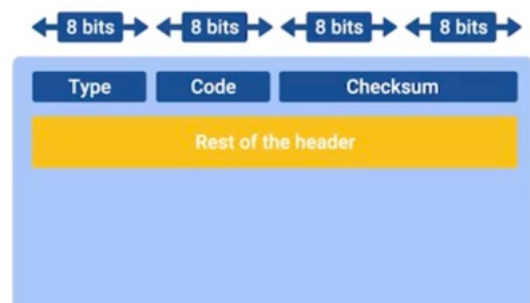
- Beim Senden von Daten über einen kabelgebundenen Link sind die Daten teilweise automatisch geschützt -> Die einzigen Geräte, die die übertragenen Daten kennen, sind die zwei Knoten an den beiden Link-Enden
- bei WLAN: **WEP** steht für „Wired Equivalent Privacy“ („Schutz wie bei Verkabelung“) und ist eine Verschlüsselungstechnologie mit einem sehr geringen Schutzniveau
- ist aber nicht sicherer als die unverschlüsselte Datenübertragung über eine kabelgebundene Verbindung
- Merken Sie sich vorläufig, dass die Zahl der Bits eines Verschlüsselungsschlüssels seine Sicherheit widerspiegelt
- WEP verschlüsselt mit nur 40 Bits -> mit schnellen modernen Computern lässt sich das in wenigen Minuten knacken
- WEP wurde fast überall bald durch **WPA** oder „Wifi Protected Access“ ersetzt
- WPA verschlüsselt standardmäßig mit 128 Bits und ist dadurch deutlich schwerer zu knacken als WEP
- Der gängigste Verschlüsselungsalgorithmus für drahtlose Netzwerke ist heute WPA2, ein Update von WPA -> **WPA2** verschlüsselt mit 256 Bits und ist dadurch noch schwerer zu knacken
- **MAC-filtering:** Dabei werden die Zugangspunkte so konfiguriert, dass sie nur Verbindungen von bestimmten MAC-Adressen vertrauenswürdiger Geräte zulassen
- -> drahtloser Traffic wird damit nicht besser verschlüsselt übertragen, aber es wird eine zusätzliche Barriere geschaffen, die verhindert, dass sich unbefugte Geräte mit dem drahtlosen Netzwerk verbinden

## Einstieg in die Fehlerbehebung

- Fehlererkennung ist die Fähigkeit eines Protokolls oder Programms, festzustellen, dass etwas schiefgelaufen ist
- Fehlerbehebung ist die Fähigkeit eines Protokolls oder Programms, eine Fehlerbeseitigung zu versuchen

## Internet Control Message Protocol (ICMP)

- Das ICMP wird hauptsächlich von einem Router oder Remote-Host verwendet, um den Grund für die fehlgeschlagene Übertragung zurück zum Ursprung der Übertragung zu kommunizieren
- ICMP-Pakets -> Header mit einigen Feldern und einen Datenabschnitt, der vom Host genutzt wird, um herauszufinden, welche Übertragung den Fehler erzeugt hat
- erstes Feld: **Typfeld** -> 8 Bits lang
- gibt an, welcher Nachrichtentyp geliefert wird (z.B.: Ziel nicht erreichbar oder Zeit überschritten)
- **Code-Feld:** gibt genaueren Grund für die Nachricht an, als nur den Typ
- Beispielsweise sind bei dem Typ „Ziel nicht erreichbar“ individuelle Codes verfügbar, z. B. Zielnetzwerk nicht erreichbar oder Zielpport nicht erreichbar
- danach: 16-Bit-Prüfsumme
- danach: Rest of Header (32-Bit-Feld)
- Datennutzlast: Die Nutzlast für ein ICMP-Paket liegt vollständig vor, sodass der Empfänger der Nachricht weiß, welche Übertragung den gemeldeten Fehler verursacht hat. Sie enthält den gesamten IP-Header und die ersten acht Bytes des Datennutzlastabschnitts des problematischen Pakets



- Das ICMP wurde eigentlich nicht für die menschliche Interaktion entwickelt -> es geht darum, dass diese Fehlermeldungen automatisch zwischen vernetzten Computern zugestellt werden können
- Aber es gibt auch ein spezifisches Tool und zwei Nachrichtentypen, die für menschliche Bediener sehr nützlich sind -> **Ping**
- Ping lässt Sie einen speziellen Typ von ICMP-Nachricht senden, genannt Echo-Anfrage
- Eine ICMP-Echo-Anfrage verlangt im Wesentlichen einfach ein Ziel: Hallo, bist du da?
- Wenn das Ziel betriebsbereit ist und über das Netzwerk kommunizieren kann, sendet es eine Nachricht vom Typ Echo-Antwort an das ICMP zurück
- Sie können den Ping-Befehl von der Befehlszeile eines jeden modernen Betriebssystems aus aufrufen
- In der einfachsten Form tippen Sie einfach Ping und eine IP-Adresse ein oder auch einen voll qualifizierten Domainnamen
- In jeder Ausgabezeile wird normalerweise die Adresse angezeigt, von der die ICMP-Echo-Antwort gesendet wird und wie lange die Kommunikation hin und zurück gedauert hat
- Es beinhaltet ebenso die restliche TTL und wie groß die ICMP-Nachricht in Bytes ist
- Unter Linux und macOS läuft der Ping-Befehl so lange, bis der Endnutzer eine Unterbrechungsaufforderung sendet

## Traceroute

- Manchmal müssen Sie herausfinden, wo genau in der langen Kette der Router-Hops das Problem liegt -> dafür gibt es Traceroute
- Traceroute ist ein großartiges Tool, um die Pfade zwischen 2 Knoten zu bestimmen, und liefert Informationen zu allen Hops auf der Strecke
- Wenn das TTL-Feld 0 erreicht, wird das Paket verworfen und eine ICMP-Zeitüberschreitungsmeldung an den Ursprungshost gesendet
- Traceroute legt das TTL-Feld für das erste Paket zunächst auf 1 fest, dann auf 2 für das zweite, auf 3 für das dritte usw. -> diese clevere Methode stellt sicher, dass das erste gesendete Paket beim ersten Router-Hop verworfen wird
- Das Ergebnis ist eine ICMP-Zeitüberschreitungsmeldung
- Das wird fortgesetzt, bis das Paket sein Ziel erreicht. Traceroute sendet 3 identische Pakete für jeden Hop
- Bei Windows hat der Befehl den verkürzten Namen „tracert“ und verwendet standardmäßig ICMP-Echo-Anfragen

```
cindy@cindy-nyc:~$ traceroute google.com
traceroute to google.com (216.58.195.78), 30 hops max, 60 byte packets
 1  100.111.191.252 (100.111.191.252)  2.768 ms  3.427 ms  4.609 ms
 2  172.27.120.113 (172.27.120.113)  4.694 ms  5.065 ms  5.144 ms
 3  172.27.104.17 (172.27.104.17)  8.696 ms  8.704 ms  9.214 ms
 4  104.133.2.193 (104.133.2.193)  9.227 ms  9.547 ms  9.552 ms
 5  72.14.210.37 (72.14.210.37)  9.775 ms  72.14.210.99 (72.14.210.99)  10.480 ms  72.14.210.37 (72.14.210.37)  13.198 ms
 6  108.170.242.81 (108.170.242.81)  14.063 ms  3.441 ms  4.297 ms
 7  108.170.235.237 (108.170.235.237)  5.194 ms  5.191 ms  108.170.235.239 (108.170.235.239)  5.123 ms
 8  sfo07s16-in-f78.1e100.net (216.58.195.78)  5.150 ms  5.154 ms  5.131 ms
cindy@cindy-nyc:~$
```

- Es gibt zwei weitere Tools wie Traceroute: mtr unter Linux und Mac OS und pathping unter Windows

## Portverbindung testen

- Sie kennen jetzt viele Möglichkeiten, um die Konnektivität zwischen Geräten auf Netzwerkebene zu testen. Aber manchmal müssen Sie wissen, ob auf der Transportebene alles funktioniert
- Dafür gibt es zwei leistungsstarke Tools: **Netcat** für Linux und Mac OS und **Test-NetConnection** für Windows
- Netcat wird mit dem Befehl `nc` ausgeführt und hat zwei obligatorische Argumente: einen Host und einen Port
- Mit „`nc google.com 80`“ wird z. B. versucht, an Port 80 eine Verbindung zu `google.com` herzustellen
- Schlägt dies fehl, wird der Befehl beendet. Bei einem erfolgreichen Versuch blinkt der Cursor für weitere Eingaben

```
cindy@cindy-nyc:~$ nc google.com 80
```

- Wenn Sie nur den Portstatus abfragen möchten, geben Sie den Befehl mit dem Flag `-z` aus, das für Null-Eingabe-/Ausgabe-Modus steht
- Auch das Flag `-v` für „verbose“ oder „ausführlichen Modus“ ist hier nützlich
- Die Befehlsausgabe wird dadurch besser nachvollziehbar, während sich „non verbose“ gut für Nutzung und Scripts eignet („verbose“ heißt wörtlich übrigens so viel wie „wortreich“ oder „weitschweifig“)

```
cindy@cindy-nyc:~$ nc -z -v google.com 80
Connection to google.com 80 port [tcp/http] succeeded!
cindy@cindy-nyc:~$
```

bei Windows:

- Mit Test-NetConnection mit dem Flag `-port` lässt sich die Verbindung zu einem bestimmten Port testen

```
PS C:\Users\cindy> Test-NetConnection google.com

ComputerName           : google.com
RemoteAddress          : 2607:f8b0:4005:80a::200e
InterfaceAlias         : Wi-Fi
SourceAddress          : 2620:0:1001:fd01:b921:7702:69a2
PingSucceeded          : True
PingReplyDetails (RTT) : 731 ms

PS C:\Users\cindy>
```

## Tools zur Namensauflösung

- Angenommen, Sie möchten die IP-Adresse für twitter.com wissen, geben Sie einfach nslookup twitter.com ein und der A-Eintrag wird ausgegeben
- Um eine interaktive nslookup-Session zu starten, geben Sie einfach nslookup ein, ohne danach einen Hostnamen einzugeben
- Wenn Sie im interaktiven Modus sind und Server eintippen, und danach eine Adresse, werden alle folgenden Abfragen zur Namensauflösung unter Verwendung dieses Servers durchgeführt, anstatt mit dem Standard-Namensserver
- Sie können auch set type eingeben, Gleichheitszeichen und dann einen Ressourceneintrag

```
cindy@cindy-nyc:~$ nslookup
> coursera.org
Server:      127.0.1.1
Address:     127.0.1.1#53

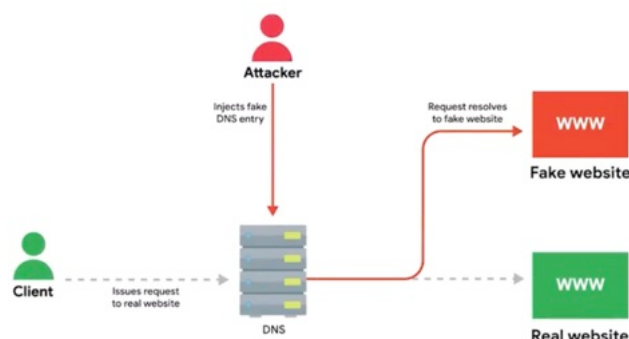
Non-authoritative answer:
Name:   coursera.org
Address: 54.192.146.230
Name:   coursera.org
Address: 54.192.146.18
Name:   coursera.org
Address: 54.192.146.32
Name:   coursera.org
Address: 54.192.146.150
Name:   coursera.org
Address: 54.192.146.234
Name:   coursera.org
Address: 54.192.146.188
Name:   coursera.org
Address: 54.192.146.67
Name:   coursera.org
Address: 54.192.146.4
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> google.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.195.78
> set type=MX
> google.com
```

- Wenn Sie wirklich ganz genau wissen wollen, was los ist, dann können Sie set debug eingeben

## öffentliche DNS-Server

- Meistens sind diese Nameserver alles, was Sie wirklich brauchen, damit Ihr Computer mit anderen Geräten im Internet kommunizieren kann
- Aber die meisten Firmen betreiben auch ihre eigenen DNS-Server
- Zumindest ist das erforderlich, um Namen interner Hosts aufzulösen
- Alles von der Namensgebung eines Computers oder eines NAIS-Laptops bis hin zum Zugriff auf einen Drucker durch einen Namen anstatt einer IP-Adresse benötigt Ihren eigenen Nameserver
- 3. Option: einen DNS als Service-Provider zu verwenden
- Einige Internet-Organisationen betreiben sogenannte öffentliche DNS-Server, das sind Nameserver, die extra eingerichtet wurden, damit jeder sie kostenlos nutzen kann
- google hat öffentliche nameserver unter 8.8.8.8 und 8.8.4.4.
- Gefahr: Abfangen ausgehender DNS-Anfragen mit fehlerhaften Antworten ->

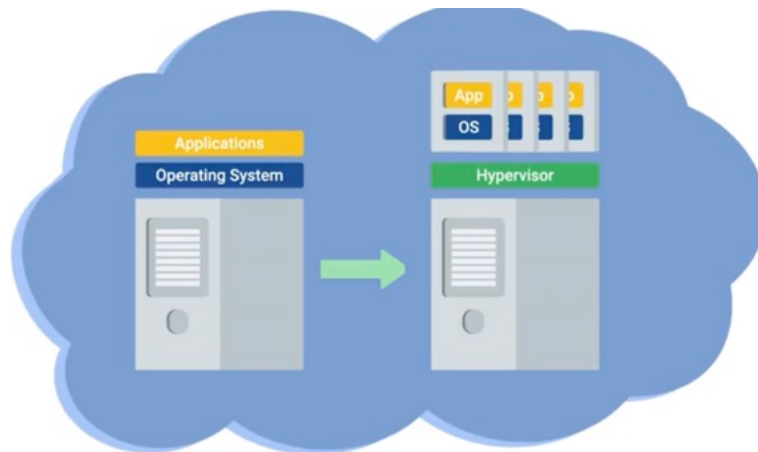


## DNS-Registrierung und -Ablaufdaten

- Denken Sie daran, dass DNS ein globales System ist, das in einer mehrstufigen Hierarchie mit der ICANN an der Spitze verwaltet wird
- Domainnamen müssen weltweit einzigartig sein, damit ein solches globales System funktionieren kann

## Was ist eine Cloud

- Im Grunde ist Cloud Computing ein technologischer Ansatz, bei dem Computerressourcen gemeinsam genutzt werden
- **Hardware-Virtualisierung** ist ein zentrales Konzept für Cloud-Computing-Technologien
- Damit kann das Konzept eines physischen und eines logischen Rechners voneinander abstrahiert werden
- Mit der Virtualisierung kann ein einziger physischer Computer, der Host, viele einzelne virtuelle Instanzen, die Gäste, ausführen
- Ein Betriebssystem erwartet, dass es auf bestimmte Weise mit der zugrunde liegenden Hardware kommunizieren kann
- Hardware-Virtualisierungsplattformen nutzen einen so genannten Hypervisor
- **Hypervisor**: eine Software, die virtuelle Maschinen ausführt und verwaltet und gleichzeitig diesen Gästen eine virtuelle Betriebsplattform bietet, die von der tatsächlichen Hardware nicht zu unterscheiden ist



- Die Cloud bringt dieses Konzept noch einen Schritt weiter: Sie bauen einen riesigen Cluster aus miteinander verbundenen Rechnern auf, die alle als Hosts für viele virtuelle Gäste fungieren können -> sie haben ein System, mit dem Sie Ressourcen unter all diesen Instanzen aufteilen können
- Beispiel: ein Unternehmen braucht eigentlich 4 Server: Mailserver, DNS-Server, einen Server für die Finanzdaten und einen Backup. Mailserver läuft auf Windows, DNS-Server auf Linux ect. -> obwohl nicht alle Ressourcen gleichzeitig benötigt werden, braucht es 4 Server und ist dadurch recht teuer -> Cloud nutzt nur die benötigten Ressourcen und ist günstiger
- es gibt public Clouds und private Clouds
- hybrid Cloud: kein eigenes Konzept -> steht für Situationen, in denen Unternehmen beispielsweise Dinge wie ihre sensibelsten proprietären Technologien in eine Private Cloud packen, während sie ihre weniger sensiblen Server einer Public Cloud anvertrauen

- Cloud:
  - Ein neues Computermode, bei dem große Cluster von Rechnern es uns ermöglichen, die gesamten verfügbaren Ressourcen besser zu nutzen.
  - Mit der Cloud können Sie schnell einen neuen Server bereitstellen und viele bestehende Dienste nutzen, anstatt eigene zu entwickeln
- X as a service
- Infrastructure as a Service oder IaaS
- -> Die Idee hinter IaaS ist, dass Sie sich nicht um den Aufbau Ihres eigenen Netzwerks oder Ihrer eigenen Server kümmern müssen
- Cloud umfasst mittlerweile aber noch mehr: **Platform-as-a-Service oder PaaS, und Software-as-a-Service oder SaaS**
- Platform as a Service ist eine Untergruppe des Cloud Computing, bei dem eine Plattform für Kunden bereitgestellt wird -> für jede Software, die jemand ausführen möchte, steht eine Ausführungsmaschine bereit
- Sie benötigen nur eine Umgebung für ihre Webanwendung und keinen ganzen Server mit einem komplexen Dateisystem
- **Infrastructure as a Service abstrahiert die benötigte physische Infrastruktur und Platform as a Service abstrahiert die benötigten Serverinstanzen. Mit Software as a Service kann die Nutzung von Software an andere lizenziert werden, wobei die Software im Wesentlichen gehostet und verwaltet wird**
- Beispiel für SaaS: Email-Dienste (gmail) -> läuft im Browser
- das Netzwerk eines Unternehmens dient heute nur noch dazu, eine Internetverbindung für den Zugriff auf Software oder Daten in der Cloud zu haben

## IPv6-Adressen und -Subnetze

- Bei IPv6 besteht die Loopback-Adresse aus 31 Nullen mit einer Eins am Ende, die sich zu ::1 zusammenfassen lässt
- So wird zum Beispiel jede Adresse, die mit FF00:: beginnt, für Multi-Cast verwendet, eine Möglichkeit, Gruppen von Hosts auf einmal zu adressieren. Adressen, die mit FE80:: beginnen, werden für verbindungslokale Unicast-Adressen verwendet
- Diese ermöglichen die Kommunikation in lokalen Netzwerksegmenten und werden auf Basis der MAC-Adresse eines Hosts konfiguriert
- Die ersten 64 Bits jeder IPv6-Adresse bilden die Netzwerk-ID und die zweiten 64 Bits jeder IPv6-Adresse ist die Host-ID
- IPv6 bringt nicht nur größere Adressen, sondern auch grundlegende Verbesserungen
- **Ziel:** Einfacherer Header, bessere Leistung und Priorisierung von Datenverkehr

### IPv6-Header – Aufbau und Felder:

- Version (4 Bit): Gibt an, ob IPv6 verwendet wird (wie bei IPv4).
- Traffic Class (8 Bit): Definiert Priorität des Datenverkehrs (Quality of Service).
- Flow Label (20 Bit): Identifiziert Datenströme, ermöglicht spezielle Behandlung durch Router.
- Payload-Länge (16 Bit): Gibt die Länge des Dateninhalts an (ohne Header).
- Next Header: Gibt an, welcher Header als nächstes folgt (z. B. TCP, UDP oder optionaler Header).
- Hop Limit (8 Bit): Entspricht dem TTL-Feld bei IPv4 – begrenzt Lebensdauer des Pakets.
- Quell- & Zieladresse (je 128 Bit): Größerer Adressraum als bei IPv4 (32 Bit).
- Zusätzliche Merkmale:
- IPv6-Adressen sind viermal so lang wie IPv4-Adressen.
- Längere Adressen bedeuten mehr Daten, daher wurde der Header so kurz wie möglich gehalten.
- Optionale Felder wurden aus dem Haupt-Header ausgelagert.
- Zusätzliche Header sind optional und können bei Bedarf verkettet werden.

