



Unternehmen für Bildung.

Clients im Rechnernetzwerk einbinden

Modul: **ITG / C**

Version: 1.0
Oktober 2021

Erstellt von: Markus Bohnenkamp

Modul: **ITG / C - Clients im Rechnernetzwerk einbinden**

Version, Datum: 1.0, Oktober 2021

Erstellt von: Markus Bohnenkamp

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie oder einem anderen Verfahren) ohne Genehmigung des Herausgebers reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Die Modulunterlage und alle ihre Bestandteile wurden mit großer Sorgfalt erstellt und geprüft. Dennoch können Fehler nicht vollkommen ausgeschlossen werden. Der Herausgeber und die Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Literaturhinweis

Titel: IT-Berufe Grundstufe

ISBN: 978-3-14-220000-2

Verlag: Westermann Gruppe

Inhalt

TAG 1 - Eine Einführung in das Netzwerk des Ausbildungsbetriebs geben	7
Lernzielkontrollen TAG 1	10
TAG 2 und TAG 3 - Hauptbestandteile von Computernetzen unterscheiden	12
LE 1 - Computernetzwerke und deren Hauptbestandteile im Überblick unterscheiden	12
LE 2 - Netzbereiche im Überblick unterscheiden.....	14
(1) VLAN (virtuelles LAN).....	15
(2) VPN (Virtual Private Network)	15
LE 3 - Rechenzentren und Serversysteme unterscheiden	16
(1) Lokales Rechenzentrum (On-Premises)	16
(2) Externes Rechenzentrum (Off-Premises)	17
(3) Colocation.....	17
(4) Servertypen und deren Dienste beschreiben	18
LE 4 - Clients im Überblick unterscheiden.....	18
Netzwerk-Clients	19
Lernzielkontrollen TAG 2 und TAG 3.....	21
TAG 4 und TAG 5 - Grundlagen der Datenübertragung in Netzwerken	24
LE 1 - Funktionsweise von Rechnernetzen verstehen	25
(1) Datenübertragung und deren Kenngrößen	25
(2) Übertragungsarten.....	29
(3) Adressierungsarten im Netzwerk.....	30
LE 2 - Den Zugriff auf die Netzwerkmedien verstehen	30
LE 3 - Ethernet als Netzwerkstandard verwenden	31
(1) Ethernet-Frame-Aufbau	32
(2) Ethernet-Frame-Aufbau mit VLAN-Erweiterung	32
LE 4 - TCP/IP als Netzwerkstandard verwenden	33
LE 5 - Cloud-, Fog- und Edge-Computing unterscheiden	34
Lernzielkontrollen TAG 4 und TAG 5.....	36
TAG 6, TAG 7 und TAG 8- Netzwerkstrukturen, -komponenten, -standards und -modelle unterscheiden	39
LE 1- Netzwerktopologien unterscheiden	39
LE 2 - Strukturierte Verkabelung herstellen.....	40
(1) Beschriftung von Dosen und Verteilern	43
(2) Netzwerkmedien	44
(3) Komponentenkategorien und Verkabelungsklassen	44
(4) Funk, elektromagnetische Wellen	45
(5) Gängige Netzwerkbezeichnungen.....	45
LE 3 - Netzwerkmedien unterscheiden und spezifizieren.....	46
(1) Kupferleitungen.....	47
(2) Lichtwellenleiter	47
(3) Funk, WLAN/Wi-Fi.....	49
LE 4 - Netzwerkkomponenten unterscheiden.....	50
(1) Switchtypen	52

(2) Managebare Switches	53
(3) Die Arbeitsweise von Routern verstehen	54
LE 5 - Netzwerkstandards unterscheiden	54
LE 6 - ISO/OSI- und TCP/IP-Modell unterscheiden	56
(1) Netzwerkprotokollstapel	58
(2) Dienst-Protokolle	59
LE 7 - Adressen im Netzwerk unterscheiden.....	60
(1) Aufbau von MAC-Adressen	60
(2) Aufbau von IP-Adressen.....	61
(3) Einteilen der IP-Adressen in Adressklassen (historisch).....	62
(4) IP-Spezialadressen	63
(5) Private IP-Adressbereiche	63
LE 8 - Neue Entwicklungen der Netzwerktechnik präsentieren.....	63
Lernzielkontrollen TAG 6, TAG 7 und TAG 8	64
TAG 9 - Selbstständig die Integration von Clients in ein Netzwerk planen und durchführen	71
LE 1 - Anforderungen der Clients und des Netzwerkes prüfen	71
(1) Ist-Aufnahme durchführen	73
(2) Das Netzwerk dokumentieren	75
(3) Clients ins Netz einbinden	79
(4) Clients mit einem WLAN verbinden.....	80
(5) IP-Konfiguration einstellen und überprüfen (Windows und Linux)	81
(6) Statische und dynamische IP-Adressen/DHCP	84
LE 2 -Cloud-Dienste nutzen.....	84
(1) Anbieter von Cloud-Services	84
(2) Speicher in der Cloud nutzen	84
(3) Büroanwendungen in der Cloud nutzen	85
LE 3 - Benutzer anmelden	86
(1) Lokalen Benutzer erstellen	86
(2) Netzwerkbenutzer	87
Lernzielkontrollen TAG 9	87
TAG 10 - Die Netzwerkfunktion der Clients prüfen und warten	90
LE 1 - Verbindungstest durchführen	90
(1) Ping-Befehl	90
(2) Traceroute	92
LE 2 - Namensauflösung prüfen und einen Schnelltest durchführen	92
(1) Namensauflösung des Domain Name Systems (DNS) testen	92
(2) Schnelltest durchführen.....	93
LE 3 - Management und vorbeugende Wartung.....	93
(1) Agieren und Reagieren.....	93
(2) Systemüberwachung mit Bordmitteln	94
Lernzielkontrollen TAG 10	94
TAG 11 - Netzwerkkomponenten auswählen und konfigurieren.....	95
LE 1 - Switch auswählen.....	95

LE 2 - Router auswählen	96
(1) WLAN-Access-Point	96
(2) Professionelle Router	99
LE 3 - Neue Entwicklungen und Trends präsentieren	99
Lernzielkontrollen TAG 11	99
TAG 12 und TAG 13 - Grundlagen der Daten- und Netzwerksicherheit beschreiben	101
LE 1 - RAID-Systeme unterscheiden	103
LE 2 - Backupstrategien unterscheiden	106
(1) Off-Premises Backup	107
(2) Bandsicherung	107
(3) Backup auf Cloud-Speicher	107
LE 3 - Netzwerksicherheit herstellen	109
(1) Proxy	109
(2) Firewall/DMZ	110
(3) Software Defined Network	110
LE 4 - Verfügbarkeit und Ausfallzeiten von IT-Systemen berechnen	112
(1) Verfügbarkeit	112
(2) Ausfallwahrscheinlichkeit p	113
(3) Erhöhen der Systemverfügbarkeit	113
Lernzielkontrollen TAG 12 und TAG 13	114
TAG 14 - Geräte mit Strom versorgen	116
LE 1 - Stromversorgung allgemein	116
(1) Themen rund um die Stromversorgung	117
(2) Gefahren durch elektrischen Strom	118
(3) Energieversorgung von IT und Rechenzentren	120
(4) Unterbrechungsfreie Stromversorgung (USV)	121
(5) Wirkungsgrad und Laufzeit einer USV	125
(6) Leistungsfaktor Cosinus Phi	126
LE 2 - Green-IT in Netzwerken berücksichtigen	127
(1) Alternativgeräte auswählen (Refurbished IT)	127
(2) Den Stromverbrauch der IT optimieren	127
Lernzielkontrollen TAG 14	128
TAG 15 - Vertiefung des Wissens und Modulprüfung	131
LE 1 Einleitung	131
LE 2 - Modulprüfung	131
Lösungen:	132
TAG 1	132
TAG 2 und TAG 3	132
TAG 4 und TAG 5	133
TAG 6, TAG 7 und TAG 8	136
TAG 9	140
TAG 10	140
TAG 11	140

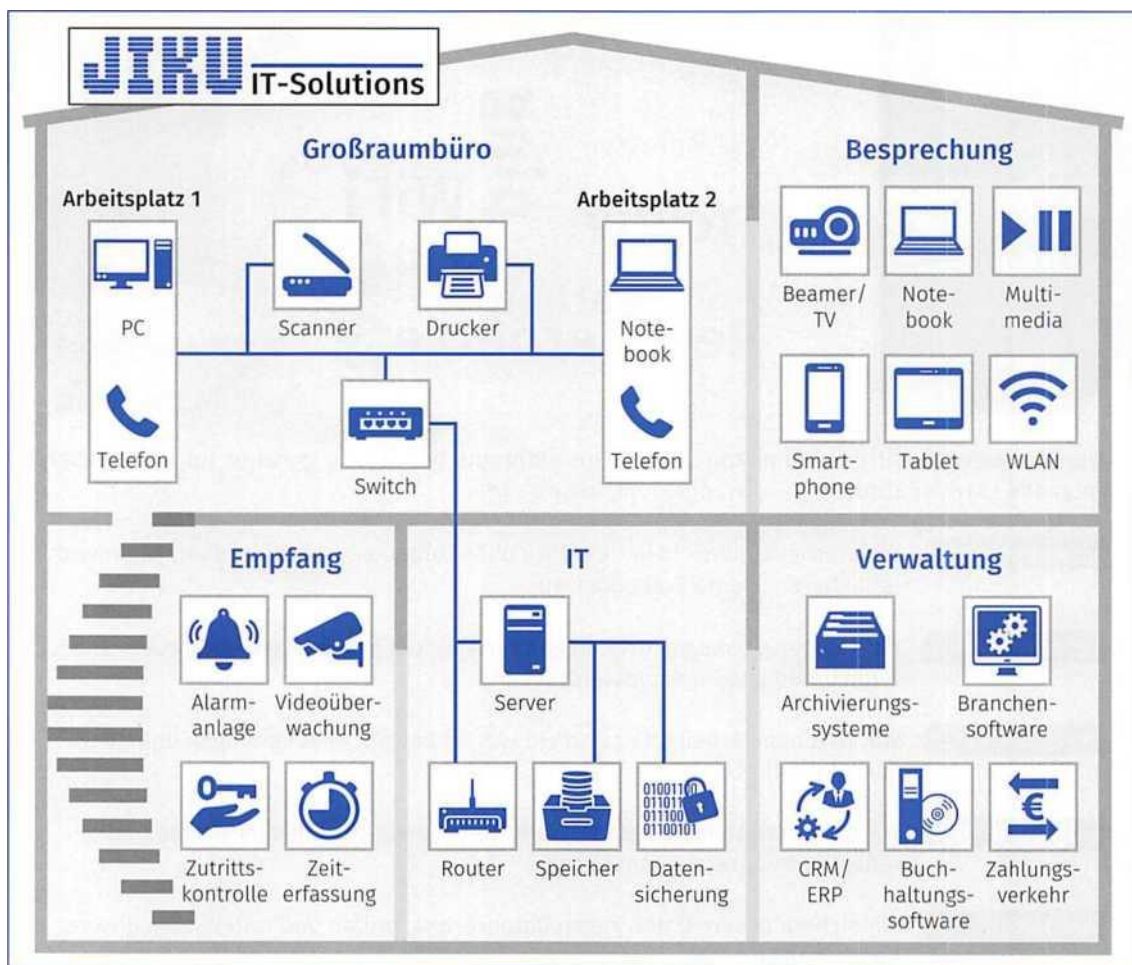
TAG 12 und TAG 13	140
TAG 14.....	142

TAG 1 - Eine Einführung in das Netzwerk des Ausbildungsbetriebs geben

Während Ihrer Ausbildung in den IT-Berufen lernen Sie, die Netzinfrastruktur zu analysieren und Computer, Drucker und andere Geräte (Devices) als Clients (Client = „Kunde“ eines Servers) an bestehende Netzwerke anzuschließen (zu integrieren). Dieses Lernfeld 3 informiert Sie zunächst über die Strukturen und Komponenten von Netzwerken. Im weiteren Verlauf werden die Grundlagen der Rechnernetzung erarbeitet, Topologien und Netzwerkmedien unterschieden und die verschiedenen Netzwerkgeräte und deren Einsatz verglichen. Die Grundlagen der Adressierung im Netz und die Konfiguration der Rechner und Geräte werden betrachtet, Einstellungen überprüft und Tests durchgeführt.

Sie erhalten eine Einführung in das Netzwerk des Ausbildungsbetriebs, das Modellunternehmen JIKU IT-Solutions. Sie sollen kurz über verschiedene Einsatzbereiche und Komponenten des Netzwerkes berichten.

Zunächst wird Ihnen das Netzwerk des IT-Systemhauses JIKU (siehe Kapitel 1.3.1) anhand des folgenden Schaubildes und eines Rundganges erläutert.



Schon beim Betreten des Gebäudes werden Sie am Empfang auf Anlagen aufmerksam gemacht, die Daten erfassen und weitergeben, z.B. die Zutrittskontrolle und Zeiterfassung sowie die Gefahrenmeldeanlage, Alarmanlage und Videoüberwachung. In der Verwaltung sind Programme im Einsatz, mit denen die Mitarbeiter Aufträge erfassen und bearbeiten, Buchhaltung betreiben, Belege scannen und die Daten in digitaler Form in Archiven speichern. Diese Daten werden über das Netzwerk zentral gespeichert.

Alle Geräte bzw. Devices sind mit IP-Adressen versehen, über die jedes Gerät angesprochen (adressiert) werden kann. Alle Rechner im Netzwerk (z. B. Arbeitsplatzrechner, Tablets, Laptops) können über das **LAN** (Local Area Network, lokales Netzwerk) oder das WLAN (Wireless LAN, drahtloses Netzwerk) auf die zentralen Daten zugreifen.

Im Besprechungsraum können Dateien über Beamer oder Großbildschirm gezeigt werden. Die Anbindung von jedem Device (auch Drucker oder Scanner) geschieht über die Netzwerkverkabelung. In den Stockwerks- und im Gebäudeverteiler befinden sich **Switches**, die die Daten zielgerichtet weiterleiten. Die Telefone sind sog. **IP-Telefone**, die ebenfalls über das Netzwerk angeschlossen sind. Die Telefonanlage (TK-Anlage) ist ein Server, der den Telefondienst versieht. Die in der IT-Abteilung aufgestellten zentralen **Server** sind leistungsstarke Rechner, die spezielle Dienste im LAN zur Verfügung stellen. Server und Netzwerkdienste können auch in entfernte Rechenzentren ausgelagert werden. Der Zugriff erfolgt dann über das Internet. Die Systemadministratoren der IT-Abteilung betreuen das Netzwerk und die Devices. Der Anschluss des LANS an das Internet regelt ein Router.

Fachbegriffe zum betrieblichen Netzwerk eines Dienstleistungsunternehmens	
Alarmanlage	Teil der Gefahrenmeldeanlage, löst bei Eintreten von bestimmten Ereignissen Alarm aus
Archivierungssystem	Auch Dokumentenmanagementsystem genannt; dient dazu, den aktuellen Stand der Daten innerhalb einer Anwendung zu sichern, unabhängig von der Datensicherung im Datacenter (Rechenzentrum, Rechnerraum, IT-Bereich)
Anwendungssoftware	Programme für bestimmte Anwendungen, z. B. CAD (Computer Aided Design)
CRM	Customer Relationship Management (Kundenbeziehungsmanagement)
ERP	Enterprise Resource Planning, bedarfsgerechte Planung und Steuerung von Unternehmensressourcen wie Personal oder Betriebsmitteln, Unternehmenssoftware für Auftragsbearbeitung, Lagerhaltung, Finanzbuchhaltung, u.a.
Datacenter	Rechenzentrum, abgeschlossener Raum, in dem Server, Netzwerkspeicher und andere zentrale IT-Einrichtungen untergebracht sind
Datenendgerät	Erstes Gerät im Netzwerk (erzeugt und sendet Daten ins Netz) und letztes Gerät im Netzwerk (empfängt Daten), z. B. Rechner, Server, Drucker
Datensicherung	Regelmäßiges Sichern der Daten auf Magnetbänder zum Schutz vor Datenverlust
Drucker	Drucker direkt an einzelnen Arbeitsplätzen und Drucker an zentralen Punkten als Arbeitsgruppendrucker
Gefahrenmeldeanlage	Können Gefahren erkennen, Benachrichtigungen verschicken, Alarmer auslösen, Schutzmaßnahmen einleiten, z.B. Melder (Tür- und Fensterkontakte), Bewegungsmelder, Brandmelder, Wassermelder
Host	Als Hosts oder Datenendgeräte (s.o.) werden die letzten Geräte im Netz bezeichnet, die Daten empfangen oder erzeugen.
IP-Adresse	Jedes Gerät im LAN hat eine eindeutige IP-Adresse. Das IP (Internet Protocol) als „Verfahrensvorschrift“ transportiert die Daten im Netzwerk an den Rechner mit der angegebenen Ziel-IP-Adresse.
Kopierer	Kopierer verfügen fast immer über Netzwerkanschluss und werden als leistungsfähige Drucker und auch als Scanner verwendet.

Fachbegriffe zum betrieblichen Netzwerk eines Dienstleistungsunternehmens	
LAN	Local Area Network, lokal begrenztes Netzwerk, in der Regel auf ein Betriebsgelände begrenzt, Ausdehnung bis mehrere Kilometer.
Scanner	Bringen Dokumente von Papier in Dateiformat
Network Devices	Netzwerkgeräte, Netzwerkkomponenten; physische Geräte, die die Datenpakete im Netzwerk weiterleiten. Endgeräte sind an Switches angeschlossen, Mobilgeräte verbinden sich mit Access Points, Router verbinden mehrere Netzwerke (z.B. LAN und Internet).
PC-Arbeitsplätze	Mit unterschiedlichen PCs und Laptops zum Erledigen der täglichen Arbeit
Router	Network Device zum Verbinden mehrerer Netzwerke
Rechenzentrum	Abgeschlossener Raum, in dem Server, Netzwerkspeicher und andere zentrale IT-Einrichtungen untergebracht sind.
Paket	Daten werden immer in Datenpaketen übertragen, nicht als kontinuierlicher Datenstrom.
Server	Leistungsfähige Rechner im Datacenter (Rechenzentrum, Rechnerraum), die Dienste (Services) im Netzwerk anbieten, sie befinden sich im Rechenzentrum
Speicher	Zentraler Datenspeicher im Datacenter
Switch	Network Device zum Anschluss von Endgeräten
Telefone	Gerätetelefonie intern und nach außen, auch weltweit
TK-Anlage	Telefonanlage, verbindet Telefone intern und über Internet oder über öffentliche Telefonnetze auch extern
Videoüberwachung	Eingangsbereich und sonstige wichtige Bereiche werden gefilmt und mit Zeitstempel gespeichert.
WLAN/Wi-Fi	Wireless LAN, drahtloses Netzwerk für Mobilgeräte
Zahlungsverkehr	Arbeitsplatz zum Bearbeiten des elektronischen, sicheren Zahlungsverkehrs mit Kunden und Lieferanten
Zeiterfassung	Anwesenheitszeiten, Arbeits- und Pausenzeiten werden erfasst
Zutrittskontrolle	Terminal zur Ausweiskontrolle, Bilderkennung, Fingerabdruckscanner, Iris Scanner (Augenerkennung); gewährt oder verhindert Zutritt zu Gebäuden oder sicherheitsrelevanten Gebäudeteilen

Ein Datennetzwerk im Betrieb ist vielfältig und hat viele wichtige Aufgaben zu bewältigen.

Aufgaben eines lokalen Datennetzwerkes	
Aufgaben	Erläuterung
Kommunikationsverbund	Schnelle Kommunikation mit allen Arbeitsplätzen (Text, Bild, Video, Ton, Signale, sonstige Daten)
Datenverbund	Zugriff auf verteilte und zentrale Datenbestände von jedem Arbeitsplatz

Aufgaben eines lokalen Datennetzwerkes	
Aufgaben	Erläuterung
Funktionsverbund	Nutzung von Funktionen und Softwareanwendungen anderer Arbeitsplätze, Steuerung von Abläufen
Ressourcenverbund	Nutzung von Betriebsmitteln (z. B. Drucker) anderer Arbeitsplätze oder zur gemeinsamen Verwendung
Last- und Leistungsverbund	Verteilung von Lasten (z.B. aufwendige Datenauswertungen) auf wenig genutzte Arbeitsplätze oder Systeme; erreicht wird daher auch eine Verbesserung der Antwort- und Transaktionszeiten. Aufgrund von großen Schwankungen in der Netzauslastung ist die Skalierbarkeit (Leistungsanpassung) des Netzwerkes wichtig.
Sicherheits- und Verfügbarkeitsverbund	Reserven bei Ausfall einzelner Komponenten und zur sicheren Datenspeicherung

Von jedem Arbeitsplatz kann mit den anderen vernetzten Arbeitsplätzen und Servern kommuniziert werden. Das Rechnernetz stellt die Verbindung von räumlich getrennten Datenbeständen her - zum Zwecke des Austausches, der Speicherung oder der Zusammenarbeit. Durch die zentrale Speicherung der Daten an einem einzigen Ort wird die **Konsistenz der Daten** sichergestellt. Es kommt nicht durch Mehrfachspeicherung auf mehreren Rechnern zu inkonsistenten (uneinheitlichen) Datenbeständen.

Die zur Verfügung stehenden Ressourcen können in einem Netzwerk besser genutzt werden. Beispielsweise ist ein leistungsfähiger Laserdrucker im Netzwerk kosteneffizienter als mehrere einfache Drucker an jedem Einzelrechner.

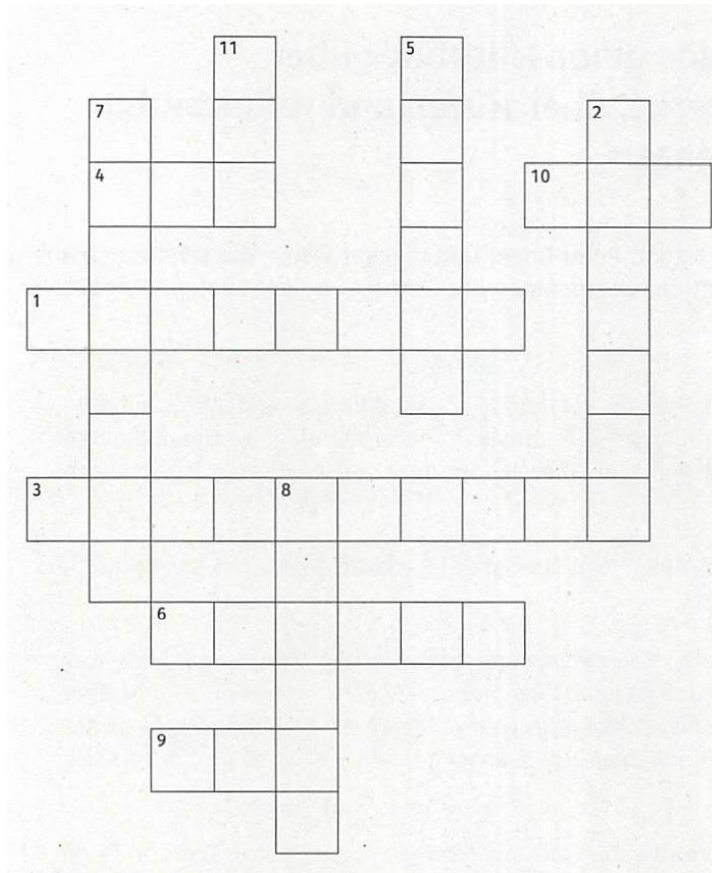
Dienste im Netzwerk, die von Servern erbracht werden, können auf mehrere Rechner **verteilt** werden. Ein sogenannter Load Balancer (Lastverteiler, Lastausgleicher) sorgt für eine gleichmäßige Auslastung der Server, sodass der einzelne Server nicht übermäßig beansprucht wird.

Durch redundante Systeme kann die Sicherheit der Daten und die Verfügbarkeit im Netz sichergestellt werden.

Lernzielkontrollen TAG 1

1. Erläutern Sie mit eigenen Worten das Schaubild auf S. 7 des Moduls.
2. Erläutern Sie kurz, was unter inkonsistenten Daten zu verstehen ist.
3. Wahr oder falsch?
 - a) Ein PC speichert die wichtigen Daten lokal auf seiner Festplatte.
 - b) Ein Datacenter ist ein Datenspeicher auf einem Arbeitsplatzrechner.
 - c) Ein LAN kann mehrere Kilometer Ausdehnung haben.
 - d) Ein LAN ist auf ein Betriebsgelände beschränkt.
 - e) Alle Netzwerkdrucker und PC (außer WLAN-Geräte) sind über Leitungen mit einem Switch verbunden.
4. Prüfen Sie Ihr Wissen in einem Kreuzworträtsel.
 1. Weltweites Datennetz
 2. Dienstleister, der Übertragungskapazität auf Fernleitungen anbietet
 3. Englische Bezeichnung für ein Rechenzentrum
 4. Lokales Netzwerk (Abkürzung)
 5. Gerät, welches Netzwerke miteinander verbindet
 6. Gerät, welches Endgeräte miteinander verbindet

7. Englischer Begriff für VLAN-Kennung
8. Endgerät im Netzwerk
9. Sichere Verbindung eines Home-PCs mit dem Firmennetz (Abkürzung)
10. Englische Abkürzung für Speichernetzwerk
11. Englische Abkürzung für Weitverkehrsnetz



5. Prüfen Sie Ihr Wissen zur Netzwerktechnik. Welche Aussage ist richtig oder falsch.
 1. Drucker sind meistens an das Netzwerk angeschlossen.
 2. Das Datacenter ist der Server, auf dem die Daten gespeichert werden, die über das Netzwerk abrufbar sind.
 3. Ein Switch ist das zentrale Element, an welches die Endgeräte angeschlossen werden.
 4. Die Zugangskontrolle wird lokal eingerichtet und ist aus Sicherheitsgründen nicht mit dem Netzwerk verbunden.
 5. Jedes Endgerät im Netzwerk hat eine eigene IP-Adresse.
6. Tragen Sie alle vernetzten Komponenten bei Ihrem Rundgang im Betrieb oder der Schule, die Sie mit der IT in Verbindung bringen, in die Tabelle ein.

Gebäude/ Raum-Nr.	Gerät/ Rechner	Funktion	Bemerkungen
2.Etage Aufgang A	Zeiterfassungsterminal	Erfassen der Arbeitszeit, etc.	
2.Etage Aufgang B	Netzwerkdosen	Anschluss von PC, Druckern	Zwei Steckplätze pro Dose
...	...	...	...
...	...	...	...

TAG 2 und TAG 3 - Hauptbestandteile von Computernetzen unterscheiden

Sie sollen die verschiedenen Netztypen und die Bestandteile der Computernetze kennen und unterscheiden können.

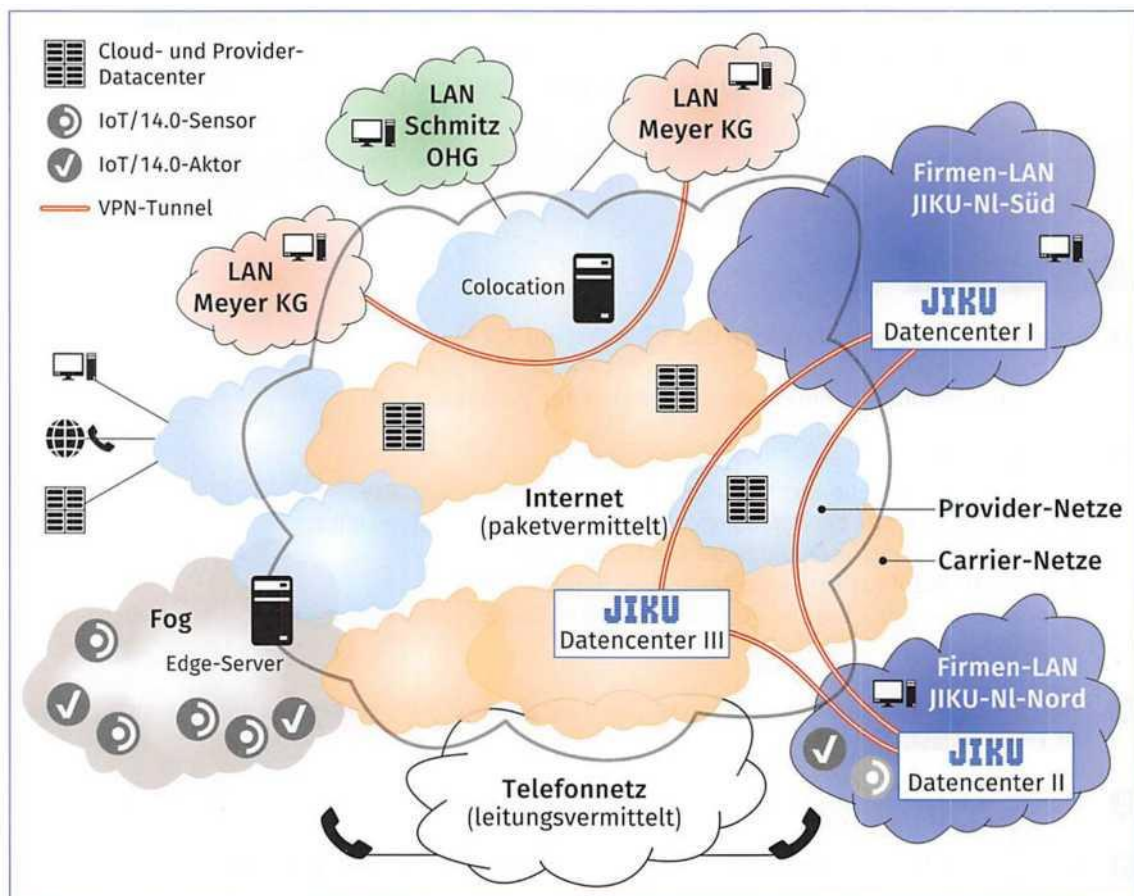
Computernetz

Ein Computernetz oder Rechnernetz(-werk) ist die Menge an Verbindungen, von selbständigen Rechnern unterschiedlichster Bauform, Funktion und Leistungsfähigkeit, welches den Datenaustausch der Geräte untereinander ermöglicht. Dies umfasst neben normalen PCs und Servern auch Messwertaufnehmer/Sensoren, Stellglieder/Aktoren, Ausgabegeräte wie z. B. Drucker oder Eingabegeräte wie Scanner.

LE 1 - Computernetzwerke und deren Hauptbestandteile im Überblick unterscheiden

Sie sollen die wichtigsten Bezeichnungen und Abkürzungen kennen und unterscheiden können.

Im Beispiel des Modellunternehmens JIKU wurde nur die Vernetzung innerhalb des Unternehmens aufgezeigt. Heutzutage ist jedoch die gesamte Welt miteinander vernetzt. Weltweit sind über 5 Milliarden Menschen über das Internet vernetzt, und es gibt etwa 20 Milliarden vernetzte Geräte weltweit. Das folgende Schaubild soll einen Eindruck vermitteln, mit welcher Vielfalt an Netzen Datenaustausch und Kommunikation erfolgen.



Das Internet ist das Netz der Netze. Eine Fülle von Netzwerken unterschiedlicher Größen sind weltweit miteinander verbunden. Das Schaubild zeigt rechts zwei LANs der JIKU-Niederlassungen Nord und Süd, jeweils mit eigenem Datacenter. Im Internet befindet sich das JIKU Datacenter III. Diese drei Datacenter sind per VPN-Tunnel (VPN = Virtual Private Network) über das Internet miteinander verbunden. Das betriebliche Intranet erlaubt den Zugriff

über Webbrowser auf die bereitgestellten Daten innerhalb des gesamten Unternehmens (über alle betrieblichen LANs).

Provider ermöglichen Unternehmen, Behörden, Privatpersonen usw. den Zugang zu diesem weltweiten Daten-Verbundnetz. Anstelle der älteren Telefontechniken und separaten Telefonnetze wird heute immer mehr Telefonie über das Internet (IP-Telefonie oder Voice over IP) genutzt. Das alte Telefonnetz deckt sich teilweise mit dem modernen Datennetz, wird aber immer mehr durch das Internet verdrängt. Die bestehenden Fernverbindungsstrecken werden zu Datenleitungen. Carrier (oft Telekommunikationsunternehmen) betreiben großflächige Datennetze, teilweise weltweit, um Datenpakete zu transportieren. Sie verkaufen Datenübertragungsleistungen für Geschäftskunden.

Auf Cloud-Dienste im Internet kann man zu jeder Zeit zugreifen. Man kann Dienste nutzen, ohne eine eigene physische IT-Infrastruktur zu besitzen. Industrie 4.0 und das IoT (Internet of Things, Internet der Dinge) erfordern neue Strukturen wie Fog Computing oder Edge-Server (am Übergang vom Sensor-/Aktornetz zum Internet). Dabei werden zeitkritische Daten, nahe am Entstehungsort der Daten, am Rand des Internets verarbeitet. Lange Latenzzeiten (Verzögerungszeiten) durch das Übertragen in ein Cloud-Rechenzentrum entfallen.

VPN-Tunnel gewährleisten sichere Verbindungen auch über das unsichere Internet. Die in Netzwerken zu übertragenden Daten werden in einzelne Datenpakete gepackt und mit einem Header versehen, der die Ziel-IP-Adresse und die Absender-IP-Adresse enthält. Anhand der Zieladresse werden die einzelnen Pakete durch die Netze hindurch transportiert. Der Dateninhalt eines Paketes ist begrenzt. Sind mehr Daten zu übertragen, als in ein Paket passen, werden die Originaldaten in viele Pakete zerlegt, nacheinander versendet und beim Empfänger wieder zusammengesetzt. Daten werden im VPN-Tunnel verschlüsselt übertragen und sind daher sicher vor Abhören und Manipulation. Jedes Unternehmen, jede Behörde und fast jeder Privathaushalt verfügt heute über ein LAN, ein Local Area Network. Dies kann mehrere tausend Rechner umfassen oder auch nur einen Router und einen einzelnen PC. Die verwendete Technologie ist LAN-intern dieselbe. Ethernet ist der weltweite Standard für LANs. Das Internetprotokoll benutzt Ethernet als Basis.

Computernetze unterscheiden	
Internet	Weltweites Datennetz, paketvermittelt (Daten werden paketweise übertragen), Internetdienst mit Webbrowsern als Benutzerschnittstelle
Intranet	Unternehmensweites abgeschottetes Netzwerk, das aus mehreren über sichere Verbindungen verbundene LANs bestehen kann; Zugriff erfolgt wie im Internet über Webbrowser als Benutzerschnittstelle
Telefonnetz	Analoger Telefondienst, auch PSTN (Public Switched Telefon Network) und POTS (Plain Old Telephone Service); weltweites Netz, leitungsvermittelt, d. h. dauerhafte Verbindung von Telefon zu Telefon während des Telefonats
Providernetz	Zugangsnetz der Internetprovider, um Unternehmen-, Behörden- und Privatnetze mit dem Internet zu verbinden
Firmen-LAN	LAN von Unternehmen und Privatpersonen, mit eigenem oder ohne eigenes Rechenzentrum
Carrier-Netz	(Glasfaser-)Netz eines Carriers. Ein Carrier ist ein Netzbetreiber, der meist großflächige Datennetze betreibt. Erstellt für seine Kunden kostenpflichtig Datenübertragungsdienste oder Leitungen zur Verfügung. Kunden von Carriern sind Provider, staatliche Institutionen, Großkonzerne. Oft sind Telefongesellschaften Carrier, z. B. Deutsche Telekom, Versatel, Colt,...

LE 2 - Netzbereiche im Überblick unterscheiden

Sie sollen die wichtigsten Bezeichnungen und Abkürzungen kennen und unterscheiden können.

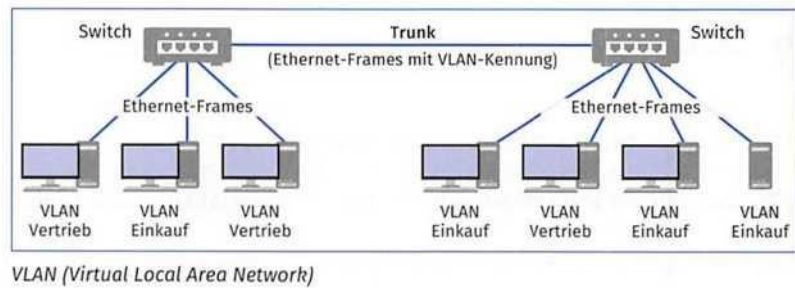
Netzwerke lassen sich in zwei Bereichen einteilen: die privaten Netze und die öffentlichen Netze. Private Netze werden von Behörden, Betrieben, Schulen, Privathaushalten usw. genutzt und verwaltet. Sie liegen in der Verantwortung des jeweiligen Betreibers und sind lokal begrenzt. Öffentlichen Netze werden von Internet Providern und Dienstleistungsunternehmen betrieben, die Großkunden und Providern Zugang zu überregionalen Datendiensten ermöglichen.

Netzbereiche - private Netze			
	Abkürzung	Bezeichnung	Bemerkungen/Beispiel
Private Netze	Sie nutzen IP-Adressen aus den privaten-IP-Adressbereichen; Pakete mit privaten IP-Adressen werden nicht im Internet weitergeleitet (siehe Kapitel 3.3.8). Sie werden von Unternehmen, Behörden, Schulen, Hochschulen, Privathaushalten usw. intern benutzt; Betreiber sind für ihre privaten Netzwerke selbst verantwortlich.		
	LAN	Local Area Network, lokales Netzwerk	Auf ein Betriebsgelände begrenztes Netzwerk, Ethernet mit TCP/IP, aber auch kleinste „Heim- Netze“ für Privatleute
	WLAN	Wireless LAN	Drahtloses, in ein LAN eingebundenes Funknetz, für LAN-Zugang mobiler Rechner
	VLAN	Virtuelles LAN	Aufteilen von LANs in abgetrennte virtuelle LANs auf einer gemeinsamen LAN-Verkabelung
	VPN	Virtual Private Network	Sichere (LAN-)Verbindungen durch ein unsicheres Netzwerk (Internet oder LAN)
	SAN	Storage Area Network, Speichernetz	Verbindungsnetz für Massenspeicher (in Rechenzentren)
	PAN	Personal Area Network, persönliches Netz, Piconet	Netz mit geringer Reichweite, das von Kleingeräten wie PDAs oder Mobiltelefonen ad hoc auf- und abgebaut werden kann, z. B. Bluetooth, NFC
Öffentliche Netze	Sie sind hierarchisch aufgebaut, nutzen öffentliche IP-Adressen zum Adressieren von Netzen und Rechnern im Netz. Sie werden betrieben von Providern (Dienstanbieter, Versorger) und Carriern (Träger, Betreiber). Sie verbinden einzelne Stationen mit einem Netzwerk, z. B. Kabelnetzbetreiber. Sie verbinden LANs auch über große Distanzen miteinander.		
	WAN	Wide Area Network, Weitverkehrsnetz	Öffentliche Netze über große Distanzen, Provider- Netze, DSL, Kabelmodem
	LPWAN	Low Power WAN	Funknetzwerk für batteriebetriebene Endgeräte zum Anschluss ans Netzwerk
	MAN	Metropolitan Area Network, Stadtnetz	Von lokalen Providern betrieben (in Deutschland eher unüblich)
	GAN	Global Area Network, globales Netz	Internet, Telefonnetz usw.

Virtuelle Netze sind besonders geschützte Netzbereiche.

(1) VLAN (virtuelles LAN)

In größeren Netzen möchte man häufig eine klare Trennung von Arbeitsgruppen oder Abteilungen. Um aber nicht separate Verkabelungen für jede Gruppe zu erstellen, wird auf der gemeinsamen LAN-Verkabelung eine Auftrennung in verschiedene VLANs gemacht.



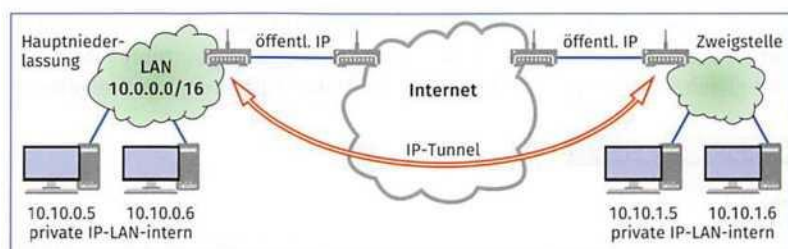
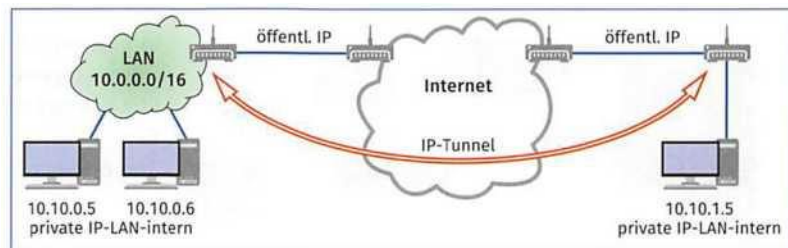
Daten werden zum Transport über ein Netzwerk in kleine Pakete verpackt. Diese Pakete werden entsprechend der VLAN-Zugehörigkeit gekennzeichnet.

Der Standard ist das Ethernet-Protokoll mit einer Paketgröße von maximal 1 500 Byte Nutzdaten. Diesen Nutzdaten wird ein Header mit der Ziel- und der Quell-(Absender-)Adresse der Netzwerkkarten vorangestellt. Diese Ethernet-Datagramme werden bei VLAN Einsatz um 4 Byte vergrößert. In den Ethernet-Header wird eine zusätzliche Information eingeschoben, der VLAN-TAG oder das VLAN-Kennzeichen. Er beinhaltet eine 12-Bit-Zahl zum Unterscheiden der VLANs. Damit sind also 2^{12} VLANs unterscheidbar (siehe auch Kapitel 3.3.3, Seite 302).

Die Verbindungsleitungen zwischen den Switches müssen diese VLAN-Kennung mit übertragen. Eine solche Leitung nennt man Trunk. Die Leitungen zwischen PC und Switch transportieren die ursprünglichen Ethernet-Datagramme ohne VLAN-Tag (untagged ethernet frames). Die Switches erweitern die Frames um den VLAN-Tag (tagged ethernet frames).

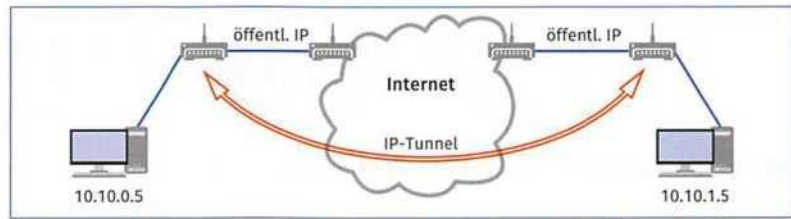
(2) VPN (Virtual Private Network)

Ein VPN ist ein aus einem LAN ausgelagerter Netzwerkteil. Dies kann ein einzelner Rechner oder ein ganzer Netzbereich sein. Die IP-Datenpakete, die intern im LAN verschickt werden, werden bei dieser Technik zusätzlich in IP-Pakete für das Internet verpackt. Vorher werden sie verschlüsselt. Die verschlüsselten Pakete erreichen über das Internet als Transportmedium ihr Ziel. Dort werden die Internet-Pakete wieder entpackt und entschlüsselt. Heraus kommen die LAN-internen IP-Pakete, die jetzt im entfernten Rechner oder im entfernten Netz bearbeitet werden können. Diese Technik der Verschlüsselung von IP-Paketen und nochmaliges Verpacken in IP-Pakete des (unsicheren) Internets nennt man IP-Tunneling. Die Internetverbindung nennt man VPN-Tunnel.



Wird nur ein einzelner Rechner ausgelagert, spricht man von End-to-Site-VPN. Dies sind die typischen Heimarbeitsplätze (Homeoffice).

Wird ein ganzes Niederlassungsnetz ausgelagert, so spricht man von einem Site-to-Site-VPN. Das Netz in der

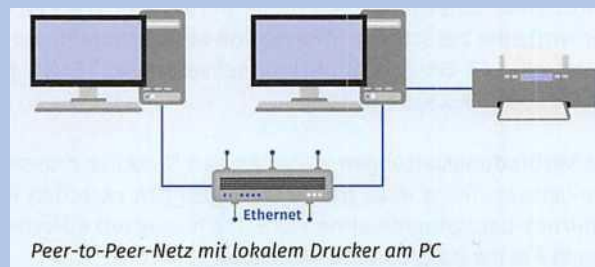


End-to-End-VPN

Zweigniederlassung ist ein Teil des Netzes der Hauptniederlassung. Es können auf diese Weise viele Niederlassungen miteinander verbunden werden. Eine dritte Variante ist das sichere Verbinden von zwei Rechnern, z. B. zwei Gaming-PCs. Man nennt dies dann End-to-End-VPN.

Peer-to-Peer-Netz

Ein Rechner kann gleichzeitig Client (= Kunde) und Server (= Diener) sein. Er kann Dienste von anderen nutzen und ist daher Client. Er kann aber auch selbst Dienste anbieten, dann ist er Server. Ein Netzwerk, in dem Rechner gleichzeitig Client und Server sein können, nennt man Peer-to-Peer-Netz.

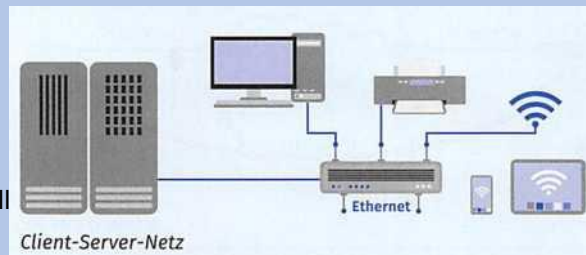


Peer-to-Peer-Netz mit lokalem Drucker am PC

Client-Server-Netz

In größeren Netzen werden separate, dedizierte Rechner als Server eingesetzt. Jeder Client nutzt nur die Dienste dieser zentralen Server. Ein solches Netz nennt man Client-Server-Netz.

In der IT-Praxis findet man in professionell Netzen immer Client-Server-Netze mit zentralen Servern. Daneben können einzelne Arbeitsplatzrechner Freigaben einzelner Ressourcen für andere Clients einrichten und gleichzeitig zusätzliche Peer-to-Peer-Netze aufbauen, z. B. Freigabe von lokalen Daten oder Druckern.



Client-Server-Netz

LE 3 - Rechenzentren und Serversysteme unterscheiden

Sie sollen Rechenzentren und Serversysteme unterscheiden können.

(1) Lokales Rechenzentrum (On-Premises)

Oftmals werden die Server eines Netzwerkes in geeigneten, abschließbaren und klimatisierten Räumen in einem Gebäude auf dem Betriebsgelände untergebracht. Handelt es sich um wenige Server, so spricht man auch vom Serverraum. Größere Unternehmen mit entsprechend mehr Servern und höherer Rechenleistung betreiben ein Rechenzentrum (RZ), auch Datacenter (DC) genannt (vgl. S. 62).

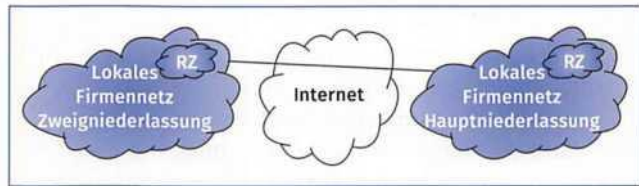


Wichtige Voraussetzungen für den Betrieb sind eine sichere Stromversorgung, die Klimatisierung und die Anbindung an LAN und Internet. Da die elektrische Leistung, die ein Rechenzentrum verbraucht, als Wärme freigesetzt wird und Erwärmung den Rechnerbetrieb stören kann, muss diese Wärme mittels Klimatisierung auch wieder abgeführt werden.

Werden mehrere Niederlassungen eines Unternehmens miteinander verbunden, kann ein einzelnes Rechenzentrum alle

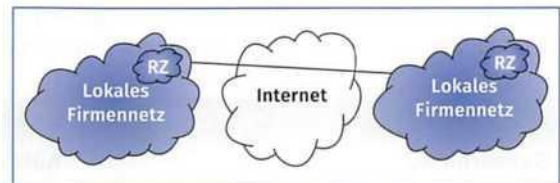
Niederlassungsnetze über VPN-Verbindungen versorgen. Auch angemietete Leitungen (Kupfer oder

Lichtwellenleiter) können zum Einsatz kommen. Aus Sicherheits- und Performancegründen ist dies jedoch nicht zu empfehlen. Besser ist es, wenn jede große Niederlassung über ein eigenes Rechenzentrum verfügt. Die Daten können zwischen den Rechenzentren gespiegelt (also doppelt gespeichert) werden. So schafft man eine große Sicherheit gegen Datenverlust. Bei Ausfall eines Rechenzentrums kann das verbleibende die Dienste übernehmen.

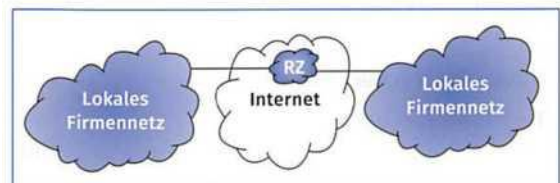
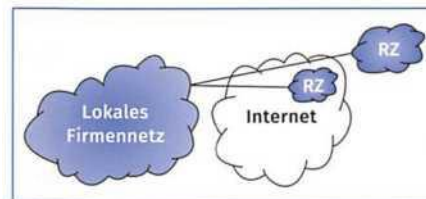


(2) Externes Rechenzentrum (Off-Premises)

Ein Rechenzentrum muss nicht zwingend im eigenen LAN stehen. Über schnelle Datenleitungen (Lichtwellenleiter) können auch weit entfernte Rechenzentren ohne Performanceverluste genutzt werden. Dabei kann das externe Rechenzentrum ein eigenständiges Netz außerhalb des Internets sein oder sich ebenfalls in einem großen Rechenzentrum im Internet befinden.



Wird das Rechenzentrum nicht selbst betrieben, kümmern sich RZ-Profis darum. Sie bieten je nach Bedarf eine IT-Rechenzentrums- und Serverinfrastruktur an. Dazu stehen viele Dienstleistungen je nach Wunsch des Unternehmens zur Verfügung, z.B. die Bereitstellung aktueller Anwenderprogramme oder laufende Datensicherungen. Die Betreiber des Rechenzentrums kümmern sich außerdem um die Stromversorgung, Datensicherung und Klimatisierung. Diese bedarfsgerecht angemieteten Cloud-Systeme stehen für alle Niederlassungen bereit und benötigen weniger administrativen Aufwand als lokale Rechenzentren.



(3) Colocation

Internetprovider und Carrier verfügen über eigene Rechenzentren, die sehr gut vernetzt sind. Meist haben sie direkten Anschluss an die schnellen Glasfaserfernleitungen des Internets, die sogenannten Backbone-Leitungen.

In diesen Rechenzentren werden oftmals Stellplätze für Racks oder auch nur Einschubplätze in den Racks vermietet. Kunden können ihre eigenen Server hier unterbringen oder hinzufügen. Damit werden Rechenleistung und Speicherplatz vom eigenen lokalen Rechenzentrum nach außen verlagert. Man verfügt aber weiterhin über die Daten und Hardware. Hochsensible Daten aus der Entwicklung oder Buchhaltung bleiben so besser geschützt, da sie nicht an andere (Cloudbetreiber) weitergegeben werden. Der Colocation-Anbieter kümmert sich um die allgemeinen Sicherheitsanforderungen im Rechenzentrum, d.h. um die Anforderungen vom Brandschutz bis zur Zutrittsberechtigung, um sichere, redundante Stromversorgung und um sichere, schnelle (hochbitratige) Anbindung ans Internet zu erfüllen.

Vorteile einer Colocation-Lösung in einem fremden Datacenter

- Eigene Hardware, Daten bleiben auf eigenen Rechnern
- Sehr gute Anbindung ans Internet
- Redundante Stromversorgung vom Vermieter
- Kühlung/Klimatisierung vom Vermieter
- Zutrittskontrolle, Brandschutz etc. vom Vermieter

Die Nachfrage nach Rechenzentrumsflächen, die für Colocation benutzt wird, steigt laufend. Sie betrug 2020 bereits 35 % der gesamten Rechenzentrumsflächen in Deutschland. Colocation zu nutzen kann viel kostengünstiger sein, als sich ein eigenes Datacenter aufzubauen oder das bestehende zu erweitern.

(4) Servertypen und deren Dienste beschreiben

Rechner, die ihre Dienste (Services) im Netzwerk anbieten, nennt man Server. Bietet ein Server Dateidienste an, also das Speichern und die Zurverfügungstellung von Dateien, dann nennt man dies einen File-Server oder Datenserver. Ein Rechner, der Druckdienste anbietet, ist ein Print-Server.

Servertypen	
Servername	Aufgabe
File-Server	Stellt Dateidienste zur Verfügung (z. B. FTP, SMB)
Print-Server	Stellt Druckdienste zur Verfügung
Mail-Server	Stellt E-Mail-Dienste zur Verfügung
DNS-Server	Stellt Namensauflösungsdienste zur Verfügung
Shop-Server	Stellt Onlineshop-Dienste zur Verfügung
Web-Server	Stellt Web-Dienste (browserfähige Inhalte) zur Verfügung
Update-Server	Stellt Software-Updates zur Verfügung
Anwendungsserver	Stellt Anwendungen, z. B. Warenwirtschaftssysteme, zur Verfügung
Network Attached Storage (NAS)	Netzwerkspeicher; stellt Speicherplatz zur Verfügung
Terminal-Server	Stellt virtuelle Arbeitsplatzrechner zum Anschließen von Thin Clients zur Verfügung

LE 4 - Clients im Überblick unterscheiden

Sie sollen alle Arten von Netzwerk-Clients einordnen und verschaffen sich einen Überblick.

Ein Client im Allgemeinen, ist ein Kunde oder ein Klient. In der IT ist ein Client ein Rechner, der Daten und Dienste von einem anderen Rechner (Server) anfordert und erhält. Der Client nutzt die Dienste (Services) anderer Rechner. Die Bauformen von Clients sind vielfältig. So vielfältig wie deren Aufgaben. Dabei sind Clients sowohl typische Arbeitsplatzrechner als auch „versteckte“ Rechner im Netzwerk, denen man Ihre Aufgabe nicht ohne weiteres ansieht (siehe auch Lernfeld 2, Kapitel 2.2.2 und 2.7).

Netzwerk-Clients



Tower



Tablet



Laptop



Fat Client



Embedded-PC



Rackmount-PC



Smartphone



Sensor/Aktor



Thin Client

Clients in LAN und Internet	
Desktop-PC	Arbeitsplatzrechner auf dem Tisch
Tower-PC	Arbeitsplatzrechner hochkant, auf oder unter dem Tisch meist besser ausgestattet und leistungsfähiger als Desktop-PCs
Smartphone	Allzweckrechner mit drahtloser Netzverbindung (WLAN, Bluetooth oder Mobilfunk), mit Telefoniefunktion
Embedded System	Kleiner, teilweise sehr leistungsfähiger Rechner mit Sensoren, Aktoren, Netzanbindung oder per Kabel oder WLAN
Tablet-PC	In eine Anzeige integrierter, leistungsfähiger Kleinrechner mit Touchscreen- Bedienung, Netzanbindung per WLAN oder Mobilfunk
Drucker	Zum Ausdrucken der Daten auf Papier
IP-Telefon	Zum Austauschen von Sprachdaten, Digitaltelefonie
Fat Client	Leistungsstarker Rechner im Netzwerk, alle Applikationen laufen lokal auf diesem PC
Thin Client	Kleiner, leistungsschwacher Rechner, meist ohne Massenspeicher
BYOD	Abkürzung für „Bring Your Own Device“; Mitarbeiter bringen ihre eigenen Geräte mit zur Arbeit und werden in das LAN integriert
Cyber Physical System	Elektrisch-mechanisches System in der Produktion mit Netzwerkanbindung, Rackmount-PCs als Steuerungsrechner

Jedes Gerät mit Netzwerkschnittstelle, welches in ein Netzwerk eingebunden wird, ist ein Netzwerk- Client.

