DHBW CAS
Duale Hochschule
Baden-Württemberg
Center for Advanced Studies

Kommunikationssysteme

Teil 1

Grundlagen der Informations- und Kommunikationstechnik

Ausgabe 1.2, 30.04.2023
Autor: Stephan Rupp

Kontakt: stephan.rupp@srupp.de
Web: http://www.srupp.de

Inhaltsverzeichnis

1. Industrielle Feldbusse

1.1. Grundlagen

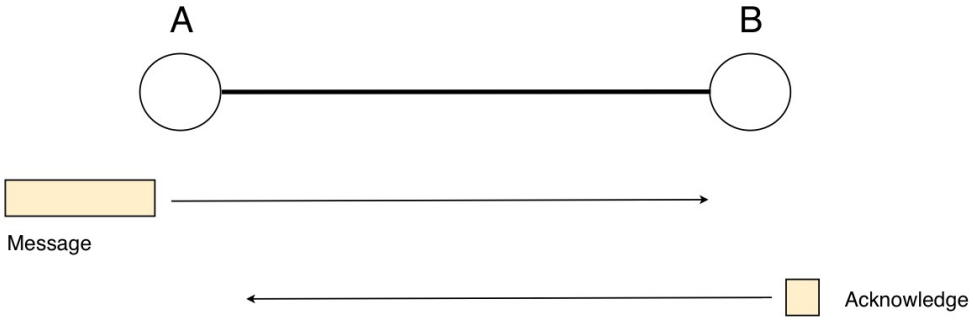
Für Kommunikationsprotokolle unterscheidet das Schichtenmodell folgende Aufgaben:

(1) Schicht 1: physikalische Übertragung (z.B. Modulationsverfahren)

(2) Schicht 2: Rahmenprotokoll mit Absicherung gegen Fehler

(3) Schicht 3: Verwendung von Netzwerkadressen für Sender und Empfänger

Frage 1.1.1: Physikalische Schicht. Von A (Sender) nach B (Empfänger) soll eine Nachricht über eine gegebene Entfernung übermittelt werden. Diskutieren Sie den Einfluß der Ausbreitungs-geschwindigkeit und der Übertragungsrate.



Frage 1.1.2: Rahmenprotokoll. Eine Datenmenge von insgesamt 10 000 Bytes sollen über eine Luftschnittstelle übertragen werden, die eine Bitfehlerrate von 10^{-4} hat. Hierzu wird ein Rahmenprotokoll verwendet (HDLC Protokoll (High Level Data Link Control) mit folgenden Parametern:

Fall I): Jeder Rahmen fasst 128 Bytes an Daten

Fall II): Jeder Rahmen fasst 512 Bytes an Daten

In beiden Fällen gilt: Sofern bei der Übertragung ein Fehler passiert ist (was der Empfänger mit Hilfe einer Prüfsumme festgestellt kann), sollte der betroffene Rahmen nochmals gesendet werden. Für das Übertragungsprotokoll ist pro Rahmen ein Nachrichtenkopf (engl. header) von 6 Bytes vorgesehen.

Frage 1.1.2.1: Wie viele Rahmen müssen in den beiden Fällen I und II insgesamt übertragen werden (inklusive der wegen Übertragungsfehlern wiederholten Rahmen)?

Frage 1.1.2.2: Wie lange dauert die Übertragung in beiden Fällen über einen Kanal mit einer Übertragungsrate von 32000 bit/s (Laufzeiten für Quittungen und Wartezeiten nicht eingerechnet)?

Frage 1.1.2.3: Welcher der beiden Fälle ist in Bezug auf die insgesamt pro Sekunde transportierte Menge an Nutzinformationen effizienter?

Frage 1.1.2.4: Welcher der beiden Fälle wäre effizienter, wenn die Bitfehlerrate 10^{-6} beträgt?

