NETT HS 2021

Victor Fernández

1. Januar 2022

Inhaltsverzeichnis

Teil I
SW 01 - Networking Today & Networking Trends

1 Lernziele (Leitfragen)

1. Wieso sind Computernetzwerke wichtig in unserem Leben?
2. Wieso sind Computernetzwerke wichtig für Unternehmen und unsere Berufe?
3. Wieso ist Kenntnis der Computernetzwerke wichtig für die Wirtschaftsinformatik?
4. Was ist ein «End Device» (Endgerät)? Geben Sie Beispiele.
5. Was ist ein “intermediary (network) device” (Netzwerkkomponente), oder Netzwerkgerät? Geben Sie Beispiele.
6. Wie funktioniert das «Client-Server» Modell? Geben Sie Beispiele.
7. Wie funktioniert das «Peer-to-peer» Modell? Geben Sie Beispiele.
8. Wie unterscheiden sich physikalische und logische Netzwerkdiagramme?
9. Wie kann man anhand ihrer Grösse Computernetzwerke klassifizieren?
10. Wie unterschieden sich LANs und WANs? Was ist ihre Beziehung?
11. Was ist das Internet? Wer besitzt das Internet? Was für Organisationen sind in der Entwicklung des Internets beteiligt?
12. Was ist der Unterschied zwischen einem Intranet und einem Extranet?
13. Wie verbinden sich normalerweise Häuser, Wohnungen und HomeOffices mit dem Internet?
14. Wie verbinden sich normalerweise Büros und Unternehmern mit dem Internet?
15. Was bedeutet Konvergenz im Kontext der Computernetzwerke?
16. Was bedeutet «fault tolerance» (Fehlertoleranz) im Kontext der Computernetzwerke? Geben Sie ein Beispiel
17. Was bedeutet «scalability» (Skalierbarkeit) im Kontext der Computernetzwerke? Geben Sie ein Beispiel
18. Was bedeutet «quality of service (QoS)» im Kontext der Computernetzwerke? Geben Sie ein Beispiel
19. Wieso ist Netzwerksicherheit wichtig?
20. Was sind die drei Hauptinformationssicherheitsziele?
21. Was ist «BYOD» und was sind seine Auswirkungen für Geschäfte und Unternehmen?
22. Was ist «cloud computing» ? Was für Cloud Arten gibt es?
23. Was ist die Verbindung zwischen «cloud computing» und Computernetzwerken?

2 Antworten

Wieso sind Computernetzwerke wichtig in unserem Leben?

Die zunehmende Digitalisierung erfordert eine immer grössere Vernetzung im Alltag. Sei es beruflich mit E-Mails, Website, Dateitransfer, cloudbasierte Lösungen etc. oder auch privat mit digitalem Fernsehen, Streamingangeboten von Videos und Musik, bis zur Smart-Watch.

Wieso sind Computernetzwerke wichtig für Unternehmen und unsere Berufe?

Für moderne Unternehmen ist es heutzutage wichtig vernetzt zu sein. Man verfügt beispielsweise über IP-Telefone, Fileserver, Mailserver, Virtual-Machine-Server, Rendering-Server etc. Um auf all diese Dienste zugreifen zu können, muss ein Computernetzwerk bestehen.

Wieso ist Kenntnis der Computernetzwerke wichtig für die Wirtschaftsinformatik?

Die Berufsausrichtung/-aussicht der Wirtschaftsinformatikspezialisten tendiert dazu, dass sie leitende Angestellte werden. Genehmigungen für Budgetanträge im Bereich der Informatik erfordern daher ein gutes Know-How von Komponenten, die in der Branche verwendet werden.

Was ist ein «End Device» (Endgerät)? Geben Sie Beispiele.

- Smartphone & IP-Telefone
- Drucker
- Notebook
- Server (physisch)
- Tablet
- IoT-Geräte

Was ist ein "intermediary (network) device" (Netzwerkkomponente), oder Netzwerkgerät? Geben Sie Beispiele.

- (Wireless-)Router
- LAN & Multilayer Switches

Wie funktioniert das «Client-Server» Modell? Geben Sie Beispiele.

Das Modell beschreibt die Rolle eines zentralen Dienstanbieters (Server), der Dienstnutzern (Clients) den Zugang zu seinen Diensten verschafft. Der Client bezieht lediglich den Dienst, indem es dem Server einen ***request*** sendet, der Server antwortet mit der ***response***.

Wie funktioniert das «Peer-to-peer» Modell? Geben Sie Beispiele.

Hier übernimmt ein Client gleichzeitig die Funktion eines Servers. Dadurch wird der Client zu einem ***Peer***. Peers bieten daher Dienste und Ressourcen an und nehmen aber gleichzeitig Dienste von anderen Peers in Anspruch.

Wie unterscheiden sich physikalische und logische Netzwerkdiagramme?

Das physikalisches Netzwerkdiagramm zeigt, wie der Name sagt, den ***räumlich physikalischen Standort*** der Netzwerkkomponenten.

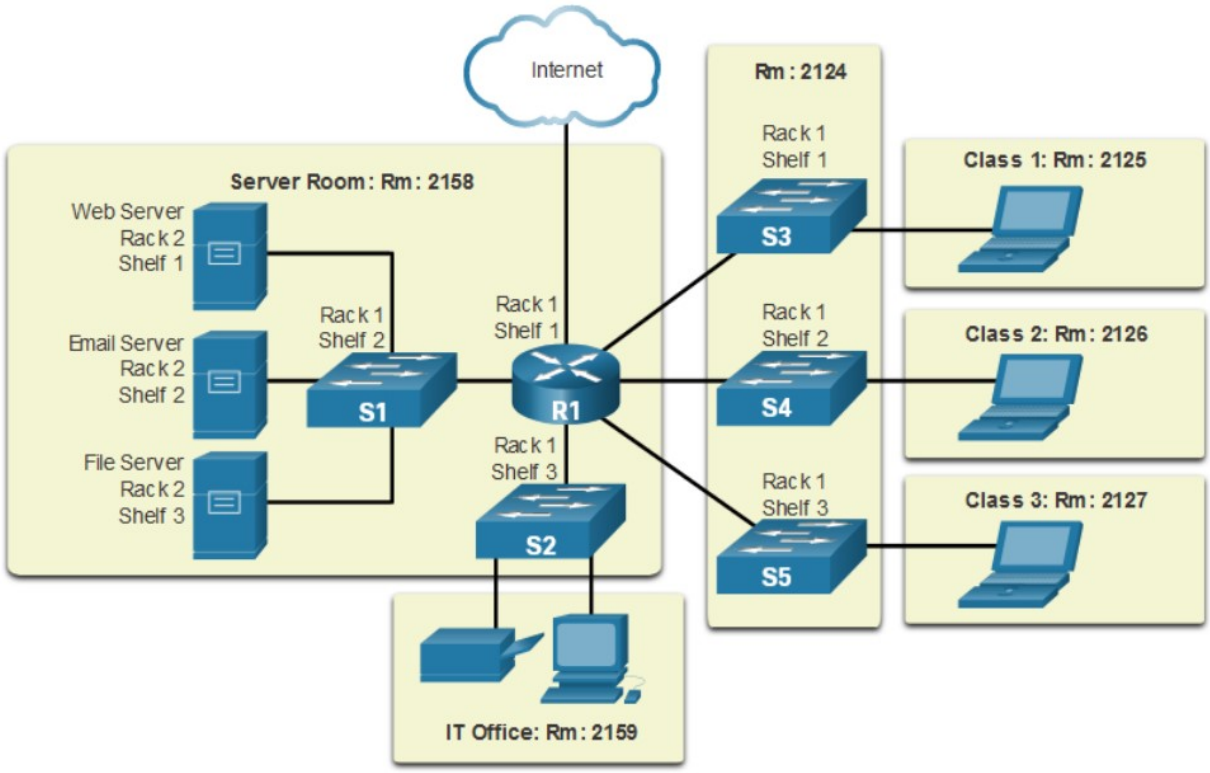

Abbildung 1: Physikalisches Netzwerkdiagramm (©Cisco)

Das logische Netzwerkdiagramm zeigt hingegen über welche ***Ports (interfaces)*** die Komponenten angeschlossen sind, sowie welche ***Netzwerkadressierung*** gegeben wurde. Merkmale sind Netzwerkadressen, IP-Adressen von Endgeräten, Subnetzmasken, je nach Anwendung auch MAC-Adressen. Man spricht auch von einer *physischen Adresse* oder *Geräteadresse*.

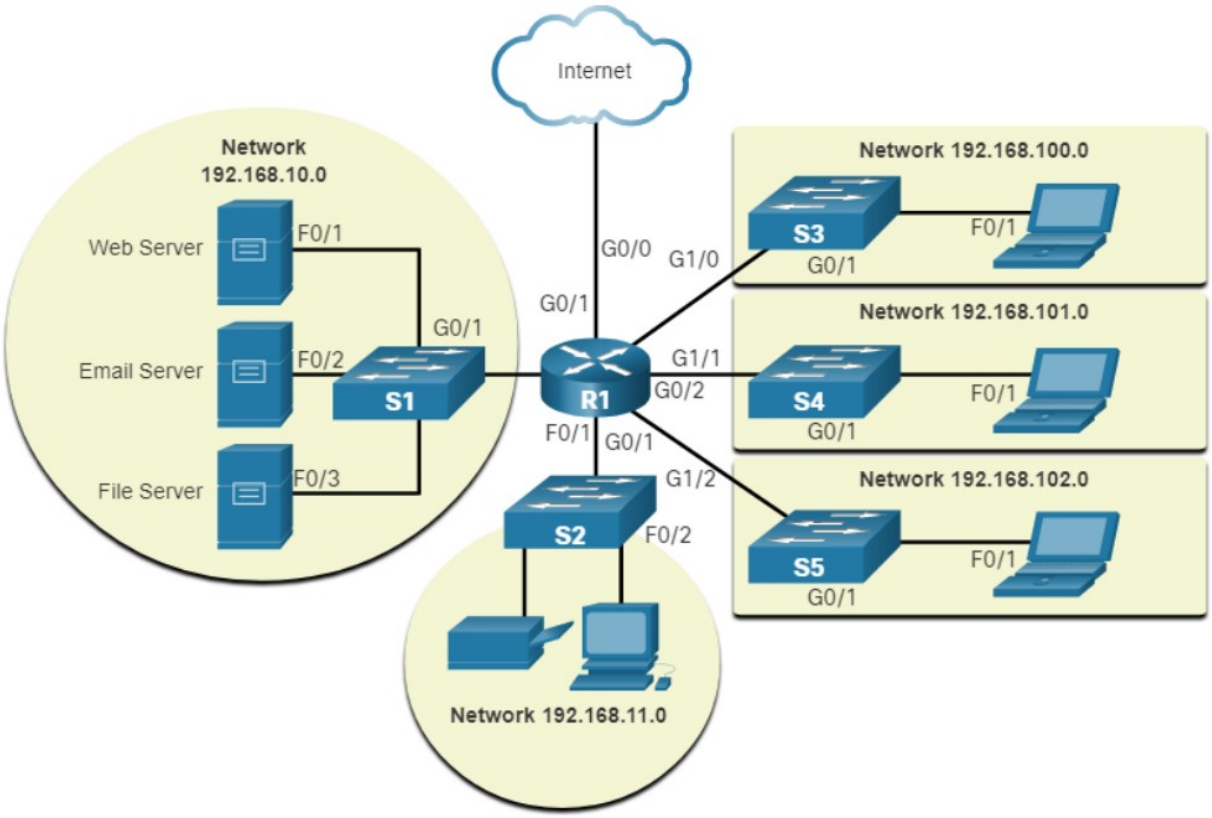

Abbildung 2: Logisches Netzwerkdiagramm (©Cisco)

Wie kann man anhand ihrer Grösse Computernetzwerke klassifizieren?

Es gibt diverse Grössen von Netzwerken. Namentlich sind das:

- LAN - Local Area Network. Lokales Netz, mal abgesehen von Subnetzen, auf die Wohnung, Büro oder Firma beschränkt.
- MAN - Metropolitan Area Network. Meistens ein Verbund von LANs, welche auf "kürzere Distanzen" (bis zu ca. 100 km) durch einen Backbone (Netz mit besonders grosser Übertragungsrate über Glasfaser) vernetzt sind. MANs werden durch Internetdienstanbieter (ISP - Internet Service Provider) betrieben.
- WAN - Wide Area Network. Verbund und Backbone von MANs. Salopp: "das Internet".

Die Aufzählung ist nicht abschliessend, denn es gibt z.B. Body Area Network (z.B. medizinische Geräte), Personal Are Network (z.B. Bluetooth), City Area Network, Global Area Network etc.

Wie unterschieden sich LANs und WANs? Was ist ihre Beziehung?

Ein **LAN** beschränkt sich auf das interne Netzwerk einer Firma oder privat in der Wohnung. Es gibt private IP-Adressen, welche nur im Intranet existieren (Siehe Private/Public IPs, Seite 28). Ein **WAN** ist einfach ausgedrückt das Internet. Die Beziehung zueinander ist so, dass man normalerweise vom LAN auf das WAN zugreifen kann, umgekehrt aber nicht. Weitere Infos über IPs siehe Network Layer, Seite 27.

Was ist das Internet? Wer besitzt das Internet? Was für Organisationen sind in der Entwicklung des Internets beteiligt?

Das Internet ist ein globaler Verbund von Rechnernetzwerken, welches die Nutzung von diversen Diensten wie WWW, Email, FTP u.v.m. bietet. Das Internet gehört im Grunde genommen niemandem. Die Organisation IETF befasst sich jedoch mit der Weiterentwicklung des Internets, um dessen Funktionsweise zu verbessern.[1]

[1] Fun: `https://www.facebook.com/Ballybegpostofficeandgeneralconveniencestore/videos/845703122288697/`

Was ist der Unterschied zwischen einem Intranet und einem Extranet?

