184.738 Computer Networks

Fragenkatalog SS22

6-7 Fragen pro Einheit

Zoom-Link:
https://tuwien.zoom.us/j/98277649292?pwd=N2RubmRGV2tCWFhXNS9RbGgrQmhwZz09

Bsp.: Network Engineering WS21/22 Network Engineering Collaborative Mitschrift

Fragenkatalog bestätigt von Siegl: Computer Networks - Fragenkatalog

Präsentationen: 5min pro Person harte Grenze

TERMINE:
Erste Präsentation: **7.4.22**
Zweite Präsentation: **2.6.22**
Prüfung: **23.6.22**
Paper Abgabe: **30.6.22**

10.3.2022

1. Was ist ein Netz?
    a. Ein Netz besteht aus Knoten und Kanten.
    b. Knoten können
        i. **Endnodes**: Können Sender/Empfänger von Informationen sein
        ii. **Forwarding Nodes**: Informationen weiterleiten (Benötigt dafür Metainformationen)
2. Was charakterisiert Shared Media?
    a. z.B. WLAN, Ethernet
    b. Alle Geräte müssen sich die Bandbreite teilen
    c. Funktioniert nur, wenn die benötigte Bandbreite aller Endpoints zusammen weniger ist als die gesamte vom Medium zur Verfügung stehende Bandbreite.
3. Welche Grundannahmen sind wichtig damit Shared Media funktioniert?:
    a. **Eindeutiger Namensraum:** Adressierung durch eine eindeutige Kennung z.B. IP-Addresse. Dieser kann von der Anzahl an Teilnehmern abweichen. Eine eindeutige Kennung durch Nachrichtentypen ist ebenfalls möglich.
    b. **Selbstbeschränkung**: Es sind “Sendepausen” (Inter-Packet gap) notwendig. *Broadcast*: Eine Nachricht an ALLE. Jede Forwarding node muss die Nachricht an ALLE Teilnehmer weiterleiten
    c. **Zugriffsmethode**: Wer kommt als nächstes dran bei shared media?
4. Welche Art von Zugriffsmethoden gibt es?
    a. Master-Slave Prinzip (Einer bestimmt wer wann reden darf).

    b. Token-Passing System (Token Ring): “Zettel” mit einer Information. Dieser wird (wenn bereits ein Inhalt am Zettel ist) nur weitergereicht. Nur wenn der Zettel “leer” ist, kann man selbst Informationen weitergeben.
    c. Ethernet Zugriffsmethode: CSMA/CD (Carrier Sense Multiple Access / Collision Detection)
5. CSMA/CD (Carrier Sense Multiple Access / Collision Detection) Funktionsweise
    a. CS: “Lauschen”
    b. MA: Wenn nichts gehört wird → Kann **jeder** jederzeit zu senden beginnen (also, wichtig: auch mehrere Teilnehmer gleichzeitig).
    c. CD: Wenn für mehrere Teilnehmer “nichts zu hören ist” kann es sein, dass diese zur gleichen Zeit senden und es somit zu einer Kollision kommt. → Es ist eine Collision Detection notwendig. Wenn Collision erkannt wird, warten die Teilnehmer eine zufällige Zeit lang → kann dann trotzdem wieder zu einer Kollision kommen, bis zu 8 Mal; Unterschied zu Token Ring: Bei Token Ring hat man Sättigung, hier kann es passieren, dass das System kippt, d.h. keine Übertragung mehr möglich ist.
6. Was bedeutet gleichzeitig bei Ethernet?
    a. Die Dauer die eine Nachricht von einem Knoten bis zum Ende des Netzes braucht und zurück
        i. Sender A sendet -> Kurz bevor es bei Sender B ankommt lauscht dieser -> Sender B hört nichts und sendet ebenfalls -> Sender A sendet weiter bis die Nachricht von B bei ihm ankommt.
7. Wo beginnt ein Datennetz und wo endet es?
    a. Nicht eindeutig wo LAN, Betriebssystem und Applikation ihre Grenzen haben
        i. Grenzen sollten definiert werden, ansonsten kann es bei Fehlern dazu kommen,
        ii. Dadurch bei Fehlern im Datennetz müssen “alle” Gruppen beweisen dass es nicht an ihnen liegt.
    b. Praktisch nicht umsetzbar!

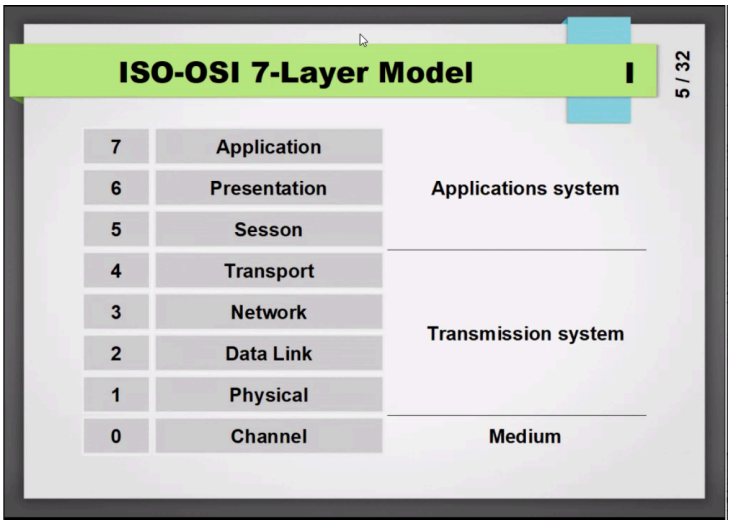
17.3.2022

1. **Nenne die 7 Layer des ISO OSI Modells und deren Unterteilung**
   (Diensterbringung nach oben, Dienstanforderung nach unten)
    a. Physical: Wie werden die Signale übertragen
    b. DataLink: Bitströme (ausreichend für Punkt-zu-Punkt Übertragung, Layer 3 nicht zwingend erforderlich);
       Gibt payload and Layer 3 weiter, Layer 3 zerpflückt dann die payload in das eigentliche IP-Packet (Header + Data)
    c. Network (bei einfachen “Werkzeugen” optional): Nicht immer implementiert!
    d. Transport (bei einfachen “Werkzeugen” optional):
    e. Session (bei einfachen “Werkzeugen” optional):
    f. Presentation:

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

g. Application:

h.



2. **Welche Layer benötigt man um Kommunikation zwischen zwei Geräten zu ermöglichen?**
    a. Einfache Kommunikationswerkzeuge können sich unter umständen auf niedrige Layer z.B. Layer 2 beschränken. Eine Konfiguration ist dann nur mit spezieller Software und per Kabel möglich (Kein Switch!).+
    b. Wozu braucht man dann die höheren Layer? Was fehlt wenn man nur die niedrigen verwendet?
3. **Vor/Nachteile von Herstellerspezifischen Features, die vom Standard abweichen**
    a. Oft bessere Lösungen als der Standard
    b. Arbeiten außerhalb der Normen und Standards
    c. Bindung an den einen Hersteller
    d. Keine Kompatibilität zwischen Geräten unterschiedlicher Hersteller
    e. zB.: Cisco

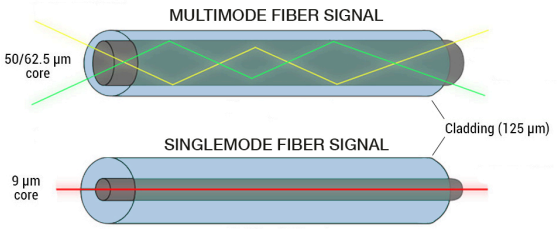
~~4. Problem bzgl. Performance: Da die Interfaces zwischen den Layern klar und sauber abgegrenzt sein müssen, gibt es keine Möglichkeiten, "Shortcuts" zu nehmen (es kann kein Layer übersprungen werden) und daher performance zu gewinnen.~~

~~5. Wie schnell sind elektromagnetische Wellen in anderen Medien?~~
    ~~a. ⅔ in Glasfaserkabel (PI*Daumen = 2*10^8 m/s)~~