Lösungen:

Frage 1 Fall I): Benötigte Rahmen = 10000 / 128 = 78,125 => 79 Rahmen

Anzahl Bytes = 10000 + 79 * 6 = 10474 Bytes

Anzahl Bits = 10747 * 8 = 83792 bit

Anzahl Fehler = 83792 * 10^{-4} = 8,38 => 9 fehlerhafte Rahmen

Anzahl benötigter Rahmen (inkl. fehlerhafter Rahmen) = 79 + 9 = 88 Rahmen

Frage 1 Fall II): Benötigte Rahmen = 10000 / 512 = 19,53 => 20 Rahmen

Anzahl Bytes = 10000 + 20 * 6 = 10120 Bytes

Anzahl Bits = 10120 * 8 = 80960 bit

Anzahl Fehler = 80960 * 10^{-4} = 8,1 => 9 fehlerhafte Rahmen

Anzahl benötigter Rahmen (inkl. fehlerhafter Rahmen) = 20 + 9 = 29 Rahmen

Frage 2 Fall I) Anzahl Bytes (inkl. fehlerhafter Rahmen) = 10474 + 9 * (128 + 6) = 11680 Bytes

Anzahl Bits = 11680 * 8 = 93440 bit Übertragungsdauer = 93440 / 32000 = 2,92 s

Frage 2 Fall II):

Anzahl Bytes (inkl. fehlerhafter Rahmen) = 10120 + 9 * (512 + 6) = 14782 Bytes

Anzahl Bits = 14782 * 8 = 118256 bit Übertragungsdauer = 118256 / 32000 = 3,7 s

Frage 3 Fall I):

Bytes (eff.) pro Sekunde = 10000 / 2,92 = 3424,66 Bytes pro Sekunde

Bits (eff.) pro Sekunde = 3424, 66 * 8 = 27397,28 bit/s (eff.)

Frage 3 Fall II):

Bytes (eff.) pro Sekunde = 10000 / 3,7 = 2702,70 Bytes pro Sekunde

Bits (eff.) pro Sekunde = 2702, 70 * 8 = 21621,6 bit/s (eff.)

Antwort auf Frage 3: Fall I ist effizienter.

Frage 4) Bei einer Bitfehlerrate von 10^{-6} erhält man in beiden Fällen einen fehlerhaften Rahmen (siehe Antworten zu Frage 1).

Frage 4) Fall I: Anzahl der Bytes (inkl. fehlerhafte Rahmen) = 10474 + 1 * (128 + 6) = 10608 Bytes

Anzahl der Bits = 10608 * 8 = 84864 bit Übertragungsdauer = 84864 / 3200 = 2,65 s

Frage 4 Fall II: Anzahl der Bytes (inkl. fehlerhafte Rahmen) = 10120 + 1 * (512 + 6) = 10638 Bytes

Anzahl der Bits = 10638 * 8 = 85104 bit Übertragungsdauer = 85101 / 3200 = 2,66 s

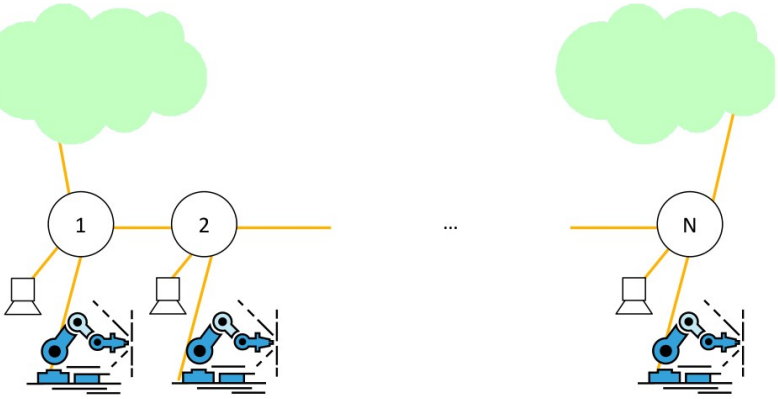
Antwort auf Frage 4): Beide Rahmengrößen sind vergleichbar effizient.