Auf das Intranet kann nur von innerhalb des LANs zugegriffen werden. Das Extranet bietet hingegen eine Erweiterung des Intranets, die von einer Gruppe von externen Benutzer verwendet werden darf. Extranets bieten Informationen die z.B. an Kunden oder Partnern zugänglich gemacht werden.

Wie verbinden sich normalerweise Häuser, Wohnungen und HomeOffices mit dem Internet?

Kabelnetz, DSL, Dial-Up Modem, GSM, Satellit.

Wie verbinden sich normalerweise Büros und Unternehmern mit dem Internet?

Dedicated Leased Lines, Metro Ethernet (ethernetbasierte MANs), Business DSL, Satellit.

Was bedeutet Konvergenz im Kontext der Computernetzwerke?

Voneinander getrennte Netze werden zusammengeführt. Bsp.: klassische Telefonie funktioniert zunehmend über VoIP.

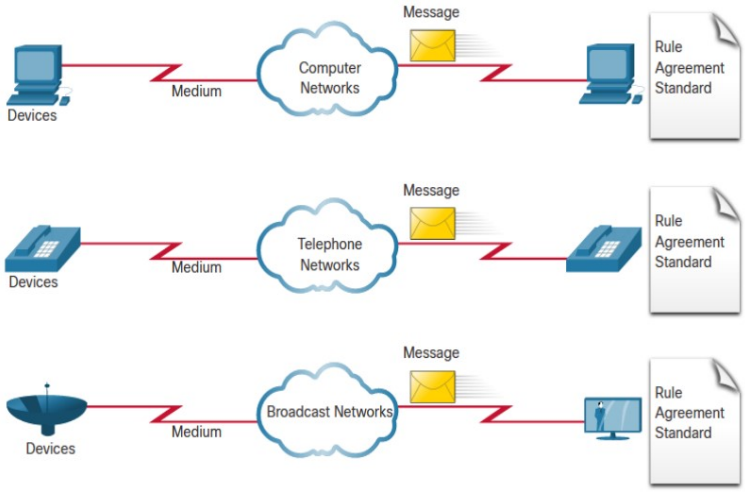

Abbildung 3: Klassisches Netz (©Cisco)

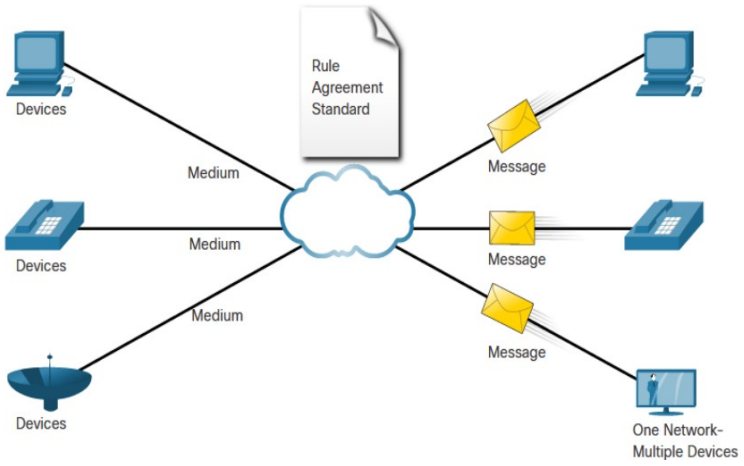

Abbildung 4: Modernes, konvergiertes Netz (©Cisco)

Was bedeutet «fault tolerance» (Fehlertoleranz) im Kontext der Computernetzwerke? Geben Sie ein Beispiel

Beim Ausfall einer wichtigen Netzwerkkomponente wie z.B. Router, wird mit redundantem Aufbau eines Netzwerkes die Verbindung weiterhin gewährleistet.

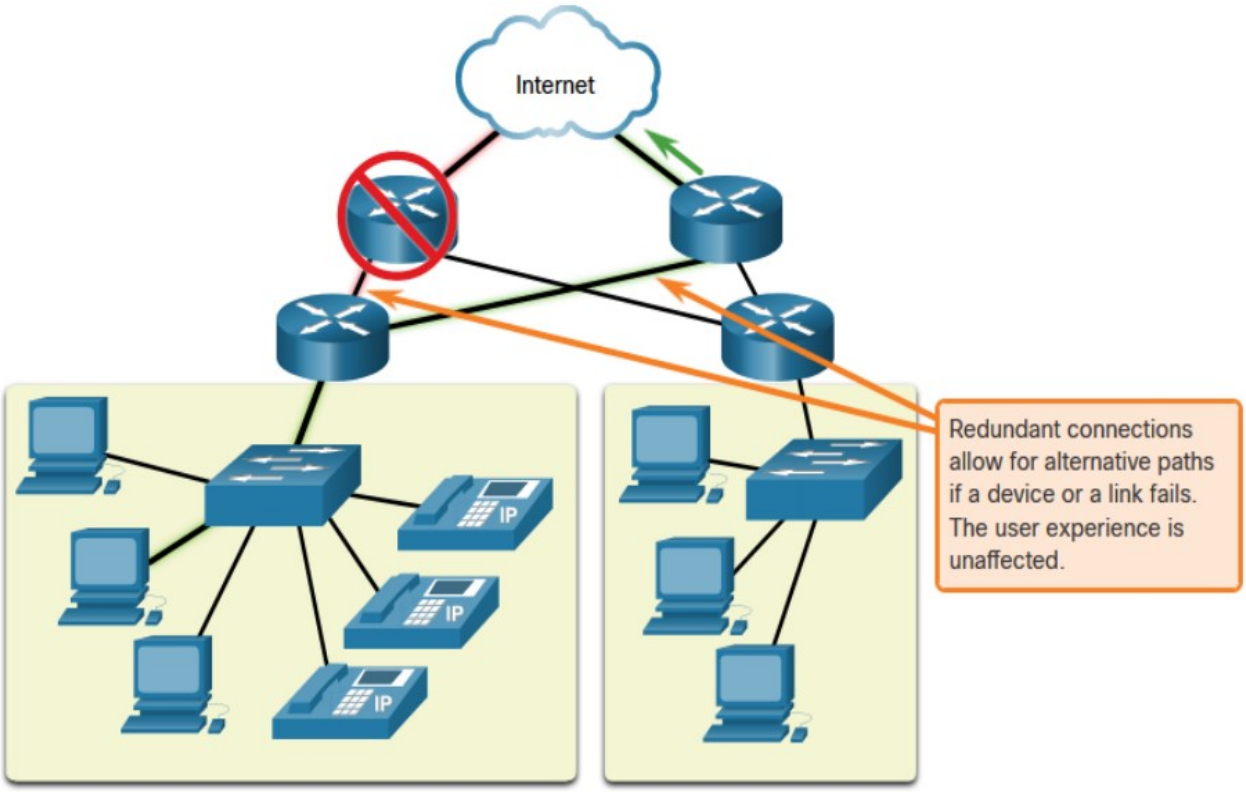

Abbildung 5: Fault tolerance - Fehlertoleranz (©Cisco)

Was bedeutet «scalability» (Skalierbarkeit) im Kontext der Computernetzwerke? Geben Sie ein Beispiel

Die Skalierbarkeit eines Netzwerkes beschreibt die Fähigkeit/Möglichkeit, ein Netzwerk ohne grossen Aufwand zu erweitern.

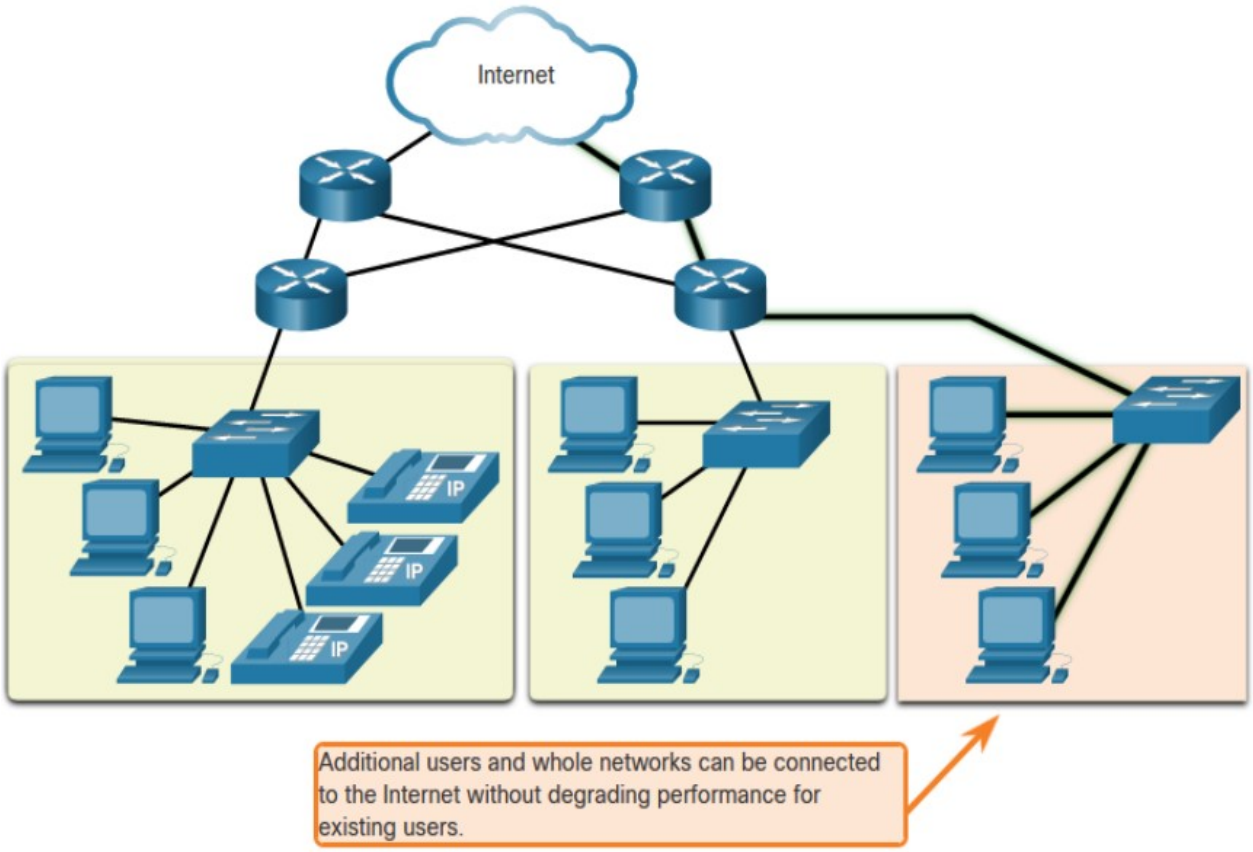

Abbildung 6: scalability - Skalierbarkeit (©Cisco)

Was bedeutet «quality of service (QoS)» im Kontext der Computernetzwerke? Geben Sie ein Beispiel

Das QoS dient zur Priorisierung von Netzwerkdiensten und -paketen. Ein Telefonat über VoIP ist wichtiger als eine Webseite, die vielleicht ein paar Millisekunden länger braucht um angezeigt zu werden.

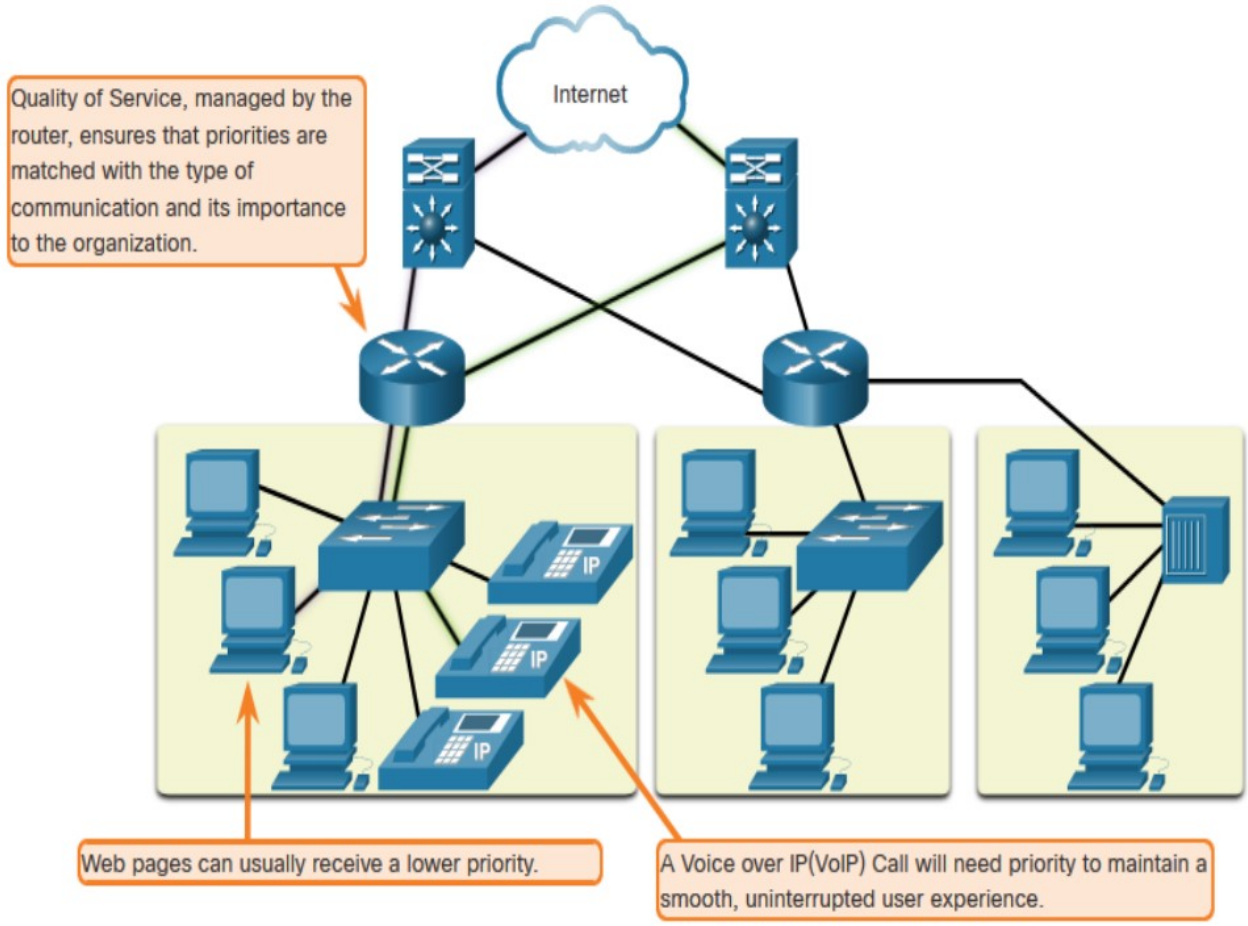

Abbildung 7: Quality of service

Wieso ist Netzwerksicherheit wichtig?

