

ISO/OSI und TCP/IP

Tabelle

NR:	OSI Schicht: Ablauf (2 Mal)	Aufgabe:	NR:	TCP/IP-Schicht:	Adressierung:	Komponente:	Einheiten:	Protokolle:
7	Application Layer Anwendungsschicht Brief	Anwendung	4	Application Layer Anwendungsschicht		PC (Host)	Daten	HTTP FTP HTTPS SMTP LDAP NCP
6	Presentation Layer Darstellungsschicht Couvert Briefkasten							
5	Session Layer Sitzungsschicht Briefkasten geleert							
4	Transport Layer Transportschicht Poststelle	Transport	3	Transport Layer Transportschicht	Portnummern	Firewall (oder höher)	TCP = Segmente UDP = Datagramme	TCP UDP SCTP SPX
3	Network Layer Netzwerkschicht Wagen	Vermittlung	2	Internet Layer Netzwerkschicht	IP Adresse	Router Layer-3 Switch	Pakete	ICMP IGMP IP IPsec IPX
2	Data Link Layer Verbindungsschicht Container	Netzzugriff	1	Network Access Layer Verbindungsschicht	Mac Adresse (OSI 2)	Bridge Switch Hub (eher)	Ethernet Frames	Ethernet Token Ring FDDI ARCNET
1	Physical Layer Physikalische Schicht (Bit) Strasse					Hub, Kabel(Koaxial, Twisted Pair, Glas), WLAN AP, Repeater(Verstärker)	Bits Symbole Pakete	

OSI Schicht 1: Der Physical Layer (Physikalische Schicht) stellt, wie der Name schon sagt, die physikalische Einheit der Kommunikationsschnittstelle dar. In dieser Schicht (auch als Bitübertragungsschicht bezeichnet) werden sämtliche Definitionen und Spezifikationen für das Übertragungsmedium (Strom-, Spannungswerte), das Übertragungsverfahren oder auch Vorgaben für die Pin-Belegung und die Anschlusswiderstände festgelegt.

OSI Schicht 2: Aufgabe der zweiten Schicht, der sogenannten Verbindungsschicht (Data Link Layer), ist die erste Bewertung der eingehenden Daten. Durch Überprüfung auf korrekte Reihenfolge und Vollständigkeit der Datenpakete werden beispielsweise Übertragungsfehler direkt erkannt. Dazu werden die zu sendenden Daten in kleinere Einheiten zerlegt und als Blöcke übertragen. Ist ein Fehler aufgetreten, werden einfach die als fehlerhaft erkannten Blöcke erneut übertragen. Die Sicherungsschicht sorgt auch für eine synchrone Datenübertragung, wobei durch zusätzliche Steuersignale gewährleistet wird, dass der Empfänger genau in dem Moment empfangsbereit ist, wenn eine Datenübertragung beginnt.

OSI Schicht 3: Die dritte Schicht (Netzwerkschicht) übernimmt bei einer Übertragung die eigentliche Verwaltung der beteiligten Kommunikationspartner. Dabei werden insbesondere die ankommenden bzw. abgehenden Datenpakete verwaltet. So erfolgt in dieser Schicht, die auch als Vermittlungsschicht bezeichnet wird, unter anderem eine eindeutige Zuordnung über die Vergabe der Netzwerk-Adressen. Dies geschieht insbesondere, indem der Verbindung weitere Steuer- und Statusinformationen hinzugefügt werden.

OSI Schicht 4: Die Transportschicht stellt die Verbindung zwischen den Systemschichten 1 bis 3 und den Anwendungsschichten 5 bis 7 her. Dies geschieht, indem die Informationen zur Adressierung und zum Ansprechen der Datenendgeräte (z.B. Arbeitsstationen) hinzugefügt werden. Aus dem Grund enthält diese Schicht auch die meiste Logik sämtlicher Schichten.

Während die Schichten 1 bis 3 als systembezogene Schichten bezeichnet werden, sind die Schichten 5 bis 7 immer anwendungsbezogen.

OSI Schicht 5: Der Session Layer ist die sogenannte Steuerungsschicht der Kommunikation (Sitzungsschicht). Auf dieser Ebene wird der Verbindungsaufbau festgelegt und sofern es bei einer Übertragung zu einem Fehler oder zu einer Unterbrechung t, wird dies von der Schicht 5 (Kommunikationsschicht) abgefangen und entsprechend ausgewertet. Die Hauptkriterien der Auswertung beziehen sich dabei beispielsweise auf die Passwörter, die Stationsnamen (logische Adressierung), auf Dialogverfahren oder auch auf die Verbindungs-Synchronisation und den Wiederaufbau einer Sitzung nach einem Ausfall in den unteren vier Schichten.