- **Ziel von IPv6: Effizienz, Einfachheit und Erweiterbarkeit bei deutlich größerem Adressraum**

## Koexistenz von IPv4 und IPv6 – Übergangslösungen

### Allgemeines:

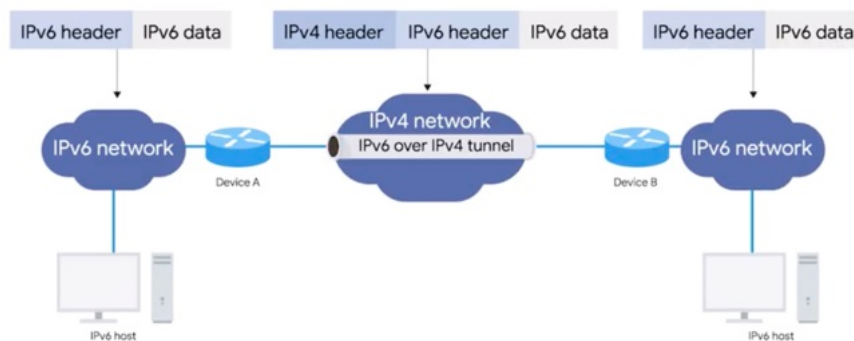
- Ein gleichzeitiger, globaler Umstieg auf IPv6 ist nicht möglich.
- Zu viele alte Geräte unterstützen IPv6 noch nicht.
- IPv6 und IPv4 müssen daher eine Zeit lang parallel existieren können.
- Unternehmen können individuell auf IPv6 umsteigen.

### IPv4-mapped IPv6-Adressen:

- Spezielle IPv6-Adressen beginnen mit 80 Nullen + 16 Einsen.
- Die letzten 32 Bit enthalten die ursprüngliche IPv4-Adresse.
- Erlaubt es, IPv4-Traffic über IPv6-Netzwerke zu transportieren.

### IPv6 über IPv4 – Tunnel:

- IPv6-Traffic kann auch durch IPv4-Netzwerke laufen.
- Lösung: IPv6-Tunnel, bestehend aus zwei Tunnelservern.
- Tunnelserver kapseln IPv6-Daten in IPv4-Datenpakete ein.
- Am Ziel entpackt der zweite Server die Daten wieder.
- So funktioniert IPv6 über bestehende IPv4-Infrastruktur.



### Tunnelbroker:

- Dienstleister, die IPv6-Tunnel-Endpunkte bereitstellen.
- Vorteil: keine zusätzliche eigene Ausrüstung nötig.
- Unterstützen verschiedene Tunnelprotokolle.

### Zukunft:

- Aktuell konkurrieren verschiedene Tunneltechnologien.
- Langfristig wird IPv6 vollständig übernommen werden.
- Tunnel werden dann überflüssig – die Zukunft ist "tunnellos".



## Betriebssysteme / Windows & Linux

- In Betriebssystemen sind Dateien und Ordner oder Verzeichnisse in einer hierarchischen Verzeichnisstruktur organisiert
- Ein Hauptverzeichnis verzweigt sich und enthält andere Verzeichnisse und Dateien
- Die Orte dieser Dateien und Verzeichnisse bezeichnen wir als Pfade
- Die meisten Pfade in Windows sehen in etwa so aus: C:\Users\Cindy\Desktop
- In Windows werden Dateisysteme Laufwerksbuchstaben zugewiesen, z. B. C:, D: oder X:. Jeder Laufwerksbuchstabe ist ein Dateisystem
- Dateisysteme dienen zum Überwachen von Dateien auf dem Computer
- Windows: \
  - Linux: /
- Wir verwenden den Befehl „ls“ zur Verzeichnisauflistung und geben den Pfad für unsere Suche ein

```
windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\cindy> ls C:\

    Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----          10/5/2017   3:40 PM             Intel
d-----          3/18/2017   2:03 PM             PerfLogs
d-r---          10/5/2017   3:46 PM          Program Files
d-r---          10/5/2017   3:29 PM          Program Files (x86)
d-r---          10/5/2017   3:38 PM             Users
d-----          10/5/2017   3:44 PM        Vacation Pictures
d-----          10/5/2017   3:42 PM            windows

PS C:\Users\cindy> 
```

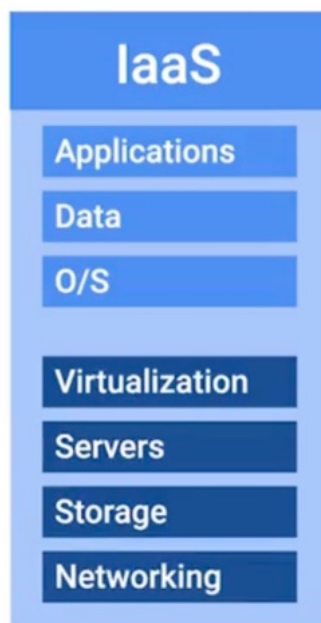
## siehe extra PDF für die Betriebssysteme!

- Kleinere Unternehmen könnten dies auch tun, aber normalerweise mieten sie Teile eines Rechenzentrums für ihren Bedarf
- Wenn Sie einen Cloud-Dienst nutzen, werden diese Daten in der Regel in einem oder mehreren Rechenzentren gespeichert, die groß genug sind, um die Informationen von Millionen oder sogar Milliarden von Nutzern zu speichern
- Anstatt Ihre eigenen Server zu verwalten, können Sie Internetdienste nutzen, die alles für Sie erledigen, einschließlich Sicherheitsupdates, Server-Hardware, regelmäßige Software-Updates und vieles mehr



# Cloud

- Sie können die Cloud-Alternative nutzen, um Ihre eigene Infrastruktur zu warten
- Dies wird als „**Infrastructure as a service**“ oder **IaaS** bezeichnet.
- IaaS-Anbieter bieten Ihnen vorkonfigurierte virtuelle Maschinen, die Sie genauso nutzen können wie einen physischen Server
- Bekannte IaaS-Anbieter sind Amazon Web Services mit ihren Elastic Compute Cloud oder EC2-Instanzen, Linode als Vermieter virtueller Server sowie Windows Azure und die Google Compute Engine



- Das Netzwerk kann in einen IaaS-Anbieter integriert werden, aber in den letzten Jahren wurde es auch als eigener Cloud-Dienst „**Networking as a Service**“ (**NaaS**) ausgegliedert
- NaaS ermöglicht Unternehmen, ihre Netzwerkdienste auszulagern, sodass sie sich nicht um teure Netzwerk-Hardware kümmern müssen
- Die Unternehmen müssen also nicht ihre eigene Netzwerksicherheit aufstellen, das eigene Routing verwalten, eigene und private Internetzugänge einrichten usw.
- Die Cloud-Alternative zur Wartung Ihrer Software ist als „**Software as a Service**“ oder **SaaS** bekannt.
- Anstatt auf jedem Rechner ein Textverarbeitungsprogramm zu installieren, können Sie Microsoft Office 365 oder Google G Suite nutzen
- Wenn Sie eine Komplettlösung zu Aufbau und Bereitstellung einer Web-Anwendung möchten, können Sie „**Platform as a Service**“ oder **PaaS** nutzen.
- PaaS bietet eine Plattform, um den Code zu erstellen, Informationen in einer Datenbank zu speichern und die Anwendung von nur einer Plattform bereitzustellen.
- Der letzte IT-Infrastrukturdienst, den wir besprechen werden, ist die Verwaltung von Nutzern, Zugang und Berechtigungen
- Ein Verzeichnisdienst zentralisiert Nutzer und Computer Ihrer Organisation an einem Ort, damit Sie Nutzer und Computer hinzufügen, aktualisieren und entfernen können
- Verzeichnisdienste können auch in der Cloud eingesetzt werden mithilfe von „**Directory as a Service**“ - oder **DaaS-Anbietern**

# Remote-Verbindungen

## Remote-Verbindungen

Sie haben sich bereits mit den Grundlagen des Remote-Zugriffs vertraut gemacht. In diesem Artikel stellen wir verschiedene Methoden und Tools vor, mit denen Sie eine Remote-Verbindung herstellen können. Außerdem erfahren Sie, auf welche Sicherheitsrisiken Sie dabei achten sollten.

Mithilfe einer Remote-Verbindung können Sie als IT-Supportmitarbeiter Probleme bei entfernten Systemen beheben. Dazu gehören Laptops, PCs, Workstations, Server, Geräte in Rechenzentren und andere IT-Geräte, auf die Remote-Zugriff gewährt wird. Außerdem lassen sich Remote-Verbindungen für Dateiübertragungen und Terminalemulationen einsetzen. Software für Remote-Zugriff erspart Ihnen Zeitaufwand, da Sie so nicht zum jeweiligen Standort fahren müssen.

Diese Art von Software eignet sich auch für flexible Arbeitsmodelle, die sich in den letzten Jahren zunehmender Beliebtheit erfreuen. Zahlreiche Unternehmen bieten ihren Mitarbeitern anhand von Remote-, Hybrid- und flexibler Arbeitsmodelle die Möglichkeit, im Homeoffice zu arbeiten. Aufgrund dieser Entwicklung erkennen immer mehr Arbeitgeber und Mitarbeiter die Vorteile dieser Angebote. Mitarbeiter sparen Zeit und Geld, da sie nicht mehr zur Arbeit pendeln müssen. Viele geben an, dadurch ihre Work-Life-Balance verbessert zu haben. Arbeitgeber sparen Kosten, da sie weniger physische Büroräumlichkeiten unterhalten müssen. Außerdem können sie so ihren Personalpool weit über ihren eigenen Standort hinaus erweitern und Arbeitskräfte aus anderen Städten, Regionen oder sogar anderen Ländern einstellen.

Mehrere Umfragen haben ergeben, dass bis zu 95 % der US-Arbeitgeber und -nehmer ihre Remote-, Hybrid- und/oder flexiblen Arbeitsmodelle gerne dauerhaft beibehalten würden. Laut einem kürzlich veröffentlichten Bericht von Microsoft stellen 66 % der Arbeitgeber weltweit ihre Arbeitsplätze auf hybride Modelle um. (Näheres dazu finden Sie unten im Abschnitt „Weitere Informationen“.) Angesichts dieser Veränderungen werden IT-Supportmitarbeiter immer häufiger damit betraut, Remote-Verbindungen für Unternehmensnetzwerke herzustellen, zu konfigurieren, zu verwalten und/oder damit verbundene Fehler zu beheben.

## Remote-Zugriff-Software für die IT-Verwaltung

Im Gegensatz zu RDP (Remote Desktop Protocol) und VPN (Virtual Private Network) wird manche Software für den Remote-Zugriff in der Regel nur von IT-Managern und anderen Supportmitarbeitern verwendet. Mithilfe dieser Remote-Anwendungen können IT-Supportteams große Netzwerke effizienter verwalten und überwachen.

· **Secure Shell oder Secure Socket Shell (SSH):** SSH ist ein Netzwerkprotokoll, das mehrere Tools umfasst, mit denen eine sichere Internetverbindung zwischen einem Computer und einem privaten Netzwerk hergestellt werden kann. SSH ist in den Betriebssystemen Linux/Unix und Mac OS X Server enthalten. Es bietet Protokolle zur Identitäts- und Zugriffsverwaltung über zuverlässige Passwort- und Public-Key-Authentifizierung. SSH verschlüsselt außerdem Datenübertragungen über das Internet.

Sitzungen werden anhand einer SSH-Clientanwendung aufgebaut, um eine Verbindung zu einem SSH-Server herzustellen. Aus Sicherheitsgründen werden SSH-Schlüssel verwendet, um Dienste zur Einmalanmeldung (Single Sign-On, SSO) bereitzustellen und den Zugriff auf Server zu automatisieren. So können Skripts und Sicherungen ausgeführt sowie Konfigurationstools verwendet werden. SSH wird vor allem von IT-Supportmitarbeitern verwendet, um per Remote-Zugriff Dateiübertragungen und Terminalemulatoren auf Linux/Unix-Systemen zu verwalten. Mithilfe des SSH-Netzwerkprotokolls kann z. B. ein verschlüsselter Tunnel eingerichtet werden, der ihren Computer über ein Netzwerk mit einem Remote-Server verbindet. Anschließend können sie mit dem SSH-Dateiübertragungstool eine Datei, z. B. ein Firmware-Update-Paket, auf den Remote-Server übertragen. Und anhand des SSH-Terminalemulators kann die Firmware dann per Befehlszeile auf dem Remote-Server installiert werden.

• **Remote Monitoring and Management (RMM):** IT-Supportexperten nutzen RMM, um Informationssysteme aus der Ferne zu überwachen und zu verwalten. Um RMM zu implementieren, muss ein RMM-Agent auf jedem Endpunkt eines Netzwerks installiert werden, einschließlich Servern, Arbeitsstationen und Mobilgeräten. Über die Agents erhalten die IT-Supportmitarbeiter dann regelmäßige Statusberichte über den Zustand jedes Endpunkts. RMM-Tools ermöglichen außerdem die Remote-Installation von Sicherheits-Patches und -Updates und erleichtern so die proaktive Wartung des Netzwerks. Wenn bei einem Endgerät ein Problem auftritt, erstellt der RMM-Agent ein Ticket, klassifiziert die Art und den Schweregrad des Problems und leitet das Ticket dann an die IT-Supportmitarbeiter weiter. Mit RMM-Systemen können IT-Supportanbieter Informationssysteme effizienter verwalten. Sie haben die Möglichkeit, über ein einheitliches RMM-Dashboard routinemäßige Wartungen für mehrere Endgeräte gleichzeitig zu verwalten und sogar zu automatisieren.

## Software für den Remote-Zugriff

Um eine Remote-Verbindung zwischen einem Endnutzer und einem Unternehmensnetzwerk herzustellen, kann Software für den Remote-Zugriff eingesetzt werden. Diese Art von Software bietet IT-Experten außerdem die Möglichkeit, Unternehmensnetzwerke aus der Ferne zu verwalten. Es gibt verschiedene Lösungen für den Fernzugriff, von denen jede bestimmte Vor- und Nachteile mit sich bringt. Nachfolgend einige Optionen für verschiedene Anwendungsfälle, Unternehmensgrößen und Netzwerkumgebungen:

- **Remote Desktop Protocol (RDP):** RDP ist ein von Microsoft entwickeltes Remote-Protokoll. Das Protokoll ist kompatibel mit den meisten Windows- und Mac-Betriebssystemen. Eine Lösung auf Basis von RDP eignet sich gut für flexible oder hybride Arbeitsumgebungen, in denen die Mitarbeiter sowohl im Büro als auch remote arbeiten. Mit RDP können Endnutzer nicht nur auf den Desktop, die Software, die Dateien und das Netzwerk zugreifen, sondern auch auf die physischen Computer, die sich an ihren Arbeitsplätzen befinden. IT-Supportmitarbeiter nutzen RDP-Software auch zur Fehlerbehebung und dazu, Patches und Updates auf den Endnutzercomputern zu installieren, ohne sich am jeweiligen Standort aufhalten zu müssen.

Mit RDP werden der Desktop sowie Daten, Tastatureingaben und Mausbewegungen des Benutzers verschlüsselt und über das Internet übertragen. Während der Übertragung kann es vorkommen, dass Nutzer verzögerte Reaktionen auf ihre Tastatureingaben und

Mausaktivitäten feststellen. Das RDP-System erstellt einen dedizierten Netzwerkkanal und verwendet den Netzwerkport 3389, um die Informationen über das TCP/IP-Protokoll zu übertragen. Leider entsteht durch die Nutzung eines einzigen dedizierten Ports eine Sicherheitslücke, die Cyberkriminelle für On-Path-Angriffe nutzen können. Dazu kommt, dass bei RDP keine starken Anmeldedaten erzwungen werden, deshalb sind RDP-Systeme anfällig für den Diebstahl von Anmeldedaten und Brute-Force-Angriffe.

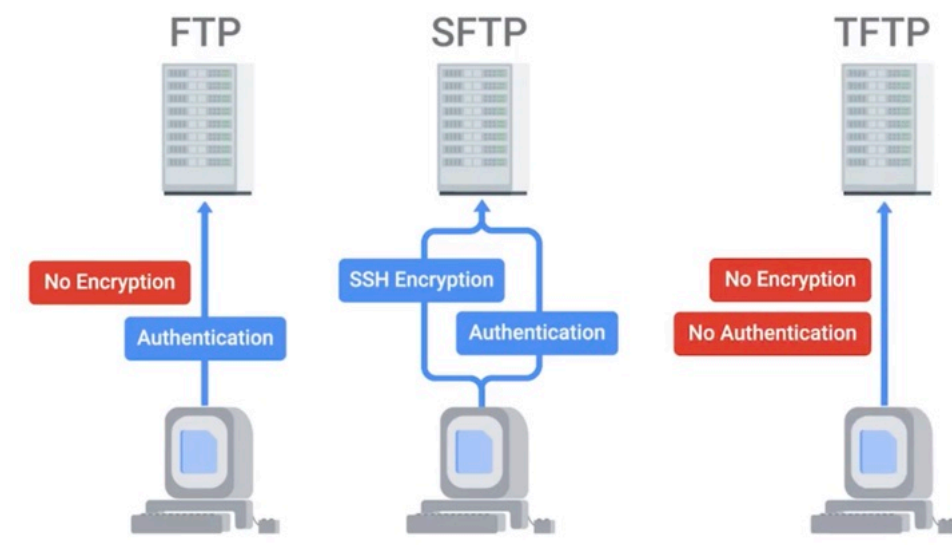
- **Virtuelles privates Netzwerk (VPN):** VPNs werden oft als eine Art privater Tunnel durch das öffentliche Internet beschrieben. Über VPNs werden verschlüsselte Internetverbindungen zwischen entfernten Computern oder Mobilgeräten und den Netzwerken eines Unternehmens hergestellt. VPNs lassen sich als Software implementieren, die auf Netzwerkservers oder Routern mit aktivierten VPN-Funktionen ausgeführt wird. Wenn sich die Mitarbeiter remote mit ihrem VPN verbinden, können sie auf das Netzwerk ihres Unternehmens zugreifen, als wären sie direkt vor Ort. Die persönliche Anwesenheit im Büro ist also nicht länger erforderlich. VPNs eignen sich gut für kleine bis mittelgroße Firmen, erfüllen aber möglicherweise nicht die Anforderungen von größeren Unternehmen. Außerdem sind VPNs keine gute Lösung für Unternehmen, die bestimmten Personengruppen wie z. B. Auftragnehmern oder Anbietern eingeschränkten Netzwerkzugang zur Verfügung stellen müssen.