Um Unbefugten nicht versehentlichen oder absichtlichen Zugriff auf das Netzwerk zu gewähren.

Was sind die drei Hauptinformationssicherheitsziele?

Informationssicherheit ist das höchste Gut, der heilige Grahl der Informatik. Die drei Hauptziele sind:

- **Vertraulichkeit** (confidentiality): lediglich autorisierte Benutzer dürfen entsprechende Daten lesen (z.B. eavesdropper) oder ändern. Dies gilt beim Zugriff auf gespeicherte Daten, wie auch während der Übertragung.
- **Integrität** (integrity): Daten dürfen nicht unbemerkt verändert werden (z.B. man in the middle attack) und alle Änderungen müssen nachvollziehbar sein.
- **Verfügbarkeit** (availability): Verhinderung von Systemausfällen und Gewährleistung der Verfügbarkeit der Daten innerhalb eines definierten Zeitraums.

Informationssicherheit wird im Modul ISF - Information Security Fundamentals genauer erarbeitet.

Was ist «BYOD» und was sind seine Auswirkungen für Geschäfte und Unternehmen?

Bring Your Own Device. Für Unternehmen bedeutet dies, dass Komponenten wie Smartphones und Notebooks in das Netzwerk eingebunden werden, welche vielleicht nicht über spezielle Schutzmassnahmen verfügen, als wenn es von der firmeneigenen Informatikabteilung zur Verfügung gestellt werden würde. Umso besser muss das Netzwerk gegen mögliche Bedrohungen, die dieses Philosophie mit sich bringt, geschützt werden.

Was ist «cloud computing»? Was für Cloud Arten gibt es?

Clouds sind verschiedene Dienstleistungen, welche physisch nicht mehr verfügbar sind. Bekanntestes Anwendungsbeispiel ist die File-Cloud. Man hat nicht einen eigenen File-Server, sondern einen externen Anbieter, einen CSP - Could Service Provider, der den Zugang auf die darunterliegende Infrastruktur ermöglicht. Im Grunde gibt es drei Hauptformen von Angeboten:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Wichtig dabei ist, dass es vier verschiedene Arten von Clouds gibt.

- Private
  - Ein Unternehmen hat Zugriff auf eine Cloud-Infrastruktur, welche nicht von anderen Firmen genutzt wird (z.B. Dedicated Server). Sicher was Datenschutz angeht, jedoch Verfügbarkeit könnte bei einem Ausfall vielleicht nicht gewährleistet sein.
- Public
  - Ein Unternehmen teilt sich eine Cloud-Infrastruktur mit anderen Firmen (z.B. Shared Server). Das heisst also, eine Firma bekommt eine definierte Anzahl an Ressourcen zur Verfügung gestellt, hat aber keinen Zugriff auf die gesamte Infrastruktur. Normalerweise sehr hohe Verfügbarkeit, jedoch vom Datenschutz her nicht optimal, da sich Infrastruktur global befindet (Big Brother is watching you), jedoch deswegen auch günstiger im Angebot.
- Hybrid
  - Hybride Cloud-Infrastrukturen sind in private und public Clouds geteilt. Sensitive Daten werden in der privaten cloud verarbeitet. Operationen die von sensitiven Daten keinen Gebrauch machen können günstig in einer public Cloud verarbeitet werden. Je nach bedarf kann die public Cloud skaliert werden.
- Community
  - Die Community Cloud ist eine spezielle Form der Cloud. Spezifische Sektoren wie Gesundheits-, Recht-, Finanzbereich u.a. unterliegen oft regulatorischen Konformitäten. Diese “Sektorsphären” sind als die Communities anzusehen. CSPs haben aufgrund dieser Konformitäten ein gewisses Angebotsstandard für die Sektoren geschaffen. Vom Datenschutz fast wie eine private Cloud, jedoch von der Funktionalität wie eine public cloud, das heisst, andere Firmen aus derselben Branche nutzen die Cloud mit.

Wie bei allem gibt es Vor- und Nachteile bei der Nutzung solcher Angebote.

Was ist die Verbindung zwischen «cloud computing» und Computernetzwerken?

Cloud Computing ist ein Dienstleitungsangebot von Cloud Service Providern. Ein Computernetzwerk ist die darunterliegende Struktur zur Gewährleistung der Datenübertragung.

Teil II
SW 02 - ISO/OSI Modell

3 Lernziele (Leitfragen)

1. Was sind die Schichten des TCP/IP Models? Beschreiben Sie den Zweck jeder Schicht
2. Was sind die Schichten des OSI Models? Beschreiben Sie den Zweck jeder Schicht
3. Was ist die Verbindung zwischen dem TCP/IP Modell und dem OSI Modell?
4. Nehmen Sie eine typische Netzwerkapplikation als Beispiel. Anhand des TCP/IP Models, erläutern Sie wie Nachrichten zwischen den End-Devices ausgetauscht sind.
5. Wieso muss man Zahlensysteme verstehen, wenn man sich mit Computernetzwerken beschäftigt?
6. Wie kann man einfach und schnell zwischen Binär, Hexadezimal und Dezimal umrechnen?

4 Antworten

Was sind die Schichten des TCP/IP Models? Beschreiben Sie den Zweck jeder Schicht

Das TCP/IP Modell besteht aus vier Schichten.
Eselsbrücke: Alle Tiere In Noah's Arche

Layer	Zusammenfassung	Protokolle
Application	- Am nächsten zum User - Datenaustausch zwischen Programmen - Allgemeine Funktionen zur Kommunikation im Internet	Web (HTTP, HTTPS) Email (POP, IMAP, SMTP) Namensauflösung (DNS) Datenaustausch (FTP)
Transport	- Segmentierung und Zusammenfügen von Daten - Management von Verlässlichkeitsanforderungen einer Konversation - Multiplexing und Konversationen verfolgen	Verbindungsorierntiert (TCP) Verbindungslos (UDP)
Internet	- Datenaustausch über Sub-Netzwerke - Adressierung von Endgeräten - Routing - verbindungslos, best effort und medienunabhängig	Datenaustausch (IPv4, IPv6) Routing (OSPF, BGP) Steuerung (ICMPv4, ICMPv6)
Network Access	- Adressierung von Sub-Netzwerken - Media access control (MAC) - Abstraktion der physischen Medien der oberen Schichten - Bits auf die Medien setzen	Address Resolution (ARP) Data Link (Ethernet, WLAN)

Tabelle 1: TCP/IP Modell

Was sind die Schichten des OSI Models? Beschreiben Sie den Zweck jeder Schicht

Das OSI Modell besteht aus 7 Schichten.
Eselsbrücke: Alle Priester Saufen Tequilla Nach Der Predigt

Layer	Zusammenfassung	Protokolle
↓Anwendungsorientiert↓		
Layer VII Anwendungen (Application)	Die Anwendungsschicht interagiert direkt mit der Software (Anwendung), die eine Netzwerkübertragung anfordert. Sie ermittelt, ob die Möglichkeit einer Verbindung besteht, und identifiziert und sucht Ressourcen.	DHCP DNS FTP HTTPS LDAP SMTP ...
Layer VI Darstellung (Presentation)	Die Darstellungsschicht sorgt dafür, dass die Daten so bearbeitet werden, dass sie optimal ausgetauscht und verarbeitet werden können. Hierfür gibt es etliche standardisierte Kodierungs-, Konvertierungs- und Kompressionsverfahren, zum Beispiel für Verschlüsselungsroutinen, Zeichendarstellungen, Video- und Audioübertragungen.	
Layer V Kommunikations-/ Sitzungsschicht (Session)	Die Kommunikationsschicht ist hauptsächlich eine „Serviceschicht“ für die bidirektionale Kommunikation von Anwendungen in verschiedenen Endgeräten. Sitzungen und Datenströme werden angefordert, aufgebaut, kontrolliert und koordiniert. Meist bedienen sich die Services der Schicht 5 dabei der Dienstangebote der Schicht 4.	
Layer IV Transportschicht (Transport)	In der Transportschicht sind Sicherungsmechanismen für einen zuverlässigen Datentransport beschrieben. Die Schicht 4 regelt das Datenmultiplexing und die Flusskontrolle, das heisst, mehrere Anwendungen höherer Protokolle können gleichzeitig Daten über eine Verbingdung tranportieren. In der Tranportschicht sind verbindugslose und verbindungsorientierte Dienste implementiret. Verbindungsorientierte Diense können einen sehr sicheren Datenaustausch durchführen. Der Sender und der Empfänger kontrollieren ihre Möglickeiten der Kommunikation (Aufbau einer virtuellen Verbindung), die Daten werden erst nach dieser Prfung versandt. Eine weitgehende Fehlerkontrolle prüft die Daten und fordert entweder verlorene oder korrumpierte Daten zur erneuten Übersendung an. Am Ende der Kommunikation wird die Verbindung gezielt und kontrolliert wieder abgebaut. Im Layer 4 wird nach definierten Anwendungen unterschieden. Hier beginnt die Kommunikation zwischen dem Netzwerk un der Anwendung.	TCP UDP ...
↓Transportorientiert↓		
Layer III Vermittlungsschicht (Network)	In der Schicht 3 des OSI-Modells wird die logische Adressierung (segmentübergreifend bis weltweit) der Geräte definiert. Die Routing-Protokolle dieser Schicht ermöglichen die Wegfindung in grossen (bis weltweiten) Netzwerken und redundante Wege ohne Konflikte. Routing-Protokolle sorgen ebenfalls dafür, dass die Ressourcen in vermaschten Netzen mit vielen redundanten Wegen bei dem Ausfall einer Verbindung weiterhin benutzt werden können.	ICMP IP IPsec IPX ...
Layer II Sicherungsschicht (Data Link)	Die Sicherungsschicht ist für eine zuverlässige Übertragung der Daten zuständig. Sie regelt die Flusssteuerung, regelt den Zugriff, verhindert eine Überlastung des Empfängers und ist für die physikalische Adressierung innerhalb eines Netzsegmentes auf dieser Schicht verantwortlich. Hier ist die erste Fehlererkennung implementiert. Die Topologie eines Netzwerkes ist stark von dieser Schicht abhängig, sie definiert die Art und Weise, wie die Rechner und Netzwerkgeräte miteinander verbunden sind.	IEEE 802.3 (Ethernet) IEEE 802.11 (WLAN) MAC ...
Layer I Physikalische Schicht (Physical)	Hier sind die physikalischen Parameter definiert. Dazu gehören Kapeltypen, die Anschlüsse, die Streckenlängen, die elektrischen Eckdaten wie Spannungen, Frequenzen etc. Getrennt wird hier in drei Bereiche: • Der Nahbereich (LAN) • mittlere Entfernungen (MAN) • und Fernverbindungen (WAN).	1000BASE-T 10BASE-T Token Ring ...

Tabelle 2: OSI Modell[1]

Was ist die Verbindung zwischen dem TCP/IP Modell und dem OSI Modell?