6. **Wie breitet sich Licht in Lichtwellenleitern aus?**
    a. Nicht gerade sondern wird ständig reflektiert

b. Funktion mittels Totalreflexion
c. Leiter muss ein Kernglas haben mit einem Mantelglas umgeben

7. **Was ist der Unterschied zwischen Singlemode und Multimode Glasfaser?**
   a. Singlemode - Weniger “Verschmierung” des Signals - gut für längere Distanzen - 10 micrometer Außendurchmesser - nur 4% der Leistung, siehe Quadratische Skalierung von Single auf Multimode
   b. Multimode - nutzt man für kürzere - Außendurchmesser 50 micrometer
8. **Eigenschaften von Glasfaser/Lichtwellenleiter**
   a. Lichtwellenleiter funktionieren gut, solange sie nicht zu stark gebogen werden (zu starke Verluste (Abstrahlung von Kern in den Mantel), daher minimaler Biegeradius bei Glasfaserkabeln von ca. 6 cm).
   b. Die “Rampen” werden im Laufe der Strecke immer “flacher” bis es gar nicht mehr an den Rand zur Reflexion kommt
   c. Glasfaser besteht aus zwei verschiedenen Gläsern: Mantelglas und Kernglas, Mantelglas transportiert Licht NICHT, ist nur zur Reflexion da
   d. Diese sind desweiteren mit einem “Coating” umhüllt → siehe Blown-fiber
   e. Durchmesser:
      i. **Singlemode:**
         1. Kernglas, Innen 0µ, **Außen (9/)10µ**
         2. Mantelglas, Innen 10µ, Außen 125µ
      ii. **Multimode**:
         1. Kernglas, Innen 0µ, **Außen 50µ**
         2. Mantelglas, Innen 50µ, Außen 125µ



   f. Wenn Querschnittsfläche größer als Wellenlänge(Multimode) des zu transportierenden Lichts, führt zu schnellerer Dispersion
   g. Multimode für kurze Distanzen, Single für große
   h. Multimode hat den 25-fachen möglichen Energiewert (Quadratisches Verhältnis der Flächeninhalte), d.h. man kann nicht Multimode auf Singlemode einfach “zusammenstecken”, da man 96% verlieren würde → Daher wird bei Singlemode Fasern ein Laser benötigt (teuer als Leuchtdiode)
      Wenn man heutzutage Multimode einsetzt, dann 300 bis 500 m Einsatzbereich, alles darüber hinaus → Singlemode

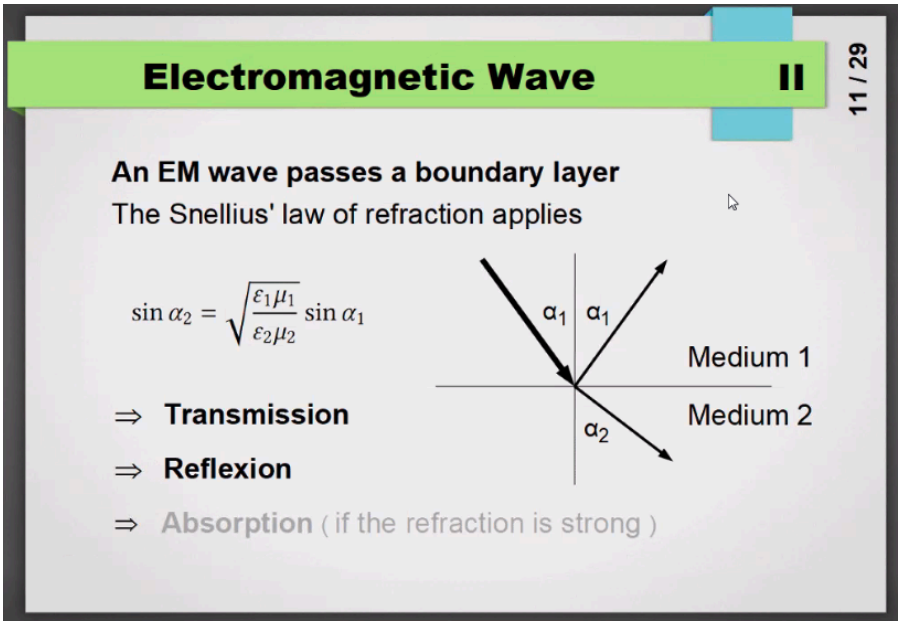
~~9. Warum sollte man nicht in ein Glasfaserkabel sehen?~~
   ~~a. Durch die kleine Querschnittsfläche ist es wichtig, nicht in ein Glasfaserkabel zu schauen -> Netzhautablösung~~

~~10. Wie sehen Glasfaserkabel heute aus bzw. wie werden sie verlegt?~~
   ~~a. als ganze Kabelstränge~~

~~11. Blown-fiber: leere Röhrchen (Kunststoffkanäle) von 3-7? mm mit coating (raue Schicht). Coating auf Mantelglas ist dazu da, um durch geblasene Luft die gesamte~~

~~Faser gleichmäßig durch die Röhrchen durchzuschieben (Luft hat an dem rauen coating Halt)~~

12. **Was ist eine Totalreflexion?** Wann kommts dazu, was passiert, warum braucht man das? (genommen)
    a. 2 verschiedene Medien => unterschiedliche alpha. Wenn alpha 1 größer wird, wird auch alpha 2 größer, bis zur Totalreflexion (=ausschließlich Reflexion, keine Transmission mehr). Bei Totalreflexion beträgt alpha2 90°.



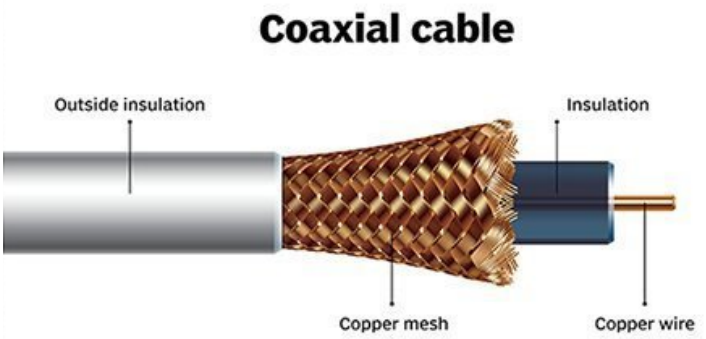
    b. Nur beim Übergang vom optisch dichteren zum optisch dünneren Medium kann Totalreflexion auftreten.
    c. Dieses Phänomen entsteht auch bei einer Fata Morgana (heiß und kalte Luft treffen aufeinander), wodurch das Licht unterschiedlich gebrochen wird. Der Lichtwellenleiter nutzt die Totalreflexion. => Lichtwellenleiter funktionieren gut, solange sie nicht zu stark gebogen werden (zu starke Verluste (Abstrahlung von Kern in den Mantel), daher minimaler Biegeradius bei Glasfaserkabeln von ca. 6 cm).

Hausaufgabe:
Bitstrom 10101010; Laser in Lichtwellenleiter (Wien-München). Wie lange ist ein Bit auf dieser Leitung? (=Wellenlänge = 3*10^8 / frequ) bei 1Mbit/s.

