

Ausarbeitung-Themenkatalog

1. Benutzerendgeräte und Peripheriegeräte (Vertiefung)

1.1 Hardwaresysteme

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

Hardwaresysteme	2
1.1.1 Fachbegriff Multicore-Prozessor	2
1.1.2 Unterschiede Desktop- vs. Server-Prozessoren	2
Mainboards & Architektur	2
1.1.3 Aufbau und Funktionsweise eines Mainboards	2
1.1.4 Fachbegriff Chipset (Chipsatz)	2
1.1.5 Fachbegriffe Jumper & DIP-Schalter	3
1.1.6 Formfaktoren (ATX, Micro-ATX)	3
1.1.7 Bussysteme	3
1.1.8 UEFI-Einstellungen (Unified Extensible Firmware Interface)	3
Drucker & Scanner	4
1.1.9 Plotter	4
1.1.10 Bubblejet- vs. Piezo-Technik.....	4
1.1.11 3D-Drucker (FDM-Verfahren)	4
Speicher & Netzteile.....	4
1.1.12 Das Netzteil (PSU)	4
1.1.13 HDD (Hard Disk Drive)	4
1.1.14 SSD (Solid State Drive)	5
1.1.15 SATA-Standards	5
Optische Medien & Monitore	5
1.1.16 Blu-ray (BD).....	5
1.1.17 Monitore & Auflösung	5
Schnittstellen.....	5

Hardwaresysteme

1.1.1 Fachbegriff Multicore-Prozessor

Ein Multicore-Prozessor vereint zwei oder mehr unabhängige Rechenkerne (**Cores**) auf einem einzigen Chip (Die).

- **Funktionsweise:** Durch **Parallelisierung** können mehrere Aufgaben gleichzeitig abgearbeitet werden.
- **Vorteil:** Höhere Gesamtleistung bei moderater Taktrate, was die Wärmeentwicklung reduziert.
- **Hyper-Threading:** Eine Technik (von Intel), bei der ein physischer Kern zwei logische Aufgaben (Threads) gleichzeitig bearbeiten kann.

1.1.2 Unterschiede Desktop- vs. Server-Prozessoren

Merkmal	Desktop-CPU (z. B. Intel Core, AMD Ryzen)	Server-CPU (z. B. Intel Xeon, AMD EPYC)
Kerne	Optimiert auf hohe Taktrate für Einzelleistungen.	Sehr hohe Kernanzahl für parallele Workloads.
Speicher	Unterstützt meist nur Standard-RAM (Dual-Channel).	Unterstützt ECC-RAM (Fehlerkorrektur) und viele Kanäle (Octa-Channel).
Dauerbetrieb	Für ca. 8-12 Std./Tag ausgelegt.	Ausgelegt auf 24/7-Dauerlast .
Cache	Kleinerer Cache.	Riesiger L3-Cache für schnelle Datenbereitstellung.
Multisockel	Nur eine CPU pro Mainboard.	Unterstützung für Mainboards mit 2, 4 oder mehr CPUs.

Mainboards & Architektur

1.1.3 Aufbau und Funktionsweise eines Mainboards

Das Mainboard (Motherboard) ist die zentrale Platine. Es verbindet alle Komponenten und stellt die Kommunikation sicher.

- **Komponenten:** CPU-Sockel, RAM-Slots, Chipsatz, PCIe-Steckplätze, SATA/M.2-Anschlüsse, Spannungsphasen (VRMs) und I/O-Panel (Anschlüsse hinten).

1.1.4 Fachbegriff Chipset (Chipsatz)

Der Chipsatz ist das „Gehirn“ des Mainboards. Er steuert den Datenfluss zwischen CPU, Speicher und Peripherie.

- **Früher:** Unterteilt in **Northbridge** (schnell: CPU, RAM, Grafik) und **Southbridge** (langsam: USB, SATA, PCI).
- **Heute:** Die Northbridge ist fast vollständig in die CPU gewandert. Der verbleibende Chipsatz (PCH - Platform Controller Hub) steuert die restlichen Schnittstellen.

1.1.5 Fachbegriffe Jumper & DIP-Schalter

Beide dienen der mechanischen Konfiguration von Hardware-Einstellungen (heute selten, meist im BIOS/UEFI ersetzt).

- **Jumper:** Eine kleine leitende Brücke, die zwei Pins kurzschließt, um eine Option zu aktivieren (z. B. BIOS-Reset).
- **DIP-Schalter:** Eine Reihe kleiner Schalter in einem Gehäuse (Dual In-line Package), die z. B. auf Industrie-Mainboards zur Adressierung genutzt werden.

1.1.6 Formfaktoren (ATX, Micro-ATX)

Der Formfaktor bestimmt die Abmessungen, Befestigungspunkte und die Anzahl der Steckplätze.

- **ATX (Advanced Technology Extended):** Standardgröße (ca. 305 × 244 mm). Viel Platz für Erweiterungskarten.
- **Micro-ATX (µATX):** Quadratischer, kompakter (ca. 244 × 244 mm). Passt in kleinere Gehäuse, hat aber weniger PCIe-Slots.

1.1.7 Bussysteme

Bussysteme sind „Datenautobahnen“.

- **PCI Express (PCIe):** Die aktuell wichtigste serielle Schnittstelle für Grafikkarten und NVMe-SSDs. Sie arbeitet mit **Lanes** (x1, x4, x8, x16).
- **Systembus:** Verbindet die CPU direkt mit dem Arbeitsspeicher.

1.1.8 UEFI-Einstellungen (Unified Extensible Firmware Interface)

Der moderne Nachfolger des BIOS. Wesentliche Einstellungen:

- **Boot Priority:** Reihenfolge der Laufwerke beim Start.
 - **Secure Boot:** Verhindert das Laden nicht signierter (potenziell schädlicher) Betriebssysteme.
 - **XMP/DOCP:** Profile zur automatischen Übertaktung des RAMs auf die Spezifikation.
 - **SATA-Mode:** Umstellung zwischen AHCI (Standard) und RAID.
-

Drucker & Scanner

1.1.9 Plotter

Ein Großformatdrucker. Klassische Plotter führen einen Stift über das Papier (**Vektor-Plotter**), moderne Plotter arbeiten meist mit großformatiger Tintenstrahltechnik für CAD-Pläne oder Werbebanner.

1.1.10 Bubblejet- vs. Piezo-Technik

- **Bubblejet (Canon/HP):** Tinte wird durch Erhitzen stoßartig verdampft. Die entstehende Gasblase drückt den Tropfen aus der Düse.
- **Piezo (Epson/Brother):** Ein Piezo-Kristall verformt sich durch elektrische Spannung mechanisch und drückt so den Tropfen heraus. Vorteil: Präziser und langlebiger, da keine Hitze entsteht.

1.1.11 3D-Drucker (FDM-Verfahren)

Das **Fused Deposition Modeling** ist am weitesten verbreitet. Ein Kunststoffdraht (**Filament**) wird geschmolzen und Schicht für Schicht auf ein Druckbett aufgetragen, bis das Objekt fertig ist.

1.1.12 Fachbegriffe Scanner

- **Interpolation:** Softwareseitiges „Hochrechnen“ der Auflösung (vorgeschwindelte Schärfe).
- **TWAIN:** Ein Standard-Protokoll zur Kommunikation zwischen Scanner und Software.
- **OCR (Optical Character Recognition):** Texterkennung, die gescanntes Bildmaterial in bearbeitbaren Text umwandelt.

Speicher & Netzteile

1.1.13 Das Netzteil (PSU)

- **Funktion:** Wandelt Wechselstrom (230V AC) in Gleichstrom (+3.3V, +5V, +12V DC) um.
- **Leistungsdaten:** Wichtig ist die **Effizienz (80 Plus Zertifikat)** und die Leistung auf der **12V-Schiene** (wichtig für CPU und GPU).

1.1.14 HDD (Hard Disk Drive)

- **Aufbau:** Magnetisierte rotierende Scheiben und bewegliche Leseköpfe.
- **Werte:** 5.400 oder 7.200 **U/min**. **Zugriffszeit** liegt im Millisekundenbereich (langsam durch mechanische Bewegung).

1.1.15 SSD (Solid State Drive)

- **Aufbau:** Flash-Speicher (NAND) ohne bewegliche Teile.
- **Zellentypen:**
 - **SLC (Single Level Cell):** 1 Bit pro Zelle. Teuer, extrem langlebig, schnell.
 - **MLC (Multi Level Cell):** 2 Bit pro Zelle. Guter Kompromiss.
 - **TLC (Triple Level Cell):** 3 Bit pro Zelle. Standard für Konsumenten, günstiger.

1.1.16 SATA-Standards

- **SATA III (6G):** Aktueller Standard mit max. **600 MB/s** Brutto-Datendurchsatz.

Optische Medien & Monitore

1.1.17 Blu-ray (BD)

- **BD-ROM:** Nur lesbar (gepresste Filme).
- **BD-R:** Einmal beschreibbar.
- **BD-RE:** Mehrfach wiederbeschreibbar (Rewritable).
- **Regionalcodes:** Begrenzen die Abspielbarkeit auf bestimmte Weltregionen (z. B. Region B für Europa).

1.1.18 Monitore & Auflösung

- **LCD (Liquid Crystal Display):** Flüssigkristalle, die Licht (Hintergrundbeleuchtung) filtern.
- **Full-HD:** 1920 × 1080 Pixel.
- **UHD (4K):** 3840 × 2160 Pixel.

Schnittstellen

- **HDMI:** Digitale Übertragung von Bild und Ton (Heimelektronik).
- **DisplayPort (DP):** Standard im IT-Bereich, höhere Bandbreite für hohe Bildwiederholraten, daisy-chain fähig.
- **Thunderbolt:** Basiert auf USB-C Stecker. Kombiniert PCIe und DisplayPort (extrem schnell, bis zu 80 Gbit/s).
- **USB (Universal Serial Bus):**
 - **USB 3.2 Gen 2x2:** 20 Gbit/s.
 - **USB4:** Basiert auf Thunderbolt 3 Technologie.
- **Serielle Schnittstelle (RS-232):** Überträgt Daten Bit für Bit nacheinander. Heute noch in der Industrie/Konsole zur Konfiguration von Switchen genutzt.

- **Firewire (IEEE 1394):** Früher Standard für Videokameras. Heute durch USB 3.0/Thunderbolt ersetzt.