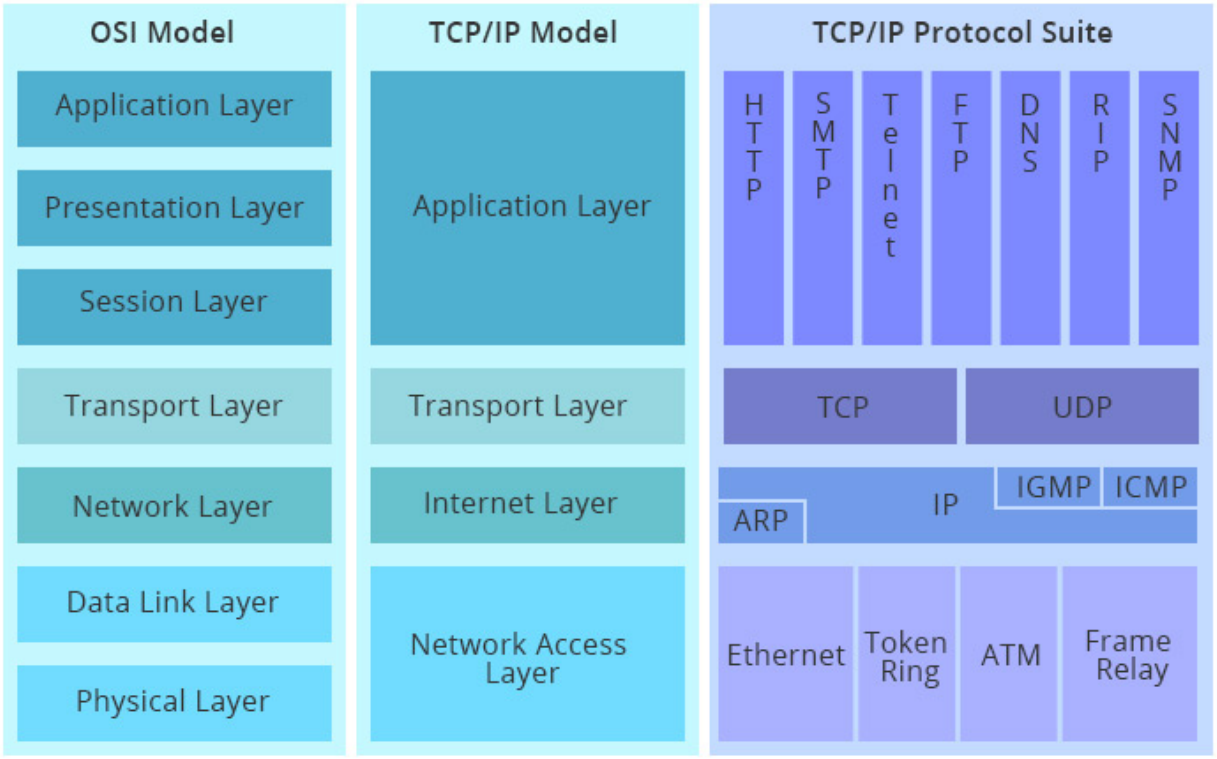

Abbildung 8: Vergleich OSI mit TCP/IP Modell[2]

Nehmen Sie eine typische Netzwerkapplikation als Beispiel. Anhand des TCP/IP Models, erläutern Sie wie Nachrichten zwischen den End-Devices ausgetauscht sind.

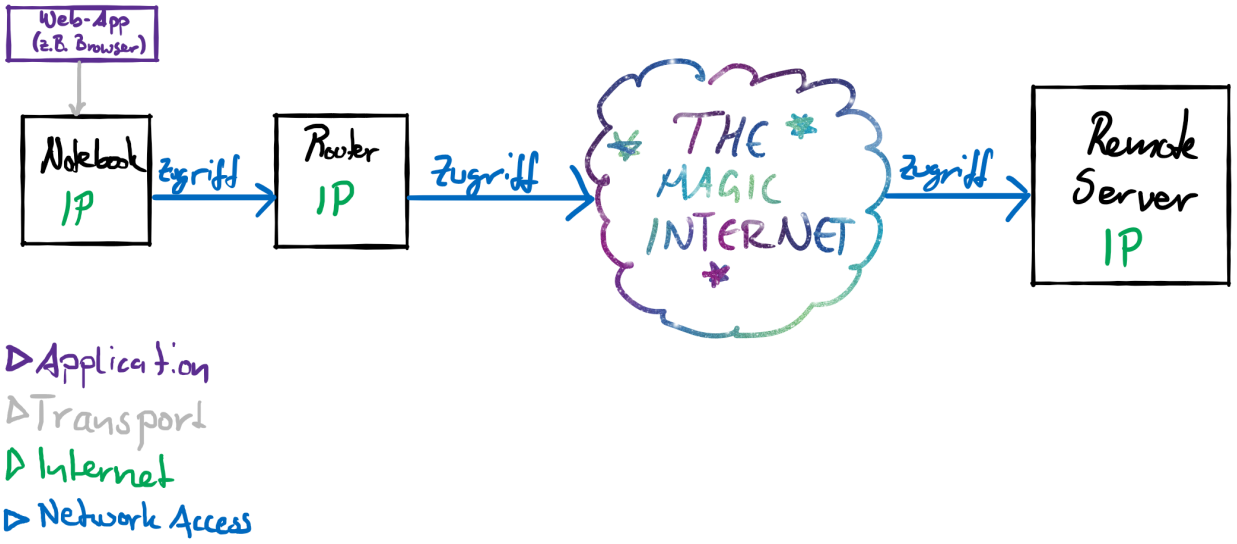

Abbildung 9: Weg eines Datenpaketes

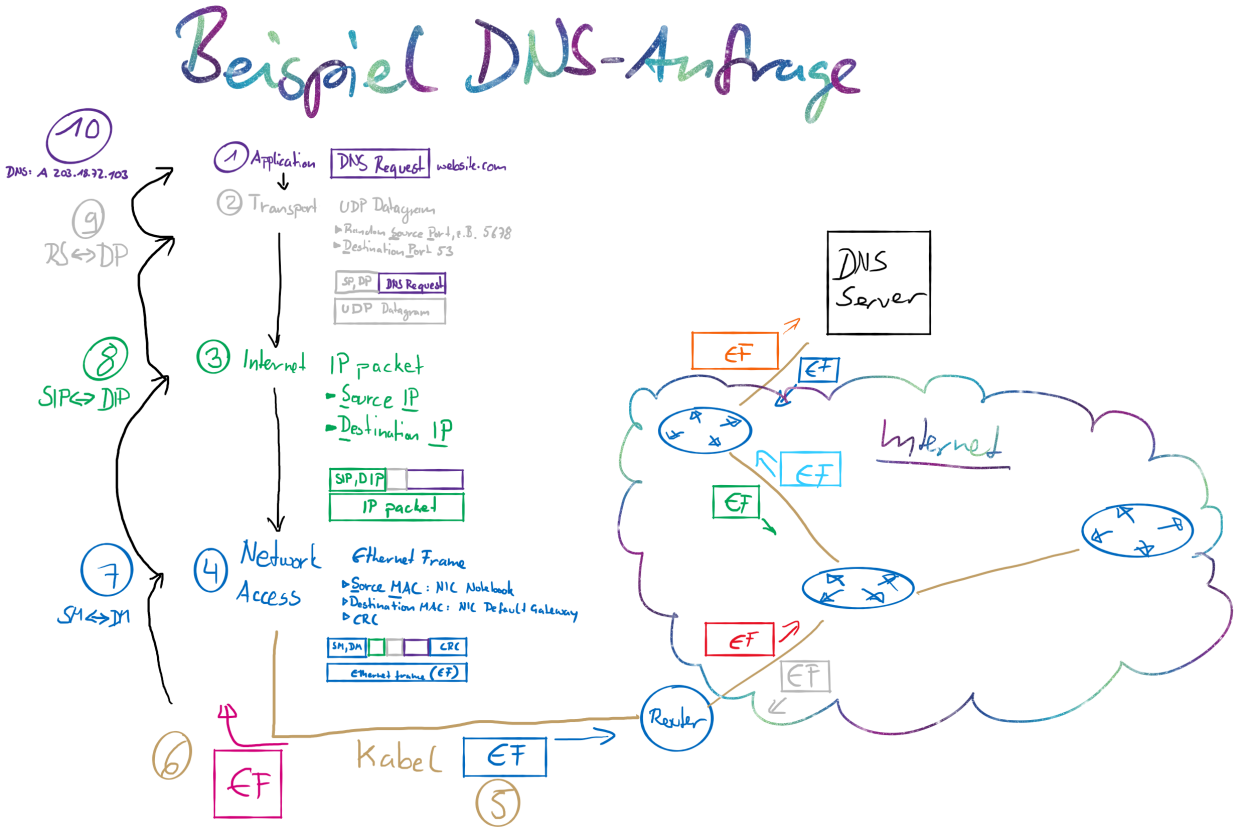

Abbildung 10: Einzelschritte der Kapselung, Beispiel anhand DNS request

Wieso muss man Zahlensysteme verstehen, wenn man sich mit Computernetzwerken beschäftigt?

Das Rechnen mit anderen Zahlensystemen wie Binär ist im Umgang mit Computernetzwerken insofern wichtig, weil gewisse Rechnungen (z.B. Subnetz) einfacher sind. Auch sind gewisse Zahlen in anderen Formaten dargestellt wie MAC-Adressen oder IPv6, welche in Hexadezimal dargestellt werden, weil diese kompakter sind als Dezimal.

Wie kann man einfach und schnell zwischen Binär, Hexadezimal und Dezimal umrechnen?

Über den Rechner vom Betriebssystem:

Abbildung 11: Windows Taschenrechner

Oder ganz easy von Hand ausrechnen.

Binär Beispiel 125_{10} zu Binär. Den Rest zusammenfügen:

$$
\begin{array}{rcll}
125 & \div & 2 = 62 & \text{R } 1 \text{ (ganz rechts)} \\
62 & \div & 2 = 31 & \text{R } 0 \\
31 & \div & 2 = 15 & \text{R } 1 \\
15 & \div & 2 = 7 & \text{R } 1 \\
7 & \div & 2 = 3 & \text{R } 1 \\
3 & \div & 2 = 1 & \text{R } 1 \\
1 & \div & 2 = 0 & \text{R } 1 \text{ (ganz links)}
\end{array}
$$

Dann ist das Ergebnis also: 0b111 1101

Um die Binärzahl in Dezimal umzuwandeln, liest man von rechts die Einsen und fängt mit der Potenz 0 zur Basis 2 an. Unser Zahlenbeispiel als Byte:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
0	1	1	1	1	1	0	1

Daraus erhält man, dort wo eine 1 steht:
$2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^0 = 64 + 32 + 16 + 8 + 4 + 1 = 125.$

Hexadezimal Hexadezimal ist da schon etwas komplizierter, aber machbar. Hier rechnet man auch mit Potenzen zur Basis 16. Dazu muss man vorgängig aber schon das 16^x unterhalb der Zahl kennen.
$16^2 = 256$ ist also zu hoch für unsere 125. Bleibt also die nächst tiefere Potenz $16^1 = 16$.
Wir teilen also mit 16:

125	÷	16	(16^1)	= 7 (ganz links)	R 13 (mit nächst tiefere Potenz teilen)
13	÷	1	(16^0)	= 13	

Also hat man jetzt $7 \times 16^1 + 13 \times 16^0$. Das Hexadezimalsystem geht ja aber von 0-F, somit ist die 13 ein D (. . . , 9, 10=A, 11=B, 12=C, 13=D, 14=E, 15=F). Das Ergebnis ist als 0x7D. Auch easy.

Umgekehrt von Hexadezimal auf Dezimal umzurechnen, folgt man dem nun bekannten Potenz-Prinzip.
$7 \times 16^1 + 13 \times 16^0 = 125_{10}$

Hexadezimal und Binär ist Bubieinfach. Dazu nimmt man Binär halbe Bytes (Nibble) und stellt die Zahlen gegenüber.

2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
0	1	1	1	1	1	0	1
7				13 = D			

Was ist mit grossen Zahlen? Dazu brauchen wir einen Taschenrechner mit der Log-Funktion. Nehmen wir als Beispiel $1'106'132_{10}$. Um die Potenz x von 16^x herauszufinden, logarithmieren wir diese Zahl mit dem Taschenrechner: $\frac{\log 1106132}{\log 16} = 5.00000103189442\ldots$
Wir wissen nun, das es sich beim Exponenten um die Potenz 5 handelt. Teilen die Zahl mit 16^5 und erhalten $1.0548\ldots$ Wir subtrahieren die 1 vom Ergebnis und die Nachkommastellen×Divisor (hier 16^5) ergeben den Rest von 57556. Den Rest wieder logarithmieren für nächste Potenz u.s.w. Wir rechnen nun (Zwischenschritt für Rest und Potenz nicht dabei):

1106132	÷	1048576	(16^5)	= 1 (ganz links)	R 57556 (mit nächst tiefere Potenz teilen)
57556	÷	4096	(16^3)	= 14	R 212
212	÷	16	(16^1)	= 13	R 4
4	÷	1	(16^0)	= 4	R 0

Nun können wir überall dort, wo ein Exponent steht, die Zahl Schreiben. Überall dort wo kein Exponent ist (hier: 4, 2), wird 0 geschrieben:

2^3	2^2	2^1	2^0		2^3	2^2	2^1	2^0		2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
0	0	0	1	0000	1	1	1	0	0000	1	1	0	1	0	1	0	0
1				0	14 = E				0	13 = D				4			

Das Ergebnis ist also 0x10E0D4, Binär 0b0001 0000 1110 0000 1101 0100.

Hexadezimal zu Dezimal wie vorhin bereits beschrieben: $1 \times 16^5 + 14 \times 16^3 + 13 \times 16^1 + 4 \times 16^0 = 1106132_{10}$

Teil III
SW 03 - Präsentationen zu physikalischer Schicht

5 Lernziele (Leitfragen)

- Die physikalische Schicht und Zugriffsverfahren (T1)
  1. Was ist der Zweck der physikalischen Schicht?
  2. Was sind die Hauptmerkmale der physikalischen Schicht?
  3. Was ist der Unterschied zwischen «Simplex», «half-duplex» and «full duplex»?
  4. Welches sind die am häufigsten verwendeten Zugriffsverfahren?
  5. Was bedeutet „Late Collision“?
  6. Was muss man noch unbedingt über die physikalische Schicht und Zugriffsverfahren wissen?

- Topologien und “Bandwidth” (T2)
  1. Was für Topologien findet man in Computernetzwerken?
  2. Wo ist der Unterschied zwischen «Bandwidth», «Throughput» und «Goodput»? Wie kann man diese Konzepte visualisieren und verstehen?
  3. Was ist «Latency» und «Jitter»? Wie kann man diese Konzepte visualisieren und verstehen?
  4. Was muss man noch unbedingt über Topologien und “Bandwidth” wissen?