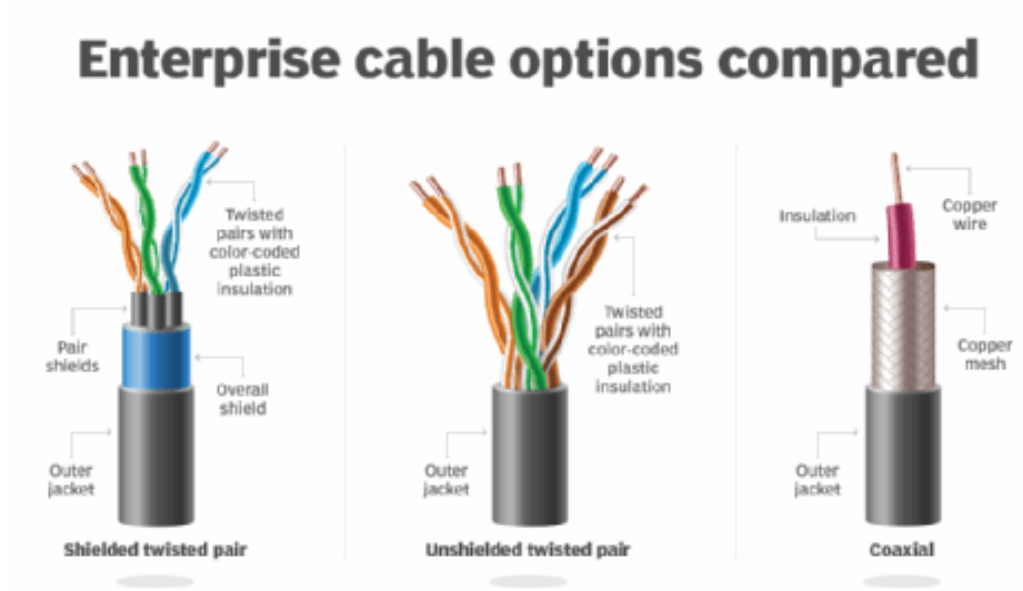
24.3.2022

1. **<u>Was bedeutet Coaxial?</u>**

- gleichachsig
- Achse in der Mitte, darum herum das Kupferkabel, darum eine Isolation (Weiß), außenzylinder Kupfergeflecht = 2 Drähte (notwendig)
- Benötigt einen Innenleiter (CopperWire) und einen Außenleiter (CopperMesh)
- “Asymmetrisches Kabel”-Signalleiter + Masseleiter =Kupfergeflecht
- für hochfrequente Übertragung



2. **<u>Welche Aufbauarten von Twisted Pair gibt es?</u>**
   Für jedes Paar gilt: In einem Kabel fließt der Strom hinein, in dem anderen hinaus.



Wie beeinflussen sich die Magnetfelder der einzelnen Kabel gegenseitig? - Twisted Pair wird verwendet um diese Einflüsse der Magnetfleder möglichst gering zu halten.
z.B. ein RJ45 Stecker hat 4x2 Paare.

3. **Was hat es mit den goldfarbenen Kontakten bei RJ45 Steckern auf sich?**

- Die Kontakte sind vergoldet um eine Oxidation zu verhindern (Edelmetalle reagieren nicht mit Sauerstoff ⇔ Rosten nicht).
- Die vergoldeten Kontakte sind sehr gut leitfähig

- Die Kontakte sind nach einem gewissen Steckzyklus zu stark abgenutzt und müssen getauscht werden.

4. Wie kann man einen “Stecker” designen?
- Stifte wie bei Schuko.
- Drückelement wie bei RJ45

5. Wie entsteht Crosstalk?
- Aufgrund vom RJ45 Stecker und elektromagnetischen Wellen “springen” Signale von den einzelnen Twisted Pairs auf andere Twisted Pairs, man bekommt Störsignale

6. <u>Was sind die Arten des Übersprechens/Crosstalk?</u>
- **NEXT** - Near End Crosstalk (passiert schon am Ausgang des Senders) - an der ersten RJ45 Schnittstelle - das was man sendet bekommt man wieder zurück (wenn man sich selbst auf dem Kabel hört).
    - Dieser Effekt entsteht durch elektromagnetische Felder → Signal auf dem sendenden Kabel springt auf das empfangende Kabel über.
    - Da der Sender die Inhalte genau kennt, kann er diese eliminieren/ herausrechnen.
- **FEXT** - FAR End Crosstalk (Passiert am Eingang des Empfängers) - analog zu NEXT nur am anderen Ende der Leitung mit Zeitversatz, wo wieder ein RJ45 Stecker ist
    - Entsteht auch aufgrund von elektromagnetischen Feldern.
    - Da der Sender die Inhalte auch hier genau kennt, kann er diese eliminieren/ herausrechnen.
- **AXT** - Alien Crosstalk - Wie die anderen beiden, nur dass man hier Signale von anderen hört, was dazu führt, dass es schwer zu filtern ist. Passiert wenn sehr viele Stecker/Kabel nahe beieinander sind z.B. bei einem Switch.

7. <u>Wie löst man Alien Crosstalk (Maßnahmen gegen)?</u>
- Mögliche Lösungen: Dickere Mäntel/größere Abstände zwischen Pärchen/Kabel
- Übliche Lösung: Schirmung (STP = shielded twisted pair (siehe Grafik oben) und nicht UTP = unshielded twisted pair)
- Shielded twisted Pairs können zusätzlich auch noch mit einem Geflechtschirm (Aluminium-Folie oder einem Kupfergeflecht) umspannt werden, um gegen niedrige Frequenzen abzuschirmen.

8. Warum lecken Kühe Autos (gehört zu Goldkontakten Frage)?
- Weil sie den Lack von den Autos brauchen um richtig *bum zua* zu werden

31.3.2022

1. Qualitätsnormen der Verkabelung im Haus
    a. 2 Arten der Hersteller: Hersteller des Endgeräts/Interfaces, Hersteller der Kabel/Buchsen; beide haben unterschiedliche Anforderungen, auch hinsichtlich Normung.
        i. Wenn z.B. mehr Crosstalk/Störungen, dann teurer für Interfacehersteller (bessere Filter etc. benötigt)

ii. Wenn Kabel gute Qualität haben, dann günstiger für Interfacehersteller

→ für die Norm muss Kompromiss gefunden werden
Norm gibt also z.B. für Interfacehersteller eine bestimmte Qualität der Strecke vor, nach der diese ihre Geräte bauen und vice versa

2. Was stellen Qualitätsangaben der Einzelkomponenten (**Kategorien**) sicher?
   - Dass alle Komponenten zueinander passen
   - Früher hatten alle Teile z.B. Kategorie 6a, zusammenstecken funktionierte
   - heute müssen Stecker und Buchse aufeinander abgestimmt werden (hohe Datenübertragungsraten wie 10 Gbit/s → minimale Fertigungstoleranzen)
   - 10 Gbit/s benötigt z.B. 500 MHz Frequenz (Vergleich Ö3: 100MHz)

3. **Was ist wichtig beim Verbauen einer Verkabelung bezüglich der Kabelstrecke (Qualität)?**

- Bestimmung der Qualität der gesamten (fertig installierten) Strecke (=**Klasse** z.B. c,d,e) auf einer Baustelle: wichtig wie der Installateur die gesamte Strecke in der Praxis verlegt/aufgebaut hat
  1 Gbit braucht Klasse d (100 MHz)
  Klasse f
  Klasse ea (500 MHz) kam erst nach f, ea ermöglicht 10 GBit/s über Kupferleitungen

Kategorie	Klasse	Typ	Bandbreite	Geschwindigkeit	Anwendungen
Cat 1	A	UTP	0,1 MHz	1 Mbit/s	Telefon- und Modem-Leitungen
Cat 2	B		1 MHz	4 Mbit/s	ältere Terminalsysteme, z. B. IBM 3270
Cat 3	C		16 MHz	10 Mbit/s	10BASE-T und 100BASE-T4
Cat 4			20 MHz	16 Mbit/s	16-Mbit/s-Token Ring
Cat 5	D		100 MHz	100 Mbit/s	100BASE-TX
Cat 5e	D		100 MHz	1 Gbit/s	1000BASE-T, 2.5GBASE-T und 5GBASE-T@<75m
Cat 6	E		250 MHz	1 Gbit/s	5GBASE-T und 10GBASE-T@<55m
Cat 6A	E_A	STP	500 MHz	10 Gbit/s	10GBASE-T
Cat 7	F	S/FTP	600 MHz	10 Gbit/s	CCTV
Cat 7a	F_A		1000 MHz	10 Gbit/s	
Cat 8.1/8.2	I/II		2000 MHz	40 Gbit/s	25GBASE-T und 40GBASE-T