„Normale“ PCs, also Arbeitsplatzrechner, Workstations, Laptops usw., sind voll ausgestattete Rechner und verfügen über alles, damit sie eigenständig und autonom arbeiten können. Sie booten ihr Betriebssystem von einem Massenspeicher und führen Anwendungsprogramme aus. Diese Rechner werden als Fat Clients bezeichnet. Die Anbindung ans Netzwerk geschieht meist über eine LAN-Leitung.

Thin Clients hingegen sind abgespeckte Rechner, die teilweise gar nicht über Massenspeicher verfügen und ihr Betriebssystem über das Netzwerk beziehen (Diskless Workstations). Man nennt sie auch Slim Clients oder Lean Clients. Sie verfügen über wenig Rechenleistung und sind i.d.R. nicht in der Lage, Anwendungsprogramme lokal auszuführen. Sie dienen als „Datensichtgeräte“, d.h. als Terminals. Tastatur- und Mauseingaben werden über das Netzwerk an einen Terminal-Server übertragen. Auf diesem Terminal-Server laufen mehrere virtuelle Maschinen als Desktop-Rechner. Der Thin Client verbindet sich mit einer virtuellen Maschine. Alle Anwendungsprogramme, die an diesem Arbeitsplatz benötigt werden, werden auf der virtuellen Maschine ausgeführt. Das Ergebnis, also die Bildschirmanzeige wird über das Netzwerk zum Thin Client übertragen und dort angezeigt (siehe auch Lernfeld 2, Kap. 2.7.3). Die Anbindung ans Netzwerk geschieht meist über eine LAN-Leitung.



Der Datenverkehr zwischen Server und Thin Client ist sehr gering. Durch die Minimalausstattung des Thin Clients ist auch der Energiebedarf sehr gering. Oft finden diese Rechner im Monitor oder in der Tastatur Platz. Das Fehlen von Schnittstellen für externe Festplatten und USB-Speicher macht diese Systeme auch sicher gegen das Einschleusen von Schadsoftware. Der Datenverkehr von Servern zum Client findet innerhalb des Rechenzentrums statt. Hierbei handelt es sich um einen horizontalen Datenfluss, da der Client eine virtuelle Maschine auf dem Terminalserver ist. Zwischen Thin Client und Terminalserver wird nur der Bildschirminhalt (Server → Client) sowie Tastatureingaben und Mausbewegungen (Client → Server) übertragen. Das heißt, dass das Datenvolumen auf der Netzwerkleitung des Thin Clients sehr gering ist. Es reicht zur Not auch eine ISDN-Telefonverbindung. Dies macht wiederum Homeoffice-Plätze möglich, auch wenn kein schnelles Internet zur Verfügung steht. Ältere und leistungsschwache PCs und Laptops lassen sich sehr gut mit einem abgespeckten Betriebssystem und einem Client-Programm als Thin Clients weiter benutzen.

BYOD ist eine große Herausforderung für alle Administratoren. Die Mitarbeiter bringen ihre eigenen Geräte, meist Laptops oder Tablet- PCs, von zu Hause mit zur Arbeit. Sie verbinden sich mit dem Unternehmensnetz und müssen auf alle Systemressourcen Zugriff haben wie normale Arbeitsplätze. Aus Sicht der Administratoren ist jedes dieser Geräte eine Sicherheitslücke. Oftmals werden den Mitarbeitern vom Arbeitgeber aber auch mobile Rechner zur Verfügung gestellt, die die Mitarbeiter auch zu Hause benutzen dürfen. Diese Rechner werden so eingerichtet, dass ein sicheres Arbeiten möglich ist. Die Anbindung ans Netzwerk geschieht meist über WLAN, da es sich um mobile Geräte handelt. Werden im Betrieb Dockingstation (mit großen Bildschirm, Maus und Tastatur) verwendet, in die man die Mobilgeräte einsteckt, erfolgt die Netzanbindung über eine LAN-Leitung.



Cyber-physische Systeme (CPS) sind Maschinen und Roboter, die mechanische Arbeiten verrichten und von Rechnern gesteuert werden. Dies können Industrie-PCs in Rack-Bauweise, Embedded Systems oder herkömmliche speicherprogrammierbare Steuerungen (SPS) sein. Diese Module werden über Netzwerke verbunden und können sowohl untereinander als auch mit darüber liegenden Schichten bis hinauf zur Produktionsplanung und Entwicklung miteinander kommunizieren. Durch die intelligente Vernetzung von Maschinen und Abläufen in der Industrie 4.0 mit Hilfe von Informations- und Kommunikationstechnologie, wird eine flexible Produktion ermöglicht, da die Auslastung der Maschinen besser geplant und Produktionsprozesse besser abgestimmt werden



können. Die Netzanbindung erfordert keine besondere Datenübertragungsrate, da sich das Datenvolumen in Grenzen hält. Die Latenzzeiten im Netz müssen aber sehr gering sein. Oftmals ist es nicht möglich, die Maschine an ein Kabelnetz oder per WLAN anzuschließen. Hier kommt die neue Mobilfunkgeneration 5.0 zum Einsatz, die mit geringer Sendeleistung in Werkshallen eingesetzt werden kann und so die Maschine, Sensoren und Aktoren mit den darüber liegenden Ebenen verbindet.

Lernzielkontrollen TAG 2 und TAG 3

1. Betrachten Sie das Bild „Computernetze“ im Modul auf Seite 12. Darin sind viele Informationen enthalten. Beantworten Sie folgende Fragen. Bei Unklarheiten recherchieren Sie im Internet.
 1. Bei welchen Netzen wird eine exklusive Leitung während der Kommunikation bereitgestellt?
 2. Internet-Service-Provider (ISP) sind Betreiber von Netzwerken mit Anschluss ans Internet. Welches sind die hauptsächlichen Dienste, die diese Provider anbieten?
 3. Nennen Sie jeweils drei Beispiele für Sensoren und Aktoren.
 4. Unterscheiden Sie das Internet vom Intranet.
2. Wahr oder falsch?
 - a) VPN-Verbindungen sind sicher gegen Abhören und Verändern von Daten.
 - b) Ein VLAN ermöglicht den Zugang vom Internet zu einem Server im LAN.
 - c) Der Zugang vom Internet zu einem LAN-internen Server geschieht über VPN.
 - d) IP-Adressen adressieren Rechner im Internet oder LAN.
 - e) VPN und Tunneling sind zwei Begriffe für dieselbe Technik.
 - f) VPN kann einzelne Rechner sicher miteinander verbinden.
 - g) VPN kann mehrere Standortnetze sicher miteinander verbinden.
 - h) Trunk ist ein anderer Ausdruck für Cloud.
 - i) In einem Peer-to-Peer-Netz können sich mehrere Server befinden.
 - j) Ein Home-Office-Arbeitsplatz ist in der Regel ein Site-to-Site-VPN.
 - k) Bei Peer-to-Peer sind zwei PCs direkt über ein Kabel miteinander verbunden.
3. In wie viele VLANs kann man ein Netzwerk aufteilen? Begründen Sie Ihre Antwort.
4. Auf welchen Teilstrecken zwischen zwei Rechnern eines VLANs werden getaggte und auf welchen werden untaggte Frames übertragen?
5. Prüfen Sie Ihr Wissen zu Computernetzen. Welche Aussage ist richtig oder falsch.
 1. Ein LAN kann beliebig groß sein.
 2. Ein WAN beschränkt sich auf ein Betriebsgelände
 3. In privaten Netzen werden IP-Adressen aus anderen Adressbereichen verwendet als in öffentlichen Netzen.
 4. Wenn ein Rechner Daten auf seiner Festplatte freigibt, ist er ein Fileserver.
 5. Fungiert ein Arbeitsplatzrechner als Server für andere Clients, nennt man dies Point-to-Point-Netz.
 6. Mit VPN können einzelne Rechner an ein LAN angeschlossen werden.
 7. Mit VPN können ganze Niederlassungen miteinander sicher verbunden werden.
 8. Bei einem End-to-Site-VPN wird nur ein Rechner für eine sichere Netzverbindung ausgelagert.
 9. Bei einer Site-to-Site-Verbindung werden genau zwei Rechner verschlüsselt verbunden.
 10. Bei einem Client-Server-Netz kann jeder Rechner gleichzeitig Server und Client sein.
6. Wahr oder falsch?
 - a) On-Premises Datacenter werden von IT-Dienstleistungsunternehmen bereitgestellt.
 - b) Off-Premises Datacenter sind in einem Nebengebäude untergebracht.
 - c) Wenn man den eigenen Server bei einem großen Rechenzentrumsbetreiber in dessen Rechenzentrum einstellt, nennt man dies Colocation.
 - d) Ein Web-Server liefert Inhalte zum Abrufen mit einem Webbrowser.
 - e) Ein Daten-Server liefert Inhalte zum Abrufen mit einem Webbrowser.
 - f) Nutzt man Server in einem Off-Prem-Rechenzentrum dann ist man selbst für die Stromversorgung und Klimatisierung verantwortlich.

- g) Bei einem On-Prem-Rechenzentrum hat man eine optimale Anbindung ans Internet.
7. Mit welchen Datenraten greifen Sie auf den verschiedenen Rechenzentren (On-Prem, Off-Prem, Colocation) zu?
8. Welchen Typ von Rechenzentrum würden Sie empfehlen, wenn ein Betrieb im ländlichen Raum mit sehr schlechter Internetanbindung seine Umsätze hauptsächlich mit seinem Online-Shop macht?
9. Ergänzen Sie die Liste der möglichen Serverdienste. Erklären Sie stichwortartig, welche Dienste geleistet werden. Versuchen Sie zunächst, die Liste ohne Hilfsmittel zu ergänzen. Wenn Sie nicht mehr weiterkommen, nehmen Sie das Modul zu Hilfe oder recherchieren Sie im Internet.

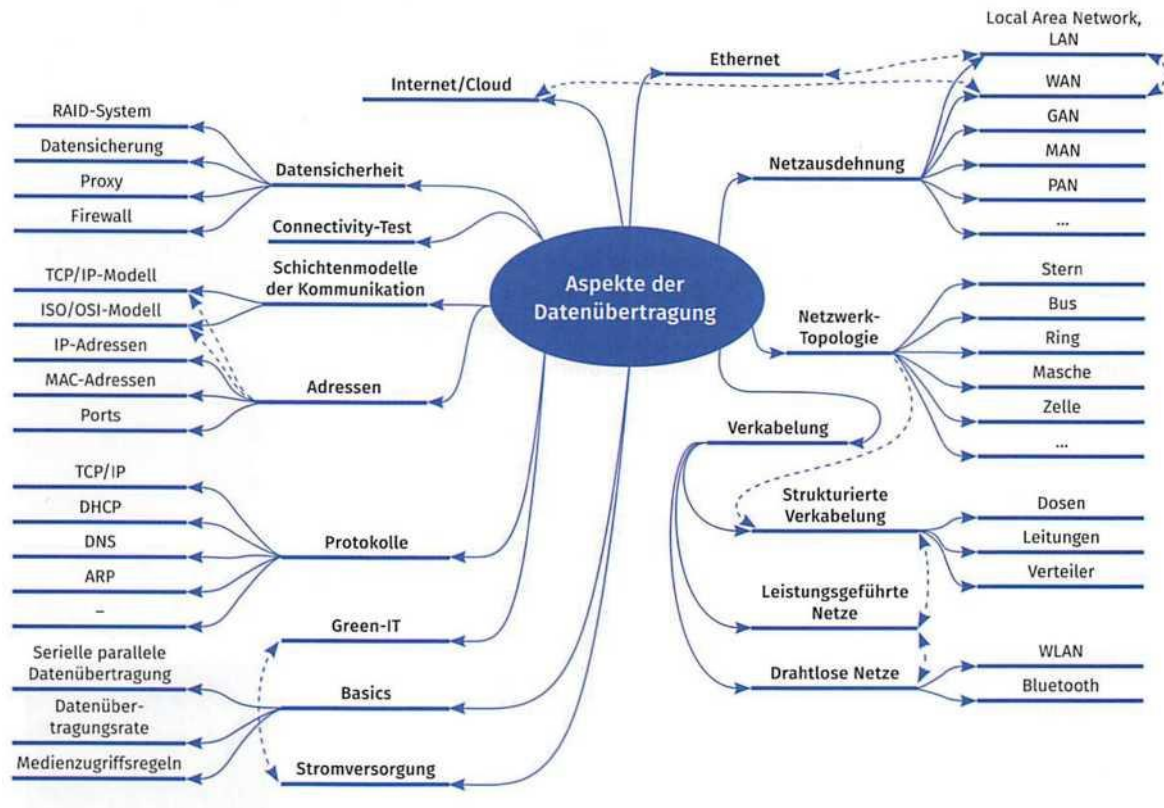
Serverdienste	Erklärung
Fileservice	Bietet Speicherplatz im Netzwerk an (wie eine lokal angeschlossene Festplatte)
...	...
...	...

10. Wie nennt man die Fernleitungen, die wichtige Knotenpunkte in Internet miteinander verbinden?
11. Welche Funktion hat ein Internet-Provider?
12. Wie nennt man ein Unternehmen, welches großflächige (nationale oder internationale) Datennetze betreibt und anderen Unternehmen gegen Gebühr Datenübertragungsleistungen anbietet?
13. Was ist richtig, was ist falsch?
1. Fat Clients werden immer über WLAN mit dem Netzwerk verbunden.
 2. Jedes Gerät im Netzwerk, welches Dienste von anderen Rechnern nutzt, ist ein Client.
 3. Ein Thin Client braucht zwingend einen Netzwerkanschluss.
 4. Ein Thin Client verfügt über eine hohe Rechenleistung.
 5. BYOD bringt dem Admin viele Probleme ins Haus.
 6. BYOD lohnt sich für den Betrieb, da die Mitarbeiter ihre eigenen Geräte zur Arbeit mitbringen.
 7. CPS können sehr komplexe Strukturen annehmen.
 8. Embedded Systems werden nicht als Arbeitsplatzrechner verwendet.
 9. Ein Embedded PC wird auch als Arbeitsplatzrechner verwendet.
14. Wie nennt man ein Rechenzentrum, welches sich nicht im Unternehmen-LAN befindet?
15. Ordnen Sie den Arbeitsplätzen die am besten geeigneten Rechner zu.
- Sie haben fünf Typen von Arbeitsplatzrechnern standardisiert.
1. Desktop-PC mit mittlerer Leistung, 100 Mb/s Ethernet.
 2. Tower-PC mit hoher Rechenleistung, sehr guter Grafikkarte und zwei Flachbildschirmen, 10 Gb/s Ethernet
 3. Laptop-PC mit mittlerer Leistung, Dockingstation mit Tastatur, Maus und Flachbildschirm, 1000 Mb/s Ethernet
 4. Tablet-PC, WLAN 802.11n
 5. Thin-Client, in die Tastatur integrierter Rechner mit LAN-Anschluss, integrierter Maus (als Trackball) und externer Flachbildschirm, 10 Mb/s Ethernet, keine weiteren Schnittstellen

Arbeitsplatz	Rechner	Begründung
Service-Desk im Kunden-Eingangsbereich		
Softwareentwicklung		
Sachbearbeiter Einkauf		
Sachbearbeiter Verkauf/ 50% Homeoffice		
Vertrieb – Innendienst mit Außendienst		
Konstruktion/ CAD		
Lager – Büro		
Lager – Kommissionierung mit Gabelstapler		
Marketing – Erstellen von Werbebroschüren		

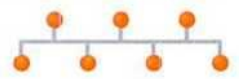
TAG 4 und TAG 5 - Grundlagen der Datenübertragung in Netzwerken

Sie lernen die Grundlagen der Datenübertragung und Netzwerktechnik, um Clients in ein bestehendes Netzwerk einzubinden.



Ein Computernetz besteht aus einer Vielzahl von Komponenten und Informationen. Nicht nur Hardware, auch Software und Einstellungen (z.B. Adressen) gehören dazu. Wir machen gedanklich einen Rundgang durch ein modernes Unternehmen und betrachten uns dabei das komplette Computernetz. Einiges, was wir finden, ist in folgender Tabelle zusammengefasst:

Computernetzwerk, Local Area Network (LAN)			
Netzwerkknoten (Nodes)	Clients	Clients sind „Kunden“ im Netzwerk, z.B. Arbeitsplatzrechner, Drucker	
	Server	Server stellen den Clients Dienste (Services) zur Verfügung	
	Drucker	An einzelnen Arbeitsplätzen und an zentralen Punkten als Arbeitsgruppendrucker	
Netzwerkgeräte	Switch	Sorgen für den Transport und das Weiterleiten der Daten vom Sender zum Empfänger - über Leitungen und Funk	
	Router		
	Access Point		

Computernetzwerk, Local Area Network (LAN)				
Adressen im Netzwerk	Host im Netzwerk		48-Bit MAC-Adresse (Interface-Adr.)	
	Interface am Host (z.B. Ethernet 1, WLAN)		32-Bit IP-Adresse (Version 4) 128-Bit IPv6-Adresse 32-Bit Subnetmask (trennt Netz- und Host-Anteil einer IP-Adresse)	
	Applikation auf dem Host (z. B. Webservice, E-Mail-Service)			
Strukturierte Verkabelung	Verteiler Anschlussdosen Leitungen		Verteilerschranke mit 19 Zoll Breite zum Anschluss von Rechnern, Telefonen, Druckern und zum Verbinden von Verteilern, Dosen, Geräten	
Netzwerk-Medien	Kupferleitungen		Kabel verbinden Verteiler und Anschlussdosen; Schnüre zum Anschließen von Endgeräten und zum Patchen im Verteiler	
	Glasfaser-leitungen			
	Funk			
Topologie	„Landkarte“ des Netzwerks; die Topologie beschreibt, wie die Leitungen verlegt werden und welchen Weg die Daten nehmen			
Netzwerk-Protokolle	TCP/IP	ARP	Regeln zum Versenden und Empfangen von Daten	
	UDP	DNS		
	IP	DHCP		
	etc.			
Cloud Computing	Über das Netz (Internet) bereitgestellte IT-Infrastruktur wie Speicher, Rechenleistung, Anwendungsprogramme			

LE 1 - Funktionsweise von Rechnernetzen verstehen

Sie sollen die grundlegende Funktionsweise von Computernetzwerken und Datenaustausch verstehen, um darauf aufbauen zu können.

(1) Datenübertragung und deren Kenngrößen

Die Informatik erzeugt und nutzt eine Unmenge an Daten - und laufend werden es mehr. Wir wollen auf Daten zurückgreifen, die nicht auf unserem Rechner gespeichert sind, wollen aber dazu keine langen Wartezeiten in Kauf nehmen. Daten, die am anderen Ende der Welt gespeichert sind, wollen wir nutzen, als ob sie lokal vorhanden wären. Diese Daten werden nicht auf Datenträgern, USB-Sticks oder DVDs per Post verschickt. Sie werden Bit für Bit nacheinander als physikalische Signale über Netzwerkmedien übertragen. Zusammen bilden sie ein Rechnernetzwerk.



Kenngrößen in der Datenübertragungstechnik		
Bezeichnung	Einheit	Formel, Wert, Bemerkung
Datenmenge D	Bit, Byte	Dateigröße
Zeit t	s, Sekunde	t
Datenübertragungsrate im Netzwerk C	Bit/s, bps oder Byte/s, B/s	$C = \text{Datenmenge pro Zeit} = \frac{D}{t}$
Geschwindigkeit v	km/h	$V = \text{Strecke pro Zeit} = \frac{s}{t}$
Signalgeschwindigkeit c	m/s, km/s	$c = \text{Strecke pro Zeit} = \frac{D}{t}$
Lichtgeschwindigkeit im Vakuum c_0	m/s, km/s	$c_0 = 2,99792458 \cdot 10^8 \text{ m/s}$ $\approx 3 \cdot 10^8 \text{ m/s}$
Verkürzungsfaktor (NVP, Nominal Velocity of Propagation)	-	$NVP = \frac{c}{c_0}$ (Kupferleitungen NVP = 0,6 ...0,85)
Signalgeschwindigkeit bei Kupferleitungen	$c = c_0 \cdot NVP$	Typischer Wert: 2/3 der Lichtgeschwindigkeit, ca. $2 \cdot 10^8 \text{ m/s}$
Brechungsindex bei Glasfasern	$n = \frac{c_0}{c}$	Typischer Brechungsindex des Faserkerns: $n = 1,4 \dots 1,5$
Signalgeschwindigkeit bei Lichtwellenleitern	$c = \frac{c_0}{n}$	Typischer Wert: 2/3 der Lichtgeschwindigkeit, ca. $2 \cdot 10^8 \text{ m/s}$
Bandbreite B	Hertz, Hz	Differenz zwischen oberer und unterer Grenzfrequenz; für die Informationsübertragung verwendeter Frequenzbereich

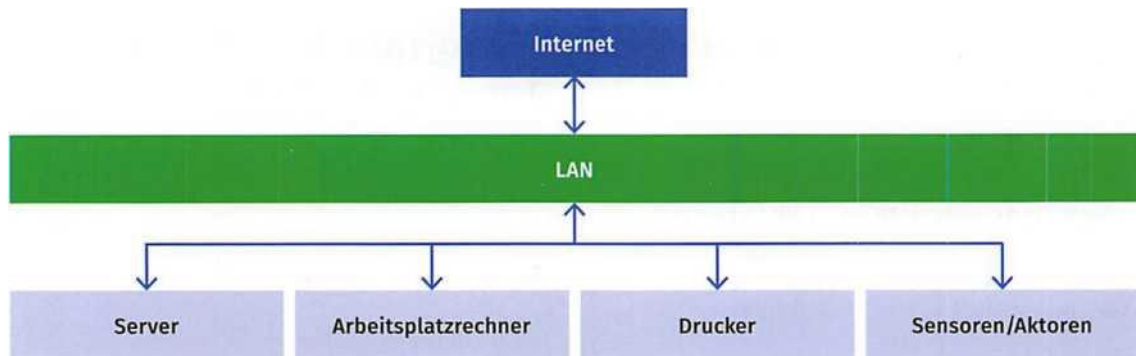
Ein Bit ist die kleinste Informationseinheit der IT. Es kann die Werte 0 und 1 enthalten. Das Formelzeichen ist Bit, bit oder b (z. B.: bit/s oder b/s oder bps jeweils für Bit pro Sekunde oder kb für kilobit, kib für kilo-binary). Ein Byte besteht aus 8 Bit (z.B.: 0101 1010). Das Formelzeichen ist Byte oder B (z. B.: MB/s für Mega Byte pro Sekunde,...), **siehe auch Kapitel 5.2.5, Seite 487.**

Signale auf Netzwerkmedien

- Elektrische Signale über Kupferleitungen
- Lichtsignale über Glasfaserleitungen
- Elektromagnetische Strahlen bei Drahtlosnetzwerken (z.B. WLAN/Wi-Fi, Bluetooth)

Jedes Haus und jede Wohnung verfügt heute über ein lokales Netzwerk (LAN, Local Area Network) mit Anschluss ans Internet. Unternehmen sind ohne LAN und Internet nicht mehr arbeitsfähig. Dieser Technik kommt also eine zentrale Bedeutung zu.

Rechnernetzwerke sind heute überall in unserem Leben vorhanden. Sie durchdringen unser gesamtes Leben in (fast) allen Lebensbereichen - oft ohne unser Wissen. Das Netzwerk, welches alle LANs verbindet - und so praktisch alle Rechner der Welt miteinander verbindet ist das **Internet**.



Rechner im Netzwerk sind nicht nur Arbeitsplatzrechner, Server oder Smartphones. Auch Sensoren (z. B. zum Messen von Temperatur, Füllstand) und Aktoren (z.B. zum Steuern von Rollladenantrieb, Pumpe, Lüftung) sind sog. Nodes (Knoten). Ein Netzwerkknoten ist jeder Teilnehmer am Rechnernetz, der Daten ins Netz sendet oder über das Netz abruft.

Datenübertragungsrate C berechnen

Wichtig für ein Übertragungsmedium ist der Durchsatz, ähnlich wie bei Autos pro Stunde auf einer Straße oder Litern pro Minute in einer Rohrleitung. Die Geschwindigkeit ist ebenfalls wichtig, ist aber nicht mit der Übertragungsrate zu verwechseln.



Der Durchsatz an Fahrzeugen hängt auch von der Straße ab.

Die Begriffe „Datenrate“, „Datenübertragungsrate“, „Übertragungsrate“, „Datendurchsatz“, „Durchsatz (Throughput)“ oder „Kanalkapazität (Channel Capacity)“ werden synonym verwendet. In der Computertechnik ist das die Datenmenge D , die in einer bestimmten Zeit t über ein Medium transportiert werden kann. Das Formelzeichen für die Datendurchsatzrate ist C (das C steht für Capacity, also die Leitungsübertragungskapazität). Dabei ist es egal, ob es sich um den Datendurchsatz eines Festplatten-Interfaces handelt, eines Druckers oder eines Netzwerk-Interfaces. Besondere Vorsicht ist geboten, damit Bits und Bytes nicht verwechselt werden.

Datenübertragungsrate C

Datenübertragungsrate $C = \frac{\text{Datenmenge}}{\text{Zeit}} = \frac{D}{t}$ in Bits pro Sekunde oder bit/s oder b/s oder bps, bzw. Byte/s oder B/s

Übertragungszeit $t = \frac{\text{Datenmenge}}{\text{Datenübertragungsrate}} = \frac{D}{C}$ in Sekunden

Beispiel

Ein Film mit 1 GB Größe soll über eine Leitung mit $C = 50 \text{ Mbit/s}$ übertragen werden. Wie lange dauert die Übertragung? Vorsicht: Bit und Byte sind zweierlei! 1 Byte sind 8 Bit!

Lösung: $D = 1 \text{ GB} = 8 \text{ Gbit} = 8 \cdot 10^9 \text{ Bit}$
 $C = 50 \text{ Mbit/s} = 50 \cdot 10^6 \text{ b/s}$

$t = \frac{D}{C} = \frac{8 \cdot 10^9 \text{ b}}{50 \cdot 10^6 \text{ b/s}} = \frac{8 \cdot 10^3}{50} \text{ s} = 160 \text{ s}$ (2 Minuten und 40 Sekunden)

Häufig spricht man in der IT von „Geschwindigkeit“, oft auch von „Bandbreite“, meint damit aber die Datenrate. Um Missverständnisse zu vermeiden, muss man sich korrekt ausdrücken!

In der IT bezeichnet die Geschwindigkeit die Laufzeit, die ein Signal braucht, um eine bestimmte Strecke zurückzulegen. Diese Datenausbreitungsgeschwindigkeit (oder Signalgeschwindigkeit) liegt bei etwa zwei Drittel der Lichtgeschwindigkeit in Vakuum. Und das ist bei Glasfaser- und bei Kupferleitungen etwa gleich. Glasfaserleitungen haben keine höhere Signalgeschwindigkeit als Kupferleitungen, wohl aber eine höhere Datenübertragungsrate.

Heute sind in lokalen Netzen Datenübertragungsraten von 10 Mbit/s bis 100 Gbit/s verfügbar. „Normale“ Büroverkabelung erlaubt oft in älteren Installationen noch Übertragungsraten von 100 Mbit/s. Neuere Verkabelung wird mit 1 Gbit/s oder 10 Gbit/s ausgelegt. Datenraten von 40 Gbit/s und 100 Gbit/s werden überwiegend in Rechenzentren eingesetzt. Verkabelung mit 10 Mbit/s ist nur noch sehr selten anzutreffen.

Datenübertragungsraten üblicher Schnittstellen		
Schnittstelle	Übertragungsrate	Bemerkungen
USB 1.0	12 Mbit/s	Full Speed (veraltet)
USB 2.0	480 Mbit/s	Hi-Speed
USB 3.0	5 Gbit/s	SuperSpeed
USB 3.1	10 Gbit/s	SuperSpeed+
USB 3.2	20 Gbit/s, 40 Gbit/s	
USB 4.0	40 Gbit/s	Nachfolger von USB 3.2, nutzt Thunderbolt-Technologie
Thunderbolt 2 (2013)	2 • 10 Gbit/s, 20 Gbit/s	Thunderbolt verwendet „aktive Leitungen“, d.h. in die Stecker ist Elektronik verbaut, welche die Leitungsanpassung vornimmt.
Thunderbolt 3 (2015)	40 Gbit/s	
Thunderbolt 4 (2020)	40 Gbit/s	Technische Basis für USB 4.0

Datenübertragungsraten üblicher Schnittstellen		
Schnittstelle	Übertragungsrate	Bemerkungen
ATA-1 bis ATA-7 (alte Bezeichnung IDE)	8,3 Mbyte/s bis 133 Mbyte/s	Paralleler Festplattenanschluss (veraltet)
SATA Express	8 Gbit/s, 16 Gbit/s	Serieller Festplattenanschluss
eSATA	6 Gbit/s	External SATA
Small Computer System Interface (SCSI)	5 Mbyte/s bis 320 Mbyte/s	Paralleler Bus für Massenspeicher und Peripheriegeräte
Serial Attached SCSI (SAS)	3 Gbit/s bis 22,5 Gbit/s	Serielle SCSI-Schnittstelle, Sternverkabelung
iSCSI (Internet SCSI)	Abhängig von der LAN-Technik	SCSI über Ethernet und TCP/IP, ermöglicht Blockzugriff (wie auf lokale Festplatten) auf entfernte Festplatten im lokalen Netzwerk oder im Internet.
FireWire	100 Mbit/s bis 3,2 Gbit/s	Externer Bus für Peripheriegeräte (veraltet), IEEE 1394
Fibre Channel (FC)	Bis 32 Gbit/s	Zum Aufbau von Speichernetzwerken
Fibre Channel over Ethernet (FCoE)	Abhängig von der LAN- Technik	Fibre-Channel-Protokoll wird über Ethernet übertragen.
Ethernet/LAN	10 Mbit/s bis 400 Gbit/s	Gängige Netzwerktechnologie
DSL	384 kbit/s bis 250 Mbit/s	WAN-Anbindung über Telefon- oder Kabelfernsehtz
ISDN	64 kbit/s	Ein Anschluss = 2 Kanäle = 128 kbit/s
V.24/RS232	Max. 115 kbit/s, typisch 9,6 kbit/s	Serielle PC-Schnittstelle

Die Tabelle zeigt die Datenübertragungsrate an der Schnittstelle. Durch Protokoll-Overhead, oder das Verwenden von entsprechenden Leitungscodes liegt die tatsächliche Übertragungsrate zum Teil wesentlich niedriger. Vorsicht: Manche Schnittstellen sind mit Bit/s, andere mit Byte/s (8 Bit = 1 Byte) angegeben.

(2) Übertragungsarten

Die Art und Weise, wie die Daten übertragen werden, ob in eine Richtung (nur Senden) oder in beide Richtungen (Senden und Empfangen), ob die Bits gleichzeitig über mehrere Leitungen oder nacheinander auf einer Leitung übertragen werden, fasst die folgende Tabelle kurz zusammen.

Übertragungsarten		
Typ	Beschreibung	Bemerkungen/ Beispiel
Seriell	Bits werden nacheinander übertragen	V.24-Schnittstelle, USB, SATA
Parallel	Mehrere Bits (z.B. 8,16, 32) werden gleichzeitig übertragen	Druckerschnittstelle, PC-System-Busse

Übertragungsarten		
Typ	Beschreibung	Bemerkungen/ Beispiel
Simplex	Datenübertragung nur in eine Richtung	Rundfunk
Duplex	Datenübertragung in beide Richtungen	
Halbduplex	Richtungsumschaltung, Übertragung immer nur in eine Richtung	Walkie-Talkie
Vollduplex	Datenübertragung in beide Richtungen gleichzeitig	Telefon
Multiplex	Mehrere Übertragungskanäle nutzen dasselbe Übertragungsmedium, dieselbe Leitung Zeitmultiplex: Kanäle werden zu unterschiedlichen Zeiten das Medium Frequenzmultiplex: Kanäle benutzen unterschiedliche Frequenzen Wellenlängenmultiplex: Kanäle benutzen unterschiedliche Wellenlängen (Farben)	Mehrfachausnutzung von Netzwerkressourcen

(3) Adressierungsarten im Netzwerk

Wie ein Redner zu einem Einzelnen, zu einer Gruppe oder gar zu allen Anwesenden sprechen kann, so werden auch in der Netzwerktechnik mehrere Adressierungsarten unterschieden. Die folgende Tabelle fasst die vier Adressierungsarten zusammen.

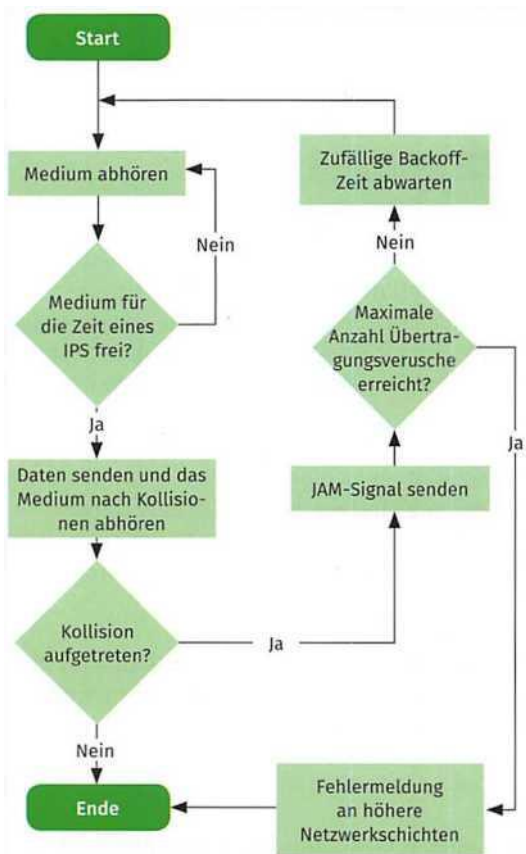
Adressierungsarten im Netzwerk		
Typ	Beschreibung	Bemerkungen/Beispiel
Unicast	Ein Sender adressiert einen einzigen Empfänger.	Einzelsprache
Multicast	Ein Sender adressiert eine Menge (eine Gruppe) von Empfängern.	Sendung „an alle Router“, „an alle Mitglieder der Gruppe XY“
Broadcast	Ein Sender adressiert alle Stationen im gesamten Netz, Spezialfall von Multicast.	„an alle Stationen im Netz: wer hat die IP-Adresse 1.2.3.4?“
Anycast	Ein Sender adressiert einen unbestimmten Empfänger einer bestimmten Gruppe.	Wird unter anderem bei Lastverteilung angewendet - derjenige Rechner mit den meisten freien Kapazitäten wird angesprochen

LE 2 - Den Zugriff auf die Netzwerkmedien verstehen

Sie wollen wissen, wie der Zugriff auf das Netzwerkmedium geregelt wird, damit sich die Stationen nicht gegenseitig stören.

Wenn zwei Stationen gleichzeitig ihre Daten auf ein Netzwerkmedium schicken, dann überlagern sich diese und werden für alle Stationen unverständlich. Man nennt dies eine **Kollision**. Es gibt mehrere Möglichkeiten, den Zugriff so zu regeln, dass immer nur eine Station sendet.

Eine zentrale Grundregel beim Medienzugriff bei Ethernet lautet: Listen Before Talk (LBT) - Erst hören - dann sprechen!

Medienzugriffsverfahren	
Verfahren	Beschreibung
Zentrale Steuerung	Zentrale Station erteilt Sendeerlaubnis an die angeschlossenen Stationen → Einsatz in Funknetzen (WLAN) durch RTS/CTS-Pakete (RTS = Request to Send = Sendeabfrage und CTS = Clear to Send = Sendeerlaubnis)
Carrier Sense Multiple Access/Collision Detection (CSMA/CD)	- Carrier Sense (Trägererkennung) bedeutet, das Abhören des Mediums, ob es frei ist - Multiple Access (Mehrfachzugriff) bedeutet, dass mehrere auf dieses Medium zugreifen können - Collision Detection (Kollisionserkennung); dabei wird während des Sendens überprüft, ob eine andere Station dazwischen sendet und es damit eine (Daten-) Kollision gibt. → Einsatz bei Ethernet  <pre> graph TD Start([Start]) --> Listen[Medium abhören] Listen --> Free{Medium für die Zeit eines IPS frei?} Free -- Ja --> Send[Daten senden und das Medium nach Kollisionen abhören] Free -- Nein --> Listen Send --> Coll{Kollision aufgetreten?} Coll -- Ja --> Jam[JAM-Signal senden] Coll -- Nein --> End([Ende]) Jam --> Backoff[Zufällige Backoff-Zeit abwarten] Backoff --> Free Jam --> Retries{Maximale Anzahl Übertragungsversuche erreicht?} Retries -- Ja --> Error[Fehlermeldung an höhere Netzwerkschichten] Retries -- Nein --> Backoff Error --> End </pre>
Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)	Kollisionsverhinderung durch Abhören des Mediums und anschließendes Abwarten einer bestimmten Zeit vor dem Senden → Einsatz in Funknetzen (WLAN)
Token Passing	Der Token ist die Sendeerlaubnis. Diejenige Station, die den Token hat, darf <u>ein einzelnes</u> Paket verschicken und muss den Token anschließend an eine andere Station weitergeben. Sie bekommt den Sendetoken erst wieder, wenn jede andere Station den Token hatte. → Einsatz bei Token-Ring (veraltet) und Glasfaserringen

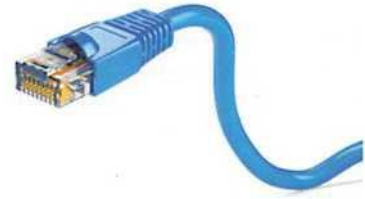
LE 3 - Ethernet als Netzwerkstandard verwenden

Sie sollen die Grundlagen von Ethernet verstehen, um es zu verwenden.

Die heute vorherrschende Technologie in lokalen Netzwerken ist das Ethernet. Es hat sich wegen seiner Einfachheit gegenüber anderen Techniken durchgesetzt und diese vollständig vom Markt verdrängt. Ethernet ist skalierbar und abwärtskompatibel. Das heißt, dass neuere Geräte auch mit älteren Ethernet-Verkabelungen und -Geräten zusammenarbeiten.

Die ersten Ethernet-Implementierungen waren als Bus-Topologie mit Koaxialleitungen und 10 MB/s realisiert. Diese waren fast 20 Jahre im Einsatz, sind aber seit der Jahrtausendwende durch Twisted-Pair-Leitungen (TP) ersetzt worden.

Ethernet geht auf eine Entwicklung an der Universität von Hawaii zurück (Aloha-Net) und wurde erstmals 1980 in der Version 1 definiert. Es war ursprünglich ein LAN-Standard mit anfänglich 1 Mbit/s Übertragungsrate. Ethernet umfasst die Software (Netzwerkprotokolle) sowie Hardware (Leitungen, Steckverbinder, Netzwerkkarten und -geräte). Es ist die Basis, auf der andere Netzwerktechniken aufsetzen. Das bekannte TCP/IP basiert in LANs auf dem Ethernet-Standard.



Heutige übliche Übertragungsraten reichen von 10 Mbit/s bis 100 Gbit/s. Neuere Entwicklungen definieren Datenraten von bis zu 400 Gbit/s. Standard in heutigen Verkabelungen sind 1 Gbit/s oder 10 Gbit/s über Twisted-Pair-Leitungen aus Kupfer. Für die meisten Datenraten gibt es Lichtwellenleiter und Kupferlösungen. Die maximale Leitungslänge bei Kupferleitungen beträgt in der Regel 100 m.

Ethernet definiert die hardwarenahe Kommunikation (siehe Kapitel 3.4.7) auf den OSI-Schichten 1 und 2.

(1) Ethernet-Frame-Aufbau

Daten, die über ein Netzwerk verschickt werden, werden nicht als kontinuierlicher Datenstrom (so wie eine Radiosendung) übertragen. Eine gewisse Anzahl von Daten wird zusammengefasst und als Datenpaket verschickt. Die Daten, die über ein Ethernet verschickt werden, werden in einen Frame, einen Rahmen, eingepackt. Der Frame wird Bit für Bit, seriell, von links nach rechts, über die Leitung übertragen. Der Frame startet mit einem Synchronisationssignal, der Preamble. Die Empfänger stellen sich dadurch auf die Übertragungsrate ein, sodass sie jedes Bit zeitgenau einlesen können.

Takt/ Synchroni- sation	Ziel- Interface- Adresse	Absender- Interface- Adresse	Typ	Nutzdaten (min. 46 Byte, max. 1 500 Byte)	Prüfsumme
8 Byte	6 Byte	6 Byte	2 Byte	46 Byte ... 1 500 Byte	4 Byte

Nach der Synchronisation wird die Adresse des Interfaces übertragen, welches die Daten empfangen soll. Dies ist die Adresse der Netzwerkkarte des Zielrechners. Nach der Zieladresse folgt die Absenderadresse. Im Typ-Feld wird angegeben, von welchem Typ die folgenden Nutzdaten sind. Wird als Nutzdaten beispielsweise ein IP-Paket übertragen, so steht hier die Kennung 0x8100. Die Nutzdaten müssen mindestens 46 Byte groß sein. Die maximale Größe beträgt 1 500 Byte. Die maximale Nutzdatengröße wird als Maximum Transmission Unit (MTU) bezeichnet. Eine Prüfsumme „rahmt“ die Daten ein und bildet das Ende des Frames. Die Prüfsumme dient dem Erkennen von Übertragungsfehlern.

Interfaceadressen und Type bilden den Protokollkopf oder Header. Zusammen mit der Prüfsumme werden 18 Byte als „Protokolloverhead“ beansprucht.

(2) Ethernet-Frame-Aufbau mit VLAN-Erweiterung

Werden VLANs eingesetzt, so wird der Frame um den VLAN-Tag erweitert.

Takt/ Synchroni- sation	Ziel-Inter- face- Adresse	Absender- Interface- Adresse	VLAN- Tag	Typ	Nutzdaten (min. 46 Byte, max. 1 500 Byte)	Prüf- summe
8 Byte	6 Byte	6 Byte	4 Byte	2 Byte	46 Byte ... 1 500 Byte	4 Byte

VLAN-Tag			
TPID	Prio	CF	VLAN-ID
2 Byte Inhalt 0x8100	3 Bit	1 B	12 Bit

Der VLAN-Tag beginnt mit der Zahlenfolge 0x8100. Dies ist sozusagen der „Spezialtyp“ für VLANs. Die VLANs können unterschiedlich priorisiert werden. Sprachdaten von einem Telefon-VLAN können beispielsweise bevorzugt transportiert werden, wogegen E-Mail seine niedrige Priorität bekommen können. Aus Kompatibilitätsgründen mit Token-Ring-Netzen ist das CF-Bit enthalten. Es ist heute bedeutungslos. Die 12-Bit große VLAN-ID ist die eigentliche Zuweisung eines Frames zu einem VLAN. Damit sind 2^{12} VLANs unterscheidbar.

LE 4 - TCP/IP als Netzwerkstandard verwenden

Sie sollen die Grundzüge des heutigen Standards TCP/IP verstehen.

TCP/IP ist eine Protokollsuite - eine Sammlung mehrerer Netzwerkprotokolle. Die wichtigsten sind Transmission Control Protocol (TCP) und Internet Protocol (IP). Diese Protokolle nutzen das darunterliegende Ethernet. Anders ausgedrückt, Ethernet transportiert als Nutzdaten die TCP/IP-Protokolle.

TCP/IP-Protokolle	
Internet-Protocol (IP)	IP-Adressen adressieren Netzwerke und Rechner, IP-Pakete werden anhand der IP-Adresse durch Netzwerke geroutet. IP ist unabhängig von der verwendeten Übertragungstechnik. IP ist verbindungslos, ohne Quittung oder Rückmeldung.
Transmission Control Protocol (TCP)	TCP-Adressen (TCP-Ports) adressieren Applikationen. TCP ist unabhängig von der verwendeten Übertragungstechnik. TCP ist verbindungsorientiert, vor der Datenübertragung wird eine Verbindung zwischen den Kommunikationspartnern aufgebaut und gehalten. TCP-Übertragung ist sicher - Zustellung wird überprüft und quittiert, fehlende Datensegmente nachgeliefert. TCP steuert den Datenfluss, greift zur Stauverhinderung (Congestion Control) ein.
User Datagram Protocol (UDP)	UDP-Adressen (UDP-Ports) adressieren Applikationen. UDP-Übertragung ist unsicher - Zustellung wird nicht überprüft, nicht quittiert, fehlende Datensegmente nicht nachgeliefert. UDP-Daten werden als Datenstrom gesendet. UDP-Header ist kleiner, einfacher als der TCP-Header → weniger Protokoll-overhead und schnellere Auslieferung. Anwendung bei Multicast. UDP macht keine Datenflusssteuerung, keine Stauverhinderung (Congestion Control) UDP ist unabhängig von der verwendeten Übertragungstechnik UDP ist verbindungslos

Mit einer IP-Adresse und einem TCP- oder UDP-Port wird ein Rechner und eine darauf laufende Applikation weltweit eindeutig adressiert. Dieses Paar von Adressen bezeichnet man als Socket.

Bei einer Kommunikation zweier Rechner sendet der Absender seine Quell-IP und den Quell-Port seiner Anwendung an die Ziel-IP und den Ziel-Port des Zielrechners. Es sind also zwei Sockets für eine Kommunikation notwendig.

Bei den Ports handelt es sich um eine 16 Bit große Zahl. Die ersten 1 024 Ports (0 bis 1 023) nennt man die „Well-known Ports“. Port-Adressen zwischen 1 024 und 49151 sind „Registered Ports“. Diesen Ports sind bereits Anwendungen zugeordnet. Die Ports darüber sind frei verwendbar.

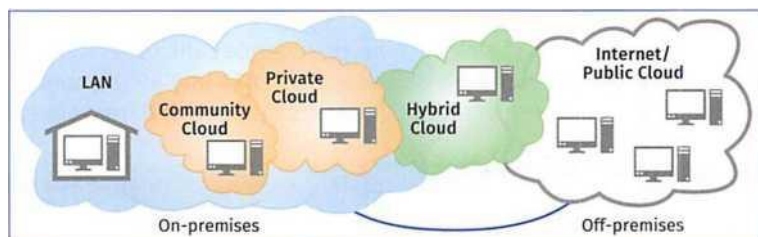
Beispiele für Well-known Ports			
Port-Nr.	TCP	UDP	Bezeichnung/Beschreibung
20	X	-	FTP-Datenübertragung
21	X	X	FTP-Steuerkanal
22	X	X	Secure Shell, Konsolensteuerung verschlüsselt (SSH)
23	X	X	Telnet, Konsolensteuerung
80	X		Hyper Text Transfer Protocol (HTTP)
110	X		PostofficeProtocol v3
123		X	Network Time Protocol
143	X	X	Internet Message Access Protocol (IMAP)
161		X	Simple Network Management Protocol (SNMP)
201	X	X	Apple Talk
433	X		HTTPS (http over SSL/TLS)
631	X	X	Internet Printing Protocol und CUPS Common Unix Printing Protocol (IPP)
636	X	X	Lightweight Directory Access Protocol (LDAP)
860	X		iSCSI
989	X	X	Data FTP over SSL/TLS (FTPS)
990	X	X	Control FTP over SSL/TLS (FTPS)
1194	X	X	OpenVPN

LE 5 - Cloud-, Fog- und Edge-Computing unterscheiden

Sie sollen ein Verständnis für Cloud-Computing entwickeln, Edge und Fog beschreiben und gegen die Cloud-Technik abgrenzen können.

Cloud ist der englische Begriff für eine Wolke, etwas Diffuses, etwas nicht

Greifbares. Cloud-Computing ist eine „Rechnerwolke“ für das Bereitstellen von IT-Infrastruktur in einem Netzwerk, unabhängig davon, wo sich die Clients als Nutzer und die Server als Cloud-Anbieter befinden. Nach gängiger Sprechweise werden vier sog. Liefermodelle von Clouds unterschieden:



- **Public Cloud** - öffentliche Rechnerwolke: IT-Infrastrukturen über das Internet, für die Öffentlichkeit nutzbar. Die Anbieter vermieten ihre Dienstleistung. Der Kunde zahlt nutzungsabhängig (Pay-As-You-Go).
- **Private Cloud** - private Rechnerwolke: IT-Infrastrukturen, die ein Unternehmen im eigenen LAN (On-Premises) oder bei einem externen Betreiber im Internet betreibt. Die Nutzung ist nur für eigene betriebliche Zwecke möglich.
- **Hybrid Cloud** - hybride Rechnerwolke: Kombination von privater und öffentlicher Cloud.

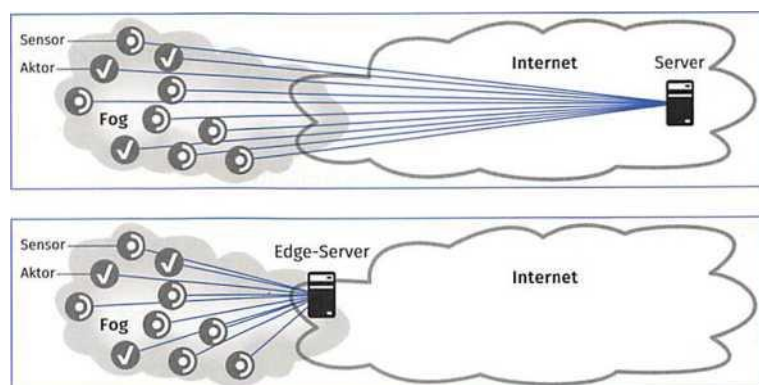
- **Community Cloud** - gemeinschaftliche Rechnerwolke: Cloud für einen speziellen Nutzerkreis, gemeinschaftliche Nutzung auch für entfernte Nutzer, wird meist als private Cloud betrieben mit Zugang für bestimmte User von außen.

Cloud-Computing-Dienste			
Cloud-Dienst	Erklärung		Beispiele
Cloud-Speicher	Stellt Speicherplatz online zur Verfügung („externe Festplatte“)		ownCloud, Open Cloud, Dropbox, Google Drive
SaaS	Software as a Service	Stellt Anwendungssoftware online zur Verfügung	Online-Textverarbeitung, Bildbearbeitung, Tabellenkalkulation, Warenwirtschaftsprogramme
	Storage as a Service	Stellt Speicherplatz online zur Verfügung	Cloud-Speicher, Amazon S3, Dropbox, Google Drive
PaaS (Platform as a Service)	Eine Computerplattform mit einer lauffähigen Entwicklungsumgebung für Webentwickler wird zur Verfügung gestellt. Auf dieser Plattform können komplette Software-Lebenszyklen durchgeführt werden, vom Design, der Entwicklung/Programmierung über den Test bis zum Betrieb der Webanwendung.		Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Google App Engine
IaaS (Infrastructure as a Service)	Infrastruktur-Ressourcen wie Rechner-Hardware, Massenspeicher und Netzwerke werden zur Verfügung gestellt. Der Kunde erstellt seine „virtuellen“ Rechner und Rechnernetze und installiert darauf seine eigenen Betriebssysteme und Anwendungen.		Amazon Web Services (AWS), Open Telekom Cloud, Google App Engine
EaaS/AaaS (Everything/Anything as a Service), XaaS	Alle möglichen Dienste werden als Cloud-Dienst angeboten. Auch Nischenapplikationen für eine kleine Anzahl möglicher Nutzer werden von Spezial- Cloud-Dienstleistern angeboten.		

Fog ist der englische Ausdruck für Nebel. Die Menge an kleinen und kleinsten vernetzten Geräten, sowohl Sensoren als auch Aktoren, wird laufend größer. Sie bilden den „Nebel“. Fog-Geräte können einfache Sensoren sein, die ihre Daten anderen Geräten und Servern zur Verfügung stellen. Es können Aktoren sein, die abhängig von anderen Geräten und Sensoren irgendwelche Aktionen ausführen. Fog ist die unterste Ebene des Cloud-Computing. Es können Rechner sein, die eigene Daten und Daten von anderen Geräten verarbeiten und Aktoren steuern.

Fog Computing und Edge Computing sind die logische Folge vom Internet der Dinge (IoT, Internet of Things).

Edge ist das englische Wort für Kante, Rand oder Ecke. Mit Edge-Computing ist der äußere Rand des Internets gemeint. Edge-Server sind an diesem äußeren Rand platziert und nicht, wie Cloud-Server, irgendwo im Internet.



1. Was ist richtig, was ist falsch?
 - a. Datenübertragung über Kupferleitungen und Glasfaserleitungen sind etwa gleich schnell.
 - b. Die Datenrate bei Glasfaserleitungen ist teilweise wesentlich höher als bei Kupferleitungen.
 - c. Daten breiten sich auf einer Kupferleitung mit Lichtgeschwindigkeit aus.
 - d. Broadcast-Adressierung ist ein Spezialfall von Multicast-Adressierung.
 - e. Bei Anycast ist nicht klar, welcher Rechner wirklich angesprochen wird und antwortet.
2. Diskussion in Plenum: Wie hängen die Geschwindigkeit und der Durchsatz zusammen? Ist die Geschwindigkeit einer Netzwerkleitung zu beeinflussen? Wie unterscheiden sich bei diesen Überlegungen die Straßen und die Datenleitungen?
3. Wie groß ist der gesamte Datendurchsatz, wenn eine 100-Mbit/s-Verbindung mit Vollduplex oder Halbduplex verwendet wird?
4. Sie wollen eine 1 GByte große Datei auf Ihrer Festplatte speichern.
 - a. Wie lange dauert das Speichern, wenn die Datenrate der Festplatte 150 MByte/s beträgt?
 - b. Wie lange dauert das Speichern, wenn die Datenrate der SSD-Festplatte 450 MByte/s beträgt?
 - c. Wie lange dauert das Speichern dieser Datei auf verschiedene USB-Speicher (USB 2.0: 40 Mbit/s, 3.0: 300 Mbit/s)?
5. Berechnen Sie die Signallaufzeiten bei Kupfer- und Glasfaserleitungen.
 - a. Wie lange braucht ein Bit (oder ein elektrisches Signal), wenn es über eine 1000 Meter lange Kupferleitung mit einem NVP von 0,7 übertragen wird? (Rechnen Sie mit einer Vakuum-Lichtgeschwindigkeit c_0 von $3 \cdot 10^8$ m/s)

Formeln allgemein:	$c = c_0 \cdot NVP$	$c = \frac{s}{t}$
t =		

- [illegible]

- | | | |
|-----|--|--------------------------|
| bfw | ITG / C
Clients im Rechnernetzwerk
einbinden | Unternehmen für Bildung. |
|-----|--|--------------------------|

Port	Anwendung	Beispiel, Erläuterungen
80	Webdienste	Browser, Webserver
1194		
	SSH	
		Genaue Uhrzeit im Internet abrufen
		Webdienst über http, gesicherte Verbindung
		FTP-Datenübertragung
		FTP-Steuerkommandos
631		
	IMAP	
80		
		Email von einem Server abrufen mit POP3
143		

15. Was ist richtig, was ist falsch?
- Cloud-Computing ist eine aktuelle Modeerscheinung und wird in Kürze wieder verschwunden sein.
 - IaaS bedeutet beim Cloud-Computing, dass eigene Hardware bei einem Cloud-Betreiber in dessen Rechenzentrum aufgestellt wird.
 - Dienste einer Private Cloud können Privatpersonen nutzen.
 - Fog und Cloud sind zwei verschiedene Begriffe für dasselbe.
16. Erstellen Sie eine Liste mit möglichen Services, die Sie als Cloud-Dienste kennen, und solche, die Sie sich als Cloud-Dienste vorstellen können.
17. Erarbeiten Sie die grundlegenden Anwendungsfälle für Cloud-Computing. In vielen Fällen ist das Auslagern von IT oder zugehöriger Teilaufgaben in eine Cloud sinnvoll. Geben Sie an, bei welchen Anwendungen es besser oder sinnvoller ist, eine Cloud-Lösung einzurichten, anstatt Rechenleistung und Ressourcen im eigenen Datacenter vorzuhalten?