- Kupferkabel (T3)
  1. Was sind die wichtigsten Merkmale von Kupferkabeln?
  2. Was für Kupferkabelarten werden heutzutage in Computernetzwerken am häufigsten verwendet?
     (a) Wie sind sie aufgebaut?
     (b) Wie sehen die Stecker aus?
  3. Worauf muss bei der Handhabung und Verlegung der Kupferkabel besonders geachtet werden und warum?
  4. Woraus resultieren die Längenbeschränkungen der Kupferverkabelung?
  5. Was muss man noch unbedingt über Kupferkabel wissen?

- Glasfaserkabel (T4)
  1. Was sind die wichtigsten Merkmale von Glasfaserkabeln?
     (a) Wie sind sie aufgebaut?
     (b) Wie sehen die Stecker aus?
  2. Worauf muss bei der Handhabung und Verlegung von Glasfaserkabeln besonders geachtet werden und warum?
  3. Woraus resultieren die Längenbeschränkungen der Glasfaserkabelverkabelung?
  4. Wo ist der Unterschied zwischen Multi- und Singlemode (Monomode)- Glasfasern?
  5. Was sind die Vor- und Nachteile von Glasfaserkabel (im Vergleich zu Kupferkabeln)?
  6. Was muss man noch unbedingt über Glasfaserkabel wissen?

- Wireless Access (T5)
  1. Was sind die wichtigsten Merkmale von «Wireless Media»?
  2. Welche Wireless Access Geräte arbeiten auf Layer I?
  3. Was für Wireless Standards gibt’s in Computernetzwerken?
     (a) Was sind ihre Hauptmerkmale und Anwendungsbereiche?
  4. Was sind die Vor- und Nachteile von «Wireless Access» Methoden im Vergleich mit «Wired Access»?

6 Antworten T1

Was ist der Zweck der physikalischen Schicht?

//TODO

Was sind die Hauptmerkmale der physikalischen Schicht?

//TODO

Was ist der Unterschied zwischen «Simplex», «half-duplex» and «full duplex»?

//TODO

Welches sind die am häufigsten verwendeten Zugriffsverfahren?

//TODO

Was bedeutet „Late Collision“?

//TODO

Was muss man noch unbedingt über die physikalische Schicht und Zugriffsverfahren wissen?

//TODO

7 Antworten T2

Was für Topologien findet man in Computernetzwerken?

//TODO

Wo ist der Unterschied zwischen «Bandwidth», «Throughput» und «Goodput»? Wie kann man diese Konzepte visualisieren und verstehen?

//TODO

Was ist «Latency» und «Jitter»? Wie kann man diese Konzepte visualisieren und verstehen?

//TODO

Was muss man noch unbedingt über Topologien und “Bandwidth” wissen?

//TODO

8 Antworten T3

Was sind die wichtigsten Merkmale von Kupferkabeln?

//TODO

Was für Kupferkabelarten werden heutzutage in Computernetzwerken am häufigsten verwendet?

//TODO

Wie sind sie aufgebaut?

//TODO

Wie sehen die Stecker aus?

//TODO

Worauf muss bei der Handhabung und Verlegung der Kupferkabel besonders geachtet werden und warum?

//TODO

Woraus resultieren die Längenbeschränkungen der Kupferverkabelung?

//TODO

Was muss man noch unbedingt über Kupferkabel wissen?

//TODO

9 Antworten T4

Was sind die wichtigsten Merkmale von Glasfaserkabeln?

//TODO

Wie sind sie aufgebaut?

//TODO

Wie sehen die Stecker aus?

//TODO

Worauf muss bei der Handhabung und Verlegung von Glasfaserkabeln besonders geachtet werden und warum?

//TODO

Woraus resultieren die Längenbeschränkungen der Glasfaserkabelverkabelung?

//TODO

Wo ist der Unterschied zwischen Multi- und Singlemode (Monomode)- Glasfasern?

//TODO

Was sind die Vor- und Nachteile von Glasfaserkabel (im Vergleich zu Kupferkabeln)?

//TODO

Was muss man noch unbedingt über Glasfaserkabel wissen?

//TODO

10 Antworten T5

Was sind die wichtigsten Merkmale von «Wireless Media»?

//TODO

Welche Wireless Access Geräte arbeiten auf Layer I?

//TODO

Was für Wireless Standards gibt's in Computernetzwerken?

//TODO

Was sind ihre Hauptmerkmale und Anwendungsbereiche?

//TODO

Was sind die Vor- und Nachteile von «Wireless Access» Methoden im Vergleich mit «Wired Access»?

//TODO

Teil IV
SW 04 - Data Link Layer - Sicherungsschicht

11 Lernziele (Leitfragen)

- Was ist der Unterschied zwischen CSMA/CD und CSMA/CA? Wo werden sie verwendet?
- Was ist der Zweck der Sicherungsschicht?
- Wie ist die Sicherungsschicht aufgeteilt? Was ist die Hauptaufgabe der LLC und MAC Schichten?
- Welches sind die am häufigsten verwendeten Zugriffsverfahren?
- Was für Felder findet man in der Sicherungsschicht Frame?
- Was sind die wichtigsten Merkmale von MAC Adressen?
- Was machen Endgeräte, wenn ihre NIC ein Frame im Medium erkennen?
- Wie werden Sicherungsschicht Frames in einem Switch bearbeitet?
- Wie funktioniert der «Learn-and-forward» Prozess?
- Was ist der Unterschied zwischen «Unicast» und «Broadcast» Frames?
- Was ist der Zweck ARPs?
- Wie funktioniert ARP?

12 Antworten

Was ist der Unterschied zwischen CSMA/CD und CSMA/CA? Wo werden sie verwendet?

//TODO Sollte für die Logik zu SW03 T1 verschoben werden.

CSMA: Carrier Sense Multiple Access
- Sender hört den Datenverkehr auf der Leitung ab (= carrier sense)
- Sender wartet, bis der Kanal frei ist
- sobald der Kanal frei ist, darf gesendet werden
- falls mehrere Sender (fast) gleichzeitig anfangen zu senden:
  Kollision → Wiederholung nach zufälliger Zeitspanne

CSMA/CA (CA = Collision Avoidance)
- Kollisionsvermeidung durch zufällige Wartezeit nach Erkennung eines freien Kanals
- z.B. WLAN 802.11-DCF (Distributed Coordination Function)

CSMA/CD (Collision Detection)
- sobald eine Kollision erkannt wird, wird die Übertragung abgebrochen
- z.B. Ethernet

CSMA/CD	CSMA/CA
• Greift nach der Kollision	• Greift vor der Kollision
• Genutzt in kabelgebundenen Netzwerken	• Genutzt in kabellosen Netzwerken
• Reduziert die ‘’recovery time” nach einer Kollision	• Minimiert Kollisionsgefahr
• Bei Konflikt wird erneut gesendet	• Sendet zuerst die Info, dass etwas übermittelt wird
• Effektiver als das einfache CSMA	• ähnlich effizient wie CSMA

Was ist der Zweck der Sicherungsschicht?

- Kommunikation zwischen Netzwerkkarten der Endgeräten
- ermöglicht höheren Protokollen den Zugriff auf die Physikalische Schicht 1
- Kapselt Pakete (IPv4 und IPv6) in das Layer 2 Frame
- Fehlererkennung und Abweisen von korrumpierten Frames

Siehe auch Schichten des OSI Modells (Seite 11).

Wie ist die Sicherungsschicht aufgeteilt? Was ist die Hauptaufgabe der LLC und MAC Schichten?

- Logical Link Control (LLC) kommuniziert zwischen Netzwerksoftware der oberen Schichten und der MAC-Subschicht.
- Media Access Control (MAC) ist für die Datenkapselung und Verwaltung des Zugriffs auf das Übertragungsmedium verantwortlich. Siehe Frage oben Unterschied CSMA/CD und CSMA/CA, Seite 21.

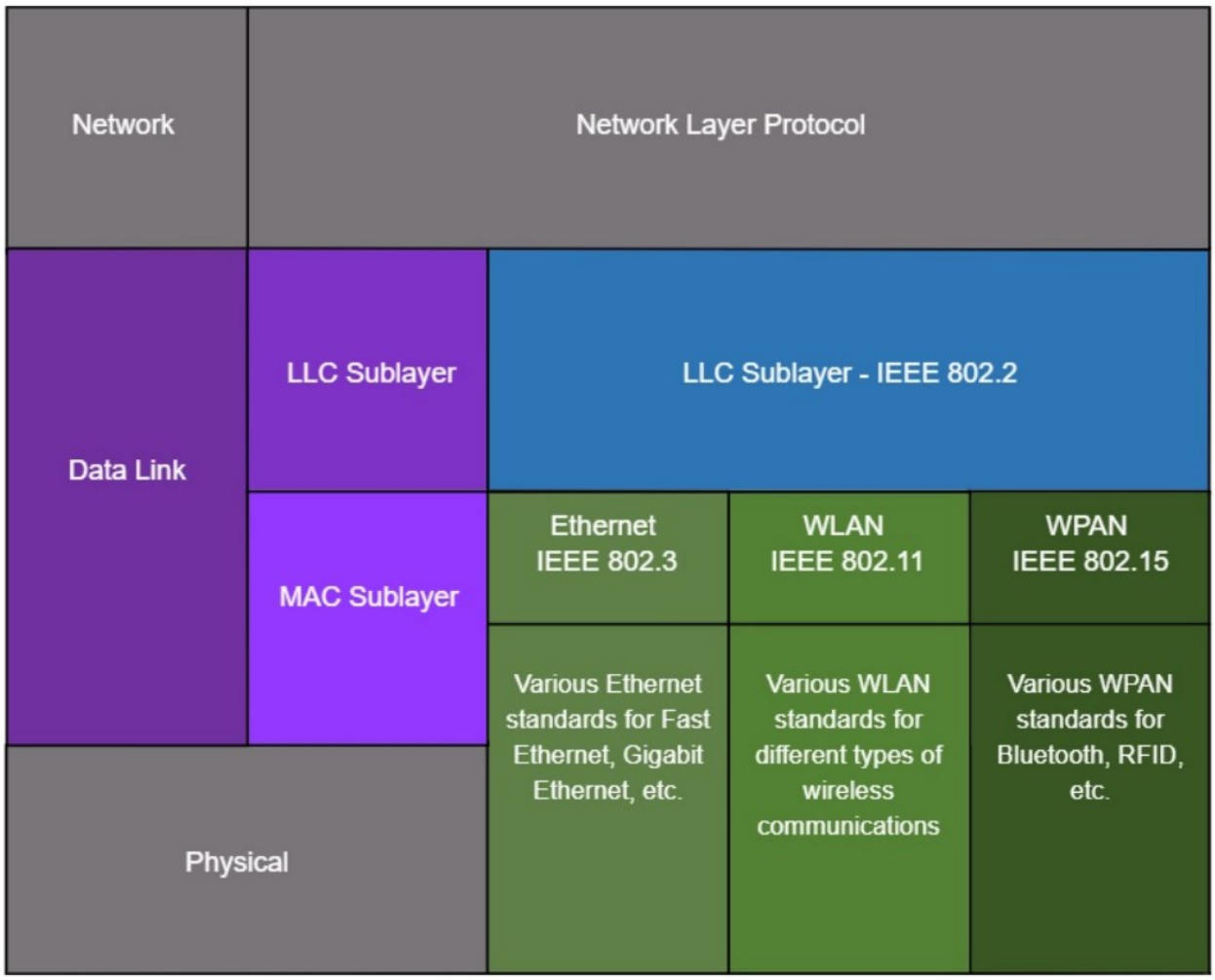

Abbildung 12: Subschichten der Sicherungsschicht / des Data Link Layers (©Cisco)

Welches sind die am häufigsten verwendeten Zugriffsverfahren?

Heutzutage wird vor allem das **CSMA/CD** im Ethernet und **CSMA/CA** im WLAN verwendet. Altertümliche Zugriffsverfahren waren zwei Varianten von **Token Passing**.

Beim **Token Ring** wird das Netzwerk in Form eines Ringes verlegt. Ein Rechner im Ring ist der Token Master. Er verwaltet und kontrolliert ein Bitmuster, das Token. Dieses wird von Gerät zu Gerät weitergereicht. Ist das Token „leer“, darf es der momentane Besitzer entnehmen. Er sendet nun Daten zum Empfänger. Der Empfänger quittiert dem Sender den Empfang der Daten, und der Sender reicht daraufhin das Token wieder weiter. Geht dsa Token verloren, wird es vom Master neu generiert.

Ein **Token Bus** ist im Prinzip dasselbe Verfahren wie Token Ring, nur dass hier nicht im Ring gearbeitet wird, sondern wieder auf Thin-Wire (Koaxial) oder der universellen Gebäudeverkabelung (UGV). Hierbei wird das Token auf dem Bus weitergereicht. Erreicht es das Ende des Busses, wird es wieder zum Anfang zurückgereicht. Damit wird virtuell die Ringstruktur im Hintergrund wiederhergestellt[1].

