Lernziele LB Modul 117

Lernziele

1. Kennt die grundsätzlichen Informationen, die aus einem einfachen Netzwerkschema hervorgehen müssen und kann aufzeigen, wie diese abgebildet werden können.

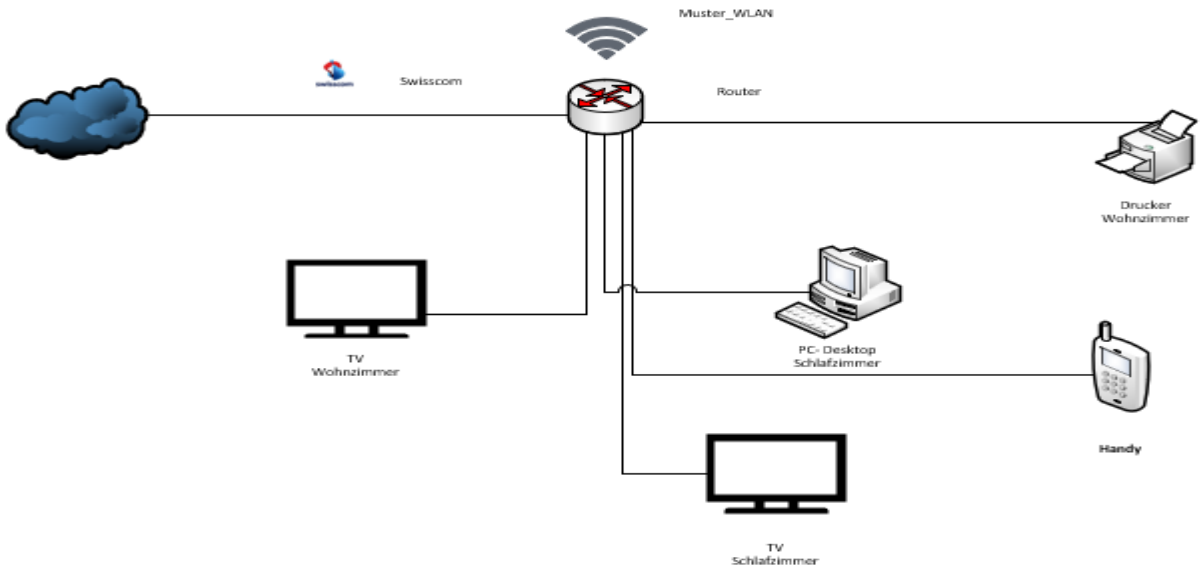
Netzwerkpläne zeigen, wie solch ein Netzwerk wirklich funktioniert. Ein Netzwerkplan wird für mehrere Aktivitäten verwendet, einschließlich:

- Strukturierung des Heim- oder Büronetzwerks
- Verstehen und Beheben von Fehlern und Irrtümern
- Upgrade oder Aktualisierung eines bestehenden Netzwerks.
- Dokumentation für Onboarding, Kommunikation, Planung usw.
- Verfolgen von Komponenten, Geräten oder Aufträgen
- Darstellung des Prozesses und der Schritte, die bei der Umsetzung eines Projekts zu unternehmen sind

Zu beachtende, wichtige Kriterien die bei einem einfachen Netzwerkschema vorzufinden sein sollten:

- Alle Symbole sind beschriftet
- Verbindungslinien sind erstellt
- Ein Titel auf dem Netzwerkplan ist ersichtlich
- Ersteller/Autor ist ersichtlich
- Datum, wann der Netzwerkplan erstellt wurde, ist ersichtlich
- Version des Netzwerkplans ist ersichtlich

Siehe nachfolgendes Beispiel:[1]



Ersteller: Müller, Hans
Dokument: XY.pdf

Netzwerkdiagramm von XY

[1] (OneNote Modul 117, kein Datum)

2. Kennt die Vorgehensweise, ein Netzwerk sowohl in einer logischen wie einer physischen Darstellung abzubilden.

Arten von Netzwerkpläne

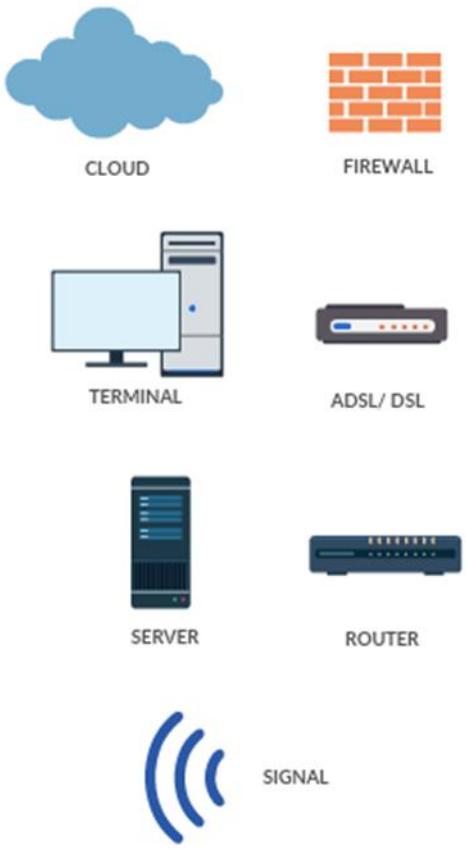
Physikalische Diagramme

Diese Art von Netzwerkplan zeigt die tatsächliche physikalische Beziehung zwischen den Geräten/Komponenten, aus denen das Netzwerk besteht.

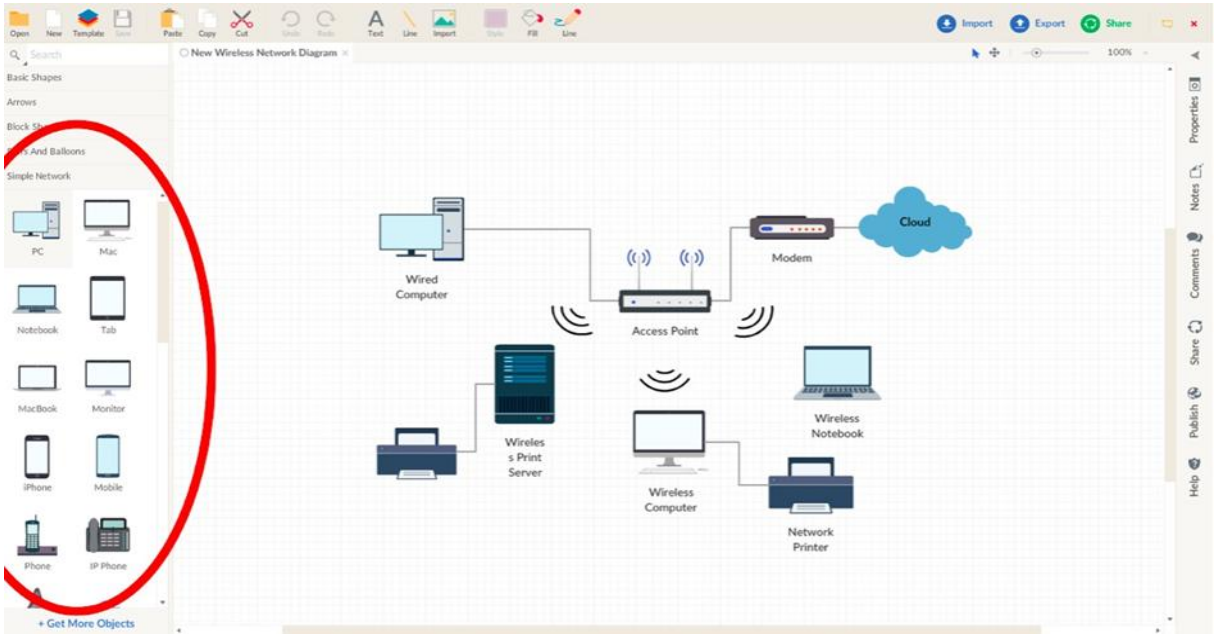
Logische Diagramme

Diese Art von Diagramm zeigt, wie die Geräte miteinander kommunizieren und Informationen durch das Netzwerk fließen. Es wird hauptsächlich zur Darstellung von Subnetzen, Netzwerkgeräten und Routing-Protokollen verwendet.

Netzwerk-Symbole



Dies sind die in einem Netzwerkplan am häufigsten verwendeten Symbolen, dazu aber gibt es noch viele andere Symbole.



Alles, was Sie tun müssen, ist, das Symbol zu ziehen und fallen zu lassen, um Ihren eigenen Netzwerkplan zu erstellen.

Aktivität

Bei einer **Aktivität** handelt sich um eine Operation, die üblicherweise durch einen Pfeil (meist zur Richtungsangabe) mit einem Ende sowie einem Startpunkt dargestellt wird. Es gibt vier Typen von Aktivitäten.

1. **Vorgänger-Aktivität**

Ist vor dem Beginn einer anderen Aktivität abzuschließen.

2. **Aktivität des Nachfolgers**

Können erst begonnen werden, wenn die Aktivitäten abgeschlossen sind. Diesen Nachfolgeaktivität sollte in unmittelbarer Folge erfolgen.

3. **Gleichzeitige Aktivität**

Soll gleichzeitig gestartet werden.

4. **Dummy-Aktivität**

Verwendet keine Ressourcen, sondern nur stellt die Abhängigkeit dar.

Ereignis

Ein Ereignis wird durch einen Kreis dargestellt (auch bekannt als Knoten) und bezeichnet den Abschluss einer oder mehrerer Aktivitäten und den Beginn neuer Aktivitäten. Ereignisse können in drei Typen klassifiziert werden:

1. **Ereignis zusammenführen**

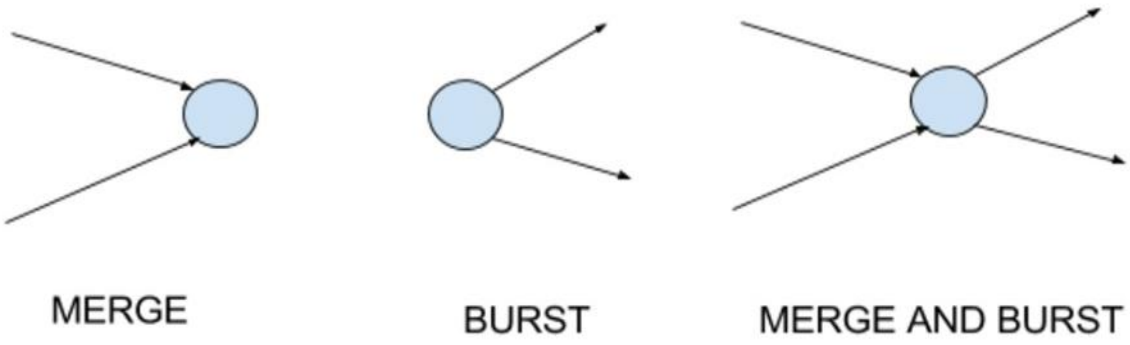
Wenn eine oder mehrere Aktivitäten mit dem Ereignis in Verbindung stehen und ineinander übergehen.

