NETT HS 2021

Victor Fernández und Loris Steiner

HSLU Wirtschaftsinformatik

12. 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.

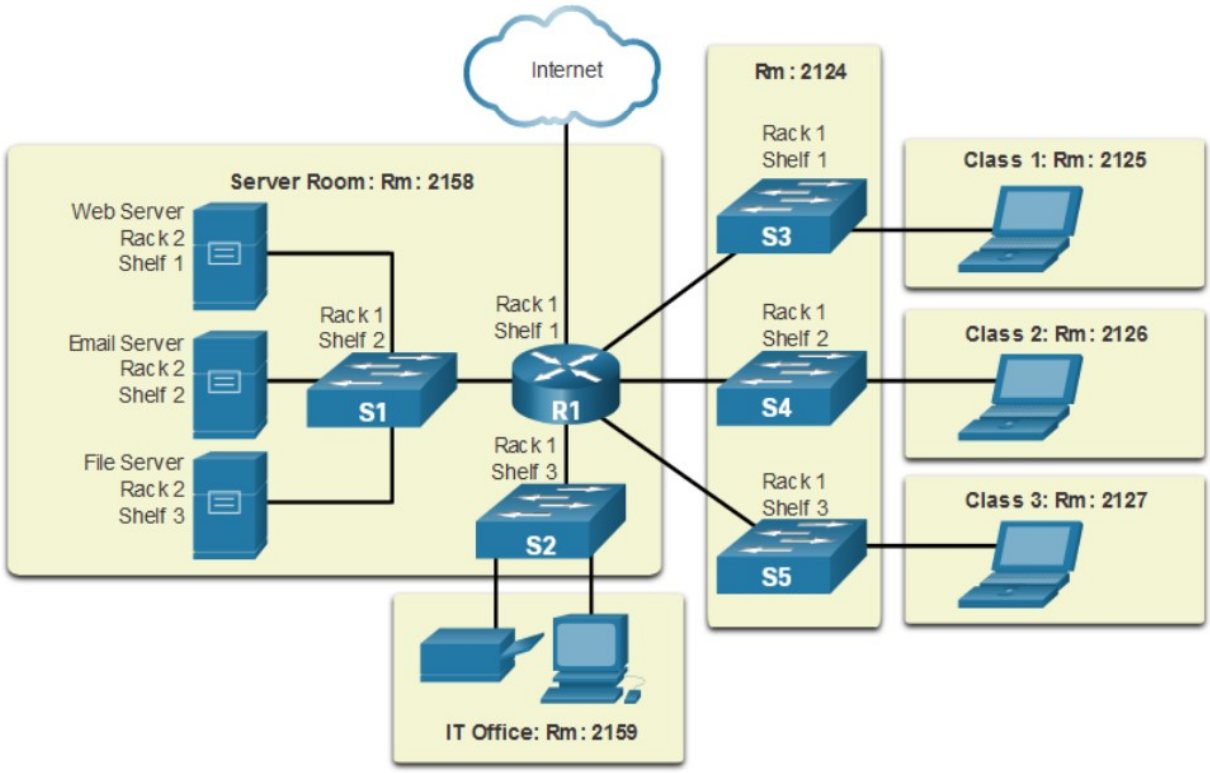


Abbildung 1: Physikalisches Netzwerkdiagramm (©Cisco)

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*.

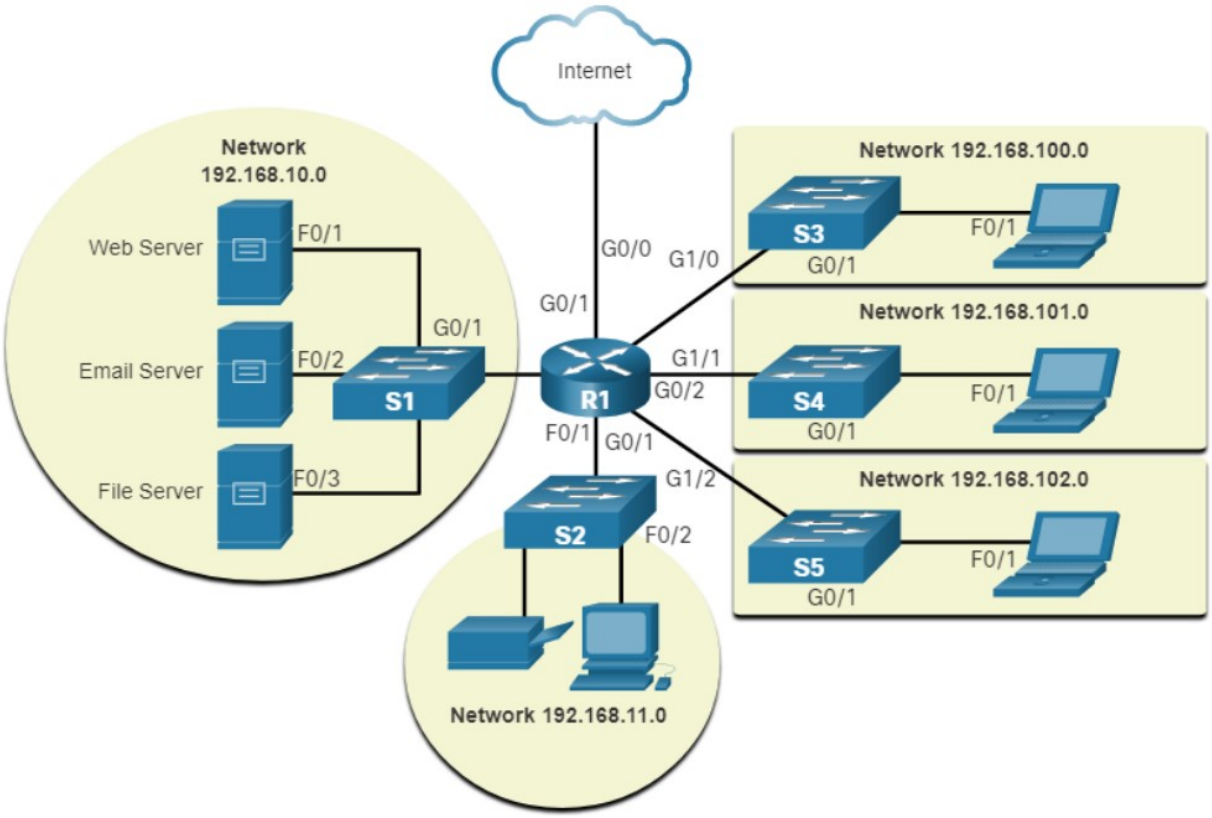


Abbildung 2: Logisches Netzwerkdiagramm (©Cisco)

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 31). 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 30.

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.

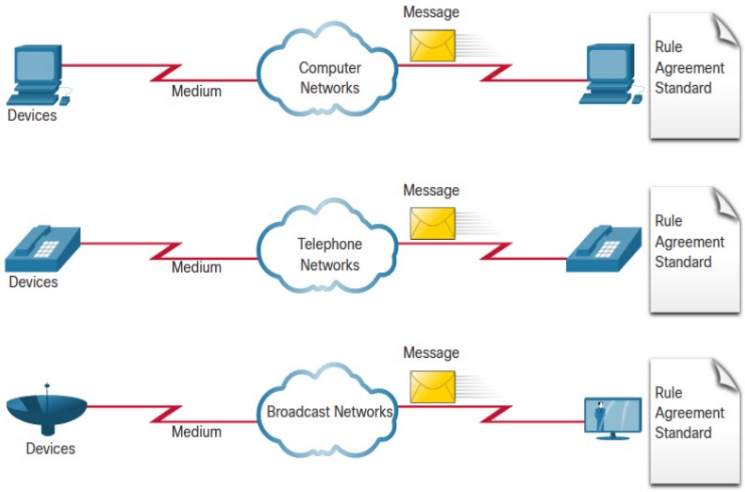


Abbildung 3: Klassisches Netz (©Cisco)

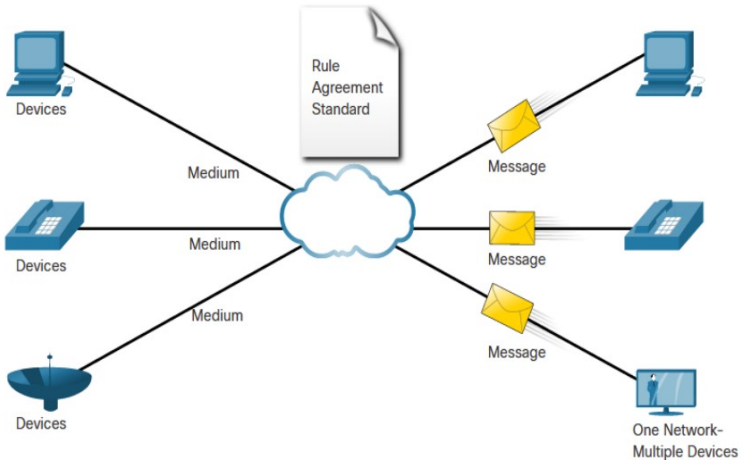


Abbildung 4: Modernes, konvergiertes Netz (©Cisco)

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.

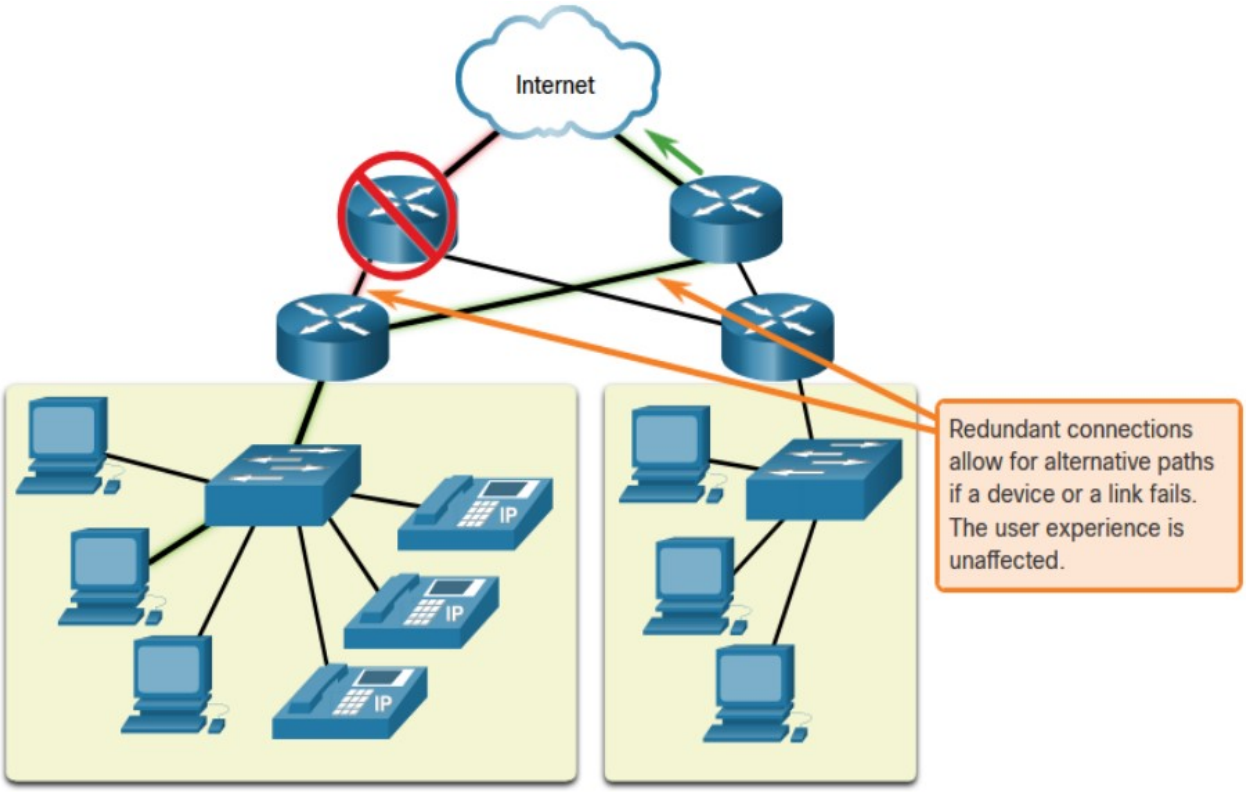


Abbildung 5: Fault tolerance - Fehlertoleranz (©Cisco)

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.

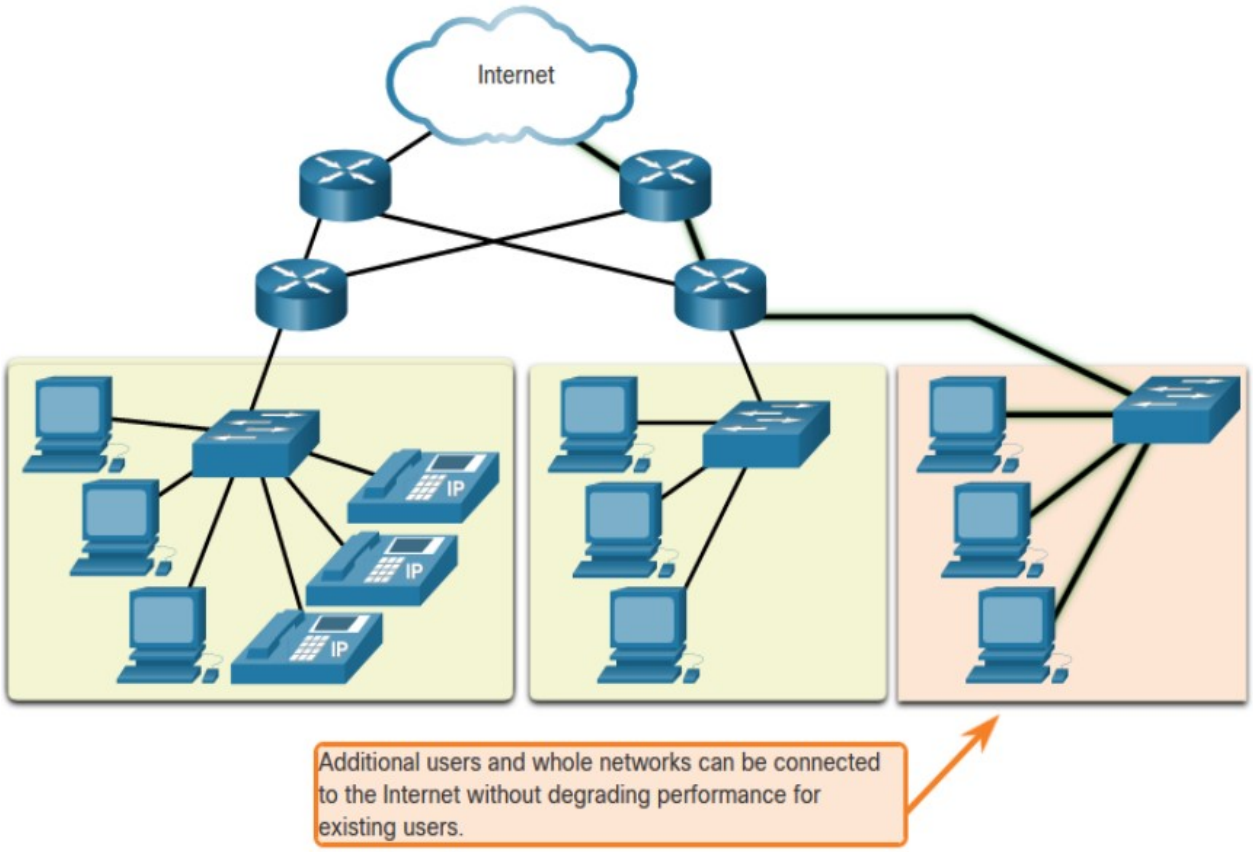


Abbildung 6: scalability - Skalierbarkeit (©Cisco)

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.