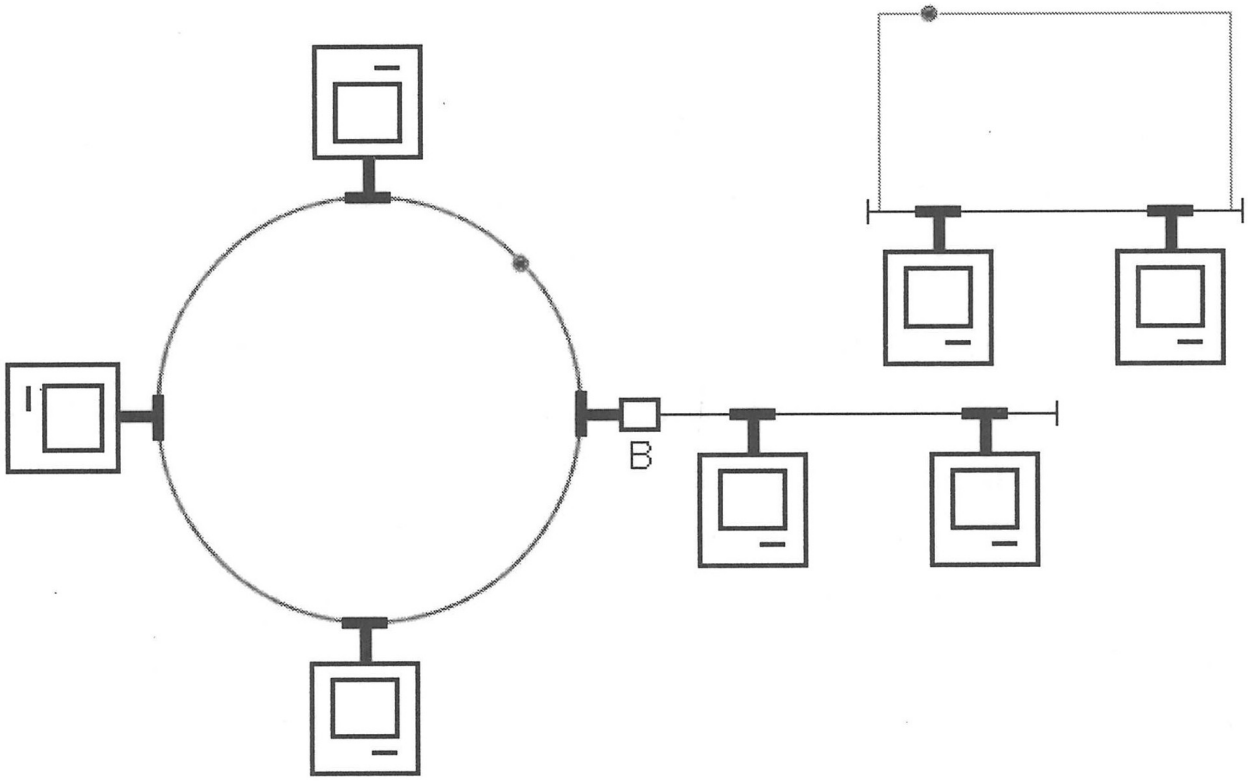

Abbildung 13: Links: Token Ring. Rechts oben kleines Bild: Token wird auf einem Bus weitergereicht und am Ende wird es zum Anfang zurückgereicht und wieder gesendet.[1]

Was für Felder findet man in der Sicherungsschicht Frame?

Es gibt einen **Header**, **Data** und einen **Trailer**. Header und Trailer sind einzelne Felder unterteilt:

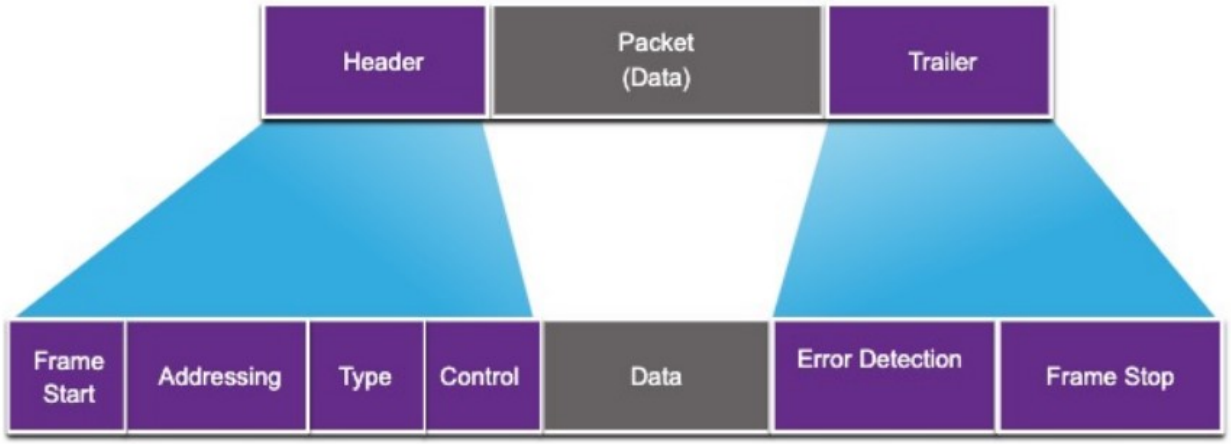

Abbildung 14: Aufbau eines Data Link Frames (©Cisco)

Feld	Beschreibung
Frame Start / Stop	Identifiziert den Anfang und das Ende des Frames
Addressing	Zeigt Source und Destination Knoten (nodes) an
Type	Identifiziert gekapseltes Protokoll von Layer 3
Control	Identifiziert Dienste für die Flusskontrolle
Data	Enthält die „Zuladung“ (payload), die zu übermittelnden Daten
Error Detection	Wird verwendet um Übermittlungsfehler zu entdecken

Das „Addressing“-Feld besteht aus zwei Einträgen, nämlich die MAC-Adressen der Netzwerkkarten

(Siehe Glossar: NIC) vom Ursprung und vom Ziel (Source, Destination). Diese wird an jedem Knoten (node) geändert.

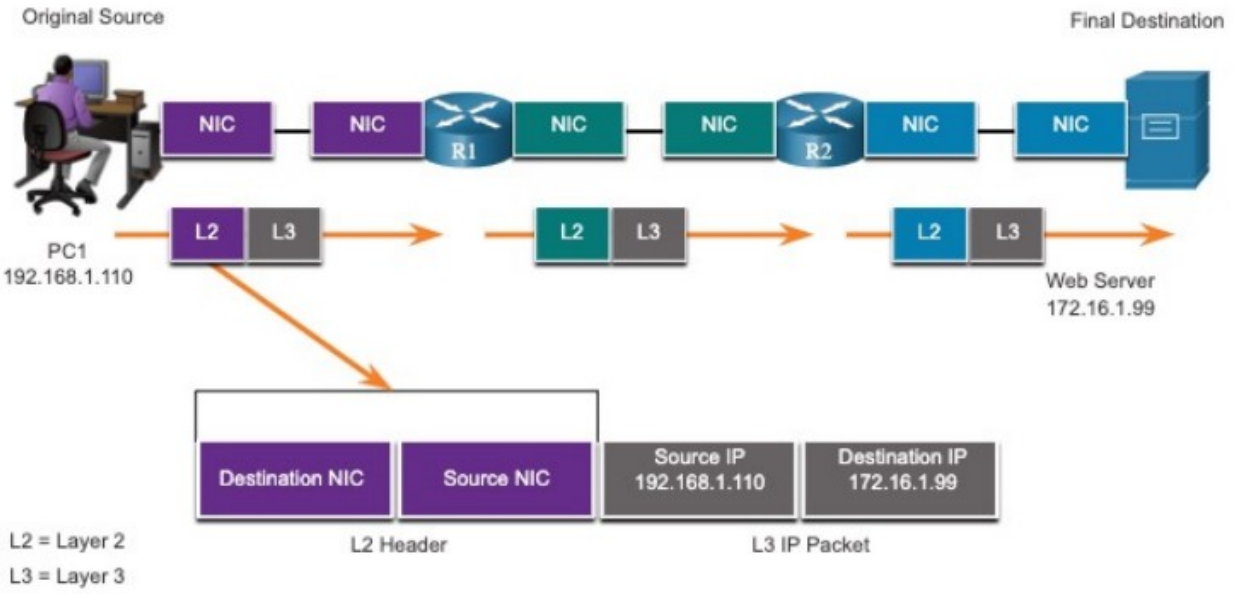

Abbildung 15: MAC-Adressen werden an jedem Knotenpunkt geändert. (©Cisco)

Was sind die wichtigsten Merkmale von MAC Adressen?

- 48 bits = 12 hex-Ziffern = 6 bytes
- einzigartig
- Erste Hälfte von Hersteller, zweite Hälfte zufällig

Beispiel Darstellung einer MAC-Adresse: 3D-8F-45-27-3C-1A oder 3D:8F:45:27:3C:1A

Was machen Endgeräte, wenn ihre NIC ein Frame im Medium erkennen?

1. Untersucht die Ziel MAC-Adresse
2. Stimmt MAC-Adresse mit der eigenen überein (oder Broadcast/Multicast)?
   - Keine Übereinstimmung: **ignoriere** (ignore) den Frame
   - Übereinstimmung: **verarbeite** (process) und übergebe Frame den höheren Schichten

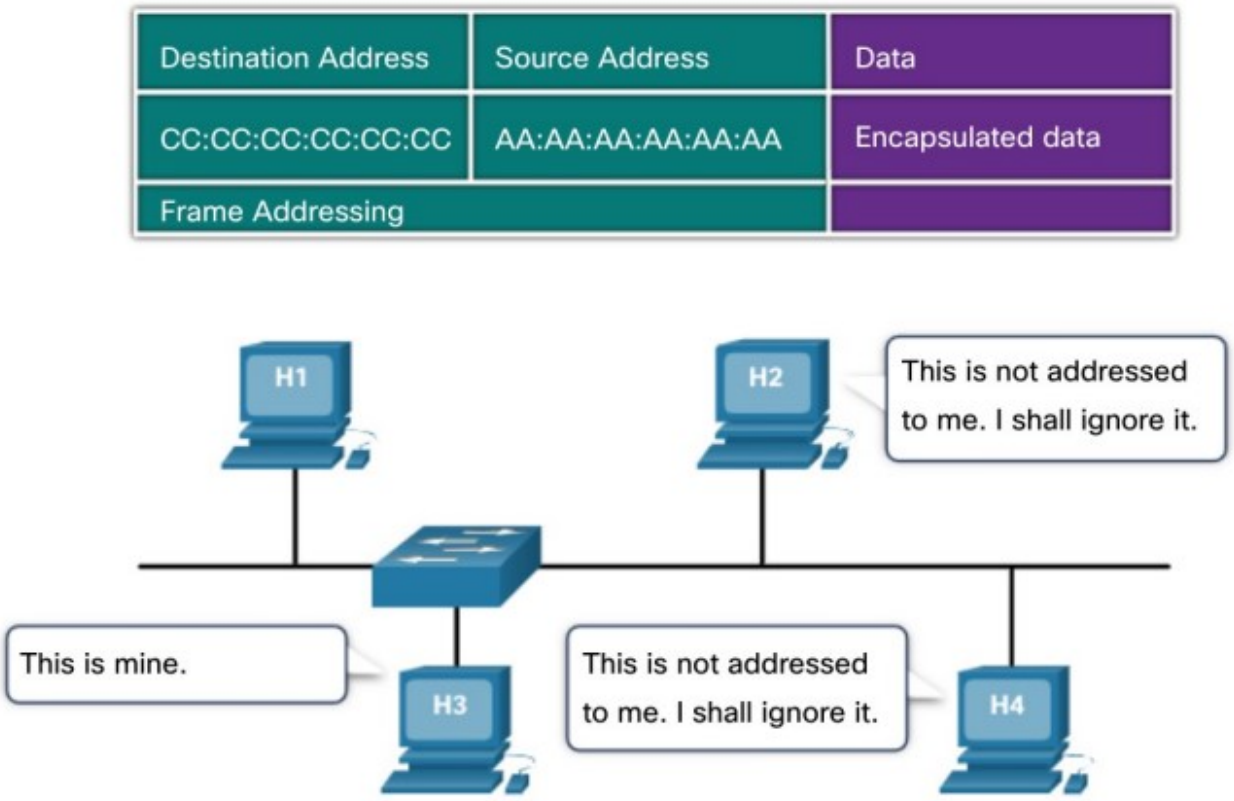

Abbildung 16: Verhalten der Netzwerkkarten (©Cisco)

Wie werden Sicherungsschicht Frames in einem Switch bearbeitet?

Ethernet-Switches
- ... nutzen MAC-Adressen, um Weiterleitungsentscheidungen (forwarding decision) zu treffen
- ... sind unwissend über den Inhalt der Daten im Datenfeld
- ... Entscheidungen über die Weiterleitung beruhen lediglich auf die Ethernet MAC-Adressen vom Layer 2
- ... untersuchen eigene MAC-Adressentabellen um Entscheidungen für jedes Frame zu treffen
- Wenn ein Switch einschaltet, ist seine MAC-Adresstabelle leer

Wie funktioniert der «Learn-and-forward» Prozess?

I. LEARN: Untersuche die Source-MAC-Adresse
1. Ein Frame erreicht den Switch
2. Switch untersucht die Source-MAC-Adresse des Frames und die Port-Nummer des Einganges
3. Source-MAC-Adresse nicht in Tabelle vorhanden:
   → füge Source-MAC-Adresse und Port-Nummer des Einganges zur MAC-Adresstabelle
3. Source-MAC-Adresse in Tabelle vorhanden:
   → Erneuere den Timer für den Eintrag in der Tabelle. Standard 5 min
3. Source-MAC-Adresse vorhanden, aber anderer Port:
   → ersetze Port und Timer-Update

II. FORWARD: Finde Destination-MAC-Adresse
- Destination-MAC-Adresse ist unicast:
  - Finde Übereinstimmung der Destination-MAC-Adresse in der Tabelle
    - Eintrag gefunden → weiterleiten des Frames an der in der Tabelle **eingetragenen** Port
    - keinen Eintrag gefunden → weiterleiten des Frames an **alle** Port, **ausser Eingangsport**

Was ist der Unterschied zwischen «Unicast» und «Broadcast» Frames?

Unicast-Frames haben die MAC-Adresse ein spezifischen Zieles angegeben,

Was ist der Zweck ARPs?