Frage 1.1.3: Netzwerkschicht. Folgende Abbildung zeigt ein Netzwerk. Was könnte man unter dem Begriff „Topologie“ verstehen? Wie lassen sich Nachrichten über das Netz schicken? Auf welchem Weg gelangt die Nachricht von A nach B? Wie kann das Netz die Nachricht eigenständig von A nach B befördern? Wie wird eine Route ausgewählt? Wie geht man vor, wenn mehrere Wege von A nach B führen? Welcher Begriff ist charakteristisch für die Netzwerkschicht?

Frage 1.1.4: Nennen Sie einige Ihnen bekannte Kommunikationsprotokolle. Wie ordnen Sie die oben genannten Schichten zu? Was verstehen Sie unter einem Adressraum? Was verstehen Sie unter einer Routing-Tabelle?

1.2. Ethernet basierte Feldbusse

Es werden N=10 Ethernet-Switches in Serie betrieben. An jedem der Switches ist ein lokaler Controller angeschlossen, sowie eine Kamera. An Anfang und am Ende der Kette befinden sich Anschlüsse an lokale Netze (LAN) mit regulärem Ethernet-Verkehr.



Zur bevorzugten Behandlung der Prozessdaten (Daten, die zwischen den lokalen Controllern ausgetauscht werden), stehen folgende Verfahren zur Auswahl: (a) Verkehrsklassen mit Priorisierung der Prozessdaten (QoS) (b) Zeitmultiplex mit alternierenden Segmenten (1) nur Prozessdaten, (2) alle anderen Daten (c) Sammelpaket: alle Prozessdaten werden in einer geeigneten Struktur in den Be-

reich der Nutzdaten im Ethernet-Rahmen gepackt. Der Datenaustausch pro Switch erfolgt durch spezielle Hardware während der Weiterleitung der Rahmen.

Es wird Fast Ethernet mit einer Übertragungsrate von 100 Mbit/s verwendet. Für Video und allgemeinen Verkehr werden die maximal möglichen Rahmenlängen angenommen. Die Prozessdaten betragen 250 Bytes pro lokalem Controller und lassen sich in Rahmen der Länge 256 Bytes übertragen. Für die Weiterleitung der Rahmen wird pro Switch eine Verarbeitungszeit (Latenz) von 0,01 ms angenommen.

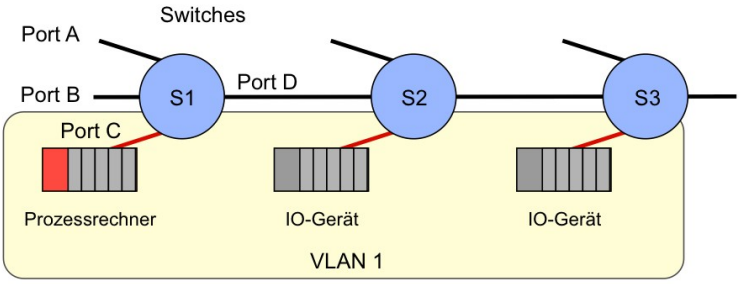
Frage 1.2.1: Berechnen Sie für das Verfahren (a) überschlägig die Laufzeitschwankungen am Ende der Kette für den unter den folgenden Annahmen: maximale Paketlänge (1) 9000 Bytes, (2) 1500 Bytes, (3) 512 Bytes.

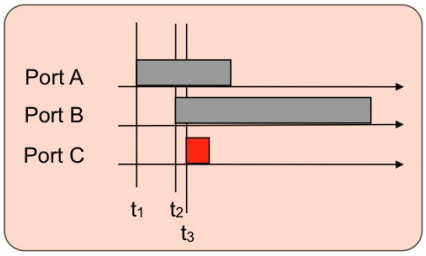
Frage 1.2.2: Berechnen Sie zum Vergleich überschlägig Verfahren (b).

Frage 1.2.3: Berechnen Sie zum Vergleich überschlägig Verfahren (c).