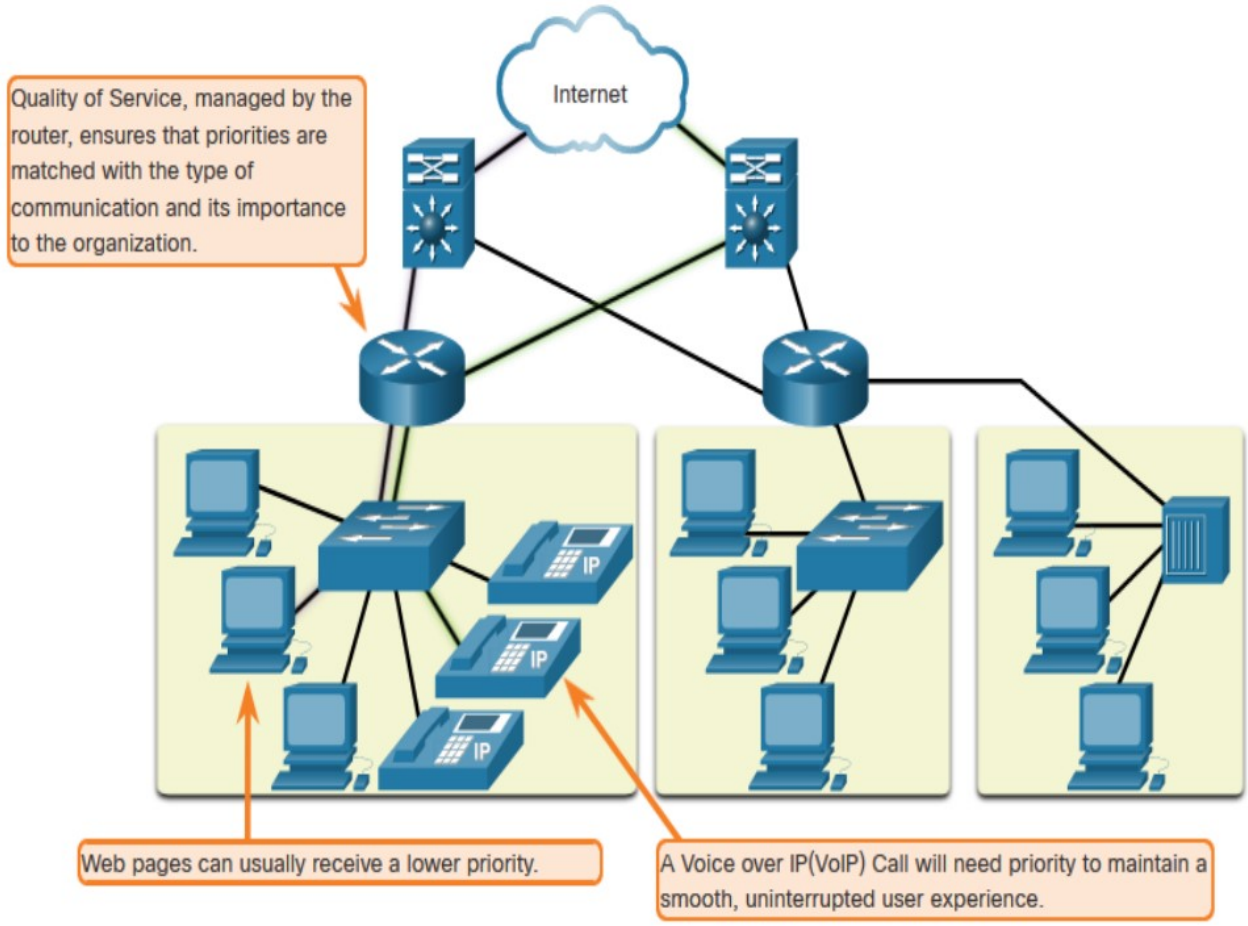


Abbildung 7: Quality of service

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?

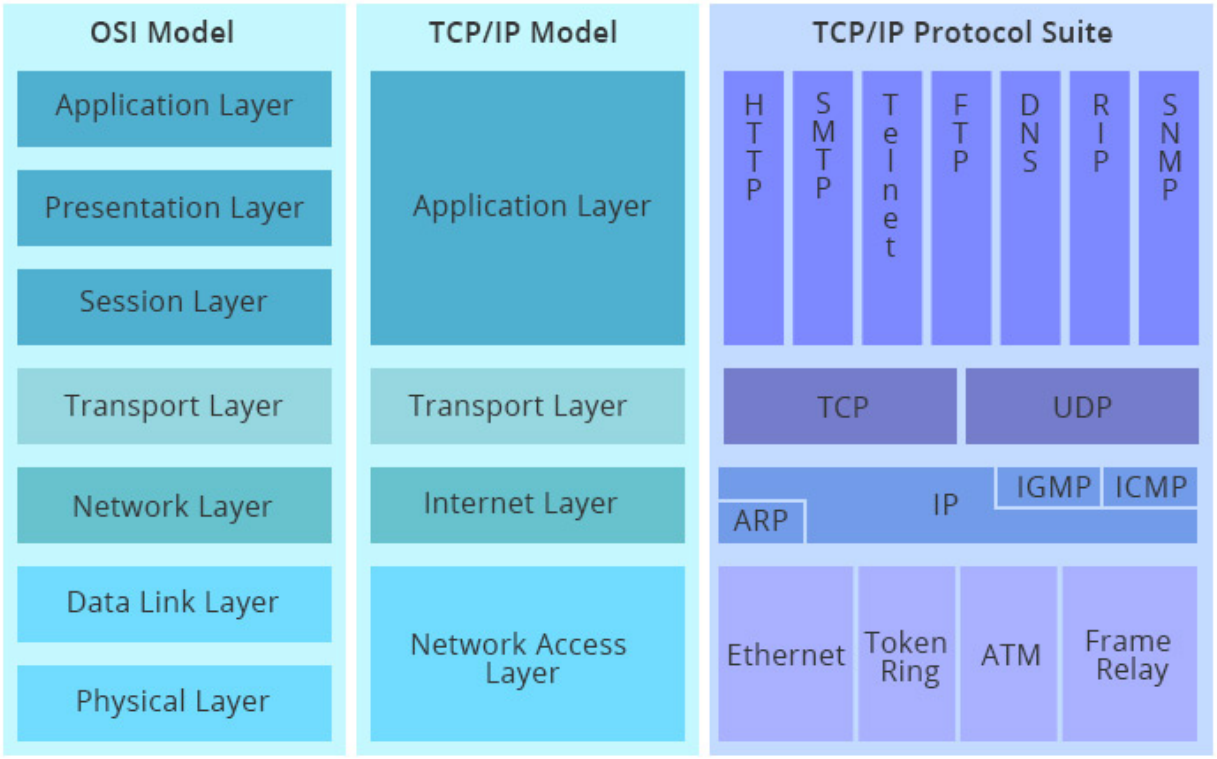


Abbildung 8: Vergleich OSI mit TCP/IP Modell[2]

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

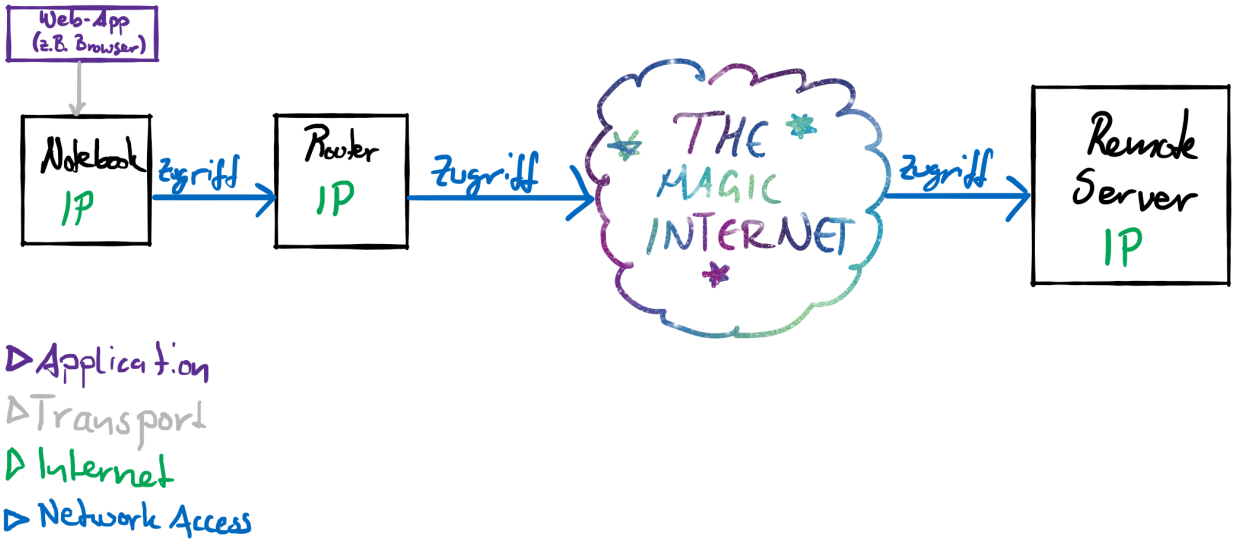


Abbildung 9: Weg eines Datenpaketes

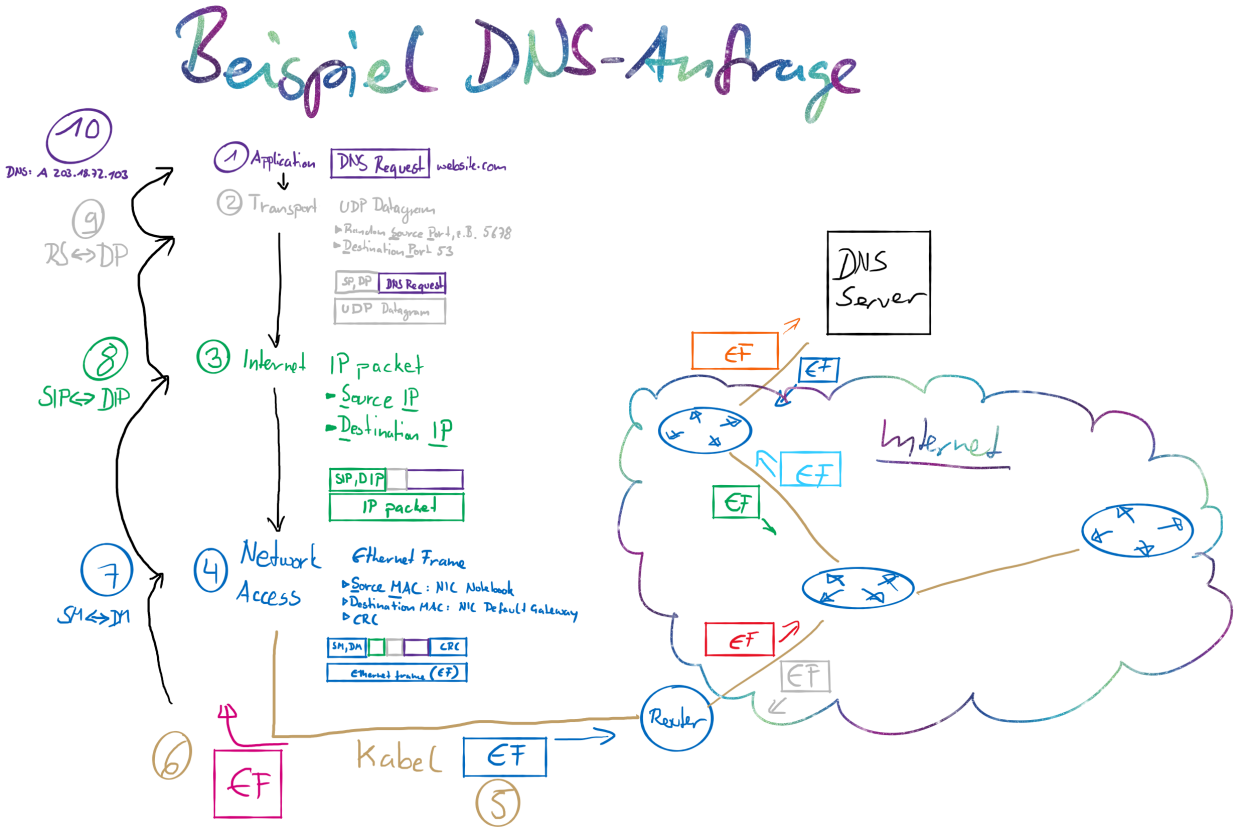


Abbildung 10: Einzelschritte der Kapselung, Beispiel anhand DNS request

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 ist der Unterschied zwischen CSMA/CD und CSMA/CA? Wo werden sie verwendet?
  6. Was bedeutet „Late Collision“?
  7. 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?

- Bietet elektrische, mechanische und funktionale Schnittstelle zum Medium
- Definiert die Grösse der Bits (Geschwindigkeit)
- Definiert die Art der Übertragung und Codierung (z.B. elektromagnetische Wellen)

- Kommunikation zwischen Übertragungsmedien
  - Lichtwellenleiter
  - Stromkabel
  - Stromnetz

Was sind die Hauptmerkmale der physikalischen Schicht?

- Digitale Bit-Übertragung: *funktioniert indem...*
  - *... über Kabel...*
    - Kupfer, Lichtwellenleiter, Stromnetz
  - *... eine Verbindung...*
    - statisches Multiplexing (synchron)
    - dynamisches Multiplexing (asynchron)
  - *... an die richtigen Steckplätze hergestellt wird....*
- Definition der Übertragung eines Bits
  - Dabei nicht nur 0 oder 1, sondern mehr
    - Lichtintensität (Glasfaser)
    - Spannung & Ströme (elektrische Leitung)
    - Binär (Datenstrom)
  - Übertragungsart muss mit Codierung versehen werden

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

Vergleiche Kommunikationsrichtung, das Senden/Empfangen, Leistung und Beispiele:

- Simplex
  - Unidirektional
  - Nur Sender schickt Daten
  - Schlechteste Leistung in Übertragung
  - Tastatur→Monitor
- Half-Duplex
  - Bidirektional: eins auf einmal
  - Sender kann Daten senden und empfangen, aber nur ein Sender auf einmal
  - Besser als Simplex
  - Walkie-Talkie
- Full-Duplex
  - Bidirektional: alle gleichzeitig
  - Sender schickt und empfängt Daten gleichzeitig
  - Beste Leistung
  - Telefon

Welches sind die am häufigsten verwendeten Zugriffsverfahren?