### Drittanbieter-Tools

- **Integrierte Anwendungen für Videokonferenzen, Bildschirmfreigabe und Desktopverwaltung:** Videokonferenz-Tools wie Google Meet, Zoom, Microsoft Teams oder Skype werden immer beliebter, da sie die Remote-Arbeit unterstützen. Bei einer Videokonferenz können sich zwei oder mehr Personen in einer virtuellen Umgebung quasi von Angesicht zu Angesicht treffen. Einige Videokonferenz-Apps bieten außerdem Tools zur Bildschirmfreigabe, Remote-Desktopsteuerung, Umfragetools, Textnachrichten, Sitzungsprotokolle, Webinar-Verwaltungsoptionen, Sitzungsaufzeichnungen und mehr. Die wachsende Beliebtheit dieser Tools für die Remote-Arbeit geht leider auch mit einer Zunahme von damit zusammenhängenden Cyberangriffen einher. Glücklicherweise aktualisieren und patchen die wichtigsten Anbieter von Videokonferenzsoftware ihre Anwendungen kontinuierlich, um auf diese Angriffe zu reagieren.
- **Plattformen zur Dateifreigabe und Übertragung:** Cloud-Speicher-Plattformen wie Google Drive, Microsoft OneDrive und Dropbox haben File Transfer Protocol-Tools (FTP) weitgehend ersetzt. Die Dateifreigabe über eine Cloud-Plattform bietet zahlreiche Vorteile, darunter asynchrone Dateiübertragungen, Verschlüsselung von Dateiübertragungen und Daten, anpassbare Sicherheits- und Authentifizierungseinstellungen sowie die Möglichkeit, mehreren Nutzern gleichzeitig Zugriff auf Dateien zu gewähren. Dateieigentümer können einzelne Dateien, Ordner oder ganze Laufwerke freigeben. Für Unternehmen, die bestimmten Datenschutzvorschriften unterliegen oder andere Sicherheitsbedenken haben, sind Cloud-Speicher-Plattformen jedoch eventuell nicht geeignet. In diesem Fall können sie weiterhin FTP-Anwendungen auf der Basis von SSH- oder HTTPS-Protokollen nutzen, um Dateien sicher über das Internet zu übertragen.

# FTP, SFTP, und TFTP (Dateiübertragungsdienste)

- **FTP**: Dies ist ein altes Verfahren zur Übertragung von Dateien von einem Computer zu einem anderen über das Internet, das heute noch verwendet wird
- Es ist kein besonders sicheres Verfahren zur Übertragung von Daten, da es keine Datenverschlüsselung gibt
- Der FTP-Dienst funktioniert sehr ähnlich wie unser SSH-Dienst -> Clients, die Zugriff auf einen FTP-Server möchten, müssen einen FTP-Client installieren
- Auf dem FTP-Server installieren wir die Software, mit der wir Informationen teilen können, die sich in einem Verzeichnis auf jenem Server befinden
- FTP wird heute hauptsächlich für das Teilen von Webinhalten benutzt
- Wenn Sie einen Website-Host-Anbieter nutzen, sehen Sie vielleicht, dass dort bereits eine FTP-Verbindung zur Verfügung steht -> Damit können Dateien auf und von Ihrer Website kopiert werden
- **SFTP** ist eine sichere Version von FTP, es ist also sinnvoll, diese Option anstelle von FTP zu wählen
- Während dieses SFTP-Prozesses werden Daten durch SSH gesendet und verschlüsselt
- **TFTP** steht für Trivial FTP -> Es ist eine einfachere Methode der Dateiübertragung als mit FTP -> TFTP verlangt keine Nutzerauthentifizierung wie FTP, also sollten hier gespeicherte Dateien allgemeiner Natur und nicht sicher sein müssen
- Eine beliebte Verwendung von TFTP ist das Hosten von Installationsdateien



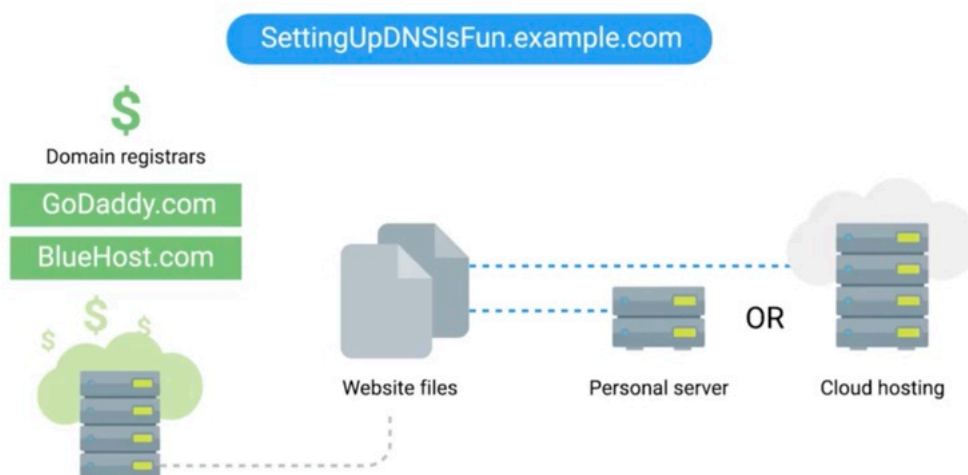
- Eine Methode zum Booten eines Computers, die wir noch nicht besprochen haben, ist PXE oder Pixie Boot, das für Preboot Execution steht -> Damit können Sie von Software booten, die über das Netzwerk verfügbar ist.
- PXE ermöglicht es, Computer ohne lokal installierte Software direkt über das Netzwerk zu starten und zum Beispiel ein OS zu installieren oder Diagnosen durchzuführen

## Intranet und Proxy-Server

- Ein Intranet ist ein internes Netzwerk innerhalb eines Unternehmens, Der Zugriff ist nur aus dem Unternehmensnetzwerk möglich
- Proxyserver fungieren als Vermittler zwischen dem Firmennetzwerk und dem Internet
- Sie empfangen den Netzwerkverkehr und leiten ihn an das Firmennetzwerk weiter

- Auf diese Weise bleibt der Datenverkehr im Firmennetzwerk vom Internet geschützt
- Das Internet erhält den Datenverkehr über einen Proxyserver, weiß aber nicht, woher er stammt
- Es kennt nur den Proxy. Proxyserver können auch eingesetzt werden, um firmeninterne Netzaktivitäten zu überwachen und zu protokollieren
- Sie können so konfiguriert werden, dass der Zugriff auf bestimmte Websites blockiert wird
- Proxyserver sind nützlich, um Datenschutz und Sicherheit im Internet zu gewährleisten und den Zugang im Unternehmen zu regeln

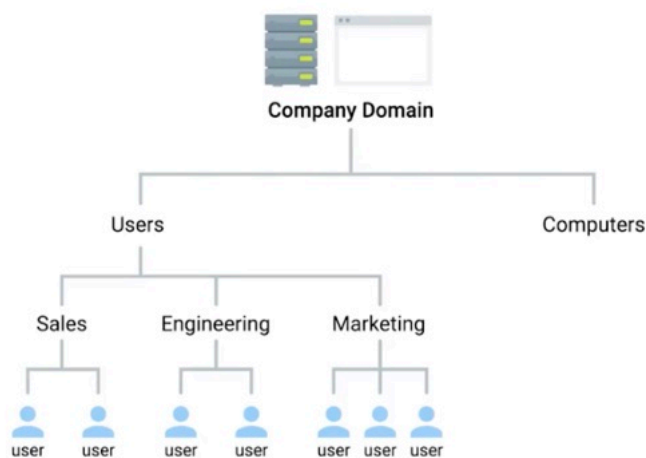
## DNS-Server



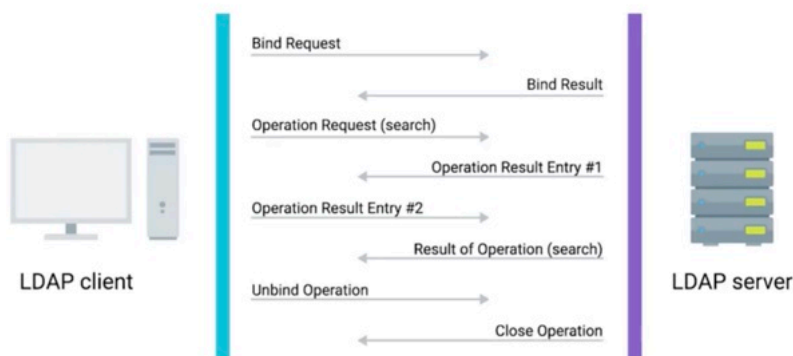
- Der andere Grund, einen eigenen DNS-Server zu verwenden, ist, damit wir unsere internen Computer zu IP-Adressen zuordnen können -> So können wir auf einen Computer mit dem Namen statt der IP-Adresse verweisen
- Unter Linux heißt unsere Hostdatei „etc/hosts“
- Wir können einen lokalen DNS-Server einrichten, mit der Zuordnung aller Computernamen der Organisation zu ihren jeweiligen IP-Adressen
- Das ist ein zentraler Speicherort für diese Informationen
- Dann ändern wir die Netzwerkeinstellungen für alle unsere Computer so, dass sie diesen DNS-Server verwenden, nicht den von unserem Internetanbieter
- Lftp ist ein ftp-Client-Programm, um einen ftp-Server zu verbinden
- dnsmasq, ein Programm, dass DNS-, DHCP-, TFTP- und PXE-Dienste in einem einfachen Paket bereitstellt

## Verzeichnisserver (Directory Server)

- Ein Verzeichnisserver bietet einen Suchdienst, der Netzwerkressourcen mit ihren Adressen verknüpft
- Er dient dazu, verschiedene Dinge zu organisieren und zu suchen, darunter zum Beispiel Nutzerkonten, Nutzergruppen Telefonnummern und freigegebene Netzwerkordner
- Anstatt Nutzerkonten und Computerdaten lokal auf jedem Rechner zu verwalten, kann man diese Daten zentral auf einem Verzeichnisserver speichern und verwalten
- Verzeichnisdienste erleichtern die Verwaltung und den Zugriff auf Daten in der Organisation
- Dies funktioniert mit einer Hierarchie aus Objekten und Containern. Die Container werden Organisationseinheiten, kurz OE, genannt
- OEs können Objekte oder weitere Organisationseinheiten enthalten
- Es funktioniert ganz ähnlich wie bei einem Dateisystem
- OEs sind wie Ordner, die Dateien oder Objekte für den Verzeichnisdienst enthalten können



- Sie könnten zum Beispiel strengere Passwortregeln für Engineering einstellen, ohne Auswirkung auf die anderen Teams
- Untergeordnete OEs erhalten alle Eigenschaften der übergeordneten OEs. Änderungen an der „Users“-OE werden auch auf „Sales“, „Marketing“ und „Engineering“ angewendet
- LDAP, oder „Lightweight Directory Access Protocol“
- LDAP dient zum Zugreifen auf Verzeichnisdienste über ein Netzwerk. Die zwei beliebtesten Verzeichnisdienste, die LDAP verwenden, sind Active Directory und Open LDAP
- Ein LDAP-Eintrag ist eine Sammlung von Informationen zu einem bestimmten Objekt
- **Bind operation:** Mit dieser werden Clients beim Verzeichnisserver authentifiziert



- Es gibt drei Authentifizierungsmethoden: „Anonym“, „Einfach“ und „SASL“, oder „Simple Authentication and Security Layer“
- Die SASL-Methode erfordert, dass der Client und der Verzeichnisserver eine Authentifizierung durchführen. Eine der meistgenutzten Authentifizierungsmethoden hierfür ist „**Kerberos**“
- Kerberos ist ein Netzwerkauthentifizierungsprotokoll zur Identitätsauthentifizierung, Sicherung der Übertragung von Anmeldedaten und vieles mehr

## ADAC



### Was ist Active Directory?

**Active Directory (AD)** ist wie das **Telefonbuch + Ausweisstelle + Türsteher** in einem großen Unternehmen.

Stell dir vor, du arbeitest bei einer Firma mit 100 Mitarbeitern und vielen Computern. Ohne AD müsste man auf jedem PC **alle Benutzer manuell anlegen**, Passwörter verwalten, Rechte vergeben ... das wäre total umständlich!



Deshalb gibt's **AD**, das zentral alles steuert:

- Wer darf sich anmelden?
- Wer darf auf welchen Ordner zugreifen?
- Welche Regeln gelten für PCs?
- Wer ist in welcher Abteilung?



### Beispiel 1: Anmeldung am Firmen-PC

Du kommst morgens ins Büro, setzt dich an deinen PC, gibst **Benutzername + Passwort** ein. Was passiert?



Dein PC fragt den **Active Directory Server (Domain Controller)**:

„Hey, darf **Anna Müller** sich anmelden?“

- Wenn ja: Du kommst rein.
- Wenn nein (z. B. falsches Passwort oder kein Konto mehr): Kein Zugriff.



**AD prüft zentral, ob du ein gültiger Benutzer bist.**



### Beispiel 2: Auf Dateien zugreifen



Dein Kollege will auf einen Ordner „**Gehaltsdaten**“ zugreifen.  
Er klickt drauf – aber AD merkt: Dieser Benutzer ist **nicht in der Personalabteilung** → kein Zugriff.

📌 **AD steuert, wer worauf Zugriff hat – auf Dateien, Drucker, Freigaben etc.**

### 🖥️ **Beispiel 3: Neuen PC einrichten**

Ein neuer Mitarbeiter bekommt einen Laptop.

- Der IT-Admin schließt den PC ans Netzwerk an
- „Join Domain“ = der PC wird bei AD angemeldet
- Jetzt gelten automatisch:
  - Firmenrichtlinien
  - Sicherheitsregeln
  - Benutzerrechte

🔄 Der PC ist jetzt **Teil der Firma**, wie ein registriertes Auto mit Nummernschild.

### 🌳 **Wie ist AD aufgebaut?**

AD ist wie ein **Stammbaum** oder eine **Ordnerstruktur**:

- **Domain** = z. B. `firma.de` → das ganze Netzwerk
- **OU (Organisationseinheiten)** = z. B. „IT“, „HR“, „Marketing“
- **Benutzer / Computer** = als Objekte darin

➡ **Beispiel:**

Anna Müller ist in der OU „HR“, hat Rechte auf Personalordner – aber nicht auf „IT-Tools“.

### 🖥️ **Domain Controller (DC) – das Herzstück**

Der **Domain Controller** ist der Server, auf dem AD läuft.

- Speichert die **Benutzerdatenbank**
- Prüft **Passwörter**
- Entscheidet über **Zugriffsrechte**
- Hält alles auf dem neuesten Stand durch **Replikation** (mehrere DCs synchronisieren sich)

Ohne DC könnte sich niemand anmelden oder arbeiten.

### **Geht das auch mit anderen Systemen?**

Ja! Obwohl AD von Microsoft ist, kann es dank dem **LDAP-Protokoll** auch mit:

- **Linux-Servern**
- **macOS**
- Druckern
- Cloud-Diensten

### **Merk dir:**

<b>Ohne AD</b>	<b>Mit AD</b>
Jeder PC hat eigene Nutzer	Alle PCs nutzen zentrale Nutzer
Manuelle Einrichtung	Automatische Konfiguration
Viele Passwörter überall	Ein Login für alles
Keine zentrale Steuerung	GPOs: zentrale Richtlinien

# Security

## CIA Triade

- Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availability (Verfügbarkeit)
- **Vertraulichkeit** bedeutet, Dinge geheim zu halten -> in der IT bedeutet es, vorhandene Daten sicher vor unbefugten Augen zu verbergen
- Eine bestimmte Methode der Vertraulichkeit, die Sie wohl täglich anwenden, ist Passwortsicherung
- **Integrität** bedeutet, dass unsere Daten präzise und unverändert bleiben
- Die Daten, die wir senden oder empfangen, müssen während ihrer gesamten Reise unverändert bleiben
- **Verfügbarkeit** bedeutet, dass die vorhandenen Informationen schnell für die Personen zugänglich sein müssen, die sie haben sollen
- Das kann viel bedeuten -> Etwa, auf Datenverlust oder einen Systemausfall vorbereitet zu sein.

## Grundbegriffe der Sicherheit

- **Risiko**: Die Möglichkeit eines Verlustes und eines Angriffs auf das System
- **Schwachstellen**: ein Mangel im System, der zu dessen Schädigung ausgenutzt werden kann -> Schwachstellen können Lücken sein, die Ihnen bewusst sind oder nicht
- **Zero-Day-Schwachstelle**, auch **Zero-Day-Lücke** genannt: kennt der Softwareentwickler oder Anbieter nicht, der Angreifer aber schon -> Der Name bezieht sich auf die Zeit, die der Softwarehersteller hatte, um zu reagieren und den Fehler zu korrigieren: null Tage
- **Exploit**: Software, die dazu dient, Sicherheitsfehler oder Schwachstellen auszunutzen
- Angreifer schreiben Exploits auf Schwachstellen zu, die sie in Software finden, um das System zu schädigen -> Angreifer entdeckt eine Zero-Day-Schwachstelle, entschließt sich, diesen zuvor unbekannten Fehler auszunutzen und schreibt einen Zero-Day-Exploit-Code
- **Bedrohung**: die Möglichkeit einer Gefahr, die eine Schwachstelle ausnutzen könnte. Bedrohungen sind nur mögliche Angreifer, etwa wie Einbrecher
- Hacker: jemand, der versucht, in Systeme einzudringen oder sie auszunutzen
- 2 Arten: Die Black-Hats, die versuchen, in böswilliger Absicht auf Systeme zuzugreifen und White-Hats, die nach Schwachstellen im System suchen, aber sie den Systembesitzern melden, damit diese sie korrigieren können, bevor andere Schaden anrichten
- **Angriff**: ein tatsächlicher Versuch, einem System zu schaden -> Es ist extrem wichtig, dass Ihnen mögliche Bedrohungen und Schwachstellen Ihres Systems bewusst sind, um sich auf sie vorbereiten zu können

## Malware

- **Malware**: Art von Schadsoftware, die dazu dient, Ihre sensiblen Daten zu erlangen oder Dateien zu löschen oder zu ändern -> Am häufigsten begegnen wir Malware der Arten Virus, Wurm, Adware, Spyware, Trojaner, Rootkit, Backdoor, Botnet
- Bei **Computerviren** heftet sich das Virus an ausführbaren Code, wie etwa ein Programm
- Bei der Ausführung kommt das Programm mit vielen Dateien in Kontakt, die nun alle für eine Ansteckung mit dem Virus empfänglich sind
- **Würmer** sind autark und verbreiten sich über Kanäle wie ein Netzwerk. Ein Fall eines berühmten Computerwurms war der I-Love-You- oder Love-Bug, der sich über Millionen von Windows-Computern ausbreitete -> Der Wurm wurde per E-Mail verbreitet

- **Adware** ist einfach Software, die Werbung anzeigt und Daten sammelt -> manchmal laden wir gezielt Adware herunter
- Ein **Trojaner** ist Malware, die sich als etwas Bestimmtes ausgibt, aber etwas anderes tut
- Genau wie das historische Trojanische Pferd von den Trojanern in die Stadt hereingelassen wurde, muss ein Computer-Trojaner vom Nutzer angenommen werden, das heißt, das Programm muss vom Nutzer ausgeführt werden
- **Spyware** ist eine Art der Malware, die Sie ausspionieren soll
- Das könnte heißen, Ihre Computerbildschirme, Tastatureingaben oder Webkameras zu überwachen und all diese Daten an Dritte weiterzuleiten
- Ein **Keylogger** ist eine häufig genutzte Art der Spyware, die jede Taste aufzeichnet, die Sie drücken -> Er kann zum Beispiel alle Nachrichten, die Sie schreiben, Ihre vertraulichen Daten und Ihre Passwörter erfassen
- Ransomware greift auf eine Art an, bei der Ihre Daten oder Ihr System für Sie unzugänglich gemacht werden, bis Sie eine Art Lösegeld bezahlen
- Es gibt Malware, die anhand eines fremden Computers eine vom Angreifer zentral gesteuerte Aufgabe ausführt -> Die betroffenen Rechner nennt man **Bots**
- Bei einer Gruppe von mehreren Bots bezeichnen wir dieses Netzwerk als **Botnetz**
- Botnetze sind darauf ausgerichtet, die Leistung der per Internet verbundenen Rechner für verteilte Operationen zu nutzen (Zum Beispiel das Mining von Bitcoins)
- **Backdoors** werden meistens installiert, nachdem ein Angreifer Zugang zu Ihrem System erlangt hat und diesen Zugang behalten möchte
- Ein **Rootkit** ist, wie der Name schon sagt, ein Kit für root, also eine Sammlung von Software oder Tools, die normalerweise ein Admin benutzt
- Es ermöglicht Änderungen am Betriebssystem auf Administratorebene
- Ein Rootkit erkennt man oft schwer, da es das System nutzt, um sich vor diesem zu verstecken
- Eine **Logikbombe** ist eine Art der Malware, die absichtlich installiert wird -> Nach einem bestimmten Ereignis oder einer bestimmten Zeit führt sie ein Schadprogramm aus