Ausarbeitung-Themenkatalog

1. Benutzerendgeräte und Peripheriegeräte (Vertiefung)

1.2 Betriebssysteme und Software

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

1. Benutzerendgeräte und Peripheriegeräte (Vertiefung)	1
1.2 Betriebssysteme und Software	1
Betriebssysteme & Steuerung.....	2
1.2.1 Kenntnisse über Server-Betriebssysteme	2
1.2.2 Fachbegriff Firmware	2
1.2.3 Energiespar-Möglichkeiten (OS-gesteuert)	2
Linux & Shell.....	3
1.2.4 Kenntnisse über die Linux-Shell "Bash"	3
Dateisysteme & Netzwerkprotokolle	3
1.2.5 Fachbegriff Journaling-Dateisystem	3
Dateisystem-Standards	3
1.2.6 Fachbegriff CIFS (Common Internet File System).....	3

Betriebssysteme & Steuerung

1.2.1 Kenntnisse über Server-Betriebssysteme

Ein Server-Betriebssystem ist darauf optimiert, Dienste (Services) für mehrere Benutzer oder Clients gleichzeitig bereitzustellen.

- **Besonderheiten:** Fokus auf Stabilität, Sicherheit und Netzwerkleistung statt auf Multimedia. Oft besitzen Server-Systeme keine grafische Benutzeroberfläche (GUI), um Ressourcen zu sparen.
- **Wichtige Vertreter:**
 - **Windows Server:** (z. B. 2022) Stark in der Benutzerverwaltung (Active Directory).
 - **Linux-Server:** (z. B. Debian, Ubuntu Server, RHEL) Bekannt für Stabilität und Kosteneffizienz.
 - **Unix-Derivate:** (z. B. FreeBSD, Solaris) Für hochspezialisierte Enterprise-Umgebungen.

1.2.2 Fachbegriff Firmware

Firmware ist Software, die fest in die Hardware eingebettet ist (meist in einem EEPROM oder Flash-Speicher).

- **Funktion:** Sie bildet die unterste Software-Schicht, die direkt mit der Hardware kommuniziert. Sie ist nötig, damit ein Gerät überhaupt funktionsfähig ist.
- **Beispiele:** Das **UEFI/BIOS** eines PCs, die Steuerung einer Festplatte oder die Software in einem Router.

1.2.3 Energiespar-Möglichkeiten (OS-gesteuert)

Das Betriebssystem verwaltet die Hardware-Leistung über Schnittstellen wie **ACPI** (Advanced Configuration and Power Interface):

- **Standby (S3/Suspend to RAM):** Der RAM bleibt unter Strom, CPU und Festplatten schalten ab. Schnelles Aufwachen.
 - **Ruhezustand (S4/Hibernate):** Der RAM-Inhalt wird auf die Festplatte geschrieben, das System schaltet komplett ab. Sicher vor Stromausfall.
 - **CPU-Scaling:** Das OS taktet die CPU bei geringer Last herunter (P-States), um Hitze und Energie zu sparen.
 - **Display-Timeout:** Automatisches Abschalten des Monitors nach Inaktivität.
-

Linux & Shell

1.2.4 Kenntnisse über die Linux-Shell "Bash"

Die **Bash** (Bourne Again Shell) ist der Standard-Kommandozeileninterpreter für die meisten Linux-Distributionen.

- **Funktion:** Sie dient als Schnittstelle zwischen Benutzer und Kernel. Befehle werden textbasiert eingegeben und ausgeführt.
- **Features:** Skriptfähigkeit (Automatisierung), Pipe-Funktion (|) zum Verbinden von Befehlen und die Tab-Vervollständigung.
- **Wichtige Befehle:** ls (Listen), cd (Ordner wechseln), sudo (Admin-Rechte), grep (Suchen).

Dateisysteme & Netzwerkprotokolle

1.2.5 Fachbegriff Journaling-Dateisystem

Ein Dateisystem, das alle geplanten Änderungen vor der eigentlichen Ausführung in einem geschützten Bereich (dem **Journal**) protokolliert.

- **Nutzen:** Nach einem Systemabsturz oder Stromausfall kann das System das Journal auslesen und die Dateistruktur schnell wieder in einen konsistenten Zustand bringen, ohne die gesamte Festplatte prüfen zu müssen (verhindert Datenkorruption).

Dateisystem-Standards

Begriff	System	Beschreibung
ext4	Linux	Das Standard-Dateisystem für Linux. Unterstützt riesige Dateien und Partitionen, bietet Journaling und hohe Performance.
APFS	macOS	(Apple File System) Optimiert für SSDs. Unterstützt Snapshots, starke Verschlüsselung und dynamische Speicherplatzverteilung.
NTFS	Windows	Standard für Windows. Unterstützt Berechtigungen (ACLs), Komprimierung und Journaling.

1.2.6 Fachbegriff CIFS (Common Internet File System)

CIFS ist ein Netzwerkprotokoll, das ursprünglich von Microsoft entwickelt wurde.

- **Funktion:** Es ermöglicht den Zugriff auf Dateien und Drucker über ein Netzwerk.
 - **Zusammenhang:** CIFS ist eine spezifische Implementierung des **SMB-Protokolls** (Server Message Block). Es wird genutzt, um Netzlaufwerke in Windows-Umgebungen (und mittels *Samba* auch unter Linux) einzubinden.
-

Ausarbeitung-Themenkatalog

1. Benutzerendgeräte und Peripheriegeräte (Vertiefung)

1.3 Betreuung von mobiler Hardware

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

1. Benutzerendgeräte und Peripheriegeräte (Vertiefung)	1
1.3 Betreuung von mobiler Hardware	1
Betreuung von mobiler Hardware	2
1.3.1 Fachbegriff MDM (Mobile Device Management)	2
1.3.2 Fachbegriff Convertible	2
Hardware-Merkmale & Displays	2
1.3.3 Merkmale von Mobile-Prozessoren	2
1.3.4 Display-Technologien: E-Ink vs. OLED	2
Konnektivität & Funkstandards.....	3
1.3.5 Mobilfunkgenerationen.....	3
1.3.6 Fachbegriff HSDPA (High Speed Downlink Packet Access).....	3
1.3.7 Fachbegriff NFC (Near Field Communication).....	3
1.3.8 Fachbegriff GPS / GPS-Tracking.....	3
Sicherheit bei Diebstahl	4
1.3.9 Daten-Zugriffsschutzmöglichkeiten.....	4

Betreuung von mobiler Hardware

Die Betreuung umfasst den gesamten Lebenszyklus eines Geräts: **Provisionierung** (Einrichtung), **Verteilung**, **Wartung** (Updates) und das sichere **Ausphasen** (Datenlöschung). Ziel ist es, die Produktivität der Mitarbeiter zu sichern und gleichzeitig das Firmennetzwerk vor unbefugtem Zugriff durch mobile Clients zu schützen.

1.3.1 Fachbegriff MDM (Mobile Device Management)

MDM ist eine Softwarelösung zur zentralen Verwaltung von Mobilgeräten (Smartphones, Tablets, Laptops).

- **Funktionen:** Durchsetzen von Passwörterichtlinien, Fernlöschung (**Remote Wipe**) bei Verlust, automatische Installation von Apps und WLAN-Profilen sowie die Trennung von privaten und geschäftlichen Daten (Containerisierung).
- **Vorteil:** Erhöhte Sicherheit und enorme Zeitersparnis für die IT-Abteilung.

1.3.2 Fachbegriff Convertible

Ein Hybrid-Gerät, das die Eigenschaften eines **Laptops** und eines **Tablets** vereint.

- **Merkmale:** Es besitzt eine fest verbaute Tastatur, die jedoch durch ein 360-Grad-Scharnier umgeklappt werden kann. Die Bedienung erfolgt primär über einen Touchscreen oder Stift.
- **Abgrenzung:** Ein "Detachable" (wie das MS Surface Pro) ermöglicht hingegen das komplette Trennen der Tastatur vom Bildschirm.

Hardware-Merkmale & Displays

1.3.3 Merkmale von Mobile-Prozessoren

Mobile CPUs (z. B. ARM-Architektur in Handys oder Intel "U"-Serie in Laptops) sind auf **Effizienz** getrimmt.

- **SoC (System-on-a-Chip):** CPU, Grafik, RAM und Funkmodule sind oft auf einem einzigen Chip vereint.
- **Big.LITTLE-Architektur:** Nutzung von leistungsstarken Kernen für Aufgaben und stromsparenden Kernen für den Hintergrundbetrieb, um die Akkulaufzeit zu maximieren.
- **Geringe TDP:** Sie erzeugen wenig Hitze und benötigen oft keine aktive Kühlung (Lüfter).

1.3.4 Display-Technologien: E-Ink vs. OLED

- **E-Ink (Elektronische Tinte):** Nutzt Mikrokapseln mit geladenen Pigmenten.
 - **Vorteil:** Verbraucht nur Strom beim Umblättern, spiegelt nicht im Sonnenlicht, extrem augenschonend.
 - **Einsatz:** E-Reader (Kindle).

- **OLED (Organic Light Emitting Diode):** Jedes Pixel leuchtet selbst.
 - *Vorteil:* Perfektes Schwarz (Pixel schalten sich ab), extrem hoher Kontrast, dünne Bauweise.
 - *Nachteil:* Höherer Preis, Gefahr des "Einbrennens" bei statischen Bildern.

Konnektivität & Funkstandards

1.3.5 Mobilfunkgenerationen

Standard	Bezeichnung	Geschwindigkeit (ca.)	Bedeutung heute
2G	EDGE	bis 220 kbit/s	Nur noch für Notfall-Telefonie/SMS relevant.
3G	UMTS / HSDPA	bis 42 Mbit/s	In Deutschland/Österreich weitgehend abgeschaltet.
4G	LTE	bis 1000 Mbit/s	Aktueller Standard für flächendeckendes mobiles Internet.
5G	New Radio	bis 10 Gbit/s	Zukunftsstandard, extrem geringe Latenz, hohe Gerätedichte.

1.3.6 Fachbegriff HSDPA (High Speed Downlink Packet Access)

- **HSDPA:** Eine Erweiterung von 3G, die den Datenempfang massiv beschleunigte (oft als "H" oder "H+" im Display zu sehen).

1.3.7 Fachbegriff NFC (Near Field Communication)

Ein Funkstandard für die Übertragung von Daten über sehr kurze Distanzen (max. 4 cm).

- **Einsatz:** Kontaktloses Bezahlen (Apple/Google Pay), Koppeln von Bluetooth-Geräten, Zutrittskontrolle.

1.3.8 Fachbegriff GPS / GPS-Tracking

Global Positioning System: Ein satellitengestütztes System zur Positionsbestimmung.