Anwendungsfall	Cloud oder eigener Serverdienst (mit Begründung)
Das tägliche Datenvolumen wächst und der Fileserver kommt bald an seine Grenzen.	
Durch eine Werbeaktion wird in den nächsten vier Wochen eine hohe Zahl an Zugriffen aus dem Internet erwartet.	
Virtuelle Server sollen lastabhängig hoch- und heruntergefahren werden.	
Die Internetanbindung eines Datacenters ist im Regelbetrieb ausreichend. Zu Stoßzeiten ist der Datendurchsatz aber zu gering.	
Es werden sensitive Daten verarbeitet, die auf keinen Fall über das Internet übertragen werden sollen.	
Es werden sensitive Daten verarbeitet, die im Geltungsbereich des deutschen Datenschutzrechtes gespeichert werden müssen.	

TAG 6, TAG 7 und TAG 8- Netzwerkstrukturen, -komponenten, -standards und -modelle unterscheiden

Sie erhalten einen Überblick über die Strukturen im Netzwerk. Sie lernen die Komponenten kennen und unterscheiden die wichtigsten Standards, die in Netzwerken angewendet werden.

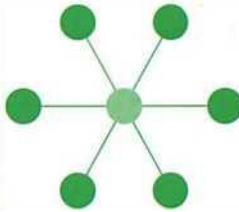
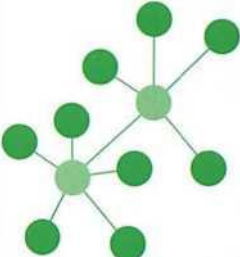
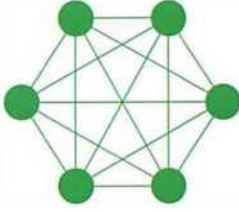
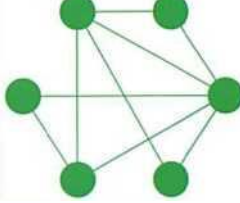
Man verschafft sich am einfachsten einen Überblick über das Netzwerk, wenn man das Netzwerk besichtigt. Dabei können Sie an Ihrem Arbeitsplatz beginnen und Netzwerk-Anschlussdosen, Leitungen und die Verteilerschränke suchen.

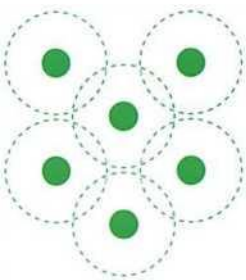
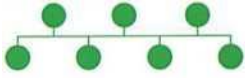
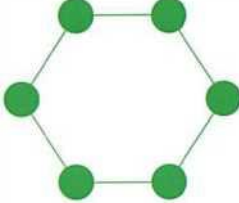
LE 1- Netzwerktopologien unterscheiden

Sie wollen wissen, welche Netzwerktopologien es gibt und welche heute gebräuchlich sind.

Topologie

Unter Topologie versteht man in der Netzwerktechnik die Art und Weise, wie Leitungen physisch verlegt werden. Topologie ist die „Landkarte“ des Netzes.

Netzwerktopologien		
Stern (Star)	Von einem Sternmittelpunkt aus gehen sternförmig die Leitungen zu den Endpunkten. → Zugriffssteuerung CSMA/CD	
Erweiterter Stern (Extended Star)	Der Endpunkt eines Sterns ist wiederum Mittelpunkt eines weiteren Sterns; üblich sind bei LANs drei Ebenen. Standard in heutigen Verkabelungen!	
Vollständige Masche (Complete Mesh)	Jede Station ist mit jeder anderen verbunden; sehr hohe Ausfallsicherheit durch sehr hohe Redundanz, aber sehr aufwendig.	
Unvollständige Masche (Incomplete Mesh)	Alle wichtigen Stationen sind mehrfach mit anderen Stationen verbunden; ausfallsichere Netze durch Redundanz; erweiterter Stern mit Querverbindungen ergibt unvollständige Masche.	

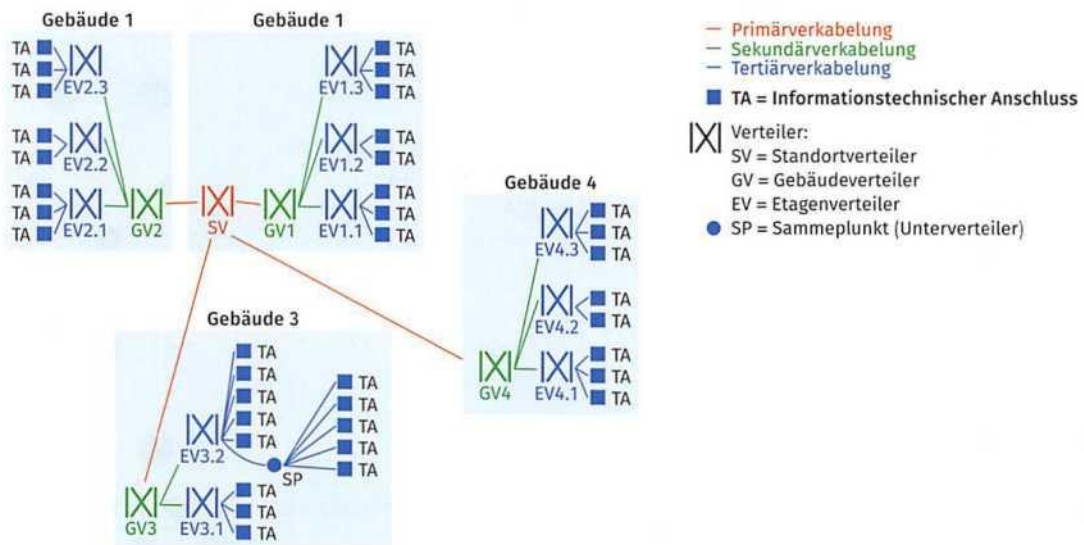
Netzwerktopologien		
Zelle (Cell)	Funkzellen decken bestimmte Bereiche mit Funkwellen ab, z. B. WLAN, Bluetooth, Mobilfunk. → Zugriffssteuerung CSMA/CA	
Punkt-Zu-Punkt (Point-to-point, P2P)	Verbindung von nur zwei Stationen.	
Bus	Alle Stationen sind parallel auf einer gemeinsamen Leitung. In LANs nicht mehr üblich. → Zugriffssteuerung CSMA/CD	
Ring	Jede Station hat eine Vorgängerstation und eine Nachfolgerstation. Daten werden nur in einer Richtung verschickt; Vorteil: sichere Datenübertragung, berechenbare Wartezeit, bis gesendet werden darf; Nachteil: etwas schwieriger Aufbau und schwierige Fehlersuche. → Zugriffssteuerung über Token Passing	

LE 2 - Strukturierte Verkabelung herstellen

Sie sollen wissen, wie eine strukturierte Verkabelung aufgebaut ist.

Eine universelle Gebäudeverkabelung, auch universelle Kommunikationsverkabelung oder strukturierte Verkabelung genannt, gliedert sich in drei Bereiche. Nach jahrzehntelangem „Wildwuchs“ bei der Telefonverkabelung in großen Gebäuden von Unternehmen, Behörden, Hotels oder Krankenhäusern hat man gelernt, dass man dies bei der Netzwerkverkabelung besser machen muss. Klare Strukturen helfen, sich in einer Verkabelung zurechtzufinden. Des Weiteren ist aufgefallen, dass mehrere Verkabelungen (z.B. Telefon, Feuer-/Rauchmelder, Rundfunk/Fernsehen) teilweise deckungsgleich übereinanderliegen. Also ist es sinnvoll, mehrere Leitungsdienste zusammenzulegen.

Schematischer Verkabelungsplan eines Betriebsgeländes

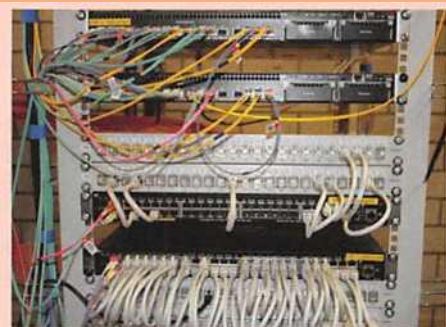


Heraus kam eine Norm zur „strukturierten dienstneutralen Gebäudeverkabelung“, die universelle Gebäudeverkabelung (UGV). Das heißt, über eine einzige Verkabelung wird telefoniert, ferngesehen, werden Daten ausgetauscht. Diese Verkabelung ist in mehreren Normen festgelegt: der EU-Norm EN 50173, ISO/ IEC 11801 und der US-Norm TIA 568A/B.

Kommunikationskabelanlage

Primärverkabelung (erste Verkabelungsebene, auch Flächenverkabelung genannt)

Im Zentrum befindet sich der Standortverteiler (SV). Von hier aus gehen sternförmig die Leitungen in alle anderen Gebäude auf dem Betriebsgelände. Sie enden am Gebäudeverteiler (GV) eines jeden Gebäudes. Hier werden zumeist Lichtwellenleiter verwendet, da diese einen hohen Datendurchsatz aufweisen und größere Distanzen überbrückt werden können.



Standortverteiler (SV)

Sekundärverkabelung (zweite Verkabelungsebene, auch Vertikalverkabelung oder Steigleitungsbereich genannt)

Ausgehend vom Gebäudeverteiler eines jeden Gebäudes gehen sternförmig die Leitungen in alle Stockwerke oder Gebäudeteile einer Ebene. Sie enden jeweils am Etagenverteiler (EV). Hier werden meist Lichtwellenleiter und Kupferleitungen verwendet.



Gebäudeverteiler mit Etagenverteiler

Tertiärverkabelung (dritte Verkabelungsebene, Horizontalverkabelung genannt)

Ausgehend von jedem Etagenverteiler EV gehen die Leitungen sternförmig in alle Zimmer der Etage und enden dort am

informationstechnischen Anschluss (TA), also der Wanddose. Hier werden zumeist Kupferleitung verwendet. In Fällen, bei denen ein sehr hoher Datendurchsatz erforderlich ist, kann auch Lichtwellenleiter bis zum Endgerät verwendet werden (FTTD, Fibre to the Desk). Faustformel: Pro 1 000 m² Fläche wird ein Etagenverteiler verwendet. Es können auch mehrere Etagen an einen Etagenverteiler angeschlossen werden, wenn wenige

informationstechnische Anschlüsse anzuschließen sind.



Etagenverteiler



Netzwerk-Anschlussdose, TA

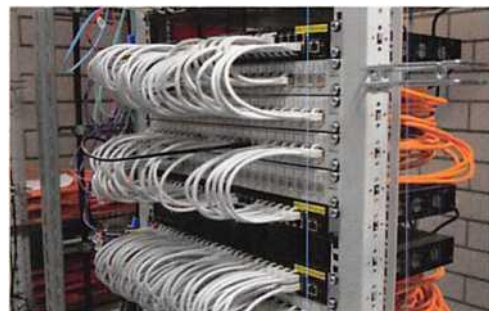
Dieses Verkabelungsschema beschreibt die passive Verkabelung eines Netzes, also nicht die aktiven Komponenten. Switches, Router usw. zählen nicht zur Verkabelung. Diese Bauteile werden in die Verteilerschränke eingebaut und bei Bedarf auch ersetzt. Sie zählen nicht zur Verkabelung. Insgesamt ergibt sich also die Gesamttopologie als erweiterter Stern (Extended Star) über drei Ebenen.

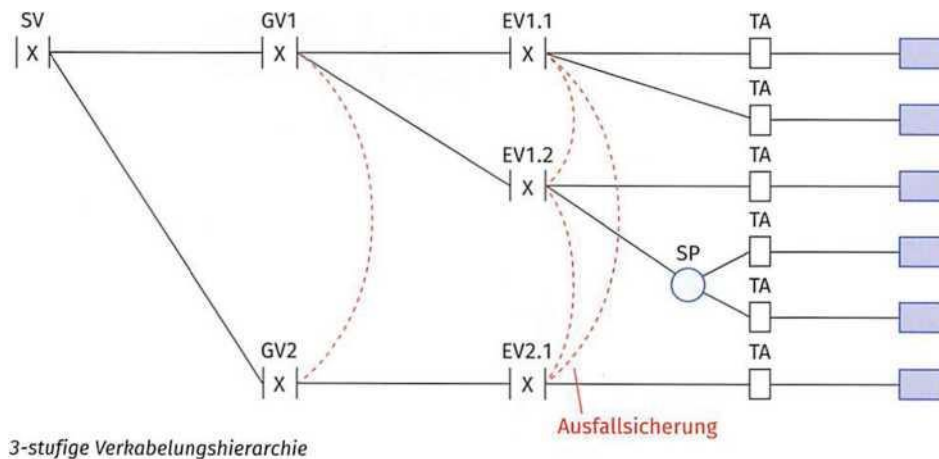
Als Ausfallsicherung werden zusätzlich Querverbindungen auf derselben Ebene eingebaut. Sowohl Gebäude als auch Etagen werden untereinander zusätzlich verbunden. Als Gesamttopologie ergibt sich damit eine unvollständige Masche (Incomplete Mesh), da jeder Verteiler mehrfach angefahren wird.

Die meisten Verteiler sind 19-Zoll-Schränke. Darin sind Patchpanels verbaut. An jeder Buchse eines Patchpanels endet eine Leitung. Die 19-Zoll-Verteilerschränke bieten genügend Platz, um die aktiven Komponenten fürs Netzwerk, aber auch Telefonanlagen und andere Geräte unterzubringen.

Mit Patch-Schnüren wird die Verbindung von einem Switchport (oder Router) auf eine Netzwerkdose hergestellt. Dieses Verbinden von Anschlüssen nennt man rangieren oder „patchen“.

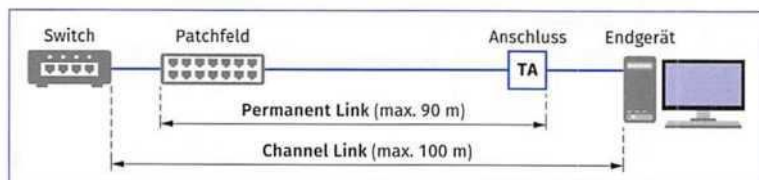
Unterverteiler sind nach Norm nicht vorgesehen. Eine Ausnahme ist laut Norm erlaubt: Auf der dritten Ebene darf ein informationstechnischer Anschluss (TA) als Sammelpunkt fungieren. An diesen werden dann innerhalb des Raumes weitere informationstechnische Anschlüsse angeschlossen. Dies wird gemacht, wenn beispielsweise in einem Schulungsraum sehr viele Rechner stehen und man nicht für jeden Rechner eine Leitung zum Etagenverteiler verlegen möchte. Dann wird der Raum nur mit wenigen informationstechnischen Anschlüssen angefahren.





Die Festverkabelung zwischen Verteiler-Patchfeld und informationstechnischem Anschluss (TA) wird Permanent Link genannt. Die gesamte Strecke vom Switch bis zum Endgerät nennt man Channel Link. Dieser umfasst auch die Anschlussschnüre vom Switch zum Patchfeld und von der Anschlussdose (TA) zum Endgerät. Die Leitungslänge für den Channel Link darf 100 m nicht überschreiten. Die maximale Leitungslänge für den Permanent Link ist mit 90 m definiert.

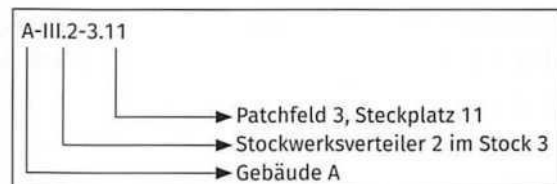
In kleinen bis normal großen Zimmern sind die Dosen meist an der Wand installiert. In Großraumbüros werden die Anschlüsse im Boden versenkt (sog. Bodentanks).



Doppel- oder Dreifachdosen sind Einfachdosen vorzuziehen, da der Installationsaufwand geringer ist.

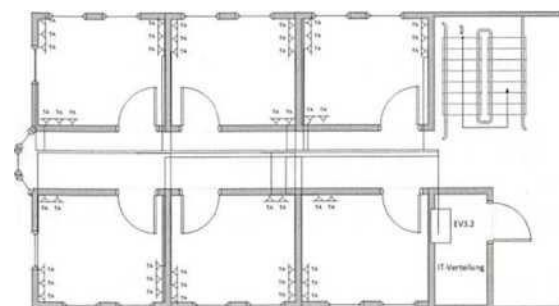
(1) Beschriftung von Dosen und Verteilern

Um sich in einer Verkabelung zurechtzufinden, ist eine Dokumentation notwendig. Dazu zeichnet man in Lagepläne der Gebäude möglichst genau die Lage der Dosen, der Leitungen und Verteiler ein.



Je nach Größe des Unternehmens bzw. des Betriebsgeländes werden alle Gebäude eindeutig gekennzeichnet. Oft nimmt man dazu Buchstaben. Die Stockwerke in jedem Gebäude werden auch eindeutig gekennzeichnet. Am besten beginnt man mit 0 im Erdgeschoss. Das erste Obergeschoss bekommt dann die Nummer 1. Dies verhindert Fehler beim Durchzählen, die entstehen können, wenn man im Erdgeschoss mit 1 beginnen würde. Sind mehrere Verteiler in einem Stockwerk vorhanden, so werden sie indiziert. III.2 bedeutet dann: dritter Stock, zweiter Verteiler. Diese Nummern werden an den Dosen angebracht. Man sieht der Dose somit an, an welchem Verteiler und an welchem Patchfeld diese Dose aufgelegt ist. Am Verteiler gibt es meist keine Kennzeichnung, wo die Dosen des Patch-Feldes enden. Hier hilft nur eine Liste mit Patchfeld bzw. Portnummer und Zimmernummer. Wenn verschiedene Leitungen bei der Installation verwendet wurden, ist es hilfreich, wenn der Leitungstyp auch vermerkt ist.

Grundrisspläne mit nummerierten Zimmern, in die Leitungen, Dosen und Verteiler eingezeichnet sind, gehören in jeden Verteiler. Ein Schnellhefter mit diesen Plänen und den Listen sollte Standard sein.



Netzwerk-Dokumentation Verteiler A-III		
Patchpanel-Nr. und Port-Nr.	Leitungstyp	Zimmer
3.1	CAT6	12
3.2	CAT6	12
3.3	CAT5e	12
3.4	CAT5e	12
3.5	CAT6a	13
...		...

(2) Netzwerkmedien

Als Medien werden Kupferleitungen als verdrehte Adernpaare und Lichtwellenleiter verwendet. Koaxialleitungen werden nicht mehr verbaut. Genau genommen kann man Funkwellen wie beispielsweise von Bluetooth und WLAN auch als Medium bezeichnen. Funkwellen benötigen keine Leitung, sie breiten sich frei im Raum aus (siehe hierzu auch Kapitel 3.7.2).

(3) Komponentenkategorien und Verkabelungsklassen

Netzwerkkomponenten (Leitungen, Dosen, Patchpanels) sind in Kategorien eingeteilt. Je nach Kategorie lassen sich unterschiedliche Datenübertragungsraten realisieren. Die Kategorie bestimmt die Bandbreite des Signals, welches übertragen werden kann. Je höher die übertragbare Frequenz, desto höher die Datendurchsatzrate.

Netzwerkkategorien und Klassen			
Kategorie (nach ISO/IEC)	Bandbreite	Verkabelungsklasse (nach ISO/IEC)	Einsatzgebiete
Kategorie 5	bis 100 MHz	Klasse D	für Datenraten bis 100 Mbit/s
Kategorie 5e	bis 100 MHz	Klasse D	für Datenraten bis 1 Gbit/s
Kategorie 6	bis 250 MHz	Klasse E	für Datenraten bis 10 Gbit/s
Kategorie 6 _A	bis 500 MHz	Klasse E _A	für Datenraten bis 10 Gbit/s
Kategorie 7	bis 600 MHz	Klasse F	für Multimedia-Anwendungen
Kategorie 7 _A	bis 1 000 MHz	Klasse F _A	für Multimedia-Anwendungen
Kategorie 8	bis 2 000 MHz	Klasse G	25 GBase-T und 40 GBase-T

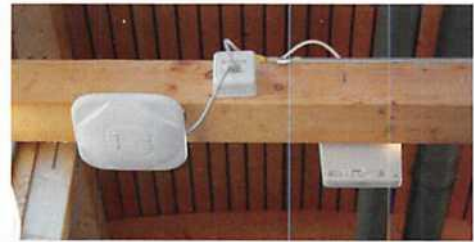
Um die Qualität einer Verkabelung qualitativ zu bestimmen, wird jede einzelne Leitung nach Fertigstellung der Verkabelung vermessen. Netzwerkverkabelungen werden in Klassen eingetragen. Damit wird gewährleistet, dass die gewünschten Übertragungsraten auch realisierbar sind. Auch wenn nur Bauteile der für eine Klasse erforderlichen Kategorie verwendet werden, kann es sein, dass durch schlampige und fehlerhafte Verarbeitung/Verlegung die gewünschte Netzwerkkategorie nicht erreicht wird.

(4) Funk, elektromagnetische Wellen

Der Tertiärbereich einer strukturierten Verkabelung stellt „die letzten Meter“ zum Anschluss eines Endgerätes dar. Funktechnik verwendet zwar keine Leitungen, aber sie wird hier ebenso zum Anschluss für Endgeräte verwendet.

Funknetze, in Deutschland Wireless LAN (WLAN) genannt, sind heute allgegenwärtig. In anderen Ländern nennt sich diese Technik Wi-Fi. WLAN-Access-Points werden an Informationstechnische Anschlüsse angeschlossen. Sie verlängern dadurch die Teritiärverkabelung.

In fast jedem Haus befindet sich ein WLAN-Zugangspunkt. Mit WLAN sind Übertragungsraten von einigen Mbit/s bis zu knapp 1 Gbit/s möglich. Allerdings teilen sich die Teilnehmer die zur Verfügung stehende Bandbreite, sodass der Datendurchsatz mit steigender Zahl der Teilnehmer merklich zurückgeht.



WLAN-Access-Point und DECT-Basisstation mit PoE-Stromversorgung

(5) Gängige Netzwerkbezeichnungen

Gängige Netzwerkbezeichnungen sind althergebracht. Sie haben die Form 10 Base-X, wobei die vordere Zahl die Datenrate in Mbit/s angibt. Base steht für Basisband und bedeutet, dass keine Trägerfrequenzen wie beim Rundfunk verwendet werden. Oft wird dieses „Base“ auch nur mit B abgekürzt. Alles was in der Bezeichnung danach folgt, bezeichnet den Leitungstyp und ist nicht einheitlich. In der folgenden Tabelle sind die wichtigsten Bezeichnungen und deren Charakteristiken aufgelistet.

Ethernet-Bezeichnungen			
Bezeichnung	Datenrate C	Leitungstyp	Max. Segmentlänge/ Bemerkungen
10Base5	10 Mbit/s	Koax RG8 (Yellow Cable)	500 m (nicht mehr gebräuchlich)
10Base2	10 Mbit/s	Koax RG58 (Thin Ethernet)	185 m (nicht mehr gebräuchlich)
10Base-T	10 Mbit/s	Twisted Pair KAT3	100 m (nicht mehr gebräuchlich)
100Base-T (Fast Ethernet)	100 Mbit/s	Twisted Pair KAT5	100 m
100Base-T1	100 Mbit/s	Twisted Pair ungeschirmt	15 m (40 m; IoT, Industrie 4.0, Kfz)
100Base-FX	100 Mbit/s	LWL Monomode	400 m
1000Base-T (Gigabit-Ethernet)	1 Gbit/s	Twisted Pair KAT5e	100 m
1000Base-T1	1 Gbit/s	Twisted Pair geschirmt	15 m (40 m; IoT, Industrie 4.0, Kfz)
1000Base-SX 1000Base-LX 1 GbitE (Gigabit-Ethernet)	1 Gbit/s	LWL	bis 550 m
10GbaseT 10 GbitE	W Gbit/s	Twisted Pair KAT7	100 m

Ethernet-Bezeichnungen			
Bezeichnung	Datenrate C	Leitungstyp	Max. Segmentlänge/ Bemerkungen
10GBaseFX 10 GbitE	W Gbit/s	LWL	bis 100 m
40GBaseCR4 40 GbitE	40 Gbit/s	Kupfer-Twinax	10 m
40GBaseSR4 40 GbitE	40 Gbit/s	Multimode-LWL mit 4 Kanälen	100 m
40GBaseLR4 40 GbitE	40 Gbit/s	Singlemode-LWL mit 4 Kanälen	10 km
100GBaseCRW 100 GbitE	100 Gbit/s	Kupfer-Twinax	10 m
100GBaseSRW 100 GbitE	100 Gbit/s	Multimode-LWL mit W Kanälen	100 m
100GBaseLRW 100 GbitE	100 Gbit/s	Singlemode-LWL mit W Kanälen	10 km
100GBaseER4 100 GbitE	100 Gbit/s	Singlemode-LWL mit 4 Kanälen	40 km

Die alten Leitungen mit 10 Mbit/s mit Twisted Pair findet man vereinzelt noch in alten Verkabelungen. Diese genügen aber unseren heutigen Ansprüchen nicht mehr. Koaxialleitungen sind so gut wie verschwunden und durch TP-Leitungen ersetzt worden. Neu sind die äußerst schnellen Verbindungen mit 40 Gbit/s und 100 Gbit/s. Sie werden vereinzelt schon eingesetzt, allerdings überwiegend in Rechenzentren und nicht in der Fläche.

Zwei weitere Neuerungen sind die 100Base-T1 und 1GBase-T1 Normen mit Datenraten von 100 Mbit/s und 1 000 Mbit/s. Dabei handelt es sich um Verbindungen über ein einziges verdrehtes Adernpaar. Die langsamere Variante benutzt ein ungeschirmtes Paar, die schnelle ein Paar mit Abschirmung. Diese ist eine Entwicklung aus der Kfz-Technik, da dort künftig große Datenmengen erzeugt und verarbeitet werden müssen. Diese Technik lässt sich dann auch in der Gebäudeautomation (Stichwort „Smart Home“) einsetzen.

LE 3 - Netzwerkmedien unterscheiden und spezifizieren

Sie sollen Netzwerkmedien kennen und unterscheiden können.

Netzwerkmedien						
leitungsgebunden				nicht leitungsgebunden		
Elektrische Signale (Kupferleitung)		Optische Signale (Lichtwellenleiter)		Funkübertragung		Optische Übertragung
Twisted-Pair-Leitung	Koaxial-Leitung	Multi-mode-Faser	Single-mode-Faser	WLAN/ Wi-Fi	Richtfunk	Laserlink

(1) Kupferleitungen

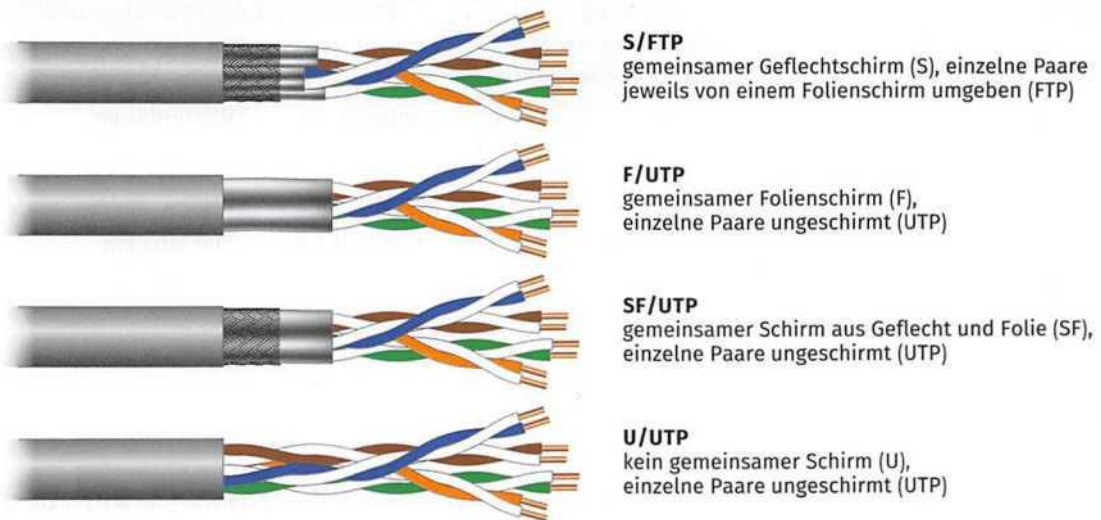
Kupferleitungen bestehen aus verdrehten Adernpaaren (Twisted Pairs). Gelegentlich findet man auch noch die alte Bezeichnung „Doppelader“. Jede Kupferrader ist mit einem Plastikmantel isoliert. Es gibt große Unterschiede im Leitungsaufbau. Dementsprechend gibt es auch unterschiedliche Qualitäten. Ein Standard-Netzwerkkabel hat vier Adernpaare. Übliche Drahtdurchmesser sind AWG22 bis AWG24 (American Wire Gauge).

Amerikanisches Drahtmaß	Aderndurchmesser in mm
AWG 22	0,644
AWG 23	0,572
AWG 24	0,511

Ein weiterer wichtiger Unterschied besteht in der Schirmung. Beim aufwendigsten Kabelaufbau werden die Adernpaare einzeln mit einer Schirmfolie eingewickelt. Dies kann eine dünne Metallfolie sein oder auch nur eine metallbeschichtete Plastikfolie. Um den Verbund von allen vier geschirmten Paaren wird noch ein gemeinsamer Schirm als Drahtgeflecht gelegt. Der einfachste Kabelaufbau enthält nur die vier Adernpaare ohne jegliche Abschirmung.

Das Verdrehen der Adernpaare verhindert das Aussenden von magnetischer Störstrahlung beim Betrieb der Leitung. Ebenso heben sich die Störungen bei von außen eingestrahlt Störungen gegenseitig auf.

Kupferdatenleitungen (Twisted Pair) werden nach dem Aufbau des Kabelschirmes unterschieden:



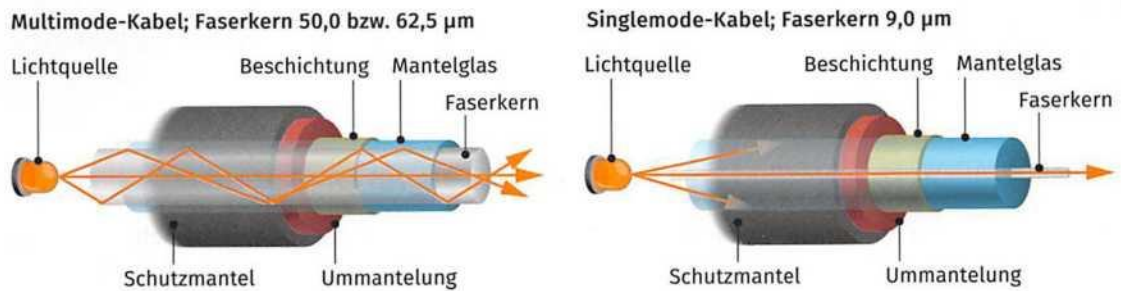
Leitungstypen (Kupfer)

Das Umwickeln mit einer leitfähigen Folie oder Schirmgeflecht (Abschirmung) verhindert das Aussenden von elektrischer Störstrahlung und verhindert ebenso, dass sich die Leitung durch äußere E-Felder stören lässt.

(2) Lichtwellenleiter

Lichtwellenleiter werden zuallermeist aus Glas hergestellt, die Glasfasern. Durch ihre geringe Dämpfung lassen sich sehr große Distanzen überbrücken. Für kurze Distanzen werden gelegentlich auch Kunststofffasern eingesetzt, die polymeroptischen Fasern (POF). Das Funktionsprinzip der Lichtwellenleiter ist die Totalreflexion. Ein in einen Faserkern längs eingespeister Lichtstrahl wird an der Grenzschicht von Kern zum Mantel vollständig reflektiert.

Es werden zwei Typen von Glasfasern unterschieden:



Multimode-Fasern haben einen Kerndurchmesser von 50 µm oder 62,5 µm. Das Licht kann in verschiedenen Winkeln durch die Faser wandern, was Laufzeitprobleme verursacht und die Länge der Faserstrecke begrenzt. Dieser Grenzwert wird als „modale Bandbreite“ oder „Bandbreiten-Längenprodukt“ bezeichnet.

Multimode-Fasern werden in fünf verschiedene Leistungsklassen eingeteilt: OM1 bis OM5. Singlemode-Fasern werden in zwei Klassen eingeteilt: OS1 und OS2.

Die Singlemode-Fasern haben einen relativ kleinen Kerndurchmesser von ca. 9 µm. Das Licht nimmt immer den „geraden“ Weg im Faserkern. Laufzeitprobleme gibt es daher nicht. Nur die Dämpfung begrenzt die Länge der Faserstrecke. Weitverkehrsleitungen sind immer Singlemode-Fasern.

Fasertyp	Faser-Kennzeichnungsfarbe	Fasertyp (Kerndurchmesser/Faserdurchmesser in µm)	Minimale modale Bandbreite B' in MHz • km	
			850 nm Wellenlänge	1 300 nm Wellenlänge
OM1	Orange	50/125 oder 62,5/125	200 MHz km	500 MHz km
OM2	Orange	50/125	500 MHz km	500 MHz km
OM3	Aqua	50/125	1 500 MHz km	500 MHz km
OM4	Violett	50/125	3500 MHz km	500 MHz km
OM5	Lime	50/125	3500 MHz km	500 MHz km
OS1	Gelb	9/125	-	-
OS2	Gelb	9/125	-	-

Rechenbeispiel: Eine Multimode-Faser OM2 mit einem Bandbreitenlängenprodukt von 500 MHz • km soll verlegt werden. Die Gesamtlänge der verlegten Faser beträgt 2,5 km. Die übertragbare Bandbreite beträgt dann

$$B = \frac{B'}{L} = \frac{500 \text{ MHz} \cdot \text{km}}{2,5 \text{ km}} = 200 \text{ MHz}$$

Maximale Dämpfungswerte von Standardfasern			
Dämpfung	Wellenlänge		
	850 nm	1 300 nm	1 550 nm
OM1.OM2	3,5 dB/km	1,5 dB/km	-
OM3, OM4, OM5	3,0 dB/km	1,5 dB/km	-

Maximale Dämpfungswerte von Standardfasern			
Dämpfung	Wellenlänge		
	850 nm	1 300 nm	1 550 nm
OM1	-	1,0 dB/km	1,0 dB/km
OM2	-	0,4 dB/km	0,4 dB/km

AT&T, NEC und Corning stellten im Mai 2009 einen neuen Weltrekord auf. Auf einer einzelnen Glasfaser übertrugen sie über eine Entfernung von 580 km auf 320 Kanälen mit einer Einzel-Datenübertragungsrate von 114 Gigabit pro Sekunde und erzielten so eine Gesamt-Datenübertragungsrate von 32 Terabit pro Sekunde.

(3) Funk, WLAN/Wi-Fi

Funknetzwerke basieren auf elektromagnetischer Strahlung in unterschiedlichen Frequenzbereichen. Im Weitverkehrsbereich werden Funknetze als Richtfunkstrecken eingesetzt, wenn keine Kupferleitungen verfügbar sind.

Funknetzwerke

Wireless LAN, WLAN, Wi-Fi, IEEE 802.11

Zwei Betriebsarten sind möglich:

- Ad-hoc-Netz, „Sofort-Netz“, bei dem sich zwei oder mehrere Netzteilnehmer gleichberechtigt in einem Netzwerk miteinander verbinden
- Infrastructure, Mobilgeräte verbinden sich mit einem zentralen Punkt, dem Access Point. Anmeldung am Access Point oder einem Anmeldeserver erforderlich.

Mehrere Normen mit zwei verschiedenen Frequenzbereichen und unterschiedlichen Datendurchsatzraten existieren:

Norm-Bezeichn.	Neue Bezeichn.	Bemerkungen
802.11		5-GHz-Band, bis 11 Mbit/s
802.11a		5-GHz-Band, bis 54 Mbit/s
802.11b		2,4-GHz-Band, bis 11 Mbit/s
802.11g		2,4-GHz-Band, bis 54 Mbit/s
802.11h		5-GHz-Band, bis 54 Mbit/s, Erweiterung des 802.11a-Standards für Europa mit erhöhter Sendeleistung
802.11 n	Wi-Fi 4	2,4-GHz- und 5 GHz-Band, bis 150 Mbit/s (Standard)
802.11ac	Wi-Fi 5	2,4-GHz- und 5 GHz-Band, bis 867 Mbit/s, theoretisch bis 6936 Mbit/s
802.11ad	Wi-Fi 6	60-GHz-Band, „Gigabit-WLAN“, bis 6 930 Mbit/s,

Wireless PAN, WPAN

Wireless PAN, genormt in 802.15, Einsatzzweck ist das Abschaffen von Leitungen und Kabelgewirr, z. B. an Maus, Keyboard oder Kopfhörer. Mehrere Technologien sind verfügbar:

Bluetooth	2,4 GHz-Band	Bemerkungen
ZigBee	868 MHz, 915 MHz und 2,4 GHz	Wird häufig in der Heim-Automatisierung eingesetzt, z.B. intelligente Lampen und Schalter, Tür-/Fensterkontakte.
NFC	13,5 MHz	Datenübertragung über wenige Zentimeter, z.B. Bezahlen mit Smartphone, Daten austauschen/übertragen zwischen zwei Smartphones, Zugangskontrolle, smarte Plakate.

Wireless WAN, WWAN

Zum drahtlosen Weitverkehrsnetz zählen alle Mobilfunkstandards (GMS, GPRS, LTE, UMTS, 5G) und Richtfunkstrecken der Telekommunikationsunternehmen.

LE 4 - Netzwerkkomponenten unterscheiden

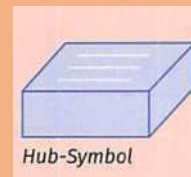
Sie sollen die üblichen Netzwerkgeräte kennen und unterscheiden können.

Netzwerkgeräte sind aktive Geräte, die in den Verteilern eingesetzt werden und Netzwerkleitungen verbinden. Sie gehören nicht zur Verkabelung. Zur strukturierten Verkabelung gehören Leitungen, Anschlussdosen (TAs) und die Patchfelder in den Verteilern. Also passive Komponenten. Heute übliche Netzwerkgeräte sind Switch und Router. Zum besseren Verständnis, werden in der Tabelle aber auch die älteren, nicht mehr gebräuchlichen, Geräte erklärt.

Netzwerkgeräte

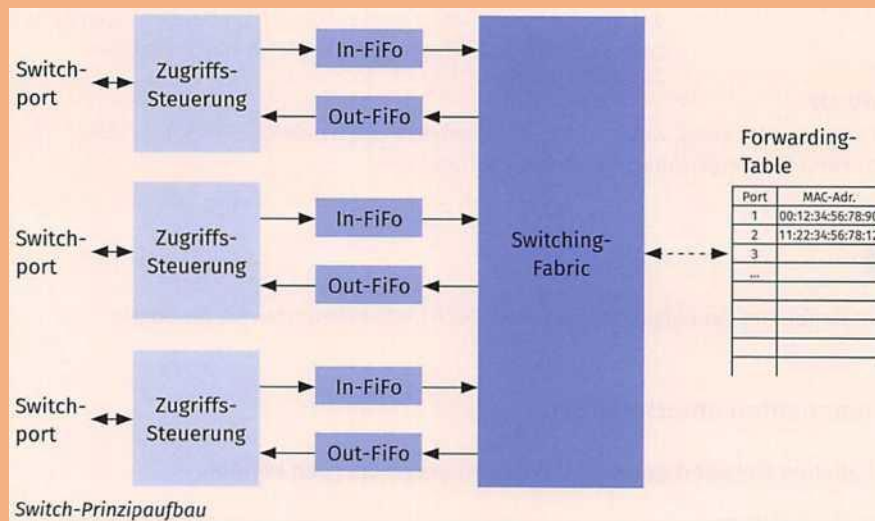
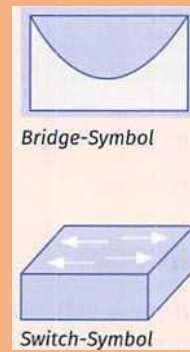
Repeater und Hub

Ein Hub ist ein bidirektionaler Verstärker. Er verstärkt die Signale. Aus einem schwachen Signal wird wieder ein Signal mit vollem Pegel hergestellt. Er arbeitet auf OSI-Layer 1, der Bitübertragungsschicht oder Physical Layer. Ein Hub mit nur zwei Anschlüssen ist ein Repeater. Hubs wurden in Sternverkabelungen eingesetzt. In der Mitte, im Sternmittelpunkt, befindet sich der Hub. Da von diesem die Leitungen sternförmig nach außen gehen, so wie die Speichen eines Rades, nennt man dieses Bauteil Hub (Nabe). Repeater oder Hub werten keine Adressen aus. Sie arbeiten auf OSI-Layer 1.



Bridge und Switch

Die Netzwerkbrücke (Bridge) verbindet zwei Netzsegmente. Jedes Netzsegment kann mehrere Geräte mit jeweils eigener Hardware-Adresse (MAC- Adresse = Media-Access-Control-Adresse) enthalten. Sie leitet ankommende Pakete nur weiter, wenn sich der Zielrechner an dem anderen Bridge Port befindet. Dadurch wird unnötiger Netzwerkverkehr herausgefiltert. Eine Bridge „lernt“ nach dem Einschalten, welche MAC-Adressen sich an welchem Port befinden, und bildet eine Weiterleitungstabelle (Bridge Table). Mehrere Brücken in einem Gerät ergeben eine Multiport Bridge, den Switch. Der Switch ist das wichtigste aktive Bauteil eines zeitgemäßen Rechnernetzes. Ein Switch „lernt“, welche Knoten an welchem seiner Anschlüsse angeschlossen sind. Er baut daraus seine Weiterleitungstabelle (Forwarding Table). Man nennt diese Tabelle auch Switching Table oder Bridge Table. Ankommende Datenpakete werden auf OSI-Layer 2 inspiziert und die im Header befindlichen MAC-Adressen ausgelesen. Neue Absender-MAC-Adressen werden in die Weiterleitungstabelle eingetragen. Bei ankommenden Paketen werden die Ziel-MAC-Adressen gelesen und mit der Weiterleitungstabelle verglichen. Findet sich ein Anschluss, an dem sich der Knoten mit dieser Adresse befindet, dann wird das Datagramm an diesem Anschluss weitergeschickt. Ein Switch arbeitet auf OSI-Layer 2.



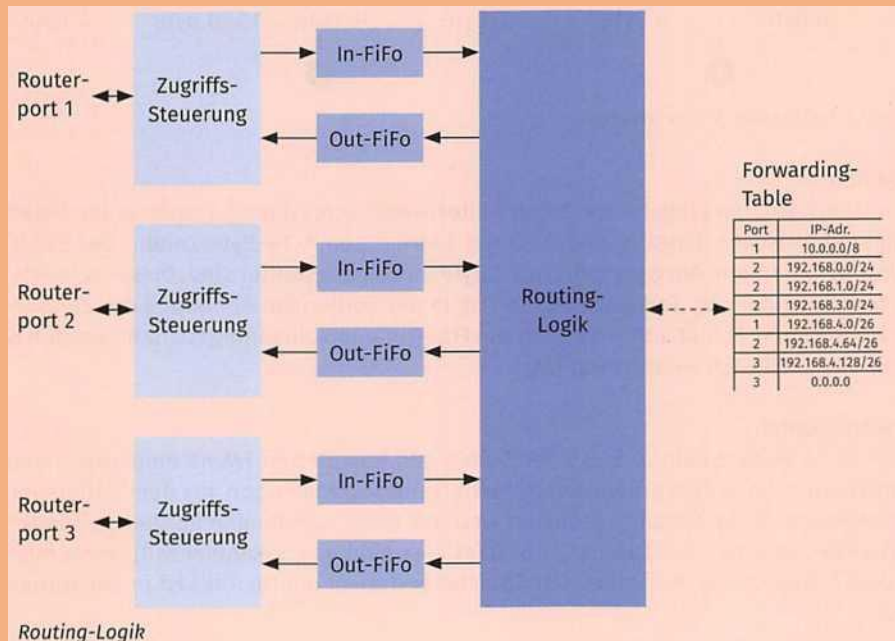
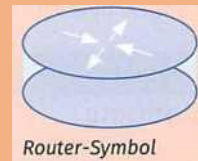
Jeder Switchport verfügt über einen Eingangspuffer, den Input-FIFO. FIFO bedeutet First In - First Out. Die Daten, die zuerst hineingeschoben werden, werden hinten auch zuerst wieder herausgeschoben. Ebenso hat jeder Switchport einen Ausgangspuffer, in dem die Daten auf das Senden warten. Zwischen den beiden Pufferspeichern und dem Anschluss befindet sich die Zugriffssteuerung. Diese sorgt dafür, dass keine Datenkollisionen auftreten, wenn beispielsweise gesendet werden soll, während Daten hereinkommen. Die Switching Fabric sorgt für das Weiterleiten von empfangenen Daten an den entsprechenden Ausgangsport. Sie greift dazu auf die Forwarding Table zu.

Je nach angeschlossenem Gerät kann ein Switchport die Datenübertragungsrate entsprechend einstellen. Beispielsweise kann an einem Port ein Gerät mit 10 Gbit/s kommunizieren und an einem anderen Port mit 10 Mbit/s. Die Fabric funktioniert wie ein sehr schnelles internes Netzwerk. Die Daten landen in Hochgeschwindigkeit im Ausgangspuffer des Ausgangsports. Schickt nun ein Gerät seine Daten mit hoher Übertragungsrate an ein Gerät mit geringerer Datenrate, dann landen diese Daten zwar sehr schnell im Ausgangspuffer des Ausgangsports. Von dort werden sie dann aber mit der geringeren Datenrate gesendet.

Fehler können auftreten, wenn sehr schnell viele Daten an einem Port ankommen und der Pufferspeicher überläuft. Sowohl der Eingangs- als auch der Ausgangs-FIFO-Speicher können überlaufen. Es gibt keine Datenflusssteuerung. Wenn ein Puffer voll ist, dann gehen alle weiteren Daten, die in den Puffer geschoben werden, verloren. Diese Fehler müssen von den Endgeräten behoben werden. Switches sind nur für das Weiterleiten zuständig.

Router

Ein Router verbindet zwei oder mehrere Netze miteinander. Dazu wertet er den Netzwerk-Anteil der IP-Adresse aus. Router verfügen über Routing-Tabellen, Weiterleitungstabellen, in denen nicht einzelne Adressen hinterlegt sind, sondern ganze Adressbereiche, die Netzkennungen. Für jeden einzelnen Routerport werden die darüber erreichbaren Netzwerke hinterlegt.



Große Netzwerke können durch Subnetting in kleinere Netze unterteilt werden. Ein Router kann damit auch ein großes Netz in mehrere kleine Subnetze aufteilen. Router werten die Netzwerk-Adressen auf **OSI-Layer 3** aus. Im LAN sind dies die IP-Adressen.

WLAN-Access-Point, Wi-Fi-Access-Point, Hotspot

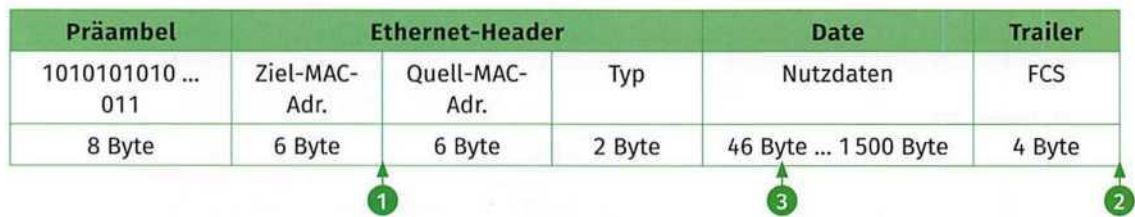
Ein Access Point bildet den Mittelpunkt einer Funkzelle, die mit dem LAN verbunden ist. Mobilgeräte (z.B. Laptops, Smartphones) können sich mit dieser Funkzelle verbinden und sind somit Teil des lokalen Netzwerkes.



(1) Switchtypen

Ein Switch, der Daten empfängt, muss diese an demjenigen Anschluss wieder ausgeben, an dem sich der Zielrechner befindet. Es stellt sich die Fragen, zu welchem Zeitpunkt dies geschieht. Dazu muss man zunächst den Aufbau eines Ethernet-Datenpaketes betrachten. Die zu übertragenden Nutzdaten werden in den Ethernet-Frame (= Rahmen) zwischen Header und Trailer eingebettet. Als erstes wird die Präambel gesendet (Synchronisierungsbits ohne Informationsgehalt). Im Anschluss daran kommt der Ethernet-Header. Dann folgen die Nutzdaten. Am Ende wird eine Rahmenprüfsumme übertragen (FCS = Frame Check Sequence). Die Verweildauer der Daten im Switch wird als Latenzzeit bezeichnet. Sie sollte möglichst kurz sein.

Die ersten 6 Bytes im Header sind die Ziel-MAC-Adresse.



Ethernet-Frame und Durchschaltzeitpunkte von Switches

Cut-Through-Switch

Der frühestmögliche Zeitpunkt, um eingehende Daten weiterzuschicken, ist nach Empfang der Zieladresse. Die Verzögerungszeit zwischen Eingang und Ausgang beträgt somit 14-Byte-Zeiten. Der Speicherbedarf ist sehr gering, da bei freiem Ausgangsport nur 6 Byte im Eingangspuffer sind. Dieser schnelle und verzögerungsarme Switch ist der sog. Fast Forward Switch, in der vorherigen Abbildung der Zeitpunkt 1. Wenn während der Übertragung Fehler auftreten oder ein Frame gar unvollständig ist, dann werden diese Frames trotzdem mit diesem Switch weitergeschickt.

Store-and-Forward-Switch

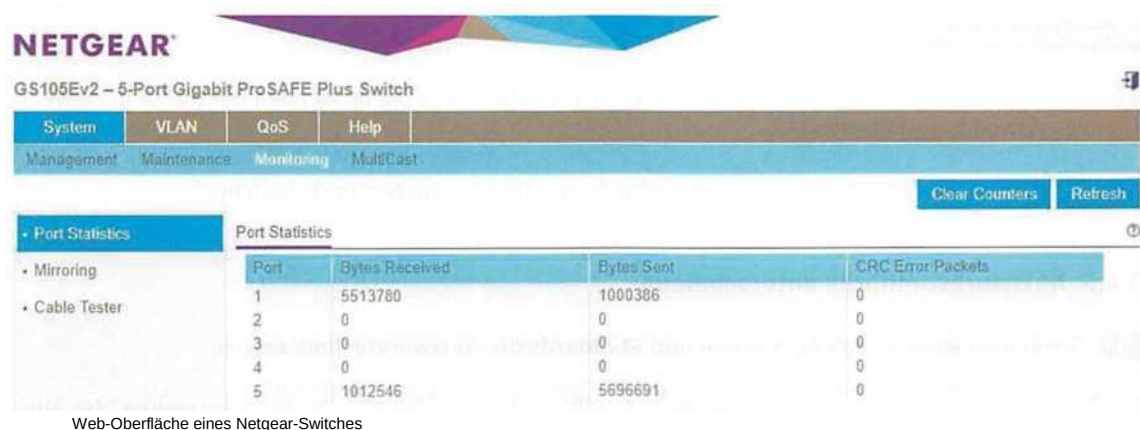
Um nur fehlerfreie Frames weiterzuleiten, muss der Switch den kompletten Frame empfangen und am Ende die Rahmenprüfsumme (FCS) überprüfen. Fehlerhafte Frames werden dann aus dem Pufferspeicher gelöscht und nicht weitergeschickt. Dadurch reduziert sich das Datenaufkommen auf den Leitungen, da defekte Frames aussortiert werden. Die Latenzzeit beträgt hier eine ganze Rahmenzeit, somit maximal 1 518-Byte-Zeiten plus 8-Byte-Zeiten Präambel. Der Speicherbedarf ist enorm. Dies ist in der vorherigen Abbildung der Typ 2.

Fast-Forward-Switch oder auch Fragment-free-Switch

Diese beiden obigen Typen sind die beiden Extreme. Es hat sich gezeigt, dass abgebrochene Frames sehr kurz sind. Es kommt sehr selten vor, dass ein Frame kurz vor Ende der Übertragung abbricht, meist wird am Anfang abgebrochen. Der Mittelweg ist nun, dass ein Switch den Anfang der Datenübertragung abwartet und erst dann schaltet. Dies ist in vorherigen Abbildung der Typ 3. Dieser Typ schaltet nach 64 empfangenen Bytes durch. Er hat somit eine geringe Latenzzeit und wenig Speicherbedarf.

(2) Managebare Switches

Einfache Switches sind Plug and Play („einstecken und abspielen“). Sie sind preiswert und für einfache Heimnetze und Kleinunternehmen ausreichend. Bessere und teurere Switches verfügen über Konfigurationsmöglichkeiten. Sie sind managebar. Dazu verfügen sie meist über eine Web-Oberfläche. Von einem PC im selben Netz kann man einen solchen Switch konfigurieren. Grundvoraussetzung, um ein Gerät im Netzwerk ansprechen zu können, ist, dass das Gerät über eine IP-Adresse verfügt. Über die Web-Oberfläche kann man jeden einzelnen Port ein- und ausschalten und individuell die Datenübertragungsraten festlegen. Auch lassen sich Statistiken über die Verkehrsaufkommen an jedem Port erstellen. Auch ist es bei einigen Typen möglich, sog. Mirrorports einzurichten. Datenverkehr auf ausgesuchten Ports kann auf die Mirrorports gespiegelt werden. Dort können dann Analysetools wie Wireshark-Rechner (für Netzwerkprotokollanalyse) oder Intrusion-Detection-Systeme (IDS) zum Aufspüren von Eindringlingen angeschlossen werden.



(3) Die Arbeitsweise von Routern verstehen

Unter Routing versteht man das Weiterleiten von Datenpaketen von einem Netzwerk in ein anderes, das Finden eines Pfades für die Daten von einem Rechner zu einem anderen. Dabei wird die Netzadresse (OSI-Layer 3) ausgewertet.