4. **Was für Strecken Unterscheidungen gibt es bei Ethernet?**

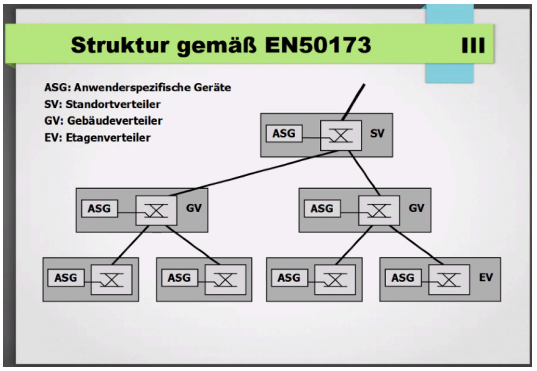
- permanent Link: Patchkabel spielt keine Rolle (Buchse und Kabel fest im Haus verlegt); hat höhere Qualitätsanforderungen Anforderungen; (Permanent Link Messung)
- Channel: das sind beide Patchkabel (am Anfang zum permanent Link und am anderen Ende vom permanent Link wieder zurück). Diese spielen auch eine wichtige Rolle (ein schlechtes Patchkabel ruiniert die Qualität der gesamten Strecke)

5. **Was ist ein Gewerk?**

- Etwas was ein “Professionist” baut (z.B. ein Maurer der die Wände hochzieht, ein Elektriker, eine Datenverkabelung)

6. **Wie verlegt man die Kabel in einem Gebäude (gemäß Norm EN50173)? EN50173 grundsätzlicher Aufbau und Verkabelungsschema**

- (vom Internet zum) Standortverteiler werden ausschließlich LWL genutzt (z.B. ein Gebäude)
- Zwischen Standortverteiler und Gebäudeverteiler (z.B. ein Trakt eines größeren Gebäudes) befindet sich primäre Bereich (hier wird Glasfaser=Lichtwellenleiter verlegt. Mit Glasfaser sind Strecken von 300-500 m überbrückbar)
- Zwischen GV und EV wird auch LWL verwendet (sekundärer Bereich)
- Von Etagenverteiler zu Endgeräten (tertiärer Bereich) wird Kupfer verwendet (ist aber auch Glasfaser möglich, wird aber aufgrund der hohen benötigten Kabelmenge oft nicht gemacht;



- Consolidation points siehe Bodentank
- Praxisbeispiel TU Wien Gebäude Gusshausstraße neues ET: 250km Kabel insgesamt verlegt; ca. pro Fenster welches von außen sichtbar ist, 10 Leitungen); Auf einer Kabeltrommel bei der Lieferung ist 1 km Kabel → 250 Kabeltrommeln

7. Wie viel Meter Luftlinie kann man mit 90m Kabellänge überqueren?

- Faustformel: 90 m Kabellänge überbrückt 45 m Luftlinie, Durchschnittswert sind 55m pro 45m Luftlinie

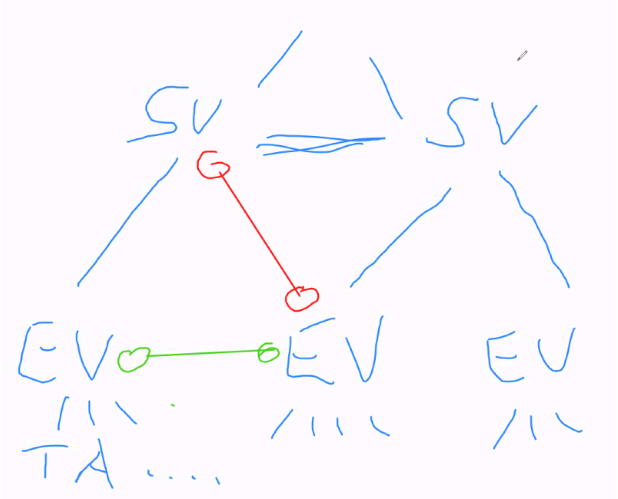
8. **Was ist ein Bodentank, Vorteile Nachteile?**

- Consolidation points unterbrechen permanent Link Strecke: Bodentanks (Hohlraum mit Deckel) zum Anstecken von Steckern in Buchsen am Boden. Diese werden zuerst installiert. Anschließend wird von Bodentank zu einer Laborstation noch ein Kabel verlegt zu einer Buchse an der Station, und dann erst ein kurzes Patchkabel.
- Vorteil: Kabel nicht quer durch den Raum verlegt
- Nachteil: Schmutz nur schwer entfernbar, muss von Reinigungskraft extra gereinigt werden

Etagenverteiler sind kleine Räume (meist ohne Fenster, klein bemessen) mit 2-3 Schränken. Benötigen Kühlung (genau wie Standortverteiler)

9. Was ist ein Nachteil von Kabelstrukturen laut **EN50173** und wie geht man mit diesem um?

- Struktur gemäß EN50173 bietet keinerlei Redundanz; ist aber möglich diese einzubauen
- Fix 1 (rot eingezeichnet): Zusätzliche Verbindungen zwischen SVs und EVs die laut EN50173 “nicht vorhanden” sind. Braucht aber ein zusätzliches Interface im SV (teuer) und im EV
- Fix 2 (grün eingezeichnet): EVs miteinander verbinden. Braucht aber zusätzliche Interfaces zwischen EVs (sind aber deutlich billiger).



Nachteil: Mittlerer EV wird aber zu “Transitswitch”, muss dann zusätzliche Arbeit leisten -> Perfomance und Leistung muss reichen, sonst hat man ein Problem

- Beide Varianten sind in Ordnung

10. Was bedeutet die Kategorie und Klasse bei Patch Kabeln?

https://www.reichelt.de/reicheltpedia/index.php/Patchkabel

- Kategorie = Leistungsklasse
- Je höher die Kategorie, desto höher die ft des Kabels
- Die darunter liegende Kategorie wird jeweils mit abgedeckt
- Werden innerhalb einer Installation Komponenten verschiedener Kategorien gemischt, definiert sich die Gesamtqualität durch die Komponente der niedrigsten Kategorie

Kategorie	Klasse	Typ	Bandbreite	Geschwindigkeit	Anwendungen
Cat 1	A	UTP	0,1 MHz	1 Mbit/s	Telefon- und Modem-Leitungen
Cat 2	B		1 MHz	4 Mbit/s	ältere Terminalsysteme, z. B. IBM 3270
Cat 3	C		16 MHz	10 Mbit/s	10BASE-T und 100BASE-T4
Cat 4			20 MHz	16 Mbit/s	16-Mbit/s-Token Ring
Cat 5	D		100 MHz	100 Mbit/s	100BASE-TX
Cat 5e	D		100 MHz	1 Gbit/s	1000BASE-T, 2.5GBASE-T und 5GBASE-T@<75m
Cat 6	E		250 MHz	1 Gbit/s	5GBASE-T und 10GBASE-T@<55m
Cat 6A	E_A	STP	500 MHz	10 Gbit/s	10GBASE-T
Cat 7	F	S/FTP	600 MHz	10 Gbit/s	CCTV
Cat 7a	F_A		1000 MHz	10 Gbit/s	
Cat 8.1/8.2	I/II		2000 MHz	40 Gbit/s	25GBASE-T und 40GBASE-T

28.4.2022

1. Was ist eine MAC Addresse?

- Steht für “Media Access Control”
- Ist eine eindeutige Nummer für NICs (Network Interface Cards) von Hersteller der NIC/Hardware
- Ist 48 bit lang (6 Octets)
- Kann auf den Hersteller der NIC hinweisen (X ist Karte von Hersteller Y)
- Kann mit Software aber gefaked werden
- Securitykonzepte auf Basis von MAC sehr unsicher

2. Wie ist die (grunsätzliche) Funktionsweise eines Layer-2-Switches?

Layer2 = Switching; Layer3 = Routing
(Es gibt keinen wirklichen Layer3 Switch - Marketing “Gag”)

a. Switches (früher Bridge) verwenden die MAC-Adresse um Pakete korrekt weiterleiten zu können. Switch verwaltete einen Table welche Geräte bzw. deren MAC Adresse welchem Port zugeordnet ist.
b. Switch hängt zwischen mehreren Netzwerken und verbindet diese
c. Wenn Ziel-MAC-Adresse nicht in der Tabelle ist, dann wird die Nachricht auf jedem Port gesendet und sendet es an alle. (Annahme: Das Gerät existiert)
d. Mögliche Fälle:
    i. **Erfolgreiche** Pakete

        ii. **Fehlerhafte** Pakete werden gedroppt, Konsequenzen:
            1. Sender wartet bis der Timeout ausläuft
            2. Muss bis dahin Ressourcen freihalten
        iii. **Zieladresse** ist **am selben Port** von dem die Nachricht gekommen ist (kann einfach verworfen werden)
        iv. **Queue geht über**: Prozessor kann Nachrichten aus der Input/Output Queue nicht schnell genug abarbeiten und daher gehen Pakete verloren.