Es gibt zwei Oberbegriffe:

- **Nichtdeterministischer/stochastische Zugriffsverfahren**
  - Jeder Teilnehmer kann zu jedem Zeitpunkt einen Kanalzugriff versuchen
  - Zuteilungszeitpunkt lässt sich nicht vorherberechnen
  - Hohe Netzauslastung & Wartezeiten
    - CSMA/CD
    - CSMA/CA
    - (Siehe nächste Frage)
- **Deterministische Zugriffsverfahren (kontrollierter Zugriff)**
  - Sender zu Beginn einer Datenübertragung eindeutig bestimmt
  - Zeitpunkt des Buszugriffs kann vorhergesagt werden (wichtig für Echtzeitanwendungen)
    - Token-Passing
    - Multiplexing-Verfahren
    - Polling

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].

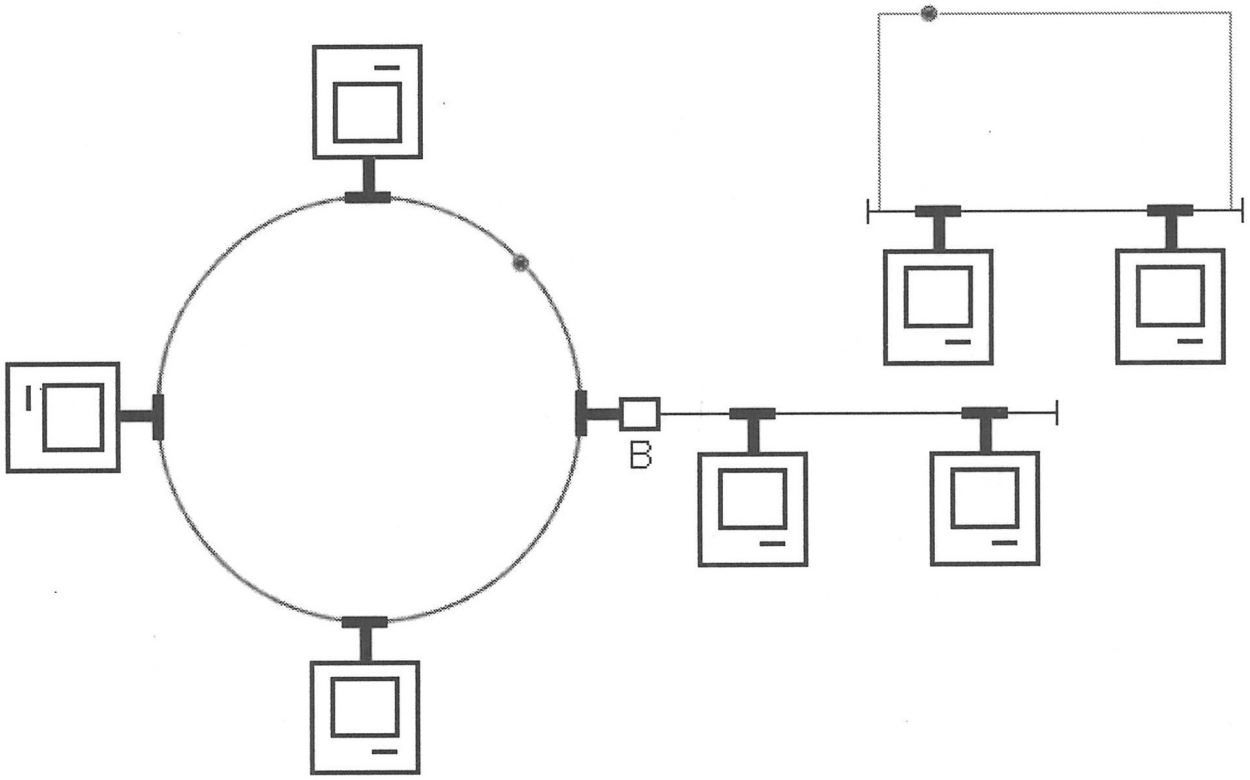


Abbildung 12: Links: Token Ring. Rechts oben kleines Bild: Token wird auf einem Bus weitergereicht und am Ende wird es zum Anfang zurückgereicht und wieder gesendet.[1]

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

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 bedeutet „Late Collision“?

- Definition:
  - Late Collisions sind ein spezieller Typ von Kollisionen im Ethernet
  - Kollision tritt nach den ersten 64 Bytes (512 bits) eines Frames auf (Mindestgrösse)
- Ursachen:
  - Ein wesentlich zu langes Netzwerkkabel
  - Falsche Duplex-Einstellungen an Netzwerkkarte oder Switch

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

- Übertragung nicht nur „physisch“ per Kabel
  - Schall
  - Licht
  - elektromagnetische Wellen
- Geräte
  - Hub
  - Repeater
  - Kabel
  - Antennen

7 Antworten T2

Was für Topologien findet man in Computernetzwerken?

Topologien beschreiben, wie Geräte in einem Netzwerk miteinander kommunizieren. Verschiedene Topologien haben Vor- und Nachteile betreffend Kommunikationsfluss, Ausfallsicherheit (Single Point of Failure) und in ihrer Komplexität (Routing oder physisch). Je nach Art können Topologien kombiniert werden.

Gängigste Topologie-Typen

- Bus
  - Vorteile
    - geringe Kosten
    - einfache Verkabelung
    - keine aktiven Netzwerkkomponenten
  - Nachteile
    - leicht abhörbar
    - kann bei einer Störung leicht blockiert werden
    - viele Kollisionen
- Ring
  - Vorteile
    - keine Kollisionen
    - alle Stationen sind Verstärker
    - gut skalierbar
  - Nachteile
    - hohe Latenzen zu entfernten Knoten
    - leicht abhörbar
    - langsamere Datenübertragung
    - hoher Energieaufwand
- Stern
  - Vorteile
    - leicht erweiterbar

    * hoher Datendurchsatz
    * Ausfall der Endpunkte hat keinen Einfluss auf das Netz
  - Nachteile
    * Single Point of Failure beim Verteiler
  - Anwendung: Heimnetzwerke
- Vermaschtes Netz
  - Vorteile
    * grundsätzlich sehr ausfallsicher
    * hoher Datendurchsatz
  - Nachteile
    * hoher Realisierungsaufwand
  - Anwendung: WAN

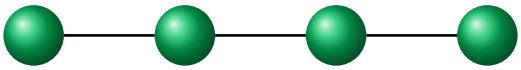


Abbildung 13: Linie Topologie

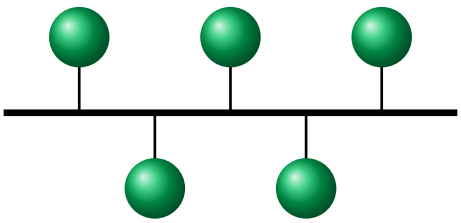


Abbildung 14: Bus Netz

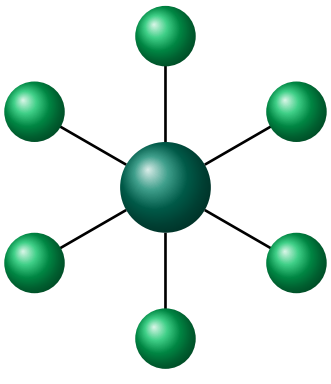


Abbildung 15: Stern Netz

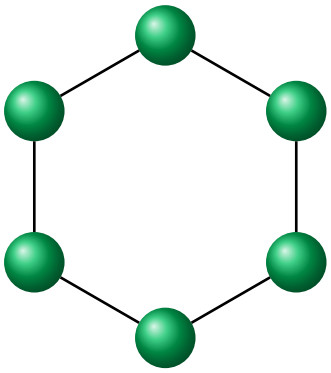


Abbildung 16: Ring Netz

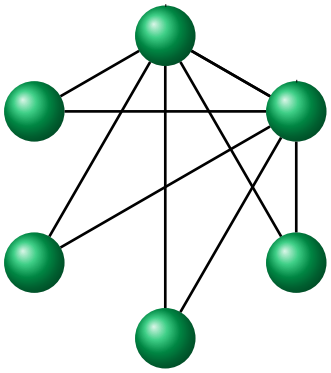


Abbildung 17: Vermaschtes Netz

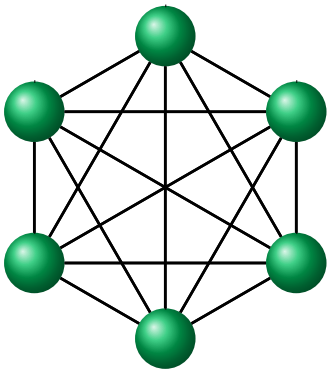


Abbildung 18: Vollvermaschtes Netz

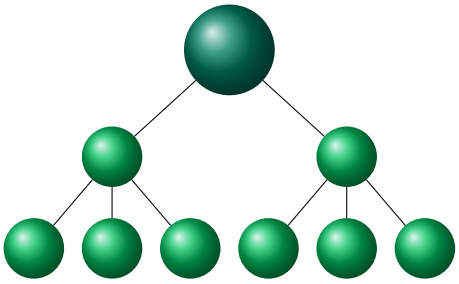


Abbildung 19: Baum Netz

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

- **Bandwith (Bandbreite):** Gibt an, wie viel Daten **theoretisch** zu einem bestimmten Zeitpunkt von einer Quelle übertragen werdne könnten.
- **Throughput (Durchsatz):** Gibt an, wie viel Daten **effektiv** zu einem bestimmten Zeitpunkt von einer Quelle übertragen wurden.
- **Goodput (Datenduchsatz):** Gibt die **Netto-Datenmenge** (ohne Overhead) pro Zeit an, welche von einer Quelle übertragen werden.

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

Die Latenz ist die Zeitverzögerung in einem Netzwerk zwischen der Anfrage und der Antwort. Beispielsweise die Zeit, bei dem mein Rechner die Antwort einer DNS-Anfrage bekommt.
Jitter ist die Zeitverzögerung zwischen einzelnen Anfragen.

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)

- (SW03 - T1) 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?
- (SW03 - T1) 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 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 19.

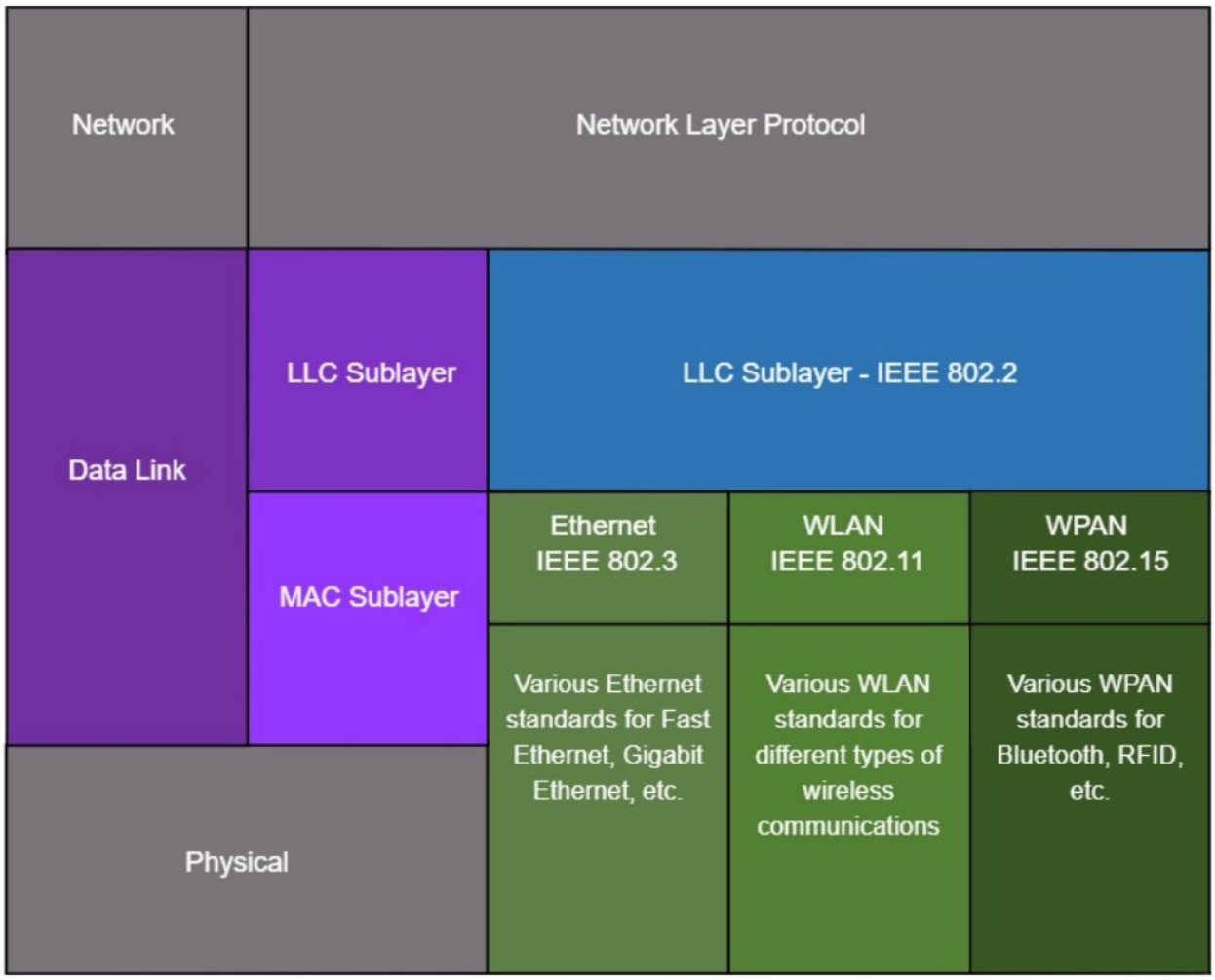


Abbildung 20: Subschichten der Sicherungsschicht / des Data Link Layers (©Cisco)

Was für Felder findet man in der Sicherungsschicht Frame?

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

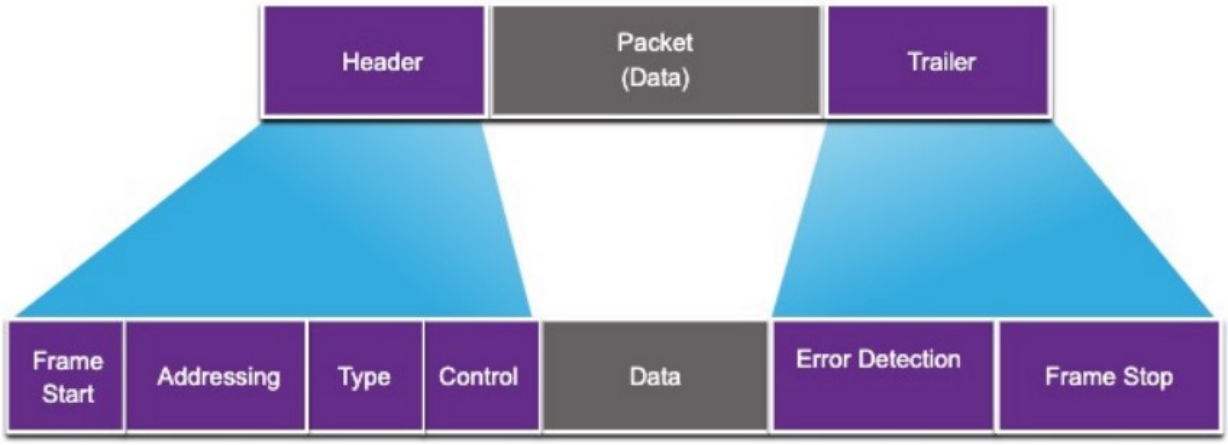


Abbildung 21: Aufbau eines Data Link Frames (©Cisco)

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.