2. **Burst-Ereignis**

Wenn eine oder mehrere Aktivitäten ein Ereignis verlassen.

3. **Ereignis “Merge and Burst“**

Wo eine oder mehrere Aktivitäten gleichzeitig ineinander übergehen und platzen.



Sequenzierung

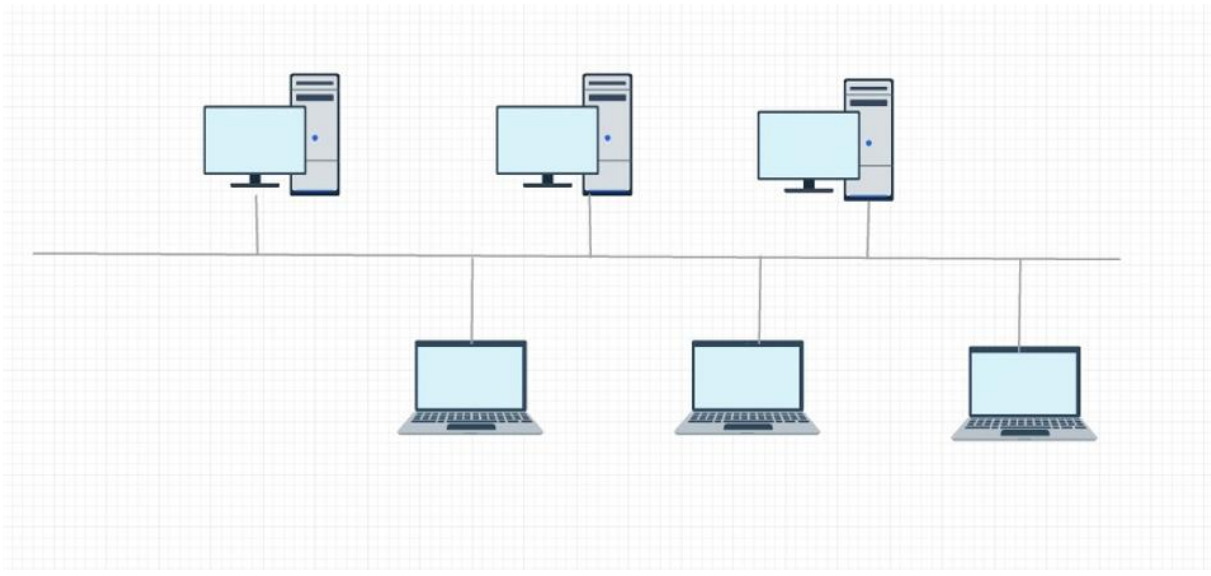
Sequenzierung bezieht sich auf den Vorrang von Beziehungen zwischen Geräten oder Aktivitäten. Die folgenden Fragen können Ihnen helfen, herauszufinden:

- Welche Arbeit wird folgen oder vorausgehen?
- Welche Jobs können (oder werden) gleichzeitig laufen?
- Was kontrolliert den Start und das Ziel?

Arten von Netzwerkwerkpläne

Bustopologie

Diese sind am einfachsten zu konfigurieren und erfordert die geringste Kabellänge. Die Computer oder das Netzwerk sind mit einer einzigen Leitung (mit zwei Endpunkten) oder einem **Backbone** verbunden. Daher ist sie im Volksmund auch als **Linientopologie** bekannt.



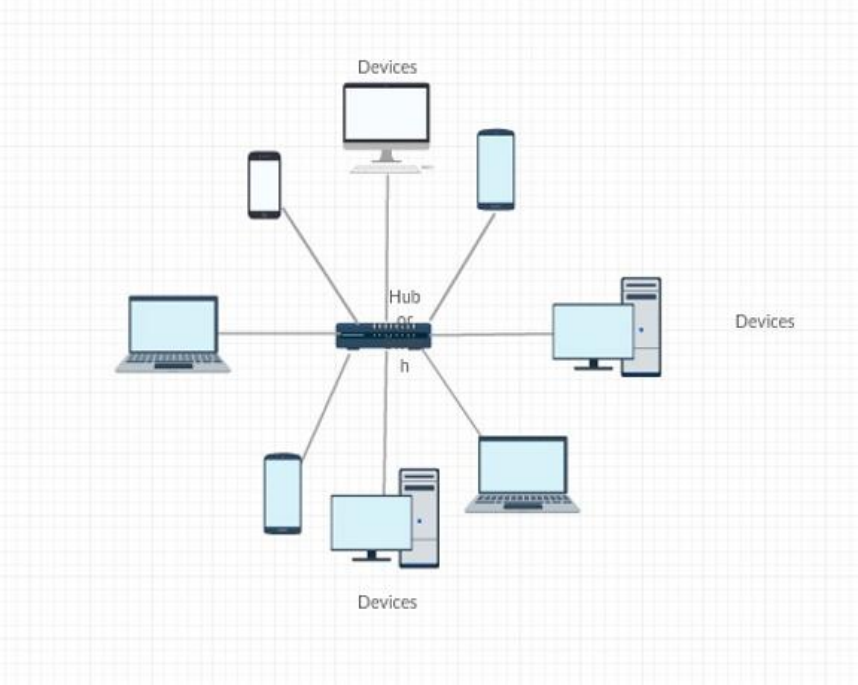
Während der größte Teil der **Bustopologie** linear wäre, gibt es noch eine weitere Form von Busnetzwerken, die als **“Verteilter Bus”** bezeichnet wird. Diese Netzwerktopologie verbindet verschiedene Knoten mit einem gemeinsamen Übertragungspunkt, und dieser Punkt hat zwei oder mehr Endpunkte zum Hinzufügen weiterer Zweige.

Die **Bustopologie** wird im Allgemeinen verwendet, wenn Sie ein kleines Netzwerk haben und Geräte linear miteinander verbinden müssen. Wenn jedoch der Bus (oder die Linie) ausfällt oder einen Fehler hat, ist es schwierig das Problem zu identifizieren und zu beheben.

Ring

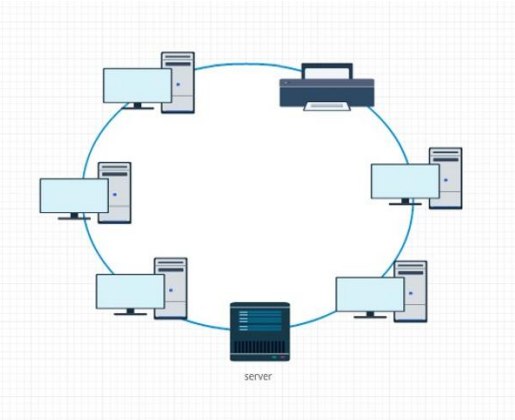
Wie der Name schon sagt, hat das Netzwerk die Form eines Rings. Jedes Gerät/Knoten verbindet sich mit genau zwei anderen, bis es zu einem Kreis wird. Die Informationen werden von Knoten zu Knoten (in zirkulärer Weise) gesendet, bis sie ihr Ziel erreichen.

Anders als bei der Bustopologie ist es einfach, einen Knoten zur **Ringtopologie** hinzuzufügen oder zu entfernen. Wenn jedoch eines der Kabel reißt oder Knoten ausfallen, fällt das gesamte Netzwerk aus.



Star

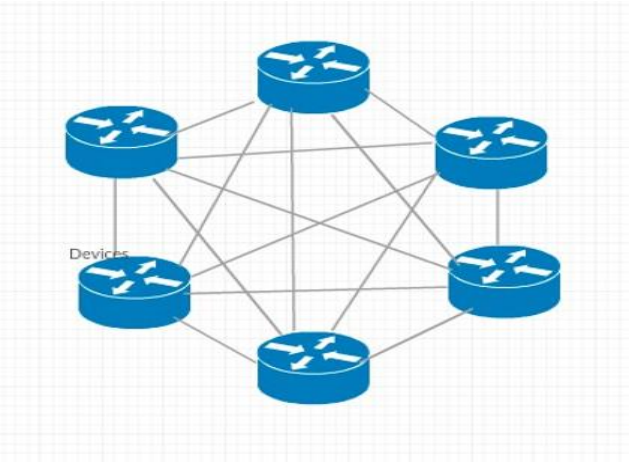
Jeder Knoten ist separat und einzeln mit einem Hub verbunden und bildet so einen **Stern**. Alle Informationen durchlaufen den Hub, bevor sie an den Bestimmungsort geschickt werden.



Obwohl die **Sterntopologie** viel mehr Kabellänge beansprucht als andere, hat der Ausfall eines Knotens keine Auswirkungen auf das Netzwerk. Und nicht nur das, jeder Knoten kann im Falle eines Bruchs oder Ausfalls leicht abgebaut werden. Fällt der Hub jedoch aus, kommt das Netzwerk zum Erliegen.

Masche

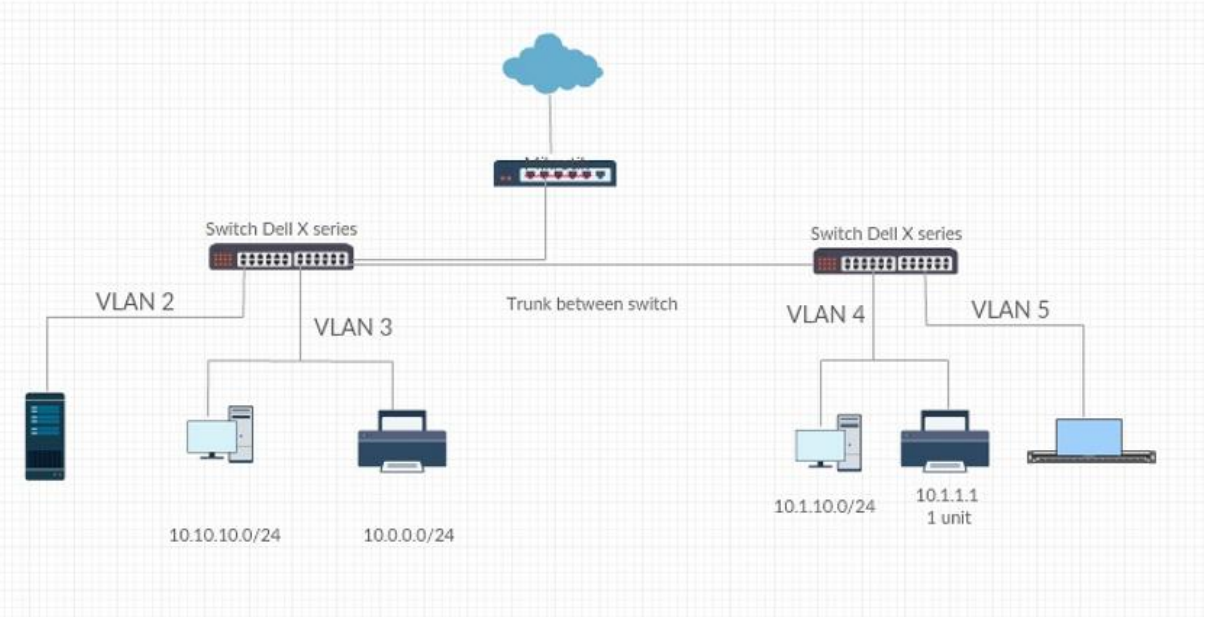
Bei dieser Art von Netzwerkdiagramm überträgt jeder Knoten Daten für das Netzwerk. Es kann von zwei Typen sein: Vollständiges Netz und teilweise verbundenes Netz.