3. **Was ist ein Broadcast (Layer 2)?**
    a. Eine Nachricht an alle.
    b. MAC-Adresse ff:ff:ff:ff:ff:ff
    c. Nachteil: Alle bekommen einen Interrupt im Netzwerk, Ressourcen auf Geräte welche nicht angesprochen werden werden trotzdem verwendet.
    d. Vorteil: Kann auch an einen Teilnehmer senden bei dem nicht klar ist wo der ist.
4. Was ist der Ablauf von Broadcast?
    a. Nachricht an ALLE (Broadcast) vs Nachricht an EINEN (Switch mit unbekanntem Empfänger, weil MAC nicht im Table)
5. **Was ist eine Layer 2 Broadcast-Domäne (gehört zu 3)?**
    a. Innerhalb der Broadcast Domäne bekommt jeder das Paket.
    b. “Wo Broadcasts propagiert und weitergeleitet werden”
    c. Außerhalb einer Broadcast Domäne werden keine Broadcasts mehr weitergeleitet (bspw. ein Router grenzt das ab)
6. **Was ist ein ARP?**
    a. “Address Resolution Protocol”
    b. Wird genutzt um zu IP Addressen entsprechende MAC Addressen zu finden
        i. “Who has” request in Form eines Broadcasts
        ii. Das Gerät mit der angefragten IP Antwortet mit seiner MAC Adresse (Unicast Paket zurück, da der Empfänger ja bekannt ist)
    c. Ist ein Layer 2 Broadcast in die Broadcast Domäne
7. **Was ist PoE und wie betreibt man PoE?**
    a. Power over Ethernet
    b. Gerät wird über LAN mit Strom versorgt
    c. Kabel können sich erwärmen! -> Achtung bei Kabelbündel, bessere Kabel mit besseren (größeren) Kupferquerschnitt kaufen
    d. Mit Injektor (hat Schuko Stecker und LAN Stecker), dran steckt man das Zielgerät auch an (mit LAN)
    e. Switch mit PoE und Schuko, hat innen drin ein Netzteil eingebaut (58 V) -> Achtung permanenter Stromverbrauch für alle Ports und Wärme!
    f. PoE kann genutzt werden, um Defekte frühzeitig vorherzusagen (stetig steigende Stromaufnahme) und dadurch unerwartete Netzwerkausfälle zu verhindern.
    g. Achtung bei Außenverwendung wegen Blitzgefahr (z.B. bei Außenkameras an Masten)
        i. Lösung Glasfaserkabel bis zum “Masten” + Stromversorgung 230V (Glasfaser leitet den Blitz nicht)
        ii. Switch wird per Glasfaserkabel verbunden + 230V Stromversorgung

iii. Vom Switch ausgehend wird die Kamera per Ethernet + PoE verbunden
iv. Blitzschutz über 230V Stromversorgung!

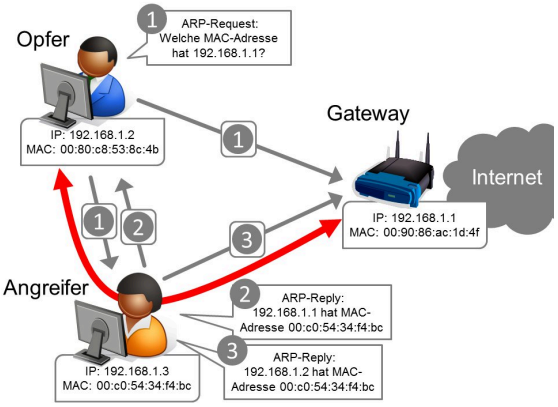
8. **Was sind die Rollen eines Switches?**
   Ein Prozessor vs multiple Prozessoren in einem Switch:
   i. Ein Prozessor ist günstiger und einfacher handzuhaben

   Bei Hochlast kommt es zu Resourcenkonflikten und es muss entsprechend eine Rolle Vorrang bekommen.
   a. **Primary Role** (Tatsächliches Routing der Pakete)
   b. **Management Role** (Zusatzfunktionen des Switches z.B. QoS, …) - Manager sollte Vorrang haben, da sich der Switch sonst “selbst überlassen” ist und keiner mehr steuernd eingreifen kann.

9. Was ist ein Snoop(ing?)y Port
   a. Kann den Traffic von anderen Ports spiegeln
   b. Geeignet zu Analysezwecken

05.05.2022

1. **Wie findet ein Windows-Rechner ein Share eines anderen Windows-Rechners?**
    a. **Broadcast an alle** “Übrigens, bei mir kann man auch drucken” (Alle Rechner die ein Netzwerk-Share anbieten, senden periodisch einen Broadcast, dass sie Dienste anbieten.)
    b. **Broadcast anfordern** “Wer hat einen Drucker?”
    c. **Dritte Instanz** (z.B. MQTT Server) verwaltet die Dienste
        i. Registriert die vorhandenen Drucker
        ii. Informiert andere Netzwerkteilnehmer über Änderungen (Voraussetzung: Netzwerkteilnehmer hat sich registriert bei der dritten Instanz und “möchte informiert werden”)
2. **Ab wievielen Geräten sollte man ein Netzwerk auftrennen (Segmentier Kriterien)?**
    a. ~200
    b. Komponenten, die viel miteinander kommunizieren, ins gleiche Netz
    c. Security beachten
    d. Hauptkriterium: Broadcasts
3. **Wie viel Einträge kann ein Mac Address Table für gewöhnlich aufnehmen und was passiert, wenn die Tabelle zu klein wird (Dimension der MAC Tabelle)?**
    a. 2000-32000 je nach Gerät
    b. Einträge werden einfach überschrieben
        i. Ermöglicht MAC Table Flooding
        ii. Wenn die Adresse nicht in der Tabelle registriert wird, dann wird das Paket an alle Adressen geschickt (Broadcast)
4. **Was nutzt ein MAC Table Flooding Angriff aus und wie funktioniert dieser?**
    a. Dass wenn die MAC Tabelle eines Switches voll ist, die Pakete einfach an alle Ports ausgesendet werden
    b. Switch sieht sich Absender-Adresse des Pakets vom Angreifer an und speichert diese in MAC-Table + speichert auch Port-Nummer
    c. Dann wird Ziel-Adresse des Pakets gesucht und je nachdem ob diese im Table vorhanden ist, wird es auf allen Ports rausgeschickt
    d. Ausnahme: Falls Zieladresse am selben Port ist wie der Absende-Port, wird dieses Paket sofort verworfen
    e. D.h. der MAC-Table wird mit immer neuen Adressen geflooded, sodass älteste Adressen “rausgeworfen” werden und somit “legitime” Pakete wieder auf allen Ports ausgesendet werden, sodass Attacker diese auch mitbekommt