1.3. Vorfahrt für Prozessdaten

Prozessrechner und ihre Peripherie (IO-Geräte) teilen sich ein Netzwerk mit Benutzer-PCs und anderer netzwerkfähiger Infrastruktur. Die folgende Abbildung zeigt eine Konfiguration mit 3 Ethernet-Switches. Prozessrechner und Peripherie kommunizieren miteinander über ein netzwerkbasiertes Feldbusprotokoll. Wegen der zeitkritischen Anforderungen werden kurze Ethernet-Rahmen von 64 Bytes verwendet. Das Netzwerk ist als Fast Ethernet mit 100 Mbit/s Übertragungsrate ausgeführt.

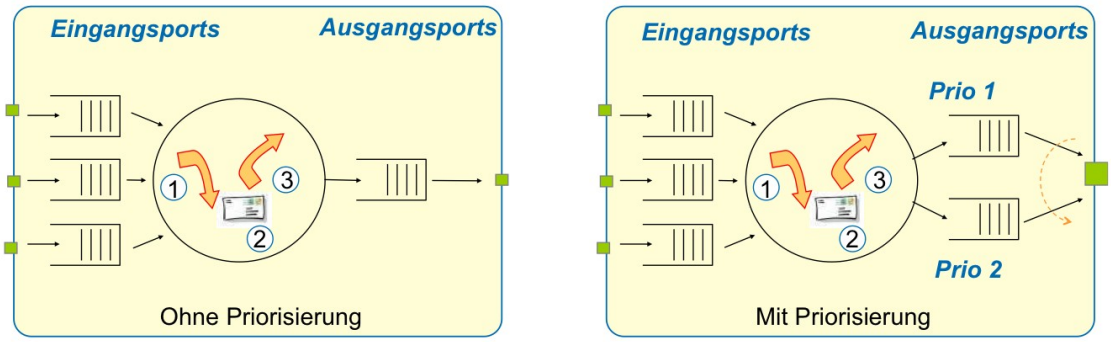




Frage 1.3.1: Am Port A von Switch S1 trifft ein Paket der Länge 512 Bytes mit Videodaten zum Zeitpunkt t1 ein, an Port B zur Zeit t2 ein Ethernet Rahmen der Länge 1500 Bytes, und an Port C zum Zeitpunkt t3 ein Rahmen mit Prozessdaten. Skizzieren Sie die Reihenfolge der Pakete am Ausgangsport D, wenn keine weiteren Massnahmen getroffen werden.

Frage 1.3.2: In welcher Größenordnung sind Laufzeitschwankungen in der gezeigten Konfiguration zu erwarten? Hinweis: angenommen sei eine geringe Systemauslastung, d.h. höchstens 1 Rahmen ist in den Eingangswarteschlangen in Bearbeitung.

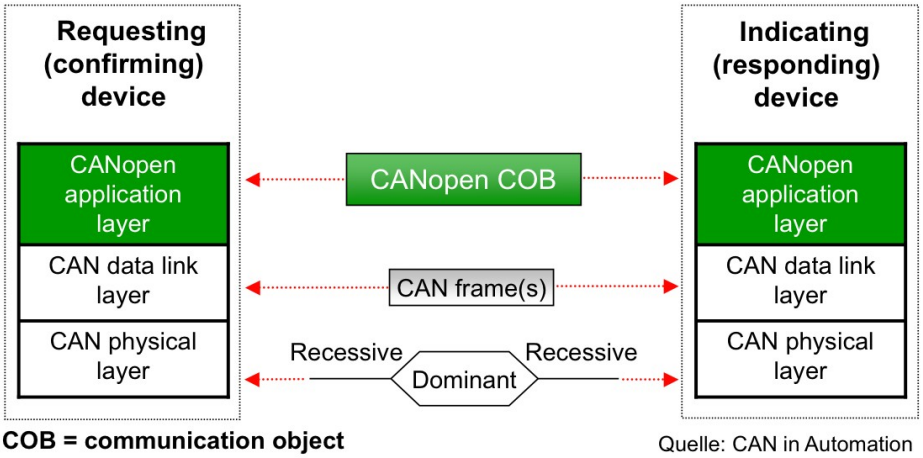
Frage 1.3.3: Die Prozessrechner und ihre Peripherie werden zu einem VLAN zusammengefasst und diesem VLAN die höchste Priorität zugeordnet, siehe folgende Abbildung. Skizzieren Sie die Reihenfolge der Pakete an Port D gemäß Frage 3.1 nach dieser Massnahme. Welchen Einfluss hat diese Massnahme auf die Laufzeit-schwankungen? Hinweis: Als zum VLAN gehörig markierten Pakete erhalten nach dem in der Abbildung oben gezeigten Mechanismus die höchste Priorität.