## Netzwerkangriffe

- Beim **DNS-Cache-Poisoning** wird ein DNS-Server dazu gebracht, gefälschte DNS-Einträge anzunehmen, die auf einen kompromittierten DNS-Server verweisen
- Beim versuchten Zugriff auf legitime Websites werden dann falsche DNS-Adressen eingespeist
- Nicht nur das -> DNS-Cache-Poisoning kann sich auch auf andere Netzwerke ausbreiten
- Wenn andere DNS-Server ihre DNS-Informationen von einem kompromittierten Server beziehen, geben sie diese falschen DNS-Einträge an andere Hostrechner weiter
- Vor einigen Jahren kam es in Brasilien zu einem groß angelegten DNS-Cache-Poisoning
- Es scheint, dass Angreifer in der Lage waren, den DNS-Cache lokaler ISPs zu kompromittieren, indem sie gefälschte DNS-Einträge für beliebte Websites wie Google, Gmail oder Hotmail einschleusten
- Wenn Nutzer versuchten, eine dieser Seiten aufzurufen, erhielten sie einen gefälschten DNS-Eintrag und wurden an einen Server unter der Kontrolle der Angreifer geleitet, der ein kleines Java-Applet bereitstellte
- Die Nutzer wurden dann dazu gebracht, das Applet zu installieren, das tatsächlich ein Trojaner war, der Zugangsdaten für Online-Banking stahl
- Ein **Man-in-the-Middle-Angriff** ist ein Angriff, bei dem der Angreifer zwischen zwei Hosts steht, die glauben, direkt miteinander zu kommunizieren
- Ein üblicher MITM-Angriff ist das **Session-Hijacking oder Cookie-Hijacking**

- Sagen wir, Sie melden sich bei einer Website an, aber nicht ab -> Sie haben sich also bereits gegenüber der Website authentifiziert und ein Sitzungstoken generiert, das Ihnen Zugriff auf diese Website gewährt
- Wenn jemand Session-Hijacking durchführen würde, könnte er dieses Token stehlen und sich auf der Website als Sie ausgeben
- MITM-Angriffe können auch über einen Angriff mit **gefälschtem Zugangspunkt** erfolgen
- Ein gefälschter Zugangspunkt ist einer, der im Netzwerk installiert wird, ohne, dass der Netzwerkadministrator es weiß
- Beim Evil-Twin-Angriff verbinden Sie sich mit einem Netzwerk, das identisch mit Ihrem ist
- Das identische Netzwerk ist der **böse Zwilling (Evil Twin)** unseres Netzwerks und wird vom Angreifer kontrolliert

## Denial of Service Angriff

- bei einem DoS-Angriff wird versucht, den Zugriff auf einen Dienst für legitime Nutzer zu verhindern, indem das Netzwerk oder der Server überlastet wird
- DoS-Angriffe brauchen die Ressourcen dieser Dienste auf und blockieren den Zugriff echter Nutzer
- Der Ping of Death oder POD ist ein Beispiel für einen ziemlich simplen DoS-Angriff
- Dabei wird ein fehlerhafter Ping an einen Computer gesendet
- Der Ping wäre größer, als es das Internetprotokoll handhaben kann
- Das führt zu einem Pufferüberlauf
- Dadurch kann das System abstürzen und potenziell die Ausführung von bösartigem Code ermöglichen
- Ein anderes Beispiel wäre die Ping-Flood, in der unzählige Ping-Pakete an ein System gesendet werden
- Genauer gesagt werden ICMP-Echo-Anfragen gesendet, da ein Ping eine gleiche Anzahl von ICMP-Echo-Antworten erwartet
- Bei einer **SYN-Flood** wird der Server mit SYN-Paketen bombardiert
- Der Server sendet SYN-Bestätigungspakete zurück, aber der Angreifer sendet keine Bestätigungsnachrichten
- Dadurch bleibt die Verbindung offen und verbraucht die Ressourcen des Servers
- **XSS-Angriffe** sind eine Art von Injection-Angriff, bei dem der Angreifer bösartigen Code einfügt und den Nutzer des Dienstes angreift
- werden häufig für Session-Hijacking verwendet -> Dabei kann ganz simpel ein bösartiges Skript in eine Website eingebettet werden und der ahnungslose Nutzer führt das Skript in seinem Browser aus
- Das Skript könnte dann die Cookies eines Opfers stehlen und auf die Anmeldung bei einer Website Zugriff haben
- Eine weitere Art von Injection-Angriff ist der **SQL-Injection-Angriff**
- Während ein XSS-Angriff einen Nutzer ins Visier nimmt, wird bei der SQL-Injection die ganze Website angegriffen, falls diese eine SQL-Datenbank verwendet
- Angreifer können potenziell SQL-Befehle ausführen lassen, mit denen sie Websitedaten löschen oder kopieren können und andere bösartige Befehle ausführen


## Passwort-Angriff










- Software wie etwa Passwort-Cracker wird eingesetzt, mit denen das Passwort erraten werden soll

- Brute-Force-Angriff, bei dem kontinuierlich verschiedene Kombinationen von Zeichen und Buchstaben ausprobiert werden. Da dabei sehr viele Passwortkombinationen getestet werden müssen, dauert diese Art von Angriff meist recht lange
- Wenn Sie bei einem Passwort-Angriff kein CAPTCHA haben, kann ein automatisiertes System die Anmeldung so lange versuchen, bis es die richtige Passwortkombination gefunden hat
- Ein CAPTCHA kann diese Angriffe abwehren

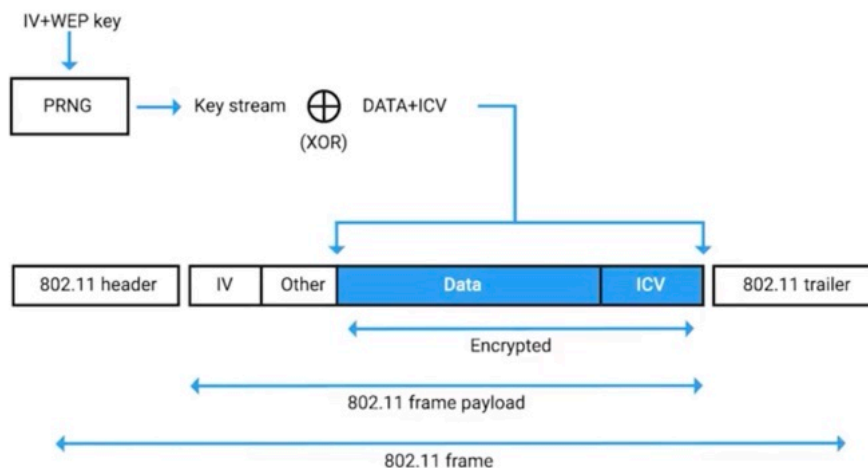
## Symmetrische Verschlüsselung

### Kryptografie

- Eine Chiffre besteht aus zwei Komponenten, dem Verschlüsselungsalgorithmus und dem Schlüssel
- Der Verschlüsselungsalgorithmus ist die zugrunde liegende Logik oder der Prozess, der zum Umwandeln von Klartext in Geheimtext verwendet wird
- Zuerst entscheidet man sich für einen Verschlüsselungsalgorithmus zur Nachrichtencodierung, dann wählt man einen Schlüssel
- Nun hat man eine Chiffre, die man auf den Klartext anwenden kann, sodass man einen verschlüsselten Geheimtext erhält, den man in alle Welt versenden kann, geschützt vor neugierigen Blicken
- Kerckhoffs' Prinzip: Ein Kryptosystem oder eine Sammlung von Algorithmen zur Schlüsselgenerierung und zum Verschlüsseln und Entschlüsseln, die einen kryptografischen Dienst bilden, sollen sicher bleiben, auch wenn alle Informationen über das System, mit Ausnahme des Schlüssels, bekannt sind
- Das bedeutet, dass selbst wenn Ihr Gegner den genauen Verschlüsselungsalgorithmus kennt, mit dem Sie Ihre Daten sichern, kann er trotzdem nicht den Klartext aus einem abgefangenen Geheimtext wiederherstellen
- Eine Substitutionschiffre ist ein Verschlüsselungsmechanismus, bei dem Teile des Klartextes mit Geheimtexten ersetzt werden
-  Blockverschlüsselung (Block Cipher)
- Prinzip:  
Die Daten werden in Blöcke fester Länge (z. B. 64 oder 128 Bit) unterteilt. Jeder Block wird einzeln mit demselben Schlüssel verschlüsselt.
- Beispiel: AES (Advanced Encryption Standard), DES.
- Eigenschaften:
- Arbeitet blockweise (z. B. 128-Bit-Blöcke).
- Kann in verschiedenen Modi betrieben werden (z. B. ECB, CBC, etc.).
- Gut für strukturierte Daten wie Dateien.
- Vergleich:  
Wie wenn du ein Buch in Kapitel aufteilst und jedes Kapitel einzeln verschlüsselst.

-  Stromchiffre (Stream Cipher)
- Prinzip:  
Die Daten werden Bit für Bit oder Byte für Byte verschlüsselt, oft mit einem pseudozufälligen Schlüsselstrom, der mit dem Klartext verodert (XOR) wird.
- Beispiel: RC4, Salsa20.
- Eigenschaften:
  - Arbeitet zeichenweise.
  - Schneller bei Datenströmen wie Audio- oder Videoübertragung.
  - Gut für Echtzeitanwendungen (z. B. verschlüsselte Sprachübertragung).
- Vergleich:  
Wie wenn du ein Gespräch Wort für Wort verschlüsselst, während du sprichst – in Echtzeit.
-  Was ist eine Stromchiffre – einfach erklärt?
- Stell dir vor, du willst eine Sprachnachricht verschlüsseln. Du benutzt eine Stromchiffre, die jede Sekunde deines gesprochenen Textes einzeln in eine geheime Sprache übersetzt.  
Das heißt: Du verschlüsselst Zeichen für Zeichen (statt ganze Absätze auf einmal wie bei Blockverschlüsselung).
-  Was ist das Problem bei Stromchiffren?
- Damit das Ganze sicher ist, brauchst du einen Schlüsselstrom – also eine Folge von geheimen Zeichen, mit denen du deinen Text verschlüsselst (zum Beispiel durch XOR).
- Aber:
  -  Wenn du denselben Schlüsselstrom zweimal verwendest, kann ein Angreifer den Text entschlüsseln!  
Das wäre wie wenn du dieselbe Geheimsprache für mehrere Nachrichten nutzt – und jemand merkt sich die Muster.
-  Was ist ein Initialisierungsvektor (IV)?
- Ein IV ist wie ein Zufallswert, den du zum Masterschlüssel hinzufügst, um jedes Mal einen neuen Schlüsselstrom zu erzeugen – auch wenn der Masterschlüssel gleich bleibt.
-  Du hast also:  
Masterschlüssel + IV  $\Rightarrow$  einmaliger Schlüsselstrom
-  Der IV wird im Klartext mitgeschickt (also unverschlüsselt), damit der Empfänger denselben Schlüsselstrom generieren und die Nachricht entschlüsseln kann.
-  Beispiel aus der Praxis: WEP (WLAN)
- WEP ist ein (unsicherer) alter WLAN-Standard. Wenn du Daten per WEP sendest:
  - Deine Nachricht wird per Stromchiffre verschlüsselt.
  - Der IV wird vor die verschlüsselten Daten gepackt und mitgesendet – im Klartext.
  - Der Empfänger nutzt Masterschlüssel + IV  $\Rightarrow$  entschlüsselt den Datenstrom.
- Problem:  
WEP hat nur 24-Bit-IVs – also nicht genug Kombinationen  $\rightarrow$  Wiederverwendung passiert oft  $\rightarrow$  Hacker können den Schlüssel knacken.
-  Zusammengefasst:
  - Stromchiffre = Zeichenweise Verschlüsselung (schnell, leicht).
  - Gefährlich, wenn derselbe Schlüsselstrom mehrmals verwendet wird.
  - IV = Zufallswert, macht jeden Schlüsselstrom einzigartig.

- IV wird mitgesendet, damit Empfänger entschlüsseln kann.
- Beispiel: WEP zeigt, was passiert, wenn IVs zu schwach oder wiederverwendet werden → unsicher.



Die Grafik zeigt anschaulich, wie WEP mit Stromchiffre und IV funktioniert – aber auch, warum WEP als unsicher gilt:

- IV ist zu kurz
- Nur Teile der Daten sind verschlüsselt
- Wiederverwendung des IVs führt zu Angreifbarkeit


☞ Deshalb wurde WEP durch WPA und WPA2 ersetzt – mit sichereren Verfahren wie AES und CBC.

- **Bei symmetrischen Verschlüsselungsalgorithmen wird derselbe Schlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln verwendet**
- Die Schlüssellänge ist in der Kryptografie extrem wichtig, da durch sie die maximal mögliche Sicherheit des Systems definiert wird.
- **AES** ist auch die erste und einzige öffentliche Chiffre, die zur Verwendung für streng geheime Daten durch die National Security Agency der USA zugelassen ist
- AES ist auch eine symmetrische Blockverschlüsselung, ähnlich wie DES, der dadurch ersetzt wurde
- Aber AES verwendet 128-Bit-Blöcke, zwei Mal so groß wie DES-Blöcke, und unterstützt Schlüssellängen von 128 Bit, 192 Bit und 256 Bit
- Wegen der großen Schlüsselgröße sind Brute-Force-Angriffe gegen AES derzeit nur eine theoretische Möglichkeit, da die Rechenzeit selbst mit moderner Computertechnik nicht praktikabel ist
- **es ist zu betonen, dass diese Algorithmen die Konzeption der Chiffren selbst darstellen -> Diese Konzeptionen müssen dann in die Soft- oder Hardware implementiert werden, damit die Verschlüsselungsfunktionen angewendet werden können**
- Idealerweise sollte ein Algorithmus nicht zu schwierig zu implementieren sein, denn ansonsten kann das wegen Bugs in der Implementation zu Fehlern und Verlust des Schutzes führen
- Je schneller kryptographische Verfahren erledigt werden können und je geringer die Auslastung des Systems, desto besser



- -> Deswegen werden bei manchen Plattformen diese kryptografischen Algorithmen in die Hardware integriert, um den Prozess zu beschleunigen und die Beanspruchung der CPU zu verringern
- Beispielsweise sind bei modernen CPUs von Intel und AMD die AES-Instruktionen direkt in der CPU integriert
- Das ermöglicht viel größere Rechengeschwindigkeiten und mehr Effizienz bei der Ausführung von kryptografischen Prozessen
- **TLS 1.2 mit AES-GCM kombiniert** hohe Sicherheit, Geschwindigkeit und Datenintegrität. Der GCM-Modus erzeugt dabei einen sicheren Schlüsselstrom mit einem Zähler, den man niemals wiederverwenden darf. So wird aus einer Blockchiffre eine Art „Stromchiffre“ – aber eben richtig sicher.

## Asymmetrische Verschlüsselung oder Verschlüsselung mit öffentlichem Schlüssel


-  Was ist asymmetrische Kryptografie?
- Asymmetrische Kryptografie (auch Public-Key-Kryptografie) ist ein Verfahren, bei dem zwei unterschiedliche, aber zusammengehörige Schlüssel verwendet werden:
- Ein öffentlicher Schlüssel (public key) → darf jeder sehen
- Ein privater Schlüssel (private key) → muss geheim bleiben

### Nachricht senden (Verschlüsselung):

Wenn Suzanne eine Nachricht an Daryll senden will:

Sie verschlüsselt die Nachricht mit Darylls öffentlichem Schlüssel

Nur Darylls privater Schlüssel kann diese Nachricht wieder entschlüsseln

 So bleibt die Nachricht vertraulich, auch wenn sie abgefangen wird

### Nachricht unterschreiben (Digitale Signatur):

Wenn Suzanne möchte, dass Daryll sicher weiß, dass die Nachricht wirklich von ihr stammt:

Sie erstellt eine digitale Signatur mit ihrem privaten Schlüssel

Daryll kann mit Suzannes öffentlichem Schlüssel überprüfen, ob die Signatur gültig ist

 Damit ist klar: Suzanne hat die Nachricht wirklich geschrieben und sie wurde nicht verändert

Asymmetrische Kryptografie bietet drei wichtige **Sicherheitsprinzipien**:

Prinzip	Beschreibung
<b>Vertraulichkeit</b>	Nur der Empfänger kann lesen, was gesendet wurde
<b>Authentizität</b>	Die Quelle der Nachricht kann bestätigt werden
<b>Nachweisbarkeit</b>	Der Sender kann später nicht bestreiten, die Nachricht gesendet zu haben



Kurzform mit Analogie:

**Öffentlicher Schlüssel = Briefkasten (jeder darf etwas einwerfen)**

**Privater Schlüssel = Briefkastenschlüssel (nur du kannst die Post rausholen)**

**Digitale Signatur = Unterschrift mit deinem Siegel, die nur du erzeugen kannst**

- es gibt auch die Kombination aus beidem (geheimer Schlüssel wird über asymmetrische Kryptographie übergeben)

### **Warum man oft beide kombiniert**

- Asymmetrische Verschlüsselung ist sicher, aber langsam und braucht viel Rechenleistung.
- Symmetrische Verschlüsselung ist schnell und effizient, besonders bei großen Datenmengen.
- Deshalb kombiniert man beides:
- Zuerst wird mit asymmetrischer Verschlüsselung der symmetrische Schlüssel sicher ausgetauscht (also "geschützt übermittelt").
- Danach verschlüsselt man die eigentlichen Nachrichten schnell und effizient mit symmetrischer Verschlüsselung.

### **Was sind MACs (Message Authentication Codes)?**

- MACs sind eine Art Prüfsumme, mit der du sicherstellst, dass eine Nachricht wirklich vom Absender kommt und unterwegs nicht verändert wurde.
- Wichtig: Der gleiche geheime Schlüssel wird zum Erstellen und Prüfen des MAC benutzt (deshalb ist es ein symmetrisches Verfahren).
- Dadurch kann man Nachrichten authentifizieren und die Integrität sichern.

### **HMAC**

- HMAC ist eine sichere Form von MAC, die einen geheimen Schlüssel und eine Hash-Funktion (z. B. SHA-1 oder MD5) kombiniert.
- Beispiel:
- Sender macht aus Nachricht + Schlüssel einen HMAC und schickt ihn mit der Nachricht.
- Empfänger macht dasselbe (aus Nachricht + Schlüssel) und vergleicht die Werte. Stimmen sie überein, ist die Nachricht echt und unverändert.

### **CMAC und CBC-MAC**

- Statt Hash-Funktionen kann man auch symmetrische Verschlüsselungen (wie AES oder DES) nutzen, um einen MAC zu erzeugen — das nennt man CMAC.
- Ein spezielles Verfahren dafür ist CBC-MAC:
- Die Nachricht wird blockweise verschlüsselt, wobei jeder Block mit dem vorherigen "verkettet" wird.
- Am Ende entsteht ein Wert, der sich bei jeder Änderung in der Nachricht ändert, so erkennt man Manipulationen.