Das Address Resolution Protocol vermittelt zwischen der Sicherungsschicht - Data Link (2) und der Vermittlungsschicht - Network (3). Es dient dazu, zu einer bekannten Netzwerkadresse der Internetschicht (IPv4-Adresse) die physische Adresse der Sicherungsschicht (MAC-Adresse) zu ermitteln. Die ermittelte MAC-Adresse wird in einer ARP-Tabelle hinterlegt.

Wie funktioniert ARP?

Angenommen die ARP-Tabelle ist leer. Meine NIC möchte die MAC-Adresse vom Standardgateway wissen. Zunächst wird ein **ARP request** gesendet mit Destination „FF-FF-FF-FF-FF-FF“, also ein Broadcast. Alle Geräte erhalten den Aufruf und entscheiden (Siehe Frame-Erkennung, Seite 24). Der Gateway antwortet daraufhin mit einem **ARP reply** und teilt meiner NIC seine MAC-Adresse mit. Diese wird in die eigene ARP-Tabelle eingetragen.

Teil V
SW 05/06 - Network Layer - Vermittlungsschicht

13 Lernziele (Leitfragen) SW 05

- Was ist der Zweck der Vermittlungsschicht?
- Was für Protokolle findet man in der Vermittlungsschicht?
- Was sind die wichtigsten Merkmale des IPv4 Protokolls?
- Wie lange sind IPv4 Adressen?
- Wie sind IPv4 Adressen unterteilt?
- Wie findet man die Netzwerkadresse anhand der Hostadresse und der Subnetzmaske?
- Was ist die Verbindung zwischen Subnetzmasken und «Slash Notation»?
- Was ist der Unterschied zwischen Private und Public IPv4 Adressen?
- Wie werden Private IPv4 Adressen verwendet im Internet?
- Wieso brauchen wir Private IPv4 Adressen?
- Was ist eine Loopbackadresse? Wie wird diese Adresse verwendet?
- Was sind «Link-Local» (APIPA) Adressen? Wie und wann werden diese Adressen verwendet?
- Wie routet ein Host seine eigenen IPv4 Pakete?
- Was ist die Rolle der Default Gateway in dem Routing Prozess?

14 Antworten

Was ist der Zweck der Vermittlungsschicht?

- *Addressing end devices
- Encapsulation
  - IP encaplsulates the transport layer segment
  - IP can use either an IPv4 or IPv6 packet and not impact the layer 4 segment
  - IP packet will be examined by all layer 3 devices as it traverses the network
  - The IP addressing does not change from source to destination (except when NAT is used)
- *Routing
- De-Encapsulation

Was für Protokolle findet man in der Vermittlungsschicht?

Was sind die wichtigsten Merkmale des IPv4 Protokolls?

Network Layer is connectionless
- No connection (establishment): packets are just sent
- No control information (synchronizations, acknowledgements, etc.)
- The destination will receive the packet... hopefully!

Network Layer does best effort
- No delivery guarantee
- No mechanism to resend data
- Does not know if the other device is operational or if it received the packet

Network Layer is media independent
- IP does not care about the Data Link Layer or the Physical Layer
- With one exception: try not to exceed the Data Link Layer Maximum Transfer Unit (MTU)
  - MTU must be provided by the Data Link Layer
  - Undesirable for the Network Layer packet size to exceed the DL Layer MTU
  - What happens if the IP packet is larger than the DL MTU?

Wie lange sind IPv4 Adressen?

4 bytes = 32 bits

Wie sind IPv4 Adressen unterteilt?

- Network Address
- Host Address
- Broadcast Address

Wie findet man die Netzwerkadresse anhand der Hostadresse und der Subnetzmaske?

//TODO

Was ist die Verbindung zwischen Subnetzmasken und «Slash Notation»?

//TODO

Was ist der Unterschied zwischen Private und Public IPv4 Adressen?

Auf private IPv4 Adressen kann von aussen nicht direkt zugegriffen werden. Diese sind nach aussen hin unsichtbar.

Wie werden Private IPv4 Adressen verwendet im Internet?

NAT

Wieso brauchen wir Private IPv4 Adressen?

Um innerhalb des LANs auf Endgeräte zugreifen zu können.

Was ist eine Loopbackadresse? Wie wird diese Adresse verwendet?

Die Loopbackadresse zeigt auf den eigenen Host. Diese wird meistens dazu genutzt, um Programme, die als Server dienen können, lokal zu betreiben.

Was sind «Link-Local» (APIPA) Adressen? Wie und wann werden diese Adressen verwendet?

//TODO

Wie routet ein Host seine eigenen IPv4 Pakete?

//TODO

Was ist die Rolle der Default Gateway in dem Routing Prozess?

//TODO

15 Lernziele (Leitfragen) SW 06

- How do I find out my IPv4 configuration?
- How do I find the IP address associated to a URL?
- How do I determine if a host is “up” given its IP or URL?
- How do I find out which intermediate network devices are there between my host and another host, given its IPv4 address (or URL)?
- Wieso brauchen wir IPv6? Was sind die Nachteile von IPv4?
- Wie lange sind IPv6 Adressen?
- Was sind die Regeln, um eine IPv6 Adresse zu komprimieren?
- Wie sind IPv6 Adressen unterteilt?
- Was für IPv6 unicast Adress Arten gibt es?
- Über welche IPv6 unicast Adressen sollte ein richtig konfigurierte Host mindestens verfügen?
- Wie sind IPv6 Global Unicast Addresses (GUAs) unterteilt?
- Welche Mechanismen werden verwendet, um IPv4 und IPv6 Netzwerken miteinander zu verbinden?

16 Antworten

How do I find out my IPv4 configuration?

Windows: `ipconfig [/all]`

```
Drahtlos-LAN-Adapter WLAN:

   Verbindungsspezifisches DNS-Suffix: campus.intern
   Beschreibung. . . . . . . . . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter
   Physische Adresse . . . . . . . . . : 70-C9-4E-B9-49-EB
   DHCP aktiviert. . . . . . . . . . . : Ja
   Autokonfiguration aktiviert . . . . : Ja
   Verbindungslokale IPv6-Adresse  . . : fe80::151b:6b67:d310:a28b%27(Bevorzugt)
   IPv4-Adresse  . . . . . . . . . . . : 10.155.103.99(Bevorzugt)
   Subnetzmaske  . . . . . . . . . . . : 255.255.224.0
   Lease erhalten. . . . . . . . . . . : Dienstag, 26. Oktober 2021 08:52:17
   Lease läuft ab. . . . . . . . . . . : Dienstag, 26. Oktober 2021 23:19:28
   Standardgateway . . . . . . . . . . : 10.155.96.1
   DHCP-Server . . . . . . . . . . . . : 10.26.18.177
   DHCPv6-IAID . . . . . . . . . . . . : 124832078
   DHCPv6-Client-DUID. . . . . . . . . : 00-01-00-01-26-CE-DA-36-70-C9-4E-B9-49-EB
   DNS-Server  . . . . . . . . . . . . : 10.26.17.179
                                         10.26.17.177
   NetBIOS über TCP/IP . . . . . . . . : Aktiviert
```

Abbildung 17: Adapterkonfiguration in Windows mit `ipconfig /all`

Unix: `ifconfig`

```
administrator@Server:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Lokale Schleife)
        RX packets 44525  bytes 3318049 (3.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44525  bytes 3318049 (3.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

p2p1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.5  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 2a02:120b:2c4f:dcc0:d63d:7eff:feb0:3314  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::d63d:7eff:feb0:3314  prefixlen 64  scopeid 0x20<link>
        ether d4:3d:7e:b0:33:14  txqueuelen 1000  (Ethernet)
        RX packets 6309878  bytes 1977124401 (1.9 GB)
        RX errors 0  dropped 144109  overruns 0  frame 0
        TX packets 2785408  bytes 817332695 (817.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Abbildung 18: Adapterkonfiguration in Ubuntu mit `ifconfig`

How do I find the IP address associated to a URL?

`nslookup <URL>`

```
C:\>nslookup hslu.ch
Server:  inf47.campus.intern
Address:  10.26.17.179

Name:    hslu.ch
Address:  147.88.201.68
```

Abbildung 19: `nslookup` in Windows

```
administrator@Server:~$ nslookup hslu.ch
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   hslu.ch
Address: 147.88.201.68
```

Abbildung 20: `nslookup` in Ubuntu

How do I determine if a host is “up” given its IP or URL?

Windows:

- `ping [-4] <URL>`
- `ping <IPv4-Adresse>`

Unix: `ping <IPv4-Adresse | URL>` (Ctrl+C zum abbrechen)

```
C:\>ping hslu.ch

Ping wird ausgeführt für hslu.ch [147.88.201.68] mit 32 Bytes Daten:
Antwort von 147.88.201.68: Bytes=32 Zeit=3ms TTL=59
Antwort von 147.88.201.68: Bytes=32 Zeit=4ms TTL=59
Antwort von 147.88.201.68: Bytes=32 Zeit=6ms TTL=59
Antwort von 147.88.201.68: Bytes=32 Zeit=4ms TTL=59

Ping-Statistik für 147.88.201.68:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 3ms, Maximum = 6ms, Mittelwert = 4ms
```

Abbildung 21: `ping` in Windows

```
administrator@Server:~$ ping google.ch
PING google.ch(zrh04s16-in-x03.1e100.net (2a00:1450:400a:808::2003)) 56 data bytes
64 bytes from zrh04s16-in-x03.1e100.net (2a00:1450:400a:808::2003): icmp_seq=1 ttl=117 time=5.98 ms
64 bytes from zrh04s16-in-x03.1e100.net (2a00:1450:400a:808::2003): icmp_seq=2 ttl=117 time=5.14 ms
64 bytes from zrh04s16-in-x03.1e100.net (2a00:1450:400a:808::2003): icmp_seq=3 ttl=117 time=5.07 ms
64 bytes from zrh04s16-in-x03.1e100.net (2a00:1450:400a:808::2003): icmp_seq=4 ttl=117 time=6.49 ms
64 bytes from zrh04s16-in-x03.1e100.net (2a00:1450:400a:808::2003): icmp_seq=5 ttl=117 time=5.72 ms
64 bytes from zrh04s16-in-x03.1e100.net (2a00:1450:400a:808::2003): icmp_seq=6 ttl=117 time=5.74 ms
^C
--- google.ch ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 5.078/5.694/6.497/0.485 ms
```

Abbildung 22: `ping` in Ubuntu

How do I find out which intermediate network devices are there between my host and another host, given its IPv4 address (or URL)?

Windows:

- `tracert [-4] <URL>`
- `tracert <IPv4 Address>`

Unix: `traceroute <IPv4 Adress | URL>`

```
C:\>tracert hslu.ch

Routenverfolgung zu hslu.ch [147.88.201.68]
über maximal 30 Hops:

  1     2 ms     2 ms     2 ms  10.155.96.2
  2     3 ms     3 ms     3 ms  a-stud-u_rz1-sc-1_3553.net.intern [10.0.38.131]
  3     4 ms     4 ms     3 ms  lambda_rz1-pe-1_2505.net.intern [10.0.32.141]
  4    57 ms     3 ms     3 ms  lambda_ifw_2701.net.intern [10.7.0.10]
  5     7 ms     3 ms     4 ms  r-dmz_rz1-pe-1_2702.net.intern [10.7.8.2]
  6     6 ms     3 ms     3 ms  147.88.201.68

Ablaufverfolgung beendet.
```

Abbildung 23: `tracert` in Windows

```
administrator@Server:~$ traceroute hslu.ch
traceroute to hslu.ch (147.88.201.68), 30 hops max, 60 byte packets
 1  internetbox.home (10.0.0.1)  0.406 ms  0.501 ms  0.588 ms
 2  1.252.196.178.dynamic.wline.res.cust.swisscom.ch (178.196.252.1)  4.089 ms  3.962 ms  4.011 ms
 3  * * *
 4  * * *
 5  i71lzf-005-ae3.bb.ip-plus.net (138.187.129.196)  4.603 ms  4.501 ms  4.530 ms
 6  i79zhb-015-ae14.bb.ip-plus.net (138.187.129.195)  5.117 ms  2.580 ms  4.077 ms
 7  i79tix-025-ae11.bb.ip-plus.net (138.187.130.38)  4.111 ms  3.595 ms  3.627 ms
 8  193.134.95.27 (193.134.95.27)  3.665 ms  3.733 ms  3.629 ms
 9  swiEZ3-100GE-0-1-0-4.switch.ch (130.59.38.109)  4.384 ms  3.892 ms  4.189 ms
10  swiEZ1-P3.switch.ch (130.59.36.33)  3.515 ms  3.527 ms  4.792 ms
11  swiAG1-10GE-0-0-2-0.switch.ch (130.59.38.1)  5.621 ms  5.154 ms  5.055 ms
12  swiLZ2-10GE-1-4.switch.ch (130.59.36.214)  4.390 ms  4.359 ms *
13  147.88.192.2 (147.88.192.2)  16.073 ms  17.021 ms  16.451 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Abbildung 24: `traceroute` in Ubuntu

Wieso brauchen wir IPv6? Was sind die Nachteile von IPv4?

//TODO

Wie lange sind IPv6 Adressen?

128 bit

Was sind die Regeln, um eine IPv6 Adresse zu komprimieren?

//TODO

Wie sind IPv6 Adressen unterteilt?

//TODO

Was für IPv6 unicast Adress Arten gibt es?

//TODO

Über welche IPv6 unicast Adressen sollte ein richtig konfigurierte Host mindestens verfügen?

- 64 bit prefix
  - **Global Routing Prefix**: Portion of the address that is assigned by the provider, such as an ISP, to a customer or site. The global routing prefix will vary depending on ISP policies.
  - **Subnet ID**: Portion between the Global Routing Prefix and the Interface ID. The Subnet ID is used by an organization to identify subnets within its site.
- Interface ID: Equivalent to the host portion of an IPv4 address.