Während jeder Knoten in einem vollständigen Netz miteinander verbunden ist, werden die Knoten auf der Grundlage ihrer Interaktionsmuster in einem teilweise verbundenen Netz miteinander verbunden.

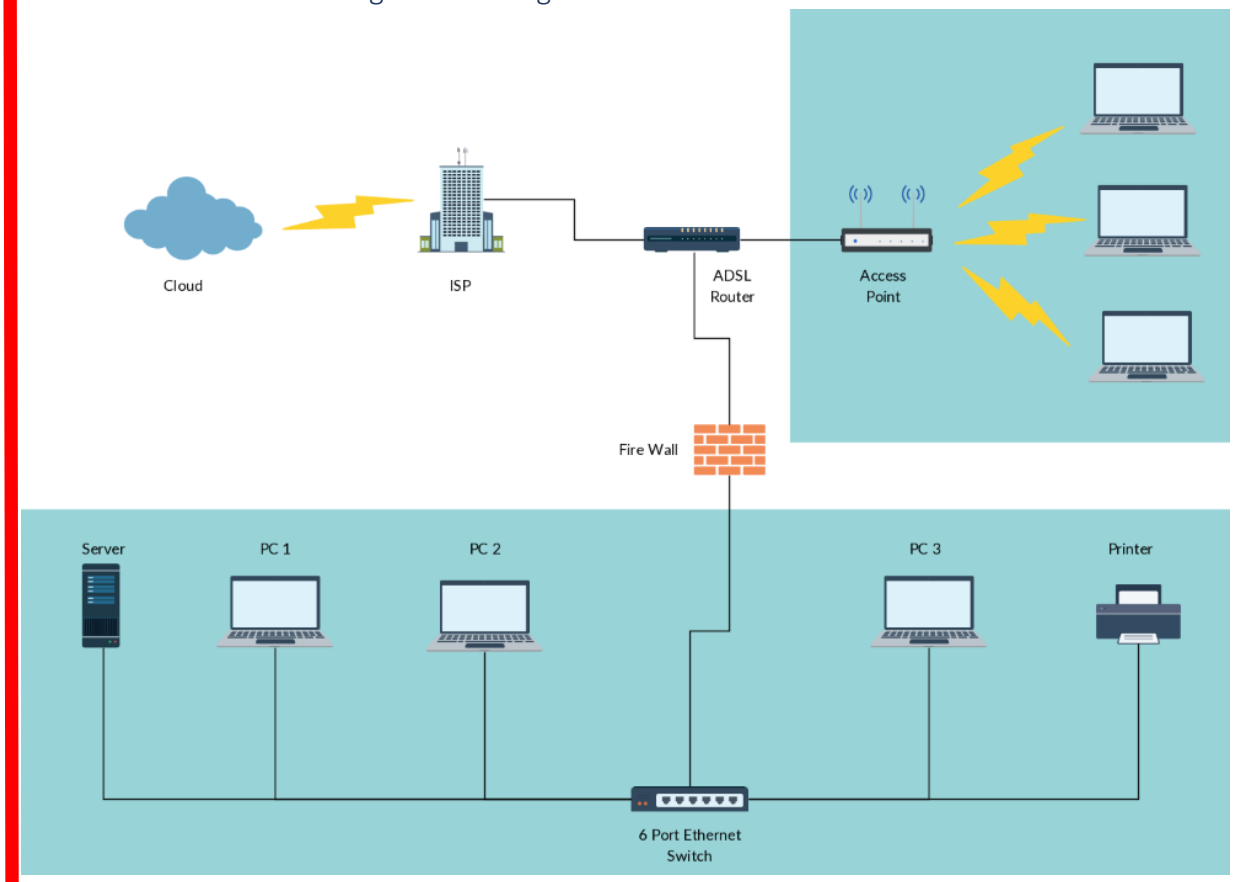
Baum

Es handelt sich um eine Kombination aus Bus- und Sterntopologie.

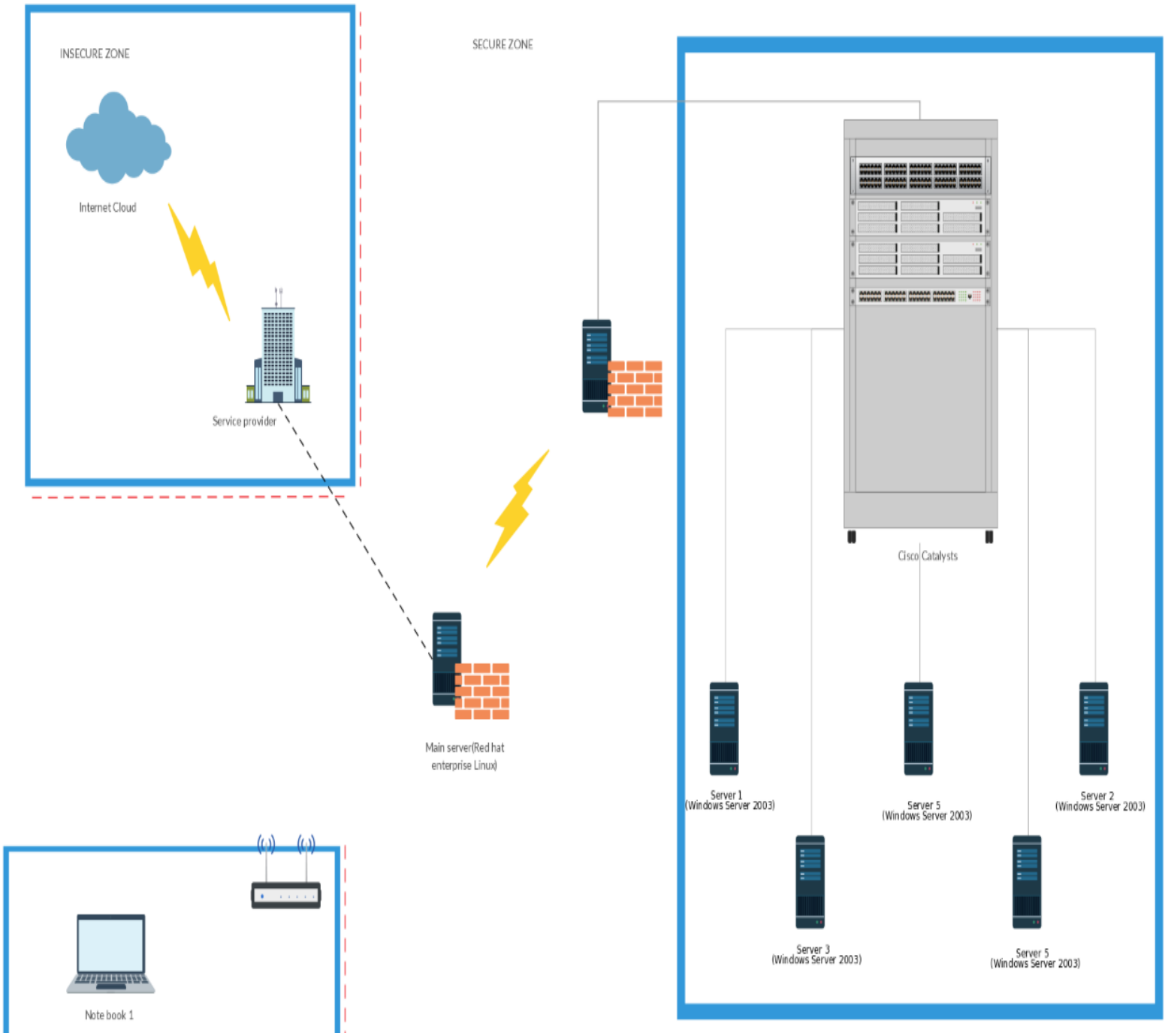


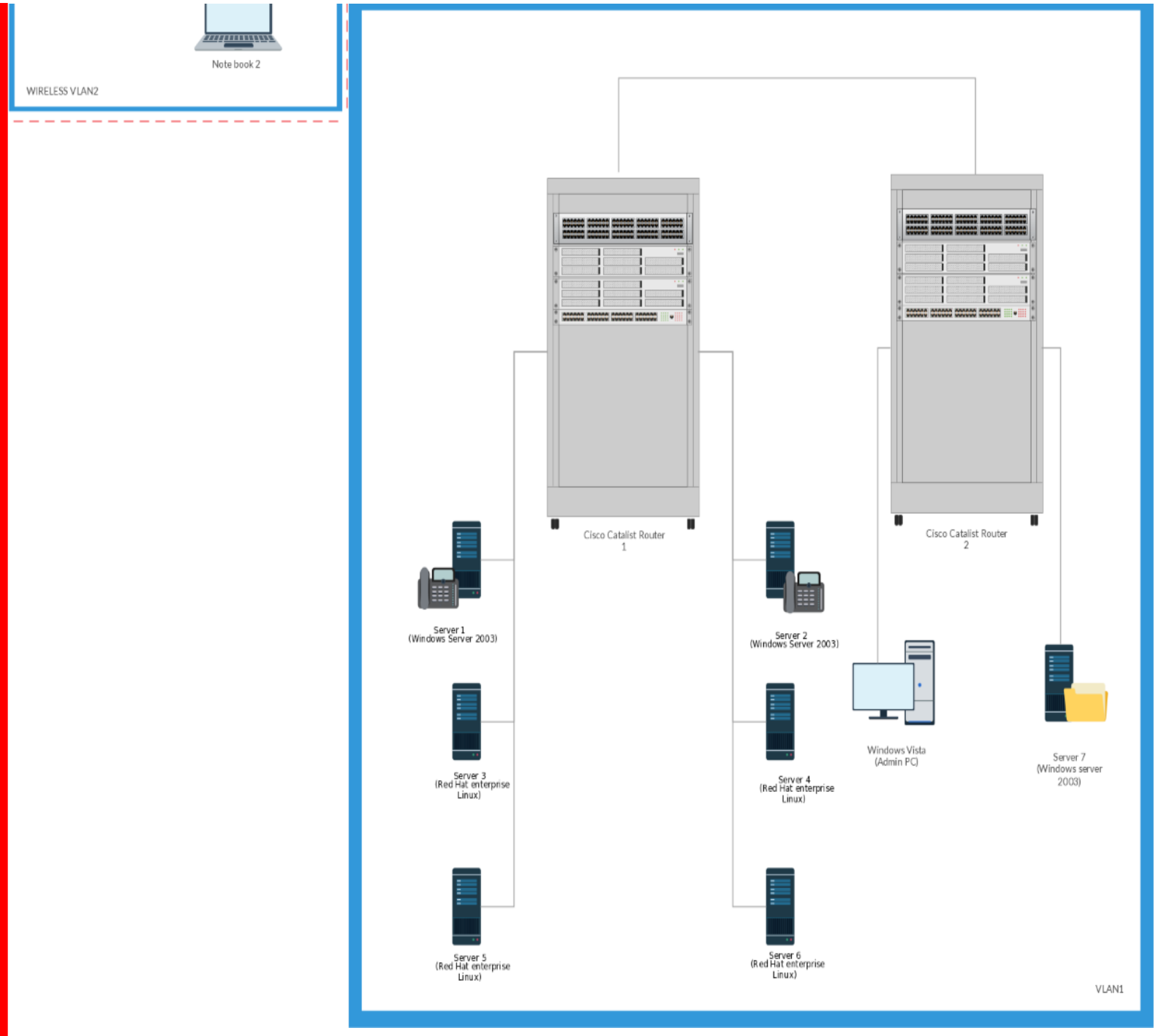
Beispiele für klassische Netzwerkdiagramme