### **Kurz gesagt:**

- **Asymmetrisch: Gut, um Schlüssel sicher zu tauschen.**
- **Symmetrisch: Gut, um große Daten schnell zu verschlüsseln.**
- **MACs: Gut, um sicherzugehen, dass die Nachricht echt und unverändert ist.**
- **HMAC: Ein MAC mit Hash-Funktionen.**
- **CMAC: Ein MAC mit symmetrischen Verschlüsselungen.**

## ✓ RSA

- Eines der ersten asymmetrischen Verschlüsselungsverfahren, heute noch weit verbreitet.
- Entwickelt von **Rivest, Shamir, Adleman** (daher RSA).
- Nutzt große **Primzahlen** zur Schlüsselerzeugung.
- Verwendbar für **Verschlüsselung und Signaturen**.
- Sicher, aber rechenintensiv (lange Schlüssel, z. B. 2048 oder 3072 Bit).

## ✍️ DSA (Digital Signature Algorithm)

- Dient **nur zur Signatur**, also zur Überprüfung von Authentizität.
- Wichtig: DSA braucht bei jeder Signatur einen **neuen zufälligen Wert**.
- Wenn dieser Wert **wiederverwendet** oder **vorhersehbar** ist, wird es **unsicher**.

### Beispiel:

Sony nutzte DSA bei der PlayStation 3 – aber ohne neue Zufallswerte für jede Signatur. Das führte 2010 dazu, dass Hacker ihren privaten Schlüssel herausfanden → illegale Spiele konnten signiert und gespielt werden.

## 🔄 Diffie-Hellman (DH) – für sicheren Schlüsselaustausch

- Wird verwendet, **um gemeinsam einen geheimen Schlüssel zu erzeugen**, obwohl man nur über ein öffentliches (unsicheres) Netzwerk kommuniziert.
- Funktioniert so:
  1. Beide Seiten einigen sich öffentlich auf eine große Zahl.
  2. Jede Seite wählt eine **geheime** Zahl.
  3. Dann tauschen sie berechnete Werte aus.
  4. Daraus entsteht auf beiden Seiten **derselbe geheime Schlüssel**, ohne dass jemand Drittes ihn kennt.
- DH wird **nicht** zur Verschlüsselung selbst verwendet, nur zur **Schlüsselverteilung**.

## 📈 Elliptische-Kurven-Kryptografie (ECC)

- Nutzt **mathematische Eigenschaften elliptischer Kurven** zur Verschlüsselung.
- **Vorteil:** Genauso sicher wie RSA, aber mit **viel kürzeren Schlüsseln** (z. B. 256-Bit statt 3072-Bit).

- Spart Rechenleistung und Speicher – ideal für Smartphones, Smartcards etc.

Beispiele für ECC-Varianten:

- **ECDSA** = Elliptische-Kurven-Version von DSA (Signaturen)
- **ECDH** = Elliptische-Kurven-Version von Diffie-Hellman (Schlüsseltausch)



### Wichtig für die Zukunft: Quantencomputer

- ECC und andere Systeme könnten in Zukunft durch **Quantencomputer** geknackt werden.
- Daher wird bereits an sogenannten **Post-Quanten-Kryptografien** gearbeitet.



### Zusammenfassung in einem Satz:

Asymmetrische Kryptografie (z. B. RSA, DSA, DH, ECC) ermöglicht sichere Kommunikation und Authentifizierung auch über unsichere Kanäle – sie funktioniert mit öffentlichen und privaten Schlüsseln und wird oft mit symmetrischer Verschlüsselung kombiniert, um Sicherheit und Effizienz zu verbinden.

## Was ist eine Hash-Funktion?

Eine **Hash-Funktion** ist eine Art Rechenregel, die aus **beliebigen Daten** (z. B. Text, Datei) einen **festen Ausgabewert** berechnet, den sogenannten **Hash-Wert** oder **Digest**.

- Egal wie lang der ursprüngliche Text ist – der Hash-Wert hat **immer dieselbe feste Länge**.
- Ein Beispiel:  
 „Hello World“ → E49A00FF  
 „hello world“ → FF1832AE  
 → Eine kleine Änderung der Eingabe erzeugt einen komplett **anderen Hash-Wert**.



## Wozu wird Hash-Technologie verwendet?

- ✓ **Schnelles Suchen** in Datenstrukturen (z. B. Hashtabellen)
- ✓ **Duplikate erkennen** in Datenbanken oder Archiven

- ✓ **Daten überprüfen**, ob sie verändert wurden (Integrität)
- ✓ **Authentifizierung**, z. B. bei Passwörtern
- ✓ **Digitale Signaturen & Sicherheitsprotokolle**



## Was macht eine *kryptografische* Hash-Funktion besonders?

Sie wird **nicht zum Verschlüsseln**, sondern zum **Überprüfen und Absichern von Daten** verwendet.

Eine gute kryptografische Hash-Funktion hat folgende Eigenschaften:

Eigenschaft	Bedeutung
<b>Deterministisch</b>	Gleiche Eingabe → immer gleiche Ausgabe
<b>Nicht rückrechenbar</b>	Aus dem Hash kann man die Eingabe nicht zurückrechnen
<b>Kollisionssicher</b>	Zwei unterschiedliche Eingaben dürfen <b>nie</b> den gleichen Hash ergeben
<b>Sensibel auf Änderungen</b>	Kleinste Änderung → komplett neuer Hash-Wert
<b>Schnell &amp; effizient</b>	Muss schnell berechnet werden können



## Merksatz:

**Hash-Funktionen sind digitale Fingerabdrücke** für Daten – kurz, eindeutig und nicht zurückverfolgbar.



# Was ist Hash-Technologie? Und was sind MD5, SHA1, SHA2?



## Was macht eine Hash-Funktion?

Eine **Hash-Funktion** nimmt beliebige Daten (z. B. ein Dokument) und erstellt daraus einen „Fingerabdruck“, den sogenannten **Hash-Wert**. Dieser ist:

- **immer gleich lang**, egal wie groß die Eingabe ist,
- **einzigartig** (im Idealfall),
- **nicht rückrechenbar** (man kann den Originaltext nicht aus dem Hash ableiten).



## Was ist eine Kollision?

Eine **Kollision** passiert, wenn **zwei unterschiedliche Daten dieselbe Hash-Ausgabe** erzeugen.

### Beispiel:

Datei A → Hash: ABC123

Datei B (ganz anders) → auch Hash: ABC123

→ Das ist eine **Kollision**.

Das ist gefährlich, weil man z. B. eine **schädliche Datei so tarnen kann**, dass sie **den gleichen Hash wie eine legitime Datei** hat – und so z. B. **digitale Signaturen austrickst**.



## Warum ist MD5 nicht mehr sicher?

- MD5 war früher sehr verbreitet.
- Schon **2004** entdeckte man, dass man **gezielt Kollisionen erzeugen** kann.
- 2008 konnte man sogar ein **gefälschtes SSL-Zertifikat** erstellen, das als **echt anerkannt wurde**.
- Spätestens ab 2012 wurde MD5 auch von **Malware** wie „Flame“ ausgenutzt.
- Empfehlung: **MD5 seit spätestens 2010 nicht mehr verwenden**.



## SHA1 – der Nachfolger von MD5

- SHA1 wurde 1995 veröffentlicht.
- Auch SHA1 erzeugt Hashes, ist aber etwas sicherer.

- Es wurde in **vielen Systemen** verwendet, z. B.:
  - TLS/SSL (Webverschlüsselung),
  - SSH/PGP (sichere Verbindungen),
  - Git (Versionskontrolle).
- Doch auch SHA1 ist heute **unsicher**, weil:
  - Forscher 2017 eine **echte Kollision** erzeugen konnten.
  - Dafür wurden sehr viele **Cloud-Ressourcen** verwendet.
  - Damit kann man z. B. **zwei PDF-Dateien erzeugen**, die denselben SHA1-Hash haben.

➡ **Fazit:** Auch SHA1 wird **nicht mehr empfohlen** – spätestens seit 2017.

## ✅ **Empfohlene Hash-Funktionen heute: SHA2 & SHA3**

- SHA2 (z. B. SHA-256) oder SHA3 gelten **aktuell als sicher**.
- Werden z. B. von Regierungen und Sicherheitsstandards verwendet.



## **MIC vs. MAC**

- **MIC (Message Integrity Check):**
  - Prüft, ob sich Daten **zufällig verändert** haben (z. B. bei Übertragung).
  - Kein Schutz gegen **gezielte Manipulation**, da kein Schlüssel verwendet wird.
- **MAC (Message Authentication Code):**
  - Nutzt **einen geheimen Schlüssel** → bietet auch **Authentifizierung**.
  - Sicherer als MIC.



## **Fazit in einfachen Worten:**

- Hash-Funktionen machen aus Daten einen „Fingerabdruck“.
- **Kollisionen sind gefährlich**, weil sie die Einzigartigkeit zerstören.
- **MD5 und SHA1** sind heute **unsicher**, weil man gezielt Kollisionen erzeugen kann.
- Besser: **SHA2 oder SHA3** verwenden.

- Für Sicherheit im Netz ist die Wahl der richtigen Hash-Funktion **absolut entscheidend**.



## Warum speichert man Passwörter nicht im Klartext?

- Passwörter im **Klartext zu speichern** ist **unsicher**.
- Wird die Datenbank gehackt, hätten Angreifer **direkten Zugang zu allen Passwörtern**.
- Lösung: **Nur den Hash des Passworts speichern** (z. B. mit SHA-256).
- Bei der Anmeldung wird das eingegebene Passwort **gehasht** und mit dem gespeicherten Hash verglichen.  
Stimmt beides überein → der Nutzer ist authentifiziert.



## Wie greifen Hacker Hashes an?

### 1. Brute-Force-Angriff

- Der Angreifer probiert **alle möglichen Passwörter durch**, bis ein Hash passt.
- Beispiel: „abc123“, „password“, „123456“...
- Sehr aufwendig – je nach Hash-Funktion können Milliarden Versuche nötig sein.

### 2. Rainbow-Table-Angriff

- Angreifer nutzen vorberechnete Tabellen (Rainbow Tables) mit:
  - Passworten und
  - deren Hashes (z. B. für MD5 oder SHA1)
- Vorteil für den Angreifer: **Kein Rechnen nötig**, nur Suchen.
- Nachteil: Braucht **viel Speicherplatz**.



## Wie schützt man sich dagegen? Mit „Salts“!

- **Salt = zufällige Zusatz-Daten**, die **an jedes Passwort angehängt** werden, **bevor** es gehasht wird.
- Ergebnis: **Jeder Hash ist einzigartig**, selbst wenn zwei Leute dasselbe Passwort nutzen.



 Beispiel:

vbnet

Passwort: "password123"

Salt: "Z8x!kT"

→ Kombiniert: "password123Z8x!kT"

→ Hash wird aus dieser Kombination berechnet.

- Dadurch funktioniert keine Rainbow Table mehr, weil:
  - Der Angreifer **nicht weiß, welchen Salt** du benutzt hast.
  - Er müsste **für jeden möglichen Salt-Wert** eine neue Tabelle bauen.
  - Bei z. B. **128-Bit-Salts** gibt es **über 340 Sextillionen** Möglichkeiten.



## Was ist eine Kollision?

- Eine **Kollision** tritt auf, wenn **zwei unterschiedliche Eingaben** denselben Hash-Wert erzeugen.
- Sehr gefährlich für Sicherheit:
  - Angreifer kann z. B. ein **bösartiges Dokument** erstellen, das denselben Hash wie ein **vertrauenswürdigen** hat.
- Gute Hash-Funktionen sollen **Kollisionen extrem unwahrscheinlich** machen.
  - Bei SHA-1 ist das **bereits gelungen** (→ unsicher).
  - Bei SHA-2 bisher **nicht möglich** (→ sicherer).



## Fazit – So schützt man sich richtig

- **Nie Klartext-Passwörter speichern**
- **Nur sichere Hash-Funktionen verwenden** (z. B. SHA-256, bcrypt, Argon2)
- **Salts hinzufügen** (mind. 128 Bit)
- **Mehrfache Hashing-Runden nutzen** (z. B. 10.000x wiederholen)
- Damit werden Angriffe **zu aufwendig oder wirtschaftlich unsinnig**

### MIC (Message Integrity Check):

- Nutzt nur eine **Hash-Funktion**, um sicherzustellen, dass die Nachricht **nicht verändert** wurde.
- **Keine Authentifizierung**, da **kein geheimer Schlüssel** beteiligt ist.
- Schützt **nur vor versehentlichen Fehlern, nicht vor Manipulation durch Angreifer**.

### MAC (Message Authentication Code):

- Nutzt **Hashing + geheimen Schlüssel**.
- Stellt sicher, dass die Nachricht **echt und unverändert** ist – und von einem **autorisierten Sender** stammt.
- **Bietet Integrität + Authentizität**.



### Was ist PKI?

Die **Public-Key-Infrastruktur (PKI)** ist ein System, das es ermöglicht, sichere digitale Kommunikation über das Internet aufzubauen. Sie wird verwendet, um:

- **Digitale Zertifikate zu erstellen, zu speichern und zu verwalten**
- **Öffentliche Schlüssel mit vertrauenswürdigen Identitäten zu verknüpfen**



### Was ist ein digitales Zertifikat?

Ein **digitales Zertifikat** ist wie ein digitaler Ausweis:

- Es enthält den **öffentlichen Schlüssel** einer Person oder Organisation
- Dazu Infos über den Besitzer (z. B. Website-Name)
- Und es ist **signiert von einer vertrauenswürdigen Stelle** (Zertifizierungsstelle), die bestätigt: *Ja, dieser Schlüssel gehört dieser Person/Organisation*



### Zentrale Rollen im PKI-System

- **Zertifizierungsstelle (CA):**

- Signiert und stellt Zertifikate aus
- Vertrauenswürdige Instanz (wie eine digitale Behörde)
- **Registrierungsstelle (RA):**
  - Prüft die Identität der Antragsteller
  - Oft in der CA integriert
- **Repository / Verwaltungssystem:**
  - Speichert Zertifikate
  - Macht sie auffindbar und verwaltbar

## Zertifikatstypen

1. **SSL/TLS-Serverzertifikat**
  - Wird von Webseiten verwendet, um eine **sichere Verbindung (HTTPS)** mit dem Browser herzustellen
  - Der Browser prüft, ob das Zertifikat zur Seite passt und von einer **vertrauenswürdigen CA** stammt
2. **Wildcard-Zertifikat**
  - Gilt für **alle Subdomains** einer Domain, z. B. **\*.example.com**
3. **Selbstsigniertes Zertifikat**
  - Von sich selbst signiert (nicht von CA)
  - **Nicht automatisch vertrauenswürdig**, z. B. für Testumgebungen
4. **Client-Zertifikat**
  - Wird vom **Client (z. B. Benutzergerät)** genutzt, um sich beim Server zu authentifizieren
  - Meist von privaten CAs verwaltet (z. B. in Unternehmen)
5. **Code-Signing-Zertifikat**
  - Wird verwendet, um **Software zu signieren**
  - Nutzer sehen, ob das Programm **authentisch und unverändert** ist



## Vertrauenskette

- PKI basiert auf einer **Vertrauenskette** (Trust Chain):
  - Ganz oben: **Root-Zertifizierungsstelle (Root-CA)**
    - Hat ein **selbstsigniertes Zertifikat** (weil sie die oberste Instanz ist)
  - Darunter: **Zwischenzertifizierungsstellen (Intermediate CAs)**
    - Können ebenfalls Zertifikate ausstellen
  - Ganz unten: **Endnutzerzertifikate** (z. B. für Websites)

Diese Struktur ist wie ein Baum:

- Root-CA = Wurzel
- Intermediates = Äste
- Endnutzerzertifikate = Blätter



### Warum vertraut man der Root-CA?

- Betriebssysteme und Browser **liefern Root-CA-Zertifikate vorinstalliert** mit
- Sie sind in einem sogenannten **Zertifikatsspeicher** gespeichert
- Wenn ein Zertifikat einer Webseite über eine **Vertrauenskette zur Root-CA** zurückverfolgt werden kann → wird es **als sicher akzeptiert**



### Fazit

Die **PKI** sorgt **dafür**, dass wir im Internet:

- **sicher kommunizieren können**
- **Webseiten, Software und Dienste verifizieren können**
- **öffentlich zugängliche Schlüssel vertrauensvoll verwenden können**

## X.509-Zertifikate – Aufbau und Funktion

- **X.509** ist ein Standard, der definiert, wie digitale Zertifikate aufgebaut sind und wie ungültige Zertifikate über eine Liste (CRL – Certificate Revocation List) verwaltet werden.
- Die aktuelle Version ist **Version 3**.

Ein X.509-Zertifikat enthält folgende wichtige Informationen:

- **Version:** Welche Version des Standards das Zertifikat verwendet.
- **Seriennummer:** Eine eindeutige ID, damit die Zertifizierungsstelle das Zertifikat verwalten kann.
- **Algorithmus für Zertifikatsignatur:** Gibt an, welche Verschlüsselungs- und Hashverfahren zum Signieren des Zertifikats verwendet werden.
- **Ausstellername:** Wer das Zertifikat ausgestellt und signiert hat (also die Zertifizierungsstelle).
- **Gültigkeit:** Von wann bis wann das Zertifikat gültig ist.
- **Zertifikatinhaber:** Wer das Zertifikat besitzt (z. B. eine Person, eine Webseite oder ein Server).
- **Schlüsselinformationen:** Der öffentliche Schlüssel des Inhabers und der verwendete Algorithmus.
- **Signatur:** Die digitale Signatur der Zertifizierungsstelle, die das Zertifikat bestätigt.

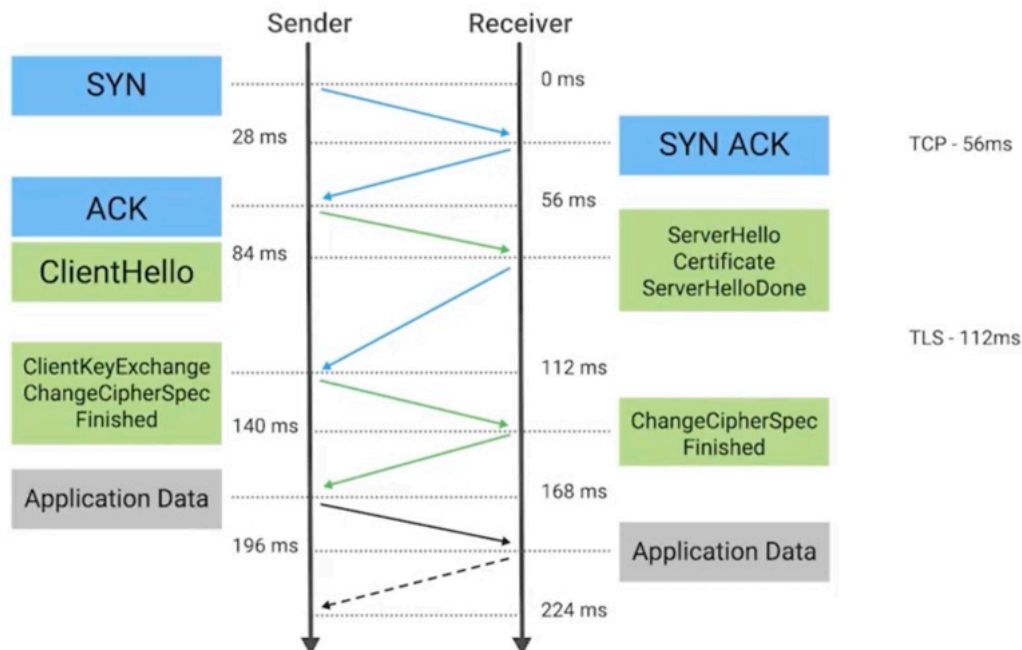
Außerdem gibt es **Zertifikat-Fingerabdrücke**: Das sind Hash-Werte des gesamten Zertifikats, die bei der Überprüfung helfen.