- **Funktion:** Das Gerät empfängt Signale von mindestens vier Satelliten und berechnet per Laufzeitmessung den Standort.
 - **Tracking:** Das kontinuierliche Aufzeichnen oder Senden dieser Koordinaten (wichtig für Flottenmanagement oder Diebstahlschutz).
-

Sicherheit bei Diebstahl

1.3.9 Daten-Zugriffsschutzmöglichkeiten

Wenn ein mobiles Endgerät verloren geht, greifen mehrere Schutzmechanismen:

1. **Verschlüsselung (Encryption):** Bei modernen Smartphones (iOS/Android) sind die Daten standardmäßig verschlüsselt. Ohne PIN/Biometrie ist der Speicherchip unlesbar.
2. **Remote Wipe (Fernlöschung):** Über das MDM oder Dienste wie "Mein Gerät finden" kann das Gerät beim nächsten Internetkontakt vollständig gelöscht werden.
3. **App-Container:** Geschäftliche Daten liegen in einem verschlüsselten Tresor, der getrennt von privaten Fotos/Apps gelöscht werden kann.
4. **Aktivierungssperre:** Verhindert, dass ein gestohlenes Gerät nach einem Hard-Reset neu eingerichtet werden kann (macht das Gerät für Diebe wertlos).
5. **MFA (Multi-Faktor-Authentifizierung):** Schützt die Accounts auf dem Gerät, selbst wenn das Entsperrmuster bekannt ist.

Ausarbeitung-Themenkatalog

1. Benutzerendgeräte und Peripheriegeräte (Vertiefung)

1.4 Server-, Storage- und Rechenzentren

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

1. Benutzerendgeräte und Peripheriegeräte (Vertiefung)	1
1.4 Server-, Storage- und Rechenzentren	1
Server-Bauformen	2
1.4.1 Kenntnis der Unterschiede von Rackmount-Server und Blade-Server	2
1.4.2 Fachbegriff SAN	2
Speicherlösungen (Storage)	2
1.4.3 Kenntnisse über NAS-Systeme und deren Einsatzbereiche	2
1.4.4 Fachbegriff Snapshot	3
1.4.5 Fachbegriff Daten-Redundanz	3
Ausfallsicherheit & RAID	3
1.4.6 Fachbegriff RAID-Level (0/1/5)	3
1.4.7 Fachbegriffe Hot-Plugging und Hot-Spare	4
1.4.8 Fachbegriff Teaming in Zusammenhang mit Netzwerk-Ports	4
1.4.9 Unterscheidung von Offline- und Online-USV-Anlagen	4
1.4.10 Kenntnisse über optimale Klimatisierung in Rechenzentren	5
1.4.11 Kenntnisse über Zutrittsschutz/Zutrittskontrolle bei Rechenzentren	5
1.4.12 Kenntnisse über Cluster-Technologien (High Availability, Heart-Beat)	5
1.4.13 Kenntnisse über Hypervisor-Technologien (XEN, KVM, ESX, Hyper-V)	5
1.4.14 Kenntnisse über Virtualisierung (Server-Virtualisierung/Desktop-Virtualisierung)	6

Server-Bauformen

1.4.1 Kenntnis der Unterschiede von Rackmount-Server und Blade-Server

Rackmount-Server sind eigenständige Server, die in einem 19-Zoll-Rack montiert werden. Jeder Server besitzt eigene Netzteile, Kühlung und Netzwerkanschlüsse. Sie sind flexibel, einfacher zu warten und besonders für kleine bis mittlere Umgebungen geeignet.

Blade-Server bestehen aus mehreren kompakten Servermodulen (Blades), die in einem gemeinsamen Chassis betrieben werden. Stromversorgung, Kühlung und Netzwerk werden gemeinsam genutzt. Dadurch sind sie platzsparend, gut skalierbar, aber in der Anschaffung teurer.

Rackmount = flexibel & einzeln

Blade = platzsparend & zentral verwaltet

1.4.2 Fachbegriff SAN

Ein **SAN** ist ein spezialisiertes Hochleistungsnetzwerk zur Anbindung von Speicher an Server. Der Zugriff erfolgt blockbasiert, sodass Server den Speicher wie lokale Festplatten verwenden können.

SANs werden vor allem in **Virtualisierungs-, Datenbank- und Rechenzentrumsumgebungen** eingesetzt. Häufige Technologien sind **Fibre Channel** oder **iSCSI**.

Vorteile: hohe Performance, hohe Ausfallsicherheit

Nachteil: hohe Kosten, komplexe Konfiguration

Speicherlösungen (Storage)

1.4.3 Kenntnisse über NAS-Systeme und deren Einsatzbereiche

Ein **NAS (Network Attached Storage)** ist ein netzwerkgebundener Dateiserver. Der Zugriff erfolgt dateibasiert über Protokolle wie **SMB/CIFS** oder **NFS**.

Einsatzbereiche

- Dateifreigaben im Unternehmen
- Backups
- Multimedia- und Archivspeicher

Vorteile: einfache Verwaltung, kostengünstig

Nachteil: geringere Performance als SAN

1.4.4 Fachbegriff Snapshot

Ein **Snapshot** ist eine Momentaufnahme eines Datenbestandes zu einem bestimmten Zeitpunkt. Er speichert nicht alle Daten neu, sondern nur Änderungen seit der Aufnahme.

Snapshots ermöglichen eine **schnelle Wiederherstellung** bei Fehlern oder versehentlichem Löschen.

Snapshots ersetzen kein Backup, sondern ergänzen es.

1.4.5 Fachbegriff Daten-Redundanz

Daten-Redundanz bedeutet, dass Daten mehrfach gespeichert werden, um sie bei einem Ausfall weiterhin verfügbar zu halten.

Redundanz schützt vor **Hardwareausfällen**, nicht jedoch vor logischen Fehlern wie Viren oder versehentlichem Löschen.

Beispiele: RAID, Spiegelungen, Cluster

Achtung: Redundanz $\neq$ Backup

Ausfallsicherheit & RAID

1.4.6 Fachbegriff RAID-Level (0/1/5)

RAID kombiniert mehrere Festplatten zu einem logischen Laufwerk.

RAID 0:

Hohe Geschwindigkeit, keine Redundanz

RAID 1:

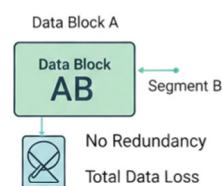
Spiegelung, hohe Datensicherheit

RAID 5:

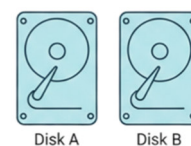
Verteilte Parität, guter Kompromiss zwischen Sicherheit und Speicherplatz

RAID (Redundant Array of Independent Disks)

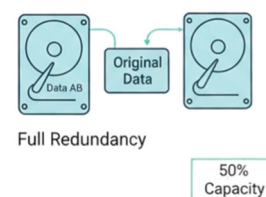
RAID 0 (Striping)



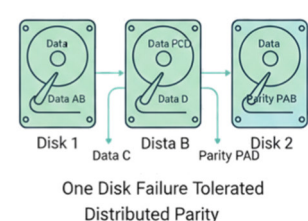
RAID 1 (Mirroring)



RAID 5 (Parity)



Disk 5 (Parity)



1.4.7 Fachbegriffe Hot-Plugging und Hot-Spare

Hot-Plugging erlaubt den Austausch von Hardware (z. B. Festplatten) im laufenden Betrieb, ohne den Server herunterzufahren.

Hot-Spare ist eine ungenutzte Ersatzfestplatte, die bei einem Defekt automatisch in ein RAID eingebunden wird.

Nutzen: höhere Verfügbarkeit, geringere Ausfallzeiten

1.4.8 Fachbegriff Teaming in Zusammenhang mit Netzwerk-Ports

Teaming bezeichnet das Zusammenschalten mehrerer Netzwerkkarten zu einer logischen Verbindung.

Ziele

- Ausfallsicherheit
- Höhere Bandbreite

Fällt eine Netzwerkkarte aus, übernehmen die anderen automatisch.

1.4.9 Unterscheidung von Offline- und Online-USV-Anlagen

Eine **USV (Unterbrechungsfreie Stromversorgung)** schützt IT-Systeme bei Stromausfall.

Offline-USV

Schaltet nur bei Stromausfall auf Batterie um

Online-USV

Versorgt Geräte permanent über Batterie und Wechselrichter

Merksatz

Offline = günstig

Online = maximaler Schutz

1.4.10 Kenntnisse über optimale Klimatisierung in Rechenzentren

Server erzeugen viel Wärme und benötigen eine kontrollierte Umgebung.

Wichtige Punkte

- Temperatur ca. 20–24 °C
- Geregelte Luftfeuchtigkeit
- Kaltgang-/Warmgang-Trennung
- Vermeidung von Hitzestau

Schlechte Kühlung führt zu **Hardwareausfällen** und kürzerer Lebensdauer.

1.4.11 Kenntnisse über Zutrittsschutz/Zutrittskontrolle bei Rechenzentren

Zutrittskontrolle ist Teil der **physischen Sicherheit**.

Maßnahmen

Chipkarten, PIN, biometrische Systeme

Protokollierung aller Zugriffe

Zutritt nur für autorisiertes Personal

Ziel: Schutz vor Diebstahl, Sabotage und Datenmissbrauch

1.4.12 Kenntnisse über Cluster-Technologien (High Availability, Heart-Beat)

Ein **Cluster** besteht aus mehreren Servern, die gemeinsam Dienste bereitstellen.

High Availability (HA): Dienste bleiben bei Serverausfall verfügbar

Heartbeat: Überwachungssignal zwischen den Knoten

Fällt ein Server aus, übernimmt automatisch ein anderer.

1.4.13 Kenntnisse über Hypervisor-Technologien (XEN, KVM, ESX, Hyper-V)

Ein Hypervisor verwaltet virtuelle Maschinen.

- Typ-1-Hypervisor: läuft direkt auf der Hardware
- Beispiele: XEN, KVM, ESX, Hyper-V

Vorteile: bessere Ressourcennutzung, flexible Serverbereitstellung

1.4.14 Kenntnisse über Virtualisierung (Server-Virtualisierung/Desktop-Virtualisierung)

Virtualisierung ermöglicht mehrere Betriebssysteme auf einer Hardware.