Frage 1.3.4: Könnte man durch Verwendung zusätzlicher Ausgangsports weitere Fortschritte erzielen? Begründen Sie Ihre Aussage. Nennen Sie Massnahmen, wie man die Laufzeitschwankungen weiter verringern könnte. Begründen Sie Ihre Aussagen.

1.4. CAN Open als Feldbus

Für das Batteriemanagement in einem Elektrofahrzeug soll der CAN-Bus in Kombination mit dem Anwendungsprofil CANopen 454 für Energie-Management-Systeme eingesetzt werden. In den Unterlagen findet sich folgende Abbildung.

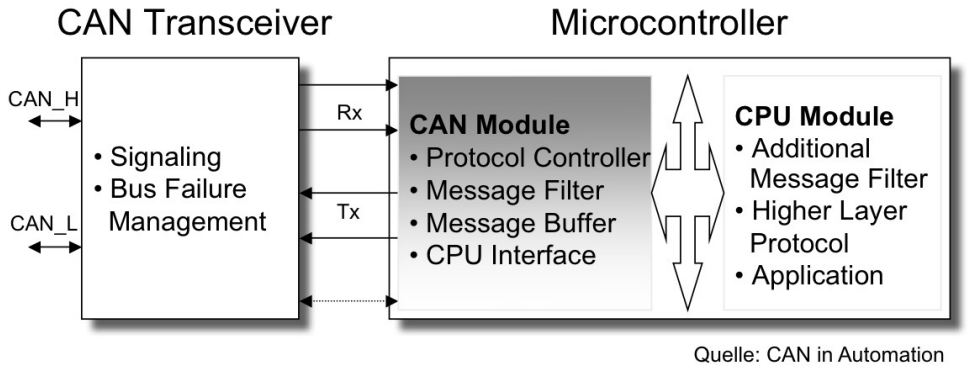


Frage 1.4.1: Interpretieren Sie die abgebildeten Protokollschichten und erläutern Sie die Funktionen jeder Schicht.

Lösung:

- Schicht 1, Physical Layer: Modulationsverfahren; wie OSI Schicht 1
- Schicht 2, Data Link: Rahmenprotokoll mit Fehlerkorrektur; wie OSI-Schicht 2
- Schicht 3, Anwendungsschicht: Schnittstelle für den Anwendungsprogrammierer, Definition von Nachrichten, Nachrichtenformaten und Objekten aus der Anwendungs-domaine; entspricht OSI Schicht 7

Frage 1.4.2: CAN funktioniert als serieller Feldbus, d.h. alle Geräte sind an einem gemeinsamen Medium (Zweidraht) angeschlossen. Der Anschluss der Geräte an den Feldbus erfolgt wie in folgender Abbildung gezeigt. Erläutern Sie die Funktion der einzelnen Komponenten im Zusammenhang mit den den Protokollschichten aus der letzten Abbildung. Welche Besonderheit hat der dargestellte Mikrocontroller?



Quelle: CAN in Automation

- CAN-Transceiver: Physical Layer, stellt für Schicht 2 eine Schnittstelle zum Senden (Transmit Tx) und Empfangen (Receive Rx) von Nachrichten zur Verfügung.
- CAN Module: Schicht 2; sowie Vorverarbeitung von Signalen, z.B. Ausfiltern relevanter Signale zur weiteren Verarbeitung, sowie Nachrichtenpuffer; stellt Schnittstelle zur Anwendungsschicht bereit.
- CPU-Module: Verarbeitung des Anwendungsprotokolls (Schicht 3), sowie der der Anwendung selbst.
- In der gezeigten Abbildung ist das CAN-Module (Schnittstellenmodul) direkt im Mikrocontroller integriert. Als Alternative wäre ein externer Baustein zu verwenden, der dann über eine serielle Schnittstelle an einen Mikrocontroller angeschlossen ist (z.B. über eine serielle Schnittstelle wie SPI).