OSI Schicht 6: Auf der Anwendungsschicht (*Presentation Layer*) werden die notwendigen Möglichkeiten für die Ein- und Ausgabe der Daten bereitgestellt. Dazu gehört beispielsweise die Anzeige von Anweisungen und entsprechenden Fehlermeldungen. So werden auf dieser Ebene beispielsweise die Daten-Ein- und Ausgabe überwacht, Übertragungskonventionen festgelegt oder auch Bildschirmdarstellungen angepasst.

OSI Schicht 7: Die oberste Schicht des OSI-Referenzmodells ist diejenige, mit der ein Anwender „in Berührung“ kommt; es ist dies die Schnittstelle zwischen dem Rechner und dem Anwendungsprogramm. Auf dieser Ebene werden die in einem Netzwerk verwendeten Programme (Anwendungen) eingesetzt, wobei darüber hinaus beispielsweise auch Netzwerk-Ressourcen zur Verfügung gestellt werden. **PC**

Allgemeines:

IPv4 Adresse: 32 Bit lang

Verbindungsgeschwindigkeiten: Verkabelung Kat. 5e = 1000 Mbit/s • WLAN = 300 Mbit/s • PowerLAN = 500 Mbit/s

Ethernet-Standard IEEE 802.3: Bei Ethernet handelt es sich um eine normierte Technik für kabelgebundene Datennetze

Grundwissen über Netzwerke:

Netzwerk: Ein Netzwerk ist die Verbindung von Computern über eine oder mehrere Leitungen oder auch per Funk. Daten jeglicher Art austauschen.

PAN: Persönliches Netzwerk für Kleingeräte.

LAN: Local Area Network (lokales Netzwerk), auf ein Grundstück begrenzt, begrenzte Ausdehnung, geringe Fehlerrate, hohe Datenübertragungsrate, wahlfreien Zugriff

MAN: Metropolitan Area Network (Netzwerk einer Stadt oder Agglomeration), Erweiterung eines Netzwerks in Stadt- oder Regionalnetz, schnellen Datenaustausch mehrere LANs zu einem MAN

WAN: Wide Area Network (überregionales Netzwerk), Bsp. kantonale Behörde kantonales eigenes Netzwerk

GAN: Global Area Network (grossräumiges, oft weltumspannendes Kommunikationssystem), Anwender tritt indirekt über die lokalen Zugangsnetze bei GAN. Ein Beispiel für ein solches Netz ist das Internet.

Peer-to-Peer-Netzwerk: In einem Peer-to-Peer-Netzwerk sind alle Computer gleichberechtigt und können sowohl Dienste in Anspruch nehmen, als auch zur Verfügung stellen. Peripheriegeräte sind auch angeschlossen

Sharing Möglichkeiten Peer-to-Peer: -File Sharing -Drucker teilen -Programm Sharing -einfacher Anschluss auf andere Netze(Internet) -CD/DVD-ROM Laufwerke gemeinsam nutzen -zentrale Datensicherung

Serverbasierten Netzwerk: •Zugriffsschutz auf bestimmte Speichermedien, Druckersteuerung, Verwaltung gemeinsamer Daten und Dokumente, Datensicherung, Weiterleitung von E-Mails an ein externes Netz (z. B. Internet) Server: Applikationsserver, Fileserver, Printserver

Unterschied Peer-to-Peer: Server verwaltet zentrale Datenbank die Zugangs- und Zugriffsberechtigungen aller Benutzer und Benutzergruppen (Benutzerrechte). Benutzername und Kennwort stellen die Login-Informationen dar. (Zentrale Verwaltung)

Erklären Sie den Zusammenhang zwischen MAC- und IP-Adressen. Stellen Sie den Ablauf eines ARP-Requests grafisch dar.

Eine MAC-Adresse identifiziert ein Gerät eindeutig und kommt nur einmal auf der ganzen Welt vor, wobei die IP-Adresse nur im jeweiligen Netzwerk einen eindeutigen Namen hat. Somit wird das Gerät adressierbar und damit erreichbar (kann auf ein Netz zugreifen).