- Server-Virtualisierung: mehrere Server auf einem Host
- Desktop-Virtualisierung: zentrale Arbeitsplätze (VDI)

Vorteile

- Kosteneinsparung
- Einfache Verwaltung
- Schnelle Wiederherstellung



Ausarbeitung-Themenkatalog

2. Netzwerke (Vertiefung)

2.1 Netzwerktechnik

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

1. Kenntnisse über den Aufbau einer Routingtabelle.....	3
2. Kenntnisse über statisches Routing, dynamisches Routing.....	3
3. Fachbegriff Uplink-Port.....	4
4. Fachbegriff VLAN.....	4
5. Aufbau eines Koaxialkabels, Twisted-Pair-Kabels.....	4
6. Kenntnis der CAT6/6a/7-Spezifikationen.....	5
7. Aufbau eines LWL-Kabels.....	5
8. Unterscheidung der Fachbegriffe Monomode und Multimode.....	6
9. Fachbegriff Patch-Panel.....	6
10. Fachbegriff Netzwerkdose.....	6
11. Fachbegriff RJ45-Stecker.....	6
12. Fachbegriff PoE.....	6
13. Fachbegriff Ethernet.....	6
14. Aufbau eines Ethernet-Paketes.....	7
15. Fachbegriffe 100BaseTx, 1000Base-T, 10GBASE-T.....	7
16. Fachbegriffe Gbit-Ethernet, 10Gbit-Ethernet.....	8
17. Fachbegriff Traffic-Shaping.....	8
18. Fachbegriff Subnetmask.....	8
19. Aufbau eines IP-Paketes.....	8
20. Fachbegriffe Multicasting, Unicasting.....	8
21. Fachbegriffe Präfix und Interface Identifier in Zusammenhang mit IPv6.....	9
22. Fachbegriff Dual-Stack in Zusammenhang mit IPv4 und IPv6.....	9
23. Fachbegriff Port.....	9
24. Kenntnisse über NAT/PAT-Technologie.....	9

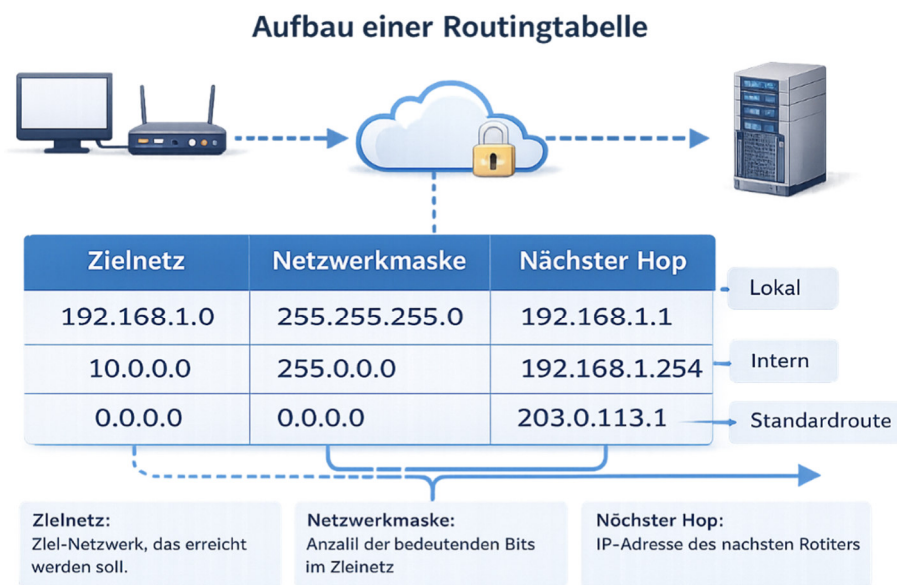
25. Kenntnisse über Port-Forwarding.....	10
26. Fachbegriff QoS.....	10
27. Fachbegriff WOL	10
28. Kenntnis über DSL-Technologien.....	10
29. Fachbegriff CATV-Modem.....	11
30. Fachbegriff FTTH	11
31. Fachbegriff Hotspot	11
32. Kenntnis der aktuellen WLAN-Standards und Verschlüsselungen	11
33. Standortwahl bei WLAN-Aufbau in Gebäuden	12
34. Fachbegriff Roaming in Zusammenhang mit Access-Points.....	13
35. Fachbegriff MAC-Filtering	13
36. Kenntnisse über VPN und Tunneling	13

2.1.1 Kenntnisse über den Aufbau einer Routingtabelle

Eine Routingtabelle enthält alle Informationen, die ein Router benötigt, um Pakete weiterzuleiten

- Zielnetz: Wohin soll das Paket?
- Subnetzmaske / Präfix: Größe des Zielnetzes
- Gateway (Next Hop): Nächster Router
- Interface: Über welchen Port gesendet wird
- Metrik: Bevorzugung bei mehreren Routen

Der Router wählt immer die spezifischste Route (Longest Prefix Match).



2.1.2 Kenntnisse über statisches Routing, dynamisches Routing

Statisches Routing

- Routen werden manuell konfiguriert
- Keine automatische Anpassung bei Ausfällen
- Typisch für kleine, übersichtliche Netze
- Sehr vorhersehbares Verhalten

Dynamisches Routing

- Router tauschen Routen über Routingprotokolle aus
- Passt sich automatisch bei Netzausfällen an
- Skaliert gut in großen Netzwerken
- Benötigt mehr Rechenleistung

2.1.3 Fachbegriff Uplink-Port

Uplink-Port

- Verbindung zwischen Switches oder Switch und Router
- Häufig höhere Geschwindigkeit
- Transportiert oft mehrere VLANs (Trunk)

2.1.4 Fachbegriff VLAN

Virtual Local Area Network

- Logische Aufteilung eines physischen Netzwerks
- Geräte können in getrennten Netzen sein, obwohl sie am selben Switch hängen
- Reduziert Broadcasts und erhöht Sicherheit

2.1.5 Aufbau eines Koaxialkabels, Twisted-Pair-Kabels

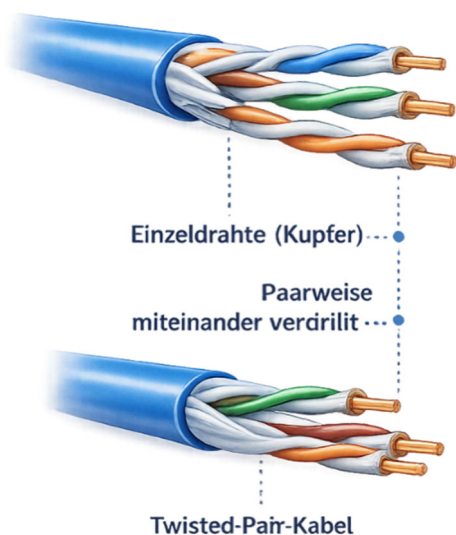
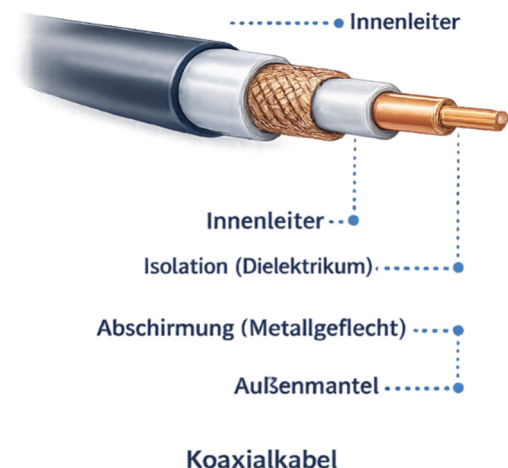
Koaxialkabel – Aufbau

Innenleiter überträgt Signal

Isolierung verhindert Kurzschluss

Abschirmung schützt vor Störungen

Heute hauptsächlich bei Kabelinternet



Twisted-Pair-Kabel – Aufbau

Vier verdrehte Adernpaare

Verdrillung reduziert elektromagnetische Störungen

Unterschiedliche Abschirmungen (UTP, STP, S/FTP)

2.1.6 Kenntnis der CAT6/6a/7-Spezifikationen

„CAT“ ist eine Kategorie für Twisted-Pair-Netzwerkkabel, die für schnelle Datenübertragungen in Netzwerken (LAN) ausgelegt sind.

Kategorie	Schirmung	Frequenz (MHz)	Datenrate	Max. Strecke	Resonderheiten
 CAT6	E oder U/UTP oder S/FTP	250	Bis zu 1 Gbit/s (10 Gbit/s)	bis zu 100 m (10 Gbit/s @ ≤ 55 m)	• 5GBASE-T und 10GBASE-T @ - 55m • welt verbreitet
 CAT8a	EA / STP	500	Bis zu 10 Gbit/s	bis zu 100 m	• Die amerikanische Norm Cat 8A ist weniger streng als die europäische Norm Cat 8A • Cat 8A ist keine offene Norm
 CAT7	F / S/FTP	600	Bis zu 10 Gbit/s	Bis zu 100 m	• CCTV • vier jeweils einzeln abgeschirmte Adempaare (Screened/Folled shielded Twisted Pair S/FP) innerhalb eines gemeinsamen Schirms

2.1.7 Aufbau eines LWL-Kabels

Aufbau eines LWL-Kabels



2.1.8 Unterscheidung der Fachbegriffe Monomode und Multimode

Monomode-(Singlemode) und **Multimode**-Glasfasern unterscheiden sich primär durch ihren Kerndurchmesser und die Art der Lichtübertragung.

Monomode-Fasern (kleiner Kern, ca. 9 μm) übertragen ein einziges Lichtsignal über sehr große Distanzen (bis zu 200 km).

Multimode-Fasern (größerer Kern, 50-62,5 μm) mehrere Lichtmoden gleichzeitig für kürzere Strecken (bis ca. 1 km) in Netzwerken nutzen.

2.1.9 Fachbegriff Patch-Panel

Ein Patchpanel (auch Patchfeld oder Rangierfeld) ist ein zentraler Verteilerkasten in der Netzwerktechnik, der als Schnittstelle zwischen fest verlegten Netzwerkkabeln (im Haus/Büro) und aktiven Geräten (wie Switches/Routern) dient.

- Endpunkt der festen Gebäudeverkabelung
- Verbindet strukturierte Verkabelung mit Switches
- Erleichtert Änderungen ohne Neuverkabelung

2.1.10 Fachbegriff Netzwerkdose

- Abschluss der strukturierten Verkabelung
- Verbindung zwischen Endgerät und Patchpanel

2.1.11 Fachbegriff RJ45-Stecker

- 8-poliger Steckverbinder
- Standard für Ethernet über Kupfer

2.1.12 Fachbegriff PoE

Power over Ethernet (PoE) ist eine Technologie, die Datenverbindung und Stromversorgung für netzwerkfähige Geräte (wie IP-Kameras, VoIP-Telefone, Access Points) über ein einziges Standard-Ethernet-Kabel (RJ45) kombiniert.

2.1.13 Fachbegriff Ethernet

Ethernet ist der Standard für die kabelgebundene Datenübertragung in lokalen Netzwerken (LAN). Es ermöglicht Geräten wie Computern, Druckern und Servern, innerhalb eines geschlossenen Systems stabil und schnell miteinander zu kommunizieren.