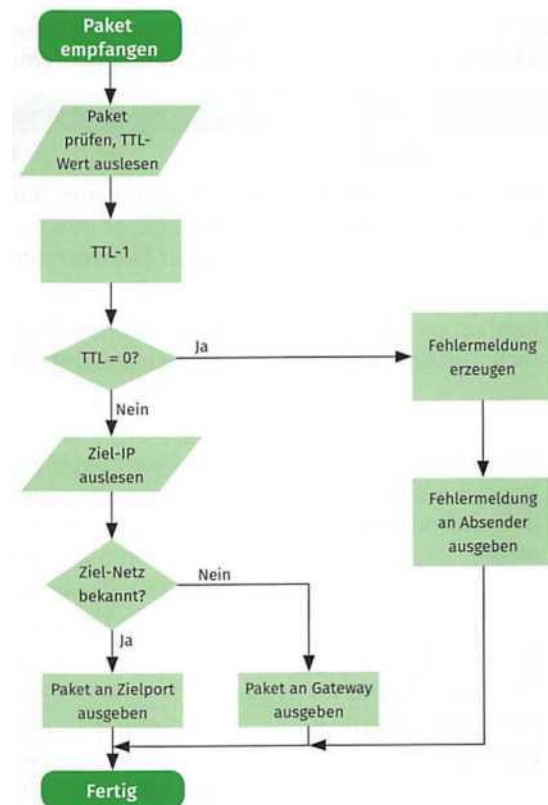
Ein Router verbindet somit mehrere Netzwerke. Zu jedem Routerport ist eine Tabelle der Netzkennungen hinterlegt, die über diesen Anschluss erreichbar sind. Subnetze werden wie separate Netze betrachtet. Ein Router kann mehrere Subnetze zu einem größeren Netzwerk zusammenfassen (siehe Fachstufenband, Lernfeld 9).

Jedes ankommende Datenpaket wird geprüft und dabei die Adresse des Zielrechners und der Wert des Feldes TTL (Time to Life) ausgelesen. Das TTL-Feld ist ein 8-Bit-Wert und wird um eins dekrementiert. Wenn das Ergebnis null ist, dann wird das Paket verworfen und eine Fehlermeldung „Ziel nicht erreichbar“ zurückgeschickt.

Im Normalfall wird in der Weiterleitungstabelle (Routing Table) nachgesehen, ob bekannt ist, über welchen Port das Zielnetz erreichbar ist. Hier wird dann das Paket wieder ausgegeben. Ist das Zielnetz nicht in der Routing Table enthalten, wird das Paket an das Default Gateway des Routers weitergeschickt.

Ein kleiner Heim-Router hat zwei Anschlüsse: einen internen LAN-Port und den externen Internet-Port. Die Weiterleitungstabelle sieht folgendermaßen aus:

Routerport	Netzwerkadressbereich	Bemerkungen
LAN	192.168.1.0/24	Internes Netzwerk
WLAN	192.168.2.0/24	Internes Funknetz
WAN	0.0.0.0	Alle anderen Netze (Internet)



LE 5 - Netzwerkstandards unterscheiden

Sie wollen wissen, welche Normen und Standards die Netzwerktechnik regeln.

Es gibt nicht die eine Norm für das Netzwerk. Es gibt auch nicht das eine Normungsgremium, das alles regelt. Eine Reihe von Normen und Standards von mehreren nationalen und internationalen Normungsgremien und Organisationen befasst sich mit diesem Thema.

Die Tabelle zeigt die wichtigsten Normungsgremien, die sich mit der Telekommunikation und Netzwerken befassen. Oft werden Standards von einem Gremium auch noch von anderen Gremien übernommen.

Normungsgremien und Organisationen		
Name	Beschreibung	
International Organization for Standardization	Internationales Normungsgremium mit Sitz in Genf/ Schweiz; erarbeitet Normen auf allen Gebieten außer Elektrotechnik	
International Electro-technical Commission	Internationale Normungsorganisation für den Bereich Elektrotechnik/Elektronik mit Sitz in Genf/ Schweiz	
International Telecommunication Union (Internationale Fernmeldeunion)	Erarbeitet unter anderem Empfehlungen zu technischen Themen der Telekommunikation; erst durch die Übernahme dieser Empfehlungen durch nationale Regulierungsbehörden wie z. B. der Bundesnetzagentur bekommen die Empfehlungen den Charakter von Normen	
Institute of Electrical and Electronics Engineers	Weltweiter Berufsverband von Ingenieurinnen und Ingenieuren, Sitz in New York	
Internet Engineering Task Force	Die Internet-Technik-Arbeitsgruppe befasst sich mit der Weiterentwicklung des Internets und der Internet-Protokolle; Sitz ist Vermont/USA	
National Institute of Standards and Technology	Zuständig für Verschlüsselungsverfahren (AES, DES)	
American National Standards Institute	Privates Normungsinstitut mit Sitz in Washington D.C./USA	
Deutsches Institut für Normung e.V.	Nationales Normungsinstitut mit Sitz in Berlin	

Europäische Normen (EN) werden von einem der drei europäischen Komitees für Standardisierung verabschiedet:

- CEN - Europäisches Komitee für Normung,
- CENELEC - Europäisches Komitee für elektrotechnische Normung und
- ETSI - Europäisches Komitee für Telekommunikationsnormen.

Europäische Normen bestehen aus den Buchstaben EN und einer Zahl. Internationale Normen können als Europäische Normen übernommen werden.

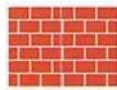
Wichtige Netzwerknormen	
IEEE 802	Netzwerkstandards auf OSI-Layer 1 und 2
IEEE 802.3	Ethernet
IEEE 802.3u	Fast Ethernet
IEEE 802.3z	Gigabit-Ethernet
IEEE 802.3ae	10-Gigabit-Ethernet
IEEE 802.3an	W-Gigabit-Ethernet mit Twisted Pair
IEEE 802.3af und IEEE 802.3at	Power over Ethernet
IEEE 802.11	Wireless LAN
IEEE 802.15.1	Wireless PAN (z.B. Bluetooth, ZigBee)
IEEE 1394	FireWire
OSI/IEC 7498-1	Open Systems Interconnection: Basic Reference Model

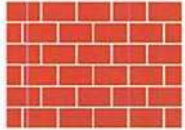
LE 6 - ISO/OSI- und TCP/IP-Modell unterscheiden

Sie sollen die beiden gängigen Netzwerkschichtensysteme verstehen.

Um komplizierte Sachverhalte zu veranschaulichen, werden oft Schichtenmodelle verwendet. Die ersten Verbindungen von Rechnern waren proprietär, d. h., dass jeder Hersteller etwas anderes gemacht hat und unterschiedliche Systeme nicht kompatibel waren. Eine Norm schaffte hier Abhilfe.

Es entstand das ISO/OSI-Schichtenmodell der Datenkommunikation (herausgegeben von der ISO). Es definiert sieben Schichten. Ganz oben befindet sich die Anwendungsschicht, auf der die Anwendung (z. B. Browser, E-Mail-Client, Warenwirtschaftssystem-Eingabefenster) läuft. Ganz unten ist die physikalische Schicht, auf der der physische Datentransport definiert wird (z.B. Strom/Spannung, Lichtsignale, Funksignale).

ISO/OSI-Schichtenmodell der Kommunikation						
Schicht-Nr.	Schichtname englisch	Schichtname deutsch	Adressen	Bemerkungen		
7	Application-Layer	Anwendungsschicht			 Firewall	 Server
6	Presentation-Layer	Darstellungsschicht		Einheitliche Darstellung der Daten		
5	Session-Layer	Sitzungsschicht		Sitzungsaufbau		

ISO/OSI-Schichtenmodell der Kommunikation					
Schicht-Nr.	Schichtname englisch	Schichtname deutsch	Adressen	Bemerkungen	Netzwerkgerät
4	Transport-Layer	Transport-schicht	Ports	Adressieren von Anwendungen	 Firewall
3	Network-Layer	Netzwerk-schicht	IP-Adressen	Adressieren von Netzen und Rechnern	 Router
2	Data-Link-Layer	Datensicherungsschicht	MAC-Adressen	Adressieren von Netzwerk-Interfaces	 Switch
1	Physical-Layer	Bit-Übertragungsschicht			 Ethernet

Parallel dazu entwickelte sich das TCP/IP-Modell mit seinen vier Schichten. Gelegentlich wird es auch DoD-Modell genannt, nach dem Department of Defense (Verteidigungsministerium der USA), das diese Entwicklung als Auftraggeber anfangs finanzierte.

TCP/IP-Modell				
Schicht-Nr.	Schichtname englisch	Schichtname deutsch	Adressen	Zum Adressieren von
4	Application-Layer	Anwendungsschicht		
3	Transport-Layer	Transportschicht	Ports	Anwendungen
2	Internetwork-Layer, Host- to-Host-Layer	Internetschicht	IP-Adressen	Netzen und Rechnern
1	Network-Access-Layer	Netzzugangsschicht	MAC-Adressen	Netzwerk-Interfaces

Die Funktion der einzelnen Schichten:

Application

Hier befinden sich die Anwendungsprogramme (z. B. Browser und Web-Server, E-Mail-Client und E-Mail-Server, Datenbank-Client und Datenbank-Server).

Presentation

Die Darstellung von Zahlen, Zeichen, Buchstaben wird hier vereinheitlicht, damit unterschiedliche Systeme Daten austauschen können. Die Zeichen werden immer in einem einheitlichen Format ausgetauscht.

Session

Hier bauen zwei Kommunikationspartner eine Sitzung auf, vergleichbar einem Telefongespräch, bei dem auch zu Beginn durch Nennen der Namen sichergestellt wird, dass man miteinander reden möchte.

Transport

Diese Schicht ist für den sicheren Datenaustausch verantwortlich. Hier werden die Daten überprüft, ob sie korrekt angekommen sind. Fehlen Daten oder sind sie fehlerhaft, dann werden sie auf dieser Schicht erneut angefordert. Anwendungen werden mit Ports (Port-Adressen) adressiert.

Network

Auf der Netzwerkschicht werden Netzwerke adressiert und Pakete von einem Netzwerk in ein anderes geroutet. Router arbeiten auf diesem Layer. Üblicherweise werden hier IP-Adressen verwendet. IP-Adressen beinhalten einen Netzanteil und einen Host-Anteil, sodass ein Zielrechner und sein Netz genau definiert sind.

Data Link

Beim Senden wird aus den Sendedaten ein Bit-Strom erstellt bzw. beim Empfänger werden aus einem Bit-Strom wieder die Originaldaten hergestellt. Die Bits werden in logische Einheiten zu 8 Bit (ein Oktett) zusammengefasst. MAC-Adressen befinden sich auf dieser Schicht. Mit ihnen werden die Netzwerk-Interfaces adressiert.

Physical Layer

Auf der Bit-Übertragungsschicht wird mit Leitungscodes definiert, wie Bits oder Bit-Muster auf dem Medium übertragen werden. Ein High kann beispielsweise 5 V und ein Low -5 V haben. Es können aber auch Bit-Muster (mehrere Bits gleichzeitig) in verschiedenen Spannungen dargestellt werden.

Das TCP/IP-Modell fasst nun mehrere Schichten zusammen. Daher verfügt dieses Modell nur über vier Layer. In der Realität finden wir immer das TCP/IP, teilweise mit Unterschichten ergänzt. Es ist wichtig, beide Modelle zu kennen, denn die Bezeichnung der Geräte basiert auf dem OSI-Modell.

(1) Netzwerkprotokollstapel

Beim Versenden von Daten über ein Netzwerk werden auf der Applikationsschicht Daten zum Versenden vorbereitet. Dies kann der Inhalt einer E-Mail sein, eine Anfrage des Browsers an einen Web-Server oder auch Telefonsprachdaten. Diese Nutzdaten werden im Schichtenmodell an die darunterliegende Schicht übergeben. Jede Schicht hängt vor die Daten ihren eigenen Protokollkopf (Header) und gibt das neue, größere Paket weiter nach unten. Auf der physikalischen Schicht werden diese Daten ohne weitere Veränderung in elektrische und eventuell optische Signale umgewandelt und auf dem Netzwerkmedium ausgegeben.

Layer 7	Application-Layer				App.-Header	App.-Nutzdaten	
Layer 4	Transport-Layer			TCP-Header	App.-Header	App.-Nutzdaten	
Layer 3	Internet-Layer		IP-Header	TCP-Header	App.-Header	App.-Nutzdaten	
Layer 2	Data-Link-Layer	Ethernet-H.	IP-Header	TCP-Header	App.-Header	App.-Nutzdaten	Eth.-Trailer
Layer 1	Physical-Layer	0101010101010101010101010101010101010101010101010101010101010101 ...					

Beim Versenden von Daten werden die Schichten von oben nach unten durchlaufen und Header angefügt. Die Nutzdaten werden „verkapselt“. Beim Empfangen von Daten läuft der Prozess rückwärts ab. Die empfangenen Daten werden nach oben weitergereicht bis zu derjenigen Anwendung, an die diese Daten adressiert wurde. Die Nutzdaten werden ausgepackt, die Header entfernt. Man nennt dies Entkapselung.

(2) Dienst-Protokolle

Einige Protokolle sind für das ordnungsgemäße Funktionieren eines Netzwerkes von grundlegender Wichtigkeit.

Protokoll			OSI-Layer
Abkürzung	Name	Aufgabe	
ARP	Address Resolution Protocol	Löst IP-Adresse in MAC-Adresse auf	Layer 2 und 3
DNS	Domain Name Service	Löst Domännennamen in IP-Adressen auf	Layer 3 und 7
DHCP	Dynamic Host Configuration Protocol	Verteilt die IP-Konfiguration an Rechner im Netz	Layer 3

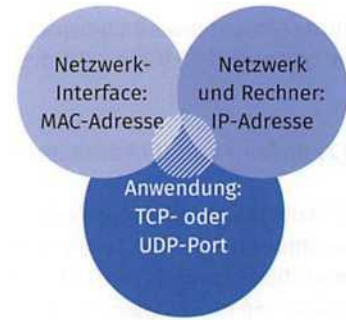
C:\Users\luri>arp -a		
Schnittstelle: 192.168.83.1 --- 0x3		
Internetadresse	Physische Adresse	Typ
192.168.83.254	00-50-56-e7-48-5e	dynamisch
192.168.83.254	ff-ff-ff-ff-ff-ff	statisch

Die Ethernet-Frames, die auf dem Netzwerkmedium übertragen werden, beinhalten die Hardware-Adressen (MAC-Adressen) vom Absender und vom Zielrechner. Switches im Netz leiten die Frames weiter bis zum Ziel. Frames werden nur innerhalb eines Netzes direkt zugestellt. Daten, die für einen externen Rechner bestimmt sind, werden an das Default Gateway, den Router in andere Netze, geschickt. Um die MAC-Adresse von einem Zielrechner im Netz zu bekommen, wird das Address Resolution Protocol (ARP) eingesetzt. Wenn ein Rechner Daten versenden möchte, muss er die Interface-Adresse des Zielrechners kennen, um sie in das Adressfeld des Ethernet-Frames einzusetzen (siehe Kapitel 3.3.3). Der Rechner lernt nach und nach die Interface-Adressen und speichert sie in seinem ARP-Cache. Der Konsolenbefehl *arp-a* listet die gespeicherten Interface-Adressen auf.

LE 7 - Adressen im Netzwerk unterscheiden

Sie sollen Adressen im Netzwerk unterscheiden.

In einem Computernetz müssen einzelne Rechner, Interfaces (Netzwerkkarten) und Anwendungen auf Rechnern und Servern adressiert werden. Daher werden drei verschiedene Adressen verwendet. Ganze Netzwerke werden von Routern adressiert. Internetprotokoll-Adressen (IP-Adressen) sind zweigeteilt. Sie beinhalten die Netzkennung und die Host-Kennung.



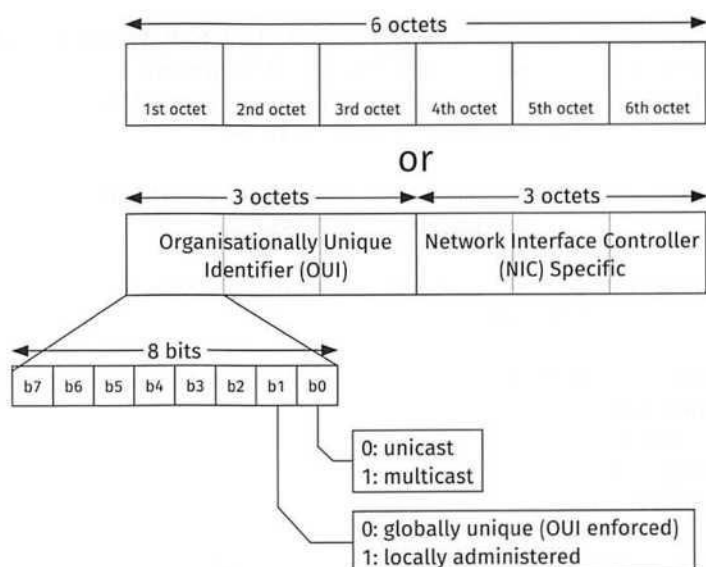
Adresse	OSI-Layer	Adressaufbau	Bemerkungen
MAC-Adresse	OSI-Layer 2	48 Bit, Schreibweise <i>hexadezimal</i> mit Trennzeichen zwischen den Bytes Beispiel: AA-BB-CC-DD-EE-FF	Jedes Netzwerk-Interface hat eine eigene, eindeutige physikalische Interface-Adresse
IP-Adresse Version 4	OSI-Layer 3	32 Bit, Schreibweise byteweise als <i>Dezimalzahl</i> mit Punkt als Trennzeichen zwischen den Bytes (Dotted Decimals) Beispiel: 10.255.0.1	Jeder Knoten im Netzwerk hat eine (oder mehrere) IP-Adresse(n).
IP-Adresse Version 6	OSI-Layer 3	128 Bit, Schreibweise: acht Wörter zu je 16 Bit in <i>hexadezimal</i> mit Doppelpunkt als Trennzeichen zwischen den Worten Beispiel: 2001:0123:5678:9ABC:DEF0:1234:5678:9ABC	Jeder Knoten im Netzwerk hat mehrere eigene, eindeutige IPv6 Adressen.
Ports	OSI-Layer 4	16 Bit, Schreibweise als <i>Dezimalzahl</i> Beispiel: 30123	Ports adressieren Applikationen, Port 80 = http, Web-Server, Browser.

(1) Aufbau von MAC-Adressen

Jedes Netzwerk-Interface hat eine eigene MAC-Adresse. MAC-Adressen bestehen aus 6 Oktetten (48 Bits). Die Adressen sind zweigeteilt in Herstellerkennung (Vendor-ID oder Organisationally Unique Identifier - OUI) und fortlaufende Nummer des Herstellers. Große Interface-Hersteller besitzen mehrere Vendor-IDs.

Die Schreibweise für MAC-Adressen ist byteweise hexadezimal, meist mit Bindestrichen oder Doppelpunkten zwischen den Bytes.

Beispiel: 24-65-11-12-5e-ce;
wobei 24-65-11 für den Hersteller AVM, Berlin, steht.



Das erste Oktett der MAC-Adresse hat zwei Bits mit besonderer Funktion: Bit 0 = Unicast- oder Multicast- Adressierung und Bit 1 geben an, ob die Adresse global oder nur im LAN einzigartig (unique) ist. Multicast-

Adressen adressieren beispielsweise alle Router im LAN oder alle Switches usw. Die MAC-Broadcast-Adresse lautet ff-ff-ff-ff-ff-ff. Mit dieser Zieladresse werden alle Interfaces im gesamten Netz angesprochen.

(2) Aufbau von IP-Adressen

IP-Adressen sind zweigeteilt in einen Netzwerkanteil und einen Host-Anteil. Um die beiden Anteile voneinander trennen zu können, benutzt man die Subnetzmaske. Dies ist vergleichbar mit einer Telefonnummer, die sich auch in ein Ortsnetz und eine Anschlussnummer aufteilt. Die Telefonnummer 0301234567890 teilen wir in Gedanken immer auf. Ein Teil ergibt das Ortsnetz Berlin 030 und der Rest ergibt die Anschlussnummer 1234567890. Dieselbe Anschlussnummer könnte auch in Hamburg vergeben sein. Allerdings würde sie sich durch den Netzanteil unterscheiden: 0401234567890. Große Netze haben kleine Netznummern und damit viele Stellen für die Anschlussnummer. Kleine Telefonnetze haben mehr Ziffern für die Netznummer, beispielsweise 0747612345678 und weniger für den Anschluss. In diesem Beispiel ist der Netzanteil 07476. Die Grenze zwischen beiden Anteilen kann man wissen - oder nicht.

Anders ist es bei den IP-Adressen. Die Subnetzmaske gibt die Grenze an zwischen Host- und Netzanteil. Eine IP-Adresse besteht aus 32 Bits. Jedes

Net-ID	Host-ID	IP-Adresse
1111'1111.1111'1111.	0000'0000.0000'0000.	Subnet-Mask

Bit kann 0 oder 1 sein. Der besseren Lesbarkeit halber werden IP-Adressen byteweise geschrieben. Jeder 8-Bit-Block wird als Dezimalzahl geschrieben und kann daher Werte von 0 bis 255 enthalten. Die Blöcke werden mit Punkten voneinander getrennt, z.B. 12.13.14.15.

Es gibt zwei Schreibweisen für die Subnetzmaske:

1. **CIDR-Schreibweise** oder Slash-Notation: Die neuere und einfachere Schreibweise gibt an, wie viele Bits der Adresse den Netzanteil darstellen. Dazu wird diese Zahl als Präfix hinter die IP-Adresse geschrieben. **12.13.14.15/16** bedeutet, dass die ersten 16 Bits der Netzanteil sind. Also ist die Netzadresse 12.13.0.0; der Hostanteil ist damit 0.0.14.15. Die Subnetzmaske gibt also die Größe des Netzwerkes an.
2. **Dotted-Decimal-Notation**: Dies ist die althergebrachte Schreibweise, die leider immer noch üblich ist. Sie wird besonders bei Microsoft-Betriebssystemen verwendet. Dabei wird die Subnetzmaske wie eine IP-Adresse geschrieben. Links stehen Einsen, rechts Nullen. Die Stellen, an denen eine Eins steht, ist eine Netzstelle. Nullen in der Subnetzmaske repräsentieren den Host-Anteil.

Das obige Beispiel in alter Schreibweise lautet: IP: 12.13.14.15, SN 255.255.0.0. Schreibt man beides als Binärzahl auf, wird schnell klar, wie das funktioniert:

IP: 0000 1100.0000 1101 . 0000 1110.0000 1111
(Binärschreibweise von 12.13.14.15)

SN: 1111 1111.1111 1111. 0000 0000.0000 0000
(Binärschreibweise von 255.255.0.0)

Netz: 0000 1100.0000 1101. 0000 0000.0000 0000
→ Netzadresse = 12.13.0.0

Die Einsen der IP-Adresse lässt man stehen, wenn die Subnetzmaske eine Eins hat. Gängige Subnetzmasken sind:

255.0.0.0 oder /8
255.255.0.0 oder /16
255.255.255.0 oder /24

Diese Standard-Subnetzmasken stammen aus der Einteilung der IP-Adressen in Klassen (siehe Tabelle, S. 62). Es sind aber auch andere Subnetzmasken möglich. Man kann diese Grenze

von 1 auf 0 bitweise nach rechts verschieben. Dadurch verkleinert sich der Hostanteil und es entstehen Subnetze im ursprünglichen Netz.

IP: 0000 1100.0000 1101 . 0000 1110.0000 1111
(Binärschreibweise von 12.13.14.15)

SN: 1111 1111 . 1111 1100.0000 0000.0000 0000
(Binärschreibweise von 255.252.0.0 oder /14)

Netz: 0000 1100.0000 1100.0000 0000.0000 0000
→ Netzadresse = 12.12.0.0

Die Größe eines Netzes kann man einfach aus der Anzahl der Netz-Bits ableiten. 32 Bit hat die IP-Adresse insgesamt. Bei einem /16-Netz bleiben $32 - 16 = 16$ Host-Bits übrig. Also sind 2^{16} Host-Adressen möglich. Bei einem /14-Netz (wie oben) sind $32 - 14 = 18$ Host-Bits übrig. Das ergibt somit ein vierfach größeres Netz mit 2^{18} Hostadressen.

(3) Einteilen der IP-Adressen in Adressklassen (historisch)

Einteilung in IP-Adressklassen (historisch)				
Klasse	Adressbereich (N = Netz-Bits, H = Host-Bits)	Subnetzmaske (CIDR-Schreibw.)	Anzahl N	Bemerkungen
A	0.0.1.0 bis 127.255.255.255 IP: 0 NNN'NNNN.HHHH'HHHH.HHHH'HHHH. HHHH'HHHH SN: 1111'1111.0000'0000.0000'0000.0000'0000	255.0.0.0 /8	8	Ursprünglich für Netze von Großkonzernen
B	128.0.0.0 bis 191.255.255.255 IP: 10 NN'NNNN.NNNN'NNNN.HHHH'HHHH. HHHH'HHHH SN: 1111'1111.1111'1111.0000'0000.0000'0000	255.255.0.0 /16	16	Ursprünglich für Netze von Konzernen
C	192.0.0.0 bis 223.255.255.255 IP: 110 N'NNNN.NNNN'NNNN. NNNN'NNNN. HHHH'HHHH SN: 1111'1111.1111'1111.1111'1111.0000'0000	255.255.255.0 /24	24	Ursprünglich für Netze von kleinen Unternehmen
D	224.0.0.0 bis 239.255.255.255 IP: 1110 'XXXX.XXXX'XXXX. XXXX'XXXX. XXXX'XXXX	-		Multicast-Adressen
E	240.0.0.0 bis 255.255.255.255 IP: 1111 'XXXX.XXXX'XXXX. XXXX'XXXX. XXXX'XXXX	-		Reserviert für Forschungszwecke

Die ersten 4 Bit einer Adresse geben die Adressklasse an (in der Tabelle fett gedruckt).

(4) IP-Spezialadressen

Bezeichnung	Adresse	Beschreibung
Localhost oder Loopback	IP 127.0.0.0/8	Adresse auf sich selbst; ein Ping auf eine Adresse aus diesem Bereich spricht den eigenen Rechner an.
Net-ID	Alle Host-Bits sind 0.	Net-ID von 10.1.2.3 /8 ist 10.0.0.0
Host-ID	Alle Net-Bits sind 0.	Host-ID von 10.1.2.3 /8 ist 0.1.2.3
Broadcast-ID	Alle Host-Bits sind 1.	Sendung „an alle in diesem Netz“ Broadcast-ID von 10.1.2.3 /8 ist 10.255.255.255

(5) Private IP-Adressbereiche

Private IP-Adressbereiche					
Klasse	Adressbereich	Subnetzmaske	Anzahl Host-Bits	Anzahl Hosts pro (Sub-)Netz	Anzahl vordefinierte Subnetze
Class A	10.0.0.0 bis 10.255.255.255	255.0.0.0	24	2^{24}	0
Class B	172.16.0.0 bis 172.31.255.255	255.255.0.0	16	2^{16}	16
Class C	192.168.0.0 bis 192.168.255.255	255.255.255.0	8	2^8	255

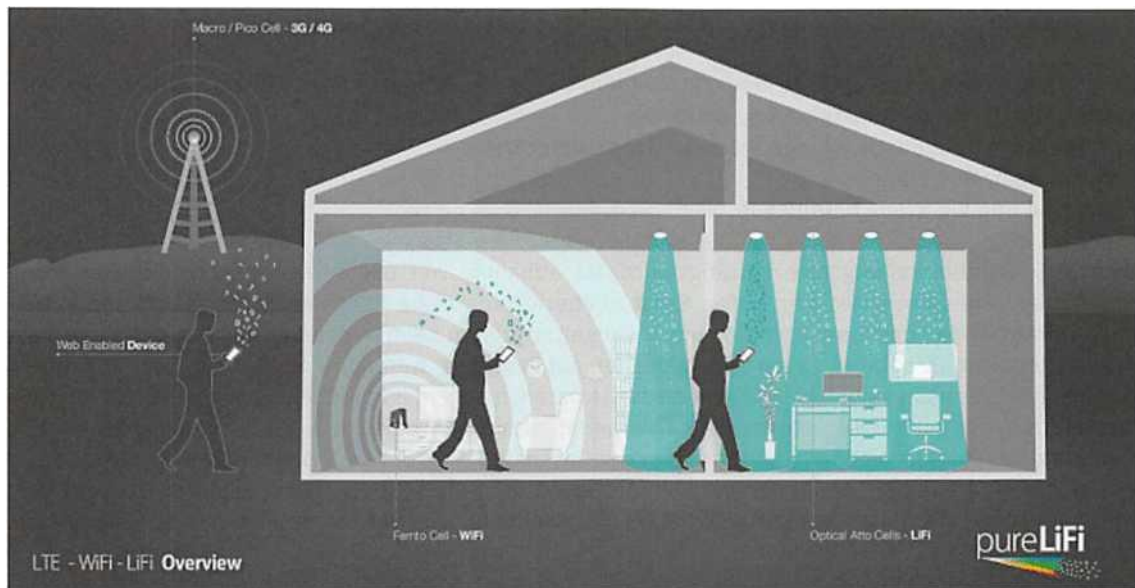
IP-Adressen aus einem privaten Adressbereich werden in LANs verwendet. Sie können in größeren LANs mit internen Subnetzen auch intern geroutet werden. Im Internet werden Pakete mit privaten IP-Adressen jedoch nicht geroutet. Die Pakete werden verworfen.

Private IP-Adressen werden im Internet nicht geroutet.

LE 8 - Neue Entwicklungen der Netzwerktechnik präsentieren

Sie sollen sich laufend informieren, was sich auf dem Gebiet der IT tut. Neue Entwicklungen können in Zukunft große Verbreitung finden.

Light Fidelity, kurz LiFi, könnte eine Nachfolgetechnologie oder Ergänzung für Funknetze werden. Dabei wird Licht als Träger der Information verwendet. Normale Beleuchtungskörper können als zusätzliche Licht-Hotspots oder Access Points fungieren. Leuchtdioden werden sehr schnell ein- und ausgeschaltet und erzeugen so den Datenstrom. Diese Technik verspricht eine sehr hohe Datenrate, die wesentlich über der Rate von WLANs liegt. LiFi können 100-mal mehr Daten transportieren als Wi-Fi (WLAN). Zudem lässt sich Licht sehr einfach abschirmen und ist in der Reichweite auf den Nahbereich beschränkt, was bei WLAN nicht der Fall ist. Dies ist in Sachen Sicherheit von großem Vorteil.



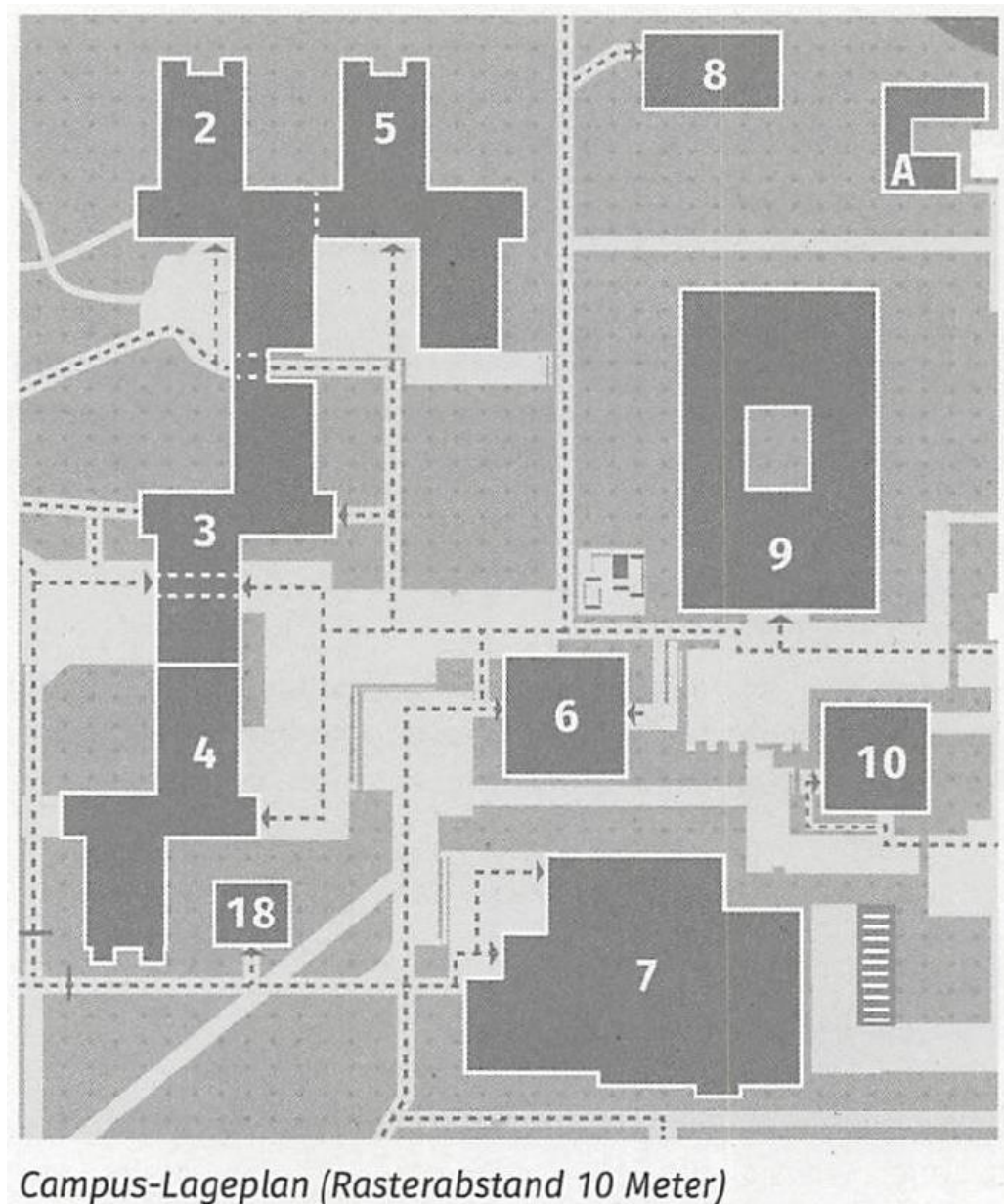
Lernzielkontrollen TAG 6, TAG 7 und TAG 8

1. Was ist richtig, was ist falsch?
 - a. Der Ring ist die vorherrschende Topologie im LAN.
 - b. Die Fehlersuche ist bei der Bus-Topologie besonders leicht.
 - c. Aus Gründen der Ausfallsicherheit ist eine Maschentopologie am besten.
 - d. Die Fehlersuche ist bei der Sterntopologie besonders leicht.
 - e. Bus-Verkabelungen trifft man in bestehenden Verkabelungen an.
 - f. In Zellnetzen ist die Fehlersuche sehr einfach.
 - g. Der Stern ist die vorherrschende Topologie im LAN.
2. Nennen Sie die drei häufigsten Netzwerktopologien, skizzieren Sie kurz deren Aufbau und beschreiben Sie, was diese Topologie auszeichnet. Überlegen Sie dabei auch, wie sich die Fehlersuche gestaltet und wie der Leitungsverbrauch ist.

Topologie	Skizze	Beschreibung

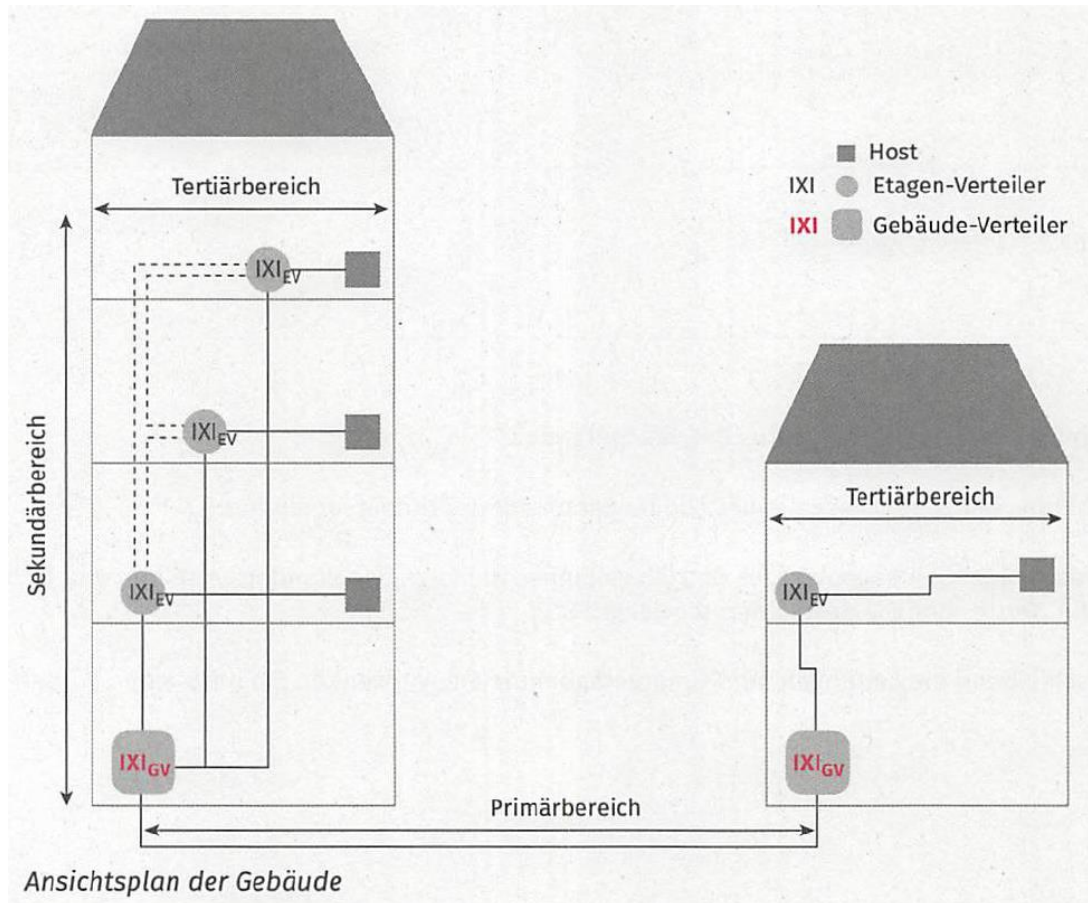
3. Was ist richtig, was ist falsch?
 - a. Durch Querverbindungen der Verteiler in einer strukturierten Verkabelung ergibt sich eine unvollständige Masche.
 - b. Der Permanent-Link einer LAN-Verkabelung darf maximal 100 m betragen.
 - c. Eine strukturierte Netzwerkverkabelung ist selbsterklärend und braucht keine weitere Dokumentation.
 - d. Eine bestehende Netzwerkdokumentation wird nach Beendigung der Arbeiten aktualisiert.
 - e. Die Netzwerkdokumentation gehört dem Ersteller und darf nicht beim Kunden gelassen werden.
4. Wie verhält sich eine Verkabelung von Patchfeld über Leitungen bis zur Anschlussdose, wenn jeweils ein Bauteil der Kategorie 5, 6 und 7 verwendet wird?
5. Eine neue Netzwerkverkabelung wurde fertiggestellt und ohne Beanstandungen abgenommen. Als ein Büromitarbeiter in ein anderes Büro umzieht, macht er die Patch-Verbindung im Etagenverteiler selbst. Später beklagt er sich, in seinem neuen Büro sei „das Netzwerk zu langsam“, weitaus langsamer als im alten Büro. Was kann die Ursache sein?

6. Wie lange darf der Permanent Link einer Netzwerkverkabelung und der Channel Link sein?
7. Planen Sie die Verkabelung eines Betriebsgeländes. Sie beginnen mit der Primärverkabelung.
 - a. Zeichnen Sie in den folgenden Lageplan des Betriebsgeländes die Lage des Standortverteilers und der Gebäudeverteiler ein. Verwenden Sie dazu einen schwarzen Stift.
 - b. Zeichnen Sie anschließend die Leitungen der Primärverkabelung ein. Verwenden Sie dazu einen Rotstift.
 - c. Verwenden Sie aktuelle Standardkomponenten und begründen Sie, warum sie was eingesetzt haben.

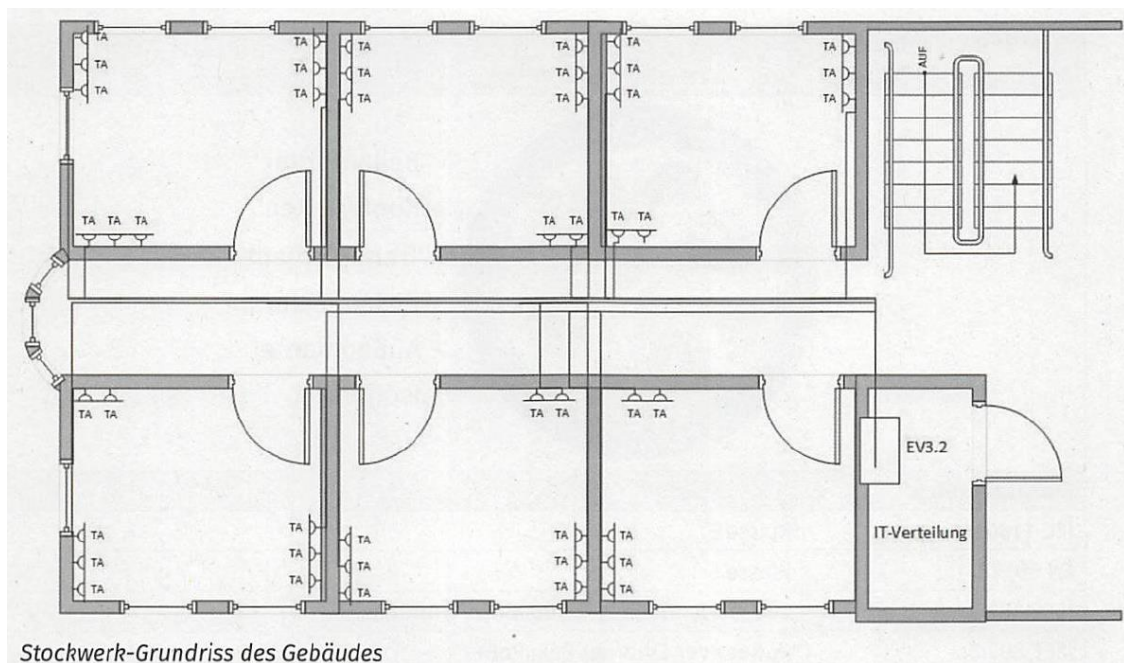


- d. Begründen Sie die Standorte.
- e. Welche Leitungen verwenden Sie? Begründen Sie Ihre Wahl.

- f. Zeichnen Sie mit grüner Farbe die Sekundärverkabelung exemplarisch für ein Gebäude in den Ansichtsplan ein.



8. Zeichnen Sie mit blauer Farbe die Tertiärverkabelung exemplarisch für ein Stockwerk in den Ansichtsplan ein. Ergänzen Sie weitere Anschlüsse.



9. Welche der Leitungen ist für welchen Anwendungsfall am besten geeignet? (Siehe die folgenden Datenblätter)

Anwendung	Leitungstyp	Begründung
Anschluss einer Grafik-Workstation		
Anschluss einer Webcam mit Stromversorgung über das Netzwerk		
Anschluss für einen PC-Arbeitsplatz und IP-Telefon		

10. Welche Beziehung besteht zwischen dem Aderndurchmesser und der Bezeichnung AWG (American Wire Gauge)?

11. Suchen Sie für die dargestellten Anwendungsfälle die passenden Geräte aus den Datenblättern. Für welche Anwendung wird welches Netzwerkgeräte benutzt? Ordnen Sie die Geräte aus der Liste den Anwendungen.

- Einfacher 8-Port-Switch 1Gb/s
- Managebarer 8-Port-Switch 1 Gb/s
- Managebarer 16-Port-Switch 1 Gb/s mit PoE-Speisung auf 8 Ports
- Router mit DSL-Modem und WLAN-Access-Point, Ethernet-Router mit 8 Ethernet-Ports

Anwendungen für Netzwerkgeräte	
In einem Kleinbetrieb werden im Büro zwei weitere PCs benötigt.	
In einem größeren Betrieb wird das Firmen-LAN in Subnetze aufgeteilt. Jedes Gebäude bekommt ein eigenes Subnetz.	
In einer Bank werden die Sicherheitsvorkehrungen verschärft. Das LAN wird in kleinere VLANs für die verschiedenen Arbeitsgruppen aufgeteilt.	

12. Beschreiben Sie die Funktionsweise von Switch und Router mit eigenen Worten. Beachten Sie dabei insbesondere die auszuwertenden Adressen in Bezug auf das ISO/OSI-Schichtenmodell.
13. Beschreiben Sie das Verfahren, welches eingesetzt wird, um Kollisionen auf dem Netzwerkmedium zu handhaben.
14. Beschreiben Sie die Hauptunterschiede zwischen Switch und Router.

15. Verbinden Sie die Netzwerkstandards mit dem dazugehörigen Datenraten (Mehrfachnennungen möglich). Siehe auch Übersichtstabelle im Modul.

Bezeichnung/Standard	Datenrate
10BaseT	10 Mb/s
10GBE	100 Mb/s
40GBE	1 Gb/s
100BaseT	2,5 Gb/s
802.3u (Fast Ethernet)	5 Gb/s
100GBE	10 Gb/s
1000BaseT-1	25 Gb/s
1GBE	40 Gb/s
100GBaseLR10	100 Gb/s
802.3ae	
100Base-T1	
250GBE	
802.3z	
10Base-2	

16. Auf welcher OSI-Schicht arbeiten Switches, auf welcher Router?

17. Stellen Sie die beiden Standardmodelle der Netzwerkkommunikation einander gegenüber. Setzen Sie die folgenden Begriffe in die passenden freien Stellen der Tabelle ein:

Switch – Transport-Layer – Hub – Router – IP-Adresse – MAC-Adresse – Port-Nr. – Network-Layer – Network-Access-Layer – Host-to-Host-Layer – Transport-Layer – Data-Link-Layer – Presentation-Layer

OSI-Layer Nr.	ISO/OSI-Modell Bezeichnung der Schicht	TCP-Layer Nr.	TCP/IP-Modell Bezeichnung der Schicht	Netzwerkgerät	Adressen
7	Application L.	4	Application L.		
6					
5	Session L.				
4		3			
3		2	Host-to-Host L.		
2		1			
1	Physical L.				

18. Welches Protokoll (Abkürzung und ausgeschriebene Bezeichnung) ist für das Übersetzen von sprechenden Internetnamen (URLs) in IP-Adressen zuständig?

19. Welches Protokoll (Abkürzung und ausgeschriebene Bezeichnung) liefert zu einer IP-Adresse die MAC-Adresse des Netzwerk-Interfaces?

20. Welches Protokoll (Abkürzung und ausgeschriebene Bezeichnung) ermöglicht die automatische Konfiguration der IP-Einstellungen eines Rechners?

21. Wahr oder falsch?

- Jedes Interface muss eine eigene MAC-Adresse haben.
- Jeder Rechner darf nur eine MAC-Adresse haben.
- Ein Rechner bezieht nach dem Einschalten seine MAC-Adresse von einem Server.
- MAC-Adressen haben 32 Bit.
- IP-Adressen haben 32 Bit.
- IP-Adressen haben 128 Bit.
- Der linke Teil einer IP-Adresse ist die Netzwerk-Adresse.
- Bei einer IP-Broadcast-Adresse werden alle Host-Bits auf Eins gesetzt.

22. Was ist richtig, was ist falsch in Bezug auf IP-Adressen?

- 1.2.3.4 ist eine korrekte IP-Adresse.
- 10.20.30.40. ist eine korrekte IP-Adresse.
- 10.200.300.400. ist eine korrekte IP-Adresse.
- Netzanteil der IP 10.20.30.40 / 16 ist 10.20.0.0.
- Netzanteil der IP 10.20.30.40 / 24 ist 10.20.30.0.
- Die Subnetzmaske 255.255.0.0 entspricht dem Präfix /16.
- Die Subnetzmaske 255.255.128.0 entspricht dem Präfix /17.

23. Zeigen Sie, dass Sie die verschiedenen Adressen im Netz kennen und unterscheiden können, dass Sie deren Schreibweise kennen und was mit ihnen adressiert wird. Füllen Sie die Lücken in der Tabelle.

Adresse	OSI-Schicht	Adressgröße (Anzahl Bits)	Schreibweise (Beispiel)	Was wird adressiert?
MAC-Adresse				
			10.20.11.12	
		32 bit		
	2			
				Netzwerk-Interface
				Netzwerk
		48 bit		
		16 bit		
			00-50-56-C0-00-08	
			2a02:8070:88a3:9d00::13dd	

24. In welchem Netz befinden sich die folgenden Hosts?

- 1.2.3.4/8
- 1.2.3.4/16
- 2.3.4.5/24
- 3.4.5.6/29
- 4.5.6.7/30

25. Welches sind gültige IP-Adressen? Streichen Sie die falschen/ fehlerhaften aus der Liste.

- a. 100.150.200.250
- b. 200.250.300.350
- c. 10.20.30.40
- d. 10.255.255.2
- e. 123.234.345.123

26. Lesen Sie im Internet den RFC 1597. Er definiert drei private Adressbereiche, in jeder Adressklasse einen. Wie viele Subnetze sind dabei vordefiniert und zu welcher Klasse gehören diese privaten IP-Adressbereiche? Nennen Sie jeweils das erste, zweite und das letzte Subnetz.

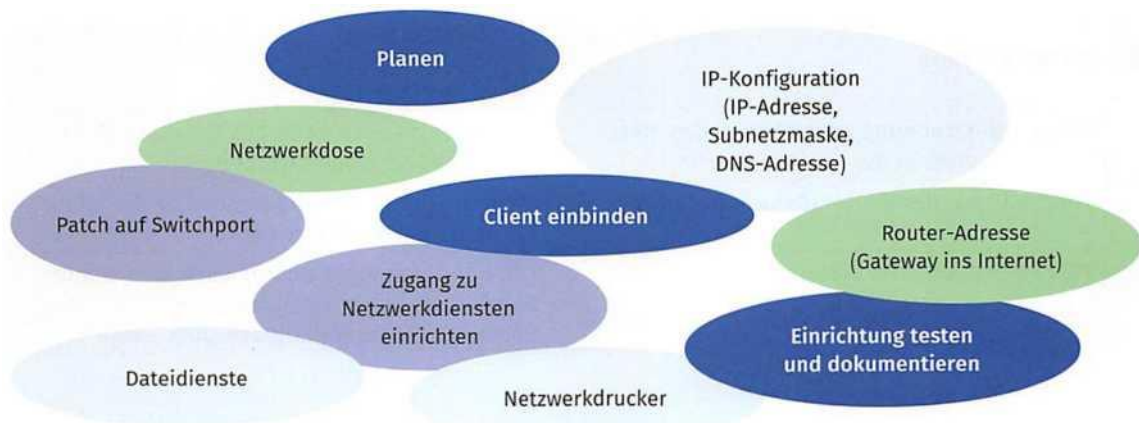
Privater IP-Adressbereich	IP-Adressklasse	Subnetze (Anzahl und Beispiele)
...	...	...
...	...	...
...	...	...

TAG 9 - Selbstständig die Integration von Clients in ein Netzwerk planen und durchführen

Sie sollen selbstständig die Integration von Clients in ein Netzwerk planen und durchführen.

Beim Einbinden eines neuen Rechners in ein bestehendes Netzwerk genügt es nicht, den Rechner mit der passenden Netzwerkdose zu verbinden. Damit alles funktioniert, muss einiges überprüft werden und es sind eventuell einige Einstellungen notwendig.

Die Anforderungen der Clients bestimmen das Netzwerk. Wenn die Anforderungen geklärt sind, wird geprüft, ob der Ist-Zustand des Netzwerkes damit übereinstimmt. Ist der aktuelle Zustand des Netzwerkes nicht bekannt und dokumentiert, muss zuerst der Ist-Zustand des Netzes aufgenommen und protokolliert werden.



LE 1 - Anforderungen der Clients und des Netzwerkes prüfen

Sie sollen die Anforderungen der Clients und des Netzwerkes prüfen. Sie sollen eine Ist-Aufnahme durchführen und den Ist-Zustand dokumentieren. Sie sollen selbstständig neue Clients in ein Netz einbinden und verstehen, was dabei zu tun ist, sowohl leitungsgebunden als auch über WLAN. Dabei sollen Sie die IP-Konfiguration in Grundzügen verstehen, die Clients entsprechend einrichten.

Im Vorfeld müssen einige Dinge bedacht werden, damit die Integration von Clients problemlos von statten geht. Folgende Punkte sind zu beachten:

- notwendige Datenübertragungsrate abschätzen/berechnen,
- IP-Konfiguration festlegen,
- Material und Werkzeug bereitlegen.

Welche Datenübertragungsrate benötigt wird, ist abhängig von den Anwendungen, die an diesem Arbeitsplatz, auf diesem Rechner laufen. Es ist zu überlegen, welche Menge an Daten wie oft und in welchen Zeitabständen übertragen werden muss. Lange Ladezeiten beim Nachladen von Daten während der Arbeit sind nicht akzeptabel. Lange Speicherzeiten auf dem Netz, während und auch am Ende der Arbeit, dürfen ebenfalls nicht sein. Das Netzwerk muss die Daten in angemessener Zeit transportieren. Eine CAD- Workstation, die mit servergestützten Daten arbeitet, verursacht beispielsweise regelmäßig eine große Netzwerklast. Ein Bürorechner zum Schreiben der Geschäftskorrespondenz produziert nur geringe Netzwerklast. Ein Streaming-Server, der permanent Videos ins Netz sendet, produziert Dauerlast auf dem Netzwerk. Man prüft daher vor der Installation des Rechners, wie groß die zu erwartende Netzwerklast sein wird.

Abschätzen der Netzwerklast und aktuelle Netzwerktechnologie

Schätzen Sie ab, welche Datenmenge zum Start geladen werden muss.	→	Wie lange ist die Ladezeit bei verschiedenen Netzwerkstandards?
Schätzen Sie ab, welche Datenmenge zum Beenden übertragen werden muss.	→	Wie lange ist die Speicherzeit beim Beenden bei verschiedenen Netzwerkstandards?
Schätzen Sie ab, welche Datenmenge während der Arbeit übertragen werden muss und wie oft dies geschieht.	→	Wie lange sind die Speicherzeiten bei verschiedenen Netzwerkstandards? →
Welche Netzwerktechnologie mit welcher Datenrate ist aktuell installiert?	→	Wenn nicht bekannt, dann muss dies in Erfahrung gebracht werden!

Die **IP-Konfiguration** ist das Wichtigste, damit die Client-Integration auch logisch funktioniert.

IP-Konfiguration

Welche Netzkennung (Net-ID) hat das Netzwerk? Wie groß ist der Adressbereich?	→	Der Adressbereich kann aus Net-ID und Subnetzmaske berechnet werden.
Welche IP hat der Router (Default Gateway)?	→	Meist ist der Router die erste oder die letzte Adresse in einem Netzwerk.
Welche IP hat der DNS-Server?	→	Oft übernimmt der Router auch den Name-Service, es kann aber auch ein separater Server - auch außerhalb des LANs - sein.
Ist ein DHCP-Server vorhanden?	→	Meist ist ein DHCP-Server vorhanden. Wenn nicht, müssen die IP-Einstellungen von Hand gemacht werden.
Sind Subnetze im LAN vorhanden?	→	Zur Überprüfung kann der Subnetz-Plan eingesehen werden.