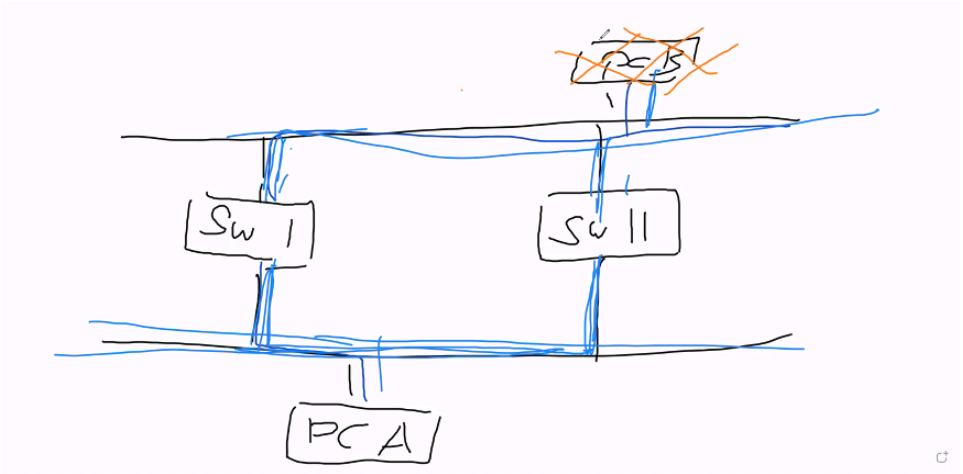
5. Was ist MAC Address Spoofing?
    a. “Who has 192.168.0.1?” (Layer 3)
    b. Angreifer antwortet auf ARP Request statt Opfer mit eigener MAC Addresse
    c. -> führt zu einem Man in the Middle

    d. geht nur im LAN auf Layer 2, aber nicht über einen Router hinweg, deswegen Stationen denen man nicht vertraut in ein anderes VLAN

6. **Was ist ein VLAN (Virtuelles LAN)?**
    a. Ist ein separates LAN, das rein durch die Software eines Switches getrennt wird
    b. Zwei VLANs sind bspw. auf “einer Platine”, also auf dem selben Switch
    c. Muss konfiguriert werden
    d. Ports werden konfiguriert, dass sie auf dem VLAN laufen, also zugeordnet
    e. Ein Switch wird zu mehreren “virtuellen Switches”
    f. Geräte untereinander können nicht über VLANs hinweg kommunizieren (LAN A <=/=> Lan B)
7. **Welche Vorteile/Nachteile haben VLANs?**
    a. Vorteile
        i. Remote Konfigurierbar
            1. Einfache reorganisation eines Unternehmens
            2. Einfach Erweiterung des Netzwerks
        ii. Beliebig viele virtuell getrennte Netzwerke einrichten
    b. Nachteile
        i. Kostet mehr
        ii. Individuelle Konfiguration des Switches verhindert einfachen austausch => Es ist NICHT damit erledigt einfach einen neuen Switch gleich anzuschließen
        iii. Selber Switch ist in ~ 2 Jahren (bei Austausch) vermutlich nicht mehr verfügbar. Andere Firmware => andere Konfiguration!
8. Warum können zwei Virtuelle Switches nicht miteinander verbunden werden?
    a. Aufgrund der gleichen MAC Adresse
9. Wie kann dynamisch eine VLAN zuordnung erfolgen
    a. Zertifikat
    b. MAC (unsicher)
    c. WebSeite (Username/Passwort) - einzige **personenbezogene** Variante, jedoch muss der PC eigenständig booten können, ohne Zugriff auf ein ActiveDirectory (AD)

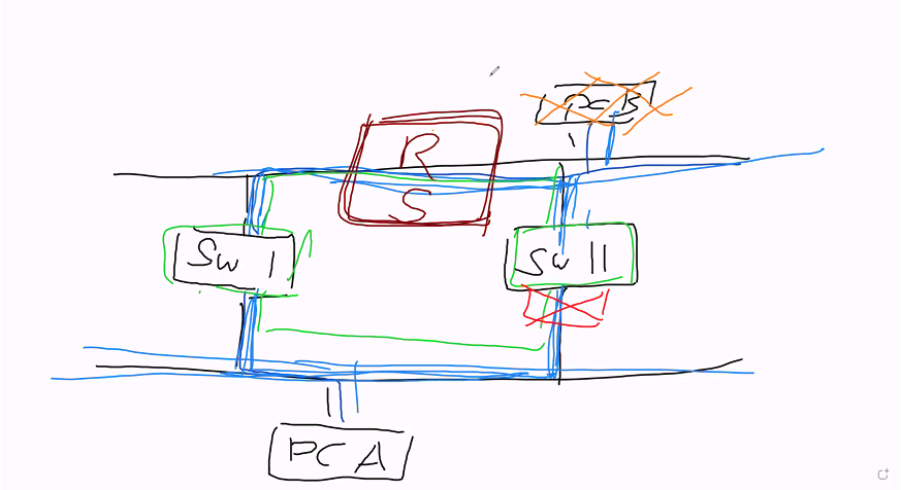
12.05.2022

1. Was für ein Issue kann auftreten bei MAC Broadcasts/Switching?
    a. Durch die Redundanz kommt es ggf. zu einer Endlosschleife → Netzwerk ausgelastet
    b. Beispiel 1: PC A → Nachricht an → PC B, dieser ist jedoch nicht online → Switch 1 & 2 kennen die MAC Adresse nicht und schicken das Paket immer an allen Ports raus → Endlosschleife
    c. Beispiel 2: Broadcast über verfügbare Services z.B. Druckerservice → Broadcast wird von Switch 2 empfangen und weitergeleitet → wird von Switch 1 wieder empfangen und weitergeleitet → …



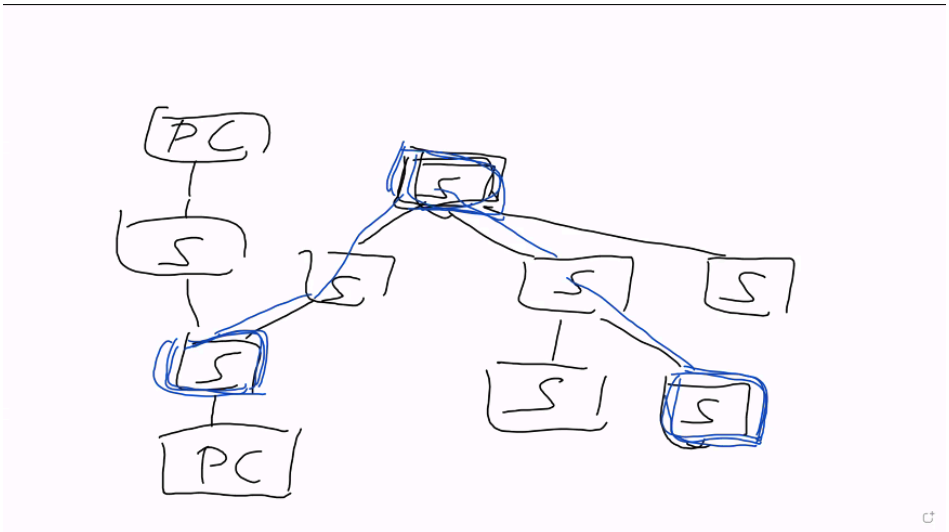
2. **Was ist ein Wartungsvertrag?**
    a. Mit Wartungsfirma einen Vertrag, die hat einige Geräte/Teile (%tueller Anteil) parat, falls ein Gerät defekt wird.
    b. Dort kann man dann anrufen und die lieferen einem ein Ersatzgerät

3. **Was ist der Spanning Tree Algorithmus?**
    a. Soll das Problem aus 1 beheben
    b. Bevor der operative Betrieb aufgenommen wird (jedoch nach dem Booten), werden Management Pakete ausgesandt um die eigenen Position im Netzwerk zu ermitteln (es wird also nicht sofort in den Forwarding-Modus gewechselt).