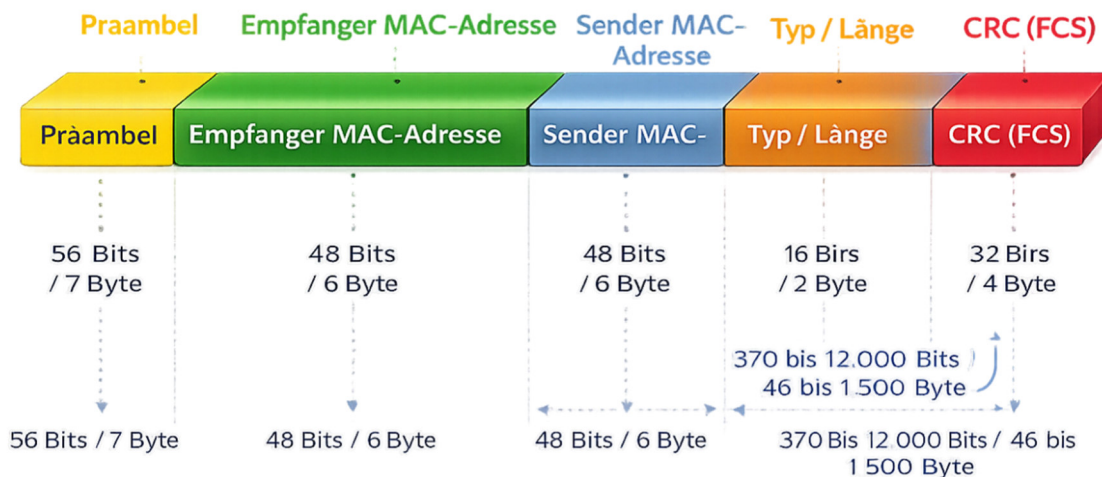
Technologie: Ethernet spezifiziert sowohl die Hardware (Kabel, Stecker wie RJ45, Netzwerkkarten) als auch die Software-Protokolle für den Datenaustausch.

Geschwindigkeit: Die Übertragungsraten reichen von 10 Megabit/s bis hin zu aktuell 400 Gigabit/s in Rechenzentren.

Vorteile: Im Vergleich zu WLAN bietet Ethernet eine höhere Stabilität, geringere Latenzzeiten und Schutz vor Funkstörungen.

Einsatz: Es wird in Privathaushalten (z. B. via Fritzbox), in Büros und in der Industrie (Industrial Ethernet) genutzt.

2.1.14 Aufbau eines Ethernet-Paketes



2.1.15 Fachbegriffe 100BaseTx, 1000Base-T, 10GBASE-T

Diese Begriffe bezeichnen verschiedene **Generationen von Ethernet-Standards**, die festlegen, wie schnell Daten über ein Kupferkabel übertragen werden (**IEEE 802.3**).

Der Aufbau der Namen

Zahl (100, 1000, 10G): Die maximale Übertragungsgeschwindigkeit in Megabit (Mbit/s) oder Gigabit (Gbit/s) pro Sekunde (TechTarget).

BASE: Steht für Basisband-Übertragung (das Signal nutzt das gesamte Kabelmedium) (Computer Weekly).

T / TX: Bezieht sich auf den Kabeltyp „Twisted Pair“ (verdrillte Kupferadern) (Zion Communication).

2.1.16 Fachbegriffe Gbit-Ethernet, 10Gbit-Ethernet

In der Netzwerktechnik beschreiben diese Begriffe die Geschwindigkeitsstufen eines Netzwerks.

Merkmal	Gigabit Ethernet (1G)	10-Gigabit Ethernet (10G)
Geschwindigkeit	1 Gbit/s (~125 MB/s)	10 Gbit/s (~1.250 MB/s)
Standard-Kabel	Cat 5e / Cat 6	Cat 6A / Cat 7 (FS.com)
Latenz	Niedrig	Sehr niedrig (wichtig für Echtzeit-Daten)
Kosten	Günstig (Standard-Hardware)	Teurer (Spezielle Netzwerkkarten/Switches)

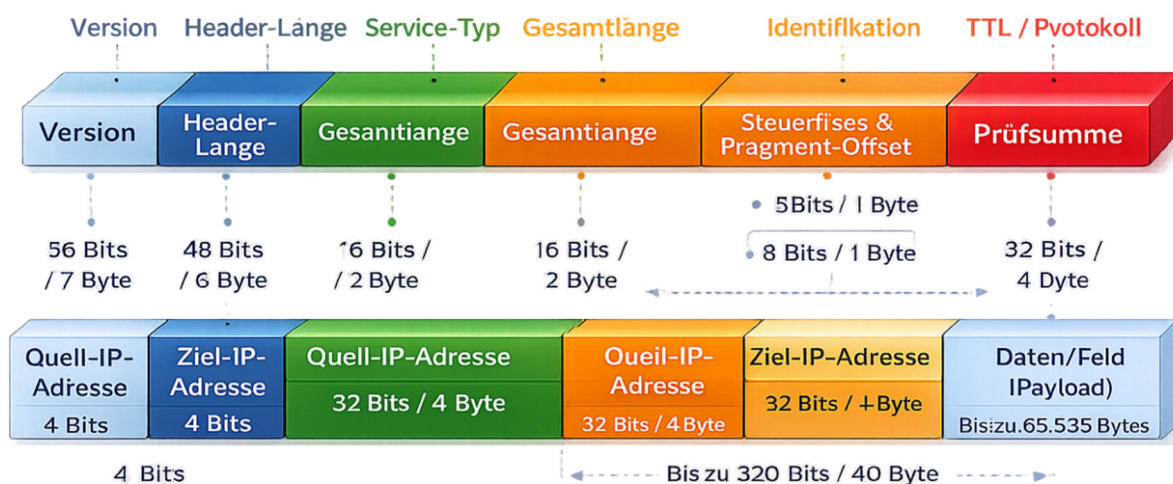
2.1.17 Fachbegriff Traffic-Shaping

Traffic Shaping (auch „Datenverkehrsformung“) ist eine Methode der Netzwerkverwaltung, bei der Datenpakete verzögert werden, um die Einhaltung eines bestimmten Bandbreitenlimits zu erzwingen.

2.1.18 Fachbegriff Subnetmask

Die Subnetzmaske ist eine Art „Trennlinie“ innerhalb einer IP-Adresse. Sie legt fest, welcher Teil der Adresse zum Netzwerk gehört und welcher Teil die einzelnen Geräte (Hosts) darin bezeichnet.

2.1.19 Aufbau eines IP-Paketes



2.1.20 Fachbegriffe Multicasting, Unicasting

Diese Begriffe beschreiben, an wie viele Empfänger ein Datenpaket im Netzwerk gesendet wird.

Unicasting: Ein Sender schickt Daten an genau **einen** bestimmten Empfänger.

Multicasting: Ein Sender schickt Daten an eine Gruppe von Empfängern gleichzeitig.

2.1.21 Fachbegriffe Präfix und Interface Identifier in Zusammenhang mit IPv6

In der Welt von IPv6 (dem Nachfolger von IPv4) besteht eine Adresse immer aus 128 Bit. Diese teilen sich in zwei genau gleich große Hälften: das Präfix und den Interface Identifier.

Das Präfix ist der Netzwerk-Teil der Adresse, es gibt an, in welchem Netzwerk sich das Gerät befindet.

Der Interface Identifier (IID) ist der Geräte-Teil der Adresse, er identifiziert das spezifische Gerät (das „Interface“) innerhalb des durch das Präfix definierten Netzwerks.

Beispiel einer IPv6-Adresse:

2001:0db8:85a3:08d3 : 1319:8a2e:0370:7344

- **Vor dem Doppelpunkt (links):** Das Präfix (Netzwerk).
- **Nach dem Doppelpunkt (rechts):** Der Interface Identifier (dein Gerät).

2.1.22 Fachbegriff Dual-Stack in Zusammenhang mit IPv4 und IPv6

Dual-Stack bezeichnet einen Betriebsmodus, bei dem ein Netzwerkgerät (wie ein Router oder PC) gleichzeitig mit IPv4 und IPv6 arbeitet.

Da das alte IPv4 und das neue IPv6 nicht direkt miteinander kompatibel sind, dient Dual-Stack als Übergangslösung.

2.1.23 Fachbegriff Port

In der Netzwerktechnik ist ein Port eine Art digitale Türnummer oder ein „Andockpunkt“ auf einem Computer.

2.1.24 Kenntnisse über NAT/PAT-Technologie

NAT (Network Address Translation) und **PAT** (Port Address Translation) sind die „Türsteher“ eines Routers. Sie ermöglichen es, dass viele Geräte in deinem privaten Netzwerk über nur eine einzige öffentliche IP-Adresse ins Internet gehen können.

NAT ist der Oberbegriff für das Verfahren, bei dem private IP-Adressen in öffentliche übersetzt werden.

PAT ist die extrem verbreitete Spezialform von NAT (oft auch „NAPT“ oder Masquerading genannt). Das ist das, was dein Router zu Hause macht.

2.1.25 Kenntnisse über Port-Forwarding

Port-Forwarding (Port-Weiterleitung) ist die bewusste Anweisung an einen Router, Anfragen aus dem Internet an ein ganz bestimmtes Gerät in deinem Heimnetzwerk durchzureichen.

Da der Router durch NAT/PAT normalerweise alle unaufgeforderten Anfragen von außen blockiert, fungiert Port-Forwarding als „gezieltes Loch“ in der Firewall.

2.1.26 Fachbegriff QoS

QoS steht für Quality of Service (Dienstgüte). Es ist ein Verfahren, mit dem sichergestellt wird, dass wichtige Anwendungen im Netzwerk bevorzugt behandelt werden, damit sie stabil und ohne Verzögerungen laufen.

Der Router erkennt, um welche Art von Daten es sich handelt und markiert die Pakete mit einem „Etikett“ (z. B. via DiffServ), das ihre Wichtigkeit anzeigt.

Wichtige Pakete werden in der Warteschlange nach vorne gereiht und zuerst versendet.

2.1.27 Fachbegriff WOL

WOL steht für Wake-on-LAN. Es ist ein Standard, der es ermöglicht, einen ausgeschalteten Computer über das Netzwerk einzuschalten

2.1.28 Kenntnis über DSL-Technologien

DSL (Digital Subscriber Line) ist eine Technologie, die das herkömmliche Kupfer-Telefonnetz nutzt, um Breitband-Internet bereitzustellen.

Technologie	Max. Download	Besonderheit
ADSL / ADSL2+	bis 16 Mbit/s	Asymmetrisch: Download deutlich schneller als Upload.
VDSL / VDSL2	bis 50 Mbit/s	Nutzt Glasfaser bis zum Verteilerkasten (FTTC) und Kupfer bis ins Haus.
Vectoring	bis 100 Mbit/s	Reduziert störendes „Übersprechen“ zwischen Kupferleitungen.
Supervectoring	bis 250 Mbit/s	Erweitert den Frequenzbereich für noch mehr Speed auf Kupfer.
G.fast	bis 1 Gbit/s	Neueste Technik für sehr kurze Distanzen (bis 250 m).