Netzwerkgeräte:

DSL Router: Kombination von Netzwerkverbinder(Ethernet) & Protokollübersetzer(VDSL ADSL)

Kabel-Modem: hat min. 1x Koaxial Anschluss & 1x RJ45

Router: Verbindet min. 2 Ethernet Netzwerke

Powerline Adapter: Netzwerkerweiterung(braucht keine baulichen Massnahmen) über Stromleitung

WLAN-Access Point: Schnittstelle für kabellose Kommunikationsgeräte

Netzwerkkarte: Schalter zum Verbinden von PC

Firewall: Router auf OSI Layer 4 & 5, Sicherungssystem

Splitter: Frequenzbereich-Trenner

Switch: Zentrum der sternförmigen Verkabelung. Leitet alle Daten im Netz weiter zum gewünschten Gerät nicht wie ein Hub der es an alle schickt.

Netzwerkdienste:

Peer to Peer: eignet sich für weniger als 10 Benutzer (Einrichtung zu gross) und es können Netzwerkdienste (z.B. Printer) gemeinsam genutzt werden.

Ethernet-Frame: wird mit MAC Adresse adressiert und Datenrahmen (Layer 2 OSI)

Gateway: Host, der lokale Netzwerke mit Nächstem verbindet

Portnummer: Adressierungsart (Layer 4 OSI)

DHCP: automatische IP Adressen Zuteilung

DNS: Verfahren von Physikalische in IP Adresse

Ping: Befehl, Erreichbarkeit von Hosts im Netzwerk testen

ARP: Verfahren zur Umsetzung der physikalischen Adresse in eine IP-Adresse.

Grundwissen über Topologie und Verkabelung

Topologie:

Stern-Topologie: alle Arbeitsstationen werden an einen zentralen Knoten(Switch) angeschlossen

Ring-Topologie:

alle Arbeitsstationen sind gleichberechtigt, kein zentraler Knoten vorhanden, jeder eigener Netzanschluss

Bus-Topologie: kein zentraler Knoten, Verbindung mit gemeinsamer Übertragungsleitung

Verkabelung:

LAN-Technik Ethernet: kabelgebundene Datennetze

Koaxialkabel: Innenleiter im Zentrum

Verdrillte Leitungen: Hin- und Rückleiter zusammengeführt und wie eine Spirale ineinander verdreht

Lichtwellenleiter: Glasfaserkabel werden anstelle elektrischer Impulse optische Signale übertragen

Twisted-Pair-Kabel: 4 x 2 Kupferdrähte, welche paarweise verdreht, •geschirmt(jedes Kabelpaar) •ungeschirmt(Gesamt)

U/UTP-Kabel: 2 Kupferadern, Ohne Abschirmung, verdreht

LanKabel Kat5e.(min. 100Mbps)

S/STP-Kabel: Abschirmung für jedes Kabelpaar & Gesamtschirm

S/UTP-Kabel: Gesamtschirm aus Kupfer

F/UTP-Kabel: Gesamtschirm aus alukaschierter Kunststoff-Folie

SF/UTP-Kabel: Gesamtschirm aus Polyesterfolie(Kombination aus S/UTP-Kabel & F/UTP-Kabel)

Abkürzung Beschreibung und Merkmale

10BaseT: 10 Mbit/s Ethernet mit Twisted-Pair-Kabel.

10BaseFL: 10 Mbit/s Ethernet-Glasfaserkabel.

100BaseTX: 100 Mbit/s Ethernet mit Twisted-Pair-Kabel.

1000BaseTX: GBit/s Ethernet Kupferkabel mit 4-Adernpaaren und einer Übertragung von 1000 Mbit/s (nicht in IEEE 802.3 standardisiert).

Ablauf Auftrag planen

1. Bedürfnisse des Kunden abklären (Ausgangs Situation/ Wünsche des Kunden)

2. Anforderungskatalog erstellen

Id	Name	Anforderung
A1	Internet	Internetanschluss für zwei oder mehr PCs Mittelstarke Internetleitung

3. Soll-Ist Vergleich

Name	Soll	Ist
Internet	Mittelstarke Internetleitung Alle Computer sollen Internet haben	iPhone Internetzugriff

4. Lösungsvorschläge erarbeiten

Netzwerkdrucker, Netzwerkgeräte)

Internetzugang

Kriterium: Verfügbarkeit für, Download, Upload, Preis pro Monat, Aufschaltgebühr, Vorteile, Nachteile

Kriterium	Swisscom	Cablecom	EWB-Quickline
-----------	----------	----------	---------------