## Alternative zum zentralen Modell: Web of Trust

- Statt dass nur zentrale Zertifizierungsstellen (CAs) Vertrauen aufbauen, gibt es das **Web of Trust** (Netz des Vertrauens).
- Hier bestätigen sich Nutzer gegenseitig ihre Identitäten und öffentliche Schlüssel.
- Dazu prüfen sie zum Beispiel Ausweise und signieren dann die öffentlichen Schlüssel des anderen, um ihre Echtheit zu garantieren.
- Dieser Prozess ist reziprok, also beide Parteien unterschreiben sich gegenseitig.
- Solche Treffen, bei denen mehrere Personen Schlüssel signieren, nennt man **Keysigning-Partys**.
- So wächst ein Netzwerk von Vertrauen, das sich auf weitere Personen und deren Bekannte ausdehnt.

## Einfach gesagt:

- **X.509-Zertifikate** sind wie digitale Ausweise mit Informationen und einer „Unterschrift“ von einer vertrauenswürdigen Instanz.
- Das **Web of Trust** ist eine dezentralere Art, Vertrauen aufzubauen, bei der Menschen sich gegenseitig bestätigen.



## Sichere Kommunikation mit HTTPS, TLS, SSH und PGP – einfach erklärt



### HTTPS & TLS – Schutz beim Surfen im Web

- **HTTPS** = Sichere Version von HTTP (Hypertext Transfer Protocol).
- **HTTPS** = HTTP über **TLS** (früher SSL) → Verschlüsselt die Verbindung z. B. beim Onlinebanking oder Einkaufen.
- **TLS** ist ein **allgemeines Sicherheitsprotokoll**, nicht nur fürs Web – auch für E-Mails, WLAN, VoIP etc.

### TLS bietet:

1. **Verschlüsselung:** Niemand kann mitlesen.
2. **Authentifizierung:** Meistens wird der Server geprüft.

### 3. **Integrität:** Daten werden unterwegs nicht verändert.



#### **TLS-Handshake – wie der sichere Kanal aufgebaut wird**

- Client sagt: „Hallo Server“ (ClientHello, mit Liste unterstützter Algorithmen).
- Server sagt: „Hallo zurück“ (ServerHello, mit ausgewähltem Algorithmus + Zertifikat).
- Client prüft Zertifikat → stimmt's mit dem Hostnamen & der CA überein?
- Dann: **Schlüsselaustausch**, Erzeugung eines gemeinsamen Sitzungsschlüssels.
- Beide senden „ChangeCipherSpec“ und verschlüsselte „Finished“-Nachricht → Kanal ist jetzt **sicher**.



**Forward Secrecy** schützt zusätzlich: Selbst wenn ein privater Schlüssel später gestohlen wird, bleiben frühere Sitzungen **sicher**, weil jede Sitzung **einen eigenen Schlüssel** nutzt.



#### **SSH – Sicherer Fernzugriff**

- **SSH (Secure Shell)** = Verschlüsseltes Protokoll zur Remote-Anmeldung.
- Ersetzt unsichere Vorgänger wie **Telnet**.
- Alles – Passwörter, Befehle, Terminalausgabe – wird verschlüsselt.
- **Authentifizierung über öffentliche/privaten Schlüssel** möglich:
  - Der Nutzer generiert ein Schlüsselpaar.
  - Der öffentliche Schlüssel wird auf dem Zielsystem hinterlegt.
  - Der private Schlüssel bleibt **nur beim Nutzer**.

SSH kann auch andere Dienste (Ports) über den sicheren Kanal tunneln.



#### **PGP – Datenschutz für E-Mails & Dateien**

- **PGP (Pretty Good Privacy)** nutzt ebenfalls asymmetrische Verschlüsselung.
- Hauptsächlich für **E-Mails**, aber auch für Dateien, Ordner oder ganze Festplatten.
- Sehr sicher – vergleichbar mit Militärstandard.
- Ursprünglich von **Phil Zimmermann** entwickelt (1991).
- Aufgrund der Exportregeln in den USA (Verschlüsselung = Waffe!) kam es zu einem Rechtsstreit, der clever gelöst wurde: Zimmermann veröffentlichte den **Quellcode in Buchform**, geschützt durch die Meinungsfreiheit.

- Ursprünglich nutzte PGP **RSA**, später **DSA**, um Lizenzprobleme zu umgehen.

## **Fazit – was du dir merken solltest**

- **TLS/HTTPS**: Schützt deinen Webverkehr vor Spionage & Manipulation.
- **SSH**: Sicherer Zugriff auf entfernte Rechner per Kommandozeile.
- **PGP**: Starke Verschlüsselung für private Kommunikation und Dateien.
- Alle Systeme nutzen **asymmetrische Kryptografie** für sicheren Schlüsselaustausch und **symmetrische Verschlüsselung** für schnelle Datenübertragung.

## **Was ist PGP?**



**PGP (Pretty Good Privacy)** ist ein Verschlüsselungssystem zur **Sicherung von Daten** und zur **digitalen Signatur** – besonders bei **E-Mails**, aber auch für Dateien oder Ordner.

Es basiert auf zwei zentralen Funktionen:

1. **Verschlüsselung** (Schutz der Vertraulichkeit)
2. **Digitale Signatur** (Sicherstellung von Integrität & Authentizität)

## **Grundprinzip: Asymmetrische Kryptografie**

PGP nutzt **asymmetrische Verschlüsselung**:

- Du hast ein **Schlüsselpaar**:
  -  **Öffentlicher Schlüssel** → gibst du anderen.
  -  **Privater Schlüssel** → bleibt **nur bei dir**, geheim.


## **Beispiel: Du willst mir eine verschlüsselte Nachricht schicken**

1. Du benutzt **meinen öffentlichen Schlüssel**, um deine Nachricht zu **verschlüsseln**.
2. Nur ich kann sie lesen – weil **nur mein privater Schlüssel** die Nachricht wieder **entschlüsseln** kann.

## **Digitale Signatur – um zu beweisen, dass du es bist**

**Beispiel: Du willst beweisen, dass eine Nachricht wirklich von dir stammt.**



1. Du **signierst** die Nachricht mit deinem **privaten Schlüssel**.
2. Ich kann die Signatur mit deinem **öffentlichen Schlüssel** prüfen.
  - Wenn sie stimmt:  Nachricht kommt wirklich von dir & wurde **nicht verändert**.



## Hybrid-Verfahren: PGP kombiniert asymmetrische + symmetrische Verschlüsselung

- Die eigentlichen **Daten** werden mit einem schnellen **symmetrischen Schlüssel** verschlüsselt (z. B. AES).
- Dieser symmetrische Schlüssel wird dann **mit dem öffentlichen Schlüssel** des Empfängers verschlüsselt.
- Das ist schneller und effizienter – nennt sich **Hybrid-Kryptosystem**.



## Was wird bei PGP gespeichert oder verschickt?

- Die **verschlüsselte Nachricht**
- Die (optional) **digitale Signatur**
- Der **verschlüsselte symmetrische Schlüssel**
- Und evtl. Zertifikatsdaten, z. B. im Format OpenPGP oder GPG



## Web of Trust statt zentraler Zertifizierungsstelle






- PGP **vertraut nicht auf zentrale Instanzen** wie bei X.509-Zertifikaten.
- Stattdessen: **Benutzer signieren gegenseitig ihre öffentlichen Schlüssel**, nachdem sie sich geprüft haben (z. B. persönlich mit Ausweis).
- Das ergibt ein **dezentrales Vertrauensnetzwerk**: das „**Web of Trust**“.



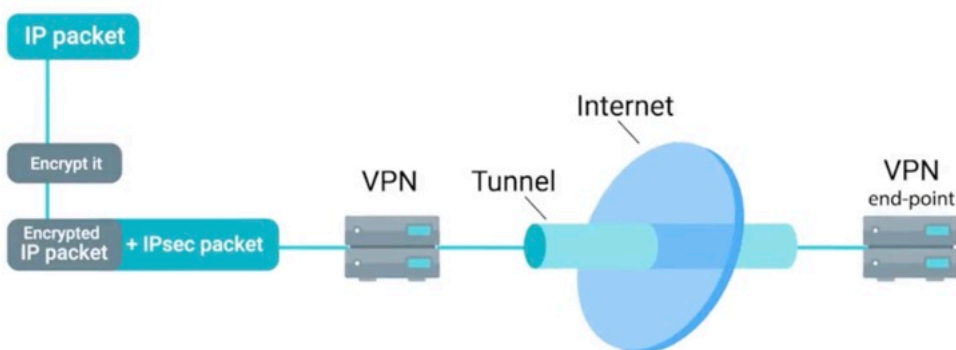
## Wie benutzt man PGP in der Praxis?

- Mit Tools wie:
  - **GPG (GnuPG)** – freie Open-Source-Implementierung von PGP
  - **E-Mail-Plugins**: z. B. Enigmail (Thunderbird), Mailvelope (für Browser)
  - **Dateiverschlüsselung**: Auch zur Sicherung von Ordnern oder Festplatten nutzbar

## Zusammengefasst: Vorteile von PGP

Vorteil	Beschreibung
 Vertraulichkeit	Nur der Empfänger kann lesen
 Authentizität	Digitale Signatur beweist Urheberschaft
 Integrität	Inhalt wurde nicht verändert
 Dezentral	Kein Zwang zu zentralen Behörden
 Sehr stark	Basiert auf sicheren Algorithmen (RSA, AES, ECC etc.)

## GESCHÜTZTER NETZWERK-TRAFFIC



## Was schützt Netzwerktraffic?

### 1. Warum Verschlüsselung?

- Verschlüsselung schützt **Daten während der Übertragung**.
- Sie sorgt für:
  - **Vertraulichkeit** (niemand kann mitlesen),
  - **Integrität** (nichts wird verändert),

- **Datenschutz.**



## 2. Was ist ein VPN?

Ein **VPN (Virtuelles Privates Netzwerk)**:

- Baut einen **sicheren Tunnel durch das Internet**.
- Schützt Daten, auch wenn die Verbindung über ein öffentliches Netzwerk läuft.
- Wird genutzt für:
  - **Remote-Zugriff** auf interne Netzwerke (z. B. Homeoffice),
  - **Anonyme Nutzung** des Internets,
  - **Verschlüsselte Verbindung zwischen zwei Netzwerken** (z. B. zwei Standorte eines Unternehmens).



## 3. VPN-Arten & Protokolle



### IPsec (Internet Protocol Security)

- Verschlüsselt IP-Pakete.
- Hat zwei Modi:
  - **Transportmodus**: verschlüsselt nur den Inhalt, nicht den IP-Header.
  - **Tunnelmodus**: verschlüsselt das **ganze** IP-Paket und packt es in ein neues.
- Wird z. B. bei Site-to-Site-VPNs verwendet.



### L2TP (Layer 2 Tunneling Protocol)

- Kein eigenes VPN, **nur Tunnelprotokoll**.
- Braucht **IPsec**, um **sicher** zu sein → Kombi heißt **L2TP/IPsec**.
- Aufbau:
  1. IPsec verhandelt den sicheren Kanal.
  2. Danach wird L2TP-Tunnel über diesen Kanal aufgemacht.
  3. Ergebnis: sicherer, getunnelter Traffic durchs Internet.

## Unterschied:

- **L2TP** = Tunnel
- **IPsec** = Sicherheit (Verschlüsselung, Authentifizierung)

## OpenVPN

- Nutzt **SSL/TLS** zur Verschlüsselung.
- Nutzt **OpenSSL**-Bibliothek → kann viele moderne Chiffren verwenden.
- Authentifizierung:
  - Pre-Shared Keys,
  - Zertifikate (am sichersten),
  - Benutzername + Passwort.
- Kann über **UDP oder TCP** laufen (Port 1194 ist Standard).
- Arbeitet im **Userspace**, was sicherer sein kann.
- Unterstützt bis zu **256-Bit-Verschlüsselung**.

## Zusammengefasst:

Protokoll	Aufgabe	Verschlüsselung	Bemerkung
IPsec	VPN-Standard	✅ Ja	Weit verbreitet, robust
L2TP	Tunneling	❌ Nein	Nutzt IPsec für Sicherheit
OpenVPN	VPN mit TLS	✅ Ja	Flexibel, sicher, weit genutzt

## Wofür braucht man das?

- Zum Schutz interner Systeme (z. B. bei Cloud-Verbindungen oder Remote-Zugriff).
- In Unternehmen, die mehrere Standorte verbinden wollen.
- Für mehr **Datenschutz und Sicherheit im Netz**.

## Was ist TPM?

- TPM ist ein **Hardware-Chip**, der in vielen Computern verbaut ist und als **sicherer Kryptoprozessor** dient.
- Er erzeugt und speichert kryptografische Schlüssel **sicher in der Hardware**.
- Jeder TPM-Chip hat einen **eindeutigen, geheimen RSA-Schlüssel**, der fest eingebrannt ist.
- TPMs ermöglichen **Hardware-Authentifizierung**, also Erkennung von unbefugten Hardware-Änderungen.
- Sie können die Software- und Hardwarekonfiguration eines Systems gegenüber einem anderen System **beweisen** (Remote Attestation).

## Funktionen von TPM:

- **Datenbindung:** Daten werden mit einem Schlüssel verschlüsselt, der an das TPM gebunden ist. Nur dieses TPM kann die Daten entschlüsseln.
- **Datenversiegelung:** Daten sind verschlüsselt und können nur entschlüsselt werden, wenn das TPM sich in einem bestimmten Zustand befindet (z.B. wenn keine Manipulationen am System vorliegen).
- TPM kann in verschiedenen Formen kommen: als einzelner Chip (am sichersten), als Firmware, Software oder virtuell.

## Vergleich zu Mobilgeräten:

- Mobilgeräte haben ein ähnliches Konzept, das **sichere Element** genannt wird.
- Das ist ebenfalls ein manipulationsgeschützter Chip, der Schlüssel speichert und sichere Anwendungen ausführt.
- Erweiterung: **Trusted Execution Environment (TEE)** – eine isolierte Umgebung, die parallel zum Hauptbetriebssystem läuft und Anwendungen schützt.

## Kritik und Sicherheit:

- Man muss dem Hersteller vertrauen, da der geheime Schlüssel bei der Herstellung eingebrannt wird.
- Theoretisch könnte der Hersteller Zugriff auf diesen Schlüssel haben.
- Es gab Fälle, bei denen Sicherheitsforscher TPMs mit teuren und aufwendigen Methoden geknackt haben, aber das ist sehr schwer und aufwendig.

## Anwendung von TPM:

- TPM schützt die **Integrität der Plattform** (also dass Hard- und Software nicht manipuliert wurden).
- TPM wird oft bei **Full Disk Encryption (FDE)** eingesetzt, also der vollständigen Verschlüsselung eines Datenträgers.
- Bekannte Programme, die TPM unterstützen, sind z.B. Microsoft Bitlocker, Apple FileVault 2, PGP und Linux dm-crypt.
- Beim Systemstart gibt es eine kleine unverschlüsselte Boot-Partition, die das System hochfährt und eine Passphrase zum Entsperren der verschlüsselten Daten abfragt.
- TPM kann dafür sorgen, dass die Festplatte nur entsperrt wird, wenn die Systemkonfiguration unverändert ist, was vor Angriffen wie Hardware-Manipulationen schützt.

### **Wichtiges Konzept: Zufälligkeit**

- Alle Kryptosysteme brauchen wirklich **zufällige Zahlen**, sonst entstehen Muster, die Angreifer ausnutzen können.
- Systeme nutzen **Entropie-Pools** (Quellen für echte Zufälligkeit) und spezielle Zufallszahlengeneratoren, um sichere Schlüssel zu erzeugen.

### **Zusammenfassung:**

Das TPM ist ein wichtiger Hardware-Sicherheitsbaustein, der hilft, Geräte und Daten vor Manipulation und Diebstahl zu schützen – vor allem durch sichere Schlüsselverwaltung und Plattformintegritätsprüfung. Es arbeitet oft im Hintergrund und ist ein Kernbestandteil moderner IT-Sicherheit, vor allem bei der Verschlüsselung kompletter Festplatten und dem Schutz vor Hardware-Angriffen.



## Die drei "A"s der IT-Sicherheit: Authentifizierung, Autorisierung und Accounting

### 1. Authentifizierung (authn)

Dabei beweist jemand, **wer er ist**.

Beispiel: Du gibst deine E-Mail-Adresse (Identifikation) und dein Passwort ein (Authentifizierung), um dich bei einem E-Mail-Dienst anzumelden.

### 2. Autorisierung (authz)

Bedeutet: **Was darfst du tun?**

Beispiel: Du darfst auf deinen Posteingang zugreifen – aber nicht auf den einer anderen Person. Die Rechte werden nach der erfolgreichen Authentifizierung vergeben.

### 3. Accounting (Ressourcenerfassung)

Heißt: **Wer hat was gemacht?**

Es wird protokolliert, wer auf welche Ressourcen zugegriffen hat. Wichtig für Kontrolle, Audits und Nachverfolgung.



## Multi-Faktor-Authentifizierung (MFA) – Zusammenfassung & Erklärung

### Definition:

MFA verlangt **mehrere unabhängige Faktoren**, um die Identität eines Nutzers zu bestätigen.



### Die drei Arten von Faktoren:

1. **Wissen:** Etwas, das man **weiß** (z. B. Passwort, PIN).
2. **Besitz:** Etwas, das man **hat** (z. B. Token, Karte, Smartphone).
3. **Biometrie:** Etwas, das man **ist** (z. B. Fingerabdruck, Iris-Scan).



Ein sicheres MFA-System kombiniert **mindestens zwei unterschiedliche Arten**.



### Warum MFA sicherer ist:

- Mehrere Faktoren zu stehlen ist **viel schwerer** als nur ein Passwort.
- Kombination von Passwort + physischem Token ist **viel sicherer** als mehrere Passwörter.



### Beispiele für MFA-Methoden:



### Physische Token:

- Z. B. USB-Stick oder ein Gerät, das **Einmalpasswörter (OTP)** generiert.
- Besonders verbreitet: **TOTP (zeitbasiert)** – z. B. mit RSA SecureID oder Smartphone-App.
- Zeit und Startwert erzeugen gemeinsam ein sich änderndes Passwort.
- Zeitabgleich erfolgt über **NTP (Network Time Protocol)**.



#### **Zählerbasierte Token (HOTP):**

- Nutzt zusätzlich einen **Zähler**, der sich bei jedem Login erhöht.
- Noch sicherer, weil der Zähler schnell aus dem Takt gerät, wenn das Token geklont wurde.



#### **Smartphone-Apps (z. B. Google Authenticator, Authy):**

- Bequeme Alternative zu Hardware-Token.
- Gleiche Funktionsweise wie physische Token, aber praktischer.



#### **Schwachstelle: SMS als zweiter Faktor**

- **Unsicher**, da SMS nicht verschlüsselt sind.
- Angriffe möglich durch:
  - **Abhören der SMS**
  - **SIM-Swapping** (Angreifer täuscht Mobilfunkanbieter)



#### **Risiken & Nachteile von MFA:**

- **Phishing bleibt eine Gefahr:** Nutzer könnten Login + OTP auf gefälschten Seiten eingeben.
- **Physische Token können verloren, beschädigt oder veraltet sein.**
- **Benutzerfreundlichkeit leidet**, da MFA zusätzliche Schritte erfordert.



#### **Fazit:**

MFA bietet **deutlich mehr Sicherheit** als reine Passwortauthentifizierung, **aber:**

- Nicht alle Methoden sind gleich sicher.
- **Kombination mit starken Passwortrichtlinien und Benutzerschulung** ist entscheidend.