2.1.29 Fachbegriff CATV-Modem

Ein CATV-Modem (meist einfach Kabelmodem genannt) ist das Empfangsgerät für Internet über das Fernseekabelnetz.

Das Kürzel CATV steht historisch für Community Antenna Television (Kabelfernsehen).

2.1.30 Fachbegriff FTTH

FTTH steht für **Fiber to the Home** („Glasfaser bis in die Wohnung“). Es ist die derzeit leistungsfähigste Form des Internetanschlusses.

Das Besondere an FTTH

Im Gegensatz zu älteren Technologien (wie DSL oder VDSL) wird das Glasfaserkabel nicht nur bis zum Verteilerkasten an der Straße gelegt, sondern führt direkt bis in das Haus oder die Wohnung des Nutzers.

2.1.31 Fachbegriff Hotspot

Ein Hotspot ist ein öffentlicher oder privater Internet-Zugriffspunkt, der meist über WLAN (Wireless LAN) bereitgestellt wird.

Öffentliche Hotspots: Kostenlose oder kostenpflichtige Zugänge an Plätzen wie Flughäfen, Hotels, Cafés oder in Zügen.

Mobiler Hotspot (Tethering): Die Funktion eines Smartphones, seine mobile Datenverbindung (LTE/5G) per WLAN mit anderen Geräten wie Laptops oder Tablets zu teilen.

Privat-Hotspots: Router-Funktionen von Providern, bei denen ein Teil der Bandbreite (getrennt vom privaten Netz) für andere Kunden des Anbieters freigegeben wird.

2.1.32 Kenntnis der aktuellen WLAN-Standards und Verschlüsselungen

Generation	Technischer Name	Frequenzbänder	Max. Speed (theoretisch)	Fokus / Besonderheit
Wi-Fi 6 / 6E	802.11ax	2.4, 5, 6 GHz	bis 9,6 Gbit/s	Effizienz in dichten Netzen (viele Geräte).
Wi-Fi 7	802.11be	2.4, 5, 6 GHz	bis 46 Gbit/s	Extrem hoher Durchsatz ("Extremely High Throughput") und sehr geringe Latenz.
Wi-Fi 8	802.11bn	2.4, 5, 6 GHz	Fokus auf Zuverlässigkeit	Zielt auf Ultra High Reliability (UHR) ab; Finalisierung bis 2028 erwartet.

Aktuelle WLAN-Verschlüsselungen

Zur Absicherung des Datenverkehrs sind heute nur noch zwei Standards relevant, wobei der neuere Standard deutliche Sicherheitsvorteile bietet.

WPA3 (Wi-Fi Protected Access 3)

Der aktuelle Goldstandard

WPA2 (CCMP/AES)

Der langjährige Standard, der nach wie vor als sicher gilt, aber anfälliger für bestimmte Angriffe (z. B. KRACK) ist als WPA3.

Wird oft im Mixed Mode (WPA2 + WPA3) betrieben, um die Kompatibilität mit älteren Geräten zu gewährleisten.

2.1.33 Standortwahl bei WLAN-Aufbau in Gebäuden

- 1 Zentrale Positionierung
- 2 Erhöhte Aufstellung
- 3 Hindernisse und Störfaktoren
- 4 Abdeckung über Stockwerke



Bei der Standortwahl für WLAN-Router oder Access Points gilt: Die physikalische Platzierung ist oft wichtiger als die Sendeleistung. Hier sind die entscheidenden Regeln:

1. Zentrale Positionierung

360-Grad-Abdeckung: Funkwellen breiten sich kugelförmig aus. Platzieren Sie den Router in der Mitte der Wohnung/Etage, nicht in der Ecke oder im Abstellraum.

2. Erhöhte Aufstellung

Hindernisvermeidung: Möbel, Menschen und Haustiere dämpfen das Signal. Ein Standort in Augenhöhe oder höher (auf einem Schrank oder an der Wand) sorgt für eine bessere Sichtverbindung zu den Endgeräten.

3. Hindernisse und Störfaktoren

Materialien: Wasser (Aquarien), Metall (Heizkörper, Spiegelflächen) und Stahlbetonwände blockieren das Signal massiv.

Elektrosmog: Halten Sie Abstand zu Mikrowellen, Bluetooth-Geräten und Schnurlostelefonen, da diese oft auf demselben 2,4-GHz-Band funken.

4. Abdeckung über Stockwerke

Deckenmontage: In mehrgeschossigen Gebäuden ist eine versetzte Platzierung oder die Nutzung von Mesh-Repeater sinnvoll, da Decken aus Stahlbeton das Signal oft komplett schlucken.

2.1.34 Fachbegriff Roaming in Zusammenhang mit Access-Points

In der Netzwerktechnik beschreibt WLAN-Roaming den Vorgang, bei dem ein mobiles Endgerät (z. B. ein Smartphone) automatisch die Verbindung von einem Access Point zum nächsten wechselt, während du dich durch ein Gebäude bewegst.

2.1.35 Fachbegriff MAC-Filtering

- Nur bekannte Geräte dürfen ins WLAN
- Zusatzschutz, aber nicht allein ausreichend

2.1.36 Kenntnisse über VPN und Tunneling

Ein **VPN** (Virtual Private Network) ist ein **geschützter „Tunnel“**, der deine Daten verschlüsselt durch ein öffentliches Netzwerk (wie das Internet) leitet.

Beim Tunneling werden Datenpakete eines Netzwerkprotokolls in ein anderes Paket „eingepackt“ (Encapsulation).

VPN baut eine gesicherte Punkt-zu-Punkt-Verbindung auf, die Vertraulichkeit und Integrität deiner Daten im Internet garantiert.

Business-VPN (Remote Access): Ein Mitarbeiter startet auf seinem Laptop den Cisco AnyConnect oder FortiClient.

Privater Fernzugriff (Home-VPN): Du nutzt WireGuard auf deiner Fritz!Box, um im Urlaub über dein Smartphone sicher auf deine Smart-Home-Steuerung oder deine private Cloud (NAS) zuzugreifen.

Kommerzielle VPN-Dienste (Privatsphäre & Streaming): Dienste von Drittanbietern, um die eigene IP zu maskieren oder Ländersperren zu umgehen. → NordVPN, ExpressVPN oder Mullvad

Site-to-Site VPN (Standortkoppelung): Verbindet zwei komplette Netzwerke dauerhaft miteinander. → Die Zentrale einer Firma in Berlin ist dauerhaft über einen verschlüsselten Tunnel mit der Filiale in München verbunden.

Ausarbeitung-Themenkatalog

2. Netzwerke (Vertiefung)

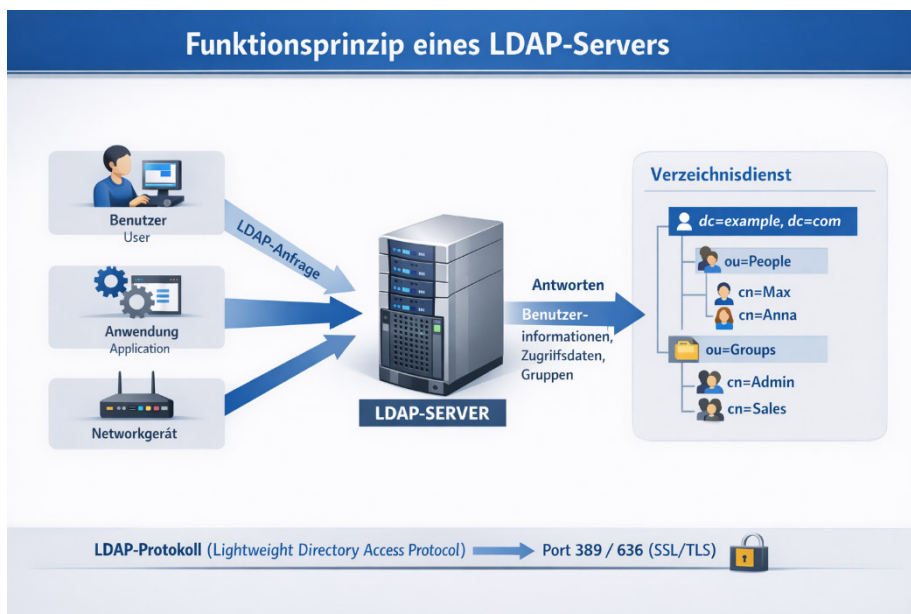
2.1 Netzwerkdienste

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrags im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

2. Netzwerke (Vertiefung).....	1
2.1 Netzwerkdienste	1
2.1.1 Funktionsprinzip eines LDAP-Servers	2
2.1.2 Funktionsprinzip eines Print-Servers.....	2
2.1.3 Kenntnisse über TFTP	3
2.1.4 Kenntnisse über SSH/Telnet	3
2.1.5 Kenntnisse über RDP	3
2.1.6 Kenntnisse über NFS.....	3
2.1.7 Kenntnisse über SMB.....	4
2.1.8 Fachbegriff NTP	5
2.1.9 Fachbegriff VoIP.....	5
2.1.10 Kenntnisse über die energieeffiziente Planung von IT-Systemen (Green-IT)	5

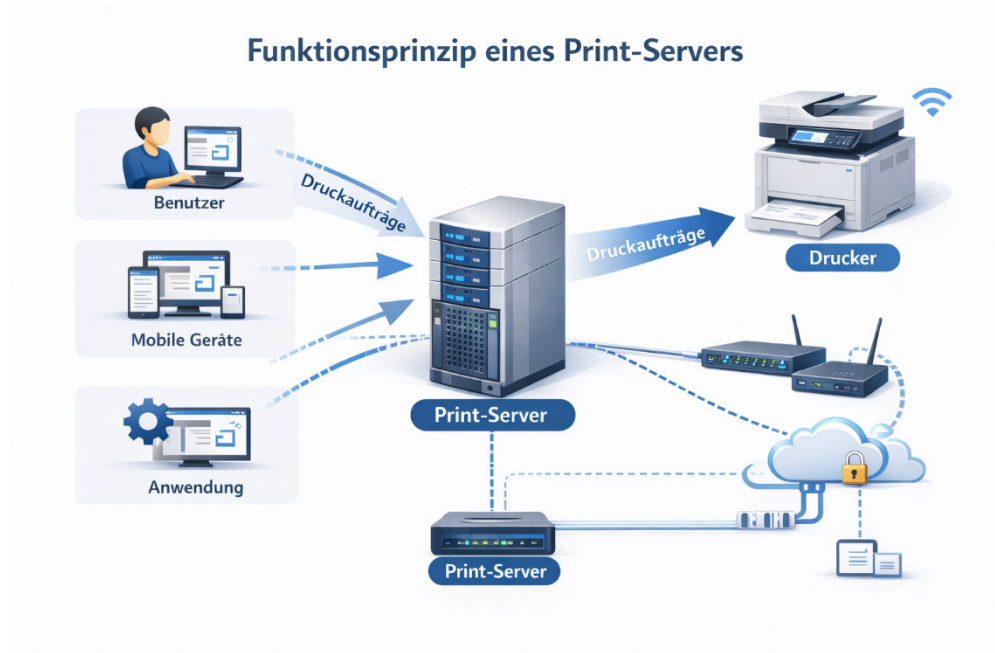
2.1.1 Funktionsprinzip eines LDAP-Servers



Ein LDAP-Server fungiert als zentraler Verzeichnisdienst, der auf einem Client-Server-Modell basiert, um Benutzeridentitäten, Zugangsdaten und Ressourcen in einer hierarchischen Baumstruktur zu speichern und zu verwalten.