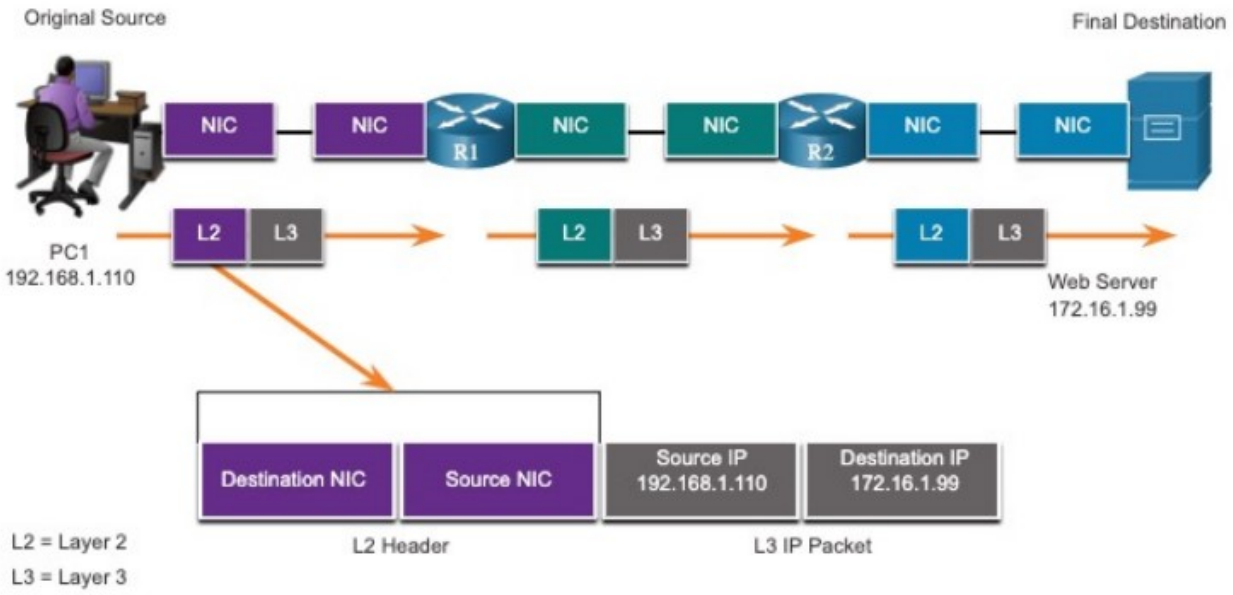


Abbildung 22: MAC-Adressen werden an jedem Knotenpunkt geändert. (©Cisco)

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

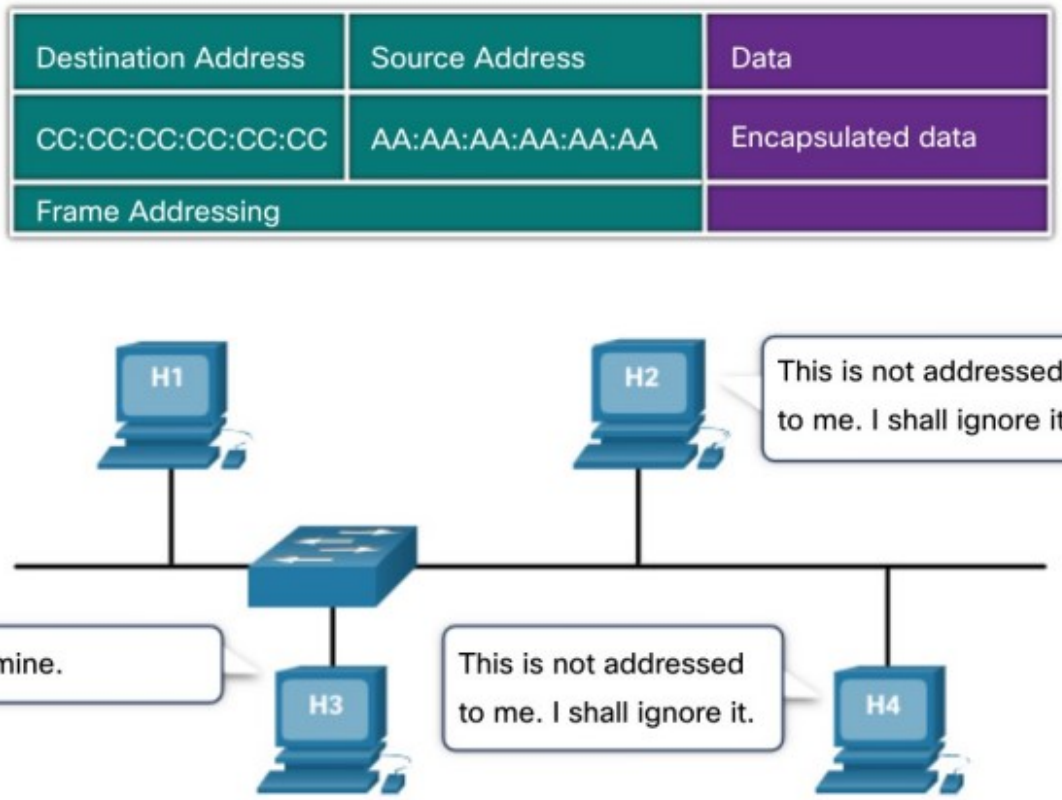


Abbildung 23: Verhalten der Netzwerkkarten (©Cisco)

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 28). 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?

- **Adressierung von Endgeräten**
- Datenkapselung
  - IP kapselt das Transport Layer Segment
  - IP kann entweder ein **IPv4 oder IPv6** Paket verwenden ohne Einfluss auf das Layer 4 Segment zu haben
  - IP Paket **wird von allen Layer 3 Geräten untersucht**, während es durch das Netzwerk übertragen wird
  - Die IP Adressierung ändert sich vom Ursprung (source) bis zum Ziel (destination) nicht, mit Ausnahme wenn NAT verwendet wird (Siehe Glossar: Network Address Translation (NAT))
- **Routen**
- Entkapselung

Siehe auch Schichten des OSI Modells (Seite 11).

Was für Protokolle findet man in der Vermittlungsschicht?

Allgemein *Internet Protocol*. **IP - Internet Protocol (v4&v6), IPsec - Internet Protocol Security, ICMP - Internet Control Message Protocol, IPX - Internet Packet Exchange (veraltet, von Firma Novell)**.

Was sind die wichtigsten Merkmale des IPv4 Protokolls?

Die Funktionsweise vom Internet Protocol ist
- Adressierung von Endgeräten
- Kapselung
- Routing
- Entkapselung

IP ist so gestaltet, dass es einen möglichst geringen „Overhead“ hat. Folglich:
- Es ist verbindungslos
  - Keinen Verbindungsaufbau: Pakete werden einfach gesendet
  - Keine Kontrollinformationen (synchronizations, acknowledgements, etc.)
  - Das Ziel wird das Paket... ***vielleicht***... erhalten

- Es funktioniert nach dem *best effort* Prinzip
  - Keine Garantie für Zustellung
  - Kein Mechanismus um Daten erneut zu senden
  - Unwissen darüber, ob Ziel betriebsbereit ist oder ob es das Paket erhalten hat
- Unabhängig des Übertragungsmediums
  - IP interessiert sich nicht über das Data Link Layer (Sicherungsschicht) oder des Physical Layer (physikalische Schicht)
  - Mit einer Ausnahme: nicht die die maximale Übertragungseinheit, Maximum Transfer Unit (MTU), der Sicherungsschicht überschreiten!
    * MTU muss durch das Data Link Layer gegeben werden
    * Es ist unerwünscht, dass das Paket des Network Layers (Vermittlungsschicht) die MTU des Data Link Layer (Sicherungsschicht) überschreitet
    * Was passiert, wenn das Paket grösser als die MTU ist? (→ Fragmentierung des Paketes in mehrere Pakete)

Wie lange sind IPv4 Adressen?

4 bytes = 32 bits

Wie sind IPv4 Adressen unterteilt?

- Netzwerkadresse
- Hostadresse
- Broadcast Adresse

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

Angenommen, die Hostadresse ist 192.168.10.11 und die Subnetzmaske 255.255.248.0. Man stellt beide Adressen als Binärwerte dar. Die Bits der beiden Adressen werden UND-verknüpft ($1 \wedge 1 = 1$, $0 \wedge 1 = 0$).

	Netzwerk Teil							Host Teil
IPv4 Hostadresse	192	.	168	.	10	.		11
	1100 0000	.	1010 1000	.	0000 1010	.		0000 1011
Subnetzmaske	255	.	255	.	248	.		0
	1111 1111	.	1111 1111	.	1111 1 000	.		0000 0000
IPv4 Netzwerkadresse	192	.	168	.	8	.		0
	1100 0000	.	1010 1000	.	0000 1000	.		0000 0000

Achtung! Die orange 10 gehört eigentlich schon zum Host. Das dritte Byte in der Subnetzmaske zeigt welche Bits zum Netzwerk gehören und welche zum Host. Die Netzwerkadresse ist 192.168.8.0/21, der Hostbereich also 192.168.8.1-192.168.15.254. Betrachtet man die 1000 bei der Subnetzmaske und diese dann auf 1111 „auffüllt“, gibt das ja 15. Deswegen ist der Hostbereich auf diesem Byte 8-15.

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

Die Subnetzmaske stellt die 4 Bytes in dezimaler Form dar. Sie definiert, welcher Bereich zu welchem Netz gehört. Die Slash Notation gibt an, wie viele 1 von links nach rechts es gibt.

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?

Gar nicht. Mittels NAT wird die private Adresse in eine öffentliche getauscht. Jeder Router bekommt vom Internetprovider (z.B. Swisscom, UPC etc.) eine öffentliche Adresse zugewiesen. Öffentliche IP-Adressen sind einzigartig, private kommen aber in jedem LAN vor.

Wieso brauchen wir Private IPv4 Adressen?

Um innerhalb des LANs auf Endgeräte zugreifen zu können. Auch deswegen, weil es inzwischen mehr Netzwerkgeräte gibt als es IP-Adressen zur Verfügung hat.

Was ist eine Loopbackadresse? Wie wird diese Adresse verwendet?

Die Loopbackadresse zeigt auf den eigenen Host, das eigene NIC. Diese wird meistens dazu genutzt, um Programme, die als Server dienen können, lokal zu betreiben oder um zu überprüfen, ob die eigene Netzwerkkarte betriebsbereit ist.

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

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 (169.254.0.0 - 169.254.255.255).

Wie routet ein Host seine eigenen IPv4 Pakete?

Er schickt sie an den Gateway, vorausgesetzt es geht ins Internet. Im LAN geht es direkt an das Ziel.

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

Geht ein Datenpaket ins Internet, „übersetzt“ der Router die private IP-Adresse in eine öffentliche. (Siehe Glossar: NAT)

15 Lernziele (Leitfragen) SW 06

- Wie finde ich meine IPv4 Konfiguration?
- Wie finde ich eine IP-Adresse in Verbindung zu einer URL?
- Wie finde ich heraus, ob ein Host anhand seiner IP oder URL verfügbar ist?
- Wie finde ich heraus, welche Intermediate Network Devices sich zwischen meinem und einem anderen Host befinden, vorausgesetzt es ist eine IPv4 Adresse oder 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

Wie finde ich meine IPv4 Konfiguration?

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 24: 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 25: Adapterkonfiguration in Ubuntu mit `ifconfig`

Wie finde ich eine IP-Adresse in Verbindung zu einer 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 26: `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 27: `nslookup` in Ubuntu

Wie finde ich heraus, ob ein Host anhand seiner IP oder URL verfügbar ist?

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

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

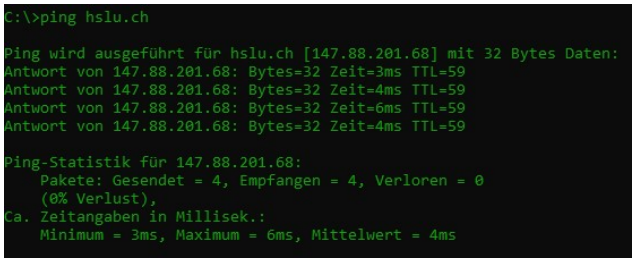


Abbildung 28: `ping` in Windows

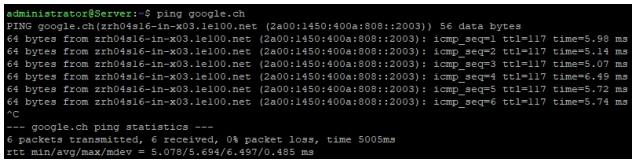


Abbildung 29: `ping` in Ubuntu

Wie finde ich heraus, welche Intermediate Network Devices sich zwischen meinem und einem anderen Host befinden, vorausgesetzt es ist eine IPv4 Adresse oder URL?

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

Unix: `traceroute <IPv4 Adress | URL>`

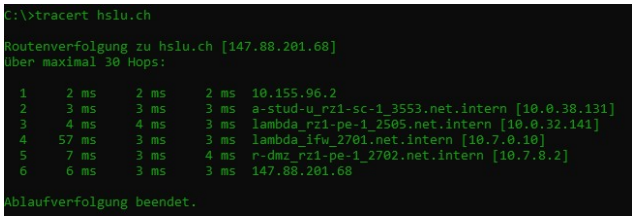


Abbildung 30: `tracert` in Windows

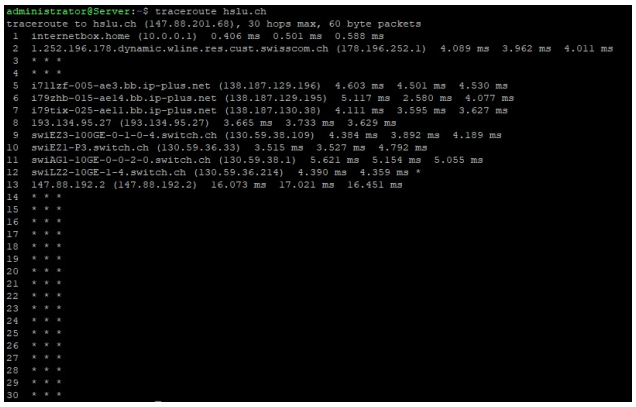


Abbildung 31: `traceroute` in Ubuntu

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

Auf die Länge von 32 bits gibt es lediglich $2^{32} = 4'228'250'625$ IPv4 Adressen. Vergleichsweise weniger als die Hälfte der Weltbevölkerung. Es kommt deshalb zu einem Engpass an verfügbaren öffentlichen IPv4 Adressen. IPv6 mit 128 bits hat $2^{128} = 3.4 \times 10^{38}$. Das ist viel mehr als die geschätzte Anzahl Sandkörner auf der Erde (6.63×10^{222}) oder Galaxien im Universum (10^{22} - 10^{243}

Wie lange sind IPv6 Adressen?

16 bytes = 128 bits, wie bereits erwähnt.