Fileserver für Datenablage

Kriterium: Kosten für Gerät und Betriebssystem, Wartungsaufwand, Strom-verbrauch, Stromkosten pro Jahr, Platzbedarf, Vorteile, Nachteile

Kriterium	Windows Server	Linux Server	Zyxel NAS
-----------	----------------	--------------	-----------

Netzwerkdrucker

Netzwerkgeräte

Gerät	Aufgabe	Begründung
-------	---------	------------

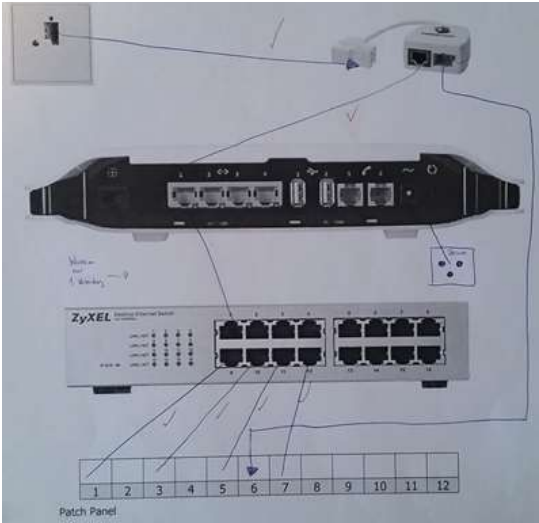
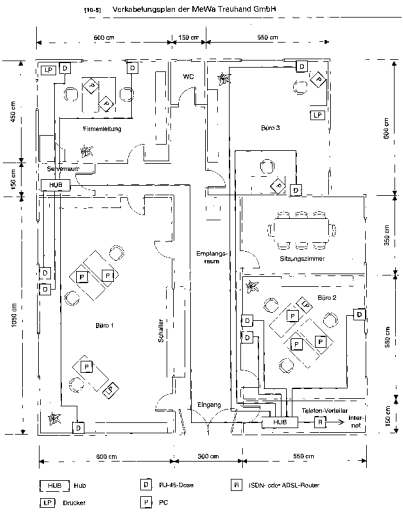
5. Netzwerk planen

Verbindungen planen

Kriterium: Kosten für Anbindung, Strom-verbrauch, Daten-Durchsatz(netto/brutto), Strahlung, Vorteile, Nachteile

Kriterium	Verkabelung Kat. 5e	WLAN	PowerLAN
-----------	---------------------	------	----------

Verkabelungsplan



Legende:	
PP	Patch-Panel
SW	Switch
D	RJ-45-Dose
R	Router
P	PC
LP	Drucker
Fs	File-Server
T	Telefon-Anschluss / Telefon
Sp	Splitter
blau:	UG-Verkabelung Kat 5e
rot:	Patchkabel Kat. 5e
grün:	Endgeräte, Möbel
orange:	Netzwerk-Komponenten

IP Adressen Konzept

Kriterium: Klasse, Subnetz-Maske, Max. Anzahl Hosts, Bereich für private Adressen, Netz-Adresse, Gateway, DNS-Server, File-Server, PC-Dänzer, PC Herren, DHCP-Bereich, Drucker, Broadcast

Kriterium	Adresse / Bereich / Klasse	Bemerkungen
-----------	----------------------------	-------------

Namenskonzept

Geräte: Swisscom-Router, Fileserver, PC Dänzer, PC Herren, Netzwerkdrucker

Gerät	Hostname
Swisscom-Router	

Benutzer, Gruppen, Shares und Berechtigungen planen

Benutzer	GL	MA	SU
pd			
mh			
sd			
eh			
supporter			

Netzlaufwerk	GL	MA	SU
S:			
T:			
V:			
U:			

X=Vollzugriff, L=Leseberechtigung, U= unsichtbar

Ablauf Auftrag durchführen

- Die Vorgaben kennenlernen
- Windows-Clients einrichten
- Benutzer und Gruppen einrichten
- Windows-Freigabe einrichten
- Netzwerkdrucker einrichten
- CD-Laufwerk freigeben
- Groupware AlphaAgent einrichten
- Samba-Server auf Ubuntu einrichten und konfigurieren

Ablauf Auftrag dokumentieren

- Projektübersicht erstellen
- Netz-Übersicht zeichnen
- Netzwerk-Diagramm zeichnen
- Konzepte darstellen
- Netzwerkgeräte auflisten
- Server und Arbeitsstationen dokumentieren
- Ansprechpartner auflisten
- Anhang erstellen

Konsolenbefehle

ip config /all, Ping IP-Adresse(zb. 192.168.210.11)

Warum werden gewisse Netzkabel mit Abschirmungen versehen?