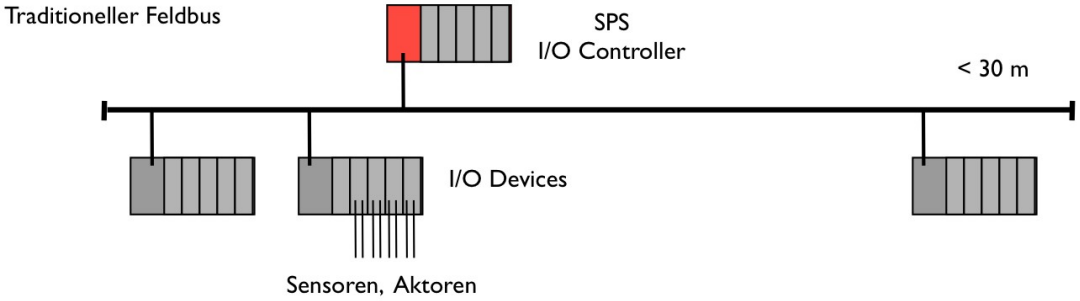
Frage 1.4.3: Der Feldbus wird mit einer Datenrate von 1 Mbit/s betrieben. Die Länge einer Nachricht beträgt 6 Bytes für den Nachrichtenkopf (Header), sowie 0 bis 8 Bytes für Daten. Die Geräte kommunizieren Kollisionen unter einander (mehrere Geräte senden gleichzeitig), sowie Quittungen empfangener Nachrichten unmittelbar durch den Signalpegel eines einzelnen Bits (in Art einer Open-Kollektor-Schaltung bzw. verdrahteter ODER-Logik der Anschlüsse an den Bus). Wie lange darf die Länge ℓ des Feldbusses höchstens sein, damit eine Nachricht von einem Ende zum anderen laufen kann und von dort eine Quittung empfangen werden kann (als Ausbreitungsgeschwindigkeit seien 200 * 10^6 m/s angenommen)? Wie viele Nachrichten pro Sekunde kann der Bus übertragen, wenn jede Nachricht 8 Bytes Daten enthält? Nennen Sie eine Möglichkeiten, Nachrichten bevorzugt zu behandeln (z.B. Steuerinformationen vor Messwerten).

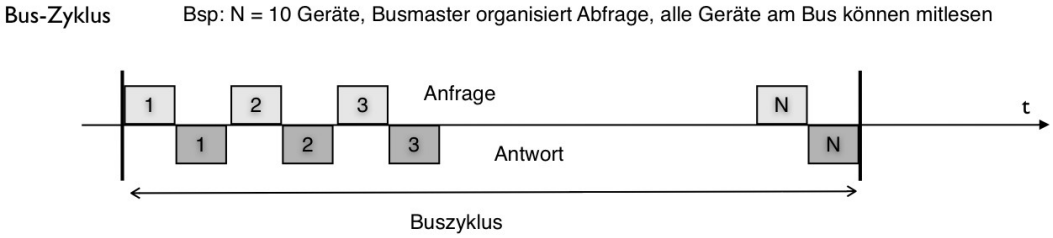
- Die Übertragungsdauer eines Bits beträgt 1 us (zu berechnen aus der Datenrate). Während dieser Zeit wird mit der gegebenen Ausbreitungsgeschwindigkeit eine Ent-fernung von 200 m durchlaufen. Die Buslänge darf also 100 m nicht überschreiten, damit eine Quittung nach einer us zurücklaufen kann. Damit die Quittung innerhalb der Bitdauer ankommt, sollte die Buslänge deutlich kürzer sein (max. 40 m).
- Nachrichtenlänge: 14 Bytes = 14 * 8 = 112 bits => 112 us pro Nachricht. Somit können pro Sekunde 8929 Nachrichten übertragen werden.
- Die Priorität der Nachricht wird im Nachrichtenkopf kennzeichnen. Die Auswertung erfolgt entweder durch die Anwendung (Software im Mikrocontroller), bzw. gleich bitweise durch den Buspegel.