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

Es werden möglichst alle (führenden) Nullen komprimiert. Sind mehrere Hextete (vier Hexadezimalwerte) hintereinander nullen, so fasst man es mit einem doppelten Doppelpunkt (::) zusammen. Dies ist aber nur einmal möglich!

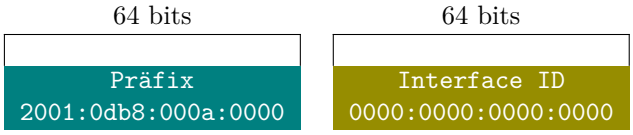
[2] `https://www.why.is/svar.php?id=4803`
[3] `https://www.esa.int/Science_Exploration/Space_Science/Herschel/How_many_stars_are_there_in_the_Universe`

Typ	Format
Normal	2001:0000:0000:1111:0000:0000:0000:0200
Komprimiert	2001:0:0:1111::200

Wie sind IPv6 Adressen unterteilt?

Die Präfixlänge ist in der *Slash Notation* geschrieben und zeigt den Netzwerk Teil der IPv6 Adresse an. Die Präfixlänge kann von 0 bis 128 gehen. Allgemein wird eine Präfixlänge von /64 empfohlen.

Nachfolgend ein Beispiel für `2001:db8:a::/64`



Was für IPv6 unicast Adress Arten gibt es?

Für IPv6 Adressen gibt es folgende Typen:

- Anycast
- Multicast
- Unicast
  - Normalerweise:
    - Global Unicast (GUA) `[2000::/3]`
    - Wenigstens aber:
      - Link-Local (LLA) `[fe80::/10]`
      - Loopback `[::1/128]`
  - Unspecified `[::/128]`
  - Unique Local (ULA) `[fc00::/7]`

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

- 64 bit Präfix
  - **Global Routing Prefix**: Teil der Adresse wird vom Internet Service Provider (ISP) an den Kunden gegeben. Das Global Routing Prefix variiert je nach ISP.
  - **Subnet ID**: Teil zwischen Global Routing Prefix und der Interface ID. Die Subnetz ID wird von Firmen dazu verwendet um Subnetze innerhalb des Netzwerkes zu identifizieren.
- Interface ID: Equivalent zum Host Teil der IPv4 Adresse.

Wie sind IPv6 Global Unicast Addresses (GUAs) unterteilt?

Prefix		Interface ID
Global Routing Prefix	Subnet ID	Interface ID
Durch den ISP gegeben.	Teil zwischen Präfix und Interface ID.	Wie Host Teil in IPv4

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

1. Dual stack - Die Geräte betreiben sowohl IPv4 wie auch IPv6 Protokolle gleichzeitig.
2. Tunneling - Eine Methode um IPv6 Pakete über einem IPv4 Netzwerk zu übermitteln. Das IPv6 Paket ist innerhalb eines IPv4 Paketes gekapselt.
3. Translation - Network Address Translation 64 (NAT64) ermöglicht Geräten mit aktiviertem IPv6 mit Geräten mit IPv4 zu kommunizieren, mit ähnlichen Übersetzungsmechanismen wie das NAT für 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)
- Segmentierung der Daten und wieder zusammenfügen
- Header Information hinzufügen
- Identifizieren, Teilen und verschiedene Konversationen managen
- Segmentierung

Siehe auch Schichten des OSI Modells (Seite 11).

Was für Protokolle findet man in der Transportschicht?

- TCP - Transmission Control Protocoll
  - nicht zeitkritisch, dafür zuverlässig
    - Email, Webbrowsing
    - Wichtig, dass alle Datenpakete ankommen
- UDP - User Datagram Protocol
  - zeitkritisch, aber unzuverlässig → nicht alle Pakete müssen ankommen, um das Mitgeteilte zu verstehen
    - Realtime Apps
    - Telefonanrufe
    - Streams

Was sind die wichtigsten Merkmale des TCP Protokolls?

- 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

Was sind die wichtigsten Merkmale des UDP Protokolls?

- minimaler „Overhead“

- ohne Zuverlässigkeit - without Reliability
- ohne Durchsatzkontrolle - without Flow Control

Wozu werden Ports in der Transportschicht verwendet?

Die Protokolle verwenden Ports um **mehrfache, gleichzeitige Verbindungen** zu verwalten. Der Source-Port gehört zu der Anwendung auf dem Client, der Destination-Port ist mit der Anwendung auf dem Remote-Server assoziiert. Eine Portnummer enthält **16 bits**, also gibt es $2^{16} = 65'536$ verschiedene Portnummern. Dabei gibt es 3 Gruppen:

Gruppe	Nummernereich	Beschreibung
Low / Well-known Ports	0-1'023	Reserviert für bekannte Dienste und Anwendungen wie Browser, Email Clients und Remote Access Clients. Ermöglicht einen Client einen Service einfach zu ermitteln.
Registered Ports	1'024-49'151	Von der IANA - Internet Assigned Numbers Authority vergeben. Individuelle Anwendungen, die ein Benutzer installiert hat. Clientseitig oft als kurzlebige Ports verwendet.
Private and/or Dynamic Ports	49'152-65'535	Kurzlebige Ports. Dynamisch vom Host-Betriebssystem als Source-Ports zugeordnet, wenn eine Verbindung aufgebaut wird.

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?

Siehe Wozu werden Ports in der Transportschicht verwendet?, Seite 37.

Wie realisiert TCP zuverlässige Verbindungen?

Daten werden segmentiert und „nummeriert“ gesendet. Weil Pakete verschiedene Routen nehmen können, können schon mal Pakete verloren gehen. Der Zielhost ordnet die Pakete und bemerkt fehlende Pakete und fordert diese an.

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?

Client A möchte Verbindung mit Client B herstellen:

1. Send SYN (SEQ=100 CTL=SYN) ⇒ SYN received
2. SYN, ACK received ⇐ Send SYN, ACK (SEQ=300 ACK=101 CTL=SYN, ACK)
3. Established (SEQ=101 ACK=301 CTL=ACK) ⇒ ACK received

Wie werden Verbindungen in TCP richtig beendet?

1. Send FIN ⇒ FIN received
2. ACK received ⇐ Send ACK
3. FIN received ⇐ Send FIN
4. Send ACK ⇒ ACK received

Was ist der Zweck von «Selective Acknowledgements»?

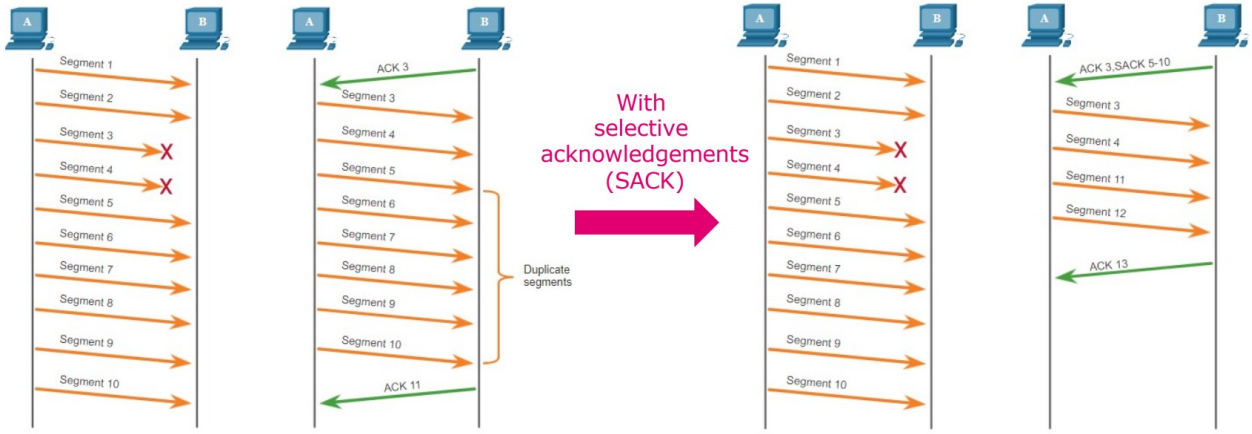


Abbildung 32: Datenverlust und nochmaliges Versenden (©Cisco)

Teil VII
SW 08-09 T1-T5

19 Lernziele (Leitfragen) - T1

- Wie wird eine DNS Anfrage bearbeitet?
- Was ist der Unterschied zwischen rekursiver und iterativer DNS?
- Was für DNS Record Arten gibt es?
- Was ist die Topologie des DNS Systems? Ist es zentralisiert?
- Wie kann ich direkt eine DNS Anfrage aus meinem Computer ausführen?
- Was sind die Sicherheitsmerkmale von DNS?
- Was für Sicherheitserweiterungen gibt es für DNS?
- Wie geht DNS mit den verschiedenen IP Versionen um?

20 Antworten

Wie wird eine DNS Anfrage bearbeitet?

//TODO Abbildung 15: Grafik aus Unterricht

- Forward Lookup
  - Ich kenne die IP noch nicht
  - Steps
    1. Client (DNS Client, sucht etwas)
       * Client muss wissen, welchen Server er kontaktieren muss
       * Client fragt nach www.yahoo.com
    2. ISP (Internet Service Provider)
       * Erhält die Anfrage des Clients
       * Kennt die www.yahoo.com noch nicht
       * Der ISP geht zu einem der Root Server
    3. Root Server
       * Erhält die Anfrage des ISP und sagt, frag den .com Server
    4. Dieser meldet sich beim ISP und der ISP meldet an den Client, die IP des Servers von yahoo.com
    5. Reverse Lookup
  - Ich kenne den Host Name aber die IP noch nicht
    * DNS Cache dient dazu, dass nicht jedes Mal das ganze Spiel gemacht werden muss, werden die Angaben zwischengespeichert

Was ist der Unterschied zwischen rekursiver und iterativer DNS?

Recursive Query //TODO Abbildung 16: Screenshot YT https://www.youtube.com/watch?v=PS0UppB3-fg

Iterative Query //TODO Abbildung 17: Screenshot YT https://www.youtube.com/watch?v=PS0UppB3-fg

Was für DNS Record Arten gibt es?

- CNAME
- A
- AAAA
- MX Record
- TXT
- SRV

Was ist die Topologie des DNS Systems? Ist es zentralisiert?

Es ist verteilt, verschiedene Server haben Zugriff.

Wie kann ich direkt eine DNS Anfrage aus meinem Computer ausführen?

Mittels NS Lookup kann man die IP oder Domain eines bestimmten Computers herausfinden.

Was sind die Sicherheitsmerkmale von DNS?

DNS kennt nur System innerhalb des Netzwerks. Initial wurden keine Sicherheitsmechanismen eingebaut. Diese wird gewährleistet durch die Anbieter, z. B. von CloudFlare. Diese bieten Schutz vor DDoS-Attacken, DNS-Spoofing etc. an.

Was für Sicherheitserweiterungen gibt es für DNS?

Domain Name System Security Extensions (DNSSEC) DNSSEC verhindert, dass Angreifer die Antworten auf DNS-Anfragen verfälschen oder manipulieren.

Wie geht DNS mit den verschiedenen IP Versionen um?

- A für ipv4
- AAAA für ipv6

21 Lernziele (Leitfragen) - T2

- Wie erhält ein Host seine IPv4 Konfiguration mit DHCP?
- Welche Nachrichten des DHCP Protokolls sind Broadcasts und wieso?
- Was passiert, wenn mehr als ein DHCP Server in dem lokalen Netzwerk verfügbar ist? Ist das möglich? Ist das wünschenswert?
- Welche Parameter werden typischerweise von einem DHCP Server vergeben?
- Was macht ein Host, wenn er keine IPv4 Konfiguration via DHCP bekommt? Kann er mit anderen Hosts kommunizieren?
- Wie erhält ein Host seine IPv6 Konfiguration mit DHCPv6?

22 Antworten

Wie erhält ein Host seine IPv4 Konfiguration mit DHCP?

- DHCP oder «Dynamic Host Configuration Protocol»wird in der Netzwerktechnik verwendet, um einem Client alle nötigen Netzwerkinformationen zuzuweisen, wie:
  - IP-Adresse
  - Subnetzmaske
  - Standardgateway
  - Domain Name Server (DNS)
- Es können mehrere DHCP Server in einem Netzwerk vorhanden sein, dies ist für die Availability des Services von Vorteil, sollte ein DHCP Server Probleme aufweisen
- Discover-Offer-Request-Acknowledgement (DORA)
  - DHCP Discover als Broadcast
  - DHCP Offer
    - Mit Client MAC, IP, Subnetz, Gateway, Leasttime und IP des DHCP
  - DHCP Request als Broadcast
    - Annahme der IP Daten
  - DHCP Acknowledgment
    - Bestätigung mit weiteren Optionen

Welche Nachrichten des DHCP Protokolls sind Broadcasts und wieso?

- Discover, weil er das Netzwerk noch nicht kennt und die IP des DHCP Servers braucht
- Request, weil alle im Netz wissen müssen, dass diese IP nun vergeben wurde

Was passiert, wenn mehr als ein DHCP Server in dem lokalen Netzwerk verfügbar ist? Ist das möglich? Ist das wünschenswert?

- Hat man mehrere DHCP Server im Netz, gibt es mehrere Offers
- Mittels Request der als Broadcast fungiert werden alle DHCP Servers darüber informiert, dass der Client diese gewählt hat

Welche Parameter werden typischerweise von einem DHCP Server vergeben?

IP, Subnetz, Standardgateway

Was macht ein Host, wenn er keine IPv4 Konfiguration via DHCP bekommt? Kann er mit anderen Hosts kommunizieren?

- Werden keine statischen IP-Adressen an einen Client vergeben, weisen sich die Clients bei einem Ausfall vom DHCP automatisch eine IP-Adresse in folgenden IP-Range zu: 169.254.0.0 - 169.254.255.255.
- Diese sogenannten Link-Local Adressen ermöglichen eine Kommunikation in einem gemeinsamen lokalen Netzwerk

Wie erhält ein Host seine IPv6 Konfiguration mit DHCPv6?

Für DHCPv6 gibt es zwei verschiedene Verfahren:
- **Stateless Config:** Router verteilt die IPv6 Präfix und der DHCPv6 die restlichen Parameter
- **Statefull Config:** Der DHCPv6 verteilt IPv6 Präfix als auch die restlichen Parameter Für IPv6 wird das Protokoll DHCPv6 benützt

23 Lernziele (Leitfragen) - T3

- Wie wird ein E-Mail mit SMTP verschickt (end-to-end)?
- Wie wird der Nutzer des SMTP Servers authentifiziert?
- Welche Sicherheitseigenschaften hat SMTP? Was für Sicherheitserweiterungen gibt es?
- Kriegt die Empfängerin das E-Mail sobald es von dem SMTP Server empfangen wird?
- Wie wird auf E-Mails mit POP3 zugegriffen?
- Wie wird auf E-Mails mit IMAP zugegriffen?
- Was sind die Hauptunterschiede zwischen POP3 und IMAP? Wann wird es empfohlen sie zu verwenden?

24 Antworten

Wie wird ein E-Mail mit SMTP verschickt (end-to-end)?

SMTP - Simple Mail Transfer Protocol gehört zur Anwendungsschicht, bedeutet Simple Mail Transfer Protocol und dient, wie der Name sagt, zum Austauschen von E-Mails. SMTP funktioniert über **TCP**. Kann auch als Gedankenstütze mit Sending-Mail-To-People genutzt werden.