Büronetzwerk-Netzwerkdiagramm-Vorlage

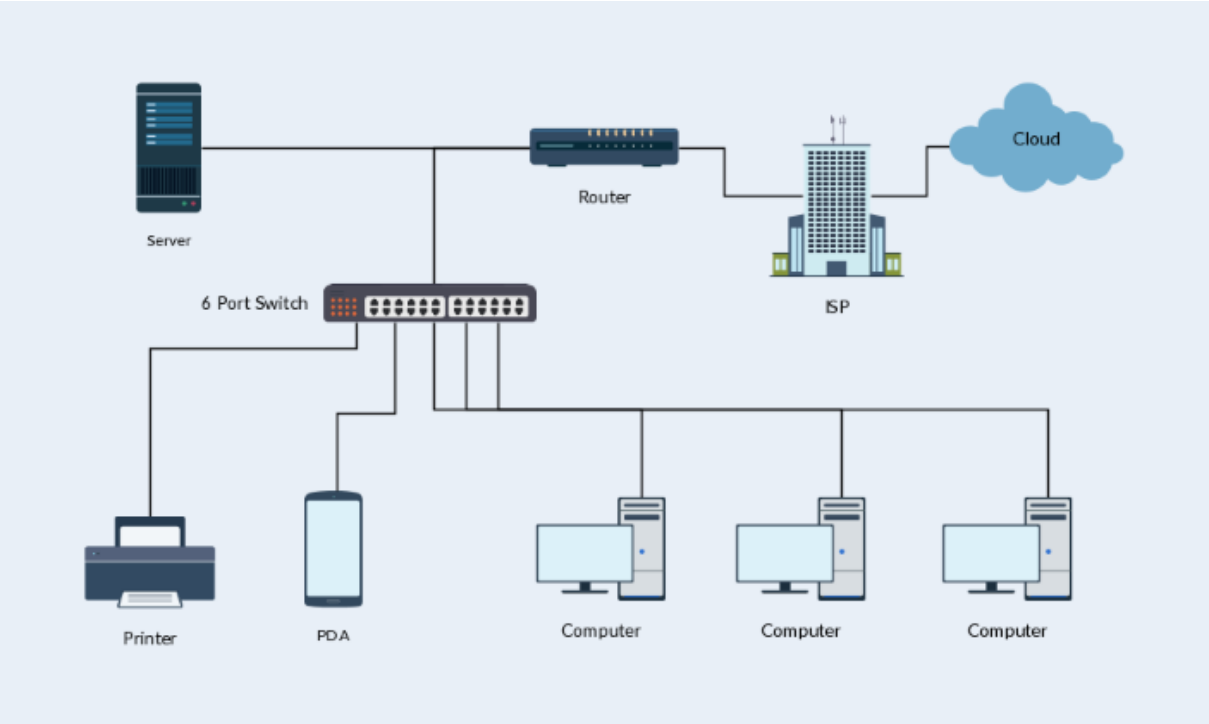


VLAN-Netzwerkdiagramm-Vorlage




Note book 2
WIRELESS VLAN2
Cisco Catalist Router 1
Cisco Catalist Router 2
Server 1 (Windows Server 2003)
Server 2 (Windows Server 2003)
Server 3 (Red Hat enterprise Linux)
Server 4 (Red Hat enterprise Linux)
Server 5 (Red Hat enterprise Linux)
Server 6 (Red Hat enterprise Linux)
Windows Vista (Admin PC)
Server 7 (Windows server 2003)
VLAN1

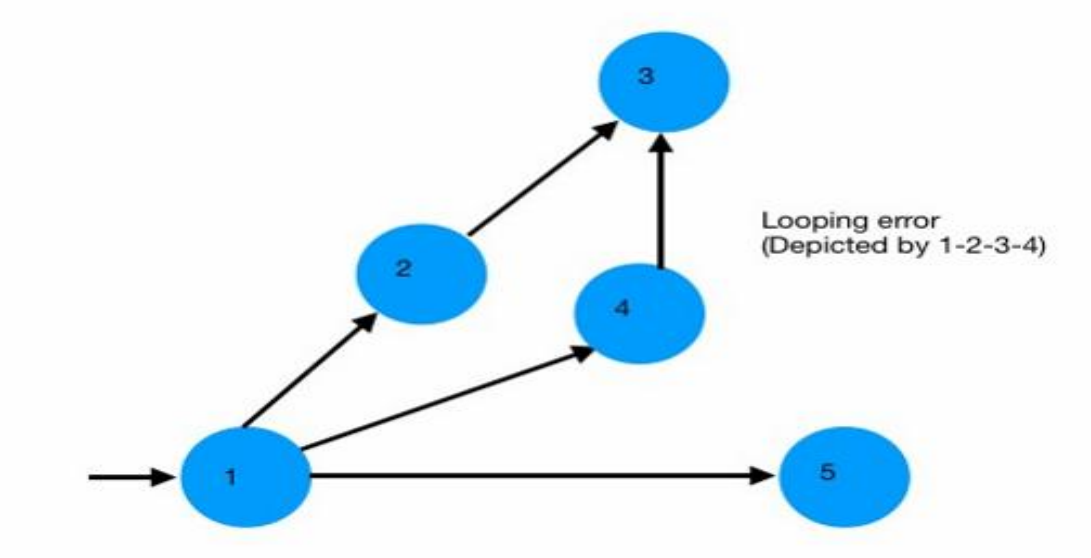
Grundlegende Netzwerkdiagramm-Vorlage



Häufige Fehler bei Netzwerkdiagramme

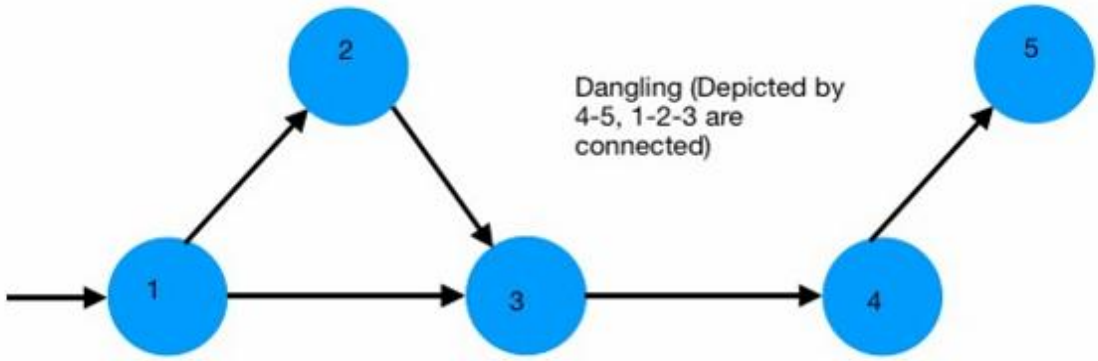
Schleife

Wie der Name schon sagt, handelt es sich um eine Situation, in der Sie am Ende eine Endlosschleife im Netzwerkdiagramm bilden.



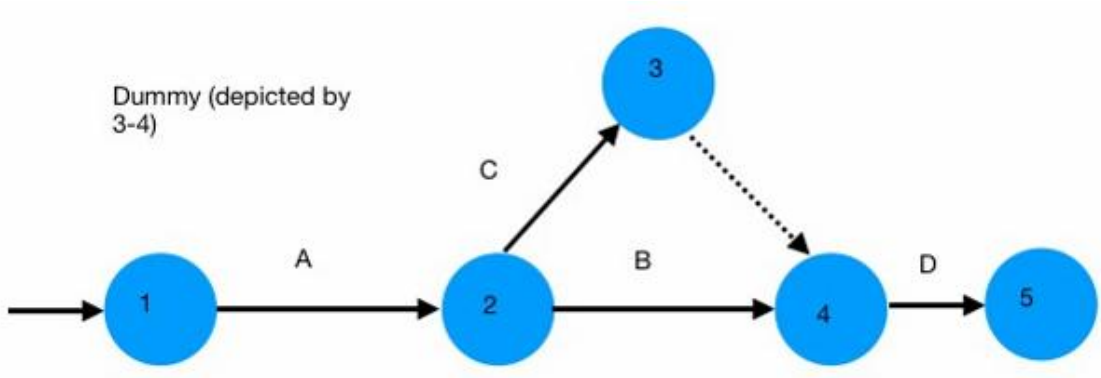
Dangling

Es ist eine Situation, in der ein Ereignis von einer anderen Aktivität abgekoppelt ist. Während eine Aktivität mit dem Ereignis verschmilzt, gibt es keine Aktivität, die von diesem Ereignis ausgeht oder aus ihm hervorgeht. Damit ist diese Veranstaltung vom Netzwerk abgekoppelt.



Dummy

Es existiert nicht und ist imaginär. Es wird im Netzwerkdiagramm (normalerweise durch einen gepunkteten Pfeil dargestellt) verwendet, um die Abhängigkeit oder Konnektivität zwischen zwei oder mehr Aktivitäten zu zeigen. Zum Beispiel sind A und B gleichzeitig. C ist abhängig von A; D ist abhängig von A und B. Diese Beziehung wird mit Hilfe des gestrichelten Pfeils dargestellt.