Frage 1.4.4: In Fahrzeugen (speziell PKW und LKW) wird CAN-Bus als serieller Bus weiterhin für Echtzeitanwendungen eingesetzt. In fast allen anderen Anwendungen, inklusive der Steuerung von Schienen-fahrzeugen und Flugzeugen werden Ethernet basierte Feldbusse verwendet. Welche Gründe gibt es hierfür?

1.5. Buszyklus und serielle Feldbusse

Folgend Abbildung zeigt ein serielles Feldbussystem. Der Bus wird mit einer Übertragungsrate von 1 Mbit/s betrieben, die Größe einer Nachricht beträgt 12 Bytes.





Frage 1.5.1: Erläutern Sie die Funktionsweise des seriellen Feldbus. Verwenden Sie hierzu die Begriffe Buszyklus, Dauer des Buszyklus, Echtzeit.

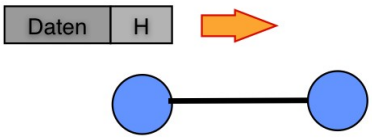
Erläuterungen: serieller Feldbus

- Laufzeit der Signale: 300 * 106 m/s ⇒ 300 m/µs. 30 m werden also in 100 ns durchlaufen.
- Übertragungsrate am Bus: 1 Mbit/s. 1 Bit dauert 1 µs, damit quaistationäre Verhältnisse auf der Leitung.
- Größe der Telegramme bzw. Nachrichten: z.B. 12 Bytes = ca 100 Bits
- Dauer eines Telegramms somit ca. 100 µs.
- Dauer: > 2 * N * Dauer einer Nachricht (für 10 Geräte und 100 µs: 2 ms)

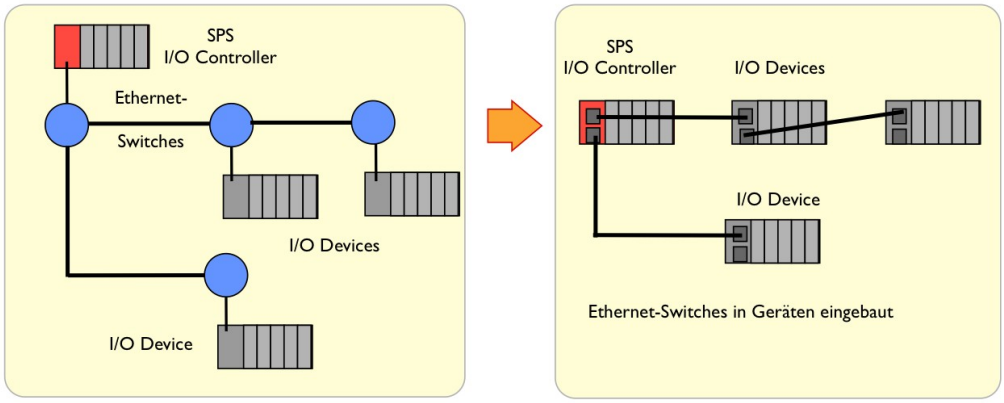
Frage 1.5.2: Skizzieren Sie im Vergleich hierzu den Aufbau eines Ethernet basierten Feldbusses. Erläutern Sie die Begriffe Buszyklus und Reaktionszeiten für den Ethernet basierten Feldbus. Welche Topologien lassen sich hierfür einsetzen?