Wie sind IPv6 Global Unicast Addresses (GUAs) unterteilt?

//TODO

Welche Mechanismen werden verwendet, um IPv4 und IPv6 Netzwerken miteinander zu verbinden?

1. Dual stack - The devices run both IPv4 and IPv6 protocol stacks simultaneously.
2. Tunneling - A method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet.
3. Translation - Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4.

Teil VI
SW 07 - Transport Layer - Transportschicht

17 Lernziele (Leitfragen)

- Was ist der Zweck der Transportschicht?
- Was für Protokolle findet man in der Transportschicht?
- Was sind die wichtigsten Merkmale des TCP Protokolls?
- Was sind die wichtigsten Merkmale des UDP Protokolls?
- Wozu werden Ports in der Transportschicht verwendet?
- Was ist ein Socket?
- Was ist ein «Socket Pair»?
- Geben Sie Beispiele von Anwendungen die TCP verwenden
- Für welche Applikationsarten ist UDP besser geeignet als TCP?
- Welches Portintervall verwenden normalerweise bekannte Netzwerkapplikationen und -dienste?
- Wie realisiert TCP zuverlässige Verbindungen?
- Was ist der Zweck des TCP Handshake?
- Wie funktioniert der TCP Handshake?
- Wie werden Verbindungen in TCP richtig beendet?
- Was ist der Zweck von «Selective Acknowledgements»?

18 Antworten

Was ist der Zweck der Transportschicht?

- Multiplexing: Logische Kommunikation zwischen Applikationen, welche auf verschiedenen Hosts laufen
- Link zwischen Application Layer und darunterliegenden Layern
- Individuelle Kommunikationen verfolgen (jeder Tab im Browser) //TODO pic
- Segmentierung der Daten und wieder zusammenfügen
- Header Information hinzufügen
- Identifizieren, Teilen und verschiedene Konversationen managen
- Segmentierung //TODO Folie schauen

Was für Protokolle findet man in der Transportschicht?

- TCP - Transmission Control Protocoll
  - Zuverlässigkeit - Reliability
    - Nummerieren von Datensegmenten
    - Bestätigen von übertragenen Daten
    - Erneutes Senden von Daten, wenn Zeit abgelaufen
    - Reorganisation von Daten, wenn in falscher Reihenfolge empfangen: $1, 3, 5, 4, 2 \rightarrow 1, 2, 3, 4, 5$
  - Durchsatzkontrolle - Flow Control
    - Effizienteste Rate für Empfänger
- UDP - User Datagram Protocol
  - //TODO

Was sind die wichtigsten Merkmale des TCP Protokolls?

//TODO

Was sind die wichtigsten Merkmale des UDP Protokolls?

//TODO

Wozu werden Ports in der Transportschicht verwendet?

//TODO

Was ist ein Socket?

Ein Socket ist die Kombination von Source IP Address & Source Port oder Destination IP Address & Destination Port

Was ist ein «Socket Pair»?

Unique Identifier für eine Verbindung.

Geben Sie Beispiele von Anwendungen die TCP verwenden

- Mail (POP, IMAP)
- Secure Shell (SSH)
- FTP
- HTTP

Für welche Applikationsarten ist UDP besser geeignet als TCP?

- DHCP
- DNS
- SNMP
- TFTP
- VoIP
- Video Conferencing

Welches Portintervall verwenden normalerweise bekannte Netzwerkapplikationen und -dienste?

- Low Ports / Well-known Ports: 0-1023, //TODO
- Registered Ports: 1024-49151, //TODO
- Private and/or Dynamic Ports: 49152-65535, //TODO

Wie realisiert TCP zuverlässige Verbindungen?

//TODO

Was ist der Zweck des TCP Handshake?

- Wissen, dass Server da ist
- Client ist fähig Verbindung herzustellen
- Server weiss, dass Client verbinden möchte
- Vereinbarung zwischen Geräten über Session Control Parametern und optionalen Eigenschaften

Wie funktioniert der TCP Handshake?

//TODO

Wie werden Verbindungen in TCP richtig beendet?

//TODO

Was ist der Zweck von «Selective Acknowledgements»?

//TODO

Teil VII
SW 08

19 Lernziele (Leitfragen)

-
-
-
-
-
-
-
-
-
-
-
-
-
-

20 Antworten

Teil VIII
SW 11

21 Lernziele (Leitfragen)

-
-
-
-
-
-
-
-
-
-
-
-
-
-

22 Antworten

Teil IX
SW 12

23 Lernziele (Leitfragen)

- Welche Adressen können in einem typischen TCP/IP Netzwerk gefälscht (spoof) werden? Was kann ein Angreifer erreichen, wenn eine solche Fälschung nicht erkannt oder verhindert wird?
- Geben Sie ein Beispiel von einem 'Man-in-the-middle' Angriff
- Wie funktioniert einem 'Trust Exploitation' Angriff?
- Geben Sie ein Beispiel für eine typische Softwareschwachstelle und eventuelle Folgen deren Nutzung (exploitation)
- Geben Sie ein Beispiel von einem 'Denial-of-Service' Angriff
- Wieso sind 'Denial-of-Service' Angriffe i.d.R. schwierig zu verhindern?
- Was ist 'Defense-in-depth'?
- Wozu werden IDSs und IPSs verwendet? Wie unterschieden sie sich?
- Was Sind 'Data Loss Prevention Systems'? Geben Sie ein Beispiel eines solchen Systems
- Geben Sie drei Beispiele von unsicheren Netzwerkprotokollen und deren entsprechenden sicheren Protokolle
- Wieso sind Backups wichtig? Was ist bei der Durchführung von Backups zu beachten (aus Sicherheits- und Betriebssicht)?
- Wieso ist Multifaktor Authentifizierung den Passwörtern zu bevorzugen?
- Was ist der Zweck einer Firewall?
- Wie funktioniert eine «First Generation (Packet Filter) Firewall»?
- Wie funktioniert eine «Second Generation (Stateful) Firewall»?
- Wie funktioniert eine moderne Firewall?
- Was ist ein «Proxy» und was ist sein Zweck?
- Was ist der Zweck einer Web Application Firewall (WAF)?
- Was ist eine VPN? Wieso ist es «Virtual», wieso ist es «Private»?
- Was sind die Vorteile von VPNs im Vergleich zu traditionellen privaten Netzwerken?
- Was sind die Hauptarten von VPNs?
- Was sind die Hauptarten von Remote Access VPNs?
- Was ist IPSec? Was ist seine Verwendung?
- Woraus besteht eine IPSec Security Association?
- Was ist der Unterschied zwischen Transport und Tunnel Modi in IPSec?

24 Antworten

Welche Adressen können in einem typischen TCP/IP Netzwerk gefälscht (spoof) werden? Was kann ein Angreifer erreichen, wenn eine solche Fälschung nicht erkannt oder verhindert wird?

Beispielsweise können MAC-Adressen, IP-Adressen wie Default-Gateway, DNS etc. gefälscht werden. Die Folge wäre ein DoS (Denial of Service).

Geben Sie ein Beispiel von einem 'Man-in-the-middle' Angriff

Ein Angreifer stellt sich zwischen

Wie funktioniert einem 'Trust Exploitation' Angriff?

Eve <-x-> Alice <—> Bob <—> Eve

Geben Sie ein Beispiel für eine typische Softwareschwachstelle und eventuelle Folgen deren Nutzung (exploitation)

RDP

Geben Sie ein Beispiel von einem 'Denial-of-Service' Angriff

Wieso sind 'Denial-of-Service' Angriffe i.d.R. schwierig zu verhindern?

Was ist 'Defense-in-depth'?

Verschiedene Verteidigungsmechanismen auf verschiedenen Layern bereitstellen.

Wozu werden IDSs und IPSs verwendet? Wie unterschieden sie sich?

- Intrusion Detection System: Ein Angriff wird erkannt und geblockt
- Intrusion Prevention System: Ein Angriff wird im Vornherein erkannt und unterbrochen.

Was Sind 'Data Loss Prevention Systems'? Geben Sie ein Beispiel eines solchen Systems

Verhindern, dass sensitive Daten beispielsweise auf USB-Sticks kopiert werden, oder Emails keine sensitive Daten als Anhang haben.

Geben Sie drei Beispiele von unsicheren Netzwerkprotokollen und deren entsprechenden sicheren Protokolle

FTP(S), HTTP(S), Telnet <-> SSH.

Wieso sind Backups wichtig? Was ist bei der Durchführung von Backups zu beachten (aus Sicherheits- und Betriebssicht)?

Wieso ist Multifaktor Authentifizierung den Passwörtern zu bevorzugen?

Was ist der Zweck einer Firewall?

- Kontrollpunkt: Netzwerk-/ Datenverkehr erlauben oder verweigern
- Realisierung: Hard- und/oder Software
- Datenverkehr durch die Firewall muss autorisiert werden: Firewall-Rules
- Sie selbst muss gegen Angriffe möglichst resistent sein

Wie funktioniert eine «First Generation (Packet Filter) Firewall»?

Vorteile:
- Jedes Paket
  - einzeln angeschaut
  - in jede Richtung separat
  - Paketinhalt nicht kontrolliert
- In wenigen Fällen angewendet
- Kann mit modernen Routern realisiert werdenSehr schnell & günstig

Nachteile:
- Schwierig zu konfigurieren
- Probleme mit gewissen Protokollen wie FTP
  - Ankommende Verbindung für FTP Data

  //TODO

Wie funktioniert eine «Second Generation (Stateful) Firewall»?

- Paket Filter mit Intelligenz
- Zusammenhänge zwischen Paketen werden berücksichtigt
- Antwort auf ein vorher ausgehendes Paket wird wieder reingelassen
- Paket-Inhalt (Daten) nicht kontrolliert

Wie funktioniert eine moderne Firewall?

- System: Software und ev. Hardware
- Kann (auch) ausgefeilte Angriffe erkennen und blockieren
- Fassen drei Schlüsselfunktionen zusammen:
  - Techniken von professionellen (stateful) Firewalls
  - Intrusion Detection & Prevention Systems (IDS & IPS)
  - Applikations-Kontrolle (mittels Deep-Packet-Inspection)
- Evtl. externe (freie und kostenpflichtige) Quellen (feeds) mit weiteren Informationen integriert
  - Somit könnten z.B. bei einer bekannt gewordenen Phishing-Attacke automatisch solche Sites direkt auf der Firewall gesperrt werden

Was ist ein «Proxy» und was ist sein Zweck?

Vorteile:
- Einfacher zu konfigurieren
- Keine vertieften TCP/IP Kenntnisse erforderlich
- Relativ sicher im Vergleich zu Packet Filter

Nachteile:
- Relativ langsam im Vergleich zum Paket Filter
- Falls neue oder nicht unterstützte Protokolle verwendet werden, sollen, muss eine neue Firewall //TODO
- Ressourcenintensiv

Was ist der Zweck einer Web Application Firewall (WAF)?

- Schutz eines oder mehrerer Web-Server
- Zusätzlich zur „normalen“ Firewall (nicht als Ersatz)
- Schutz gegen SQL-Injection, XSS etc. (z.B. OWASP Top 10)
- Evtl. Validierung von Cookies, Session State, User etc.
- Proaktiver Schutz gegen neue (ev. noch nicht entdeckte) Sicherheitslücken
- Know-How Transfer Software-Entwickler → Firewall Administrator

Was ist eine VPN? Wieso ist es «Virtual», wieso ist es «Private»?

Was sind die Vorteile von VPNs im Vergleich zu traditionellen privaten Netzwerken?

Was sind die Hauptarten von VPNs?

Was sind die Hauptarten von Remote Access VPNs?

Was ist IPSec? Was ist seine Verwendung?

Woraus besteht eine IPSec Security Association?

Was ist der Unterschied zwischen Transport und Tunnel Modi in IPSec?

Abbildungsverzeichnis

Akronyme

APIPA Automatic Private IP Addressing

BOYD Bring your own Device

DSL Digital Subscriber Line

GSM Global System for Mobile Communication

IETF Internet Engineering Task Force

IoT Internet of Things

MAC Media Access Control

NIC Network Interface Controller/Card

VoIP Voice over IP

Glossar

Automatic Private IP Addressing Automatic Private IP Addressing (APIPA) ist eine sogenannte Link-Local Address. Es ist eine vom Betriebssystem automatisch zugewiesene IP-Adresse, falls das System auf DHCP eingestellt ist, jedoch nichts vom DHCP offeriert wurde. Dies weil entweder kein DHCP-Server im Netzwerk vorhanden ist oder dieser keine Antwort gibt.
Der Adressbereich in IPv4 ist 169.254.0.0/16 (196.254.0.0 - 169.254.255.255).

Internet of Things Begriff für Technologien einer globalen Infrastruktur der Informationsgesellschaften, die es ermöglicht, physische und virtuelle Objekte miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen. Vernetzung allerlei Dinge von der Wetterstation zuhause, dem intelligenten Kühlschrank bis hin zum selbstfahrenden Auto.

Network Interface Controller/Card Ein NIC ist die Netzwerkkarte eines Clients.

Index

Tabellenverzeichnis

Quellen

[1] Rüdiger Schreiner. *Computernetzwerke - Von den Grundlagen zur Funktion und Anwendung*. M: Carl Hanser Verlag GmbH Co KG, 2019. ISBN: 978-3-446-46010-2.

[2] FS.COM GmbH. URL: `https://media.fs.com/images/community/wp-content/uploads/2017/11/comparison-of-OSI-and-TCPIP.jpg` (besucht am 31. 12. 2021).