Weitere Hinweise

- Vermeiden Sie die Verwendung von Pfeilen die sich kreuzen
- Gerade Pfeile verwenden
- Stellen Sie die Zeit nicht mit der Länge der Pfeile dar
- Verwenden Sie immer Pfeile von links nach rechts.
- Benutzen Sie minimale Dummies (verwenden Sie sie gegebenenfalls für Ihren Entwurf)
- Das Netzwerk sollte nur einen Eintrittspunkt haben, der als Anfangsereignis bezeichnet wird, und einen Austrittspunkt, der als Endereignis bezeichnet wird.[2]

[2] (OneNote Modul 117, kein Datum)

3. Kennt die prinzipiellen Aufgaben der Netzwerkkomponenten Switch, Accesspoint und Router und kann aufzeigen, wo und zu welchem Zweck diese in einem Netzwerk eingesetzt werden.

Geräteübersicht

Zur Vergrößerung von Netzwerken bzw. zur Überwindung vorhandener Einschränkungen wie Längen oder Bandbreitenengpässe gibt es verschiedene Geräte unterschiedlicher Funktionalität. Je höher die Einbindung eines Gerätes im Referenzmodell erfolgt, desto komplexer ist die in ihm realisierte Funktionalität.

Angelehnt an das OSI-Modell zeigt die folgende Tabelle eine Übersicht von aktiven Netzwerkkomponenten, auch wenn diese z. T. nicht mehr marktüblich sind.

OSI-Schicht	Netzwerkkomponenten	Kennzeichen
7	Gateway, Proxy, Application-Layer-Firewall	Protokollumsetzung auf Applikationsebene
4	Layer-4-Switch, Stateful-Inspection-Firewall	Segmentierung, Fehlerkorrektur (TCP), Portfilterung
3	Router, Multilayerswitch (Layer-3-Switch), Paketfirewall	Routing, IPv4/IPv6-Adressierung, IP-Filterung
2	Bridge, Switch, Accesspoint, Netzwerkadapter	Switching, MAC-Adressierung. Daten werden zur Übertragung in Frames (Datagramme) gepackt.
1	Repeater, Hub, Medienkonverter	Signalregenerierung, Autonegotiation, Autosensing

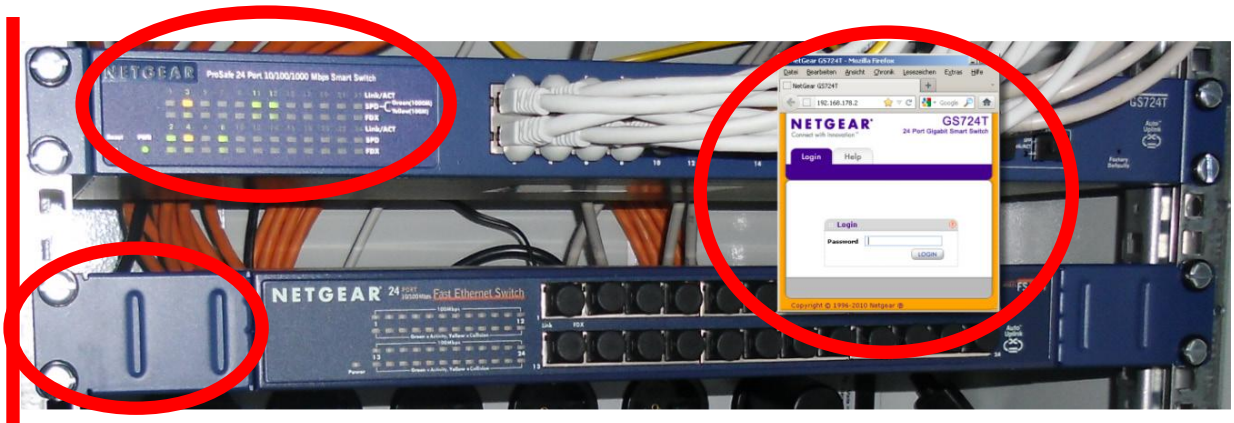
Sie können Netzwerkkomponenten unterschiedlicher Hersteller miteinander kombinieren. Einige Hersteller haben jedoch zusätzliche proprietäre Erweiterungen implementiert, um sich im Netzwerkmarkt abzugrenzen.

Switch

Definition

Ein **Switch** (engl. für „Schalter“) ist eine Multiport-Bridge, welche die Vorteile einer Bridge auf mehrere Ports überträgt. Durch Schalten („switchen“) von Verbindungen ist es für miteinander kommunizierende Geräte so, als ob sie direkt miteinander verbunden wären.

Per **Kaskadierung** lässt sich mit Switchen eine Vergrößerung der Gesamt**portanzahl** ermöglichen. Dabei bilden diese Verbindungen einen Flaschenhals für den Datenverkehr, und die **Latenzzeit** erhöht sich. Dieses Problem wird mit **Stacking** gelöst (vgl. Kapitel 12.4). Vor allem bei einer Kaskadierung können sehr viele Geräte miteinander verbunden sein, daher verfügen bereits einfache Desktop-Switches über internen Speicherplatz für 1000 und mehr MAC-Adressen.



Der obere Switch: Managed

Der untere Switch: Unmanaged

Die Website: Webinterface des Managed Switches

Sogenannte Managed Switches können konfiguriert werden (meist per Webinterface). Desktop-Switches sind in der Regel unmanaged und damit nicht konfigurierbar, aber dafür sofort einsetzbar. Managed Switches benötigen eine eigene IP-Adresse zur Konfiguration.

Arbeitsweise

Damit ein Switch schnell die **Frames** zwischen den **Ports** vermitteln kann, muss er über eine **interne Verdrahtung (Backplane)** mit sehr hoher Geschwindigkeit verfügen.

Ein Switch kann im Prinzip mit einer Telefonanlage verglichen werden, bei der zeitlich begrenzt zwischen kommunizierenden Telefonen eine exklusive Verbindung besteht. Die für diese Verbindung benutzten Ports können so mit ihrer maximalen Geschwindigkeit arbeiten.

Bei serverbasierten Netzwerken, bei denen nahezu alle Arbeitsstationen Daten vom gleichen Server benötigen, ist dies für die Verbindung zum Server nicht mehr der Fall. Kollisionen werden dabei durch die Flusskontrolle der Übertragung vermieden.

Flusskontrolle der Übertragung

Im Duplexmodus wird durch Pause-Frames den sendewilligen Geräten signalisiert, eine Pause per Flow-Control nach IEEE 802.3x einzulegen, falls der Port mit der Leitung zum Empfänger bereits mit der Übertragung von einem anderen Frame belegt ist.

Bei **Priority Flow Control** (PFC nach IEEE 802.1p von 1998, bzw. Priority based Flow Control nach IEEE 802.1Qbb ab 2008) wird auf OSI-Layer 2 von einem Switch ein 3 Bit großes Feld (PCP, Priority Code Point) in das 4 Byte lange VLAN-Tag des Ethernet-Frames eingefügt.

Etliche Switches haben die Funktion Auto-VoIP, mit der sie automatisch VoIP-Pakete erkennen und passende VLAN-Tags generieren.

Prioritäten können auch von Einträgen im IP-Header auf Layer 3 stammen, die dort als Differentiated Service Codepoint (DSCP)-Flag bzw. Type of Service (ToS) bekannt sind. Diese Einstellungen bleiben auf dem gesamten Weg bis zum Empfänger erhalten. Ein derartiger Switch (Layer-3-Switch bzw. Smart-Switch genannt) kann daher Ethernet-Frames bis zum IP-Header auf Layer 3 auspacken, um die eingebetteten Information auszuwerten.

Mit **Traffic Shaping** beschleunigt sich die gesamte Übertragung, und damit verbessern sich auch Verbindungen von sensiblen Anwendungen wie VoIP. Etliche Managed Switches und DSL-Router (z. B. viele Fritz!Boxen) verwenden diese Technik, die auf VLAN-Tags verzichtet.

Die verschiedenen Modi der Weiterleitung

Sowohl bei einem Switch als auch bei einer Bridge haben sich grundsätzlich folgende drei Verfahren etabliert, wobei die Ports zwischen den Verfahren nach Bedarf umschalten können. Dies hängt von den angeschlossenen Stationen und der Ausstattung der Komponente ab.

Cut-Through

Beim **Fast-Forward-Modus** beginnt der Switch sofort mit dem Weiterleiten (Forward) der Daten zur Ziel-MAC-Adresse, nachdem er die Zieladresse gelesen hat. Diese befindet sich am Anfang des Ethernet-Frames.

Beim **Fragment-Free-Modus** prüft der Switch erst, ob der Frame die minimale Länge von 64 Byte hat, indem er die ersten 64 Bytes liest. Erst danach leitet er den Frame weiter (Forward). Kürzere Frames verwirft er. In beiden Modi von **Cut-Through** müssen die Ports gleiche Übertragungsraten und Übertragungsmedien haben. Anderenfalls weicht der Switch auf **Store-and-Forward** aus (wie z. B. beim Übergang von Twisted-Pair auf Glasfaser).

Der Nachteil dieser beiden Modi ist, dass bei der Übertragung nicht auf fehlerhafte oder unvollständige Frames geprüft wird. Dafür ist die Geschwindigkeit höher als im Store-and-Forward-Modus.

Store-and-Forward

Bei diesem Modus speichert der Switch den Frame vollständig zwischen, bevor er ihn zum Zielport weiterschickt. **Store-and-Forward** muss verwendet werden, wenn zwischen Quell- und Zielport unterschiedliche Übertragungsraten verwendet werden, z. B. von 1 Gbit/s nach 100 Mbit/s. Beim Zwischenspeichern überprüft der Switch die Daten auf Fehler anhand der im Ethernetframe vorhandenen FCS-Prüfsumme. Somit werden fehlerhafte Frames nicht weitergeleitet, was jedoch eine längere Latenzzeit zur Folge hat.

Error-Free-Cut-Through

Dies ist eine Mischform aus den vorgenannten Modi, zwischen denen der Switch je nach Qualität der Datenübertragung (Fehlerrate etc.) wechseln kann. Somit können je nach Situation die Vorteile aller oben genannten Modi kombiniert werden. Diesen Modus nennt man auch **Adaptive Switching**.

Interne Switcharchitektur

Auch bei der internen Behandlung der Frames gibt es bei Switches unterschiedliche Methoden. So bestehen bei einem **Cross-Bar-Switch** dedizierte Verbindungen zwischen allen Ports, was einen maximalen Datendurchsatz garantiert. Sobald der Weg zwischen Quelle und Ziel bekannt ist, werden die Daten über die entsprechende Verbindung weitergeleitet, ohne von anderem Datenverkehr behindert oder blockiert zu werden. Ein Nachteil dieser Methode liegt in der schlechteren Skalierbarkeit bei steigender Portzahl.

Beim **Cell-Backplane-Switch** kommunizieren alle Ports über einen schnellen internen Bus. Der Switch zerlegt die Frames in kleinere Zellen und fügt jeder Zelle einen Header mit der

Adresse des Zielports hinzu. Dort werden die Zellen zwischengespeichert, zum Ausgangsframe zusammengesetzt und endgültig an das Ziel weitergeleitet.