2.1.2 Funktionsprinzip eines Print-Servers

Ein Print-Server fungiert als Vermittler in einem Netzwerk, der Druckaufträge von verschiedenen Clients (PCs) entgegennimmt, in einer Warteschlange (Spooler) ordnet und nacheinander an den angeschlossenen Drucker weiterleitet.



2.1.3 Kenntnisse über TFTP

TFTP (Trivial File Transfer Protocol) ist ein sehr einfaches, leichtgewichtiges Netzwerkprotokoll zur Dateiübertragung, das primär in lokalen Netzwerken (LAN) eingesetzt wird. Es basiert auf UDP (Port 69), bietet keine Authentifizierung oder Verschlüsselung und wird hauptsächlich für das Booten von Geräten (PXE) sowie das Übertragen von Firmware/Konfigurationen auf Router oder IP-Telefone genutzt.

2.1.4 Kenntnisse über SSH/Telnet

SSH (Secure Shell) und Telnet sind Netzwerkprotokolle zur Fernsteuerung von Computern, Routern oder Servern über eine Befehlszeilenschnittstelle. Während Telnet Daten unverschlüsselt im Klartext überträgt, bietet **SSH eine verschlüsselte Verbindung**, was es zum modernen Standard für sichere Remote-Verwaltungen macht.

2.1.5 Kenntnisse über RDP

Das **Remote Desktop Protocol (RDP)** ist ein von Microsoft entwickeltes Netzwerkprotokoll, das den Fernzugriff auf einen anderen Computer (Server oder PC) über eine grafische Oberfläche ermöglicht. Es überträgt Maus- und Tastatureingaben sowie Bildschirminhalte, sodass Nutzer arbeiten können, als säßen sie direkt vor dem entfernten Gerät.

Funktionsweise

RDP nutzt Port 3389 und verschlüsselt die Datenübertragung. Es erfordert einen RDP-Client (auf dem lokalen Rechner) und einen RDP-Server (auf dem Zielrechner).

Anwendungsbereiche

Fernwartung durch IT-Personal, Homeoffice-Zugriff auf Arbeitsplatzrechner, Zugriff auf virtuelle Maschinen in der Cloud.

Betriebssysteme

Hauptsächlich für Windows (Pro/Enterprise), aber auch Clients für macOS, Linux, Android und iOS verfügbar.

Vorteile

Ermöglicht ortsunabhängiges Arbeiten ohne zwingend ein VPN.

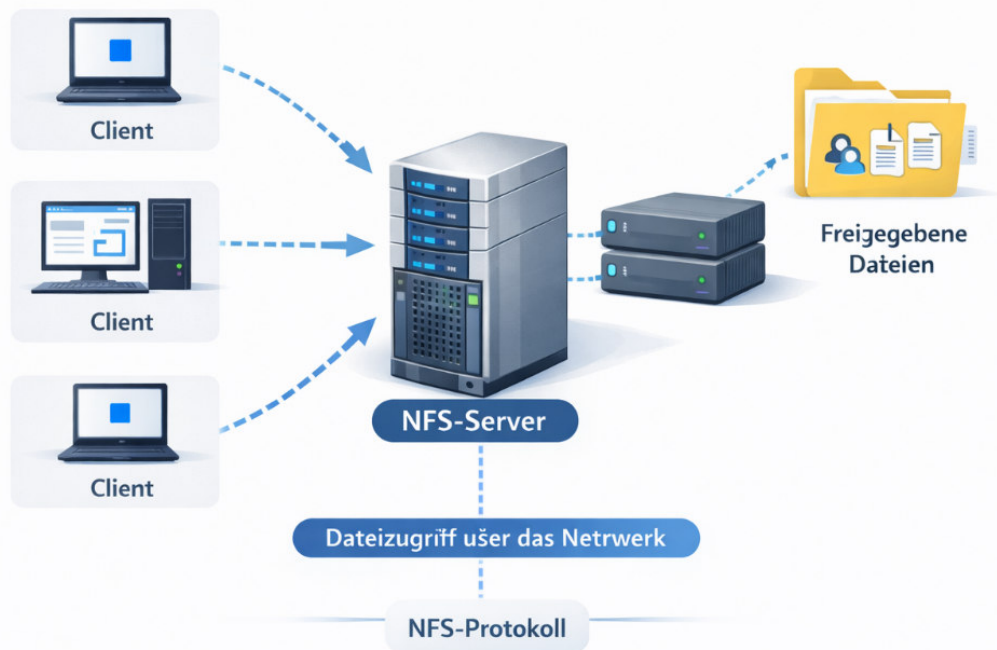
Sicherheitsrisiken

Offene RDP-Ports im Internet können Ziel von Hackerangriffen (Brute-Force) sein.

2.1.6 Kenntnisse über NFS

Network File System (NFS) ist ein von Sun Microsystems entwickeltes Client-Server-Protokoll, das den Zugriff auf Dateien über ein Netzwerk ermöglicht. Es erlaubt Benutzern, entfernte Verzeichnisse auf Unix/Linux-Systemen so zu mounten und zu bearbeiten, als wären sie lokale Festplatten. NFS ist ideal für den Datenaustausch und zentralisierte Speicherlösungen.

Funktionsprinzip von NFS (Network File System)



2.1.7 Kenntnisse über SMB

Server Message Block (SMB) ist ein weit verbreitetes Netzwerkprotokoll, das den gemeinsamen Zugriff auf Dateien, Drucker und andere Netzwerkressourcen ermöglicht. Es fungiert als Client-Server-Protokoll, hauptsächlich in Windows-Umgebungen, und ermöglicht das Lesen, Schreiben und Bearbeiten von Daten auf Remote-Servern oder NAS-Systemen über das lokale Netzwerk (LAN).

Funktion: Es ermöglicht das Freigeben von Dateien und Verzeichnissen sowie den Zugriff auf Drucker.

Betriebssysteme: Hauptsächlich in Windows genutzt, aber auch auf Linux und macOS verfügbar (oft via Samba).

Protokoll-Versionen: SMB hat sich weiterentwickelt, wobei ältere Versionen wie SMB1 als unsicher gelten. Moderne Versionen sind **SMB2, SMB3**.

Port: Heutige Versionen nutzen den **TCP-Port 445**.

SMB ist essenziell für die Arbeit in Unternehmensnetzwerken, da es den Zugriff auf zentralen Speicher (NAS) erlaubt.

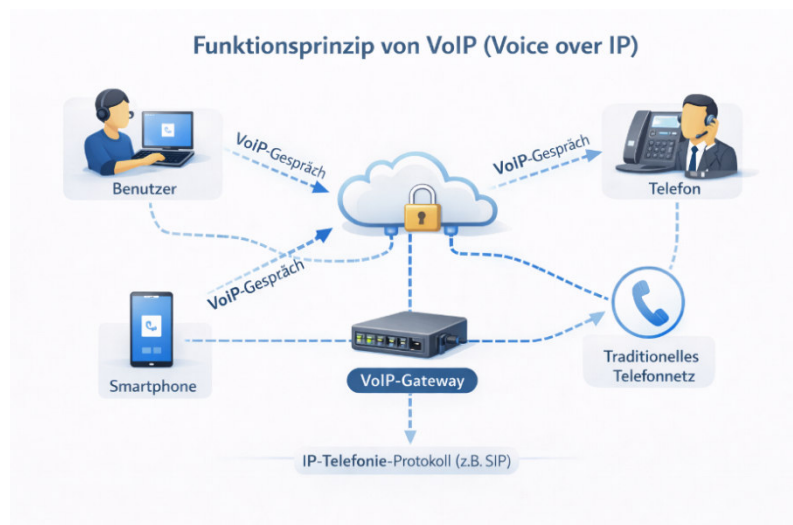
2.1.8 Fachbegriff NTP

NTP (**Network Time Protocol**) ist ein Standardprotokoll, um Uhren von Computersystemen über paketbasierte Netzwerke (LAN/Internet) zu synchronisieren.

Es ermöglicht die präzise Angleichung an die koordinierte Weltzeit (UTC), meist im Millisekundenbereich, und läuft typischerweise über **UDP-Port 123**. NTP ist essenziell für Logfiles, Sicherheitszertifikate und Netzwerksynchronisation.

2.1.9 Fachbegriff VoIP

Voice over Internet Protocol (VoIP) ist eine Technologie zum Telefonieren über das Internet statt über herkömmliche Telefonleitungen. Sprachsignale werden digitalisiert, in Datenpakete umgewandelt und via IP-Netzwerk (Internet) übertragen. Diese Methode ermöglicht kostengünstigere Gespräche, Flexibilität (Home-Office) und ist der heutige Standard (All-IP).



2.1.10 Kenntnisse über die energieeffiziente Planung von IT-Systemen (Green-IT)



Die energieeffiziente Planung von IT-Systemen (Green-IT) zielt darauf ab, den gesamten Lebenszyklus von IT-Infrastruktur – von Herstellung über Nutzung bis zur Entsorgung – umweltfreundlicher zu gestalten, um Energie zu sparen, Ressourcen zu schonen und Emissionen zu reduzieren. Dies umfasst den Einsatz stromsparender Hardware, Virtualisierung, optimierter Rechenzentren und nachhaltiger Software.