## Biometrische Authentifizierung – Überblick

### Was ist das?

Identifikation anhand **einzigartiger, physiologischer Merkmale** wie:

- Fingerabdruck
- Gesicht
- Iris
- Stimme

### Vorteile:

- Sehr **personenbezogen**, nicht leicht übertragbar
- Geräte wie Smartphones nutzen Fingerabdrucksensoren oder Gesichtserkennung
- **Schnell & bequem** in der Anwendung

### Datenschutz & Sicherheit:

- **Biometrische Daten werden nicht direkt gespeichert**, sondern gehasht
- Kompromittierung schwerwiegender als bei Passwörtern (nicht änderbar)
- Missbrauch kann Privatsphäre stark gefährden

### Missbrauchsmöglichkeiten:

- Gefälschte Fingerabdrücke z. B. mit Klebstoff (z. B. bei Schülern)
- Dennoch schwerer zu umgehen als Passwörter

### Beispiel: Windows Hello

- Nutzt Fingerabdruck, Iris, Gesicht
- Arbeitet mit Farb- und Infrarotkamera (Tiefensensorik)
- Schützt vor Täuschung durch Fotos oder Ausdrücke



## Sicherheitsschlüssel (U2F – Universal 2nd Factor)

### Was ist U2F?

Ein **sicherer Standard für Zwei-Faktor-Authentifizierung**, entwickelt von Google, Yubico und NXP, verwaltet von der **FIDO Alliance**.

### Funktion & Ablauf:

1. **Registrierung:**

- Generierung eines Schlüsselpaares (privat/öffentlich)
- Der **öffentliche Schlüssel** wird bei der Website gespeichert

## 2. Authentifizierung (Challenge-Response-Verfahren):

- Website sendet eine Challenge (zufällige Daten)
- Der Sicherheitsschlüssel signiert die Challenge mit dem **privaten Schlüssel**
- Website prüft die Signatur mit dem registrierten **öffentlichen Schlüssel**

### Sicherheitsvorteile gegenüber OTP:

- Kein **Phishing** möglich (interaktive Bestätigung durch Nutzer nötig)
- **Schutz vor Replay-Angriffen**
- **Nicht klonbar**, da Hardware eindeutige, eingebettete Daten enthält

### Benutzerfreundlichkeit:

- Kein Eintippen von Codes nötig
- **Ein Klick reicht** – deutlich einfacher als OTPs



### Relevanz für IT-Fachkräfte

- Kenntnisse über MFA-Methoden sind wichtig für:
  - **Support**
  - **Implementierung**
  - **Sicherheitsberatung**
- Biometrie und Sicherheitsschlüssel bieten **moderne, starke Alternativen** zu klassischen Passwörtern oder OTPs

## **Single Sign-on (SSO) – Zusammenfassung**

### **Was ist SSO?**

Single Sign-on (SSO) ist ein Authentifizierungsverfahren, bei dem sich Nutzer **einmalig anmelden**, um auf **mehrere Dienste** zuzugreifen – ohne sich bei jedem Dienst erneut authentifizieren zu müssen.

### **Wie funktioniert es?**

- Die Anmeldung erfolgt zentral, z. B. über einen **LDAP-Server** oder ein **Kerberos-System**.
- Nach der Authentifizierung erhält der Nutzer ein **Token** oder **Ticket**, mit dem er auf andere Anwendungen zugreifen kann.
- Beispiel: **Kerberos** nutzt ein sogenanntes *Ticket Granting Ticket (TGT)* für diesen Zweck.

### **Vorteile:**

- Nur **ein Satz Anmeldedaten** notwendig
- Weniger **Passwort-Reset-Anfragen**
- Höhere **Benutzerfreundlichkeit** und **Produktivität**

### **Sicherheitsrisiken:**

- Bei Kompromittierung eines Kontos erhält der Angreifer **Zugriff auf viele Dienste gleichzeitig**
- **SSO-Tokens oder -Cookies** können gestohlen und missbraucht werden
- Multi-Faktor-Authentifizierung (MFA) ist empfohlen, schützt aber nicht vor **Session-Token-Diebstahl**

### **Beispiel: OpenID**

- OpenID ist ein **dezentrales SSO-System**
- Websites lagern die Authentifizierung an einen **externen Identitätsanbieter** aus
- Nutzer melden sich dort an und erhalten ein **Token**, das die Authentifizierung gegenüber anderen Diensten bestätigt
- Vorteil: **Keine zusätzliche Registrierung** auf jeder unterstützenden Website nötig

## OAuth

- **OAuth** ist ein offener Standard zur **Autorisierung** von Drittanbieter-Apps, ohne dass Nutzer ihre Anmeldedaten direkt weitergeben müssen.
- Nutzer bestätigen, dass eine Drittanbieter-Anwendung auf bestimmte Daten oder Dienste in ihrem Konto zugreifen darf (z. B. E-Mail).
- Nach der Zustimmung erhält die Drittanbieter-App ein **Zugriffstoken** mit festgelegtem Umfang („Scope“), das den Zugriff nur auf erlaubte Daten ermöglicht.
- Typisches Beispiel: Eine Website möchte E-Mails im Namen des Nutzers senden, dafür wird per OAuth der Zugriff auf das E-Mail-Konto angefragt und gewährt, aber nicht auf andere Dienste wie Cloudspeicher.
- **Sicherheitsrisiko:** Phishing-Angriffe können OAuth-Anfragen imitieren, um unberechtigten Zugriff über Tokens zu erlangen (z.B. 2017 Google-Dokument-Wurmangriff).
- **Wichtig:** OAuth ist ein **Autorisierungssystem**, kein Authentifizierungssystem.
- OpenID ist ein Authentifizierungsstandard; **OpenID Connect** kombiniert OpenID mit OAuth für Authentifizierung plus Autorisierung.

## AAA-Systeme (z.B. TACACS+, RADIUS)

- **TACACS+** ist ein vollständiges AAA-System:
  - **Authentifizierung:** Nutzer melden sich an.
  - **Autorisierung:** Festlegung, welche Befehle oder Geräte der Nutzer verwenden darf (z.B. Admin- oder schreibgeschützter Zugriff).
  - **Abrechnung (Accounting):** Protokollierung von Aktionen (nicht im Text erwähnt, aber Teil von AAA).
- Beispiel: Netzwerkteam erhält Adminzugriff, Support-Team schreibgeschützten Zugriff, andere Nutzer keinen Zugang.
- **RADIUS** wird oft für Netzwerkzugang verwendet, z.B. um WLAN- oder VPN-Zugriff zu autorisieren. Der Server gibt dann an, welche Dienste erlaubt sind.

## Was ist „Accounting“ im AAA-System?

„Accounting“ ist der dritte Bestandteil des AAA-Sicherheitsmodells:

- **Authentication** – Wer bist du?
- **Authorization** – Was darfst du?

- **Accounting** – Was hast du gemacht?

## **Worum geht es beim Accounting?**

Accounting dient dazu, zu protokollieren, welche Nutzer auf welche Ressourcen zugegriffen haben und welche Aktionen sie ausgeführt haben.

Wichtig: Das Sammeln von Daten allein reicht nicht – sie müssen auch ausgewertet werden, zum Beispiel im Rahmen von Audits zur Erkennung ungewöhnlicher Aktivitäten.

## **Beispiele für Accounting-Systeme**

### **TACACS+ (für Gerätezugriff)**

- Überwacht die Authentifizierung von Nutzern
- Zeichnet ausgeführte Befehle auf
- Erfasst Aktionen im privilegierten Modus
- Meldet Änderungen an Geräten (z. B. Neustarts oder neue Konfigurationen)

### **RADIUS (für Netzwerkzugriff)**

- Dokumentiert Sitzungsdauer, Clientstandort, Bandbreite und Ressourcenverbrauch
- Wird von Internetanbietern zur Abrechnung verwendet
- Unterstützt Daten- und Zeitlimits
- Zeichnet keine Details über die Inhalte der Sitzung auf (z. B. keine Protokolle, keine Webseiten)

## **Wie funktioniert RADIUS-Accounting technisch?**

1. Der Network Access Server (NAS) sendet ein „Accounting-Start“-Paket mit Sitzungsdaten an den Accounting-Server.
2. Während der Sitzung sendet der NAS regelmäßig Status-Updates.
3. Am Ende der Sitzung wird ein „Accounting-Stop“-Paket gesendet.

## **Fazit**

Accounting ist ein zentraler Bestandteil der Sicherheitsüberwachung. Es ermöglicht eine nachvollziehbare Nutzungskontrolle, hilft bei der Abrechnung und unterstützt Sicherheitsanalysen. Inhalte der Aktivitäten werden dabei in der Regel nicht erfasst.

## **Netzwerkhärtung – Überblick**

- Ziel: Netzwerke durch Konfigurationsänderungen und gezielte Maßnahmen sicherer machen.
- Schwerpunkt: Reduzierung von Sicherheitslücken.
- Wichtige Themen: Netzwerksicherheit, Überwachung, Analyse, Firewalls und Segmentierung.

## **Grundprinzipien der Netzwerksicherheit**

- Unnötige Dienste deaktivieren oder den Zugriff darauf beschränken.
- Jeder aktive Dienst stellt ein potenzielles Sicherheitsrisiko dar.
- „Implicit Deny“-Prinzip:
  - Alles wird standardmäßig blockiert, es sei denn, es ist ausdrücklich erlaubt.
  - Umsetzung über Access Control Lists (ACLs) und Firewalls.
  - Fokus liegt auf einer Positivliste („Erlauben“ statt „Blockieren“).
  - Mehr Sicherheit, aber auch mehr Aufwand bei neuen Diensten.

## **Netzwerküberwachung und -analyse**

- Ziel: Abweichungen vom normalen Netzwerkverhalten erkennen.
- Voraussetzung: Definition eines Normalzustands (Baseline).
- Protokollanalyse:
  - Sammeln und Auswerten von Logs (Firewalls, Authentifizierungsserver, Anwendungen).
  - Erkennung von Malware, unberechtigten Zugriffen, verdächtigem Verhalten.
- Extern erreichbare Dienste besonders kritisch überwachen.

## **Protokollanalyse im Detail**

- Hinweise auf Angriffe erkennen (z. B. Zugriff von verdächtigen IPs).
- Verbindung von Protokollen unterschiedlicher Systeme zur besseren Analyse.
- Schadensanalyse nach Angriffen:
  - Was ist passiert?
  - Welche Systeme waren betroffen?

- Wurden Daten gestohlen?

## **Tools und Systeme**

- Beispiel: Splunk
  - Leistungsfähiges Tool zur Protokollsammlung, Analyse, Visualisierung und Alarmierung.
- Alarmierungssysteme:
  - Warnmeldungen nach Regelverstößen
  - Priorisierung und Kategorisierung von Warnungen
  - Benachrichtigungen z. B. per E-Mail oder SMS

## **Flood Guards und Schutz vor DoS-Angriffen**

- Schutz der Verfügbarkeit (Teil der CIA-Triade).
- Erkennen und blockieren typischer Angriffsarten (z. B. SYN-Floods).
- Einsatz auf Routern und Firewalls möglich.
- Beispiel: Fail2ban
  - Open-Source-Tool, erkennt Angriffe und blockiert IP-Adressen automatisch.

## **Netzwerksegmentierung**

- Trennung von Geräten und Diensten in unterschiedliche virtuelle Netzwerke (VLANs).
- Vorteile:
  - Mehr Sicherheit durch begrenzten Zugriff.
  - Bessere Übersicht und Kontrolle.
- Beispiel: Trennung von Mitarbeiter- und Druckernetz.
  - Zugriff der Mitarbeiter über Routing und ACLs gezielt erlauben.

## **Netzwerkhardware-Härtung:**

- DHCP weist Geräten im Netzwerk wichtige Konfigurationsdaten (IP, Gateway, DNS) zu.

- Rogue DHCP-Server können falsche Daten ausgeben, um Traffic abzufangen oder umzuleiten (Rogue DHCP-Angriff).
- DHCP-Snooping auf Enterprise-Switches überwacht DHCP-Traffic und erstellt eine IP-zu-Port-Liste.
- DHCP-Snooping schützt auch vor IP-Spoofing und ARP-Poisoning.
- Uplink-Ports können als „trusted“ markiert werden, legitime DHCP-Antworten werden akzeptiert, andere verworfen.
- Dynamic ARP Inspection (DAI) verhindert Man-in-the-Middle-Angriffe über gefälschte ARP-Antworten.
- DAI nutzt die DHCP-Snooping-Tabelle zur Erkennung gefälschter ARP-Pakete und begrenzt ARP-Anfragen pro Port.
- IP Source Guard (IPSG) blockiert Pakete mit gefälschten IP-Adressen basierend auf DHCP-Snooping-Daten.
- 802.1X (EAPoL) ist ein Authentifizierungsstandard für Netzwerke, bei dem der Client (Supplicant) sich vor dem Zugriff authentifizieren muss. Authenticator (z. B. Switch) leitet Authentifizierungsanfragen an einen Authentifizierungsserver (meist RADIUS) weiter.
- EAP-TLS verwendet TLS für gegenseitige Authentifizierung mit Zertifikaten – sehr sicher, z.B. in WLANs.
- EAP-TLS erfordert Verwaltung von Zertifikaten und sicheren Umgang mit privaten Schlüsseln.
- Bindung von Zertifikaten an TPM erhöht Sicherheit (Schutz vor Diebstahl).
- Kombination mit Full-Disk-Encryption (FDE) schützt Geräte und Netzwerk bei Geräteverlust.
- Verständnis dieser Technologien hilft bei Fehlerbehebung und Sicherheit im Netzwerk.

## **Netzwerksoftware-Härtung:**

### **1. Firewalls – Überblick und Einsatz**

- **Zweck:** Kontrollieren den Datenverkehr und schützen Netzwerke bzw. Geräte vor unautorisierten Zugriffen.
- **Arten:**
  - **Netzwerkbasierende Firewalls:**
    - Befinden sich am Übergangspunkt zwischen internem Netzwerk und Internet.



- Regeln den gesamten ein- und ausgehenden Netzwerkverkehr.
- Beispiel: Firewall im Heimrouter oder Unternehmensgateway.
- **Hostbasierte Firewalls:**
  - Installiert direkt auf einem Endgerät (z. B. Windows Firewall).
  - Schützt den einzelnen Host (Laptop, PC) vor Netzwerkangriffen.
  - Besonders nützlich in öffentlichen Netzwerken wie WLAN-Hotspots.
- **Empfehlung:** Kombination aus beiden Arten für umfassenden Schutz.

## 2. VPN (Virtual Private Network) – Überblick

- **Zweck:** Sichere Verbindung über ein unsicheres Netzwerk (z. B. Internet).
- **Einsatzszenarien:**
  - **Remotezugriff:** Mitarbeiter greifen sicher von unterwegs auf interne Firmendienste zu.
  - **Site-to-Site-VPN:** Verbindet zwei entfernte Netzwerke (z. B. zwei Bürostandorte), als wären sie lokal verbunden.
- **Sicherheit:**
  - Verschlüsselung schützt die Daten vor Mitlesen.
  - Authentifizierung kann erforderlich sein (z. B. Benutzername, Zertifikat).
- **Vorteile:**
  - Hohe Sicherheit durch Verschlüsselung.
  - Ermöglicht Zugriff auf interne Dienste unabhängig vom Standort.

## 3. Proxy – Überblick und Funktion

- **Zweck:** Vermittlungsstelle zwischen Client und Zielserver. Der Client kommuniziert nicht direkt mit dem Ziel, sondern über den Proxy.
- **Arten:**
  - **Forward Proxy** (klassischer Webproxy):
    - Client schickt Webanfrage an den Proxy.
    - Proxy leitet die Anfrage ans Internet weiter und gibt die Antwort zurück.
    - Verwendung:

- Zugriffskontrolle, Inhaltsfilterung.
- Logging und Überwachung des Traffics.
- Kann gewisse Webseiten blockieren.
- **Reverse Proxy:**
  - Wird im Unternehmensnetzwerk vor Webservern platziert.
  - Externe Anfragen gehen an den Reverse Proxy.
  - Dieser leitet sie an interne Dienste weiter.
  - Verwendung:
    - Sicherer Zugriff auf interne Webanwendungen (ohne VPN).
    - Verteilung von Last (Load Balancing).
    - Verschlüsselung (TLS) und Authentifizierung.
- **Beispiele für Proxysoftware:**
  - HAProxy, Nginx, Apache (als Reverse-Proxy einsetzbar).

## WPA 2

### 1. WPA2 – Verbesserungen gegenüber WPA

- WPA2 nutzt **CCMP (Counter Mode with CBC-MAC Protocol)** anstelle von TKIP.
- **CCMP basiert auf der AES-Verschlüsselung**, nicht auf der veralteten und unsicheren RC4-Chiffre.
- Der Schlüsselableitungsprozess bleibt wie bei WPA.
- Pre-Shared Key (PSK) wird weiterhin verwendet, wenn kein Enterprise-Setup vorhanden ist.

### 2. CCMP (AES mit Authentifizierung)

- Kombiniert **Verschlüsselung und Authentifizierung** in einem Protokoll.

- CBC-MAC erzeugt einen Authentifizierungscode (Digest), der anschließend verschlüsselt wird.
- AES im **Counter Mode (CTR)** verwandelt die Blockchiffre in eine Stromchiffre zur effizienten Datenverschlüsselung.

### 3. Vier-Wege-Handshake (WPA2-PSK)

Ziel: **Sichere Generierung des Sitzungsschlüssels (PTK)** aus dem Langzeitschlüssel (PMK), ohne diesen direkt zu übertragen.

#### Ablauf:

1. Access Point (AP) sendet **Nonce (zufälliger Wert)** an den Client.
2. Client sendet eigene Nonce zurück.
3. AP überträgt den **GTK (Groupwise Transient Key)** verschlüsselt.
4. Client bestätigt den Empfang mit einem **ACK**.

#### Wichtige Schlüssel:

- **PMK (Pairwise Master Key)**: Langzeitschlüssel aus PSK oder EAP-Methode.
- **PTK (Pairwise Transient Key)**: Abgeleitet aus PMK + Nonces + MAC-Adressen.
  - Besteht aus mehreren Teilschlüsseln:
    - Für EAPoL-Paketverschlüsselung
    - Für MIC-Berechnung
    - Für temporäre Datenverschlüsselung
- **GTK (Groupwise Transient Key)**: Für Broadcast- und Multicast-Datenverkehr, wird an alle Clients verteilt.

### 4. Authentifizierungsarten in WPA2

- **WPA2-Enterprise (802.1X)**:
  - Verwendung von RADIUS-Servern zur Authentifizierung.
  - AP fungiert als Authentifikator, nicht als Entscheidungsinstanz.
- **WPA2-Personal (PSK)**:
  - Kein Authentifizierungsserver.
  - Pre-Shared Key wird lokal auf Client und AP konfiguriert.

## 5. Schwächen & Angriffsmöglichkeiten

- **Offline-Brute-Force-Angriffe** auf den PSK sind möglich, wenn ein Angreifer den Vier-Wege-Handshake mitschneidet.
  - Enthält alle nötigen Infos (Nonces, MAC-Adressen), um PTKs lokal zu berechnen.
  - Ziel ist es, den richtigen PMK zu erraten und zu prüfen, ob der PTK stimmt (z. B. über MIC-Validierung).
- **Rechenaufwand:**
  - PMK wird aus PSK + SSID über 4096 Hash-Iterationen (PBKDF2) berechnet.
  - Angriffe lassen sich mit **GPU-Beschleunigung und Cloud-Diensten** stark beschleunigen.
- **Rainbow Tables:**
  - Vorausberechnete Tabellen aus gängigen SSID-Passwort-Kombinationen.
  - Reduzieren den Aufwand für Brute-Force-Angriffe erheblich.
  - Für viele Standard-SSIDs und schwache Passwörter verfügbar.

## 6. Zusatz: WPS – Komfort, aber Risiko

- **Wi-Fi Protected Setup (WPS):**
  - Erleichtert das Hinzufügen von Geräten zum Netzwerk per Knopfdruck oder PIN.
  - Ist **keine Sicherheitsfunktion**, sondern eher ein **Komfort-Feature**.
  - Gilt als **unsicher**, da es durch einfache PIN-Angriffe kompromittierbar ist.