Weitere Entwicklungen

Etliche Hersteller bieten Hochleistungs-Switches an, die nicht nur auf der Schicht 2 des OSI-Modells arbeiten, wie dies bei einem klassischen Switch der Fall ist, sondern auf Schicht 3 und höher handelt es sich um **Multilayer-Switches**.

Layer-3-Switching

In einem Netzwerk ohne Priority Flow Control sind prioritätsgesteuerte Übertragungen nur dann auf Layer 2 möglich, wenn der Switch nicht nur die ankommenden Frames weiterleitet, sondern zusätzlich auf Layer 3 die IP-Header analysiert und sie auf **ToS**-Attribute bzw. das **DSCP**-Flag untersucht (siehe „Flusskontrolle“ weiter oben). Von daher kommt der Ausdruck Layer-3-Switch.

Routing kommt erst dann hinzu, wenn ein zusätzliches Routermodul in ein derartiges Gerät eingebaut ist. In diesem Fall handelt es sich um ein Multifunktionsgerät. Ein Switch allein verbindet keine unterschiedlichen Netzwerke. Dennoch wird der Ausdruck „Layer-3-Switch“ oft fälschlicherweise als Synonym für Router benutzt.

Layer-4-Switching

Auf der Schicht 4 des OSI-Modells sind die Portnummern angesiedelt (vgl. Kapitel 11.2). Beim Layer-4-Switching stehen somit die Paket-Informationen der Schicht 4 zur Verfügung, sodass z. B. ein Administrator über Zugriffsregeln **(Access Control List (ACL))** festlegen kann, welcher Verkehr vom Switch behandelt wird. Der Switch kann damit, abhängig von der Anwendung (deren Portnummer), eine Entscheidung über den Weitertransport eines Datenpaketes treffen und damit Datenverkehr filtern oder priorisieren. Damit können Sie eine einfache Paketfirewall einrichten.

Layer-7-Switching

Switche, die bis hinauf zur Schicht 7 arbeiten, können neben der Portnummer weitere Angaben, wie z. B. eine Web-Adresse, für die Steuerung des Datenverkehrs nutzen. Insbesondere auf dem Gebiet der Bereitstellung von Daten für Webanfragen werden solche Geräte eingesetzt.

Sie dienen im Rahmen von Serverfarmen dazu, gleichzeitige Anfragen von Tausenden von Clients per Load Balancing (Lastverteilung) auf die Server zu verteilen. Häufig finden sich daher für Layer- 7-Switche auch die Begriffe Load-Balancer, Web-Switches oder Content-Switches.

Accesspoint

In einem WLAN ist ein Access Point (AP) eine Station, die Daten empfängt und sendet. Ein Access Point verbindet Anwender mit anderen Nutzern im Netzwerk und kann auch als Verbindungspunkt zwischen dem Funknetz und dem drahtgebundenen Netzwerk (LAN) fungieren.

Access Points werden oft auch drahtloser Zugriffspunkt oder Basisstation genannt. Als **Hotspot** bezeichnet man öffentlich zugängliche Access Points. Im Englischen wird selten auch

der Oberbegriff Transceiver verwendet, der sich von transmit (senden) und receive (empfangen) ableitet.

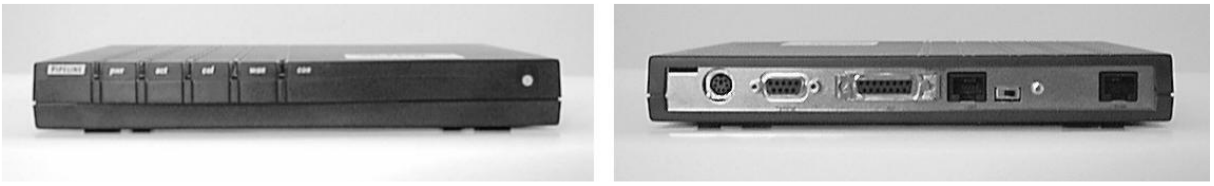
Router

Definition

Ein **Router** ist ein Gerät, das getrennte Netzwerke mit unterschiedlichen Adressräumen oder verschiedenen Netzwerktechnologien koppelt oder Netzwerke in **Subnetze** aufteilen kann. Die wesentliche Funktion ist die „Vermittlung", oder anders gesagt, die Kenntnis der verschiedenen Netze und der Wege zu diesen Netzen.

Einordnung und Arbeitsweise

Die einfachste Form eines Routers ist ein PC mit mehreren Netzwerkadaptern, die jeweils Kontakt zu unterschiedlichen Netzwerken haben. Die Funktion **„IP Forwarding"** muss dabei aktiviert sein, sonst erfolgt keine Weiterleitung der Pakete.



SOHO-Router (Vorder- und Rückseite)

Router arbeiten auf **der Schicht 3** (Network/Vermittlung) des OSI-Modells. Das bedeutet, dass sie Netzwerke mit unterschiedlichen **Topologien** der darunter liegenden Schichten 1 und 2 verbinden können. Allerdings müssen alle beteiligten Netzwerke die gleiche Art der Adressierung ihrer Datenpakete verwenden, d. h. die gleichen **Protokolle** auf Schicht 3. Ist dies der Fall, z. B. beim Einsatz von IP-Adressen im Netzwerk, dann kann ein Router ankommende Frames bearbeiten und an ein anderes Netzwerk übergeben.

Dazu muss ein Router das IP-Paket des empfangenen Frames auf Schicht 3 auspacken, um aus dem IP-Header die **IP-Adresse des Ziels** zu ermitteln. Das IP-Paket selbst packt er nach der Ermittlung des weiteren Weges in einen neu erstellten Frame und schickt diesen über die entsprechende Schnittstelle in ein anderes Netzwerk weiter. Dieser Vorgang kostet Zeit, und so ist der Router im Normalfall langsamer als Switch oder Bridge.

Multiprotokollfähig

Ein wichtiges Unterscheidungskriterium von Routern ist die Frage, ob es sich bei dem Gerät um einen **Einzelprotokoll-** oder **Multiprotokoll-Router** handelt. Ein Router, der nur ein Protokoll kennt, ist lediglich in der Lage, Netzwerke mit gleichem Protokoll zu verbinden. (z. B. IPv4).

Ist der Router multiprotokollfähig, beherrscht er mehrere Protokolle, ohne diese zu vermischen (z. B. IPv4 und IPv6). Dies heißt aber nicht, dass ein Multiprotokoll-Router ein Protokoll direkt in ein anderes umwandeln kann, sondern nur, dass er in der Lage ist, unterschiedliche Protokolle weiterzuleiten.

Tunneling

Mittels **Tunnelings** können die Datenpakete eines Protokolls in den Nutzdaten (**Payload**) eines anderen Protokolls transportiert werden. Dies wird nötig, wenn ein Netzwerk

überbrückt, werden muss. Am Ende der Übertragung bzw. am Ende des „Tunnels“ wird der Transportrahmen entfernt, wodurch das Paket wieder in seinen ursprünglichen Zustand gebracht wird.

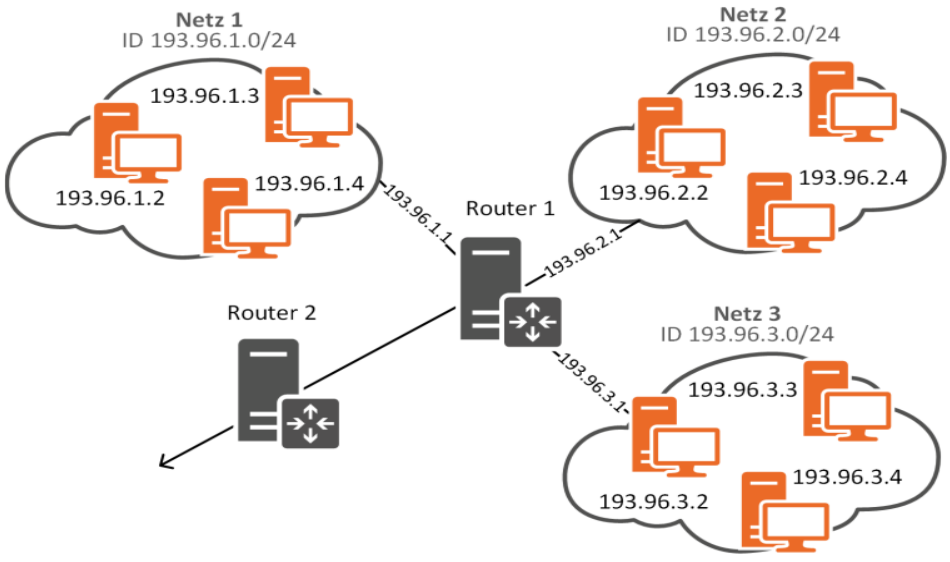
Ein Beispiel für solch ein Verfahren könnte der Transport von IPv6-Paketen über ein reines IPv4-Netzwerk sein. Damit können zwei IPv6-Netzwerke über ein IPv4-Netz gekoppelt werden. Beispiele für solche Verfahren sind **4in6, 6in4, Teredo**.

Tunneling-Protokolle ermöglichen grundsätzlich nur eine erhöhte Sicherheit während der Übertragung, wenn sie auf Tunnel-Kryptografie aufsetzen. Hierzu werden u. a. die Protokolle **Layer 2 Tunneling Protocol (L2TP) / IPsec, OpenVPN**, und weitere verwendet.

Routing-Tabellen

Die Hauptfunktion eines Routers besteht in der Pfadbestimmung (**Routing**) für IP-Pakete zum Zielnetzwerk. Dazu verwenden Router sogenannte **Routing-Tabellen** (eine für jedes Routing protokoll), in denen die an dem Router direkt angeschlossenen Netzwerke (inkl. Netzmasken) und Wege zu benachbarten Netzen hinterlegt sind. Empfängt der Router ein IP-Paket und hat die geforderte Zieladresse ermittelt, muss er den weiteren Weg bestimmen.

Der Router prüft erst anhand der Einträge in den Routing-Tabellen, ob das Gerät mit der Ziel-Adresse **direkt** angeschlossen ist. Dann kann der Router das IP-Paket in einen neuen Frame packen und diesen direkt zum Ziel weiterleiten. Anderenfalls wird er das Paket an einen anderen Router weiterschicken. Dieser nächste Router, der auch als **„Next Hop“** bezeichnet wird, versucht dann auf seine Weise das Paket weiter zuzustellen. Eine wichtige Voraussetzung dafür ist, dass die **Time to live (TTL)** des Pakets noch nicht den Wert 0 erreicht hat. Bei der TTL handelt es sich um einen Zähler, der von jedem Router reduziert wird, nachdem das Routing stattgefunden hat.