(1) Ist-Aufnahme durchführen

Leitungen und Anschlussdosen

Als erstes verschafft man sich einen Überblick über den aktuellen LAN-Ausbau. Beginnen Sie mit der Dokumentation des Netzes. Überprüfen Sie, ob die Unterlagen mit der Realität übereinstimmen. Eine Netzwerkdokumentation muss laufend aktualisiert werden.

LAN-Ausbau		
Ist die Lage von Dosen und Verteilern bekannt?	→	Sind die Lagepläne auf dem neusten Stand?
Wie sind Dosen und Verteiler bezeichnet?	→	Sind die Lagepläne auf dem neusten Stand?
Sind Leitungen dokumentiert?	→	Welcher Standard wird erreicht, welcher Datendurchsatz? Sind Messprotokolle vorhanden?
Sind Patch-Pläne bekannt?	→	Die Patches in den Verteilern müssen dokumentiert sein.

Direkt vor Ort wird überprüft, ob die Gegebenheiten so sind, wie sie dokumentiert sind. Um zu prüfen, ob alle Leitungen und Dosen vorhanden sind, die man zum Anschluss der Clients braucht, ist eine Ortsbesichtigung meistens absolut notwendig.



Fortgefahren wird mit der Dokumentation der Verteiler. An dem Verteiler, an den die Dose, die benutzt werden soll, angeschlossen ist, muss geprüft werden, ob die Patches dokumentiert sind (siehe Beispielabbildungen, S. 41 im Modul).

WLAN-Anschlussmöglichkeiten prüfen und suchen



Sichtbarer Access Point mit Basisstation für das DECT-Funktelefon

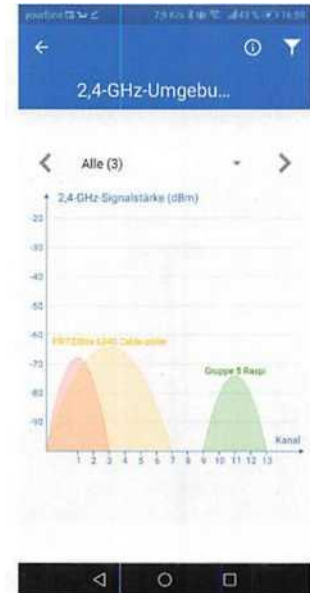
Schwer auffindbar: Access Points hinter Wand- und Deckenverkleidungen, nur die Antennen sind sichtbar

Um die WLAN-Anschlussmöglichkeiten zu prüfen, verschafft man sich auch hier zuerst einen Überblick mithilfe der Dokumentation: Gibt es mehrere WLANs? Wie ist die Lage der Access Points? Ist der Arbeitsbereich der Mobilstation funkmäßig gut ausgeleuchtet?

Manche Access Points sind einfach zu finden. Die Anschlussdose ist dann gut sichtbar und auch die Beschriftung ist lesbar. Andere Access Points sind schwerer zu finden. Sie können beispielsweise hinter Wand- und Deckenverkleidungen versteckt sein.

Um Access Points und Funknetze zu finden, gibt es Messgeräte, die die Sender aufspüren und die Funkfeldstärke messen. Diese Werte sollten in einem Lageplan eingetragen sein.

Für den schnellen Überblick kann man sich auch mit einem Smartphone behelfen. WLAN-Analyse-Apps gibt es zum Teil kostenlos als Download. Der nebenstehende Screenshot des Smartphones zeigt, welche Funknetze aktuell verfügbar sind. Man sieht die Feldstärke (y-Achse) und die Sendekanäle (x-Achse). Eventuell vorhandene Störquellen können auch erfasst und angezeigt werden. Dies sind beispielsweise Bluetooth-Geräte oder Mikrowellenherde.



Wardriving oder Warwalking wird das systematische Absuchen von Straßen und Gebäuden nach offenen WLANs mit dem Auto oder zu Fuß genannt.

IP-Konfiguration

Die IP-Konfiguration ist für die protokollmäßige Anbindung von größter Wichtigkeit. Jedes Netzwerkgerät benötigt eine eindeutige IP-Adresse mit Subnetzmaske, die IP-Adresse des Routers (Default Gateway) sowie die IP- Adresse des DNS-Servers.

Der Konsolenbefehl „*ipconfig*“ listet die aktuellen IP-Konfigurationen von allen vorhandenen Netzwerkschnittstellen auf. Diese Angaben sind verlässlich.

IP-Einstellungen werden über die grafische Oberfläche vorgenommen. Möglicherweise stimmen die Angaben dieser Anzeige nicht mit der aktuellen IP-Konfiguration überein, weil die Einstellungen gegebenenfalls noch nicht gespeichert wurden. Daher verlässt man sich beim Überprüfen der Einstellungen nur auf die Aufgaben, die *ipconfig* liefert.

```
C:\Users\admin> ipconfig

Windows-IP-Konfiguration

Ethernet-Adapter Lan-Verbindung:
Verbindungsspezifisches DNS-Suffix:
Verbindungslokale IPv6-Adresse ..... : ffe80::dlaa:fcd7:55a7:d2a8%16
IPv4-Adresse ..... : 192.168.2.120
Subnetzmaske ..... : 255.255.255.0
Standardgateway ..... : 192.168.2.1

Drahtlos-LAN-Adapter Drahtlosnetzwerkverbindung:

Medienstatus ..... : Medium getrennt
Verbindungsspezifisches DNS-Suffix.. : fritz.box

C:\Users\admin>
```

Im obigen Beispiel ist ersichtlich, dass der Ethernet-Adapter eine komplette IPv4-Konfiguration hat.

(2) Das Netzwerk dokumentieren

Ein Netzwerk muss genauestens dokumentiert sein - zu jeder Zeit! Diese Dokumentation ist Eigentum des Netzwerkbetreibers und bleibt beim Betreiber. Das heißt, dass Änderungen am Netz laufend in die Dokumentation eingepflegt werden. Jeder, der das Netzwerk verändert, hat dies zu dokumentieren. Zur Dokumentation kann man eine einfache Textdatei (MS-Word, Writer) verwenden.

Zur Dokumentation von Netzwerken gibt es professionelle Hilfsmittel. Manche erlauben auch das Scannen des Netzwerkes nach neuen Netzwerkgeräten. Es kann aber auch mit alltäglichen Programmen dokumentiert werden.

Was wird dokumentiert?	Womit wird dokumentiert?
Lagepläne	z. B. MS Visio, Dia, NetworkNotepad
Listen	Textverarbeitung (z. B. MS Word, Writer), eventuell Tabellenkalkulation (z.B. MS Excel, Calc)
Messprotokolle	Tabellenkalkulation
Netzwerkpläne	z. B. MS Visio, Dia, NetworkNotepad, jNetMap (Scannen und Struktur dokumentieren)
IP-Adressbereiche und IP-Subnetze	Tabellenkalkulation, Textverarbeitung

Ein PC-Erfassungsbogen kann folgendermaßen aussehen:

[illegible]

Zum Erfassen der installierten Drucker kann man eine Tabelle wie die folgende erstellen:

Bestandserfassung IT-Ausstattung - Drucker										
Lfd. Nr.	Standort (Gebäude, Zimmernr., Arbeitsplatz)	Drucker (Hersteller, Typ)	Bauart (z.B. Laser SW, Laser color, Tintenstrahl)	Jahr der Inbetriebnahme	Papier-vorrat (Blatt)	Interface: USB, Parallel, Netzwerk (IP-Adresse)	Sonstiges	Netzwerk (max. Datenrate)		Bemerkungen
								Kabel	Wi-Fi	
Bsp.	H1	Samsung CLP415N	Laptop	2077	500	10.1.0.200		7 000	Wi-Fi4	Arbeitsgruppen-drucker mit Sortiereinrichtung
1										
2										
3										
4										
5										

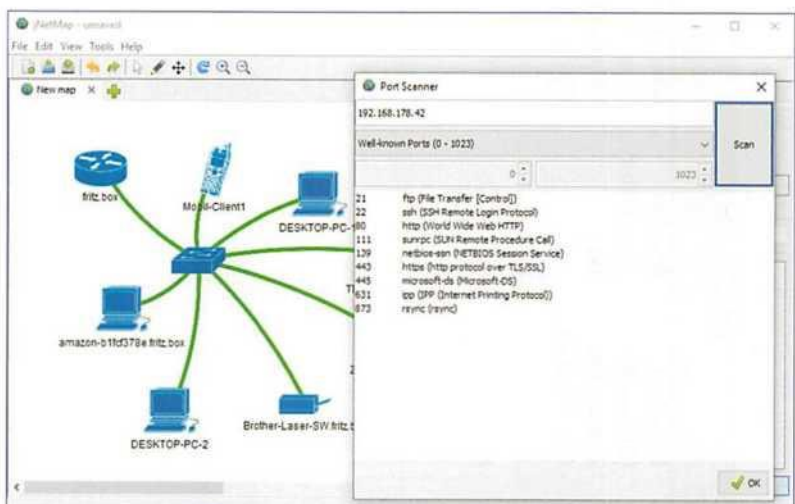
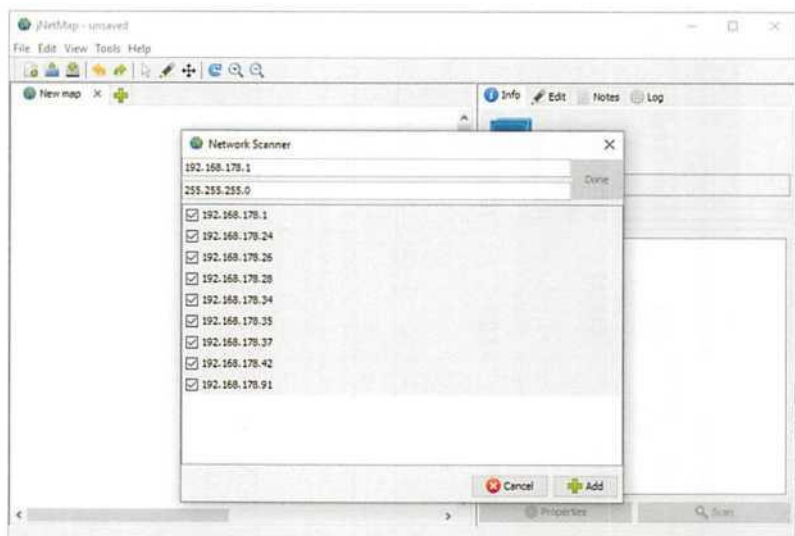
Im Downloadbereich befinden sich die obigen Beispiele sowie ein Textdokument als Vorlage für eine Netzwerkdokumentation.

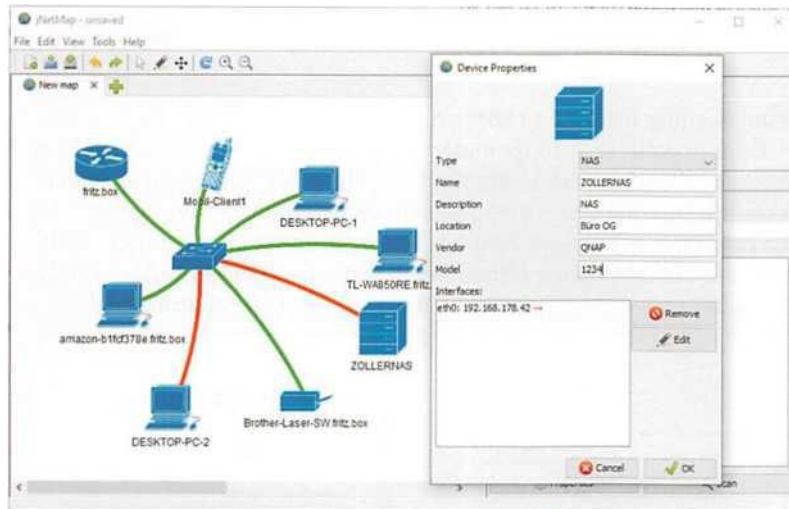
Für jede einzelne Netzwerkleitung muss ein Messprotokoll erstellt werden - vom Verteiler zur Dose in der tertiären Verkabelung und von Verteiler zu Verteiler in der Primär- und Sekundärverkabelung. Dabei werden eine Reihe von elektrisch-physikalischen Parametern gemessen und festgehalten. Unter anderem wird gemessen: Leitungslänge, Verdrahtung (Pinbelegung), Litungsdämpfung, Übersprechdämpfung von einem Leitungspaar zu einem anderen, Signallaufzeit, Laufzeitunterschiede der Paare und einige mehr.

Jede Leitung muss die Prüfung nach geltenden Normen bestehen. Auf dem Messprotokoll wird das Bestehen der Prüfung mit PASS oder FAIL angegeben. Diese Messprotokolle werden vom Ersteller der Verkabelung angefertigt und bei Übergabe der Verkabelungsanlage dem Betreiber überreicht.

Die Lage der WLAN-Access-Points muss auch in die Lagepläne aufgenommen werden. Feldstärkemessungen (die sog. Funkabdeckung oder -ausleuchtung) sind an repräsentativen Punkten im Gebäude und gegebenenfalls auch außerhalb zu messen und in die Pläne einzutragen.

Es gibt viele Programme, um eine Netzwerkdokumentation zu erstellen. jNetMap von rakudave.ch ist ein sehr einfaches und nützliches Tool. Man kann einen IP-Adress-Scan in einem bestimmten Adressbereich ausführen. In einer Liste werden alle Adressen gezeigt, die im LAN erreichbar sind. Die Geräte zu diesen Adressen werden anschließend auf der Karte platziert. Das Programm stellt alle Geräte in der linken oberen Ecke dar. Man zieht die einzelnen Geräte heraus und platziert sie auf der Karte. Durch Rechtsklick auf ein Gerät kann man seine Eigenschaften einstellen. Man kann jedes Gerät auf offene Ports scannen, Telnet oder SSH-Sitzungen aufbauen und vieles mehr. Für jedes Gerät können Eigenschaften angegeben werden wie Standort, Modell usw. In beschränktem Umfang kann mit diesem Programm auch das Netzwerk überwacht werden.





(3) Clients ins Netz einbinden

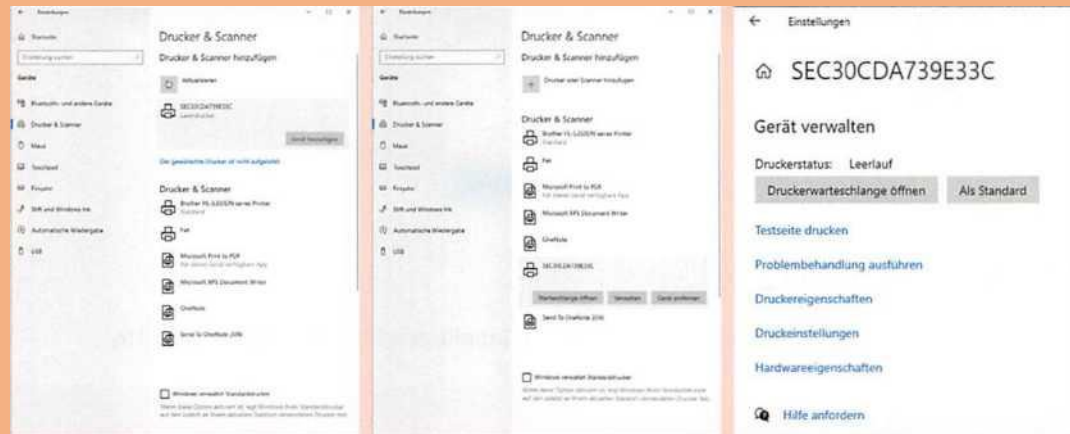
Dabei ist im Vorfeld einiges zu beachten. Die folgende Tabelle zeigt die wichtigsten Schritte.

Rechner aufstellen und anschließen	
Hardwareanschluss herstellen	→ Anschlussdose vorhanden? • Passt die Kategorie der Dose zur gewünschten Übertragungsrate? • Verteiler und Anschlussbuchse dieser Leitung suchen • Freien Switchport suchen
	→ Verbindungsschnüre prüfen, ob die Kategorie passt
	→ Verbindungen herstellen (patchen): • Rechner-Anschlussdose • Switchport - Anschlussbuchse im Verteiler
Anschluss logisch herstellen	→ Rechner hochfahren und testen: • Hat der Rechner seine IP-Konfiguration bekommen? • Wenn nicht, am PC die Netzwerkeinstellungen auf „IP automatisch beziehen“ einstellen • Sind die Server erreichbar? • Ist das Internet erreichbar?
Testen und dokumentieren	→ Ping auf eine Internetseite • Prüft die Namensauflösung (DNS) • Prüft Erreichbarkeit des Routers • Prüft den Zugang zum Internet
	→ Konsolenbefehl ipconfig zeigt die aktuelle IP-Konfiguration an • Stimmt die IP-Adresse?
	→ Rechnername mit Nummer der Anschlussdose, IP-Adresse, Betriebssystem, ... notieren/dokumentieren

Clients beziehen ihre Netzwerkeinstellungen immer automatisch. Einstellungen von Hand sind zu fehleranfällig und werden vermieden. Beim Einrichten eines Netzwerks wird ein DHCP-Server eingerichtet. Dieser verfügt über einen Pool von IP-Adressen, die an die angeschlossenen Rechner automatisch verteilt werden (siehe hierzu S. 84 im Modul).

Drucker auf Clients einrichten

Um mit einem neu eingerichteten Rechner drucken zu können, muss man einen oder mehrere Drucker dem PC bekannt machen. Über **Drucker & Scanner** in den Systemeinstellungen kann man das Netzwerk nach verfügbaren Druckern absuchen. Eine Liste von neu gefundenen Druckern erscheint. Man wählt den oder die Drucker aus, die man benötigt. Danach werden vom Betriebssystem die Druckertreiber installiert. Nach erfolgter Installation wird ein Testausdruck gemacht. Durch Anklicken eines Druckers kann man seine Warteschlange öffnen und bearbeiten. Der Verwalten-Button öffnet das Fenster, um weitere Einstellungen vorzunehmen und um die Testseite zu drucken.



(4) Clients mit einem WLAN verbinden

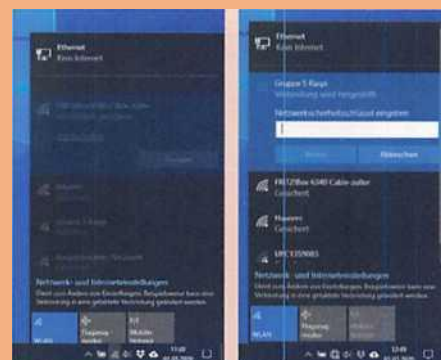
Mobile Clients spielen eine immer größere Rolle in Unternehmensnetzwerken.



Am rechten unteren Rand des Windows-Bildschirms kann man den Internetzugriff einstellen. Ein Klick öffnet das Popup-Window mit den verfügbaren Netzwerken, Funknetze und Festnetze.

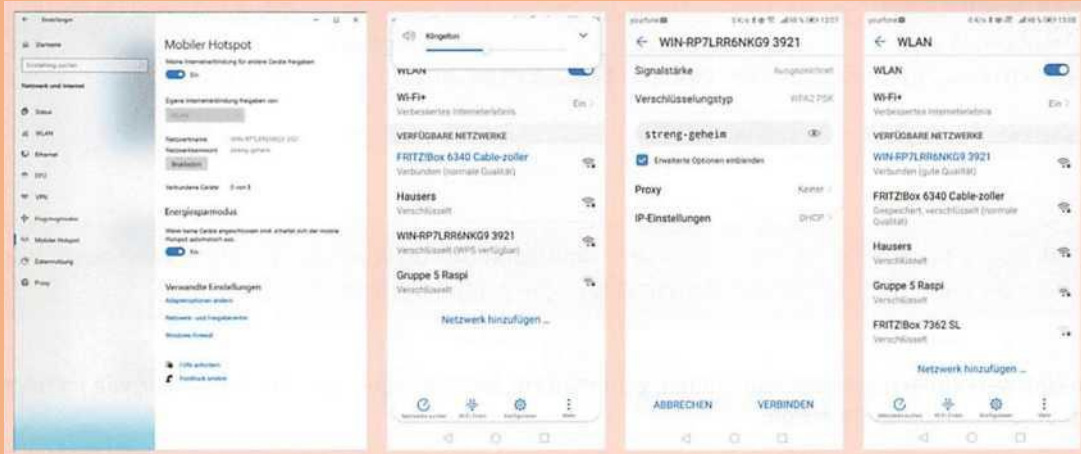
Client mit WLAN verbinden

Bei Ethernet verbindet sich der Rechner direkt mit dem Netzwerk. Bei WLAN muss man sich mit dem WLAN-Passwort anmelden. Es handelt sich hierbei um das sog. PSK-Verfahren (PSK = Pre-Shared Key), was bedeutet, dass der Schlüssel zum Anmelden vorher bekannt sein muss. Beim Einrichten des Funknetzes werden beim Konfigurieren des Access Points der Name des Funknetzes angegeben (SSID = Service Set Identifier) und das Passwort eingestellt.



Mobilen Hotspot einrichten und verbinden

Ein Laptop mit Internetzugang lässt sich auch als Access Point benutzen. Er wird zum mobilen Hotspot. Zum Einrichten des Hotspots müssen die Einstellungen des Rechners aufgerufen werden, z.B. über Rechtsklick auf den Hotspot-Button. In den Eigenschaften wird das Passwort vergeben.



Mit einem anderen Mobilgerät, z.B. einem Smartphone, ist jetzt dieses neue WLAN sichtbar und man kann sich damit verbinden. Dazu wählt man das neue WLAN aus, gibt das Passwort ein und hat nun über den Hotspot Internetzugang. Der Rechner mit Hotspot hat nun die Funktion eines Routers übernommen.

Der Flugmodus bei Mobilgeräten (z.B. Smartphones, Laptops) schaltet alle Funk-Interfaces ab. Dadurch sendet das Gerät keine Funkstrahlen mehr aus, die beispielsweise die Bordelektronik von Flugzeugen oder die medizinischen Geräte in Krankenhäusern stören könnten. Außerdem wird der Stromverbrauch des Gerätes reduziert und die Akkulaufzeit erhöht.

(5) IP-Konfiguration einstellen und überprüfen (Windows und Linux)

Windows

Zur Fehlersuche oder Prüfung der eigenen IP-Einstellungen ist es am einfachsten, die IP-Einstellungen von der Konsole aus abzurufen.

Die Konsole, bei Windows „Eingabeaufforderung“ genannt, öffnet man beispielsweise über die Tastenkombination [Alt Gr] + [r] und tippt dann „cmd“ ein. Der Befehl „ipconfig“ liefert einen kurzen Überblick über die IP-Einstellungen. Wenn dies nicht genügt, so übergibt man noch den Parameter „/all“

```
C:\Users\admin> ipconfig
```

Windows-IP-Konfiguration

Ethernet-Adapter Lan-Verbindung:

Verbindungsspezifisches DNS-Suffix:
 Verbindungslokale IPv6-Adresse : fe80::dlaa:fcd7:55a7:d2a8%16
 IPv4-Adresse : 192.168.2.120
 Subnetzmaske : 255.255.255.0
 Standardgateway : 192.168.2.1

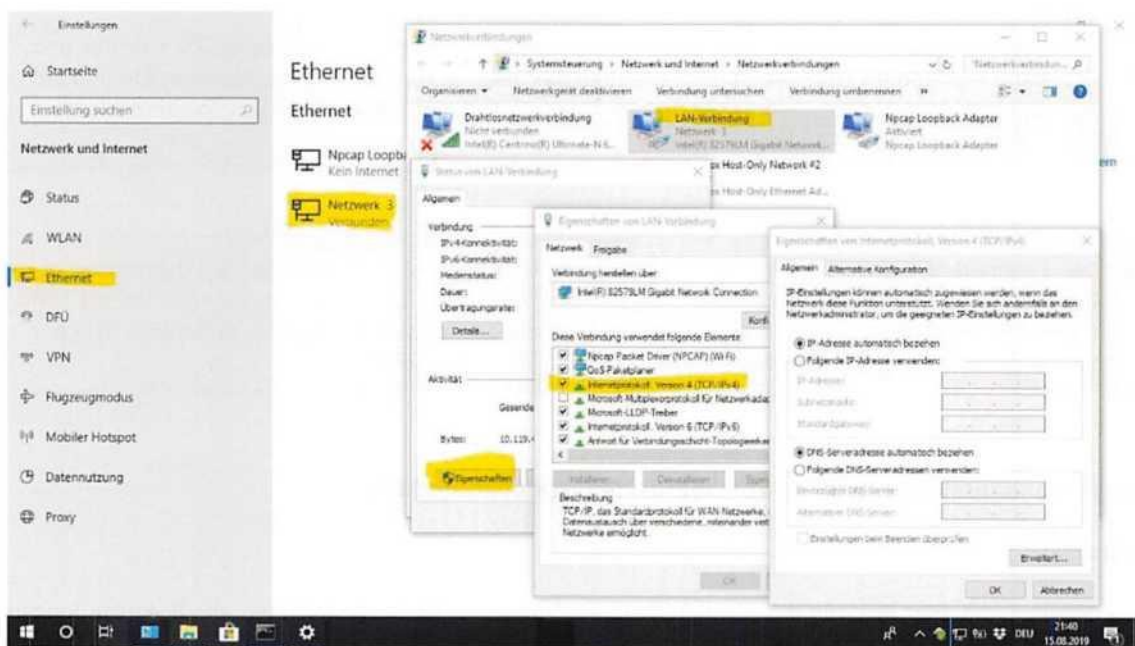
Drahtlos-LAN-Adapter Drahtlosnetzwerkverbindung:

Medienstatus : Medium getrennt
 Verbindungsspezifisches DNS-Suffix : fritz.box

```
C : \Users\admin>
```

Mit dem „**ipconfig**“ kann man die aktuelle Konfiguration von Windows-Rechnern anschauen. Man kann sie nicht verändern. Dazu verwendet man die graphische Oberfläche.

Um Netzwerkeinstellungen vorzunehmen, geht man zu „Einstellungen“ und geht dann vor, wie im folgenden Screenshot skizziert wurde.



Netzwerkeinstellungen unter Windows

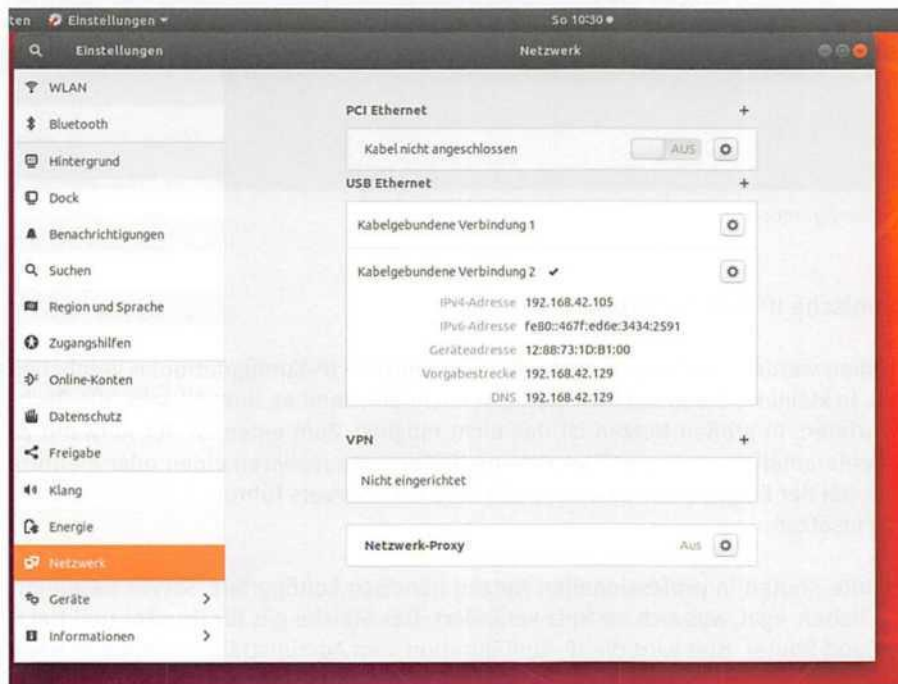
Im Screenshot ist dargestellt, wie man zu den Netzwerkeinstellungen unter Windows findet. Die IP-Adresse (und damit die gesamte IP-Konfiguration) werden hier automatisch bezogen. Um die IP-Konfiguration zu sehen, benutzt man am einfachsten die Konsole. Hier kann man die IP-Konfiguration auch manuell eintragen, wenn man die Automatik nicht verwenden will.

Linux

Auch unter Linux stehen diese Informationen zur Verfügung. Es gibt viele verschiedene Linux-Distributionen, die teilweise sehr unterschiedlich aussehen. Im Screenshot werden die IP-Einstellungen für das verbreitete Linux Ubuntu gezeigt.

Über die Einstellungen gelangt man zu den Netzwerkeinstellungen. In der Abbildung sieht man, dass die eigene IP-Adresse die 192.168.42.105 ist. Der Router hat die IP 192.168.42.129, hier

Vorgabestrecke genannt (für Default Gateway). Des Weiteren sieht man die IPv6-Adresse und die Adresse des DNS-Servers. Die Adresse des DNS-Servers ist hier identisch mit der Router-Adresse. Das bedeutet, dass alle DNS- Anfragen an den Router geschickt werden und dieser die Anfrage ins Internet weiterleitet. Über die Konsole bekommt man hier ebenfalls eine schnelle Antwort, allerdings mit wesentlich mehr Infos.



Netzwerkeinstellungen Linux Ubuntu

Der Befehl „ip“ liefert viele Infos rund um das Netzwerk. Mit „ip address“ bekommt man eine Liste von allen Netzwerk-Interfaces des Rechners. Der Screenshot zeigt vier Interfaces. Interface 1 ist die loop- back-Schnittstelle *lo* mit der IP 127.0.0.1. Interface 2 ist die Ethernet-Schnittstelle, die momentan nicht benutzt wird und daher keine IP-Adresse hat. Interface 3 ist das WLAN-Interface. Momentan auch nicht aktiv und daher auch ohne IP. Das Interface 6 ist die aktive Netzwerkverbindung. Es handelt sich hier um eine USB-Verbindung mit einem Smartphone, sog. Tethering. Man sieht die IP-Adressen Version 4 und Version 6 (vgl. mit der Ausgabe der graphischen Oberfläche). Der Befehl „ip route“ zeigt die eingerichteten Routen an - man sieht die Einstellung für das Gateway, den Router ins Internet.

Bei Linux müssen die Befehle nicht ausgeschriebenen werden. Es reicht, wenn man so viel tippt, dass der Befehl eindeutig ist. Hier genügt also „ip a“ statt „ip address“.

```

url@url-V5-18: ~
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
url@url-V5-18:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp4s0f0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 20:89:84:81:92:40 brd ff:ff:ff:ff:ff:ff
3: wlp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether bc:85:56:a9:e8:af brd ff:ff:ff:ff:ff:ff
6: enp0s29u1u2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 12:88:73:1d:b1:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.42.105/24 brd 192.168.42.255 scope global dynamic noprefixroute enp0s29u1u2
        valid_lft 3441sec preferred_lft 3441sec
    inet6 fe80::467f:ed6e:3434:2591/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
url@url-V5-18:~$ ip route
default via 192.168.42.129 dev enp0s29u1u2 proto dhcp metric 20100
169.254.0.0/16 dev enp0s29u1u2 scope link metric 1000
192.168.42.0/24 dev enp0s29u1u2 proto kernel scope link src 192.168.42.105 metric 100
url@url-V5-18:~$
  
```

Konsolenbefehle für Netzwerkkonfiguration unter Linux

(6) Statische und dynamische IP-Adressen/DHCP

Statische IP-Konfigurationen werden von Hand eingetragen. Dynamische IP-Konfigurationen geschehen über das DHCP-Protokoll. In kleinen Netzen mit sehr wenigen Rechnern, kann es sinnvoll sein, alle Rechner von Hand zu konfigurieren. In großen Netzen ist das nicht möglich. Zum einen ist der Aufwand zu groß, zum anderen die Fehleranfälligkeit. Doppelt vergebene IP-Adressen isolieren einen oder mehrere Rechner vom Netz. Fehler bei der Eingabe des Gateways oder des DNS-Servers führen zu Fehlfunktionen und unnötigen Support-Einsätzen.

Dennoch werden bestimmte Knoten in professionellen Netzen händisch konfiguriert. Server sollen immer dieselbe IP-Adresse haben, egal, was sich im Netz verändert. Das Gleiche gilt für Drucker und Netzwerkgeräte wie Switches und Router. Hier wird die IP-Konfiguration vom Administrator immer von Hand eingegeben und dokumentiert.

Die Dokumentation eines Netzes und der verwendeten IP-Adressen ist von essenzieller Wichtigkeit. So können auch Kollegen und Kolleginnen ohne Administratorberechtigungen im Bedarfsfall die Konfiguration einsehen.

LE 2 -Cloud-Dienste nutzen

Sie sollen lernen, wie Cloud-Dienste von einem Client genutzt werden können.

(1) Anbieter von Cloud-Services

Es gibt sehr viele Anbieter von Cloud-Lösungen, wenige große und viele kleine. Der größte Anbieter ist zurzeit Amazon Web Service (AWS). Weitere große Cloud-Anbieter sind Microsoft Azure und Google Cloud Plattform (GCP). Viele Dienste können kostenlos getestet werden.

Zahlreiche Großbetriebe nutzen Cloud-Dienste. Und auch viele Kleinbetriebe verzichten auf ein eigenes Datacenter und nutzen stattdessen Infrastructure as a Service (IaaS). Die Preise hängen dabei direkt von den benötigten Diensten ab, sodass man dynamisch die Dienste den Anforderungen anpasst und nur das in Anspruch genommene bezahlt. Lastspitzen können so durch zeitweises Hochfahren der Dienste abgefangen werden, ohne dauerhaft hohe Systemleistungen vorhalten zu müssen.

(2) Speicher in der Cloud nutzen

Viele Anbieter bieten Festplattenplatz in der Cloud an (Web Storage). Durch Dateitransferprogramme wie FTP (File Transfer Protocol) lassen sich Dateien vom lokalen Rechner in die Cloud hoch- oder herunterladen. Elegantere Lösungen integrieren den Cloud-Speicher in das lokale Dateisystem, sie erscheinen wie lokale Festplatten.

Vorteile sind:

- Dateien werden lokal gespeichert und nach dem Speichern im Hintergrund mit dem Cloud-Speicher synchronisiert.
- Mehrere Computer können sich mit dem Cloud-Speicher verbinden und werden automatisch synchronisiert. Beispielsweise kann man zu Hause am Desktop-PC arbeiten und anschließend unterwegs am Laptop mit dem aktuellen Datenstand Weiterarbeiten. Im Büro werden die Dateien ebenso abgeglichen, sodass man dort direkt mit denselben Daten Weiterarbeiten kann.
- Viele Systeme verfügen über eine Versionsverwaltung. Das heißt, dass frühere Datenstände gespeichert bleiben und man bei Bedarf auf ältere Daten oder auch gelöschte Dateien zugreifen kann.

Vorsicht: Bei vielen Anbietern ist nicht klar, in welchem Land der Erde die Daten wirklich gespeichert sind. Für das Speichern von Daten gelten die Gesetze des Landes, in dem die Daten physisch liegen. Daten, die in den USA liegen, sind daher potenziell nicht sicher. Selbstverständlich sollten Daten verschlüsselt übertragen werden und auch verschlüsselt abgespeichert werden. Am besten ist es, die Daten werden bereits lokal verschlüsselt abgespeichert. Dies erschwert allerdings die Zusammenarbeit im Team mit Teamkollegen. Die Datenschutzgrundverordnung ist dabei immer zu berücksichtigen.

Beispiele für Anbieter von Web Storage:

- Dropbox
- Google Drive
- Microsoft OneDrive
- Apple iCloud
- Amazon Speicher S3
- Strato HiDrive (Hosting in Deutschland)

Die beste Lösung ist das Einrichten einer eigenen Cloud, beispielsweise OwnCloud oder Next-Cloud. Diese kann auf einem Cloud-Server eingerichtet werden oder auch im LAN. Bei der Installation auf einem eigenen Server im LAN ist der Speicher für interne Rechner erreichbar. Durch Öffnen von Routerports und Dynamischem DNS (DynDNS) kann auch vom Internet aus auf den privaten Cloud-Speicher zugegriffen werden.

(3) Büroanwendungen in der Cloud nutzen

Standardanwendungen im Büro werden seit einigen Jahren als Cloud-Dienste angeboten. Um Textverarbeitung, Tabellenkalkulation oder Präsentationssoftware zu nutzen, muss man keine Software mehr lokal installieren. Es genügt, eine entsprechende Anwendung im Internet zu buchen. Die meisten Office-Dienste in der Cloud beinhalten nicht nur die Nutzung der Programme auf Servern im Internet, sondern auch Speicherplatz zum Ablegen der Dateien.

Vorteile gegenüber einer lokalen Installation:

- Eine Installation auf dem Rechner ist nicht notwendig.
- Die Software ist immer auf dem aktuellen Stand.
- Mehrere Nutzer können auf dieselben Daten zugreifen (Teamarbeit).
- Die Nutzung ist unabhängig vom Rechner, der Zugang zu einem internetfähigen Rechner genügt. Beispiele für Anbieter:
- Google Docs
- Microsoft OnlineOffice
- Colabora Office
- Apple iWork für iCloud
- OnlyOffice

LE 3 - Benutzer anmelden

Um sich an einem PC anmelden zu können, benötigt man ein Benutzerkonto. Privatpersonen und -haushalte haben in der Regel ein Benutzerkonto für jeden Benutzer auf jedem Rechner. Diese Konten werden lokal an diesem Rechner verwaltet. In Unternehmensnetzwerken müssen die Benutzer zentral verwaltet werden. Man muss Zugriffe auf Netzwerkressourcen gewähren oder verbieten.

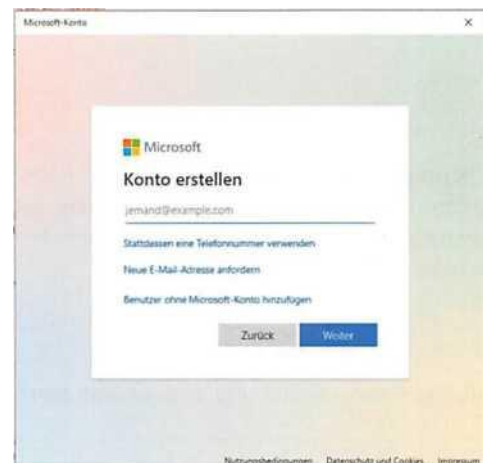
(1) Lokalen Benutzer erstellen

Um einen lokalen Benutzer anzulegen, geht man in den Einstellungen auf „Familie und andere Benutzer“.



Es öffnet sich ein neues Fenster. Hier kann man die E-Mail- Adresse des neuen Benutzers angeben, wenn der Benutzer bereits über ein Microsoft-Konto verfügt. Zum Anlegen eines neuen Benutzers ohne bestehendes Microsoft-Konto wählt man „Ich kenne die Anmeldeinformationen für diese Person nicht“ aus.

Anschließend kann man ein neues Microsoft-Konto erstellen oder den neuen Benutzer nur lokal anlegen. Man wählt hier „Benutzer ohne Microsoft-Konto hinzufügen“ und gibt anschließend den Namen des neuen Benutzers und das Startpasswort ein.



(2) Netzwerkbenutzer

Benutzer, die sich am Netzwerk anmelden sollen, werden auf einem System auf einem oder mehreren Servern eingerichtet. Netzwerk-User werden über das Netzwerk bei dem Anmeldedienst authentifiziert. Von diesem Dienst werden die Berechtigungen zugeteilt, die festlegen, in welcher Weise auf Netzwerkressourcen zugegriffen werden kann.

Bei Windows-Netzwerken ist dies das Active Directory (AD). Ein anderes System ist RADIUS.

RADIUS steht für „Remote Authentication Dial-In User Service“ (auf deutsch „Authentifizierungsdienst für sich einwählende Benutzer“). RADIUS ist ein Client-Server-Protokoll, das zur Authentifizierung, Autorisierung und zum Accounting (Triple-A-System) von Benutzern dient. RADIUS ist der De-facto-Standard bei der zentralen Authentifizierung von Einwahlverbindungen über Modem, ISDN, VPN, WLAN (IEEE 802.1X) und DSL.

Der RADIUS-Server übernimmt den AAA-Dienst:

Authentifizierung	Service zum Überprüfen von Benutzername und Kennwort
Autorisierung	Berechtigungen für den Zugriff auf Netzwerkressourcen wie Daten, Drucker,...
Accounting	Abrechnung der IT-Nutzung nach Benutzung der IT

Ein RADIUS-Server bezieht seine Daten aus eigenen Konfigurationsdateien oder Datenbanken. Er kann mit anderen RADIUS-Servern verbunden werden und Daten dort einholen. Ein bekanntes Beispiel ist Education Roaming (eduroam). Dies ist der Zusammenschluss der RADIUS-Server der meisten europäischen Universitäten und Hochschulen. Durch diese Initiative ist es Hochschulangehörigen möglich, sich nicht nur an der eigenen Hochschule am WLAN anzumelden, sondern an fast jeder Hochschule Europas. Zudem hat man Zugang zu eigenen Daten auf dem Dateiserver an der Heimathochschule.

Lernzielkontrollen TAG 9

1. Sie möchten überprüfen, ob Ihr Rechner in demselben Subnetz ist wie der Router. „ipconfig“ liefert Ihnen folgende Angaben:

IP-Address	192.168.1.210
SN	255.255.255.128
Default-GW	192.168.1.1

Sind beide in demselben Subnetz? Wird ein Ping funktionieren?

2. Sie bekommen folgenden Screenshot eines Rechners, nach dem Ausführen des Befehls „ipconfig / all“.

```
Drahtlos-LAN-Adapter WLAN:
Verbindungsspezifisches DNS-Suffix : fritz.box
Beschreibung : Intel(R) Dual Band Wireless-AC 7260
Physische Adresse : E8-B1-FC-03-2D-0C
DHCP aktiviert : Ja
Autokonfiguration aktiviert : Ja
IPv6-Adresse : 2a02:8070:88b0:ba00:d534:566b:8c8a:13ef(Bevorzugt)
Temporäre IPv6-Adresse : 2a02:8070:88b0:ba00:ecbe:71e7:801:e881(Bevorzugt)
Verbindungslokale IPv6-Adresse : fe80::d534:566b:8c8a:13ef%32(Bevorzugt)
IPv4-Adresse : 192.168.178.27(Bevorzugt)
Subnetzmaske : 255.255.255.0
Lease erhalten : Sonntag, 1. März 2020 14:42:09
Lease läuft ab : Mittwoch, 11. März 2020 14:42:06
Standardgateway : fe80::2665:11ff:fe12:5ece%32
                  192.168.178.1
DHCP-Server : 192.168.178.1
DHCPv6-IAID : 334017020
DHCPv6-Client-DUID : 00-01-00-01-25-0C-19-AF-28-D2-44-F2-C0-AD
DNS-Server : fd00::2665:11ff:fe12:5ece
              192.168.178.1
NetBIOS über TCP/IP : Aktiviert
```

- a. Welche Aussagen können Sie treffen?
 - b. Welche IP-Adresse hat der Rechner, welche der Router, welche das Gateway?
 - c. Wie lautet die MAC-Adresse des Rechner-Interfaces?
 - d. Wie lange ist die Gültigkeitsdauer von IP-Adressen?
3. Wie verhält sich ein Rechner, wenn er die korrekte IP des DNS-Servers nicht kennt? Wie verhält sich ein Rechner, wenn er die IP des Routers-Servers nicht kennt?
4. Erstellen Sie einen Netzwerkplan. Zeichnen Sie mit einem gängigen Zeichenprogramm (z.B. Dia, Visio, Draw) ein Netzwerk bestehend aus vier PCs, einem Server, einem Switch und einem Router ins Internet. Verwenden Sie den IP-Adressbereich 192.168.200.64/26 und schreiben Sie zu den Geräten die jeweilige IP-Konfiguration mit IP-Adresse, Subnetmask und Default-Gateway. Präsentieren und vergleichen Sie Ihre Ausarbeitungen.
5. Erarbeiten Sie ein Formular zur Abnahme und zur Übergabe eines PCs an den Kunden. Erstellen Sie mithilfe eines gängigen Textverarbeitungs- oder Tabellenkalkulationsprogramms ein Formblatt, in dem alle Punkte, die zur Abnahme gehören, aufgelistet sind. Sehen Sie die Felder für den Prüfer und den Kunden zur Unterschrift vor. Präsentieren und vergleichen Sie die Ergebnisse.
6. Was ist richtig, was ist falsch?
- a. Daten werden in Cloud-Speichern grundsätzlich verschlüsselt gespeichert. Deshalb ist es egal, in welchem Land die Daten liegen.
 - b. Dateien können vor dem Übertragen zu Cloud-Speichern verschlüsselt werden, um sie verschlüsselt zu übertragen und verschlüsselt in der Cloud zu speichern.
 - c. Office-Anwendungen müssen immer lokal installiert werden.
 - d. Bei der Buchung von Cloud-Servern bezahlt man auch die Server, die bereitstehen, aber nicht benutzt werden.
7. Wofür steht der Begriff AAA-Dienst?
8. Was versteht man unter Authentifizierung und was unter Autorisierung?

9. Legen Sie einen neuen Benutzer an Ihrem Rechner an.
Um Benutzer anzulegen, gibt es meist mehrere Möglichkeiten, und zwar über
- Die grafische Oberfläche,
 - Die Konsole (WIN-Taste + R, cmd als Administrator ausführen).
- a. Legen Sie einen Benutzer über die **GUI** an. Nennen Sie kurz die Schritte und die Eingaben, die Sie tätigen.
- b. Legen Sie einen Benutzer über die **Konsole** an. Nennen Sie kurz die Schritte und die Eingaben, die Sie tätigen. (Hinweis: Benutzen Sie die Hilfe zu den Windows-Befehlen. Beginnen Sie mit dem Befehl „net ?“.)

TAG 10 - Die Netzwerkfunktion der Clients prüfen und warten

Sie sollen die korrekte Funktion eines Clients überprüfen.

<pre>C:\Users\uri>ping 1.2.3.4</pre> Ping wird ausgeführt für 1.2.3.4 mit 21 Bytes Daten: Zeitüberschreitung der Anforderung Zeitüberschreitung der Anforderung Zeitüberschreitung der Anforderung Zeitüberschreitung der Anforderung Ping-Statistik für 1.2.3.4: Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4 (100% Verlust),	 Kein Internet Versuchen Sie Folgendes. • Netzwerkkabel, Modem und Router prüfen • WLAN-Verbindung erneut herstellen • Windows-Netzwerkdiagnose ausführen DNS_PROBE_FINISHED_NO_INTERNET
--	---

Nachdem ein Rechner installiert ist und mit dem Netzwerk verbunden, müssen die Netzwerkkonfiguration überprüft und die Verbindung mit dem Netz getestet werden. Die Einstellungen überprüft man mit dem Konsolenbefehl „ipconfig“ (siehe Kapitel 3.5.1, S. 341). Wenn die IP-Konfiguration stimmt, kann mit dem Connectivity-Test weitergemacht werden. Andernfalls müssen die Einstellungen wiederholt werden.

LE 1 - Verbindungstest durchführen

Sie sollen einen Verbindungstest durchführen.

Beim Verbindungstest (Connectivity-Test) geht es darum, sehr schnell herauszufinden, ob alle Funktionen im Netzwerk korrekt arbeiten. Man „pingt“ den Router an und eine Adresse im Internet. Man testet, ob der DNS-Server erreichbar ist.

(1) Ping-Befehl

Der Ping-Befehl läuft auf jedem System mit TCP/IP. Der Befehl schickt ein Datenpaket zu der angegebenen Adresse. Die Zielrechner schickt das Paket unverzüglich wieder an den Absender zurück. Die Ping-Zeit vom Absenden des Paketes bis zum Ankommen der Antwort ist die Signallaufzeit über die Leitung und alle zwischen Sender und Empfänger befindlichen Netzwerkgeräte. Man nennt diese Zeit die Round Trip Time (RTT), also die Rundlaufzeit. Je größer die RTT, desto langsamer die Netzverbindung.

<pre>~\$ ping <IP-Adresse></pre>	„pingt“ die angegebene IP-Adresse an, z.B. ping 120.1.2.3. Setzt man die IP-Adresse des Routers ein (oft 192.168.0.1, 192.168.1.1 oder 192.168.178.1), wird die Erreichbarkeit des Routers geprüft. Gibt man anstatt der IP-Adresse eine URL an, so wird dieser Server im Internet angesprochen.
--	--

Bei Windows ist der ping-Befehl so voreingestellt, dass er vier Pakete mit jeweils 32 Byte Daten verschickt. Für jedes Paket wird die Zeit gemessen, bis die Antwort eintrifft. Dies ist die RTT. Am Ende wird noch angezeigt, wie viele Pakete angekommen oder verloren gegangen sind, wie die kürzeste, die längste Ping-Antwortzeit war und der Durchschnitt der Antwortzeit.

<pre>C:\Users\uri>ping 192.168.178.1</pre> Ping wird ausgeführt für 192.168.178.1 mit 32 Bytes Daten: Antwort von 192.168.178.1: Bytes=32 Zeit=6ms TTL=64 Antwort von 192.168.178.1: Bytes=32 Zeit=3ms TTL=64 Antwort von 192.168.178.1: Bytes=32 Zeit=20ms TTL=64 Antwort von 192.168.178.1: Bytes=32 Zeit=2ms TTL=64 Ping-Statistik für 192.168.178.1: Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust), Ca. Zeitangaben in Millisek.: Minimum = 2ms, Maximum = 20ms, Mittelwert = 7ms <pre>C:\Users\uri></pre>
--

Statt der IP-Adresse des Zielrechners kann man auch seinen symbolischen Namen angeben.

```
~$ ping www.google.de
```

„pingt“ den Rechner mit der angegebenen URL, hier: google.de, an

Hier wird die URL google.de „angepingt“. Man sieht, dass in Wirklichkeit der Rechner 2a00:1450:4001:821::2003 „angepingt“ wird. DNS hat den Namen in diese IPv6-Adresse aufgelöst.

```
C:\Users\luri>ping google.de
```

Ping wird ausgeführt für google.de [2a00:1450:4001:821::2003] mit 32 Bytes Daten:

Antwort von 2a00:1450:4001:821::2003 Zeit=20ms

Antwort von 2a00:1450:4001:821::2003 Zeit=38ms

Antwort von 2a00:1450:4001:821::2003 Zeit=23ms

Antwort von 2a00:1450:4001:821::2003 Zeit=25ms

Ping-Statistik für 2a00:1450:4001:821::2003:

Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),

Ca. Zeitangaben in Millisek.:

Minimum = 20ms, Maximum = 38ms, Mittelwert = 26ms

Der Parameter -4 in diesem Beispiel gibt an, dass der Ping mit IP-Version 4 ausgeführt werden soll. Man sieht, dass in Wirklichkeit der Rechner 172.217.18.3 „angepingt“ wird. DNS hat den Namen in diese IP aufgelöst. Bei Geräten, die beide IP-Versionen beherrschen, wird vorzugsweise Version 6 benutzt.

```
C:\Users\luri>ping google.de -4
```

Ping wird ausgeführt für google.de [172.217.18.3] mit 32 Bytes Daten:

Antwort von 172.217.18.3: Bytes=32 Zeit=19ms TTL=55

Antwort von 172.217.18.3: Bytes=32 Zeit=43ms TTL=55

Antwort von 172.217.18.3: Bytes=32 Zeit=38ms TTL=55

Antwort von 172.217.18.3: Bytes=32 Zeit=17ms TTL=55

Ping-Statistik für 172.217.18.3:

Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),

Ca. Zeitangaben in Millisek.:

Minimum = 17ms, Maximum = 43ms, Mittelwert = 29ms

```
C:\Users\luri>
```

Wenn ein Ping nicht funktioniert, muss das nicht unter allen Umständen heißen, dass der „angepingte“ Rechner nicht erreichbar ist. Gegebenenfalls wird der Ping von der Firewall geblockt.

```
C:\Users\luri>ping bundestag.de
```

Ping wird ausgeführt für bundestag.de [46.243.122.48] mit 32 Bytes Daten:

Zeitüberschreitung der Anforderung

Zeitüberschreitung der Anforderung

Zeitüberschreitung der Anforderung

Zeitüberschreitung der Anforderung

Ping-Statistik für 172.217.18.3:

Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4 (100% Verlust),

(2) Traceroute

Um zu verhindern, dass unzustellbare IP-Pakete im Internet umherirren, sind sie mit einer Lebensdauer (TTL, *Time to live*), versehen. Jeder Router verringert das TTL-Feld des IP-Paketes um eins. Der Router, der auf null zählt, vernichtet das Paket und schickt eine Meldung zurück zum Absender.

Diese Funktion macht sich die Traceroute-Funktion zunutze. Es werden, ähnlich der Ping-Funktion, Datenpakete an einen Zielrechner geschickt. Das erste Paket wird mit einem TTL-Wert von eins losgeschickt. Der erste Router verringert diese Zahl, zählt auf null und schickt eine Fehlermeldung zum Absender zurück. Das nächste Paket wird mit einem TTL von zwei losgeschickt. Der erste Router erniedrigt auf eins, der zweite Router auf null - und schickt eine Fehlermeldung zurück. So geht es weiter, bis das Ziel erreicht ist. Und jeder Router unterwegs hat eine Fehlermeldung geschickt, sodass man eine Liste von Routern erhält, die zwischen Absender und Ziel liegen.

```
C:\Users\admin>tracert google.de

Routenverfolgung zu google.de [172.217.22.99] über maximal 30      Hops :
 1  1  ms  1  ms <1  ms  192.168.2.1
 2  4  ms  1  ms 1    ms  192.168.178.1
 3 20  ms 18  ms 15   ms  81.210.141.53
 4 26  ms 19  ms 26   ms  de-fra01b-rcl-ae37-0.aorta.net    [84.116.191.173]
 5 23  ms 28  ms 16   ms  de-fra01b-rcl-ae37-0.aorta.net    [84.116.132.178]
 6 17  ms 17  ms 19   ms  213.46.177.42
 7 25  ms 24  ms 24   ms  108.170.252.1
 8 34  ms 18  ms 32   ms  72.14.234.113
 9 20  ms 17  ms 19   ms  fra5sl8-in-f99.lel00.net          [172.217.22.99]
Ablaufverfolgung beendet
```

Traceroute zu www.google.de

Die obige Abbildung zeigt ein Beispiel für eine Routenverfolgung zu einem Rechner von www.google.de. Den Traceroute-Befehl gibt es für jedes Betriebssystem, welches TCP/IP beherrscht. Es kann, je nach Betriebssystem, einen anderen Namen haben, beispielsweise „tracert“ (bei Windows) und „tracpath“ (bei Linux Ubuntu).

LE 2 - Namensauflösung prüfen und einen Schnelltest durchführen

Sie sollen prüfen, ob Internetnamen in IP-Adressen aufgelöst werden.