Ausarbeitung-Themenkatalog

2. Netzwerke

2.1 Systemadministration

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrage im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

2. Netzwerke	1
2.1 Systemadministration	1
Systemadministration	2
2.1.1 Kenntnisse über Active Directory (AD)	2
2.1.1.1 Fachbegriffe: Rollen und Features (Windows Server)	2
2.1.2 Konfiguration der IP-Adresse und Netzwerkeinstellungen	2
2.1.3 Einrichten eines Backup-Jobs	2
2.1.4 Installation und Aktualisierung von Treibern	3
2.1.5 Vorgangsweise bei Sicherheits-Patches	3
2.1.6 Vorgangsweise bei Service-Packs	3
2.1.7 Kenntnisse über die Registry	3
2.1.8 Anlegen neuer Benutzerprofile	3
2.1.9 Konfiguration eines neuen Mailkontos	3

Systemadministration

Die Systemadministration umfasst die **Verwaltung, Konfiguration und Wartung** von IT-Systemen (Server, Clients, Netzwerke). Ziel ist es, die Verfügbarkeit, Sicherheit und Leistungsfähigkeit der IT-Infrastruktur sicherzustellen. Dazu gehören Benutzerverwaltung, Monitoring, Backup-Management und Fehlerbehebung.

2.1.1 Kenntnisse über Active Directory (AD)

Das Active Directory ist der **zentrale Verzeichnisdienst** von Microsoft Windows Server. Es ermöglicht eine hierarchische Strukturierung von Objekten (Benutzer, Computer, Gruppen) in einer Domäne.

- **Zentrale Authentifizierung:** Benutzer melden sich einmal an und erhalten Zugriff auf alle berechtigten Ressourcen (Single Sign-On).
- **Gruppenrichtlinien (GPOs):** Zentrale Steuerung von Konfigurationen und Sicherheitsvorgaben für alle Clients.

2.1.2 Fachbegriffe: Rollen und Features (Windows Server)

- **Rollen:** Definieren die Hauptfunktion eines Servers (z. B. Domänencontroller, Fileserver, Webserver). Eine Rolle umfasst meist mehrere Dienste.
- **Features:** Zusätzliche Software-Funktionen, die die Arbeit des Servers unterstützen oder ergänzen (z. B. Backup-Software, .NET Framework, BitLocker), aber nicht die primäre Aufgabe des Servers darstellen.
-

2.1.3 Konfiguration der IP-Adresse und Netzwerkeinstellungen

Damit ein Gerät im Netzwerk kommunizieren kann, benötigt es:

- **IP-Adresse:** Eindeutige Kennung im Netzwerk.
- **Subnetzmaske:** Trennt die IP-Adresse in Netzwerk- und Host-Teil.
- **Standardgateway:** Die Adresse des Routers, der Anfragen in andere Netze (z. B. Internet) leitet.
- **DNS-Server:** Löst Namen (z. B. google.at) in IP-Adressen auf.

2.1.4 Einrichten eines Backup-Jobs

Ein Backup-Job ist ein **automatisierter Vorgang** zur Datensicherung. Er definiert:

- **Was:** (Dateien, Systemstatus oder komplettes Image).
- **Wann:** (Zeitplan, z. B. täglich 22:00 Uhr).
- **Wohin:** (Zielmedium: NAS, Cloud, Tape).
- **Wie:** (Backup-Methoden: Full, Incremental oder Differential).

2.1.5 Installation und Aktualisierung von Treibern

Ein Treiber ist die **Schnittstelle zwischen Hardware und Betriebssystem**.

- **Installation:** Einbinden der Steuerungssoftware, damit das OS die Hardware erkennt.
- **Aktualisierung:** Dient der Fehlerbehebung, Leistungssteigerung oder dem Schließen von Sicherheitslücken. Wichtig: Vorher oft Prüfung via Geräte-Manager oder Hersteller-Tools.

2.1.6 Vorgangsweise bei Sicherheits-Patches

Sicherheits-Patches beheben spezifische Schwachstellen.

1. **Testphase:** Patch in einer Testumgebung installieren.
2. **Backup:** Aktuelle Sicherung des Zielsystems erstellen.
3. **Deployment:** Rollout (meist via WSUS oder SCCM).
4. **Verifizierung:** Kontrolle, ob der Patch korrekt übernommen wurde.

2.1.7 Vorgangsweise bei Service-Packs

Ein Service-Pack (heute oft "Feature Update") ist eine **Sammlung vieler Patches und Funktionserweiterungen**.

- **Vorgehen:** Da Service-Packs tief in das System eingreifen, ist hier ein **Full-System-Backup** zwingend. Meist ist ein Neustart und eine längere Downtime einzuplanen.

2.1.8 Kenntnisse über die Registry

Die Windows-Registry ist eine **zentrale Datenbank**, in der Konfigurationsdaten des Betriebssystems und der installierten Programme gespeichert werden. Sie ist hierarchisch in "Hives" (z. B. HKEY_LOCAL_MACHINE) gegliedert.

Hinweis: Änderungen hier sind riskant und sollten nur nach einem Export (Sicherung) der Schlüssel vorgenommen werden.

2.1.9 Anlegen neuer Benutzerprofile

Ein Benutzerprofil enthält die **individuellen Einstellungen** eines Users (Desktop-Hintergrund, App-Daten, Dokumente).

- **Lokal:** Nur auf einem PC gespeichert.
- **Servergespeichert (Roaming):** Das Profil liegt auf einem Server und wird bei jeder Anmeldung auf den jeweiligen Client geladen.

2.1.10 Konfiguration eines neuen Mailkontos

Hierfür werden folgende Protokolle/Daten benötigt:

- **E-Mail-Adresse & Passwort.**

- **Posteingangsserver: IMAP** (Mails bleiben auf dem Server) oder **POP3** (Mails werden meist heruntergeladen).
- **Postausgangsserver: SMTP** (Zuständig für den Versand).
- **Verschlüsselung:** TLS/SSL für eine sichere Übertragung.

Ausarbeitung-Themenkatalog

3. IT-Management

Dieses Dokument zeigt die Ausarbeitung eines Arbeitsauftrage im Unterrichtsfach **LAP-Prüfungsvorbereitung mit Hr. Pesendorfer**.

Inhalt

3. IT-Management.....	1
IT-Management.....	2
3.1 ITIL (Information Technology Infrastructure Library)	2
3.2 CMDB (Configuration Management Database)	2
3.3 CI (Configuration Item).....	2
Incident, Problem & Change Management	2
Verträge & Dokumentation	3
3.4 Assetmanagement	3
3.5 SLA (Service Level Agreement).....	3
Praktische Umsetzung	3
3.6 Bedienungsanleitungen für Anwendungen	3
3.7 Inbetriebnahme-Protokoll.....	3
3.8 Netzwerkpläne & Technische Symbole.....	3
3.9 IT-Zertifizierungen am Markt	4

IT-Management

Die Planung, Steuerung und Überwachung der IT-Ressourcen eines Unternehmens. Ziel ist es, die IT-Infrastruktur so auszurichten, dass sie die Geschäftsziele optimal unterstützt (Business-IT-Alignment).

3.1 ITIL (Information Technology Infrastructure Library)

Ein weltweit anerkannter **Best-Practice-Leitfaden** für das IT-Service-Management (ITSM). ITIL beschreibt Prozesse, Funktionen und Rollen, um IT-Dienstleistungen effizient und kundenorientiert bereitzustellen.

3.2 CMDB (Configuration Management Database)

Eine zentrale Datenbank, die Informationen über alle Komponenten eines IT-Systems enthält. Sie speichert nicht nur die Daten der Komponenten, sondern vor allem deren **Beziehungen** untereinander.

3.3 CI (Configuration Item)

Ein CI ist die kleinste Einheit innerhalb der CMDB. Das kann Hardware (Server, PC), Software, Dokumentation oder sogar Personal sein. Jedes CI wird durch Attribute beschrieben.

Incident, Problem & Change Management

Im ITIL-Framework ist die Unterscheidung dieser Begriffe essenziell:

Fachbegriff	Definition	Ziel
Incident	Eine ungeplante Unterbrechung oder Qualitätsminderung eines IT-Services (eine Störung).	Schnellstmögliche Wiederherstellung des Service.
Problem	Die (oft unbekannte) Ursache eines oder mehrerer Incidents.	Ursachenforschung und dauerhafte Behebung (Root Cause Analysis).
Change	Das Hinzufügen, Modifizieren oder Entfernen von Komponenten, die Auswirkungen auf die IT-Services haben könnten.	Risikominimierung bei Veränderungen am System.

Verträge & Dokumentation

3.4 Assetmanagement

Die Verwaltung aller materiellen und immateriellen Werte (Assets) einer IT-Abteilung über deren gesamten Lebenszyklus hinweg (Beschaffung, Betrieb, Entsorgung). Fokus liegt hier oft auf Kosten und Inventarisierung.

3.5 SLA (Service Level Agreement)

Ein Vertrag zwischen einem IT-Dienstleister und einem Kunden. Er legt die Qualität, Verfügbarkeit und Antwortzeiten (z. B. "99,9% Uptime") der vereinbarten IT-Services fest.

Wartungsverträge (Wesentliche Inhalte)

- **Leistungsumfang:** Was wird gewartet (Hardware/Software)?
- **Reaktionszeiten:** Wie schnell muss der Support reagieren?
- **Wartungsintervalle:** Wie oft finden Überprüfungen statt?
- **Kosten:** Pauschalen oder Abrechnung nach Aufwand.
- **Haftung:** Wer kommt für Schäden bei Ausfällen auf?

Praktische Umsetzung

3.6 Bedienungsanleitungen für Anwendungen

Dokumente, die dem Endanwender Schritt für Schritt erklären, wie eine Software zu bedienen ist. Wichtig sind: Zielgruppenorientierung, klare Struktur, Screenshots und Fehlerbehebungshinweise.

3.7 Inbetriebnahme-Protokoll

Ein Dokument, das den Zustand eines IT-Systems zum Zeitpunkt der Übergabe an den Kunden festhält. Es dient als **Nachweis der ordnungsgemäßen Funktion** und als rechtliche Absicherung.

- Inhalt: Checklisten, Testergebnisse, Abnahmesignatur.

3.8 Netzwerkpläne & Technische Symbole

Grafische Darstellung der Netzwerkstruktur. Unterschieden wird zwischen:

- **Logischem Plan:** IP-Adressen, VLANs, Subnetze.
 - **Physischem Plan:** Tatsächliche Verkabelung, Standorte der Switches/Server.
 - **Symbole:** Standardisierte Icons für Router, Switch, Firewall, Server und Endgeräte.
-

3.9 IT-Zertifizierungen am Markt

Um die fachliche Kompetenz nachzuweisen, sind folgende Zertifizierungen hoch angesehen:

- **ITIL Foundation:** Basiswissen im Service Management.
- **CompTIA (A+, Network+, Security+):** Herstellerneutrale Grundlagenausbildung.
- **Microsoft Certified (AZ-900 etc.):** Fokus auf Azure und Windows-Umgebungen.
- **Cisco (CCNA):** Fokus auf Netzwerktechnik.
- **LPIC:** Zertifizierung für Linux-Administratoren.