Schritte:
1. Ein Mail-Client (Outlook) sendet E-Mail an SMTP Server.
   - Wenn Gmail genutzt wird, ist dieser Server smtp.gmail.com
2. Dieser SMTP-Server sendet dann die Mail an den SMTP Server des Empfängers.
3. E-Mail wird vom SMTP Server des Empfängers erhalten.
4. Hier endet das SMTP. Um die E-Mails abzurufen, kommen dann IMAP/POP3 zum tragen.

Wie wird der Nutzer des SMTP Servers authentifiziert?

- Authentifizierung: Beispiel mit Brief Absenderadresse, die vom Versender angepasst werden kann. Dies soll verhindert werden mit SMTP.
- SMTP Auth ist Extension von Extended SMTP was wiederum eine Erweiterung von SMTP ist.
- Somit können nur noch Vertrauenswürdige Nutzer Emails über diesen Sender Server versenden.
- Statt über den Standardport 25/TCP wird über den Port 587 kommuniziert. Obligatorische Grundlage für E SMTP. Verschiedene Authentifizierungsmechanismen (PLAIN, LOGIN, CRAM-MD5).

//TODO Abbildung 18: SMTP Eigene Grafik

Welche Sicherheitseigenschaften hat SMTP? Was für Sicherheitserweiterungen gibt es?

Eine Vertraulichkeit, Authentizität und Integrität von E-Mails kann durch SMTP allein nicht gewährleistet werden. Clientseitige Verfahren müssen genutzt werden. Ansonsten sind die Absender und Empfänger fälschbar und die E-Mailinhalte grundsätzlich lesbar und veränderbar.

- **S/MIME** ist eine Technologie, die **E-Mails verschlüsselt**, um sie vor unerwünschtem Zugriff zu schützen. Ausserdem können die **E-Mails digital signiert** werden, um den Absender als legitim zu verifizieren.
  - Zugemüse: Meistens sind S/MIME-Zertifikate kostenpflichtig, da sie als Paket auf Corporate-Level angeboten werden. Actalis[4] ist eine Root Certificate Authority und bietet kostenlose Zertifikate für ein Jahr aus, welche man jeweils erneuern kann.
- PGP (Pretty Good Privacy) ist eine alternative Methode E-Mails zu signieren und verschlüsseln. Anders als S/MIME, wo eine Root Certificate Authority Zertifikate ausstellt, basiert PGP auf ein Web of Trust.
  - Zugemüse: Wer sich interessiert, kann hier eine Infografik[5] anschauen und hier eine einfache Anleitung[6] lesen, um PGP bei sich aufzusetzen. GPG4Win[7] bietet mit Kleopatra eine benutzerfreundliche Oberfläche zum erstellen und verwalten seiner Schlüssel (auch S/MIME).
- TLS: Verschlüsselt die Verbindung und Daten während der Übertragung von Punkt A nach Punkt B. Der Schlüsselaustausch findet im Hintergrund statt, ohne Einwirken des Benutzers.

Kriegt die Empfängerin das E-Mail sobald es von dem SMTP Server empfangen wird?

Wenn ein Server eine Nachricht erhält, legt er die Nachricht entweder lokal ab oder leitet sie einem anderen E-Mail-Server weiter. Ist der Destination E-Mail-Server nicht online, oder beschäftigt, so sendet SMTP die Nachricht zu einem späteren Zeitpunkt. Wenn sie nach einer bestimmten Zeit immer noch nicht zugestellt werden kann, dann wird sie dem Sender als unzustellbar zurückgeschickt.

Wie wird auf E-Mails mit POP3 zugegriffen?

POP3 - Post Office Protocol Version 3 ist das Übertragungsprotokoll für E-Mails und stammt aus dem Jahr 1996. Dabei verbindet sich der POP3 Client mit dem Mailserver und authentifiziert sich durch ein **Passwort**. Sodann ruft der Client neue Nachrichten für die Mailadresse ab und der Server sendet diese E-Mails an den Client. Nach der Übertragung löscht der Server die Nachrichten.

Wie wird auf E-Mails mit IMAP zugegriffen?

Bei IMAP - Internet Message Access Protocol basierten Mailclients werden die Mails sowie die Ordnerstrukturen und Einstellungen auf einem Mailserver gespeichert. Der Client holt sich dann die einzelnen Informationen erst vom Server, wenn sie gebraucht werden. Eine normale IMAP Kommunikation beginnt mit einem **Login**, wobei sich der Client mit einem **Username** und einem **Password** beim Mailserver authentifiziert. Danach kann der Client dem Server diverse Anfragen stellen, um Infos über die Mails zu bekommen oder um die Mails auf dem Server zu bearbeiten (verschieben, löschen, markieren, etc.)

Was sind die Hauptunterschiede zwischen POP3 und IMAP? Wann wird es empfohlen sie zu verwenden?

Beim POP3 werden die Daten lokal abgespeichert und auf dem Server gelöscht. Mit dem IMAP ruft der Client die Daten vom Server ab. Möchte man **wenig Bandbreite** nutzen, sollte man **POP3** verwenden. Will man mit **mehreren Devices** auf die Mails zugreifen und ein sicheres Backup haben, empfiehlt es sich das **IMAP** zu verwenden.

25 Lernziele (Leitfragen) - T4

- Wie wird auf eine Website mit HTTP(S) zugegriffen?
- Was ist der Unterschied zwischen HTTP und HTTPS?
- Was sind die Hauptmerkmale von TLS? Wie funktioniert TLS (hohes Niveau)?

[4] `https://extrassl.actalis.it/portal/uapub/freemail?lang=en`
[5] `https://emailselfdefense.fsf.org/en/infographic.html`
[6] `https://emailselfdefense.fsf.org/en/index.html`
[7] `https://www.gpg4win.org/`

- Was sind andere wichtige Verwendungen von HTTP (ausser Websites zuzugreifen)?
- Was ist ein REST API?
- Was sind die Hauptmethoden von HTTP?
- Wie funktioniert ein REST API?
- Nenne ein Beispiel von einem REST API Endpoint, der die GET Methode verwendet.
- Nenne ein Beispiel von einem REST API Endpoint, der die POST Methode verwendet.
- Nenne ein Beispiel von einem REST API Endpoint, der die PUT Methode verwendet.

26 Antworten

Wie wird auf eine Website mit HTTP(S) zugegriffen?

Nach der DNS-Auflösung wird mit der GET Methode von HTTP(s) auf Webseite über den Port 80 (443 bei HTTPS) zugegriffen. Wird diese GET Anfrage vom Webserver akzeptiert, so sendet er erst Inhalt des Headers des Bereitgestellten HTML Dokuments und im Anschluss den Body. Der Body repräsentiert den Inhalt einer Webseite und ist das, was der User im Interface seines Webbrowsers sieht. Im Anschluss wird die Verbindung beendet.

Was ist der Unterschied zwischen HTTP und HTTPS?

Das „S“ von HTTPS steht für Secure. Bei einer HTTPS Verbindung wird das Webbrowser Zertifikat zum Verschlüsseln der Verbindung verwendet. Somit ist die Verbindung über SSL/TLS (Transport Layer Security) gesichert und die gesendeten Daten, können nicht oder nur schwer abgehört werden. HTTPS ist heutzutage beinahe ein *de facto* Standard für alle offiziellen Webseiten.

Was sind die Hauptmerkmale von TLS? Wie funktioniert TLS (hohes Niveau)?

TLS (Transport Layer Security) ist ein Protokoll der 5 Schicht, welches zuständig ist für eine sichere Datenübertragung im Internet. Nebst dem HTTPS Protokoll können auch Protokolle wie SMTP, FTP, POP3, etc. das TLS Protokoll verwenden. Die Funktion ist in **zwei Phasen** unterteilt: Die **erste Phase** ist der **Verbindungsaufbau** und die **zweite Phase** ist die **Übermittlung**.

Es wird mit zwei verschiedenen Schlüsseln gearbeitet (Private und Public Key).
- Der Public Key vom Empfänger ist jeweils dem Sender bekannt.
- Mit dem Public Key werden Daten verschlüsselt und mit dem Private Key werden die Daten entschlüsselt.
- Bevor die Verschlüsselung startet, wird überprüft, ob der Empfänger den echten öffentlichen Schlüssel mitteilt. Die Überprüfung findet mit Hilfe von den Zertifikaten statt.

Was sind andere wichtige Verwendungen von HTTP (ausser Websites zuzugreifen)?

Rest API → Schnittstellen bzw. Webservices verwenden HTTP.

Was ist ein REST API?

- REST - Representational State Transfer
- API - Application Programming Interface → Programmierschnittstelle, die den Austausch von Informationen ermöglicht, wenn diese sich auf unterschiedlichen Systemen befinden.

REST ist ein Software-Architektur-Stil der anleitet, wie internetbasierte Systeme sich zu verhalten haben. Beispielsweise welche Standards, wie JSON oder XML, sich wie zu verhalten haben und wie Daten über HTTP-Methoden auszutauschen sind etc. Die API bietet den Zugang zu den Ressourcen.

Was sind die Hauptmethoden von HTTP?

GET, POST, PUT, DELETE, HEAD, CONNECT, OPTIONS, TRACE

Wie funktioniert ein REST API?

Die REST Schnittstelle nutzt HTTP-Anfragen, um mit GET, POST, PUT und DELETE auf Informationen zuzugreifen. Jede URL wird als Anforderung bezeichnet, während die zurückgegeben Daten die Antwort sind. Sobald eine Client-Anfrage auf dem Server eingegangen ist, sucht die REST-API nach einer Antwort und liefert sie unverzüglich.

Nenne ein Beispiel von einem REST API Endpoint, der die GET Methode verwendet.

Aufrufen einer Ressource → Bsp: Facebook Profil aufrufen

Nenne ein Beispiel von einem REST API Endpoint, der die POST Methode verwendet.

Anlegen einer Ressource → Bsp: Facebook Account erstellen

Nenne ein Beispiel von einem REST API Endpoint, der die PUT Methode verwendet.

Verändern einer Ressource → Bsp: Facebook status ändern

27 Lernziele (Leitfragen) - T5

- Wofür wird SSH verwendet?
- Wie funktioniert SSH (hohes Niveau)?
- Was für Nutzerauthentifizierungsoptionen gibt es? Was wir empfohlen?
- Was ist RDP?
- Wie funktioniert RDP?
- Was ist VNC?
- Wie funktioniert VNC?
- Was ist VDI?
- Wie funktioniert VDI?
- Nenne Beispiele von kommerziellen VDI Lösungen
- (Zusatz) Was ist der Unterschied zwischen RDP und VNC?

28 Antworten

Wofür wird SSH verwendet?

Secure Shell (SSH) bezeichnet ein Protokoll, in welchem Clients auf entfernte Hosts zugreifen können. Administratoren können damit beispielsweise einen Computer durch Fernzugriff konfigurieren und betreuen. Wie der Name „Shell“ bereits andeutet, ist die GUI eine textbasierte Kommando-Konsole. Die Shell selbst ist ein Kommando-Übersetzer und gibt Instruktionen an den Betriebssystem-Kern (Kernel) weiter.

Wie funktioniert SSH (hohes Niveau)?

SSH gibt es standardmässig auf Linux. Neue Windowsversionen, wie Windows 11 und Windows 10 ab Update 1809, bieten einen SSH-Server auf Basis von OpenSSH. Verbindung mit SSH benötigt IMMER zwei Programme:

- Server wie z.B. OpenSSH Server auf entferntem Computer
- Client wie SSH (Linux) oder PuTTY (Windows) auf lokalem Rechner

Ablauf:

1. Verbindungsaufbau zum Server via Hostname, Domain oder IP
2. Wird Anfrage entgegengenommen, muss Nutzer mit Namen & Passwort oder durch digitales Zertifikat identifizieren
3. Dann steht textbasierte Umgebung (Shell) auf Server zur Verfügung und es kann gearbeitet werden

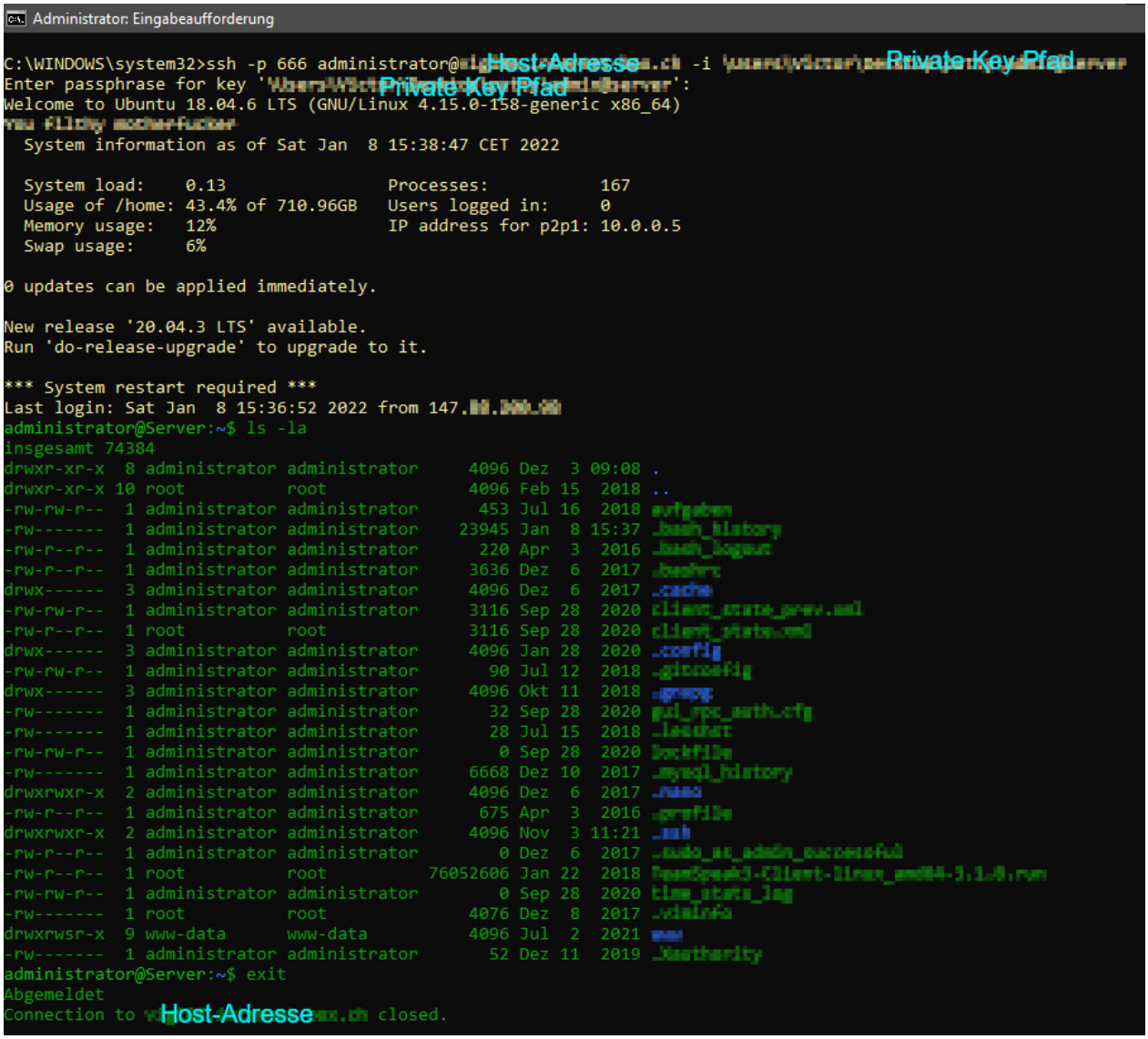


Abbildung 33: SSH von cmd.exe zu Linux-Server

Was für Nutzerauthentifizierungsoptionen gibt es? Was wir empfohlen?