## Fazit

- **WPA2 ist deutlich sicherer als WPA**, insbesondere durch AES/CCMP.
- Die Sicherheit hängt **maßgeblich von der Qualität des PSK** ab.
- **Schwache Passwörter + bekannte SSIDs = leicht angreifbar** (Brute-Force, Rainbow Tables).
- Der **Vier-Wege-Handshake ist der zentrale Angriffspunkt**, wenn er abgefangen wird.
- Kombination aus **starkem PSK, deaktiviertem WPS und ggf. WPA3** ist empfehlenswert für moderne Netzwerke.

# Thema: Sicherster Schutz für drahtlose Netzwerke

## 1. Beste Sicherheitsoption: 802.1X mit EAP-TLS

- **Was ist das?**  
Ein sehr sicheres Authentifizierungsverfahren, das Zertifikate nutzt (ähnlich wie bei HTTPS-Webseiten).
- **Wie funktioniert das?**  
Client und Netzwerk authentifizieren sich gegenseitig über digitale Zertifikate.
- **Vorteile:**
  - Sehr hohe Sicherheit, da keine Passwörter im klassischen Sinn genutzt werden.
  - Schutz vor vielen Angriffen, z. B. Passwortdiebstahl.
- **Nachteile:**
  - Hohe Komplexität und Verwaltungsaufwand.
  - Man braucht eine komplette Infrastruktur:
    - Einen RADIUS-Server für die Authentifizierung
    - Ein Backend für die Verwaltung von Zertifikaten (PKI)
    - Systeme zum Ausstellen und Verteilen der Zertifikate an alle Clients
  - Für Unternehmen oft zu aufwendig.

## 2. Alternative: WPA2 mit AES/CCMP

- **Was ist das?**  
Ein sehr verbreiteter Standard für WLAN-Sicherheit, bei dem Clients mit einem starken Passwort verbunden werden.
- **Wie kann man es sicher machen?**
  - Verwende eine **lange und komplexe Passphrase**, die nicht einfach in Wörterbüchern steht.
  - Ändere die **SSID (Netzwerkname)** in eine individuelle, damit Angreifer keine fertigen Angriffstabellen (Rainbow Tables) nutzen können.
- **Vorteile:**
  - Weniger komplex als 802.1X.
  - Für viele Unternehmen ein guter Kompromiss zwischen Sicherheit und Aufwand.

### 3. Warum sollte WPS (Wi-Fi Protected Setup) deaktiviert sein?

- **Was ist WPS?**  
Eine einfache Methode, Geräte per Knopfdruck oder PIN mit WLAN zu verbinden.
- **Problem:**
  - WPS hat bekannte Sicherheitslücken und ist anfällig für Angriffe (z. B. PIN-Brute-Force).
  - Deshalb wird WPS in Unternehmen **nicht empfohlen**.
- **Was sollte man tun?**
  - WPS auf den Access Points deaktivieren.
  - Mit Tools (z. B. „Wash“) prüfen, ob WPS wirklich ausgeschaltet ist, denn manche Geräte deaktivieren es nicht richtig, obwohl es in der Konsole so aussieht.

### Zusammenfassung:

- **Maximale Sicherheit = 802.1X mit EAP-TLS (Zertifikate, PKI)**  
→ Sehr sicher, aber komplex und aufwendig.
- **Praktische Alternative = WPA2 mit starkem Passwort und individueller SSID**  
→ Gute Sicherheit, einfacher zu handhaben.
- **WPS ist ein Risiko und sollte in Firmennetzwerken deaktiviert sein.**

### Das Netzwerk ausspähen

- **Packet Sniffing (Packet Capture)** bedeutet das Abfangen und Analysieren von Netzwerkpaketen zur Fehlerbehebung oder Überwachung.
- **Netzwerkschnittstellen** verarbeiten normalerweise nur Pakete, die an ihre eigene MAC-Adresse adressiert sind. Andere Pakete werden ignoriert.
- Um **alle Pakete** zu erfassen, versetzt man die Netzwerkschnittstelle in den **Promiscuous-Modus**. Dann nimmt sie *alle* Pakete auf, auch wenn sie nicht für sie bestimmt sind.
- Zum Aktivieren des Promiscuous-Modus braucht man in der Regel **Admin- oder Root-Rechte**.
- Wenn dein Rechner an einem **Switch** hängt, siehst du normalerweise nur den Datenverkehr, der an dich adressiert ist oder von dir stammt. Das ist wenig hilfreich, um anderen Traffic mitzulesen.

- **Port Mirroring** (Spiegeln von Ports) ist eine Funktion von verwalteten Switches, bei der der gesamte oder ausgewählte Traffic an einen bestimmten Port geschickt wird, wo man ihn mit Packet Sniffer Tools beobachten kann.
- Eine veraltete Methode ist der Einsatz eines **Hubs** statt eines Switches, da Hubs alle Pakete an alle Ports senden. Nachteil: geringere Geschwindigkeit und mehr Kollisionen.
- Bei **drahtlosen Netzwerken** gibt es zwei Modi:
  - **Promiscuous-Modus**: empfängt alle Pakete, die im eigenen WLAN gesendet werden und für andere Clients bestimmt sind.
  - **Monitormodus**: fängt *alle* WLAN-Pakete auf, unabhängig vom Zielnetzwerk, auch wenn das Gerät nicht mit einem WLAN verbunden ist. Man braucht dafür eine spezielle WLAN-Schnittstelle.
- Tools wie **Aircrack-ng** oder **Kismet** nutzen den Monitormodus zur Analyse von WLAN-Datenverkehr.
- Wenn WLAN-Daten verschlüsselt sind (z.B. WPA2), kann man zwar Pakete mitschneiden, aber ohne das **WLAN-Passwort** lassen sich die Inhalte nicht entschlüsseln.

Kurz gesagt: Packet Sniffing hilft, Netzwerkprobleme zu lösen oder Sicherheitsüberprüfungen durchzuführen, erfordert aber spezielle Einstellungen und Rechte. Bei WLANs ist der Monitormodus nötig, um den gesamten Funkverkehr zu erfassen.

## tcpdump und wireshark

### Tcpdump – was ist das?

- **Tcpdump** ist ein beliebtes, einfaches Kommandozeilenprogramm, das Pakete im Netzwerk mitschneiden und analysieren kann.
- Es nutzt die **libpcap-Bibliothek**, die viele Tools zur Paketerfassung verwenden.
- Tcpdump kann Pakete **live anzeigen** oder **in Dateien speichern**, die später analysiert oder weitergegeben werden können.
- Die Standardanzeige zeigt wichtige Informationen zu Paketen ab **Netzwerkschicht (Layer 3)** in einer menschenlesbaren Form.

### Was zeigt Tcpdump im Output?

- **Zeitstempel**: Wann das Paket verarbeitet wurde.
- **Protokoll**: Z.B. IPv4, IPv6.

- **Verbindungsquad:** Quell-IP und Port, Ziel-IP und Port.
- **TCP-Flags** und **Sequenznummer**, falls vorhanden.
- TCP-Fenstergröße, TCP-Optionen und Größe der Nutzlast (in Bytes).
- Tcpcmd versucht standardmäßig, IP-Adressen in **Hostnamen** aufzulösen und Portnummern in die entsprechenden Dienstnamen umzuwandeln (z.B. Port 80 → HTTP). Mit dem **-n** Flag schaltet man diese Auflösung aus.
- Man kann sich auch die **Rohdaten** der Pakete in hexadezimaler oder ASCII-Darstellung anzeigen lassen (mit **-x** oder **-X**).

## Wireshark – was ist das?

- **Wireshark** ist ein grafisches, sehr leistungsfähiges Paket-Analyse-Tool.
- Es verwendet ebenfalls die **libpcap-Bibliothek** zum Erfassen der Pakete.
- Im Vergleich zu Tcpcmd bietet Wireshark deutlich mehr Funktionen, z.B.:
  - **Entschlüsselung** von verschlüsselten Paketen (z.B. WPA2) wenn Schlüssel bekannt sind.
  - Erkennung und Extraktion von Nutzdaten aus Protokollen wie HTTP oder SMB.
  - **Filtern** von Paketen nach bestimmten Protokollen oder sogar Inhalten (z.B. URLs).
- Die Oberfläche zeigt Pakete in drei Bereichen:
  - Paketliste mit Farbkodierung (z.B. grün für TCP)
  - Detailansicht des ausgewählten Pakets in Schichten (Layern)
  - Hex- und ASCII-Darstellung der Daten.
- Es unterstützt über 2.000 Protokolle und ist damit sehr flexibel.
- Wireshark kann ganze **TCP-Sitzungen nachverfolgen**, sodass man den kompletten Datenfluss zwischen zwei Teilnehmern sehen kann.
- Weitere Features: Unterstützung von Bluetooth-, USB- und Zigbee-Datenverkehr, Extraktion von Audio aus VoIP-Streams, File Carving bei unverschlüsseltem Datenverkehr.

## Warum ist Paket-Analyse wichtig für Sicherheit?

- Der gesamte Netzwerkverkehr besteht aus Datenpaketen.
- Paket-Erfassung und -Analyse helfen, **versteckte Probleme zu erkennen** (z.B. Angriffe, Fehlkonfigurationen).



- Durch das Verständnis des Verkehrsflusses lässt sich besser beurteilen, ob das Netzwerk sicher ist oder nicht.
- Werkzeuge wie Tcpdump und Wireshark sind wichtige Hilfsmittel für Netzwerkadministratoren und Sicherheitsprofis.

## Systeme zur Erkennung und Verhinderung von Angriffen

### IDS (Intrusion Detection System)

- Erkennt verdächtigen oder schädlichen Datenverkehr
- Protokolliert und sendet Warnungen
- **Reagiert nicht aktiv**, blockiert keine Angriffe
- Kann netzwerk- oder hostbasiert sein

### IPS (Intrusion Prevention System)

- Erkennt **und blockiert** schädlichen Datenverkehr
- Kann Firewall-Regeln dynamisch anpassen
- Muss im Datenstrom platziert sein (Daten müssen es durchlaufen)
- Kann auch netzwerk- oder hostbasiert sein

### Netzwerkbasiertes IDS/IPS (NIDS/NIPS)

- Überwacht gesamten Netzwerkverkehr (z. B. über Switch mit Port-Mirroring)
- Erkennt Angriffe zwischen Geräten im Netzwerk
- NIDS: passiv, NIPS: aktiv (greift ein)

### Hostbasiertes IDS/IPS (HIDS/HIPS)

- Installiert auf einzelnen Geräten
- Überwacht nur Datenverkehr des jeweiligen Hosts
- Erkennt auch unautorisierte Änderungen an Systemdateien

## Unterschiede zur Firewall

- Firewall schützt **vor externem** Datenverkehr
- IDS/IPS erkennt auch **interne Bedrohungen**
- Firewalls sehen **nicht** den Verkehr zwischen Geräten im selben Netz

## Funktionsweise der Erkennung

- Meist **signaturbasiert** (bekannte Angriffsmuster)
- Erkennung neuer, unbekannter Angriffe schwierig
- Benutzerdefinierte Regeln möglich für auffälligen, noch nicht klassifizierten Verkehr

## Reaktion bei Entdeckung

- Ereignis wird protokolliert
- Paketmitschnitt wird gespeichert
- Warnung wird ausgelöst (z. B. E-Mail, Ticket)
- Reaktion hängt von Schweregrad ab

# Einheitliches Bedrohungsmanagement (Unified Threat Management, UTM)

## Allgemeines zu UTM

- Kombination mehrerer Sicherheitstools in einer Lösung
- Zentrale Verwaltungsoberfläche für einfachere Konfiguration und Überwachung
- Ziel: ganzheitlicher Schutz des Netzwerks

## Formen der UTM-Lösungen

- **Hardware**-Appliance (eigenständig oder integriert in Netzwerkgeräte)
- **Software**-Anwendungen auf Servern
- Schutz für **einzelne Hosts** oder **ganze Netzwerke**

## UTM-Sicherheitsfunktionen

- **Firewall**: Filtert ein- und ausgehende Datenpakete, schützt vor externen Bedrohungen
- **IDS** (Intrusion Detection System): Erkennt und meldet verdächtigen Verkehr, greift nicht aktiv ein
- **IPS** (Intrusion Prevention System): Erkennt und **blockiert** schädlichen Verkehr automatisch oder manuell
- **Antivirus**: Erkennt und entfernt bekannte Schadsoftware mithilfe von Signaturen
- **Anti-Malware**: Erkennt bekannte und neue Bedrohungen (auch heuristisch + Sandbox)
- **Spam-Gateway**: Filtert unerwünschte E-Mails
- **Web-/Inhaltsfilter**: Sperrt Zugriff auf gefährliche oder unerwünschte Websites
- **DLP (Data Loss Prevention)**: Erkennt und verhindert unautorisierte Datenübertragungen nach außen
- **VPN**: Verschlüsselter Tunnel für sichere Datenübertragung über öffentliche Netze

## Prüfverfahren

- **Streambasiert**: Schnell, prüft während der Datenübertragung (Stichproben)
- **Proxybasiert**: Gründlicher, aber langsamer – vollständige Analyse nach Zwischenspeicherung

## Vorteile von UTM

- **Kostenersparnis**: Weniger Aufwand und günstiger als Einzeltools
- **Flexibilität**: Module individuell konfigurierbar
- **Zentrale Verwaltung**: Übersichtliche Steuerung und einfachere Updates

## Risiken und Nachteile

- **Single Point of Failure**: Bei Ausfall der UTM-Komponente kann das ganze Sicherheitssystem gefährdet sein

- **Überdimensionierung für kleine Unternehmen:** Hoher Aufwand trotz geringem Nutzen bei kleinen Netzwerken

## Was macht **tcpdump** standardmäßig?

- **tcpdump analysiert den Netzwerkverkehr** und zeigt an, was über das Netzwerk gesendet wird.
- **Standardmäßig macht tcpdump eine einfache Protokollanalyse** – also erkennt grundlegende Netzwerkprotokolle (z. B. IP, TCP, UDP).

## Was bewirkt die **-v**-Option?

- Die **-v**-Option steht für „**verbose**“ (**detailliert**).
- Sie **aktiviert eine ausführlichere Ausgabe**, also zeigt mehr Details über die erfassten Pakete an.
- Noch mehr Details bekommst du mit **-vv** oder **-vvv**.

## Was macht **tcpdump** sonst noch automatisch?

- Es versucht **IP-Adressen in Hostnamen umzuwandeln**, also statt **192.168.1.1** zeigt es z. B. **example.com**.
- Es ersetzt **Portnummern durch bekannte Dienstnamen**, z. B. zeigt es **http** statt **Port 80**.

## Warum sollte man **-n** verwenden?

- Die Option **-n unterdrückt die DNS-Auflösung und Portnamen-Ersetzung**.
- Das ist hilfreich, weil:
  - **DNS-Anfragen erzeugen zusätzlichen Netzwerkverkehr**, der die Analyse stören kann.
  - Es ist **schneller**, da tcpdump keine externen Nachschlagearbeiten machen muss.
- Daher: **-n wird empfohlen**, wenn du reinen Netzwerkverkehr sehen willst – so, wie er wirklich ist.

## Beispielbefehl:

bash

tcpdump -n -v

Das würde:

- **detaillierte Paketinfos anzeigen (-v)**
- **IP-Adressen und Ports nicht auflösen (-n)**

**logs:**

**Protokollierung und Warnmeldungen** sind wichtige Bestandteile jeder Sicherheitsarchitektur.

Nur Schutzmaßnahmen zu haben reicht nicht, man muss auch wissen, ob sie funktionieren (Einblick in Sicherheitssysteme).

Protokolle müssen gesichert, analysiert und überprüft werden.

In kleinen Unternehmen übernimmt oft das IT-Team die Analyse, in großen Unternehmen oft ein spezielles Sicherheitsteam.

Viele Systeme erstellen Protokolle (Logs) mit verschiedenen Details, z. B. Authentifizierungsversuche oder Firewall-Datenverkehr.

Protokolle helfen, Angriffsversuche und Kompromittierungen zu erkennen.

Unterschiedliche Systeme erzeugen Logs in verschiedenen Formaten, was die Analyse erschwert.

**SIEM-Systeme** (Security Information and Event Management) sammeln und konsolidieren Logs zentral.

Logs werden normalisiert, also in ein einheitliches Format gebracht, um sie einfacher analysieren zu können.

Es ist wichtig, das richtige Maß beim Protokollieren zu finden: Nicht zu viel (zu viel Daten), nicht zu wenig (zu wenig Infos).

Wichtige Log-Informationen: Zeitstempel, Ereigniscodes, Nutzerkonten, IP-Adressen, beteiligte Geräte.

Zentralisierte Log-Server erleichtern auch den Schutz der Logs vor Manipulation durch Angreifer.

Forensische Teams können so Ereignisse nach Sicherheitsvorfällen rekonstruieren.

Analyse der Logs hilft, Muster zu erkennen, z. B. ungewöhnlicher Datenverkehr oder wiederholte Fehlschläge bei Authentifizierungen.

Automatische Warnmeldungen können bei bestimmten Regeln ausgelöst werden (z. B. viele fehlgeschlagene Logins).

Viele SIEM-Lösungen bieten Dashboards zur besseren Visualisierung der Daten.

Logging-Analyse kann auch eigene Überwachungssysteme unterstützen.

Wichtig ist auch die **Aufbewahrung** von Logs: Dauer und Umfang beeinflussen Speicherbedarf.

Beispiele für Log- und SIEM-Tools: rsyslog (Open Source), Splunk, IBM Qradar, RSA Security Analytics.

## Laufwerkverschlüsselung:

- **Datenträgervollverschlüsselung (FDE)** schützt vor physischen Angriffen, z. B. bei Diebstahl oder Verlust von Geräten.
- FDE verschlüsselt die gesamte Festplatte, sodass Daten ohne Passwort unlesbar sind.
- Wichtig für Laptops, Smartphones, Tablets, aber auch empfohlen für Desktops und Server.
- FDE schützt nicht nur Vertraulichkeit, sondern auch die Integrität der Daten (böartige Manipulation wird erschwert).
- Zum Booten gibt es eine unverschlüsselte Partition mit kritischen Dateien (Kernel, Bootloader).
- Diese unverschlüsselte Partition ist potenziell angreifbar, aber Secure Boot schützt durch Code-Signatur vor Manipulation.
- Secure Boot nutzt Public-Key-Kryptographie: Nur signierte, vertrauenswürdige Bootdateien werden ausgeführt.
- Bekannte FDE-Lösungen: Microsoft BitLocker, Apple FileVault2, Linux dm-crypt, sowie Drittanbieter wie VeraCrypt.
- Verschlüsselung arbeitet mit geheimem Schlüssel, der oft durch Passwort geschützt ist.
- Passwort wird benötigt, um den Schlüssel zu entsperren und Zugriff auf Daten zu bekommen.
- Unternehmen nutzen Schlüsselaufbewahrung (Escrow), um bei vergessenen Passwörtern den Zugang wiederherzustellen.
- Unterschied FDE vs. dateibasierte Verschlüsselung (z. B. Home-Directory):
  - FDE verschlüsselt das ganze Laufwerk, Schutz bereits vor Booten erforderlich.

- Dateibasierte Verschlüsselung schützt nur einzelne Dateien/Ordner, ist benutzerfreundlicher, aber weniger sicher.
- Beim Neustart von vollverschlüsselten Systemen ist das Passwort vor dem Systemstart erforderlich.
- Dateibasierte Verschlüsselung bietet keinen Schutz gegen Manipulation der Systemdateien durch Angreifer mit physischem Zugriff.
- Sicherheitsarchitektur sollte Bedrohungen kennen und passende Maßnahmen (wie FDE) wählen.