(1) Namensauflösung des Domain Name Systems (DNS) testen

Im Internet werden symbolischen Namen für Rechner verwendet (z.B.: www8.hp.com). Diese müssen in IP-Adressen umgewandelt werden. Diese Aufgabe übernimmt das DNS). Wenn die Namensauflösung nicht funktioniert, dann sind andere Rechner nur mit ihrer IP-Adresse erreichbar, nicht aber mit ihrem symbolischen Namen. Der Befehl „nameserverlookup“ schlägt im weltweiten Internet-Adressbuch die angefragte Adresse nach und liefert die IP-Adresse der angefragten URL. Der nslookup-Befehl ist auf den meisten Betriebssystemen mit TCP/IP verfügbar. Eine ähnliche Funktion hat der Befehl „dig“ (auf Linux-Systemen).

```
C:\Users\luri>nslookup www.bild.de
Server: fritz.box
Address: fd00::2665:11ff:fe12:5ece

Nichtautorisierende Antwort:
Name: e24152.g.akamaiedge.net
Addresses: 95.101.83.17
           95.101.83.162
Aliases:   www.bild.de
           www.bild.de.edgekey.net

C:\Users\luri>
```

Im Beispiel: Der PC ermittelt bei der Fritz!Box nach der IP-Adresse von der URL www.bild.de. Der Fritz!Box- Router (als eingetragener DNS-Server) liefert die IP-Adressen 95.101.83.17 und 95.101.83.162 zurück. Man sieht bei dieser Anzeige, dass die lokale Fritz!Box als DNS-Server eingetragen und benutzt wird. Die Anfrage liefert in diesem Fall zwei IP-Adressen zurück. Die angefragte Seite ist auf mehreren Web-Servern erreichbar.

Man kann dem *nslookup* auch die Adresse eines bestimmten DNS-Servers mitgeben. Dann wird die Namensauflösung von diesem Server angefordert. Im Beispiel wurde der sehr leistungsstarke und über sehr viele Einträge verfügende DNS-Server von Google angefragt (IP-Adresse 8.8.8.8). Man erkennt, dass die Adresse 8.8.8.8 rückwärts aufgelöst wird und der Servername *dns.google* angezeigt wird. In diesem Beispiel werden von diesem Server vier IP-Adressen zurückgeliefert.

```
C:\Users\uri>nslookup www.bild.de 8.8.8.8
Server: dns.google
Address: 8.8.8.8

Nichtautorisierende Antwort:
Name: e24152.g.akamaiedge.net
Addresses:      2.16.218.10
                2.16.218.24
                2.16.218.42
                2.16.218.18
Aliases:        www.bild.de
                www.bild.de.edgekey.net

C:\Users\uri>
```

(2) Schnelltest durchführen

Bevor alles einzeln getestet wird, kann man mit nur einem einzelnen Ping auf ein Ziel außerhalb des eigenen Netzes fast alles auf einmal kontrollieren.

```
C:\>ping google.de
```

Gelingt dies, so stimmt die IP-Konfiguration. Das Default Gateway und auch die Namensauflösung funktioniert.

Wenn ein Rechner oder ein anderes Gerät oder auch eine ganze Verkabelung oder ein Rechenzentrum in Betrieb genommen wurde, dann erfolgt am Ende eine Abnahme bzw. eine Übergabe an den Kunden. Dies muss ordnungsgemäß protokolliert werden. Das Begleichen der Rechnung wird meist von einem Abnahmeprotokoll abhängig gemacht. Daher ist die korrekte Funktion des Systems zu belegen. Hier helfen neben Messprotokollen (soweit möglich) auch Fotos und Screenshots.

LE 3 - Management und vorbeugende Wartung

Sie sollen Grundlagen des Netzwerkmanagements und der vorbeugenden Wartung kennen.

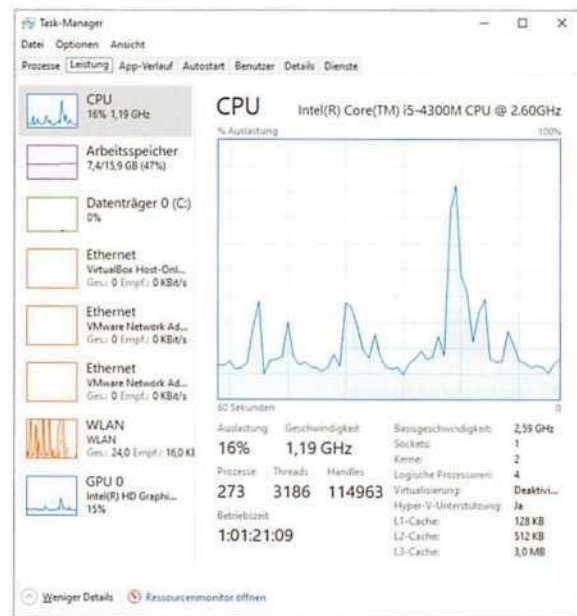
Ein Netzwerk soll nicht nur nach der Installation funktionieren. Es muss langfristig performant seinen Dienst verrichten. Das geht nicht ohne Wartung und Management.

(1) Agieren und Reagieren

Reaktives Management	Proaktives Management
Man reagiert auf auftretende Probleme und Fehler.	Man agiert im Voraus, sodass Probleme oder gar Ausfälle erst gar nicht auftreten. Man macht präventive Wartung.
Jeden Tag wird eine Menge Daten produziert und auf dem Server gespeichert. Plötzlich ist der Festplattenplatz eines Servers voll. Man kann nichts mehr auf dem Server speichern. Eventuell stürzt dabei sogar der Server ab. Schnellstmöglich muss eine weitere Platte eingebaut werden und das System wieder zum Laufen gebracht werden. Das Ganze während der Hauptgeschäftszeit. Wie ist es mit Datenverlust und Datensicherung?	Jeden Tag wird eine bestimmte Menge Daten produziert und auf dem Server gespeichert. Der freie Plattenplatz wird laufend beobachtet. Rechtzeitig bevor der freie Platz zu Ende geht, wird eine neue Platte beschafft und ins System eingebaut. Die IT-Nutzer bemerken von der Sache gar nichts.

(2) Systemüberwachung mit Bordmitteln

Rechnersysteme kann man mit speziellen Management-Tools überwachen. Für den Anfang reichen auch Systemwerkzeuge wie der Task- Manager bei Windows. Man startet den WindowsTask-Manager mit der Tastenkombination [Strg] + [Shift] + [ESC]. Hier kann man sich schnell einen Überblick über die Auslastung eines Rechners oder Servers verschaffen. Derartige Tools bringen alle gängigen Betriebssysteme mit. Wichtig beim Auswerten von Systemkennzahlen ist, dass man die Normalwerte kennt. Dies sind die Werte, die im Normalbetrieb erreicht werden. Diese Normalwerte nennt man Grundlinie oder Baseline. Zu einer Baseline gehören beispielsweise die durchschnittliche CPU-Last, die RAM-Auslastung, die Datenübertragungsrate und natürlich auch die RTT zu den wichtigsten Servern und Zielen (siehe LE 1, S. 90 im Modul)



Lernzielkontrollen TAG 10

- Wahr oder falsch?
 - Mit „nslookup“ kann man die Namensauflösung von einem bestimmten DNS-Server testen.
 - „dig“ ist bei Windows-Rechnern ein Befehl ähnlich wie „nslookup“.
 - Die Funktion des DNS testet man durch „Anpingen“ von dns.de.
 - „nslookup“ ist auf den meisten Netzwerkrechnern zu finden.
- Überlegen Sie zusammen in Kleingruppen: Woran kann es liegen, dass ein Rechner keine Verbindung ins Internet hat, lokal aber normal arbeiten kann? Diskutieren Sie Ihre Vorschläge.
- Welche Art von IT-Management ist effizienter, proaktives oder reaktives IT-Management?
- Machen Sie sich ein Bild von der aktuellen Systemauslastung Ihres Rechners

Taskmanager starten mit der Tastenkombination	
Aktuelle CPU-Auslastung	
Aktuelle Arbeitsspeicher-Auslastung	
Aktuelle Datenträger-Auslastung	
Aktuelle Netzwerk-Auslastung	

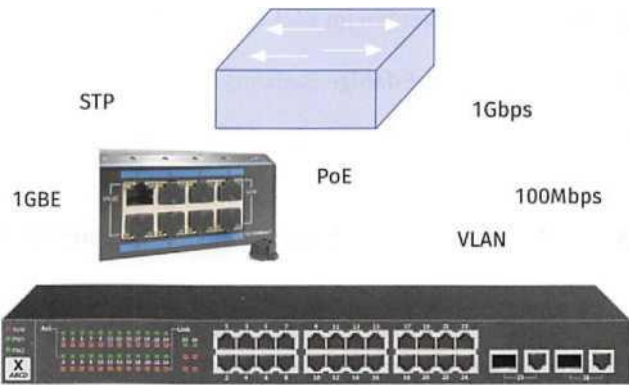
- Erzeugen Sie Rechenlast und Netzwerklast. Beobachten Sie dabei die Systemauslastung.

Taskmanager starten mit der Tastenkombination	
Aktuelle CPU-Auslastung	
Aktuelle Arbeitsspeicher-Auslastung	
Aktuelle Datenträger-Auslastung	
Aktuelle Netzwerk-Auslastung	

- Wie haben Sie die CPU-Last erhöht?
- Wie haben Sie die Netzwerklast erhöht?

TAG 11 - Netzwerkkomponenten auswählen und konfigurieren

Als Grundlage für das Verständnis der Netzwerkgeräte müssen wir uns die beiden gängigen Schichtenmodelle der Kommunikation ansehen. Denn für das Verständnis, wie die einzelnen Geräte arbeiten, sollte man wissen, was auf den einzelnen Schichten geschieht. Ebenso ist es elementar zu wissen, welche Adressen in Rechnernetzen verwendet werden und was damit adressiert wird.



LE 1 - Switch auswählen

Um den richtigen Switch einzusetzen, werden einige Eckdaten des Switches kontrolliert. Dazu muss man überprüfen, wie hoch das zu erwartende Datenaufkommen der Clients ist. Die Fähigkeiten eines Switches bestimmen auch seinen Preis.

Überprüfung Eckdaten des Switches

Größe/Bauform	→ Welche Bauform soll der Switch haben? • 19" Rack-Montage (bis 48 oder mehr Switchports) • 19" Rack-Montage (für Mini-Racks, mit bis zu 10 Switchports) • Tisch-/Wand-Gehäuse (mit 4 bis 8 Switchports)
Betriebsart	→ Switching-Funktion (Cut Through, Fragment Free, Store and Forward) einstellbar?
Datenrate	→ Welche Datenrate muss der Switch unterstützen? Wie viele Ports mit welcher Datenrate (100 Mbit/s bis 10 Gbit/s)?
PoE-Speisung	→ Muss der Switch Strom liefern für angeschlossene Geräte wie Telefone und Access Points (PSE = Power Sourcing Equipment)? Wie viele Ports müssen Speisung bringen? Welche Leistungen werden verlangt?
Managementfunktion	→ Managebare Switches sind über ein Web-Interface oder über Konsolenbefehle mittels SSH oder telnet konfigurierbar. Einstellbar ist u.a.: • VLAN-Einstellung • Port-Datenrate und halb-/vollduplex-Betriebsart • Spanning Tree (in größeren Netzen) • Mirroring (Spiegelung einzelner Ports auf einen Monitor-Port zur Fehlersuche und Netzwerküberwachung)
Größe des ARP-Speichers	→ Wie viele MAC-Adressen pro Port kann der Switch speichern (abhängig von der Größe des Netzes bzw. der Anzahl der Hosts, die an jedem Port angeschlossen werden können)?
Größe der Input- und Output-Speicher	→ Wie viel Datenverkehr ist zu erwarten? Wie viele Pakete müssen gespeichert werden, bevor sie weitergeleitet werden können?

Im Downloadbereich befinden sich einige Datenblätter von Switches zum genaueren Betrachten.

LE 2 - Router auswählen

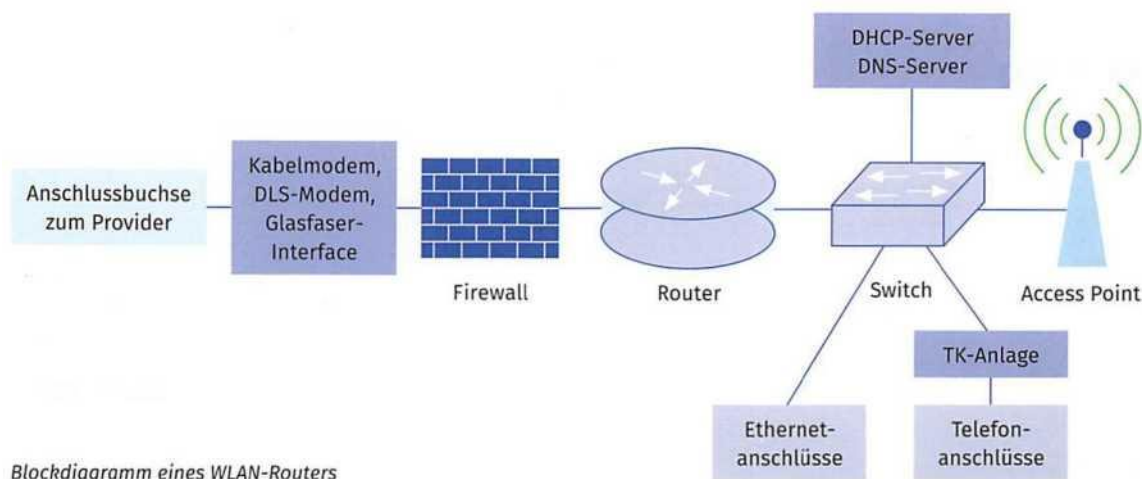
Sie sollen Router auswählen können.

Im privaten Bereich und bei kleinen Betrieben kommt es sehr auf die eingebauten Dienste der Router an. Die sog. SoHo-Router (Small Office - Home Office) stellen nicht nur die Verbindung vom LAN zum Internet her. Viele Dienste und Funktionen sind integriert.

Anschlüsse und Funktionen eines SoHo-Routers	
WAN-Anschluss	DSL-, Kabel- oder LWL-Interface zum Internetprovider
Switchports	Zwei bis fünf Ethernet-Anschlüsse für internes LAN
WLAN-Access-Point	Funknetz für Mobilgeräte (internes LAN)
DHCP-Server	Verteilt IP-Konfiguration an Clients im LAN und WLAN
TK-Anlage	Stellt Telefonanschlüsse für Internettelefonie bereit
USB-Anschluss	Zum Anschluss von USB-Massenspeicher zum Bereitstellen von Netzwerkspeicher (NAS, Network Attached Storage) für alle Rechner im LAN
Kindersicherung	Proxy-Sperrliste kann verwaltet werden für Internetseiten, die nicht angezeigt werden sollen und das Internet kann zeitlich begrenzt freigegeben und gesperrt werden
DynDNS	Anmelden des Routers bei einem Namensauflösungsdienst, damit vom Internet aus auf den internen NAS-Speicher zugegriffen werden kann
VPN	Tunnel-Endpunkt am SoHo-Router für sicheren Zugriff auf das LAN von mobilen Stationen im Internet

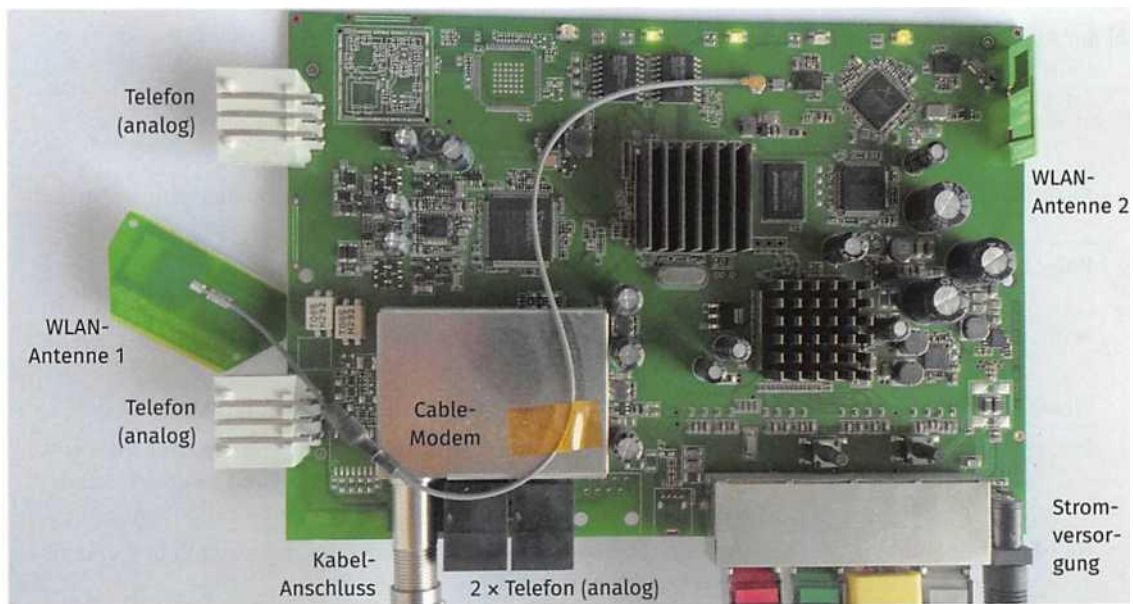
(1) WLAN-Access-Point

Jeder „normale“ Internet-Router für Privathaushalte und kleine Unternehmen hat heute eine WLAN- Funktion.



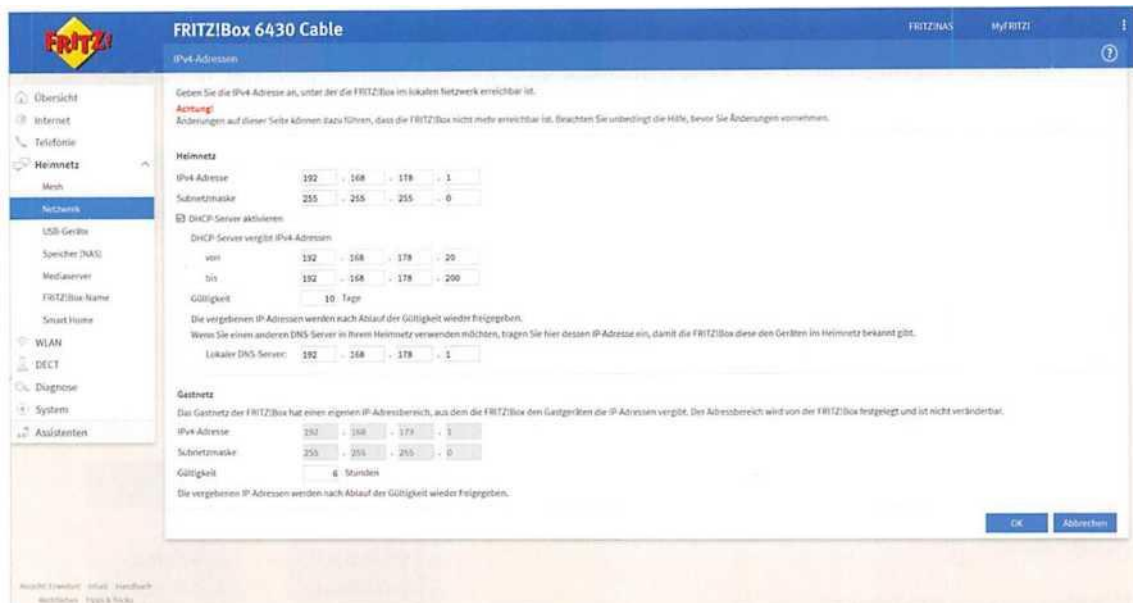
Ein solcher SoHo-Router verfügt über ein Interface zum Internet. Dies ist meist ein DLS-Modem, ein Kabelmodem oder auch ein Mobilfunk-Interface. Wenn Glasfaser im Gebäude vorhanden ist, hat der Router ein entsprechendes Glasfaser-Interface. Daran angeschlossen ist der eigentliche Router. Meist verfügt er über nur zwei Netze - das LAN und das Internet. Bessere Geräte verfügen über mehrere interne LANs. Am LAN-Anschluss des Routers befindet sich ein Switch mit Anschlussbuchsen, um PCs und andere Geräte anzuschließen. Ein WLAN-Access-Point ist meist intern mit dem LAN verbunden. Manche Geräte haben auch ein eigenes

Netz für das WLAN. Ein DHCP-Server ist immer mit integriert. Er übernimmt das Verteilen der IP-Konfigurationen an die angeschlossenen Geräte.



Innenleben einer Fritz!Box Cable

Das Bild zeigt das Innenleben einer Fritz!Box Cable. Deutlich zu erkennen sind die beiden WLAN-Antennen, das Kabel-Modem für das Kabelfernsehtz und die Telefonanschlüsse. Das Board ist ein kompletter Einplatinencomputer mit eigenem (linux-ähnlichen) Betriebssystem. Gebootet wird von einem Onboard-Flash-Speicher.



DHCP-Einstellungen eines WLAN-Routers

Der DHCP-Server ist so eingestellt, dass die Router nach dem Einstecken schon richtig funktionieren. Man kann aber die IP-Einstellungen beliebig verändern.

WLAN benutzt im Wesentlichen zwei Frequenzbereiche: 2,4 GHz und 5 GHz. Jeder Bereich ist in mehrere sich überlappende Frequenzkanäle eingeteilt. Am einfachsten ist es, man überlässt dem Access Point die Auswahl des Frequenzkanals. Dann wird, abhängig von der Kanalbelegung der Nachbar-WLANs, immer der beste Kanal ausgewählt.

Bei der Auswahl eines SoHo-Routers sind folgende Punkte zu beachten:

Auswahl eines SoHo-Routers		
Anzahl der LAN-Ports	→	Sind mehr Geräte anzuschließen, als Ports vorhanden sind, muss ein zusätzlicher Switch eingesetzt werden.
PoE-Speisung möglich	→	Wenn Netzwerktelefone angeschlossen werden sollen, können diese über PoE stromversorgt werden.
WLAN-Leistung	→	Die Leistung und die Empfindlichkeit bestimmen, wie die Reichweite für Mobilgeräte ist.
WLAN-Technologie	→	Beherrscht der Router die aktuellen WLAN-Standards?
DSL Vectoring	→	Beherrscht der DSL-Anschluss Supervectoring? Wenn der Internet-provider jetzt schon oder erst später Vectoring und eventuell Super-vectoring anbietet, dann sollte der Router das beherrschen.
NAS-Funktionalität	→	Lassen sich USB-Massenspeicher an den Router anschließen und als Netzwerkspeicher nutzen?
Kindersicherung aktivierbar	→	Lassen sich einschlägige Internetseiten für den Zugang sperren? Lässt sich der Internetzugang zeitlich begrenzen?

WLAN-Technologie ist bereits seit dem Jahr 1999 verfügbar und hat seither einige Entwicklungen durchgemacht. Die Bezeichnungen waren mit der Zeit etwas unübersichtlich. Daher wurden neue Bezeichnungen eingeführt. In Anlehnung an HiFi (High Fidelity) nennt man es nun Wi-Fi.



Bezeichnungen		Sendefrequenz	Max. Datendurchsatz	Bemerkungen
alt	neu			
802.11	Wi-Fi 1	5 GHz	2 Mbit/s	
802.11b	Wi-Fi 2	2,4 GHz	11 Mbit/s	
802.11g	Wi-Fi 3	2,4 GHz	54 Mbit/s	
802.11 n	Wi-Fi 4	2,4 und 5 GHz	72-600 Mbit/s	
802.11ac	Wi-Fi 5	5 GHz	433-6933 Mbit/s	
802.11ad	Gigabit-WLAN	60 GHz	Bis 6930 Mbit/s	Max. 10 m Reichweite wegen der hohen Dämpfung der Sendefrequenz
802.11ax	Wi-Fi 6	Freie ISM-Bänder von 1 bis 6 GHz	600-9 608 Mbit/s	
802.11ay	Wi-Fi 6E	Wie Wi-Fi6	600-9 608 Mbit/s	Zusätzliche Kanäle bei 6 GHz

(2) Professionelle Router

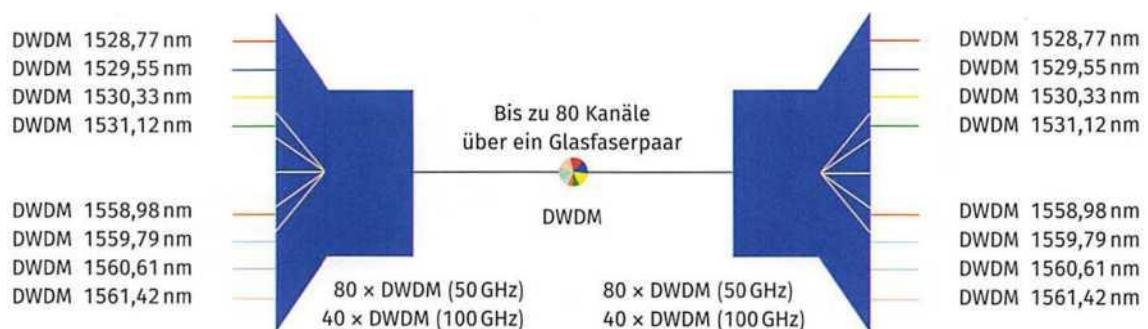
Im professionellen Umfeld kommen leistungsfähige und damit auch teure Router für 19" Rack-Montage zum Einsatz. Die Auswahl erfordert genaue Kenntnis der Produkte und Anforderungen. Hier spielt auch die Anbindung ans Internet eine große Rolle. Viele Funktionen, die bei SoHo-Router integriert sind, fehlen hier. Diese Dienste werden durch dedizierte Geräte und Server erbracht. Die Konfiguration erfolgt meist durch ssh-Zugriff, also Konsolenbefehle über eine verschlüsselte Verbindung. Das kalifornische Unternehmen Cisco Systems ist ein sehr großer Anbieter von Netzwerkgeräten wie Router und Switches. Auf diesen Geräten läuft ein eigenes, linux-ähnliches Betriebssystem, das Internetwork Operating System (IOS). Über Befehle an der Kommandozeile lassen sich alle Einstellungen tätigen. Das bedeutet, dass diese Befehlsfolgen auch als Skript abgearbeitet werden können. Damit lassen sich größere Mengen an Geräten sehr schnell und einfach einrichten. Viele andere Hersteller haben ähnliche Kommandos zum Konfigurieren ihrer Geräte. Durch den Verzicht auf eine graphische Oberfläche werden Rechenleistung und Netzwerkdatenverkehr eingespart.

Ein ausgiebiger Blick in die Datenblätter ist hier angebracht. Im Downloadbereich befinden sich einige Datenblätter von Routern zum genaueren Betrachten.

LE 3 - Neue Entwicklungen und Trends präsentieren

Die Entwicklungen in der IT gehen rasant vorwärts. Laufend kommen neue Techniken hinzu. Sie müssen sich lebenslänglich informieren und weiterbilden. Beispielsweise wird die Datenrate bei Lichtwellenleitern durch neue Entwicklungen immer weiter erhöht.

Wellenlängenmultiplex wird seit vielen Jahren bei Glasfaserleitungen eingesetzt. Dabei wird für jeden Übertragungskanal eine Lichtquelle mit eigener Wellenlänge verwendet. Viele solcher Kanäle werden über eine einzige Faser übertragen und am Faserende wieder in einzelne Wellenlängenkanäle aufgeteilt. Die grobe Aufteilung (CWDM = Coarse Wavelength Division Multiplex) ist bestens etabliert. Hierbei werden bis zu 16 Kanäle gleichzeitig über eine Faser übertragen.



Die Entwicklung des Dense Wavelength Division Multiplex (DWDM) schreitet laufend weiter voran. Derzeit sind bis zu 160 Kanäle auf einer Faser möglich - in Zukunft auch mehr.

Bei Kupferleitungen und auch bei Funkverbindungen kommen immer komplexere Codierungsverfahren für höhere Spektrale Effizienz zu Einsatz. Das heißt, dass der Informationsgehalt (= Anzahl der Bits) je Symbol, welches gesendet wird, laufend erhöht wird. Bei DSL werden aktuell pro Hertz Bandbreite (also pro Sinus-Vollwelle) 15 Bit übertragen.

Lernzielkontrollen TAG 11

1. Welche Daten werden im RAM eines Switches gespeichert?
2. Wozu werden PoE-fähige Switches benötigt?
3. Was ist richtig, was ist falsch?
 - a. Switches werden im Internet eingesetzt und verbinden Netzwerke.
 - b. 19-Zoll-Switches verfügen immer über PoE-Speisung.
 - c. Der RAM eines Switches begrenzt die ARP-Tabelle (Weiterleitungstabelle).
 - d. Ein Switch wertet IP-Adressen aus.
 - e. Jeder Switch kann VLANs aufbauen.
 - f. Switch ist ein anderer Ausdruck für Hub.

- g. Router und Switches werden in LANs eingesetzt.
 - h. Switches haben vordefinierte, universelle Weiterleitungstabelle.
 - i. Nach dem Einschalten eines Switches ist die ARP-Tabelle leer und füllt sich im Laufe der Zeit.
 - j. Switches sind nach dem Einschalten im „learning-Mode“ und lernen erst die MAC-Adresse der angeschlossenen Rechner.
 - k. Das „Hochfahren“ eines professionellen Switches kann mehrere Minuten dauern.
 - l. Die Switchports (Netzwerkbuchsen eines Switches) werden fest auf eine Datenrate eingestellt.
 - m. Ein Switch wertet MAC-Adressen aus.
 - n. Switches arbeiten auf OSI-Schicht 1.
 - o. Ein SoHo-Router (z.B. FritzBox) hat einen integrierten Switch.
4. Switches unterscheiden sich sehr voneinander durch ihre unterschiedlichen Leistungskriterien. Diese wiederum schlagen sich im Preis nieder.
1. Welche Kriterien müssen bei der Auswahl eines Switches berücksichtigt werden? Ergänzen Sie jeweils passend Beschreibungen/ Bemerkungen, vergleichen und besprechen Sie Ihre Ergebnisse. Ergänzen Sie auch Kriterien, die nicht aufgelistet sind.

Kriterium	Beschreibung/ Hinweise zum Einsatz
Anzahl der Ports	Anzahl der Geräte, die angeschlossen werden können
Datenrate der Ports	
Welche Netzwerkmedien werden unterstützt?	
Größe des Pufferspeichers	
Größe der MAC-Tabelle	
Ist der Switch managebar?	
Port-Aggregation/ Trunking möglich	
VLAN möglich	
VLAN-Zuordnung nach 802.1x	
Spanning Tree	

2. Recherchieren Sie im Internet bei den großen Hardwareherstellern und einschlägigen Fachhändlern nach dem derzeitigen Leistungsstand der Switches:
- 1. Welcher Hersteller ist derzeit Marktführer?
 - 2. Welche Features bei Switches werden am meisten propagiert?
 - 3. Wie groß ist die Preisspanne bei 5-Port-Switches?
 - 4. Wie groß ist die Preisspanne bei 48-Port-Switches?
5. Was ist wahr, was ist falsch?
- a. Ein Accesspoint ist immer ein Router.
 - b. WLAN benutzt Frequenzbänder bei 2,4 MHz.
 - c. WLAN benutzt Frequenzbänder bei 5 GHz.
 - d. WLAN benutzt Frequenzbänder bei 60 GHz.
 - e. IOS ist ein Betriebssystem für Router.
 - f. SoHo-Router werden meist mit einem Linux-Betriebssystem betrieben.
6. Wie hoch ist die spektrale Effizienz bei DSL?
7. Welche Multiplex-Technik wird bei Lichtwellenleitertechnik verwendet?
8. Recherchieren Sie im Internet, wie weit die Lichtwellenleitertechnik fortgeschritten ist.
- a. Wie viele Kanäle sind derzeit mit Wellenlängenmultiplextechnik gleichzeitig über einzelne Fasern möglich?
 - b. Wie groß ist dabei die maximale Datenrate?
 - c. Wie lang ist die weltweit längste LWL-Strecke ohne Verstärker?

TAG 12 und TAG 13 - Grundlagen der Daten- und Netzwerksicherheit beschreiben

Sie erarbeiten sich die Grundlagen der Datensicherheit. Sie schützen sich vor Datenverlust und stellen verloren gegangene Daten wieder her. Sie schützen Ihre Daten vor Manipulation und Diebstahl.

Datensicherheit ist die Sicherung der Daten gegen unberechtigte Zugriffe. Ebenso geht es um die Unveränderlichkeit der Daten und das dauerhafte Speichern der Daten.



Facetten der Daten- und Netzwerksicherheit		
RAID	Festplattenverbund (RAID = Redundant Array of Independent Discs); Genormt sind verschiedene RAID-Level (0 bis 6). Bei RAID werden mehrere Festplatten zusammengeschaltet. Sie erscheinen zum Rechner hin wie eine einzige Festplatte. Das Zusammenschalten soll die Schreib- und Lesegeschwindigkeit erhöhen und (ab Level 1) auch die Verfügbarkeit der Daten erhöhen.	
Backup	Sicherung der Massenspeicher auf einen anderen Datenträger, sodass die Daten bei Datenverlust (Löschen/Überschreiben von Dateien, Verlust der Daten, Defekt oder äußere Einflüsse) wiederhergestellt werden können.	
Bandsicherung	Backup auf Magnetband	
Cloud-Backup	Backup auf Online-Datenspeicher	
Proxy	„Stellvertreter“; ein Rechner, der stellvertretend für die Arbeitsplatzrechner auf das Internet zugreift. Oft mit Zwischenspeicher ausgestattet, um bei einem erneuten Aufruf von Internetinhalten diese sehr schnell aus diesem Cache zu liefern und Internetdatenverkehr zu minimieren. In kleinen Netzen ist der Proxy oft auf dem Internetrouter integriert. In größeren professionellen Netzen werden separate Proxys mit aufwendigen Filterlisten eingesetzt.	
Firewall	„Feuerwand“ zwischen internem und externem Netz, „Wächter am Tor“; unerwünschte Daten werden nicht durchgelassen, Angriffe abgeblockt.	
DMZ	Demilitarisierte Zone; Netz zwischen zwei Firewalls, zwischen Internet und LAN	
Schutzbedarfs-analyse	Durch systematische Analyse der gesamten IT werden der notwendige Schutz für die eigenen Daten erkannt und entsprechende Schutzmechanismen erarbeitet (siehe Kapitel 4).	

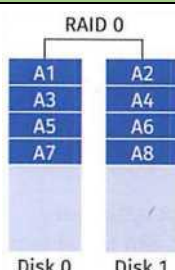
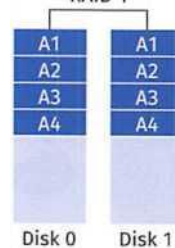
Facetten der Daten- und Netzwerksicherheit	
Zugriffsrechte/Berechtigungen	Welcher Benutzer und welche Gruppe dürfen auf welche Daten und Ressourcen zugreifen?
Zugangskontrolle	Wer hat Zugang zum Netzwerk? Dies beinhaltet den logischen Zugang durch Login ins Netz (Passwortsicherheit!) und den physischen Zugang zum Netz und Netzwerkkomponenten (z. B. Zutritt zum Rechenzentrum, Zugang/Zugriff auf Verteiler, Switches, Arbeitsplatzrechner).
Leitungscode	Durch Codieren der Daten auf den Leitungen werden Fehler bei der Übertragung minimiert.
„Faktor Mensch“	Menschliches Versagen und menschliche Schwächen stellen ein großes Problem (vielleicht sogar das größte Problem) bei der Datensicherheit dar.

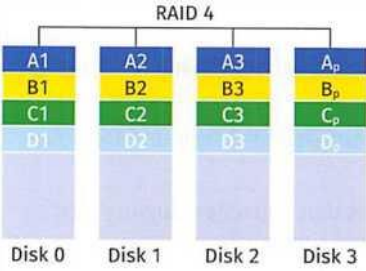
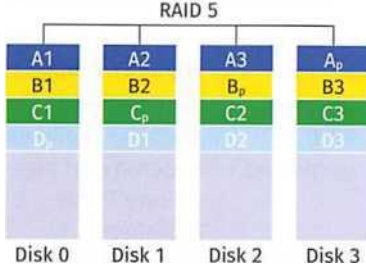
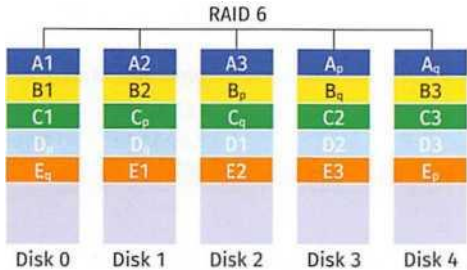
LE 1 - RAID-Systeme unterscheiden

Sie sollen RAID-Systeme unterscheiden können.

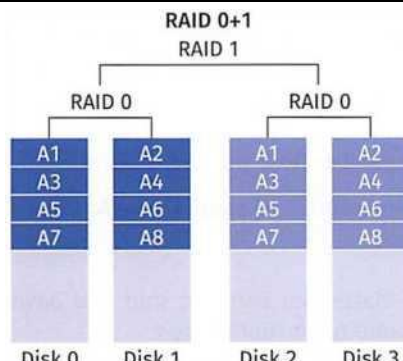
Redundant Array of Independant Discs (RAID) steht für redundantes Festplattenarray. Dabei werden zwei oder mehr Festplatten zusammengeschaltet und erscheinen systemseitig wie eine einzige Platte. Der Vorteil liegt darin, dass die Daten gleichzeitig von mehreren Platten gelesen werden können, wodurch sich die Ladezeit deutlich verringert. Ebenso erhöht sich der Datendurchsatz beim gleichzeitigen Schreiben auf mehrere Platten. Durch Hinzufügen von Prüfsummen zu den Daten (hier Parität genannt) kann für Ausfallsicherheit gesorgt werden.

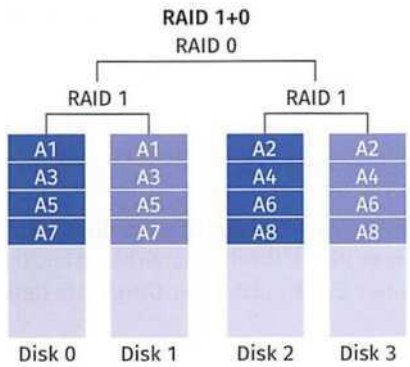
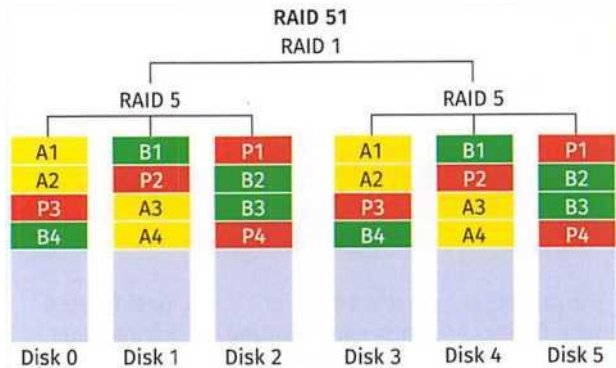
RAID-Systeme werden in Levels eingeteilt, abhängig von Funktionsprinzip. Genormt sind die Levels 0 bis 6.

Die wichtigen RAID-Level im Überblick			
Level	Alternative Bezeichnung	Beschreibung	Sicherheit
 RAID 0 Disk 0 Disk 1	Stripe Set	Beliebig große Festplatten oder Partitionen werden zu einem Volume zusammengeschaltet. Daten werden auf mehrere Platten verteilt; höhere Datenraten beim Lesen und Schreiben.	Keinerlei Sicherheit, bei Ausfall von einer Platte ist das gesamte Volume beschädigt.
 RAID 1 Disk 0 Disk 1	Mirroring	Zwei Platten werden miteinander gespiegelt. Einfache Lesegeschwindigkeit, doppelte Schreibgeschwindigkeit.	Eine Platte kann ausfallen ohne Datenverlust.

Die wichtigen RAID-Level im Überblick			
Level	Alternative Bezeichnung	Beschreibung	Sicherheit
 RAID 4 Disk 0 Disk 1 Disk 2 Disk 3	Stripe Set with Parity	Mindestens drei Platten im Verbund. Eine Platte ist die separate Paritätsplatte. Die Paritätsplatte wird stark beansprucht, da sie beim Schreiben auf jede einzelne Platte beschrieben wird.	Eine Platte kann ausfallen ohne Datenverlust.
 RAID 5 Disk 0 Disk 1 Disk 2 Disk 3	Stripe Set with Parity	Mindestens drei Platten im Verbund. Die Parität der Paritätsplatte wird auf alle Platten verteilt, damit alle Platten gleichmäßig beansprucht werden.	Eine Platte kann ausfallen ohne Datenverlust.
 RAID 6 Disk 0 Disk 1 Disk 2 Disk 3 Disk 4	Stripe Set with Parity	Mindestens vier Platten im Verbund, davon zwei Platten für verteilte Prüfsummen.	Zwei Platten können ausfallen ohne Datenverlust.

Daneben gibt es noch Kombinationen von mehreren RAID-Systemen. RAID 10 ist ein Stripe Set (RAID 0) von zwei Spiegelsystemen (RAID 1). RAID 51 ist eine Spiegelung (RAID 1) von zwei RAID-5-Systemen. Dies liefert sehr hohe Sicherheit vor Datenverlust. Die erste Zahl gibt die RAID-Zusammenschaltung der einzelnen Platten zu einem RAID-Subsystem an. Die zweite Zahl steht für das Zusammenschalten der RAID-Subsysteme.

RAID-Systeme			
Level	Bezeichnung	Beschreibung	Sicherheit
 RAID 0+1 RAID 1 RAID 0 RAID 0 Disk 0 Disk 1 Disk 2 Disk 3	RAID 01	Zwei RAID 0 werden mit einem RAID 1 gespiegelt.	Jedes RAID 0 hat doppelte Ausfallwahrscheinlichkeit. Durch die Spiegelung darf ein RAID 0 ausfallen.

RAID-Systeme			
Level	Bezeichnung	Beschreibung	Sicherheit
	RAID 10	Zwei Spiegelsysteme mit je zwei Platten werden über RAID 0 zusammengeschaltet	In jedem RAID 1 darf eine Platte ausfallen, ohne Datenverlust. Fallen 2 Platten in einem RAID 1 aus, sind alle Daten verloren.
	RAID 51	Zwei RAID-5-Systeme werden über ein RAID 1 gespiegelt.	Extrem hohe Ausfallsicherheit; ein RAID-5-Block kann komplett ausfallen, bei dem anderen darf eine weitere Platte ausfallen. Im gezeigten Beispiel werden sechs Platten verbaut. Man nutzt aber nur die Kapazität von zwei Platten.

RAIDs lassen sich mit Hardware-Controllern herstellen oder per Software vom Betriebssystem.

Hardware-RAID

Eine Erweiterungskarte auf dem Mainboard verfügt über mehrere Festplattenanschlüsse. Die RAID- Funktionen werden auf spezialisierter Hardware bereitgestellt. Die Erweiterungskarte wird vom Betriebssystem wie eine einzige Festplatte gesehen. Vorteile sind die hohe Geschwindigkeit und meist ein zusätzlicher Festplattencache. Nachteil sind die Kosten für den Controller.

Software-RAID

Software-RAID-Systeme lassen sich mit vielen Betriebssystemen herstellen. Voraussetzung ist, dass der Rechner über genügend Festplattenanschlüsse verfügt. Software-RAIDs gehen zulasten der CPU-Leistung, die dem Rechner für seine normalen Aufgaben fehlt. Der Vorteil sind die Kosten, da ein Software-RAID keinen zusätzlichen Controller benötigt.

Neuere Bezeichnungen von RAID-Systemen nennen nicht mehr einen RAID-Level, sondern die Anzahl der benutzten Platten und der Parity-Platten.

Beispiel: RAID (5,2) oder RAID 5+2 bedeutet, dass insgesamt fünf Platten im Verbund sind und davon maximal zwei Platten ausfallen dürfen. Dies entspricht also einem RAID 6 mit fünf Platten.

Die allgemeine Bezeichnung ist: RAID (n,m) oder RAID n+m, wobei n = Anzahl Platten gesamt angibt und m = Anzahl Platten, die ohne Datenverlust ausfallen dürfen.

Die Leserate (Datendurchsatzrate) gesamt ergibt sich = $n \cdot \text{Leserate Einzelplatte}$.
 Schreibrate gesamt ist = $(n - m) \cdot \text{Schreibrate Einzelplatte}$.
 Die Gesamt-Speicherkapazität des RAID-Systems ist = $(n - m) \cdot \text{Einzelkapazität}$.

Beispiel: Ein RAID 5 besteht aus vier Platten zu je 1 TByte Kapazität. Die Gesamtkapazität ist die Summe der Kapazität von drei Platten, also 3 TByte, da die Kapazität von einer Platte für die Sicherheit benötigt wird. Der Datendurchsatz beim Lesen ist viermal so groß wie bei einer Einzelplatte. Der Durchsatz beim Schreiben ist dreimal so groß wie bei einer Einzelplatte.

Manche RAID-Controller bieten ein spezielles Feature, nämlich den Einbau von Hot-Spare-Platten. Dabei werden mehr Platten angeschlossen, als das RAID benötigt. Eine oder mehrere Platten sind dabei zusätzlich verbaut und angeschlossen. Erkennt der RAID-Controller, dass eine Platte defekt ist, wird automatisch eine dieser Reserveplatten in den RAID-Verband integriert und die fehlenden Daten werden aus den vorhandenen Daten berechnet und auf diese Reserveplatte geschrieben. Während dieser Zeit sind die Zugriffszeiten auf das RAID etwas höher. Nach der Reorganisation des RAID-Verbandes läuft das System wieder mit voller Geschwindigkeit.

Oft liest man im Zusammenhang mit RAID-Controllern die Begriffe „JBOT“ oder „NRAID“. Beides sind nur Zusammenschaltungen (Concatenations) von mehreren Platten (auch unterschiedlicher Größe). Sie bringen keinen Sicherheitsgewinn, da jegliche Redundanz fehlt. JBOT ist die Abkürzung für „Just a Bunch of Disks“, also etwa: „nur ein Haufen Platten“. NRAID steht für „NotRAID“. Solche Systeme verbinden mehrere Platten zu einer größeren virtuellen Festplatte. Allerdings werden die Daten nicht auf die Platten verteilt, sondern die Platten werden einfach der Reihe nach gefüllt. Man hat dadurch auch keinen Geschwindigkeitsvorteil.

LE 2 - Backupstrategien unterscheiden

Sie sollen Backupstrategien unterscheiden.

Laut Datenrettungsunternehmen ist die Hauptursache für Datenverlust zu 72 % ein Festplattencrash. Immerhin 15% der Datenverluste entfallen auf RAID-Systeme und 13% auf SSD-Platten. 66% sind technische Defekte. Rund ein Drittel der Datenverluste sind menschliches Versagen, z. B. durch versehentliches Löschen von Daten oder Formatieren von Datenträgern.

Daten sind auf Rechnern mit RAID-Systemen zwar relativ sicher, dennoch droht laufend Datenverlust. Hier hilft nur das Sichern der Daten auf andere Server (im LAN, Off-Premises oder in einer Cloud) oder auf Magnetbänder. Ein Großteil der Unternehmen, die ihre Daten verlieren und nicht wiederherstellen können, geht innerhalb weniger Monate nach Datenverlust in Konkurs. Datensicherung ist somit ein wichtiger, sogar überlebenswichtiger Punkt.

Egal wie die Daten gesichert werden - von größter Wichtigkeit ist der ausgiebige Test des Sicherns und des Rücksicherns. Testen Sie, wenn Sie die Datensicherung einrichten, dass Sie genau diese Daten auch wiederherstellen können.

Möglichkeiten der Datensicherung		
Bezeichnung	Beschreibung	Anwendung
Off-Premises Backup	Daten auf ein anderes Datacenter kopieren	Sinnvoll bei Betrieben, die über mehrere Niederlassungen mit zwei oder mehr Rechenzentren verfügen
Bandsicherung	Daten auf Band sichern	Sinnvoll für Betriebe mit nur einer Niederlassung
Cloud-Backup	Daten auf einen Cloud-Speicher im Internet kopieren	Praktikabel für Betriebe jeder Größenordnung

(1) Off-Premises Backup

Verfügt ein Betrieb über mehrere Niederlassungen mit mindestens zwei Rechenzentren, so können die Daten auf das jeweilige andere Datacenter kopiert oder gespiegelt werden. Die Datacenters sollten aber mindestens 3 km voneinander entfernt sein, damit eine Katastrophe an einem Standort nicht auch den zweiten Standort betrifft. Dies ist auch für sehr große Datenmengen eine praktikable Lösung.

(2) Bandsicherung

Ein Bandroboter greift sich aus hunderten von Bandkassetten maximal vier und steckt sie in Bandlaufwerke. So werden Daten automatisch gesichert und können nach Bedarf wieder zurückgesichert werden.



Bandroboter der Österreichischen Mediathek

Der Bandroboter in der Abbildung sichert die Audiodateien der Österreichischen Mediathek.

Kleinere Unternehmen speichern ihre Daten auf einem einzigen Magnetband, welches täglich gewechselt wird.

Über den Bandwechsel muss man sich Gedanken machen. Immer dasselbe Band zu beschreiben ergibt wenig Sinn, wenn ältere Dateien wiederhergestellt werden sollen. Ein mögliches Schema sieht so aus:

Beispiel:

Vier Tagesbänder, Montag bis Donnerstag, die wöchentlich überschrieben werden (Mo., Di., Mi., Do.) Vier Wochenbänder, die immer freitags überschrieben werden (Fr1, Fr2, Fr3, Fr4) Zwölf Monatsbänder, die immer am letzten Freitag des Monats überschrieben werden

Schutz vor Zerstörung

Die Bänder sind außerhalb des Serverraumes in einem Safe aufzubewahren. Ein Feuer im Rechenzentrum darf die Bänder nicht zerstören. Am besten werden sie in einem anderen Gebäude, weit entfernt vom Rechenzentrum aufbewahrt. Monatssicherungen liegen am besten im Safe einer Bank!

(3) Backup auf Cloud-Speicher

Speichern in der Cloud wird immer einfacher, preiswerter und beliebter. Man bucht bei einem Anbieter Speicherplatz und greift übers Internet darauf zu. Die Kosten sind moderat, und man muss sich um vieles nicht mehr kümmern. Schutz vor Datenverlust des Cloud-Speichers, Wartung der Server, der Klimaanlage, der Stromversorgung usw. wird alles vom Cloud-Anbieter übernommen.

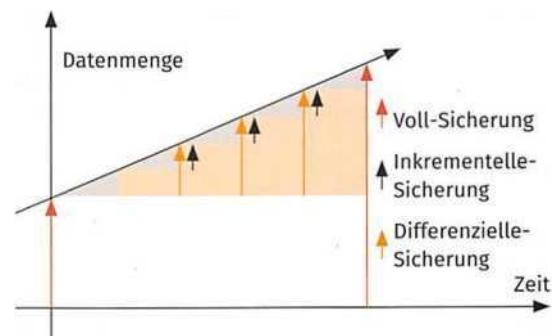
Vor Vertragsabschluss mit Cloud-Anbieter

Wie ist die Verfügbarkeit?	→ Eine Verfügbarkeit von 99,9% bedeutet eine Ausfallzeit von 0,1 %. Das sind fast vier Tage pro Jahr!
Wie sind die Auswirkungen, wenn der Cloud-Speicher nicht verfügbar ist?	→ Kann ohne Cloud-Speicher noch im LAN gearbeitet werden?
Wie lange dauert es, bis verlorene Daten wiederhergestellt sind?	→ Die Recoverytime kann mitunter sehr lange sein. Welche Wartezeit ist tolerierbar?
Wo liegen die Daten physikalisch?	→ Liegen die Daten in Deutschland, der EU oder außerhalb? Welche rechtlichen Regelungen gelten dort? EU-Datenschutzrecht gilt weder in USA noch in Russland.
Sind die Daten vor Fremdzugriff sicher?	→ Wer hat Zugriff auf die internen Daten? Bin ich sicher vor Industriespionage (auch staatlich unterstützte Spionage) oder gar Sabotage und Datenmanipulation?

Sicherungsarten

In jedem Betrieb, in dem gearbeitet wird, werden täglich Daten erzeugt und gespeichert.

Die nebenstehende Zeichnung zeigt den Anstieg des Datenvolumens. Die Unterschiede der verschiedenen Sicherungsarten werden hier deutlich.



Möglichkeiten der Datensicherung	
Bezeichnung	Beschreibung
Speicherabbild-Backup, Image-Backup	Alle Datenblöcke einer Festplatte werden gespeichert, unabhängig vom Inhalt. Dadurch wird das Dateisystem mit gesichert. Auch gelöschte Dateien, die physisch noch auf der Platte gespeichert sind, werden gesichert. Diese Backups werden von Ermittlungsbehörden auch in der Computer-Forensik verwendet.
Voll-Backup, Komplettsicherung	Alle Dateien einer Platte werden gesichert.
Differenzielles Backup	Alle Dateien, die sich seit der letzten Vollsicherung geändert haben, werden gesichert. Geänderte Dateien sind auf jedem Backup enthalten. Zum Rücksichern wird nur die letzte differenzielle Sicherung oder das letzte Vollbackup benötigt. Das Datenvolumen der Sicherung wächst stetig, ebenso die Backup-Zeit.

Möglichkeiten der Datensicherung	
Bezeichnung	Beschreibung
Inkrementelles Backup	Alle Dateien, die sich seit der letzten Vollsicherung oder inkrementellen Sicherung geändert haben, werden gesichert. Es sind nur die Dateien seit der letzten Teilsicherung auf einem Band. Beim Rücksichern werden daher alle Bänder benötigt. Viele Bänder mit relativ wenig Daten werden benötigt, die Backupzeit bleibt kurz.

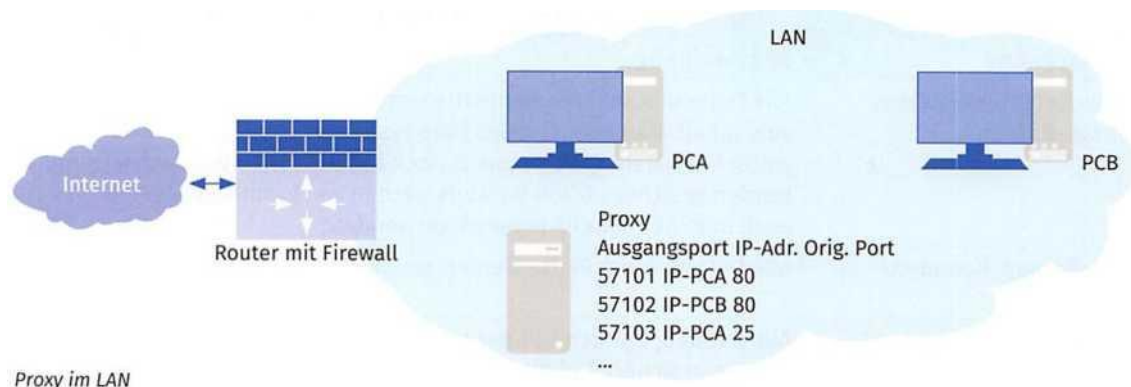
LE 3 - Netzwerksicherheit herstellen

Sie sollen Netzwerksicherheit herstellen.