Default-Router

Nicht jeder Router kann die Wege zu allen Netzen kennen. Daher wurde als Lösung der **Default-Router** eingeführt. Alle Pakete, für die das Zielnetz unbekannt ist, werden einfach an den Default-Router weitergeleitet.

Jedes IP-fähige Gerät besitzt intern eine statische Routing-Tabelle. Dort ist in jedem Fall das eigene Netzwerk mit dessen Netzmaske eingetragen. Zusätzlich gibt es meistens einen Eintrag (die Default-Route) für unbekannte Wege zum Ziel.

Alle weiteren Einträge müssen beim **statischen** Routing manuell (z. B. vom Administrator) angelegt werden. Beim **dynamischen** Routing tauschen die Router ihre Routeninformationen miteinander aus und generieren die entsprechenden Tabellen selbst.

Ein Router trifft seine **Routingentscheidung** in folgender Reihenfolge:

1. Er prüft zunächst anhand der Einträge in den Routing-Tabellen und den dazugehörigen Netzmasken, ob sich die Zieladresse in einem **direkt** angeschlossenen Netzwerk befindet. Falls ja, ermittelt er die MAC-Adresse (Ethernet-Adresse) des Ziels über das Protokoll ARP und erzeugt ein Paket mit der MAC-Adresse des gewünschten Geräts.
2. Ist das Zielnetz über einen **benachbarten Router** zu erreichen, entscheidet der Router anhand seiner Metrik (Maß für die Güte einer Verbindung), welches der richtige Weg zum Ziel ist. Das kann z. B. der Weg mit der größten Bandbreite oder aber auch der Weg mit den geringsten Kosten sein. Weitere mögliche, zur Auswahl stehende Wege können durch statische Routing-Einträge vorgegeben sein oder sind Wege, die der Router mithilfe eines dynamischen Routing-Protokolls erlernt hat. Anhand dieser Wahl leitet er das IP-Paket zum nächsten passenden Router (Next Hop), indem er es in einem neuen Frame an dessen MAC-Adresse schickt.
3. Gibt es weder einen passenden Eintrag in der statischen noch in einer dynamischen Routing-Tabelle, ist der Weg zum Ziel unbekannt. In diesem Fall leitet der Router das IP-Paket an die MAC-Adresse des Routers, der als **Default-Router** (auch Gateway of Last Resort genannt) eingetragen ist. Dieser kümmert sich um die weitere Zustellung.
4. Findet er in der genannten Reihenfolge keinen verwertbaren Eintrag, so **verwirft** er das Paket und sendet die Nachricht „Zielnetz nicht erreichbar“ an den Absender.

Dynamische Routingprotokolle

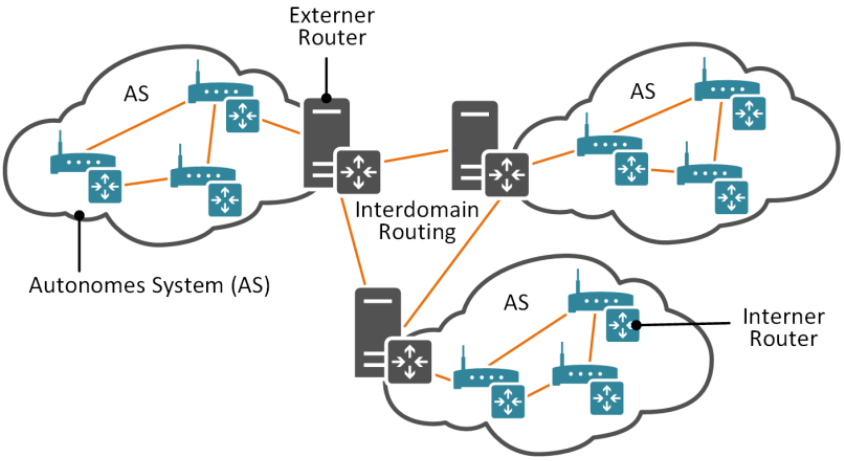
Eine Alternative zur statischen Konfiguration von Routern schaffen dynamische Routingprotokolle, mit deren Hilfe Router benachbarte Netzwerke kennen lernen. Das Ergebnis könnte die Wegewahl auf Basis der kürzesten Verbindung, der aktuellen Lastsituation oder der günstigsten Verbindungskosten sein.

Interne/externe dynamische Routingprotokolle

Interne Routingprotokolle werden ausschließlich im Intranet, also im LAN selbst bzw. innerhalb von Autonomen Systemen, eingesetzt. Typische Vertreter sind die Standardprotokolle **Routing Information Protocol (RIP)** und **Open Shortest Path First(OSPF)**. **Externe Routingprotokolle** finden Anwendung im WAN, also im Internet und zwischen Autonomen Systemen. Ein Beispiel hierfür ist das **Border Gateway Protocol (BGP)**, obwohl auch **OSPF** hierfür geeignet ist.

Autonomes System

Würde jeder Router alle verfügbaren Netze lernen, so käme er schnell an seine Grenzen. Aus diesem Grunde hat man **Autonome Systeme (AS)** eingeführt. Ein Router in einem AS erkennt nur seine Nachbarnetze.



Der Vorteil von AS besteht darin, dass die internen Router nur einen Teil der Netze kennen müssen und demzufolge ihre Routingentscheidung effizienter treffen können. **Externe Router** (auch **Border-Router** genannt) übernehmen die Vermittlung zwischen den AS. Vorrangig vernetzen sich **ISP** auf diese Weise (**Interdomain Routing**).

RIP

RIP war das erste dynamische Standardprotokoll. Es arbeitet nach dem Distanz-Vektor-Algorithmus, d. h., die Wegewahl wird anhand der geringsten Anzahl der Router (Hops) zwischen Quell- und Zielnetz getroffen. Dazu verschickt jeder Router seine Routinginformationen im 30-Sekundentakt an seine Nachbarn.

OSPF

Das Protokoll **Open Shortest Path First (OSPF)** ist ebenfalls ein dynamisches Routing-Protokoll und basiert auf der Link State Database. In dieser Datenbank sind alle benachbarten Router bzw. deren Link-Status enthalten, für die Aktualisierung der Datenbank der Router untereinander sind feste Regeln definiert.

Das OSPF-Protokoll berechnet die Güte eines Weges zu einem benachbarten Router anhand der Leitungskosten, d. h., je höher die verfügbare Bandbreite der Hops zwischen Quell- und Zielnetz ist, desto geringer sind die Kosten und desto günstiger ist der Weg dorthin.

BGP

Das **Border Gateway Protocol (BGP)** nutzt den Path-Vektor-Algorithmus, der ähnlich dem Distanz-Vektor-Algorithmus arbeitet. Jedoch können hierbei keine **Routingschleifen** auftreten. Es kann sowohl innerhalb eines Autonomen Systems als **iBGP** (internal BGP) als auch zwischen AS als **eBGP** (external BGP) eingesetzt werden.

Load Balancing

Die meisten Routing-Protokolle ermöglichen ein sogenanntes **Load Balancing**, was bedeutet, dass alternative Wege zur Zieladresse verwendet werden können. Load Balancing heißt, dass bei zwei gleichwertigen Wegen (gleiche Metrik) die Datenströme wechselseitig auf beide Wege verteilt werden.[3]

[3] (Bratvogel & Klaus Schmidt, Netzwerk Grundlagen, 2019)

4. Kennt gängige Kabeltypen, Steckertypen und Ethernet-Varianten (z.B. Twisted Pair, UTP, STP, Glasfaser, RJ45, etc.) und kann aufzeigen, bei welchen Anforderungen hinsichtlich Leistung und bei welchen räumlichen Gegebenheiten diese zum Einsatz kommen.

Kabeltypen

Anforderung

Einsatz

Steckertypen

Lichtleiterkabel (LLK) können mit unterschiedlichen Steckern ausgestattet sein. In der nachfolgenden Tabelle erhalten Sie eine Übersicht über verfügbare **Lichtwellenleiter-Stecker** sowie gängige LWL-Steckertypen.