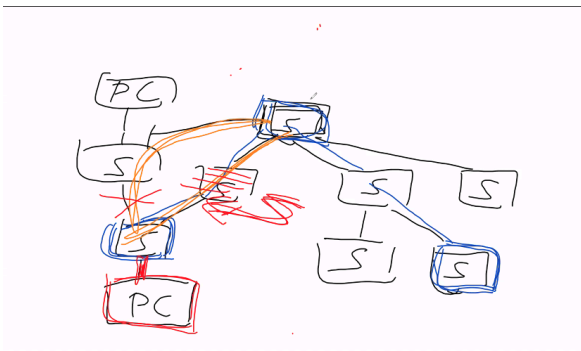
c. Dadurch können Schleifen erkannt und die entsprechenden Ports deaktiviert werden.
d. Wichtig: **Root Bridge konfigurieren**, sonst wird ein beliebiger Switch als Root ausgewählt. Dieser muss alle Pakete weiterleiten und daher über entsprechende (leistungsfähige) Hardware verfügen

4. **Worauf muss man aufpassen beim Spanning Tree Protokoll?**
   a. Welcher Switch als Root Bridge ausgewählt wird (kann ein kleiner Switch im Access Bereich sein)
   b. Problem ist, dass wenn dann Pakete von einer Hälfte zur anderen Hälfte des Spanning Trees gehen, alle über diesen einen schwachen Switch gehen.
   c. Root-Bridge muss konfiguriert werden! (damit Baum nicht schief-lastig wird)

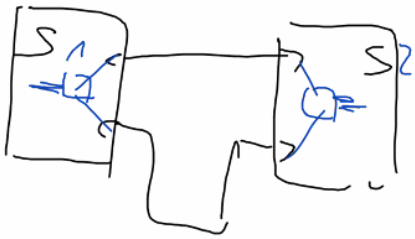


   d. Achtung Timeout-Falle: Wenn PC an Switch angeschlossen/eingeschaltet wird, kann es sein dass Switch die Pakete vom PC zu lange zurückhält (bis in Forwarding-Modus gewechselt wird, um sicher zu gehen, dass es kein Switch ist und somit keine Schleife entstehen kann) und der PC somit nicht booten kann (wenn image von Server geladen werden muss). D.h. auf dem Port an dem der PC hängt, muss Spanning Tree deaktiviert werden.

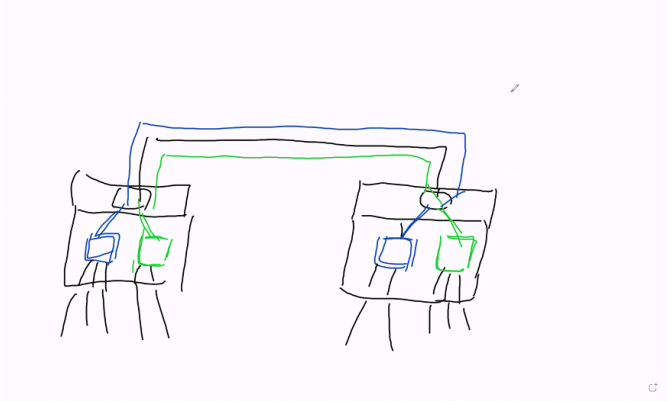
5. **Wie kann der Spanning Tree dazu beitragen Störungen zu beheben?**
   a. Der zuvor deaktivierte Port (um Schleifen zu verhindern) kann wieder aktiviert werden um fehlerhafte Switches zu ersetzen.
   b. Der Spanning Tree wird automatisch neu berechnet von den Switches mit dem Klassischen Spanning Tree Algorithmus oder dem Fast Spanning Tree Algorithmus
   c. -> Self-healing vom Netzwerk
   d. Somit sind redundante Verbindungen/Switches sehr wohl sinnvoll



6. **Was ist Port Aggregation und warum ist es sinnvoll?**
    a. Mehrer Layer 1 für ein Layer 2 (wichtig!)
    b. Verwendet, um den Nachteil von Spanning Tree (unnötig brach-liegende Leitung+Ports) anderweitig zu verwenden
    c. Die Redundanten Verbindungen (2 verschiedenen Leitungen, und 2 verschiedenen Ports) werden zu einem virtuellen Port (blau) zusammengefasst.
    d. Bedingt einsetzbar (wenn nur zwei Switche betroffen sind)



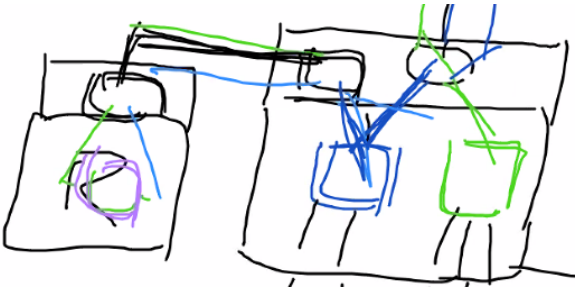
7. Wie verteilt man die Pakete bei Port Aggregation (siehe Blaue Ports)?
    a. Round-Robin einfach, aber nicht effizient
    b. Letztes Bit der MAC-Adresse hernehmen
    c. Gerade/Ungerade -> entscheidet auf welcher Leitung das Paket geschickt wird
    d. Bringt eine gute Durchmischung falls viele PCs und Server auf der jeweiligen Seite sind
    e. Schlecht falls nur 1 Server da ist und viele PCs, da dann nur eine Leitung genutzt wird
8. **Was ist der Sinn von Port Aggregation?**
    a. Erhöhung der Bandbreite
        i. 2x 1 GBit Leitungen → im Optimalfall → 2 GBit
    b. Wenn ein Port ausfällt, dann geht es instant weiter ohne Ausfall
    c. Nutzung: Beispielsweise beim Verbinden von 2 Gebäuden
    d. Besser als Spanning Tree, da da noch der Baum neu ausgehandelt werden muss
9. **Trunk-Interface (unter Verwendung von VLAN Tagging):**
    a. Mehrere Layer 2 für ein Layer 1 (wichtig!)
    b. Physikalisches Interface, das intern eine Verbindung zu zwei unterschiedlichen VLANs hat; kann Pakete unterschiedlicher LANs transportieren
    c. Vorteil: es wird nur eine physikalische Verbindung zum Connecten der Switches mit mehreren VLANs benötigt (und somit auch nur ein Interface pro Switch). Ohne dem VLAN Tagging und Trunks müsste man für jedes VLAN ein Kabel zwischen jeden Switch legen (die Anzahl der Kabel steigt schnell)



    d. Nachteil: nur eine einzelne, gemeinsame Input/Output Queue → eine Hochlast Situation kann beim anderen VLAN ein Delay bewirken
    e. Pakete müssen beim Aussenden gekennzeichnet werden und auf der anderen Seite wird das dann erkannt und dann wird das Tag entfernt (VLAN Tagging) und richtig geswitched
    f. Wenn LANs verbunden werden sollen wird Router benötigt. Dieser kann entweder klassisch mit beiden Switches verbunden werden, oder über eine

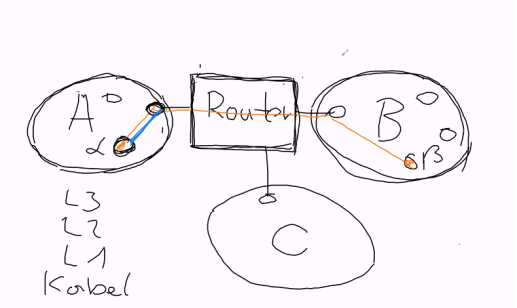
einzige Trunk-Verbindung nur an einem Switch angeschlossen werden (Single-armed Router):

10. Was ist ein Single Armed Router?
    a. Ist ein Router wie im Bild rechts, verbunden mit nur einem Switch
    b. Sinn und Zweck ist es Pakete von einem VLAN in ein anderes zu routen
    c. Heißt “Single Arm”, weil er nur mit einem Kabel Pakete aus jedem VLAN empfangen kann über ein Kabel (der Single Arm zum Switch).