Die Netzwerksicherheit spielt eine wichtige und immer wichtiger werdende Rolle in jedem Computernetz. Eindringlinge, die versuchen vom Internet aus in Unternehmensnetze einzudringen, um Daten zu stehlen, sind heute keine Seltenheit mehr. Ein anderer Ansatz von Kriminellen ist, dass ganze Festplatten verschlüsselt werden, der Betroffene keinen Zugriff auf seine Daten mehr hat, um dann Lösegeld zu erpressen für das Freischalten der „gekidnapten“ Daten.

(1) Proxy

Ein Proxy ist ein Stellvertreter. Im Netzwerk geht dieses Gerät stellvertretend für die einzelnen Rechner ins Internet. Das heißt, eine Anfrage von einem PC ins Internet, um dort eine beliebige Seite zu besuchen, geht nicht vom PC direkt ins Internet. Diese Anfrage geht an den Proxy im Netz und dieser schickt die Anfrage weiter ins Internet. Antworten werden vom Internet an den Absender der Anfrage, also den Proxy geschickt. Dieser schickt die Antwort dann weiter an den PC, der ursprünglich angefragt hatte.



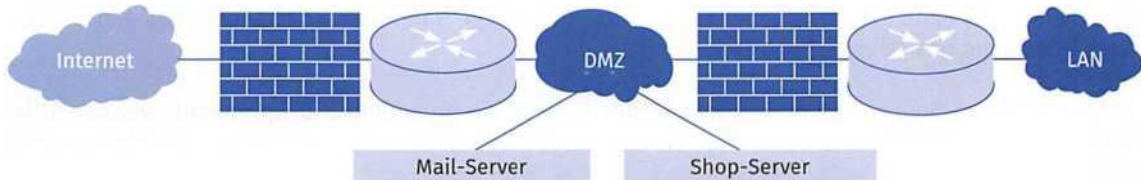
Aber wozu dieser Umweg? Auf dem Proxy lassen sich Sperrlisten einrichten für Seiten, die nicht besucht werden dürfen. Hiermit kann man beispielsweise verhindern, dass in einem Betrieb von den Arbeitsplatzrechnern aus Filme angeschaut, Aktien gehandelt oder pornografische Seiten aufgerufen werden können. Internetseiten mit dubiosem Inhalt, die als Virenschleudern bekannt sind, können ebenso geblockt werden. Weiterhin sind Proxys meist mit einem Speicher ausgestattet, um Internetseiten zu speichern. Das typische Surfverhalten der User zeigt, dass einmal aufgerufene Seiten häufig später wieder aufgerufen werden. Wird nun eine Seite aufgerufen, die vorher schon einmal aufgerufen wurde, so befinden sich diese Daten im Speicher vom Proxy und können sehr schnell direkt vom Proxy ausgeliefert werden, ohne erneut ins Internet zu gehen. Ein Proxy spart somit zum einen Datenverkehr mit dem Internet und er beschleunigt zum anderen das Surfen.

In kleinen Netzen ist der Proxy im Internetrouter integriert. Dabei allerdings meist ohne die Speicherfunktion oder mit sehr kleinem Speicher. Unternehmensnetze verfügen meist über einen eigenen Proxy-Server, der sich im Serverraum oder Rechenzentrum befindet und alle oben genannten Funktionen erfüllt. Ein wichtiger Aspekt bei dieser Proxy-Technik ist der, dass von außen nicht die einzelnen Rechner sichtbar sind, sondern nur ein einziger, nämlich der Proxy. Er muss, um diese Aufgabe zu erfüllen, die Datenpakete auf OSI-Layer 3 verändern. Er tauscht die Absender-IP-Adresse aus und ersetzt sie durch seine. Pakete aus dem Internet, allesamt an ihn adressiert, inspiziert er wieder und ersetzt die Ziel-IP-Adresse (seine!) durch

die des ursprünglichen PCs, der die Anfrage ins Internet geschickt hat. Dazu muss der Proxy eine Liste führen, welcher PC mit welchem externen Rechner eine Datenverbindung hat.

(2) Firewall/DMZ

Eine Firewall ist eine Schutzwand, die Beschuss von außen abwehrt und das Netzwerk oder einen Rechner vor Angriffen schützt. Sie befindet sich am Übergang vom LAN zum Internet. Eine Firewall inspiziert die ankommenden Pakete nach vorher festgelegten Regeln. Es gibt verschiedene Firewall-Typen, abhängig davon, wie tief sie die Pakete inspizieren und wo sie installiert sind.



DMZ als Zwischennetz zwischen LAN und Internet

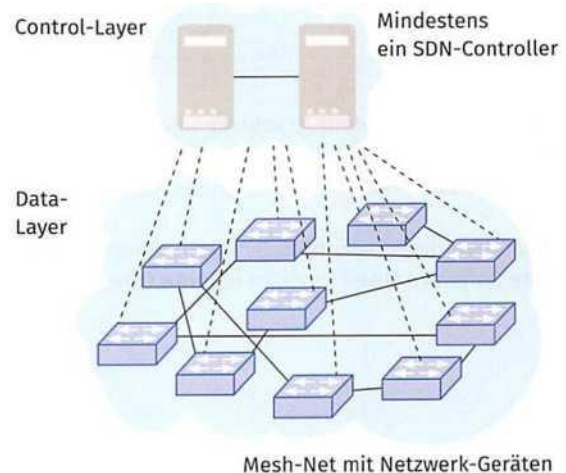
Eine einfache Firewall ist die Personal Firewall oder Desktop-Firewall, die auf einem Desktop-PC läuft und nur einfache Schutzmechanismen bietet. Die externen Firewalls sind zentral in einem Netzwerk befindliche Rechner, über die der gesamte Datenverkehr mit der Außenwelt abgewickelt wird. Einfache externe Firewalls inspizieren nur die Herkunft der ankommenden Pakete anhand der IP-Adresse. Bessere überprüfen die IP-Adresse und die TCP- und UDP-Ports und somit die Anwendungen. Pakete, die auf nicht geöffnete Ports treffen, werden nicht durchgelassen (analog zu einer verschlossenen Tür). Die aufwendigste Art der Firewall überprüft auch den Inhalt der ankommenden Pakete. Befinden sich nicht erwünschte Inhalte darin, werden die Pakete nicht durchgelassen.

(3) Software Defined Network

Ein Trend geht zur Flexibilisierung des Netzwerkes. Bisher werden Netzwerke mit Switches und Routern fest verkabelt. Sie sind starr und unflexibel. Die Netzwerkstruktur reagiert nicht auf sich ändernde Datenflüsse und Anforderungen.

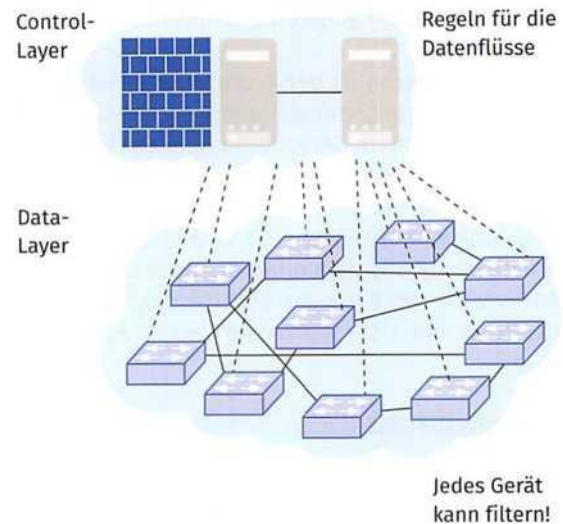
Abhilfe schafft hier das Software Defined Networking (SDN). Die SDN-Switches sollen künftig außergewöhnlich preiswert werden und auf eigene Logik verzichten. Sie ersetzen die bisherigen Switches und Router.

Dynamisiert wird das Ganze durch einen oder mehrere Controller. Dies sind Rechner, die das Regelwerk für das Gesamtnetz verwalten. Die Weiterleitungstabellen werden durch Weiterleitungsregeln ersetzt. Diese können in ihrer Mächtigkeit weit über das hinausgehen, was bisher mit Netzwerken möglich war.



Die SDN-Switches sind redundant vernetzt (Maschentopologie) und bilden das Data-Layer. Darüber befindet sich das Control-Layer mit den SDN- Controllern.

Trifft ein Datenpaket bei einem SDN-Switch ein, schaut der Switch nach, ob er eine dafür passende Regel hat. Wenn nicht, wird der Controller nach der Regel für dieses Paket gefragt. Ausgeklügelte Regeln sind machbar und verleihen dem SDN-Netz eine völlig neue Dynamik. Bestimmte Leitungen oder bestimmte Knoten im Netz können gezielt umgangen werden. Mehrere Leitungen können lastabhängig gebündelt werden. VLAN-Zuordnungen können ebenso dynamisch gestaltet werden wie Filterregeln für Firewall-Funktionen. Es sind Regeln möglich wie beispielsweise: „Wenn ein Paket von IP x.x.x.x und Port yy on eine URL in Weißrussland geschickt wird, dann leite es weiter zum Ziel und sende eine Kopie davon an den Admin-Sniffer-PC zum Mithören.“



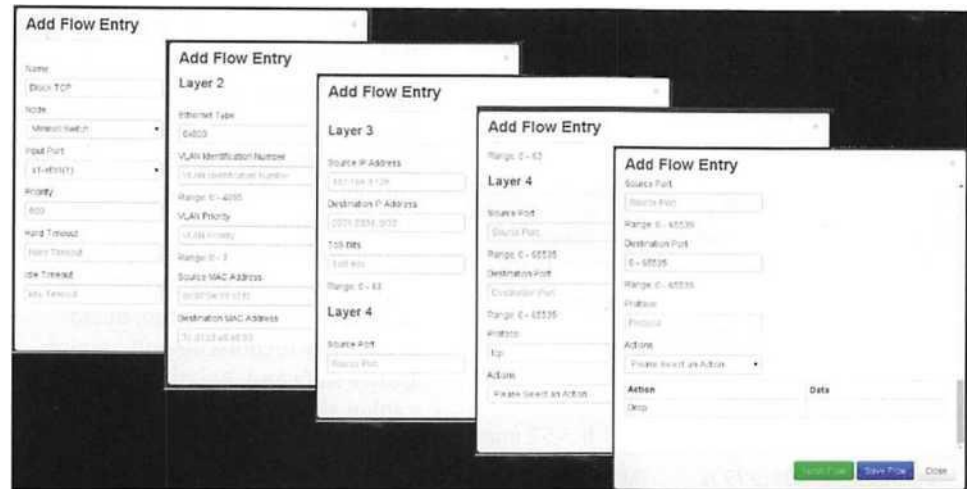
Durch entsprechende Regeln ist jeder SDN-Switch in der Lage Datenverkehr zu filtern. Das ganze Netzwerk bildet eine riesige verteilte Firewall.

SDN ist als Open-Source-Lösung verfügbar. Open Flow ist ein Kommunikationsprotokoll zwischen SDN- Switches und SDN-Controllern. Das folgende Schaubild zeigt einen einfachen Satz von Regeln für einen Switch.

SDN Controller Software							
↕							
MAC src	MAC dst	IP Src	IP Dst	TCP dport	...	Action	Count
*	10:20:.	*	*	*	*	port 1	250
*	*	*	5.6.7.8	*	*	port2	300
*	*	*	*	25	*	drop	892
*	*	*	192.*	*	*	local	120
*	*	*	*	*	*	controller	11

Die erste Zeile bedeutet: schicke alle Pakete, die mit der MAC-Adresse 10:20: beginnen, an Port 1 weiter, zweite Zeile: Ziel-IP 5.6.7.8 an Port 2 weiterleiten, dritte Zeile: Alles an TCP-Port 25 blockieren; vierte Zeile: alle Adressen, die mit 192.beginnen sind lokal und werden direkt im LAN zugestellt.

Das folgende Bild (siehe S. 111) gibt einen Einblick, wie Weiterleitungsregeln erstellt werden. Die verwendete Software Open Daylight ist eine Open-Source-Controllersoftware.



Die Datenströme können so gelenkt werden, dass Ressourcen optimal ausgenutzt werden und nichts vergeudet wird. Das weltweite Glasfasernetz von Google ist ein SDN-Netz.

LE 4 - Verfügbarkeit und Ausfallzeiten von IT-Systemen berechnen

Sie sollen Systemverfügbarkeit, Uptime und Downtime berechnen können.

Die Systemverfügbarkeit ist eine sehr wichtige Kenngröße. Die Wahrscheinlichkeit, mit der ein Gerät oder eine Baugruppe ausfällt, ermöglicht es abzuschätzen, wie betriebssicher ein System ist. Daher ist es wichtig zu wissen, was die Ausdrücke und Werte bedeuten.

(1) Verfügbarkeit

Systemverfügbarkeiten		
Bezeichnung	Formel/Berechnung	Beschreibung
Uptime	t_{up}	Die Zeit, in der ein System oder ein Dienst korrekt funktioniert
	$t_{up} = A * t_{gesamt}$	Uptime berechnen, A = Availability, Verfügbarkeit
Downtime	t_{down}	Die Zeit, in der das System oder der Dienst nicht verfügbar ist, Ausfallzeit
	$t_{down} = t_{gesamt} - t_{up} = t_{gesamt} - A * t_{gesamt}$ $t_{down} = t_{gesamt} * (1 - A)$	Downtime berechnen, A = Availability, Verfügbarkeit
Gesamtzeit	$t_{gesamt} = t_{up} + t_{down}$	Uptime plus Downtime ergibt die Gesamtzeit. Ein Jahr hat 8760 Stunden oder 525600 Minuten

Systemverfügbarkeiten			
Bezeichnung	Formel/Berechnung		
Verfügbarkeit, Availability	$A = \frac{t_{up}}{t_{gesamt}} = 1 - \frac{t_{down}}{t_{up}}$		
	Verfügbarkeit	Verfügbarkeit in %	Ausfallzeit pro Jahr
	0,99	99%	87,6 h
	0,995	99,5%	43,8 h
	0,999	99,9%	8,7 h
	0,9999	99,99%	0,87 h = 52 min
	0,99999	99,999%	0,087 h = 5,2 min
	0,999999	99,9999%	31,6 s

Beispiel: Die Stromversorgung in Deutschland hat weltweit die höchste Verfügbarkeit. Sie liegt seit Jahrzehnten dauerhaft bei über 99,997 % oder bei kleiner 0,003 % Downtime (entsprechend einer Ausfallzeit von weniger als 15 Minuten pro Jahr).

(2) Ausfallwahrscheinlichkeit p

Eine Wahrscheinlichkeit von 1 bedeutet, dass ein Ereignis ganz sicher (oder zu 100 %) eintritt. Eine Wahrscheinlichkeit von 0 bedeutet, dass ein Ereignis ganz sicher nicht (oder zu 0%) eintritt. Eine Wahrscheinlichkeit von 0,01 bedeutet, dass ein Ereignis zu einem Hundertstel (oder zu 1 %) eintritt. Anders ausgedrückt: Wenn man 100 Festplatten hat und im Laufe eines Jahres eine kaputtgeht, dann ist die Ausfallwahrscheinlichkeit 1 /100, $p = 0,01 = 1 \%$.

(3) Erhöhen der Systemverfügbarkeit

Durch Redundanz, also das mehrfache Vorhandensein einer Baugruppe oder eines Systems, kann seine Verfügbarkeit wesentlich erhöht werden. Zwar erhöht sich mit jedem Bauteil die Wahrscheinlichkeit, dass ein Bauteil ausfällt - bei zwei Bauteilen ist die Wahrscheinlichkeit, dass eines davon ausfällt, doppelt so groß! Die Wahrscheinlichkeit, dass beide gleichzeitig ausfallen, wird aber wesentlich verringert. Sie ist das Produkt der Einzel-Ausfallwahrscheinlichkeiten.

Beispiel: Angenommen, ein Netzteil hat eine Ausfallwahrscheinlichkeit von 0,001 (also 0,1 %). Wenn zwei Netzteile parallel betrieben werden, ist die Wahrscheinlichkeit, dass ein Netzteil davon ausfällt $2 \cdot 0,001 = 0,002$ (oder 0,2%). Die Wahrscheinlichkeit, dass beide gleichzeitig ausfallen ist aber $0,001 \cdot 0,001 = 0,000001$ (oder 0,00001 %). Damit ist das System um den Faktor 1 000 besser geworden. Die Ausfallwahrscheinlichkeit wird damit um den Faktor 1 000 reduziert!

Ausfallwahrscheinlichkeit

Wahrscheinlichkeit $p_{ges} = p^n$ bei gleichen Wahrscheinlichkeiten

$P_{ges} = P_1 \cdot P_2 \cdot P_3 \dots$ bei unterschiedlichen Wahrscheinlichkeiten

p = Ausfallwahrscheinlichkeit; n = Anzahl der redundanten Teile

Lernzielkontrollen TAG 12 und TAG 13

1. Wofür stehen die Abkürzungen RAID, JBOD, RAID?
2. Welche Sicherheitsvorteile bringt RAID 0, welche RAID 1?
3. Was ist richtig, was ist falsch?
 - a. Datensicherung ist dasselbe wie Datensicherheit.
 - b. Daten können auf Festplatten, Magnetbändern, CD/ DVD, USB-Speichersticks gesichert werden.
 - c. Bei jeder Datensicherung werden immer alle Daten einer Festplatte gesichert.
 - d. Datensicherung macht man am besten in der Mittagspause, da hier die Mitarbeiter nicht arbeiten.
 - e. Die Sicherungsbänder des Backup-Servers sollten in der Nähe des Servers aufbewahrt werden, damit sie schnell gewechselt werden können.
 - f. Die Sicherungsbänder des Backup-Servers sollten in einem anderen Raum oder besser in einem anderen Gebäude aufbewahrt werden.
 - g. Die Daten sichern, dauert in der Regel nur wenige Minuten.
 - h. Das Rücksichern (=Wiederherstellen) der Daten muss regelmäßig geprüft und geübt werden.
 - i. Das Sichern lokaler Daten auf einem Cloud-Speicher ist Standard.
 - j. Datensicherung ist an jedem Arbeitstag vorzunehmen.
 - k. Datensicherung einmal in der Woche ist ausreichend.
 - l. Nach einer Datensicherung werden die Daten auf den Festplatten gelöscht.

4. Berechnen Sie den zur Verfügung stehenden Speicherplatz bei verschiedenen RAID-Leveln.

Anzahl der Festplatten	RAID-Level	Gesamtkapazität/ Bemerkungen
4 * 1 TB	5	
4 * 1 TB	6	
2 * 1 TB	0	
2 * 1 TB	1	

5. Welches Backup-Verfahren speichert zwischen den Vollsicherungen die wenigsten Daten?
6. Können auf einem Backup auch alte gelöschte Daten gefunden werden?
7. Vergleichen Sie die Zuverlässigkeit bzw. die Ausfallsicherheit von folgenden RAID-Systemen.

RAID-Level	Sicherheit	Ausfallwahrscheinlichkeit
5		
6		
0		
1		

8. Berechnen Sie die Zeiten, die ein Backup der Daten eines Betriebs benötigt.
Sie haben ein Datenvolumen von 1 TiB zu sichern. Wie lange dauert das Sichern der Daten bei einem Bandlaufwerk mit einer Datentransferrate von 360 Mbyte/s (LTO 8 unkomprimiert) und 900 Mbyte/s (LTO 8 komprimiert)?
Würden Sie die Daten komprimieren oder nicht?
9. Prüfen Sie mögliche Änderungen in der Backup-Strategie eines Unternehmens.
Prüfen und rechnen Sie nach, ob das Sichern bei Nachts morgens zum Arbeitsbeginn abgeschlossen ist. Überprüfen Sie mögliche Änderungen in der Backup-Strategie.

Backup-Strategie eines Unternehmens
Ein Unternehmen arbeitet in zwei Schichten von morgens 6:00 Uhr bis abends 21:00 Uhr. Dabei werden während der Arbeitszeit Daten aus der Produktion auf den Servern abgelegt und verarbeitet. Die Datensicherung wurde vor einigen Jahren eingerichtet und deren korrekte Funktion mehrfach getestet. Die Einstellungen sind folgende:

Beginn der Sicherung (inkrementelle Sicherung) auf den Backup-Server:	Dienstag bis Freitag 4:00 Uhr
Beginn der Sicherung (Vollsicherung) auf den Backup-Server:	Samstag 4:00 Uhr
Zu sicherndes Datenvolumen zum Zeitpunkt des Einrichtens der Sicherung:	4 TiB
Tägliche Zunahme des Datenvolumens:	Bis zu 500 Mbyte
Täglich werden etwa 5% des Datenbestandes verändert.	
Verwendetes Bandlaufwerk:	Ultrium8-LTO8 unkomprimiert, 12 TB Volumen, 360 Mbyte/s Transferrate (unkomprimiert)

Wie lange dauert das Sichern der Daten? Sind dabei Komplikationen zu erwarten? Wenn ja, bitte Lösungsvorschläge machen.

10. Sie haben ein Datenvolumen von 1 TiB zu sichern. Täglich ändern sich etwa 10% der Daten und etwa 0,1% neue Daten kommen hinzu. Erstellen Sie ein Verfahren, mit dem Sie die Daten auf einem Sicherungsband sichern. Begründen Sie, wann Sie die Daten sichern und welche Sicherungsart (voll, inkrementell oder differenziell) Sie verwenden. Vervollständigen Sie die Liste.

Tag	Band-Nr.	Sicherungsart/ Bemerkungen
Montag	1	Inkrementelle Sicherung
Dienstag	2	
Mittwoch		

11. Zu welchem Zweck wird eine DMZ eingerichtet?

12. Welche Funktion hat ein Proxy-Server?

13. Wahr oder falsch?

- Redundanz erhöht die Verfügbarkeit.
- Je mehr Baugruppen ein System enthält, desto höher ist die Verfügbarkeit.
- Eine Verfügbarkeit von 99,5 % entspricht einer Downtime von fast 3 Tagen.

14. Wie lange ist ein Drucker pro Jahr verfügbar, wenn er eine Verfügbarkeit von 95 % hat? Wie lange ist die Ausfallzeit?

15. Führen Sie die Berechnung durch: Wie lange darf die Ausfallzeit pro Monat sein, wenn Ihr Vertrieb dem Kunden eine Verfügbarkeit von 99,95% zugesagt hat? Können Sie diesen Vertrag erfüllen, wenn Sie eine herkömmliche Bandsicherung verwenden? Vergleichen Sie die Alternativen.

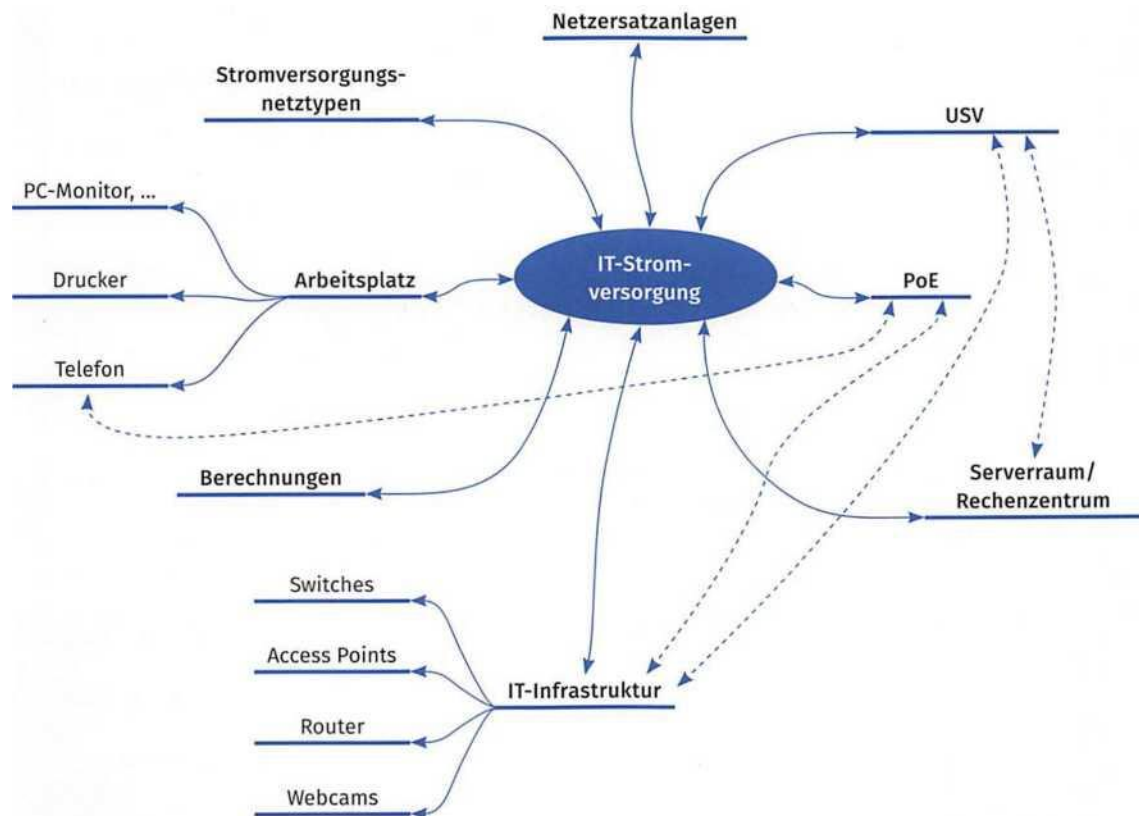
16. Das deutsche Stromnetz ist sehr sicher, es ist eines der sichersten der Welt. Die Verfügbarkeit liegt bei 99,998%. Dies entspricht einer Ausfallzeit von etwa 15min pro Jahr (Daten laut VDE-Statistik). Mit einer USV-Anlage (USV = unterbrechungsfreie Stromversorgung) gekoppelt kann man die IT sehr sicher mit Strom versorgen. Die Schwachstelle der unterbrechungsfreien Stromversorgung ist die begrenzte Lebensdauer der Akkus.
Berechnen Sie die Ausfallwahrscheinlichkeit der Stromversorgung eines Servers, wenn wir die Verfügbarkeit einer unterbrechungsfreien Stromversorgung mit nur 95% annehmen?

TAG 14 - Geräte mit Strom versorgen

Sie sollen die Grundlagen der Stromversorgung der IT verstehen.

LE 1 - Stromversorgung allgemein

Die Stromversorgung ist in der IT ein wichtiges Thema, da die komplette IT mit Strom versorgt werden muss. Wichtige Komponenten müssen sogar bei Stromausfall weiter ihren Dienst leisten. Als Fachmann in der IT muss man auch den Strombedarf seiner Geräte berechnen können und die Grundzüge der Stromversorgung kennen.



(1) Themen rund um die Stromversorgung

Komponenten der Stromversorgung

Arbeitsplatz

Die üblichen Elektrogeräte eines Arbeitsplatzes werden über die Standard-Elektroinstallation mit Strom versorgt. Die Absicherung beträgt in der Regel 16 Ampere pro Stromkreis.

Serverraum

Der Serverraum hat einen hohen Strombedarf. Er wird mit mehreren separat abgesicherten Stromkreisen angefahren. Die Stromlast muss auf allen drei Phasen etwa gleichmäßig verteilt sein. Betriebswichtige Geräte werden über eine USV (Unterbrechungsfreie Stromversorgung) angeschlossen. Die Stromversorgung des Serverraumes wird separat von der restlichen Hausinstallation ausgeführt.

IT-Infrastruktur

Switches, WLAN-Access-Points, Router, Webcams und andere Netzwerkgeräte werden in der Regel über die normale Hausinstallation strom versorgt. Die Sicherungen der Stromkreise, an denen diese Geräte angeschlossen sind, sollten nach Möglichkeit gekennzeichnet werden, um die Fehlersuche zu vereinfachen.

USV - Unterbrechungsfreie Stromversorgung

Eine USV-Anlage dient zum

- Filtern von Störungen auf der Netzspannung wie Spannungsspitzen, Überspannung, Unterspannung und Stabilisieren der Netzfrequenz
- Überbrücken von kurzzeitigen Netzausfällen
- geregelten Herunterfahren der Server bei länger anhaltenden Stromausfällen

Drei Typen von USV werden unterschieden:

- VFI (Voltage and Frequency Independent from Mains Supply): andere Bezeichnungen sind online, Double-Conversion, Dauerbetrieb oder Doppelwandler
- VI (Voltage Independent from Mains Supply): andere Bezeichnungen sind netzinteraktiv, Single-Conversion, Delta-Conversion oder aktiver Mitlaufbetrieb
- VFD (Voltage and Frequency Dependent from Mains Supply): andere Bezeichnungen sind offline, standby oder passiv

Netzersatzanlage, Ersatzstromversorgung

Stromgeneratoren, meist mit Dieselmotoren, die bei Ausfall der öffentlichen Stromversorgung die weitere Stromversorgung gewährleisten.

Netztypen der Stromversorgung

Bei den Stromversorgungsnetzen sind unterschiedliche Systeme möglich. Sie unterscheiden sich durch die Art der Erdverbindung.

- TN-System (franz. Terre Neutre), mit Neutraleiter von der Generatorseite und mit Schutzleiter PE (Protective Earth) auf der Anlagenseite
- TT-System (franz. Terre Terre), mit Neutraleiter von der Generatorseite
- IT-System (franz. Isole Terre), ohne Neutraleiter von der Generatorseite, mit Erdung PE in der Hausverteilung

Power over Ethernet (PoE; IEEE 802.3bt-2018) und Power over Dataline (PoDL; IEEE 802.3bu- 2016)

Stromversorgung für Netzwerkgeräte über die Ethernet-Leitung; typische Geräte sind Ethernet- Telefone (VoIP), WLAN-Access-Points, Webcams u.a.

Die ursprüngliche Norm IEEE 802.3af-2003 definiert bis 15,4 Watt Leistung. PoE+ liefert bis 25,5 Watt Leistung. Der Standard IEEE 802.3bt-2018 (auch 4PPoE) liefert Strom auf allen vier Adernpaaren mit bis zu 100 Watt Ausgangsleistung.

Endspan Devices oder Endspan Switches sind Netzwerkschwitches mit PoE-Fähigkeit (sog. Power Sourcing Equipment, PSE). Midspan-Geräte oder Power Injectors sind Speisegeräte, die in die Netzwerkleitung nach einem Switch eingeschleift werden, um die Energie für Endgerät einzuspeisen.

Berechnungen		
Phys. Größe und Formelzeichen	Formel	Einheit
Spannung U	$U = R * I$	Volt, V
Strom I	$I = \frac{U}{R}$	Ampere, A
Widerstand R	$R = \frac{U}{I}$	Ohm, Ω
Ohm'sches Gesetz	$U = R * I$	Volt, V
Wirkleistung P	$P = U * I$	Watt, W
Arbeit W	$W = P * t$	Wattstunde, Wh Kilowattstunde, kWh
Scheinleistung S (wenn U und I nicht in Phase sind)	$S = U * I$	Voltampere, VA
Wirkungsgrad η	$\eta = \frac{P_{aus}}{P_{ein}}$ oder $\frac{\text{abgegebene Leistung}}{\text{zugeführter Leistung}}$	
Wirkfaktor $\cos \phi$	$\cos \phi = \frac{P}{S}$	

(2) Gefahren durch elektrischen Strom

Elektrischer Strom kann lebensgefährlich sein. Die Steuerung unserer Muskeln geschieht durch elektrische Impulse. Unsere Sensoren (die „Sinne“) leiten ihre Informationen auch durch elektrische Impulse durch den Körper. Die verwendeten Leiter, die Nervenbahnen, bestehen aus Salzwasser. Isoliert werden diese Leiter durch eine nicht leitende Hülle (Myelinschicht). Kommt man mit spannungsführenden Teilen in Berührung, kann Strom durch den menschlichen Körper fließen. Dieser „Fremdstrom“ benutzt dann selbstverständlich auch unsere Nervenbahnen zum Hindurchfließen. Dabei ist es entscheidend, welchen Weg der Strom durch den



Körper nimmt. Am gefährlichsten ist es, wenn der Strom über die Brust, also über das Herz fließt.

Der Übergangswiderstand des Körpers hängt u.a. von der Leitfähigkeit der Haut ab. Eine feuchte, schwitzige Hand ist leitfähiger als eine staubtrockene Hand. Die Spannung beeinflusst auch den Widerstand der Haut: je höher die Spannung, desto niedriger der Hautwiderstand, desto mehr Strom kann fließen!

Ebenso entscheidend für die Wirkung auf den Körper ist die Einwirkdauer des Stromes. Auch ein geringer Strom, der längere Zeit einwirkt, kann verheerende Schäden verursachen.



Bereich	Stromstärke in Milliampere	Wirkung auf den Körper	Folgen
1	1-2 mA	Kribbeln	EvtL Erschrecken
1	bis 10 mA	Muskelkrampf	Lähmungen
1	bis 25 mA	Blutdruckanstieg	Bewusstlosigkeit
2	25-50 mA	Starke Krämpfe, Magenkrampf, Herzkammerflimmern	Starke Lähmungen
3	> 50 mA	Herzkammerflimmern	Herzstillstand
4	> 3000 mA	Starke Verbrennungen, Verkochen von Gewebe	Herzstillstand

Gefahren des elektrischen Stromes

Geringe Ströme merkt man nicht. Die Wahrnehmungsgrenze liegt bei ca. 1 mA. Die Loslassgrenze liegt bei nur 10 mA. Dann verkrampft sich bereits die Muskulatur und gehorcht nicht mehr dem Willen. Dadurch ist es unmöglich, spannungsführende Teile loszulassen. Man hängt wie festgebunden am Leiter.

Vorsichtsmaßnahmen für IT-Berufe

Vor dem Öffnen von Geräten immer den Netzstecker ordnungsgemäß am Griff ziehen. Gerät ausschalten reicht nicht! Sicherstellen, dass der Stecker nicht versehentlich durch eine andere Person wieder eingesteckt wird. Beim Abschalten am Sicherungskasten muss verhindert werden, dass jemand anderes die Sicherungen wieder einschaltet. Gegen Wiedereinschalten sichern!



Nicht zu vernachlässigen sind die Sekundär-Unfälle. Dies sind Unfälle, die durch einen Stromschlag ausgelöst wurden, bei denen aber keine körperlichen Schäden durch den Stromunfall selbst aufgetreten sind. Als Paradebeispiel dient hier der Hobby-Elektriker, der eine Deckenlampe installiert, einen elektrischen Schlag bekommt und dadurch von der Leiter fällt und sich verletzt.

Arbeiten an elektrischen Anlagen dürfen nur von Elektrofachpersonal ausgeführt werden! IT-Fachleute, Administratoren, Fachinformatiker gelten als Laien und alle Arbeiten an Leitungen über 50 Volt Wechselspannung und 120 Volt Gleichspannung **sind verboten!**

Durch Zusatzqualifikation können auch IT-Fachleute bestimmte Arbeiten erledigen. Sie sind dann Elektrofachkräfte für festgelegte Tätigkeiten. Dadurch können sie auch beispielsweise Steckdosen anschließen oder Serverschränke. Beim IT-Systemelektroniker ist dies Teil der Ausbildung.

Was dürfen IT-Fachleute nicht?

- Schutzkontaktstecker an eine Stromleitung anschließen
- Steckdose anschließen
- Lampe anschließen
- Arbeiten am Sicherungskasten
- Steckdose verlegen
- Mehrfachsteckdose mit einer weiteren Mehrfachsteckdose verlängern
- Sicherung gegen eine andere mit anderem Auslösestrom oder -Charakteristik tauschen

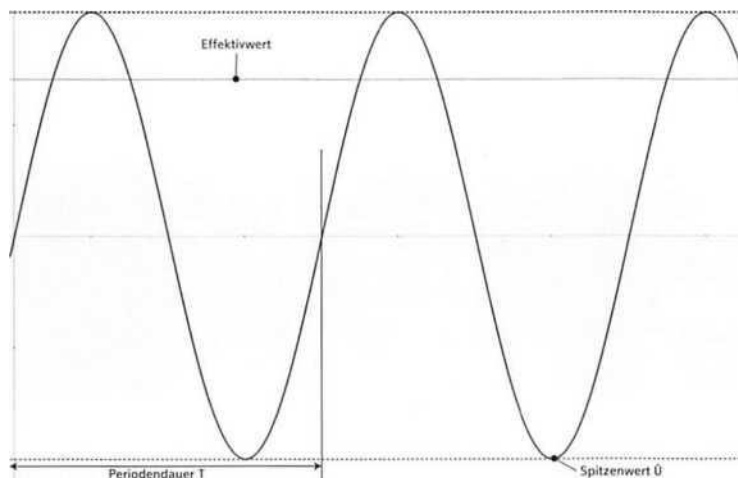
Für Arbeiten an der Elektrik muss man Elektrofachkraft sein!

(3) Energieversorgung von IT und Rechenzentren

Das Stromversorgungsnetz liefert eine sinusförmige Wechselspannung mit 230 Volt Effektivspannung und 50 Hz. Der Effektivwert ist der Wert, der der einer Gleichspannung mit gleicher Leistung entspricht. Dies sind in Deutschland 230 V. Die Spitzenspannung ist wesentlich höher. Sie beträgt $\hat{U} = \sqrt{2} \cdot U_{\text{eff}}$

Die Zeit für eine komplette Sinuswelle, also positive und negative Halbwelle, ist die Periodendauer T.

Die bei uns üblichen 50 Hz entsprechen: $T = \frac{1}{f} = \frac{1}{50\left(\frac{1}{s}\right)} = 20 \text{ ms}$



Die Leistung ist das Produkt aus Strom und Spannung: $P = U \cdot I$. Das Formelzeichen ist P, die Einheit ist Watt.

Normale Steckdosen werden mit einer 16-Ampere-Sicherung abgesichert. Die maximale Leistung, die daran angeschlossen werden kann, ist: $P_{\text{max}} = U_{\text{eff}} \cdot I_{\text{max}} = 230 \text{ V} \cdot 16 \text{ A} = 3680 \text{ Watt}$

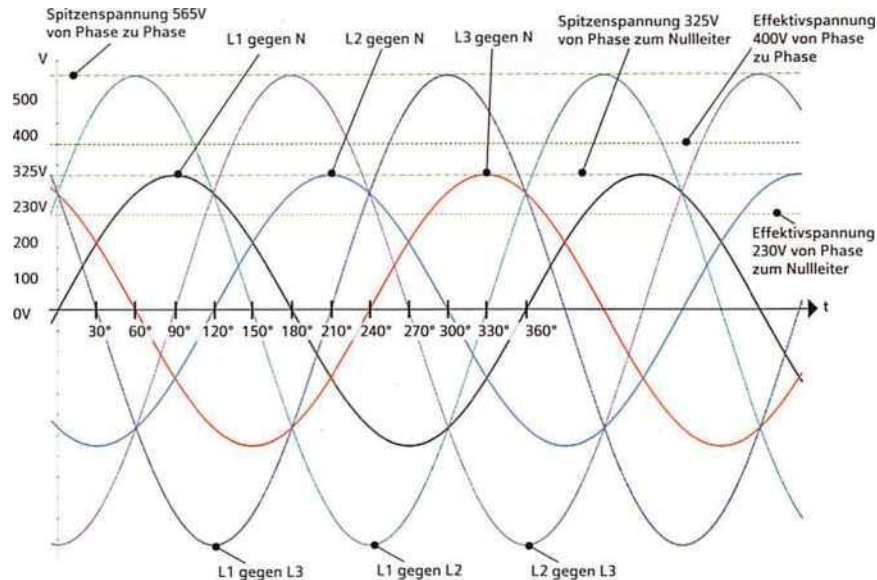
Eine Steckdose wird mit drei farbig isolierten Drähten angefahren. Dies sind:

braun oder schwarz	Phase, 230 V
blau	Neutralleiter, Nullleiter
gelb-grün	PE, Protective Earth, Schutz Erde

Alle Verbraucher werden beim Stromnetz parallel geschaltet. Der Gesamtstrom ist die Summe aller Einzelströme. Die Gesamtleistung ist die Summe aller Einzelleistungen.

Das Stromversorgungsnetz liefert Strom auf drei Leitungen, die Phasen genannt werden. Jede Phase hat eine Spannung von 230 Volt gegenüber Erde und ist separat abgesichert. Eine Starkstromsteckdose wird mit fünf farbig isolierten Drähten angefahren. Dies sind:

Dreimal braun oder schwarz	3 Phasen, 230 V
blau	Neutralleiter, Nullleiter
gelb-grün	PE, Protective Earth, Schutzterde



Die drei Phasen sind zeitlich zueinander versetzt - der Versatz beträgt 120° oder 6,66 ms (bei 50 Hz Netzfrequenz).

Vorsicht! Eine Phase hat eine Effektivspannung (rotgestrichelte Linie im Schaubild) von 230 Volt gegen Erde und damit eine Spitzenspannung von 325 Volt. Zwei Phasen haben gegeneinander 400 Volt Effektivwert und 565 Volt Spitzenspannung.

Beachten Sie unbedingt: Arbeiten an der Stromversorgung dürfen nur von Fachkräften vorgenommen werden.

Die drei Phasen werden bei der Elektroinstallation so auf die Verbraucher verteilt, dass jeder Stromkreis etwa gleich stark belastet wird. Ein Serverraum oder Rechenzentrum wird mit allen drei Phasen angefahren und auf eindeutig gekennzeichnete Steckdosen gelegt. Wichtige Komponenten wie Server, Router und Switches sind mit doppelten Netzteilen ausgestattet. Damit bei Ausfall einer Phase der Betrieb weiter aufrechterhalten werden kann, sind die beiden Netzteile auf zwei verschiedenen Phasen anzuschließen.

Damit bei Ausfall der Stromversorgung vom Energieversorger trotzdem noch gearbeitet werden kann, werden teilweise Notstromversorgungen eingesetzt. Diese sog. Netzersatzanlage besteht meist aus einem Dieselmotor, der einen Generator antreibt. Die Netzersatzanlage springt an, wenn das externe Netz ausfällt. Solche Anlagen sind aufwendig und teuer. Sie werden daher nur in sicherheitsrelevanten Umgebungen eingesetzt. Die „normale“ IT kommt ohne Netzersatzanlagen aus.

(4) Unterbrechungsfreie Stromversorgung (USV)

Unabhängig davon, ob Netzersatzanlagen eingesetzt werden oder nicht, werden Server und wichtige Netzwerkkomponenten mit einer unterbrechungsfreien Stromversorgung (USV, oder engl. UPS = Uninterruptible Power Supply) betrieben.

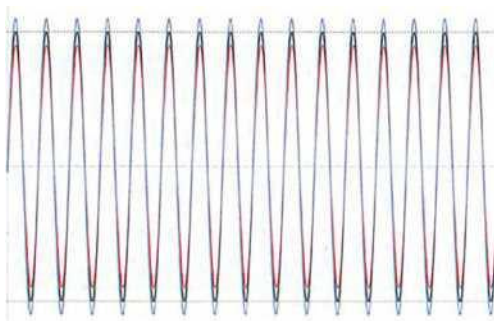


Eine USV ist ein Gerät, welches zwischen den Netzanschluss und den oder die Verbraucher geschaltet wird. Sie beinhaltet eine Pufferbatterie und kann daraus Strom liefern, wenn die Netzversorgung ausfällt.

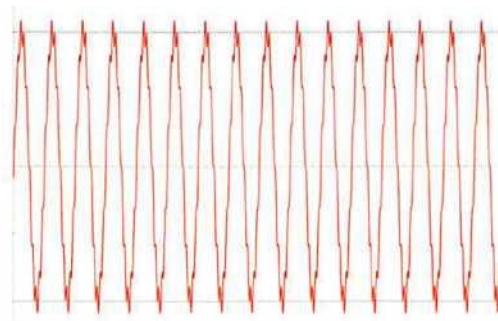
Folgende Störungen der Stromversorgung können auftreten:

- Netzausfälle von Minuten bis Stunden
- Kurzzeitige Spannungseinbrüche bzw. Spannungsschwankungen
- Kurzzeitige Spannungsschüsse
- Überspannung
- Unterspannung
- Abweichen der Netzfrequenz 50 Hz (in manchen Ländern 60 Hz)
- Spannungsspitzen (Spikes), Schaltspitzen
- Harmonische Oberschwingungen (Verzerrung der Sinusform)

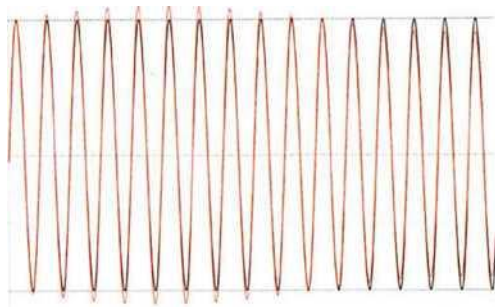
Bei **Überspannung und Unterspannung** weicht die Netzspannung von der Sollspannung von 230 Volt **ab**. Abweichungen von der Sinusform nennt man **Verzerrungen**. Hochfrequente Anteile können die Netzteile und die nachfolgende Elektronik negativ beeinflussen und stören. Bei **Spannungsschwankungen** handelt es sich abwechselnd um Überspannung und Unterspannung. Spikes sind kurzzeitige sehr hohe Spannungsspitzen. Sie entstehen beispielsweise beim Ein- und Ausschalten von induktiven Verbrauchern. Auch die Netzfrequenz muss konstant sein.



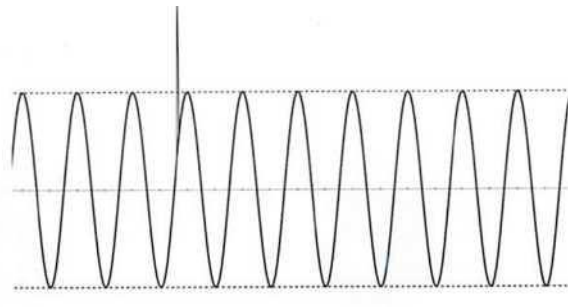
Überspannung und Unterspannung



Verzerrungen



Spannungsschwankungen



Spikes

Eine USV kann die oben genannten Störungen teilweise oder vollständig ausgleichen. Des Weiteren bieten alle professionellen Geräte eine Kommunikationsschnittstelle mit den angeschlossenen Servern. Diese dient zum Anzeigen des Betriebszustandes einer USV und zum Herunterfahren der Server, wenn im Batteriebetrieb die Pufferbatterie zur Neige geht. Unkontrolliertes Ausschalten der Server wird damit verhindert.

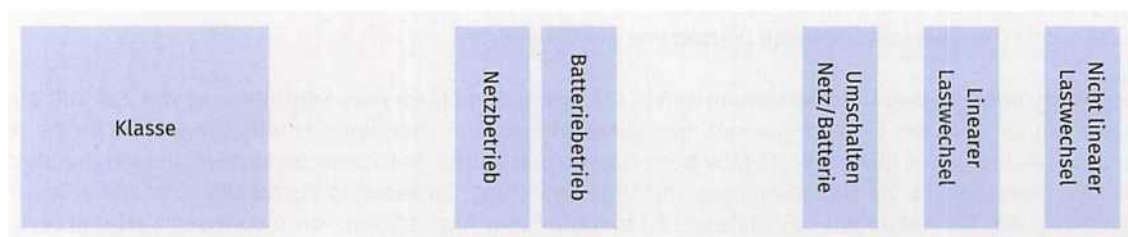
Die Norm EN 62040 klassifiziert die USV in drei Typen (Klassen):

- Klasse 1: VFI (Voltage and Frequency Independent) - spannungs- und frequenzunabhängig
- Klasse 2: VI (Voltage Independent) - spannungsunabhängig
- Klasse 3: VFD (Voltage and Frequency Dependent) - spannungs- und frequenzabhängig

Die Bezeichnung der USV ist genormt.

Genereller Aufbau: Klasse - Kurvenform - Umschaltzeit

Beispiel: VD XY 123



Klasse
VFI
VFD
VD

Formen des Ausgangssignals	
Buchstabe	Bedeutung
S	Reine Sinuskurve, geringer Verzerrfaktor ($< 0,08$)
X	Sinuskurve mit geringen Verzerrungen $< 0,08$ nur bei linearen Lastwechseln (keine sprunghaftigen Lastwechsel)
Y	Nicht sinusförmige Ausgangsspannung, kann auch trapezförmig oder rechteckig sein

Unterbrechung am Ausgang	
Wert	Bedeutung
1	keine Unterbrechung bei Umschalten Netz-/ Batteriebetrieb
2	Unterbrechung bis 1 ms
3	Unterbrechung bis 10 ms

Nach der Klassenbezeichnung wird mit zwei Buchstaben die Kurvenform des Ausgangssignals angegeben. Der erste Buchstabe spezifiziert das Signal bei Netzbetrieb, der zweite bei Batteriebetrieb. Dabei steht s für sinusförmige Ausgangsspannung, x für sinusförmige Spannung mit Verzerrungen von $< 0,08$ und y für Ausgangsspannungen von $> 0,08$

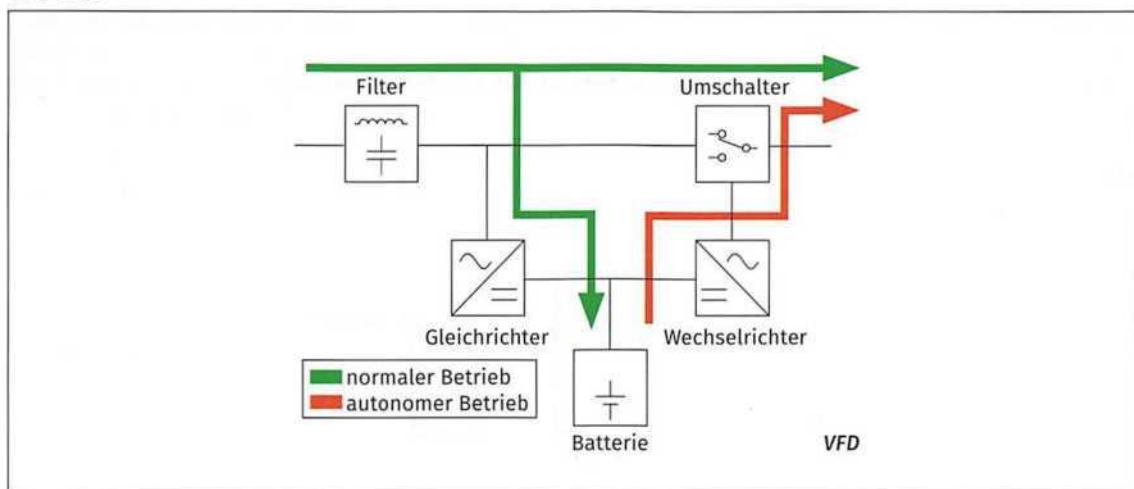
Verzerrungsfaktor gegenüber Sinusform. Eine sinusförmige Ausgangsspannung bei Netz- und Batteriebetrieb ist ideal.

An zweiter Stelle wird das Verhalten der USV bei Laständerung am Ausgang klassifiziert. Die erste Zahl gibt das Verhalten an beim Wechsel von Batterie auf Netzbetrieb und umgekehrt. Die zweite Zahl gibt das Verhalten bei linearen Lastwechseln am Ausgang an, die dritte bei nicht linearen, also sprunghaften Lastwechseln. Nicht lineare Lastwechsel sind in der IT die Regel.

Die bestmögliche USV ist eine VFI SS 111; hierbei sind die Ausgangsspannung und die Ausgangsfrequenz unabhängig von der Netzversorgung (VFI), die Ausgangsspannung ist immer sinusförmig (SS) und beim Umschalten der Betriebsarten reagiert sie immer bestmöglich (111), also ohne Umschaltzeit.

Die schlechteste mögliche USV ist eine VFD YY 333; hierbei folgt die Ausgangsspannung dem Eingangssignal (VFD), die Ausgangsspannung ist bei Netz- und Batteriebetrieb nicht sinusförmig (YY) und beim Umschalten von Netz- auf Batteriebetrieb und bei Laständerungen am Ausgang reagiert die USV schlecht möglichst (444) mit Umschaltzeiten bis zu 10 ms.

VFD-USV



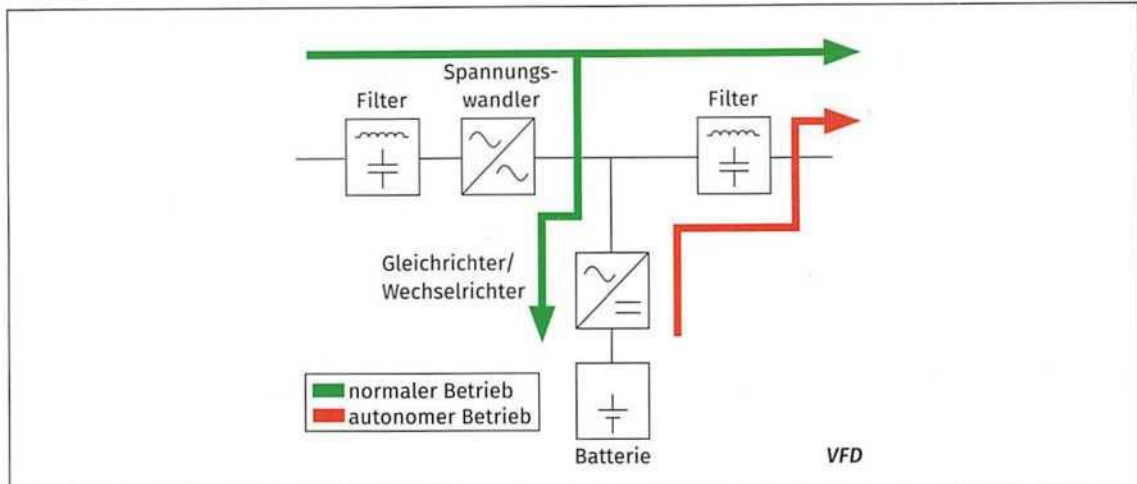
Schematischer Aufbau einer VFD-USV

Die einfachste USV verfügt über einen Eingangsfilter, um den Netzstrom zu filtern. Das gefilterte Signal steht direkt am USV-Ausgang an. Die Ausgangsspannung ist somit abhängig von der Eingangsspannung und Eingangsfrequenz.

Ein Gleichrichter lädt dabei laufend die Batterie. Ein Wechselrichter macht aus der Batterie-Gleichspannung wieder die erforderliche Netzspannung. Nur im Fall des Netzausfalls wird der USV-Ausgang umgeschaltet auf den Wechselrichter. Ein Umschalten hat also immer eine kurze Unterbrechung zur Folge. Dies ist die einfachste Form einer USV und auch die preiswerteste.

Die VI-USV verfügt über einen Eingangsfilter und einen Spannungswandler, der im Netzbetrieb die Spannung konstant hält. Diese Spannung steht gefiltert am USV-Ausgang zur Verfügung. Gleichzeitig wird über einen kombinierten Gleich- und Wechselrichter eine Pufferbatterie geladen. Bei Netzausfall übernimmt der Wechselrichter und liefert die Ausgangsspannung. Die Umschaltzeiten von Netz- auf Batteriebetrieb können somit sehr kurz sein. Bei Netzbetrieb wird allerdings nur die gefilterte und spannungsgeregelte Eingangsspannung zum Ausgang geschaltet. Die Ausgangsfrequenz ist somit abhängig von der Eingangsfrequenz. Bei Batteriebetrieb werden die Ausgangsspannung und -frequenz vom Wechselrichter geregelt.