Anforderung

Einsatz

Ethernet-Varianten

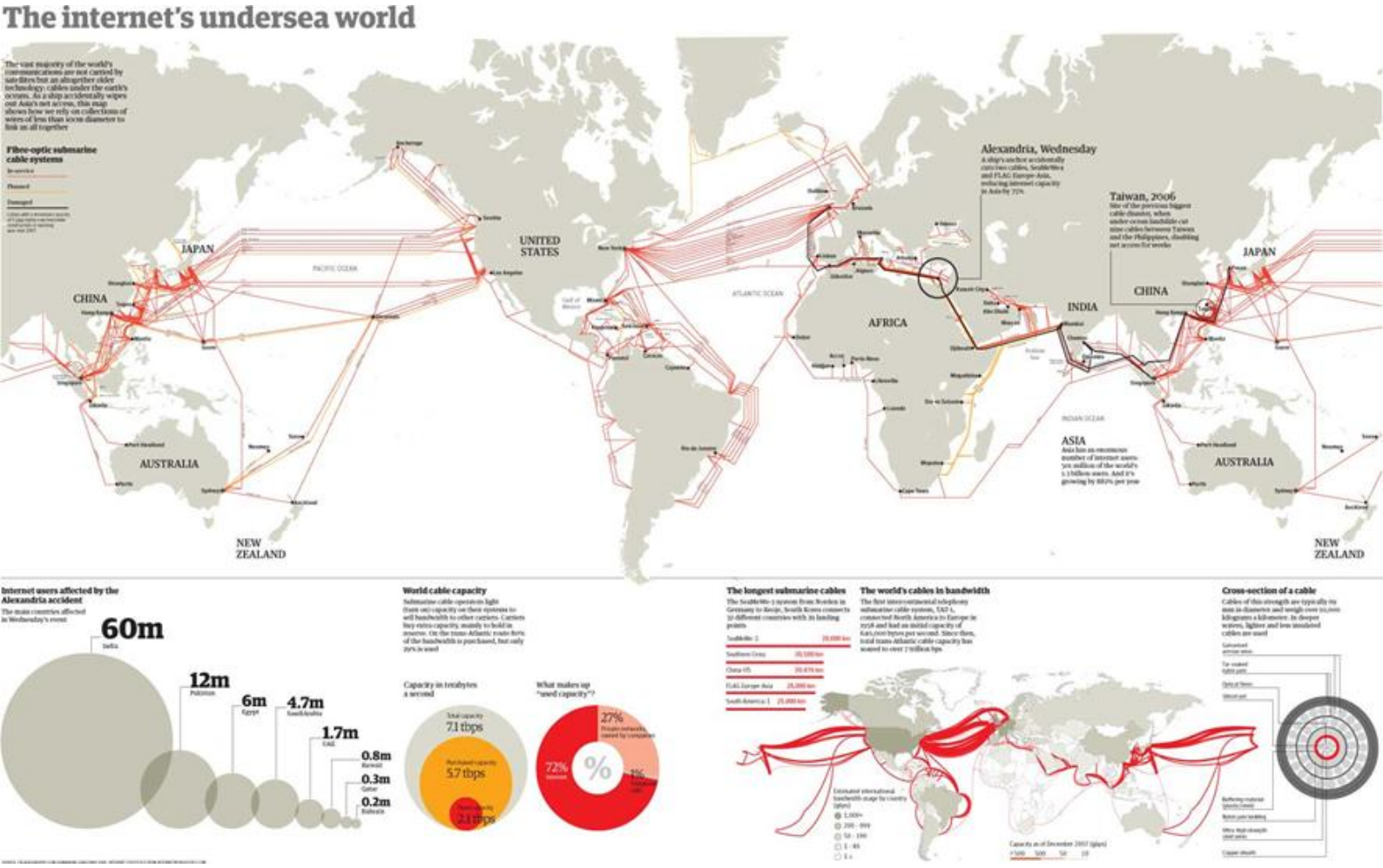
Anforderung

Einsatz

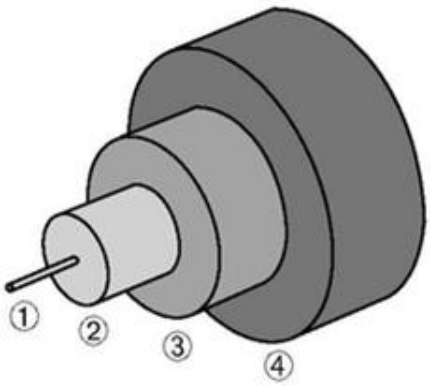
Seekabel

Einführung in Kabelarten:

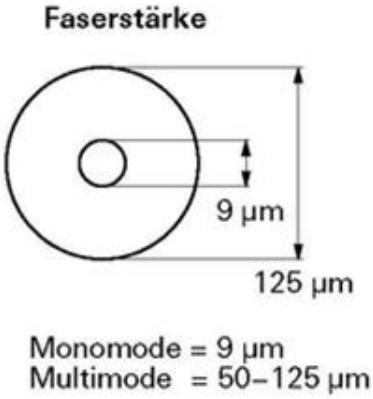
- Seekabel
- Cat UTP/STP Unterschied
- LWL
- RJ45 Stecker



Aufbau LWL

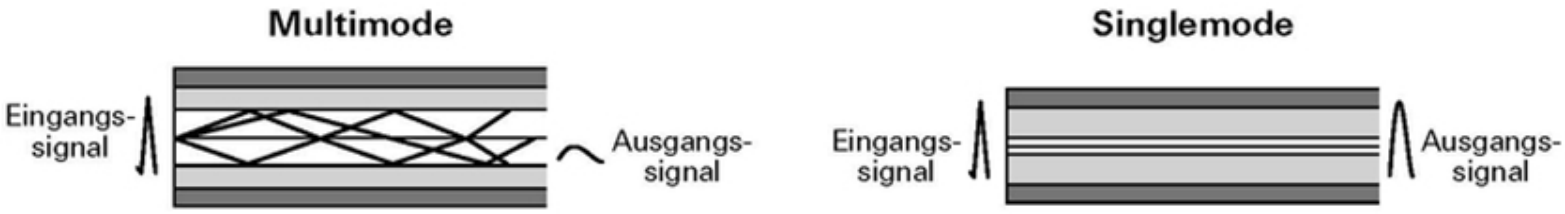


① Kern (engl. Core)
② Mantel (engl. Cladding)
③ Schutzbeschichtung (engl. Coating)
③ Äussere Hülle (engl. Jacket)



Monomode = 9 µm
Multimode = 50–125 µm

Singlemode vs. Multimode (Twisted-Pair)



Verkablung

Primärverkabelung Geländeverkabelung	Der Primärbereich wird als Campusverkabelung oder Geländeverkabelung bezeichnet. Er sieht die Verkabelung von einzelnen Gebäuden untereinander vor. Für die Verkabelung wird in der Regel Glasfaserkabel mit einer maximalen Länge von **1500 m** verwendet.
Sekundärverkabelung Gebäudeverkabelung	Der Sekundärbereich wird als Gebäudeverkabelung oder Steigbereichsverkabelung bezeichnet. Dieser Bereich sieht die Verkabelung von einzelnen Wohnungen und Stockwerken innerhalb eines Gebäudes untereinander vor. Dazu sind vorzugsweise Glasfaserkabel mit einer maximalen Länge von **500 m** vorgesehen.
Tertiärverkabelung Etagenverkabelung	Der Tertiärbereich wird auch als Etagenverkabelung bezeichnet und beinhaltet die Verkabelung von Etagen- oder Stockwerksverteilern zu den Anschlussdosen. Während sich im Netzwerkschrank ein Patchfeld befindet, mündet das Kabel am Arbeitsplatz des Anwenders in einer Anschlussdose in der Wand oder in einem Bodenkanal. Für diese relativ kurze Strecke werden in der Regel Twisted-Pair Installationskabel verwendet, deren Länge auf **90 m** beschränkt ist. Für die Patchkabel im Kabelschrank und beim Endgerät gilt eine Maximallänge von je **5 m**. Werden anstelle von Installationskabel Patchkabel eingesetzt, reduziert sich die Maximallänge auf zirka **60 m**.

[4]

5. Kennt die verbreiteten technologischen Möglichkeiten zur Erstellung eines Internetzugangs und kann erläutern, welche Konsequenzen diese für die Nutzung des Internets und die daraus resultierenden Kosten haben.

- Überprüfung auf folgende Webseite: Maps of Switzerland - Swiss Confederation - map.geo.admin.ch
- Danach Anbieter über Comparis suchen
- Glasfaser ist an diesem Standort nicht verfügbar

Ausgangslage

[4] (OneNote Modul 117, kein Datum)

Einer der ersten Schritte beim Aufbau eines Netzwerkes ist die Festlegung der Übertragungsmedien. Je nach Anforderung des Kunden kann dies ein einfaches WLAN sein. Wenn jedoch die Übertragungsgeschwindigkeit und die Übertragungszuverlässigkeit innerhalb des geplanten Netzwerkes eine Rolle spielt, wird eher ein kabelgebundenes Netz in Frage kommen.[5]

6. Kennt den Zweck und die Funktionen der Schichtenmodelle (OSI, TCP/IP-Modell) und kann die verwendeten Protokolle sowie Netzwerkkomponenten den entsprechenden Schichten zuordnen.

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP	Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

Abbildung 1: aus OneNote

[5] (OneNote Modul 117, kein Datum)

1. Kennt die verbreiteten lokalen Netzwerkdienste und kann aufzeigen, welche Anforderungen an ein Netzwerk sich daraus ergeben.
2. Kennt die grundsätzlichen Informationen, die aus einem einfachen Netzwerkschema hervorgehen müssen und kann aufzeigen, wie diese abgebildet werden können.
3. Kennt die wichtigsten Regeln für eine korrekte Netzwerkkonfiguration (IP-Adressformat, Subnetzmaske, private Adressen, Standardgateway, DNS) und kann diese anhand von Beispielen erläutern.
4. Kennt die prinzipiellen Aufgaben der Netzwerkkomponenten Switch, Accesspoint und Router und kann aufzeigen, wo und zu welchem Zweck diese in einem Netzwerk eingesetzt werden.
5. Kennt den Zweck und die Funktionen der Schichtenmodelle (OSI, TCP/IP-Modell) und kann die verwendeten Protokolle sowie Netzwerkkomponenten den entsprechenden Schichten zuordnen.
6. Kennt die verbreiteten technologischen Möglichkeiten zur Erstellung eines Internetzugangs und kann erläutern, welche Konsequenzen diese für die Nutzung des Internets und die daraus resultierenden Kosten haben.
7. Kennt gängige Kabeltypen, Steckertypen und Ethernet-Varianten (z.B. Twisted Pair, UTP, STP, Glasfaser, RJ45, etc.) und kann aufzeigen, bei welchen Anforderungen hinsichtlich Leistung und bei welchen räumlichen Gegebenheiten diese zum Einsatz kommen.
8. Kennt die Vorgehensweise, ein Netzwerk sowohl in einer logischen wie einer physischen Darstellung abzubilden.
9. Kennt die gängigen WLAN Standards.
10. Kennt die erforderlichen Arbeitsschritte und Komponenten, um eine einfache WLAN-Vernetzung einzurichten.
11. Kennt relevante bauliche Gegebenheiten und Installationsmöglichkeiten hinsichtlich der Netzwerk-Verkabelung und kann deren Auswirkungen auf Installationsaufwand, Zugänglichkeit für den Unterhalt und Kosten aufzeigen.
12. Kennt die notwendigen Einstellungen der Netzwerkkonfiguration der Netzwerkkomponenten (z.B. Computer, Router, Accesspoint) und kann aufzeigen, welchen Beitrag diese zur Sicherstellung der Kommunikation im Netzwerk leisten.
13. Kennt die wichtigsten Informationen in der Dokumentation eines einfachen Netzwerks und kann erläutern, wie diese für die Wartung und den Betrieb benötigt werden.
14. Kennt die prinzipiellen Vorkehrungen, die Netzwerkbetriebssysteme für die Ressourcenzuteilung bieten (Lese-, Schreibrecht, Benutzer, Benutzergruppen, Shares) und kann aufzeigen, wie diese die Sicherheit von Daten gewährleisten.
15. Kennt die prinzipiellen Vorkehrungen, die bei Cloudspeicherung sicherzustellen sind und kann aufzeigen, wie diese die Sicherheit von Daten gewährleisten.
16. Kennt Möglichkeiten, die Vergabe von Rechten zu dokumentieren (z.B. Matrix der Beziehungen zwischen Benutzergruppen und Shares) und kann aufzeigen, wie damit eine korrekte Vergabe der Rechte erleichtert wird.
17. Kennt die gängigen Vorgehensweisen und Methoden, einen Test mit den dazugehörigen Testszenarien durchzuführen.
18. Kennt die Vorgehensweise, einen geplanten funktionalen Test durchzuführen.
19. Kennt die Symptome der wichtigsten Fehler in einem Netzwerk und kann mögliche Ursachen (Konfigurationsfehler, Fehler bei der Verkabelung etc.) dafür beschreiben.

20. Kennt die Möglichkeiten den Datenschutz und -sicherheit zu testen und die Ergebnisse zu dokumentieren.
21. Kennt die Möglichkeiten das Netzwerk und all seine Elemente zu testen und die Ergebnisse zu dokumentieren

Literaturverzeichnis

Bratvogel, K. (2021). *PC-Technik Grundlagen.* Herdt Campus.

Bratvogel, K., & Klaus Schmidt, K. (2019). *Netzwerk Grundlagen.* Hardt Campus.

OneNote Modul 117. (kein Datum). Von OneNote. abgerufen