Damit können äussere Störeinflüsse besser reduziert und ferngehalten werden.

Nennen Sie die drei Hauptmerkmale der Netznorm „Ethernet“. Ethernet verwendet eine Bus- oder Stern-Topologie

Die Verbindung der Netzknoten erfolgt durch Koaxial-, Glasfaser- oder Twisted-Pair- Kabel.

Ethernet regelt den Datenverkehr über das Zugriffsverfahren CSMA/CD (bei Bus-& Ring-Topologie)
CSMA CD: Carrier Sense Multiple Access/Collision Detection
CSMA CA: Carrier Sense Multiple Access/Collision Avoidance

	128.168.100.25
Netzwerkanteil	
Rechneranteil	
Netzidentifikation / Netzadresse	128.168.0.0
Subnetzmaske	255.255.0.0
Mögliche Rechnerbezeichnungen / Hostadressen	128.168.0.1 - 128.168.255.254

Netz-Typ	Bereich der «privaten IP-Adressen»
Klasse A	Von 10.0.0.0 bis 10.255.255.255
Klasse B	Von 172.16.0.0 bis 172.31.255.255
Klasse C	Von 192.168.0.0 bis 192.168.255.255

Klasse	Bereich	Subnetz-Maske	Max. Anz. Netze	Max. Anz. Rechner (Hosts)
Klasse A	0.0.0.0-127.255.255.255	255.0.0.0	128	16 777 214
Klasse B	128.0.0.0-191.255.255.255	255.255.0.0	16 384	65 534
Klasse C	192.0.0.0-223.255.255.255	255.255.255.0	2097152	254

IP-Adresse	Bezeichnung	Beschreibung (Zweck)
0.0.0.0	Default Gateway	Reserviert für die standardmässige Weiterleitung
127.0.0.1	Local host	Reserviert für die interne Kommunikation
255.255.255.255	Broadcast	Reserviert für Rundrufe (grösstmögliche Adresse im Teilnetzwerk)

Netz-Typ	Subnetz Maske (binär)	Subnetz Maske (dezimal)
Klasse-A-Netz	11111111.00000000.00000000.00000000	255.0.0.0
Klasse-B-Netz	11111111.11111111.00000000.00000000	255.255.0.0
Klasse-C-Netz	11111111.11111111.11111111.00000000	255.255.255.0

Netzkategorie	Adressbereich	Netzmaske	Max. Anz Netze & Rechner
Klasse A	0.0.0.0 – 127.255.255.255	255.0.0.0	128 / 16 777 214
Klasse B	128.0.0.0 – 191.255.255.255	255.255.0.0	16 384 / 65 534
Klasse C	192.0.0.0 – 223.255.255.255	255.255.255.0	2097152 / 254
Klasse D	224.0.0.0 – 239.255.255.255	Verwendung Multicast Anwendungen	
Klasse E	240.0.0.0 – 255.255.255.255	Reserviert (zukünftige Zwecke)	

Vertraulichkeit	
Fragestellung	Elemente (Massnahmen)
Aufgrund welcher Kriterien benötigt jemand Berechtigungen, um auf Daten zuzugreifen oder Programme auszuführen?	Berechtigungen, Benutzer, Gruppen, Rollen Zugriffsrechte auf Dateisystem und Berechtigungen sowie Rollen innerhalb von Programmen Authentifizierung (Login-Vorgang) eventuell mit zusätzlichen Einrichtungen (Zertifikaten) Schutz vor unbefugtem Zugriff (z. B. Firewall)

Integrität	
Fragestellung	Elemente (Massnahmen)
Wie können wir sicherstellen, dass bestimmte Daten über einen definierten Zeitraum vollständig und unverändert bleiben?	Stammen die Daten vom angegebenen Absender bzw. vom Eigner (elektronische Unterschrift)? Sind die Daten in Datenbanken unverändert?

Sicherheit	
Fragestellung	Elemente (Massnahmen)
Wie können wir gewährleisten, dass unser IT-System sicher betrieben wird und wie gewünscht (bzw. erforderlich) verfügbar ist?	Zutrittsregelung, Schliesssysteme Datensicherung, Wiederherstellung von Daten Verfügbarkeit, redundante Systeme (Clustering), Ersatzteile Virenschutz, Patch Management, Release Management Systemüberwachung (Monitoring)