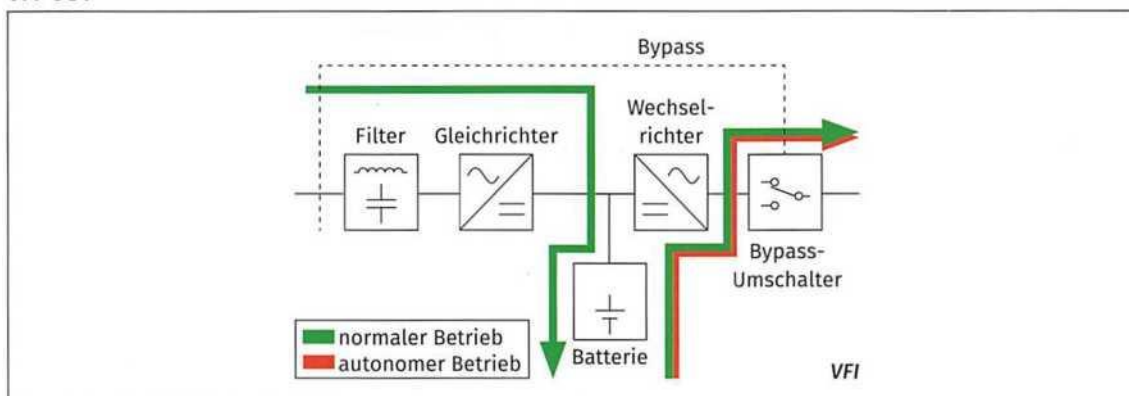
VI-USV



Schematischer Aufbau einer VI-USV

Die VFI-USV hat keinen Strompfad vom Eingang zum Ausgang. Die gefilterte Eingangsspannung wird gleichgerichtet und lädt eine Batterie. Aus dieser Batteriespannung wird immer der Wechselrichter gespeist, der die Ausgangsspannung liefert. Die Ausgangsspannung ist in maximaler Weise vom Eingang abgekoppelt. Dies ist die technisch aufwendigste Lösung, aber auch die beste. Allerdings fallen bei jeder Wandlung Verluste an. Die Wirkungsgrade von Gleichrichter und nachgeschaltetem Wechselrichter addieren sich. Die Verlustleistung einer solchen USV ist also in der Regel immer größer als bei anderen USV-Typen.

Eine VFI-USV



Schematischer Aufbau einer VFI-USV

(5) Wirkungsgrad und Laufzeit einer USV

Bei USV ist zu beachten, dass sowohl das Netzteil/Ladegerät als auch der Wechselrichter über einen gewissen Wirkungsgrad verfügen. Der Gesamtwirkungsgrad ist das Produkt aus beiden Einzelwirkungsgraden. Der Wirkungsgrad hat als Formelzeichen den griechischen Buchstaben η (Eta).

$$\eta_{\text{gesamt}} = \eta_{\text{Gleichrichter}} * \eta_{\text{Wechselrichter}}$$

Hat ein Netzgerät/Ladegerät in einer USV einen Wirkungsgrad von 90% und der Wechselrichter ebenfalls einen Wirkungsgrad von 90%, dann ist der Gesamtwirkungsgrad

$$\eta_{\text{ges}} = 0,9 * 0,9 = 0,81 = 81\%$$

Allerdings wird die Batterie nur geladen, wenn sie leer ist, also neu oder nach Stromausfall mit USV-Einsatz. Wenn die Batterie voll aufgeladen ist, fließt nur noch ein relativ geringer Ladeerhaltungsstrom in die Batterie.

Die Überbrückungszeit einer USV hängt von der Akku-Kapazität und dem Leistungsbedarf ab.

Die im Akku gespeicherte Energie ist $W = P \cdot t$.

Arbeit W	$W = P \cdot t$
Zeit t	$t = W / P$

Das bedeutet, dass beispielsweise ein Verbraucher mit 100 Watt Leistung in 10 Stunden 1 kWh Energie verbraucht. Oder andersherum gerechnet, dass ein 100 Watt Verbraucher mit 1 kWh 10 Stunden lang versorgt werden kann.

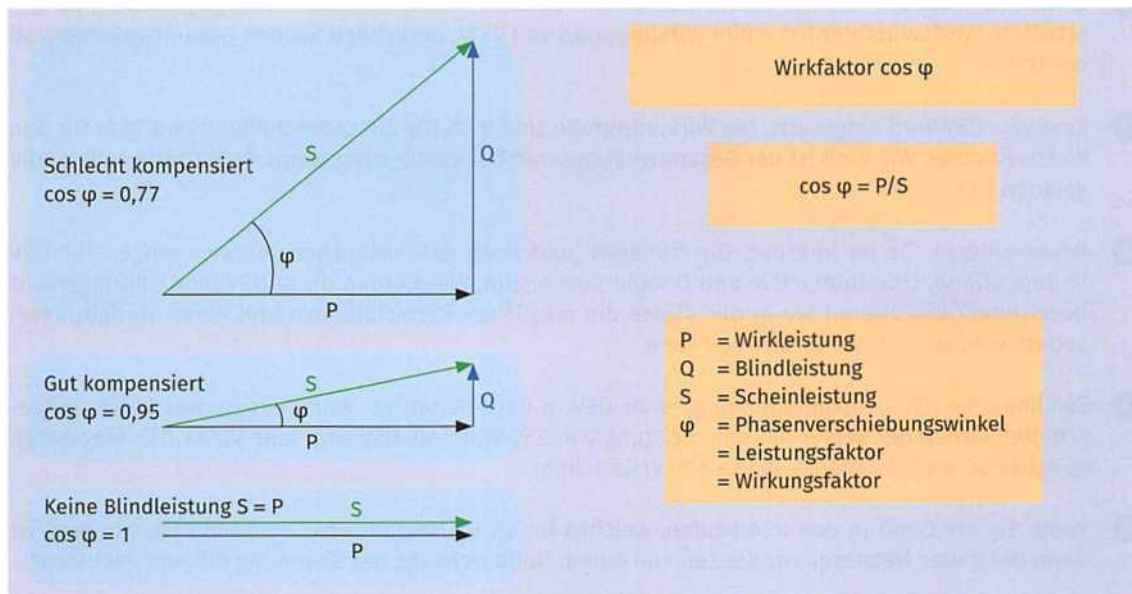
Beachten Sie bei der Dimensionierung der USV auch deren Wirkungsgrad.

Beispiel: Eine USV hat eine Kapazität von 100 Wh. Die Last, die bei Ausfall versorgt werden muss, hat eine Leistung von 100 Watt. Die Überbrückungszeit wäre dann, eine verlustfreie ideale USV vorausgesetzt: $t = W / P = 100 \text{ Wattstunden} / 100 \text{ Watt} = 1 \text{ Stunde}$.

Eine reale USV mit einem Wechselrichter-Wirkungsgrad von 90% hätte hierbei eine reale Kapazität von 90 Wh. Sie würde die Last also 0,9 Stunden mit Strom versorgen können.

(6) Leistungsfaktor Cosinus Phi

Bei kapazitiven oder induktiven Lasten sind Strom und Spannung nicht zeitgleich. Sie sind gegeneinander phasenverschoben. Netzteile sind durch die enthaltenen Trafos induktive Lasten. Das heißt, vom Eingang aus betrachtet wirkt ein Netzteil wie eine Spule. Dabei fließt zuerst ein Strom und baut in der Spule das Magnetfeld auf. Zeitlich verschoben steigt erst die Spannung an. Der dabei fließende Strom ist größer, als er bei Gleichspannung wäre.



Bei sinusförmigen Spannungen kann der Wirkfaktor zwischen 0 und 1 liegen. Das bedeutet, dass keine Blindleistung auftritt und damit die Scheinleistung gleich der Wirkleistung ist. Auch wenn nur die Wirkleistung tatsächlich gebraucht wird, so muss doch die Scheinleistung geliefert werden. Das bedeutet, dass alles größer ausgelegt werden muss als notwendig. Daher werden alle Geräte, die nennenswerte induktive Lasten haben, kompensiert. Man nennt dies Leistungsfaktorkorrektur, (Power Factor Correction, Power Factor Compensation, PFC).

PC-Netzteile weisen - mit PFC - einen Leistungsfaktor $\cos \varphi$ von 0,95 auf. Die Leistung wird in VA (Voltampere) angegeben, die Wirkleistung in Watt. Dies dient dem Veranschaulichen und Unterscheiden von Scheinleistung und Wirkleistung.

$S = U \cdot I$ (in VA)	Die Scheinleistung ist $U \cdot I$ bei Wechselspannung.
$S = \frac{P}{\cos \varphi}$	Die Scheinleistung S ist immer größer als die Wirkleistung.
$P = S \cdot \cos \varphi$ (in Watt)	Die Wirkleistung P ist immer kleiner als die Scheinleistung.
$Q = \sqrt{S^2 - P^2}$ (in var)	Die Blindleistung Q sollte möglichst klein sein.

Beispiel: Ein Netzteil wird laut Datenblatt mit 100 VA Leistung angegeben. Daraus ersehen wir, dass es sich um 100 VA Scheinleistung handelt. Der Wirkfaktor beträgt 0,9. Die Wirkleistung beträgt dann $P = S \cdot \cos \varphi = 100 \text{ VA} \cdot 0,9 = 90 \text{ Watt}$

LE 2 - Green-IT in Netzwerken berücksichtigen

Sie überprüfen Ihre Arbeit und die Auswahl der Komponenten in Bezug auf Energieeffizienz und Nachhaltigkeit.

Stellen Sie sich folgende Fragen:

- Müssen immer neue Geräte eingesetzt werden oder lässt sich die Lebensdauer durch sinnvolle Nachnutzung verlängern? Vielleicht sind Gebrauchtgeräte für Customer Service und andere weniger leistungshungrige Geräte einsetzbar?
- Haben die Geräte Energiesparoptionen? Wann wird bei Inaktivität der Bildschirm abgeschaltet und wann der PC in den Standby-Modus?
- Können Steckdosenleisten mit Schaltern jeden einzelnen Arbeitsplatz stromlos machen?
- Bei Neubeschaffung von IT: Gibt es Stromsparendere Alternativen? Lassen sich die Geräte am Ende der Nutzungsdauer recyceln? Wie und wo werden die Geräte hergestellt?

(1) Alternativgeräte auswählen (Refurbished IT)

Hierbei handelt es sich um IT (meist Computer, Notebooks und Server), die z. B. aus beendeten Leasingverträgen stammt. Diese werden vom Hersteller selbst oder von einem Händler generalüberholt, gereinigt, geprüft und schließlich wieder als Gebrauchtgerät verkauft. Da es sich hierbei in der Regel um Business-Geräte handelt, können diese aufgrund der hochwertigen verbauten Teile ohne Probleme noch längere Zeit genutzt werden. Refurbishing ist somit eine umweltschonende Methode, bereits bestehende Geräte wieder zu verwenden, um somit Ressourcen einzusparen.

Im konkreten Fall eines Kunden kann man sich fragen, ob vielleicht ein gebrauchter Rechner im Customer-Service eingesetzt werden kann. Dies wäre ressourcenschonender als ein neuer. Die benötigte Rechenleistung ist in dieser Anwendung nicht sehr hoch. Dagegen muss man den Stromverbrauch betrachten, den ein alter und ein leistungsstärkerer neuer Rechner hat.

Eine Alternative wäre der Einsatz eines Laptops. Dieser ist stromsparend und leistungsfähig. Mit einer Dockingstation mit großem Monitor, fest angeschlossener Tastatur und Maus, wäre dies ein vollwertiger Arbeitsplatz. Darüber hinaus könnte der Laptop auch mobil eingesetzt werden. Auch Laptops sind als „refurbished“ preiswert zu erhalten.

(2) Den Stromverbrauch der IT optimieren

Alle Rechner, Server und auch Netzwerkgeräte verbrauchen Strom. Dies wird häufig vergessen, besonders von jugendlichen Internetnutzern und Online-Zockern. Kleine Switches und WLAN-Access-Points verbrauchen zwar nicht viel Strom, aber alles summiert sich. Ein gängiger Router braucht, je nach Betriebsart, ca. 10 Watt bis 30 Watt. Ein einfacher 8-Port-Switch liegt bei 5 Watt bis 10 Watt. Managebare Switches und Router können ihren Energiebedarf drosseln und dem Netzaufkommen anpassen. Nicht belegte Ports werden (auch aus Sicherheitsgründen) heruntergefahren und verbrauchen keinen Strom. Access Points regeln ihre Sendeleistung je nach Empfangspegel der verbundenen Mobilgeräte.

Ein gut ausgestatteter Gaming-PC braucht, wenn er viel rechnen muss (z. B. Bilder aufbauen, Videos dekodieren), bis zu 300 Watt. Im Ruhezustand, wenn er läuft und nicht benutzt wird,

kann er 50 Watt bis 100 Watt verbrauchen. Drucker verbrauchen im Standby-Modus nur wenige Watt. Beim Druckvorgang werden aber bei Laserdruckern kurzzeitig mehrere hundert Watt verbraucht. Dies kommt vom Aufheizen der Fixiereinheit. Ein leistungsfähiger Server kann mehrere hundert Watt verbrauchen.

Die Einheit für die Arbeit ist die Wattsekunde Ws, Wattstunde Wh oder Kilowattstunde kWh. Die Energieversorger verkaufen uns elektrische Arbeit nach Kilowattstunden. Im Jahr 2019 müssen etwa 25 ct/kWh bis 30 ct/kWh bezahlt werden.

0,3 Wh!

Google veröffentlichte den Stromverbrauch, den eine durchschnittliche Google-Suche benötigt: 0,3 Wh! Das Surfen im Internet und das Abfragen von Suchmaschinen verbrauchen sehr viel Energie. Die großen Rechenzentren verbrauchen pro Jahr etwa 10 TWh bis 15 TWh elektrische Energie. Der Strombedarf der IT ist aber nicht nur der Bedarf der Server und der Geräte-Hardware. Die zugeführte Energie wird letztendlich in Wärme umgewandelt und muss abgeführt werden. Rechenzentren müssen klimatisiert werden, damit die empfindliche Hardware nicht überhitzt.

Der Strombedarf eines Rechners ist nicht konstant. Er hängt ab von der benötigten Rechenleistung. Über die BIOS-Einstellung und über die Systemeinstellungen kann man Einfluss nehmen auf den Stromverbrauch. Einzelne CPU-Kerne können abgeschaltet werden und die Taktfrequenz des Systems kann reduziert werden, wenn wenig Rechenleistung benötigt wird.

Softwaretechnisch kann man als Programmierer ebenfalls Einfluss auf den Strombedarf nehmen. Umständlich programmiert konsumiert der Rechner mehr Energie als optimierte Software. Eine der Applikationen, deren Verwendung am meisten Strom frisst, ist beispielsweise das Generieren von Bitcoins.

Lernzielkontrollen TAG 14

1. Was ist richtig, was ist falsch?
 - a. USV-Geräte sind Luxus. Man kann bei Servern getrost darauf verzichten.
 - b. Ein USV-Test muss unter möglichst realen Bedingungen erfolgen. Also alle paar Monate einmal den Netzstecker ziehen.
 - c. Jeder produktive Server muss mit einer USV gepuffert werden.
 - d. Jeder Desktop-PC muss mit einer USV gepuffert werden.
 - e. USV-Geräte kauft man nach den genormten Bezeichnungen.
2. Eine Doppelwandler-USV (VFI) hat einen Gleichrichter (Netzteil) mit 90 % Wirkungsgrad. Der nachgeschaltete Wechselrichter hat einen Wirkungsgrad von 95%. Berechnen Sie den Gesamtwirkungsgrad der USV.
3. Eine VFD-USV wird eingesetzt. Die Wirkungsgrade sind 90% für die Ladeschaltung und 95% für den Wechselrichter. Wie groß ist der Gesamtwirkungsgrad bei Netzbetrieb, wenn die Batterie vollständig geladen ist?
4. Recherchieren Sie im Internet. Die früheren (und noch gebräuchlichen) Bezeichnungen für USV lauten: offline, Line-Interactive und Double-Conversion. Wie werden diese USV heute normgerecht bezeichnet? Diskutieren Sie in der Klasse die möglichen Bezeichnungen und deren Herleitungen, sodass man sie sich besser merken kann.
5. Zeichnen Sie die Ausgangsspannung einer USV in Batteriebetrieb, wenn ein zweiter Server eingeschaltet wird. Jeder Server hat eine Leistung von 250 Watt. Als USV wird eine VD XY 333 eingesetzt. (x-Achse 50 ms/Kästchen, y-Achse 100 V/Kästchen).
6. Wenn Sie ein Gerät in den USA kaufen, welches für 60 Hz Netzfrequenz ausgelegt ist, wie groß ist dann bei dieser Netzfrequenz die Zeit von einem Nulldurchgang der Spannung bis zum nächsten?
7. Wie groß ist die Gesamtleistung, wenn Sie fünf Server mit je 500 Watt an eine Phase anschließen? Wie groß ist der Gesamtstrom? Reicht die Absicherung mit 16 A?
8. Sie möchten zwei Server und eine Speichereinheit in ein Rack schrauben. Jeder Server hat eine Leistungsaufnahme von 500 Watt. Die Speichereinheit benötigt laut Herstellerangabe

- maximal 400 Watt Wie groß ist die Stromaufnahme dieses Racks? Reicht für das Rack eine Phase mit einer Absicherung von 16 A?
9. Ein Server mit 1 kVA Leistungsaufnahme laut Herstellerdatenblatt soll mit einer USV betrieben werden. Wie groß ist die Leistungsaufnahme, wenn die USV einen Wirkfaktor von 0,9 hat?
10. Wahr oder falsch?
- Jeder Server muss mit einer USV gepuffert werden.
 - Eine USV muss den Betrieb der gesamten IP bei Stromausfall für mindestens 30 Minuten aufrechterhalten.
 - Eine USV an einem Büroarbeitsplatz ist nicht notwendig.
 - IP-Telefone werden über das Ethernet mit Strom versorgt.
 - PoE steht für Power over Earth.
 - Mit PoE lassen sich bis zu 100 Watt Energie übertragen.
 - Server können Aussetzer der Stromversorgung von wenigen Millisekunden auch ohne USV selbst überbrücken.
11. Was ist richtig, was ist falsch?
- Leistung ist Arbeit mal Zeit.
 - Arbeit ist Leistung mal Zeit.
 - Der Stromverbrauch von Gaming-PCs ist vernachlässigbar gering.
 - Neuere PCs sind leistungsfähiger bei weniger Stromverbrauch.
 - Gebrauchtgeräte sind aus Qualitätsgründen nicht empfehlenswert.
 - Energiespareinstellungen im BIOS oder im Betriebssystem sind sinnvoll.
12. Sie beobachten, dass Ihr Kollege am Feierabend nur den Monitor ausschaltet und seinen Arbeitsplatz mit laufendem Rechner verlässt. Sie machen ihn darauf aufmerksam, dass er vergessen hat, seinen Rechner herunterzufahren. Er erklärt Ihnen daraufhin, dass er dadurch morgens wieder viel schneller produktiv ist, da das lästige Hochfahren wegfällt. Sein PC zu Hause laufe auch durch, damit er, wenn er zu Hause ankommt, keine Zeit mit dem Hochfahren des Rechners verschenkt Ihnen leuchtet dies zwar ein, aber sie haben doch große Bedenken wegen des Stromverbrauchs. Also rechnen Sie aus, was der Rechner an Stromkosten verursacht, wenn er 24 Stunden, 7 Tage die Woche an 365 Tagen im Jahr durchläuft. Diese Rechnung legen Sie Ihrem Kollegen vor. Sie rechnen mit einem Stromverbrauch von nur 100 Watt und Stromkosten von 25 ct pro Kilowattstunde.
13. Sie wollen einen eigenen Server mit 250 Watt Leistungsaufnahme und zwei Laserdrucker mit einer aktiven Leistung von 120 Watt und 180 Watt in Ihr Büro stellen. Dazu noch einen DSL-Router mit 30 Watt und ein Switch mit 10 Watt. Wie groß ist der Strom, der durch die Leitung fließt?
14. Recherchieren Sie im Internet (auch wenn Sie damit Energie verbrauchen), wie viel Energie ein Einfamilienhaushalt und wie viel ein Handwerksbetrieb (z. B. Schreinerei) pro Jahr verbrauchen, wie viel Energie die Herstellung von einer Tonne Stahl oder Aluminium verbraucht, wie viel Energie ein kleines Rechenzentrum einer Schule oder einer Uni verbraucht
15. Früher, zu Zeiten der Rohrenmonitore, war es üblich - nach einer gewissen Zeit der Untätigkeit - einen Bildschirmschoner zu aktivieren. Welchen Effekt hat dies in der heutigen IT, wenn ein Bildschirmschoner aktiviert wird?
16. Welche Komponenten müssen bei der Energiebedarfsberechnung berücksichtigt werden? Kreuzen Sie an.
- Server im Datacenter
 - Workstations im Datacenter
 - Monitore im Datacenter
 - Switches im Datacenter
 - Router im Datacenter
 - Kühlung im Datacenter
 - Radio im Datacenter
 - Beleuchtung im Datacenter
 - Heizung im Datacenter

17. Wie groß sind Strom und Leistung bei standardisierten Stromanschlüssen?

Anschluss	Maximaler Strom	Maximale Leistung
Drei-Draht-Leitung mit Schuko-Steckdosen		
Fünf-Draht-Leitung mit Drehstrom- bzw. Starkstrom-Steckdose		

18. Wie lange kann eine USV die Server mit Strom versorgen? Der Server mit einer veranschlagten Leistungsaufnahme von 650 VA soll über eine unterbrechungsfreie Stromversorgung mit Strom versorgt werden, deren Bemessungsleistung 1400 VA beträgt und die zwei 12-V-Akkumulatoren mit je 10Ah enthält. Der Wirkungsgrad der unterbrechungsfreien Stromversorgung beträgt 90%. Berechnen Sie die Zeit in Minuten, die die unterbrechungsfreie Stromversorgung bei einem Netzausfall theoretisch maximal überbrücken kann.

Leistungsaufnahme Server	
Leistungsaufnahme der unterbrechungsfreien Stromversorgung	
In den Akkus gespeicherte Energie	
Überbrückungszeit der unterbrechungsfreien Stromversorgung (Zeit bis Akkus leer sind)	

19. Sind gebrauchte Geräte in der IT sinnvoll? Stellen Sie dazu Überlegungen zur Lebensdauer und Beschaffung von Laptops, Desktop-PCs und Switches an.

20. Nennen Sie die Stellen, an denen Sie Einsparpotenzial sehen und erläutern Sie sie kurz.

TAG 15 - Vertiefung des Wissens und Modulprüfung

LE 1 Einleitung

Der letzte Tag in diesem Modul bietet Ihnen die Möglichkeit der Wiederholung und Vertiefung Ihres Wissens. Sollten es noch offene, nicht vollständig bearbeitete Modul-Inhalte geben, nutzen Sie den heutigen Tag zur Komplettierung.

LE 2 - Modulprüfung

120 Minuten zu denen wir Ihnen recht viel Erfolg wünschen!

Lösungen:

TAG 1

1. individuelle Lösung
2. Inkonsistenten Daten sind fehlerhafte, nicht übereinstimmende Daten.
3. a) falsch, b) falsch, c) wahr, d) wahr, e) wahr
4. 1. INTERNET, 2. CARRIER, 3. DATACENTER, 4. LAN, 5. ROUTER, 6. SWITCH, 7. VLAN-TAG, 8. CLIENT, 9. VPN, 10. SAN, 11. WAN
5. 1. richtig 2. richtig 3. richtig 4. Falsch 5. Richtig
6. individuelle Lösung (bitte mit dem Ausbilder besprechen)

TAG 2 und TAG 3

1.
 1. Leitungsorientierte Netze, analoge Telefonnetze,
 2. Anschluss der Kunden über Telefonleitung, Kabelfernsehleitung, Funk und Verbindung mit dem Internet herstellen, ...
 3. Sensoren: Temperatur, Luftfeuchte, Druck, Wasserstand, Füllstände,...; Aktoren: Heizung, Kühlung, Rollladenbetrieb, Stellmotoren, ...;
 4. Internet: Informationen werden über WEB-Services (http) angeboten – weltweit, öffentlich, Intranet: Informationen werden über WEB-Services (http) angeboten – LAN-weit, innerbetrieblich
2. a) wahr b) wahr c) wahr d) wahr e) wahr f) wahr g) wahr h) falsch
3. 2^{12} , da 12 Bit VLAN-ID
4. zwischen den Switches
5. 1. Falsch 2. Falsch 3. Richtig 4. Richtig 5. Falsch
6. Richtig 7. Richtig 8. Richtig 9. Falsch 10. Richtig
6. a) falsch b) falsch c) wahr d) wahr e) falsch f) falsch g) falsch
7. On-Prem: LAN-Datenrate (sehr hoch); Off-Prem und Colocation abhängig von der Internetanbindung über den Provider
8. Off-Prem, da Shop im Internet permanent gut erreichbar sein muss
9. Individuelle Lösung, z.B.:
 - Print-Service: stellt Drucker im Netzwerk zur Verfügung
 - Mail-Service: empfängt und versendet E-Mails intern und im Internet
 - Namensauflösungs-Service: liefert zu Internet-Namen (URLs) die dazugehörigen IP-Adressen
 - Web-Service: stellt HTTP-Web-Inhalte zur Verfügung
 - Shop-Service: stellt eine Internet-Verkaufsplattform (Handelsplattform) zur Verfügung
 - Update-Service: hält Updates und Patches vor, um die Wartung der PCs zu erleichtern
 - Anwendungsservice: stellt verschiedene Anwendungsprogramme zur Verfügung
 - Virtualisierungsservice: stellt virtuelle Rechner für Thin Clients zur Verfügung
 - Game-Service: stellt Onlinespiele zur Verfügung
 - Telefonservice: stellt Telefondienste zur Verfügung
10. Backbone (Rückgrat)
11. Stellt den Kunden den Zugang zum Internet bereit
12. Carrier

13. 1. Falsch 2. Richtig 3. Richtig 4. Falsch 5. Richtig 6. Falsch 7. Richtig 8. Richtig
9. Falsch
14. Off-Premises
- 15.

Arbeitsplatz	Rechner	Begründung
Service-Desk im KundenEingangsbereich	5	keine Anwendungen, die Rechenleistung erfordern, geringe Netzwerkbandbreite notwendig, hohe Sicherheit, da keine externen Datenträger möglich
Softwareentwicklung	2	hohe Rechenleistung nötig, teilweise hohe Netzwerklast
Sachbearbeiter Einkauf	1	keine große Rechenleistung nötig, geringes Datenvolumen auf dem Netz
Sachbearbeiter Verkauf/ 50 % Homeoffice	3	leistungsfähiger mobiler Rechner notwendig, Inhouse mit Dockingstation, mobil mit VPN
Vertrieb - Innendienst mit Außendienst	3	leistungsfähiger mobiler Rechner notwendig, Inhouse mit Dockingstation, mobil mit VPN
Konstruktion/CAD	2	hohe Rechenleistung nötig, teilweise hohe Netzwerklast
Lager - Büro	1	keine große Rechenleistung nötig, geringes Datenvolumen auf dem Netz
Lager - Kommissionierung mit Gabelstapler	4	Mobilität mit passablem Netzwerkanschluss
Marketing - Erstellen von Werbebroschüren	2	hohe Rechenleistung nötig für Grafikprogramme, teilweise hohe Netzwerklast

TAG 4 und TAG 5

- a) richtig b) richtig c) falsch d) richtig e) richtig
- Individuelle Lösung (Besprechen Sie Ihre Lösung mit dem Ausbilder)
- 200 Mbit/s, je Richtung 100 Mbit/s
- a) 6,6 s bei 150MByte/s
b) 2,2 s bei 450MByte/s
c) USB 2.0: 200 s, USB 3.0: 26s
- a) ca. 4,7 s
b) ca. 4,7 ms
c) Die Signalausbreitung/Laufzeit ist etwa gleich schnell.
- Carrier Sense Multiple Access/Collision Detection (CSMA/CD) Listen before talk
- Individuelle Lösung, z. B.: Welche Station darf wann das Netzwerkmedium für sich beanspruchen? Auflisten und kurze Erklärung der Standardverfahren CSMA/CD und CSMA/CA
- Es sind $8(2^3)$ Prioritätsstufen bei VLAN möglich.
- a) 1 518B
b) 14 B
c) 18 B (14 Byte Header plus 4 Byte Prüfsumme)
d) 46 B Nutzdaten + 14 B Header + 4 B Prüfsumme = 64 B

- e) 1 500 B
- f) Kennung, dass es sich um einen Frame eines VLAN handelt
- g) Trunk ist die Leitung zwischen den Switches, mit ETH-Frames mit VLAN-Tags
- h) Abgrenzen und schützen von einzelnen Netzen in einem LAN
- i) Type 0800 = IP-Protokoll als Nutzdaten
- j) Type 8100 = VLAN-Tag
- 10. a) richtig b) richtig c) richtig d) richtig e) falsch
- 11. Web-Anwendung, Surfen
- 12. Individuelle Lösung, z.B.

Beispiele für Standard-Ports (TCP)

Port-Nummer	Protokoll	Anwendung
21	FTP	Dateitransfer (FTP-Server)
23	Telnet	Konsole (Server)
25	SMTP	Postausgang (SMTP-Server)
80	HTTP	World Wide Web (Webserver)
110	POP	Posteingang (POP-Server)
119	NNTP	Usenet (News-Server)

Beispiele für Standard-Ports (UDP)

Port-Nummer	Protokoll	Anwendung
53	DNS	Domain Name Server
69	TFTP	Trivial File Transfer Protocol
137	NetBIOS-ns	NetBIOS Nameserver
138	NetBIOS-DGM	NetBIOS-Datagramm-Dienst
161	SNMP	Simple Network Management Protocol

- 13. a) Well-Known-Ports b) Registered Ports c) 2

14.

Port	Anwendung	Beispiel, Erläuterung
80	Webdienste	Browser, Webserver
1194	OpenVPN	sichere Verbindung mit einem Netz über das Internet
22	SSH	sichere Kommandozeile
123	NTP	genaue Uhrzeit im Internet abrufen
433	HTTPS	Webdienst über HTTP, gesicherte Verbindung

Port	Anwendung	Beispiel, Erläuterung
20	FTP-Data	FTP-Datenübertragung
21	FTP-Command	FTP-Steuerkommandos
631	IPP	Internet Printing Protocol, drucken auf entfernte Drucker
143	IMAP	E-Mail-Dienst
80	WEB	Webdienst über HTTP
110	POP3	E-Mail von einem Server abrufen mit POP3
210	AppleTalk	Kommunikation mit Apple-Rechnern

15. a) falsch b) falsch c) falsch d) falsch

16. Individuelle Lösung, z.B.

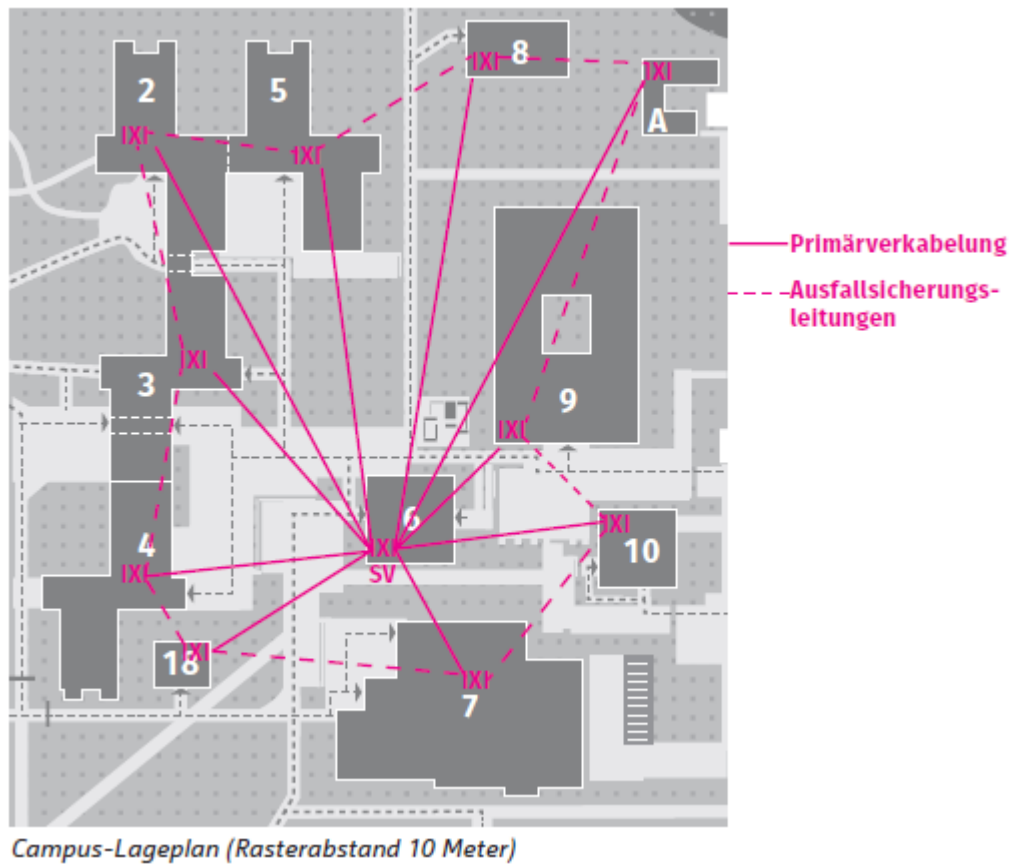
- Infrastructure-as-a-Service (IaaS) stellt Nutzern Computing-, Networking- und Storage-Ressourcen bereit.
- Platforms-as-a-Service (PaaS) bietet eine Plattform zur Ausführung von Anwendungen sowie die dazu notwendige IT-Infrastruktur.
- Software-as-a-Service (SaaS) stellt dem Nutzer im Grunde eine Cloud-Anwendung bereit sowie eine Plattform nebst zugrunde liegender Infrastruktur zu deren Ausführung zur Verfügung.
- Function-as-a-Service (FaaS) ist ein ereignisgesteuertes Ausführungsmodell, mit dem Entwickler App-Pakete ohne jegliche Wartung der Infrastruktur erstellen, ausführen und verwalten können.

17.

Anwendungsfall	Cloud oder eigener Serverdienst (mit Begründung)
Das tägliche Datenvolumen wächst und der Fileserver kommt bald an seine Grenzen.	Eigener Server, HDD ausreichend dimensionieren
Durch eine Werbeaktion wird in den nächsten vier Wochen eine hohe Zahl an Zugriffen aus dem Internet erwartet.	Cloud-Server, da Bedarf nur temporär während der Werbeaktion
Virtuelle Server sollen lastabhängig hoch- und heruntergefahren werden.	Cloud-Server, da Server nicht vorgehalten werden müssen
Die Internetanbindung eines Datacenters ist im Regelbetrieb ausreichend. Zu Stoßzeiten ist der Datendurchsatz aber zu gering.	Cloud-Server, da bessere Anbindung ans Internet
Es werden sensitive Daten verarbeitet, die auf keinen Fall über das Internet übertragen werden sollen.	Eigener Server, höhere Sicherheit, da Daten das Haus nicht verlassen
Es werden sensitive Daten verarbeitet, die im Geltungsbereich des deutschen Datenschutzrechtes gespeichert werden müssen.	Eigener Server, oder Cloud mit Hosting in D

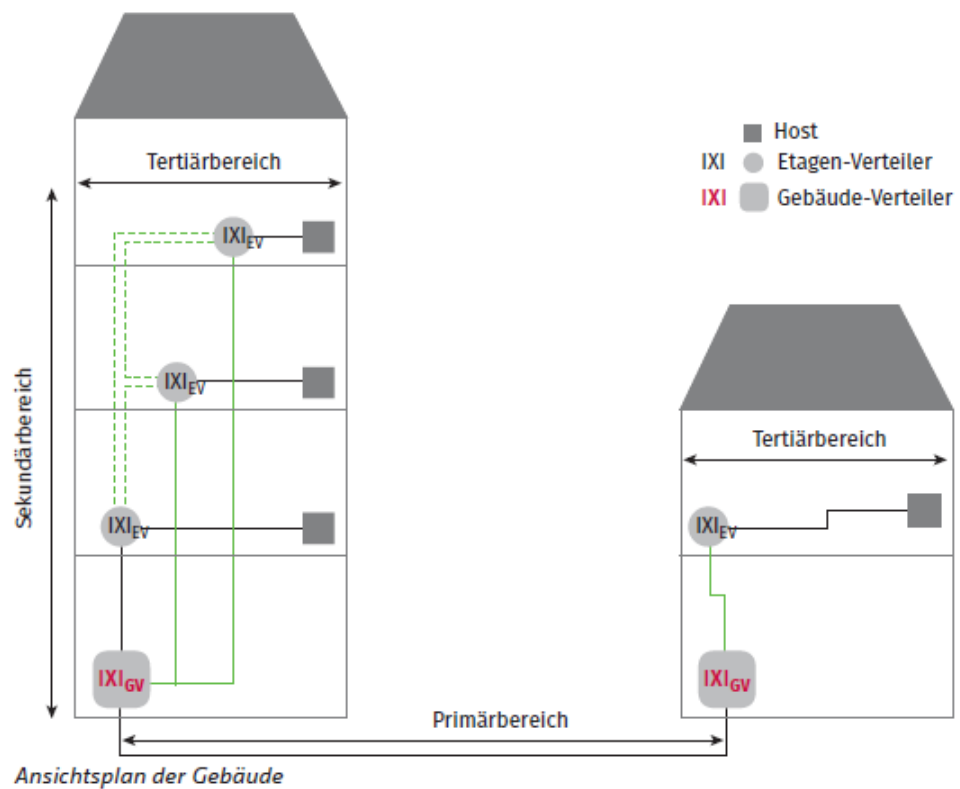
TAG 6, TAG 7 und TAG 8

1. a) falsch b) falsch c) richtig d) richtig e) falsch f) falsch g) richtig
2. Individuelle Lösung;
Skizze und Beschreibung für Stern, erweiterter Stern, unvollständige Masche
3. a) richtig b) falsch c) falsch d) richtig e) falsch
4. Das schlechteste Bauteil (hier: CAT5) bestimmt die Leistungsfähigkeit und die Verkabelungsklasse.
5. Alte, schlechtere Patchleitung oder schlechtere Anschlussleitung
6. Permanent-Link 90 m, Channel-Link 100 m
7. a) b) c)

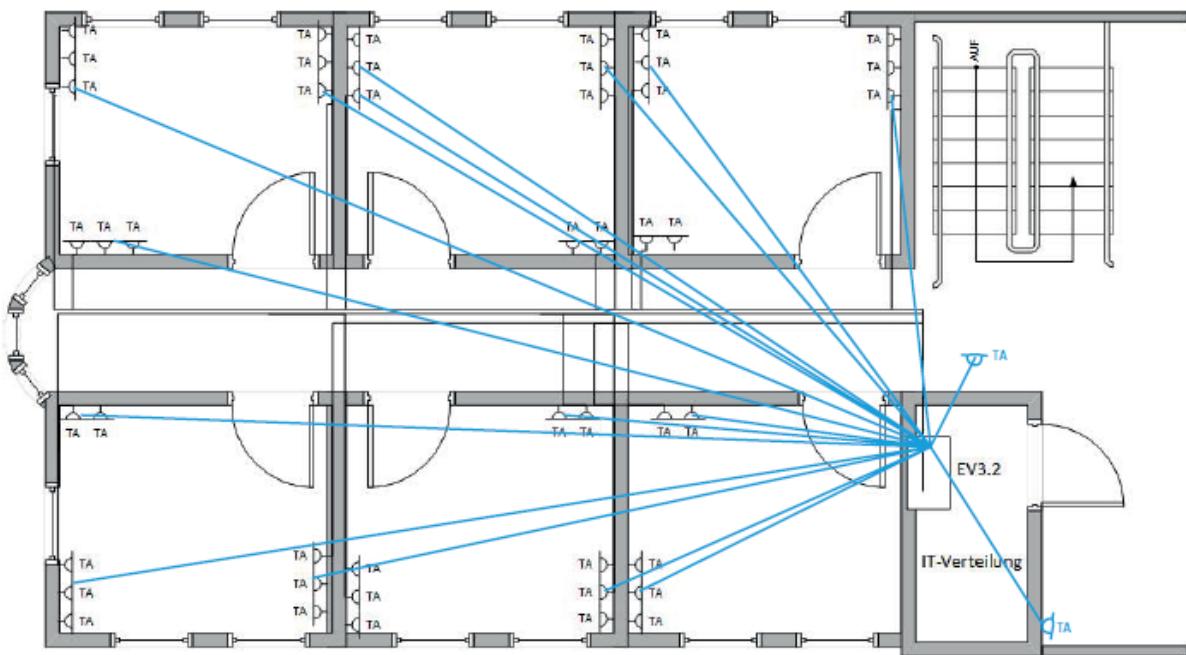


- d) Individuelle Lösung, Standortverteiler zentral, bspw. in Gebäude 6
- e) Individuelle Lösung, Glasfaser wegen der hohen Datenrate und der großen Distanzen im Primärbereich

f)



8.



9.

Anwendung	Leitungstyp	Begründung
Anschluss einer Grafik-Workstation	Leitung 2	Klasse F_A bietet ausreichenden Datendurchsatz
Anschluss einer Webcam mit Stromversorgung über das Netzwerk	Leitung 1 und Leitung 3	Klasse E ausreichend für diesen Einsatz, Leitung 3 eventuell preiswerter
Anschluss für einen PC	Leitung 1	Klasse E ausreichend, durch Folienschirm (F/UTP) weniger störempfindlich

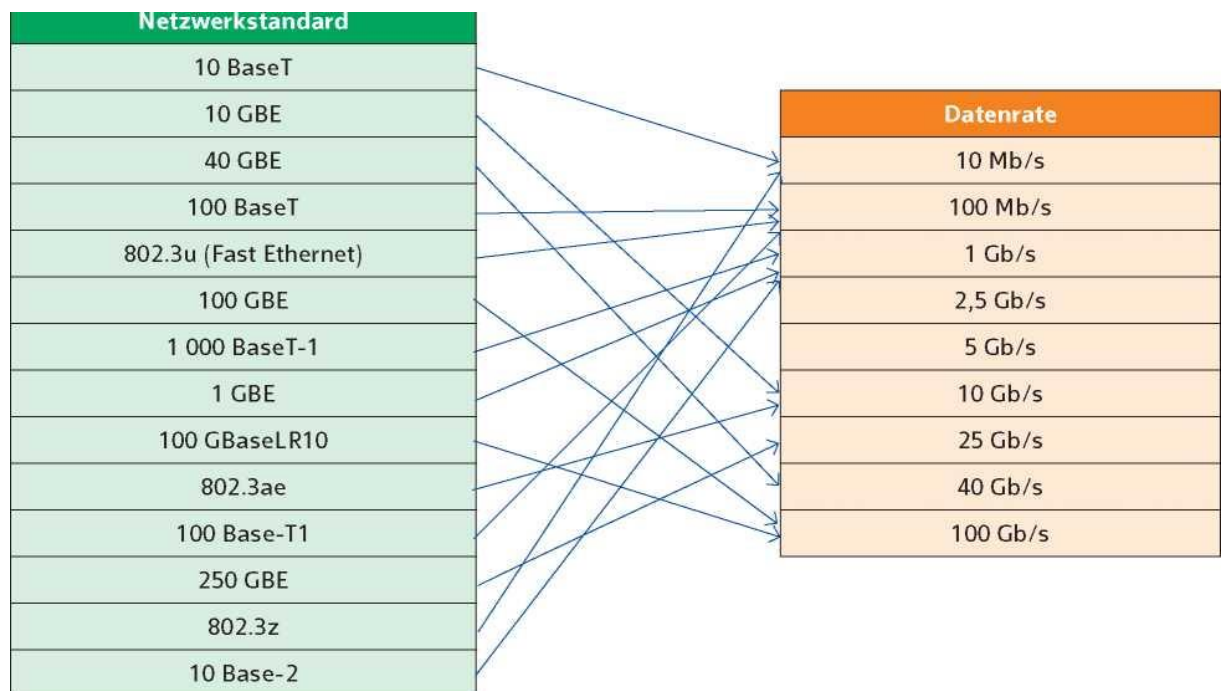
10. Je höher die AWG-Zahl desto dünner der Draht; AWG gibt die Anzahl der Ziehvorgänge an.

11.

Anwendungen für Netzwerkgeräte	
In einem Kleinbetrieb werden im Büro zwei weitere PCs benötigt.	(A) oder (B)
In einem größeren Betrieb wird das Firmen-LAN in Subnetze aufgeteilt. Jedes Gebäude bekommt ein eigenes Subnetz.	(D)
In einer Bank werden die Sicherheitsvorkehrungen verschärft. Das LAN wird in kleinere VLANs für die verschiedenen Arbeitsgruppen aufgeteilt.	(C)

12. Individuelle Lösung; z.B. MAC-Adressen auf Layer 2, Forwardingtable, ...
13. Individuelle Lösung; z.B. CSMA/CD
14. Individuelle Lösung; z.B. Switch Layer 2 mit MAC-Adr., Router Layer 3 mit IP-Adresse, größere Latenzzeit bei Router, etc.

15.



16. Switch - OSI-Layer 2, Router - OSI-Layer 3

17.

OSI-Layer Nr.	ISO/OSI-Modell Bezeichnung der Schicht	TCP-Layer Nr.	TCP/IP-Modell Bezeichnung der Schicht	Netzwerkgerät	Adressen
7	Application L.	4	Application L.		
6	Presentation L.				
5	Session L.				
4	Transport L.	3	Transport L.		Port-Nr.
3	Network L.	2	Host-to-Host L.	Router	ID-Adr.
2	Data-Link L.	1	Network-Access-L.	Switch	MAC-Adr.
1	Physical L.			Hub	

18. Domain Name System-Protocol, DNS-Protokoll

19. Address Resolution Protocol, ARP

20. Dynamic Host Configuration Protocol, DHCP

21. a) wahr b) falsch c) falsch d) falsch e) wahr f) wahr g) wahr h) wahr

22. a) richtig b) richtig c) falsch d) richtig e) richtig f) richtig g) richtig

23.

Adresse	OSI-Schicht	Adressgröße (Anzahl Bits)	Schreibweise (Beispiel)	Was wird adressiert?
MAC-Adresse	2	48 bit	00-11-22-33-44-55	Netzwerk-Interface
IP-Adresse	3	32 bit	10.20.11.12	Netz und Host
IP-Adresse	3	32 bit	10.20.11.12	Netz und Host
MAC-Adresse	2	48 bit	00-11-22-33-44-55	Netzwerk-Interface
MAC-Adresse	2	48 bit	00-11-22-33-44-55	Netzwerk-Interface
IP-Adresse	3	32 bit	10.20.0.0/16	Netzwerk
MAC-Adresse	2	48 bit	00-11-22-33-44-55	Netzwerk-Interface
Port	4	16 bit	80	Anwendung
MAC-Adresse	2	48 bit	00-50-56-C0-00-08	Netzwerk-Interface
IPv6-Adresse	3	128 bit	2a02:8070:88a3:9d00::13dd	Netz und Host

24. a) 1.0.0.0 b) 1.2.0.0 c) 2.3.4.0 d) 3.4.5.0 e) 4.5.6.4

25. a) 100.150.200.250 b) ~~200.250.300.350~~ c) 10.20.30.40 d) 10.255.255.2

e) ~~123.234.345.123~~

26.

Privater IP-Adressbereich	IP-Adressklasse	Subnetze (Anzahl und Beispiele)
10.0.0.0/8	Class A	ein Netz, keine Subnetze
172.16.0.0/12	Class B	16 Subnetze (172.16.0.0/16, 172.17.0.0/16 bis 172.31.0.0/16)
192.168.0.0/16	Class C	256 Subnetze (192.168.0.0/24, 192.168.1.0/24, bis 192.168.255.0/24)

TAG 9

1. Nein, verschiedene Netze, kein Ping
2. a) IPv6 aktiviert
b) PC: 192.168.178.27, Router = Gateway: 192.168.178.1
c) E8-B1-FC-03-2D-0C
d) 10 Tage
3. Namensauflösung funktioniert nicht ohne DNS-Adresse, aber Internet funktioniert (mit IP-Adressen); ohne Router-Adresse kein Internet
4. Individuelle Lösung
5. Individuelle Lösung
6. a) falsch b) richtig c) falsch d) richtig
7. Authentifizierung, Autorisierung, Accounting
8. Authentifizierung identifiziert einen bestimmten User, Autorisierung stattet einen User mit Berechtigungen aus.
9. a) Einstellungen öffnen - Konten - Familie und andere Benutzer - Familienmitglied hinzufügen
b) Eingabeaufforderung öffnen, Befehl „net user NAME PASSWORT /add“ eingeben, für Homeverzeichnis mit „md users\NAME“ neues Verzeichnis anlegen. Hilfe vom System über „?“, z.B.: „net user ?“ für die genaue Syntax eines Befehls

TAG 10

1. a) wahr b) falsch c) falsch d) wahr
2. Individuelle Lösung, evtl. falsche Gateway-Einstellung, Proxy-Einstellung,...
3. Proaktives IT-Management
4. Individuelle Lösung
5. Individuelle Lösung, a) und b) Individuelle Lösung

TAG 11

1. Speichern der MAC-Adressen der angeschlossenen Hosts, Speichern der Ethernet-Frames
2. PoE-fähige Switches werden zum Speisen von Endgeräten, z. B. Telefone, benötigt.
3. a. Falsch f. Falsch k. Richtig
b. Falsch g. Richtig l. Falsch
c. Richtig h. Falsch m. Richtig
d. Falsch i. Richtig n. Falsch
e. Falsch j. Richtig o. Richtig
4. 1. Individuelle Lösung, (Lösung mit Ausbilder besprechen)
2. Individuelle Lösung, (Lösung mit Ausbilder besprechen)
5. a) falsch b) falsch c) wahr d) wahr e) wahr f) wahr
6. 15 bit/s/Hz
7. Wellenlängenmultiplex
8. a) bis c) individuelle Lösung

TAG 12 und TAG 13

1. RAID: Redundant Array of independant Disks; JBOT: „Just a Bunch of Disks“; NRAID: „NotRAID“

2. RAID0 keine Sicherheit, RAID1 Sicherheit durch Spiegelung, eine Platte darf ausfallen
3. a) Falsch b) richtig c) Falsch d) falsch e) falsch
f) Richtig g) Falsch h) Richtig i) Falsch j) Richtig
k) Falsch l) Falsch

4.

4 × 1 TB 5	→ 3TB
4 × 1 TB 6	→ 2TB
2 × 1 TB 0	→ 2TB
2 × 1 TB 1	→ 1 TB

5. Inkrementelles Backup
6. Auf einem Image-Backup werden auch gelöschte Dateien gesichert, die physisch noch auf der Platte gespeichert sind

7.

0: keine Sicherheit, doppelte Ausfallwahrscheinlichkeit

1: Daten doppelt vorhanden - sehr sicher, halbe Ausfallwahrscheinlichkeit (beide Platten müssen ausfallen)

5: Daten durch Parity sehr sicher - für Datenverlust müssen zwei Platten ausfallen. Ausfallwahrscheinlichkeit 1/2

6: Daten durch doppelte Parity sehr sicher - für Datenverlust müssen drei Platten ausfallen. Ausfallwahrscheinlichkeit 1/3

10: Daten sicher durch RAID1, vergrößert mit RAID0 - geringere Ausfallwahrscheinlichkeit als RAID01

01: Daten sicher durch RAID1 über 2 unsicher RAID0 - höhere Ausfallwahrscheinlichkeit als RAID10

8.

$$2^{40} B / 360 * 10^6 B/s = 3054 s = 50,9 \text{ min}$$

$$2^{40} B / 90 * 10^6 B/s = 1\,222 s = 20,3 \text{ min}$$

aus Zeitgründen mit Datenkompression sichern

9. Datenvolumen 4 TB, Bandkapazität 12 TB, freier Bandspeicher 8 TB, tägliche Datenzunahme 500 MB, $8 \text{ TB} : 500 \text{ MB/Tag} = 16\,000 \text{ Tage}$, bis Speicherkapazität des Bandes voll ist.

Dauer der aktuellen Sicherung:

$$t = D : C = 4 \text{ TiB} : 300 \frac{\text{MB}}{\text{s}} = 1,466 * 104 s = 244,3 \text{ min} = 4,07 \text{ h.}$$

Bei Sicherungsstart um 4:00 Uhr läuft die Sicherung bis 8:00 Uhr! Sicherung muss früher gestartet werden! Auch könnte man die Datenkomprimierung verwenden. Dies reduziert die Sicherungsdauer auf etwa ein Drittel!

Sollte das Band voll sein → Sicherungsdauer 12,2 h! Mit Kompression ca. 4 h.

10.

Tag	Band-Nr.	Sicherungsart
Montag	1	Incrementell
Dienstag	2	Incrementell
Mittwoch	3	Incrementell

Tag	Band-Nr.	Sicherungsart
Donnerstag	4	Incrementell
Freitag	5	Vollsicherung Freitag 1
Samstag	X	X
Sonntag	X	X
Montag	1	Incrementell
		Incrementell
Freitag	6	Vollsicherung Freitag 2
		Incrementell
Freitag	7	Vollsicherung Freitag 3
		Incrementell
Freitag	8	Vollsicherung Monatssicherung 1

11. Server in der DMZ sind gegen Angriffe von innen und außen geschützt, ein Angreifer von außen hat zwei Firewalls zu überwinden.
12. Ein Proxy geht stellvertretend für andere Rechner ins Internet, ersetzt deren IP-Adressen durch seine. Er kann Sperrlisten verwalten und Inhalte filtern. Ein Proxy-Server speichert Webinhalte zwischen, falls sie später erneut abgerufen werden.
13. a) wahr b) falsch c) wahr
14. $8\,760\,h * 0,95 = 8322\,h$
15. $t_{ges} = 1\,Monat = 720h; t_d = (1 - A) * t_{ges} = 0,36h = 21\,min$
16. $p1 = 0,000.02; p2 = 0,05 p_{ges} = p1 * p2 = 0,000.0001 = 10^{-6}$

TAG 14

1. a) falsch b) richtig c) richtig d) falsch e) richtig
2. $0,9 * 0,95 = 0,855$ oder 85,5 %
3. 100 %, da Akku geladen ist und Last direkt am Netz hängt
4. Individuelle Lösung
5. Individuelle Lösung; sinusförmig bei Netz, trapezförmig bei Batteriebetrieb, bis 10 ms Umschaltunterbrechung
6. 13,33 ms, da $1/60\,Hz = 26,66\,ms$ Periodendauer
7. $P = 5 * 500\,W = 2\,500\,W, I = 10,87\,A$, Sicherung ist ausreichend
8. $P = 1\,400\,W, I = 6,52\,A$, Absicherung ausreichend
9. $1/0.9 = 1,11\,kW$
10. a) falsch b) falsch c) wahr d) wahr e) falsch f) wahr g) wahr
11. a) falsch b) richtig c) falsch d) richtig e) falsch f) richtig
12. $W = 8\,760\,h * 100\,Watt = 876\,000\,Wh = 876\,kWh$ bei 0,25 € pro kWh: 219,00 € Stromkosten pro Jahr oder 18,25 € pro Monat
13. $P = 590\,W, I = 2,56\,A$
14. Individuelle Lösung
15. Videokarte liefert immer ein Bild, der Monitor geht nicht in Standby
16. Richtig: 1., 2., 3., 4., 5., 6., 8., 9.