- SSH
- 2-Factor-Authentication / Multi-Factor-Authentication (MFA)
  - Passwort und Email/SMS Code
  - Doppelte Sicherheit
- External Keys
- OAuth - Open Standard Authorization Protocol
  - Open Authorization ist der Name zweier verschiedener offener Protokolle, die eine standardisierte, sichere API-Autorisierung für Desktop-, Web- und Mobile-Anwendungen erlauben. Ein User kann mit Hilfe dieses Protokolls einer Anwendung den Zugriff auf seine Daten erlauben (Autorisierung), die von einem anderen Dienst bereitgestellt werden, ohne geheime Details seiner Zugangsberechtigung (Authentifizierung) dem Client preiszugeben. Der User kann so Dritten gestatten, in seinem Namen einen Dienst zu benutzen. Typischerweise wird dabei die Übermittlung von Passwörtern an Dritte vermieden.[3]
- SAML - Security Assertion Markup Language
  - Dia SAML ist ein XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen. Sie stellt Funktionen bereit, um sicherheitsbezogene Informationen zu beschreiben und zu übertragen.
    - Single Sign-On - ein Benutzer ist nach der Anmeldung an einer Webanwendung automatisch auch zur Benutzung weiterer Anwendungen authentifiziert
    - Verteilte Transaktionen – mehrere Benutzer arbeiten gemeinsam an einer Transaktion und teilen sich

die Sicherheitsinformationen
    * Autorisierungsdienste – die Kommunikation mit einem Dienst läuft über eine Zwischenstation, die die Berechtigung überprüft

Was ist RDP?

RDP - Remote Desktop Protocol ermöglicht den Zugriff auf einen entfernten Desktop.

Wie funktioniert RDP?

User kann Aktionen auf dem entfernten Computer als Terminal durchführen. RDP öffnet einen dedizierten Kanal zwischen zwei Verbundenen Geräten und nutzt immer Port 3389. Via TCP/IP werden die Kommandos ausgetauscht.. RDP verschlüsselt alle Daten, damit die Verbindung noch sicherer ist.

Was ist VNC?

VNC - Virtual Network Computing wird im übergeordneten als Remote Desktop Sharing bezeichnet. User können damit den Computer aus dem Geschäft zuhause anzeigen lassen.

Wie funktioniert VNC?

- Funktioniert im Client-Server Modell
- User muss nur einen VNC Viewer auf einem lokalen Computer (client) haben. Dieser verbindet sich von entfernt auf einen anderen Computer, wo VNC als Server installiert ist.
- VNC ist Plattformunabhängig, beide Computer müssen lediglich TCP/IP aktiviert haben und offene Standard-Ports (TCP 5800, 5900) mit zugelassenem Traffic.

//TODO Abbildung 19: VNC, Screenshot von vpnchecked.com

(Zusätzlich) Was ist der Unterschied zwischen RDP und VNC?

- Grundsätzlich: zwei verschiedene Protokolle
  - RDP: «Client zu Client»
  - VNC: «Client zu Server»
- RDP ist schneller und eignet sich für Virtualisierung besser
- RDP unterstützt SSL/TLS und bekommt Security Updates
- Nicht jede VNC Software akzeptiert SSH, VNC gibt den Clients «Full Access»

//TODO Quelle https://www.parallels.com/blogs/ras/vnc-vs-rdp/

Was ist VDI?

Die VDI - Virtual Desktop Infrastructure sorgt dafür, dass ein Geschäftscomputer von überall her zugreifbar ist.

Wie funktioniert VDI?

- Komplexer als einfache RDP weil noch Server etc. virtualisiert drinnen mithängen.
- Desktop OS ist meisten in einem Zentralisierten Server oder einem physischen Datencenter gehostet.
- Es gibt zwei Arten:
  - Persistent Virtual Desktop - Speichern für Zukünftige Nutzung, traditioneller Desktop
  - NonPersistent - Einheitliche Desktops, wo man auf das zugreifen kann, was man braucht. Desktop geht zurück in Einheitlichen Status nachdem der User sich ausloggt

//TODO Quelle azure.microsoft.com

Nenne Beispiele von kommerziellen VDI Lösungen

- Citrix Workspace
- VirtualBox
- VM Fusion
- Amazon WorkSpaces

Teil VIII
SW 11

29 Lernziele (Leitfragen)

- Was sind typische Informationssicherheitsziele?
- Wozu braucht man Netzwerksicherheit?
- Was ist eine Bedrohung (Threat)?
- Was ist ein Asset?
- Was ist eine Schwachstelle (Vulnerability)?
- Was ist Risiko (im Kontext der Informationssicherheit)?
- Was ist ein „mitigation technique“?
- Wieso ist es so schwierig völlig sichere Systeme zu erstellen?
- Was ist Vertraulichkeit und wie ist sie normalerweise (technisch) erreicht?
- Was ist Integrität und wie ist sie normalerweise (technisch) erreicht?
- Was ist Verfügbarkeit und wie ist sie normalerweise (technisch) erreicht?
- Was ist Authentifizierung und wie ist sie normalerweise (technisch) erreicht?
- Was ist „non-repudiation“ und wie ist es normalerweise (technisch) erreicht?
- Was ist der Unterschied zwischen symmetrischer und asymmetrischer Kryptografie?
- Welche Kryptografieart (symmetrisch oder asymmetrisch) wird für digitale Unterschriften verwendet?
- Geben Sie ein Beispiel eines symmetrischen kryptografischen Algorithmus
- Geben Sie ein Beispiel eines asymmetrischen kryptografischen Algorithmus

30 Antworten

Anmerkung: viel Text wurde aus meiner eigenen ISF Zusammenfassung auf `https://github.com/vigi86/HSLU_Zusammenfassungen` entnommen. Das Fach „Information Security Fundamentals“ behandelt, wer hätte es gedacht, Informationssicherheit.

Was sind typische Informationssicherheitsziele?

Verfügbarkeit
- **Verfügbarkeit** ist gewährleistet, wenn in der vom Benutzer gewünschten Zeit auf Dienste oder Informationen zugegriffen werden kann (Ausfallquote)
- Engl.: **Availability**

Integrität
- **Integrität** ist gewährleistet, wenn Daten oder Systeme nicht unautorisiert oder zufällig manipuliert oder verändert werden können (Datensicherheit)
- Engl.: **Integrity**

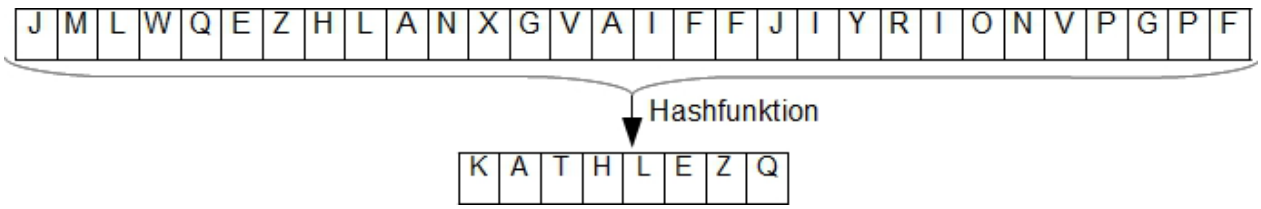


Abbildung 34: Hashfunktion (Quelle: ISF Folien, Prof. Dr. Hänggi)

Verbindlichkeit
- **Verbindlichkeit**liegt vor, wenn eine Handlung eindeutig einer Person zugeordnet und von dieser nicht geleugnet werden kann
- Engl.: **Non-Repudiation**

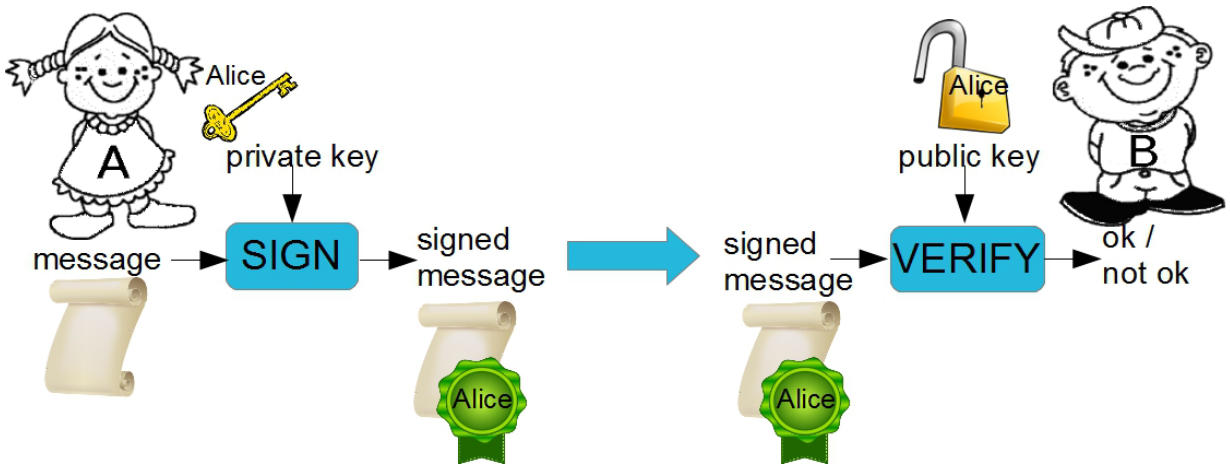


Abbildung 35: Identitätsbeweis mittels Signatur (Quelle: ISF Folien, Prof. Dr. Hänggi)

Vertraulichkeit

- **Vertraulichkeit** ist gegeben, wenn sichergestellt werden kann, dass Informationen nicht durch unautorisierte Personen, Instanzen oder Prozesse eingesehen werden können
- Engl.: **Confidentiality**

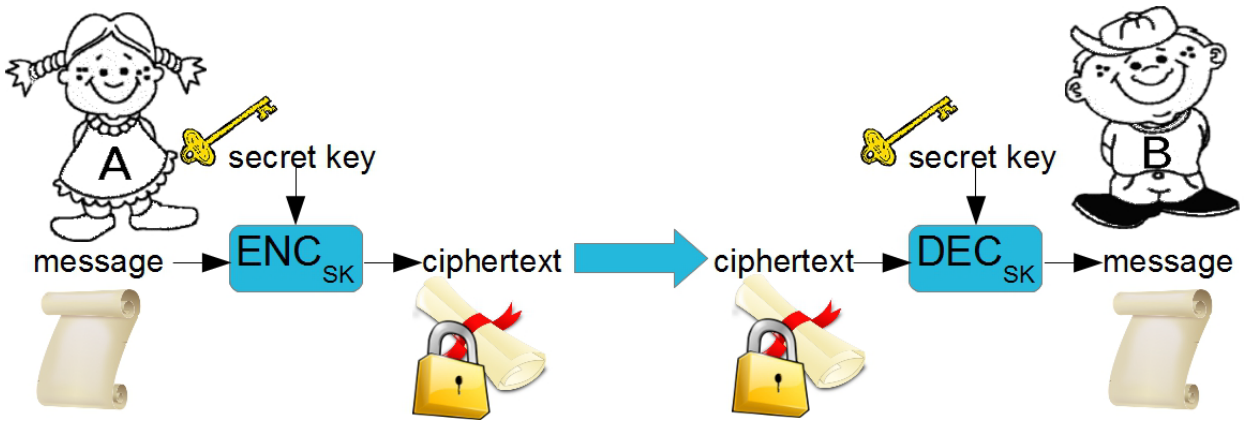


Abbildung 36: Symmetrisches Verschlüsselungsverfahren (Quelle: ISF Folien, Prof. Dr. Hänggi)

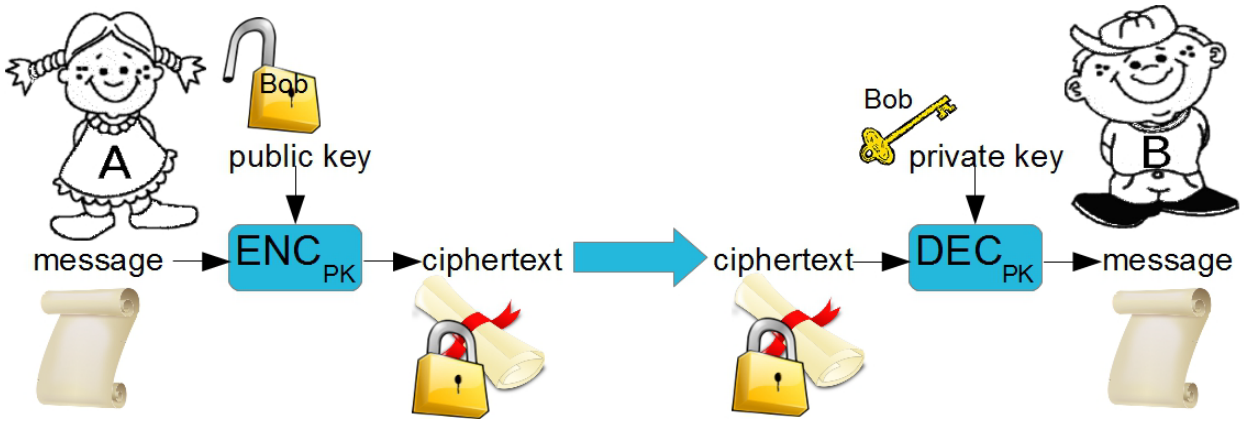


Abbildung 37: Asymmetrisches Verschlüsselungsverfahren (Quelle: ISF Folien, Prof. Dr. Hänggi)

Identität / Authentizität

- **Identität:** „Beim Menschen bezeichnet Identität die ihn kennzeichnende und als Individuum von anderen Menschen unterscheidende Eigentümlichkeit seines Wesens.“[3] Informationstechnische Anwendungen: Fingerabdruck, Iris, Handvenen.
- **Authentizität:** „In der Informationssicherheit bezeichnet Authentizität die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit. Die Überprüfung einer behaupteten Eigenschaft wird als Authentifikation bezeichnet. Durch Authentifikation des Datenursprungs wird nachgewiesen, dass Daten einem angegebenen Sender zugeordnet werden können, was durch digitale Signaturen ermöglicht werden kann.“[3] Informationstechnische Anwendung:

→ Siehe unten Authentisierung, Authentifizierung und Autorisierung.

Wichtige Grundbegriffe sind Zutritts-, Zugangs-, Zugriffskontrolle
- ***Zutrittskontrolle:*** Schutz des physischen Systems (Bsp. Serverraum, Schlüssel)
- ***Zugangskontrolle:*** Schutz des logischen Systems (Bsp. Betriebssystem, Login)
- ***Zugriffskontrolle:*** Daten-bezogen; Schutz der Operationen (Bsp. Dateisystem, Benutzerrechte)

Begriffe

Bei der Zugriffskontrolle unterscheidet man drei Begriffe: Authentisierung, Authentifizierung und Autorisierung.