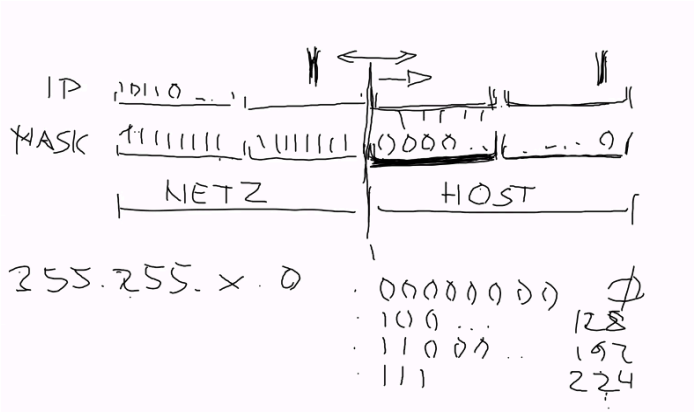


19.05.2022 **(eigentlich alles wichtig)**

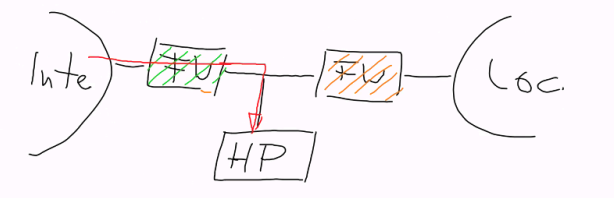
1. **Wie viele Bits hat einen IPv4 Adresse + SUBNETZE?**
    a. 32Bit (4x 8 Bit) z.B. 192.168.100.254
    b. Wertebereich 0-255
    c. Umrechnung IPv4 auf Integer
        i. (((((a*256)+b)*256)+c)*256)+d ⇔
        ii. a*256^3 + b*256^2 + c*256 + d
2. **Wie funktioniert die Idee eines Routing zwischen zwei verschiedenen Netzen (generell)?**
    a. Alpha braucht MAC Adresse des Routers
    b. Alpha schickt Paket:
        i. Layer-2: MAC Adresse des Routers
        ii. Layer-3: IP Adresse von Beta
    c. Router braucht die MAC Adresse von Beta
    d. Router schickt Paket weiter
        i. Layer-2: MAC Adresse von Beta
        ii. Layer-3: IP Adresse von Beta



3. **Wie funktionieren Subnetzmasken?**
    a. Trennen Netz von Hostanteil
    b. Sehen so aus 1111 1111.1111 1111.0000 0000.0000 0000 = trennt das Netz von den Hostadressen (kurz 255.255.0.0). Die 1er stehen für welche Bits für Netzaddressen reserviert sind und die 0er sind die Addressen für Client/Hosts
    c. Wenn man immer ein Bit mehr von den Hosts wegnimmt halbiert man die Anzahl der verfügbaren Clientaddressen
    d. 9 Möglichkeiten (0 & jeweils 1 von 8 Bits gesetzt)



4. Welche Netze gibt es?
    a. Class A Netze
        i. 8Bit Netzadresse
    b. Class B Netze
        i. 16Bit Netzadresse
    c. Class C Netze
        i. 24Bit Netzadresse
5. **Was ist ein HoneyPot**
   Vulnerable Services um Hacker “abzulenken” und deren Vorgehen analysieren zu können.



6. **Welche Adressen dürfen normalerweise nicht verwendet werden?**
    a. Broadcast Adresse 8 x 1 (255) bei der Hostadresse
    b. Netzadresse 8 x 0 (0) bei der Hostadresse
    c. RFC Adressen (Request for Command - siehe 09.06.2022)
7. **Wie kann auf Basis der IP-Adresse und Netzmaske die Broadcast bzw. Netzwerkadresse ermittelt werden? (Pflichtfrage)**

IP
NM

$BA = IP \vee \neg NM$
$NA = IP \wedge NM$
$\vee \quad \wedge \quad \neg$

8. **Wie funktioniert das Domain Name System?**
    a. Server/Dienste werden mit einem eindeutigen Namen versehen
    b. Auflösung von Namen zu IP-Adressen
    c. Namen sind Organisatorisch organisiert; Adressen sind hingegen topologisch organisiert

09.06.2022(Nicht mehr Teil der Prüfung, gelten als “1er” Fragen)

1. Was ist Reverse DNS (rDNS)?
    a. IP Adresse wird eingegeben und man bekommt einen Namen zurück -> umgekehrte von DNS
    b. Jemand anderer trägt die Verantwortung für das reverse DNS als für das DNS selbst
2. Wofür braucht man Reverse DNS?
    a. Eine IP-Adresse prüfen ob die von einem Hacker kommt oder was seriöses ist
    b. Ist ein DNS Eintrag hinter IP-Addresse X? -> deutet IP Addresse auf eine Organisation hin?
3. Wieso ist es wichtig DNS zu schützen?

    a. Wenn ein DNS System übernommen wird oder niedergerissen wird, dann funktioniert das Internet/Intranet nicht mehr oder wird irgendwie anders mishandelt (bspw. Weiterleitung an böswilligen Servern)
4. Was für DNS-Records gibt es?
    a. A-Record -> DNS Name zu IP (geht auch mit mehreren Namen zur selben IP)
    b. PTR Record -> IP zu DNS Name
    c. MX Records -> Name auf anderen Namen und dieser andere Name führt dann zu einer IP (für Mail)
    d. TXT -> Kommentare
5. Was sind RFC Addressen?
    a. Klasse C Netzwerke
    b. Wurden aus dem Pool der offiziellen Addressen rausgenommen (dürfen nicht im öffentlichen Internet vorkommen
    c. Können dafür in “privaten Inseln” genutzt werden
    d. Dürfen aber öffentlich nicht sichtbar sein
6. Was ist Masquarding?
    a. PAT und NAT -> Port Address Translation und Network Address Translation
7. Was ist PAT und NAT?
    a. Ein Router passt die internen Addressen in einem PAT/NAT Netzwerk und mapped jeweilige Pakete von innen nach außen und umgekehrt, jeweils für Ports oder interne IP Addresse.
    b. Bei NAT braucht man Schicht 4 nicht, im Vergleich zu PAT. Bei NAT wird ein Pool an offiziellen Addressen an die Masq Einheit vergeben (Router/Firewall). Wenn eine Anfrage an die lokale Seite kommt, dann schreibt er die offizielle IP rein und wenn eine Antwort kommt, schickt er es dem lokalen Gerät. Im Vergleich dazu wird bei PAT wirklich der Port umgeschrieben.
    c. Normalerweise PAT bei herkömmlichen Routern
8. Wie kommt ein Gerät zu einer IP-Addresse?
    a. Hart konfiguriert
    b. DHCP -> über das Netz eine Addresse anfordern -> DHCP Server verteilt Addressen im lokalen Netzwerk aus einem Pool an Addressen
9. Was ist das Problem mit den Jahren bei COBOL?
    a. Zahlen wurden nur mit 2 Digits gespeichert - bspw. “83” für “1983”
    b. Führte zum Jahr 2000 zu vielen Problemen, weil “00” -> “1900” und nicht “2000”
    c. Wurde gemacht um Platz zu sparen
    d. -> Immer in die Zukunft planen (30 Jahre +)
10. Was ist Schicht 4?
    a. Transport Ebene
    b. Zwei Protokolle existieren dabei:
        i. TCP -> Drei Phasen für Herstellung einer Stateful Connection. 1ste ist Setup, 2te ist Ablaufphase und 3te ist Terminierungsphase. TCP zusammen von Layer 3 und Layer 4 erlaubt die Programmierung von einem Socket.
        ii. UPD -> Connectionless = Fire and Forget, bei verwürfelten Paketen die übers WAN auf verschiedene Wege zugestellt werden, kann UDP die Pakete nimmer richtig zusammenstellen (TCP schon). UDP nur nutzen wenn Fehler “ok” sind, beispielsweise bei Videostreams, weil

das Störungen nicht bemerkbar. Hingegen bei Übertragung eines Files ist es hier wichtig das gesamte File zu richtig zu bekommen, hier TCP nutzen.

11. Was passiert bei TCP wenn die Terminierungsphase abrupt beendet wird (nicht sauber)?
    a. Die Ressourcen sind beim anderen Verbindungspartner gebunden bis der in ein Timeout läuft
    b. Nicht gut für den anderen Verbindungspartner
    c. Kann genutzt werden um Ressourcen zu verschwenden bei Zielen (Denial of Service Attacke)