Authentisierung Die Authentisierung ist ein **Nachweis einer Person**, dass sie tatsächlich die Person ist, die sie vorgibt zu sein.
- geheime Information, dass nur ihr bekannt ist (Passwort)
- Identifizierungsgegenstand (z.B. Identitätskarte)
- sie ist selbst das Identifizierungsobjekt (z.B. Fingerabdruck)

Methoden der Authentisierung
- Etwas, das ich weiss (**Wissen**)
  - Passwort
  - Pin
  - Sicherheits- / Geheimfragen
- Etwas, das ich habe (**Besitz**)
  - Physikalischer Schlüssel
  - Magnetstreifenkarte
  - Hardware-Token[8]
- Etwas, das ich bin (**Eigenschaft** / körperliches Merkmal)
  - Foto
  - Fingerabdruck
  - Iris
- Etwas, das ich kann (**Fähigkeit**)
  - Unterschrift
  - Stimmenerkennung (Sprechen)

Wissen

Vorteil
- man benötigt keine zusätzlichen Hilfsmittel

Nachteil
- kann vergessen oder (v)erraten werden (Passwort, Geheimfragen)

Besitz

Vorteil
- kann benutzerindividuelle Daten speichern
- kann sich selbst schützen und aktiv verändern (SecurID, Smartcard)

Nachteil
- Verwaltung des Besitzes ist unsicher und muss mitgeführt werden
- kann verloren gehen (Schlüssel, Karte, HW-Token)

[8] z.B. Kartenleser für E-Banking

Eigenschaft / körperliches Merkmal

Vorteil
- kann nicht verloren werden
- kann nicht an Dritte weitergegeben werden

Nachteil
- benötigt zur Erkennung spezielle Vorrichtung (Technik)
- fälschliche Akzeptanz/Zurückweisung möglich

Fähigkeit

Vorteil
- ziemlich einmalig, schwierig zu kopieren

Nachteil
- kann von Nachahmern imitiert werden
- kann Probleme beim Datenschutz aufwerfen

Authentifizierung Die Authentifizierung ist die **Prüfung der behaupteten Authentisierung**. Die Authentifizierung wird von einem **Prüfer** durchgeführt. Der Prüfer überprüft die Echtheit der Authentisierung.

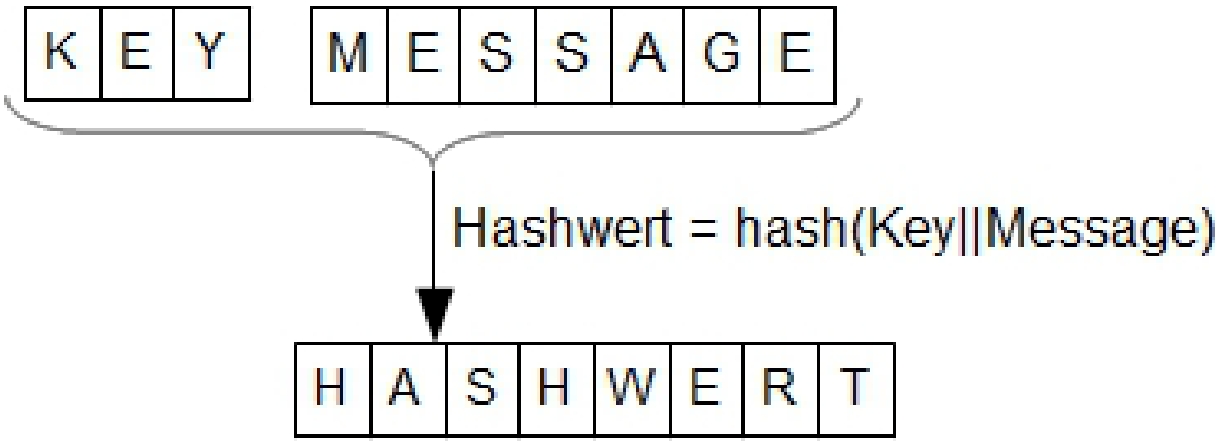


Abbildung 38: Erstellen eines HMAC

Autorisierung Die Autorisierung räumt Rechte für die Nutzung von speziellen Diensten und Leistungen ein.

Wozu braucht man Netzwerksicherheit?

Um Informationen zu sichern. Es sollte sichergestellt werden, dass niemand auf Informationen zugreifen oder verändern kann, die er nicht dürfte.

Was ist eine Bedrohung (Threat)?

- Eine Bedrohung
- Ein Threat hat mit Folgen zu tun (wirtschaftlicher Schaden)
- Angreifer bewegen sich in einem „Attack Vector“, einem angreifbarem Bereich. Etwas, das Schwachstellen aufweist.
- Beispiele
  - Informationsdiebstahl
  - Datenverlust
  - Datenmanipulation
  - Disruption of Service (Betriebsstörung)
  - VERLUST VON ZEIT UND GELD

Was gefährdet die Informationen? Welche Gefährdungen/Bedrohungen gibt es?
- Nicht vorsätzliche (zufällige) Gefährdungen/Bedrohungen
  - Naturgewalten (Blitz, Hagel, Unwetter, Erdrutsche, Hochwasser, etc.)
  - Ausfall von Strom oder Telekommunikation
  - Technische Pannen, z.B. Fehler von Hard- und/oder Software
  - Bedienerfehler / Fahrlässigkeit der Mitarbeitenden
- Vorsätzliche Gefährdungen/Bedrohungen
  - Bösartiger Code (Viren, Würmer, Trojaner, etc.)
  - Informationsdiebstahl
  - Angriffe (von Skript-Kiddies bis Hacker)
  - Wirtschaftsspionage („was die Konkurrenz wissen möchte“)
  - Missbrauch der IT-Infrastruktur

Menschliches Fehlverhalten durch Fahrlässigkeit, Gleichgültigkeit, Unwissenheit und Leichtgläubigkeit.

Vorsätzliche Manipulation
- Angriffe über das Internet
- Unerlaubter Zugriff auf Systeme
- Abhören und Modifizieren von Daten
- Angriff auf die Verfügbarkeit von Systemen
- Missbrauch von Systemen, Distributed Denial of Service (DDoS)
- Viren, Würmer und Trojanische Pferde
- Drive by Infection[9]

Organisatorische Schwachstellen
- Fehlendes Sicherheitsverständnis des Managements
- Unklare Verantwortlichkeiten
- Ungenaue oder fehlende Abläufe / Prozesse
- Mangelhafte Richtlinien
- Fehlende Strategie und Konzepte
- Mangelhafte Awareness der Mitarbeitenden
- Fehlende Kontrollen

Technisches Versagen
- Ungenügende Wartung
- Nicht funktionierende Überwachungssysteme (z.B. IDS[10], etc.)
- Falsch dimensionierte Systeme
- Fehlerhafte
  - Konfiguration
  - Applikationen
  - Betriebssysteme
  - Firmware
  - Treiber
  - etc.

Höhere Gewalt
- Ökologisch
  - Unwetter
  - Erdbeben
  - Brände
  - Überschwemmungen
  - Vulkanausbrüche
- Technisch
  - Feuer
  - Wasser
- Sozial
  - Ausschreitungen

[9] unbeabsichtigtes Downloaden von Schadsoftware
[10] Intrusion Detection System

- Geiselnahme
- Krieg

Was ist ein Asset?

- z.B. Computer = kostet etwas, hat einen Wert
- hat eine Wichtigkeit
- Kundendaten sind wichtig und aus der Sicht der Firma wertvoll uns sind ein Asset

Was ist eine Schwachstelle (Vulnerability)?

Schwachstellen sind Stellen, die für Angriffe anfällig sind. Man beachtet dabei das Mass einer Schwachstelle in einem Netzwerk oder Gerät. Schwachstellen sind inhärent[11] und unvermeidbar in Netzwerk- und Endgeräten. Sogar in Geräten mit Sicherheitseinrichtung.

Was ist Risiko (im Kontext der Informationssicherheit)?

Risiko Ein Risiko ist ein negativer Ausgang einer Unternehmung, mit dem Nachteile, Verlust, Schäden, usw. verbunden sind.

- Wahrscheinlichkeit, dass eine Gefährdung über eine Schwachstelle zu einem Schaden von bestimmten Ausmass führt
- Wahrscheinlichkeiten sind extrem schwer zu berechnen → Geschätzte Häufigkeiten
- **Risiko = Eintretenshäufigkeit × Schadensausmass**
- Die Eintretenshäufigkeit und Schaden können bewertet werden
- Sicherheit und Risiko sind voneinander abhängig

Was ist ein „mitigation technique“?

Eine Art ein Risiko zu behandeln. Nicht jedes Risiko muss aber aber abgedeckt, bzw. geschützt werden. Es gibt auch akzeptable Risikos, bei dem beispielsweise die Kosten den Nutzen übersteigen. Die Mitigation an sich ist es mit geeigneten Sicherheitsmassnahmen das Schadensausmass oder die Eintrittshäufigkeit reduzieren.

Wieso ist es so schwierig völlig sichere Systeme zu erstellen?

Systeme werden immer komplexer und diese verbergen eher Schwachstellen. Cloudsysteme sind beispielsweise komplexe Strukturen und machen die Anwendung von Sicherheitsmechanismen schwierig.

Was ist Vertraulichkeit und wie ist sie normalerweise (technisch) erreicht?

Durch Verschlüsselung. Siehe vorhin Vertraulichkeit, Seite 48.

Was ist Integrität und wie ist sie normalerweise (technisch) erreicht?

Mit Hashfunktionen. Die kleinste Änderung am Daten-Input gibt einen ganz anderen Hash-Output. Ein gleicher Daten-Input gibt aber immer denselben Hash-Output. Siehe vorhin Integrität, Seite 47.

Was ist Verfügbarkeit und wie ist sie normalerweise (technisch) erreicht?

Viel **virtualisieren**, damit Services eine hohe Verfügbarkeit bieten. Wenn mehr **Kapazität** (z.B. Daten- oder Arbeitsspeicher) notwendig ist, kann rasch mehr hinzugefügt werden. **Proxies** verhinder, dass viele Verbindungen zum Server von der gleichen IP hergestellt werden können. Siehe vorhin Verfügbarkeit, Seite 47.

Was ist Authentifizierung und wie ist sie normalerweise (technisch) erreicht?

Authentifizierung ist ein Prozess, bei dem zuletzt eine **Authentisierung** durchgeführt wird. Eine Prüfnachricht, welche von einem Prüfer (Server, Remote Client etc.) erhalten wurde, wird zusammen mit einem Secret Key (Passwort) clientseitig gehasht. Dieser erzeugte Hash ist ein sogenannter HMAC - Hashed Message Authentication Code. Der HMAC wird zurück an den Prüfer gesendet. Dieser kann eine **Authentisierung** vornehmen und deren Echtheit prüfen. Dieser Vorgang läuft im Hintergrund ab, beispielsweise wenn man

[11] „Innewohnen“

sich auf einer Webseite einloggt. In Englisch gibt es lexikalisch keine Unterscheidung, es heisst beides *Authentication*. Siehe vorhin Authentifizierung, Seite 50 und Authentisierung, Seite 49.

Was ist „non-repudiation“ und wie ist es normalerweise (technisch) erreicht?

Verbindlichkeit erzielt man mittels digitaler Signatur. Wenn ich beispielsweise jemanden eine Email sende, signiere ich die Email mit meinem privaten Schlüssel, den nur ich besitze. Der Empfänger kennt hingegen meinen öffentlichen Schlüssel und nutzt diesen, um sich zu vergewissern, dass die Email tatsächlich von mir gesendet wurde. Siehe vorhin Verbindlichkeit, Seite 47.

Was ist der Unterschied zwischen symmetrischer und asymmetrischer Kryptografie?

- Symmetrisch: verwendet einen einzigen Schlüssel. Alle Parteien besitzen denselben Schlüssel.
- Asymmetrisch: Jede Partei besitzt einen öffentlichen und einen privaten Schlüssel (public/private key). Der öffentliche Schlüssel ist für alle verfügbar. Zum verschlüsseln braucht man den öffentlichen Schlüssel des Empfängers. Der Empfänger kann mittels seinem privaten Schlüssel die Nachricht oder Dateien entschlüsseln.

Siehe vorhin Vertraulichkeit, Seite 48.

Welche Kryptografieart (symmetrisch oder asymmetrisch) wird für digitale Unterschriften verwendet?

Asymmetrisch. Siehe vorhin Verbindlichkeit, Seite 47.

Geben Sie ein Beispiel eines symmetrischen kryptografischen Algorithmus

Beispiele für symmetrische Algorithmen

Name	Blocklänge	Schlüssellänge	Jahr	Kommentar
DES	64 Bit	56 Bit	1970	gebrochen
Triple DES	64 Bit	112 Bit (3×56 Bit)		nicht mehr empfohlen
RC4	stream cipher	8-2040	1987	gebrochen
IDEA	64 Bit	128 Bit	1990	nicht mehr empfohlen
RC5	64 oder 128 Bit	4-256 Bit	1994	nicht mehr empfohlen
Camellia	128 Bit	128, 192 oder 256 Bit	2000	
Twofish	128 Bit	128, 192 oder 256 Bit	1998	
AES (Rijndal)	128 Bit	128, 192 oder 256 Bit	2000	

Geben Sie ein Beispiel eines asymmetrischen kryptografischen Algorithmus

Beispiele für asymmetrische Algorithmen

Name	Unterliegende ‘schwierige’ Funktion
RSA	Faktorisieren grosser Zahlen
Diffie-Hellman (DH)	Diskrete Logarithmen berechnen
Elliptic Curve DH (ECDH)	Diskrete Logarithmen berechnen
ElGamal Verschlüsselung	Diskrete Logarithmen berechnen

Teil IX
SW 12

31 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?

32 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. Der Client (Victim) denkt, er ist mit dem Web Server im Kontakt jedoch ist der MITM ist dazwischen. Umgekehrt denkt der Web Server, dass der MITM der Client ist.

Wie funktioniert einem 'Trust Exploitation' Angriff?

Eve <-x-> Alice <—> Bob <—> Eve Ein Angreifer nutzt das Vertrauen in Netzwerken aus. "Befälläin System und kommt durch Vertrauensnetz in das Netzwerk.

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

Angreifer sendet SYN requests an Webserver Webserver sendet SYN ACK reply an user und warter auf SYN ACKUser sendet aber auch SYN requests und der Server weiss nicht mehr, was er tun muss (DoS) Zwei Arten von DoS Buffer overflow Attacks (Mit Angriff sämtliche Ressourcen aufbrauchen) Flood Attacks (Mit Angriff den Server solange «befeuern», bis die Kapazität des Servers aufgebraucht ist)

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

Man weiss nicht, ob es ein Angreifer ist oder wirklicher Traffic

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

NAT Network Address Translation

NIC Network Interface Controller/Card

VoIP Voice over IP

Glossar

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.

Network Address Translation Ein Router übernimmt die „Übersetzung“ von privaten IP Adressen in eine öffentliche, damit eine Anfrage ins Internet (z.B. Webseitenaufruf) wieder zum eigenen Netzwerk zurückfindet.

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).

[3] Wikipedia. URL: `http://de.wikipedia.org`.