Erläuterungen: Ethernet basierter Feldbus

- Ethernet Rahmen: 64 Bytes (20 Bytes Header, 44 Bytes Nutzdaten)
- Übertragungsrate: 100 Mbit/s (Fast Ethernet, 1 Bit dauert 10 ns))
- 64 * 8 Bytes / 100 MBit/s ⇒ ca 5 µs Übertragungsdauer
- Ethernet-Switch: speichern und weiterleiten verursacht ca 5 µs Verzögerung pro Switch (auch bei längeren Ethernet Rahmen, da die Header-Information zum Auswerten der Zieladresse zum Weiterleiten genügt)

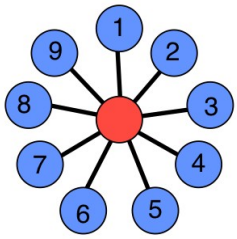


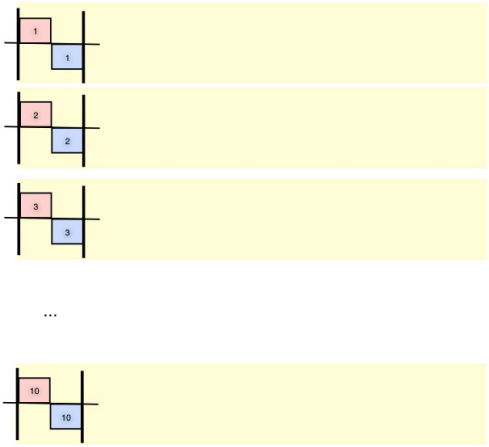
wie Schieberegister



Netz-Topologien:

Stern-Topologie im Parallelbetrieb



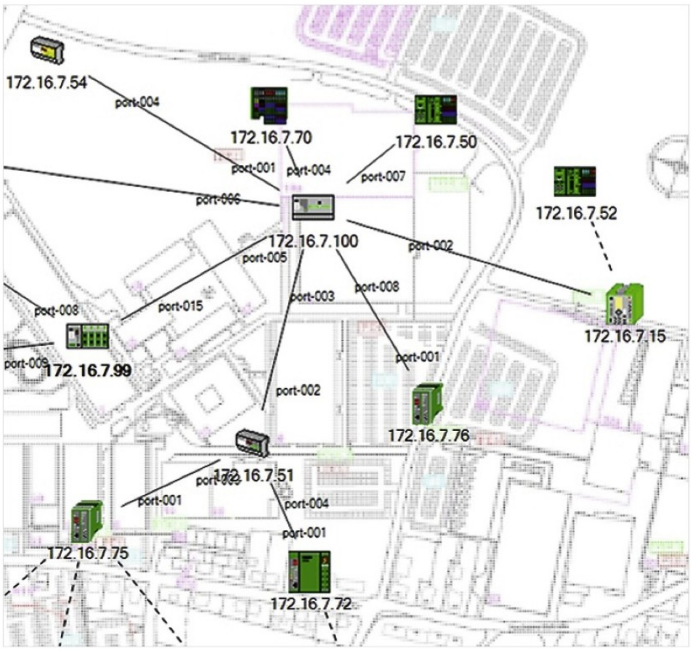


Optimierter Buszyklus:

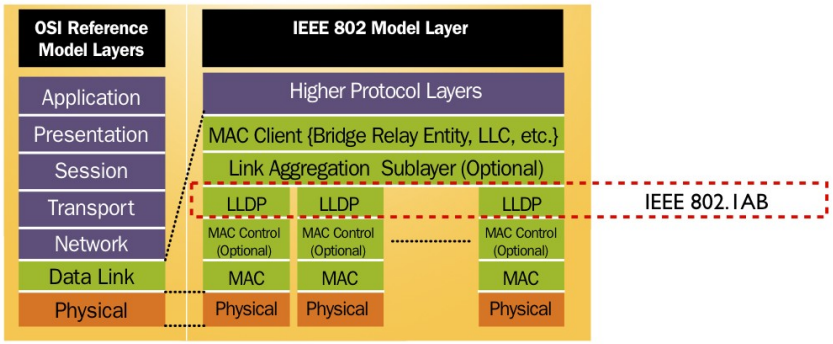
Dauer: > 2 * N * Dauer einer Nachricht (für 10 Geräte und 5 µs: **10 µs**)

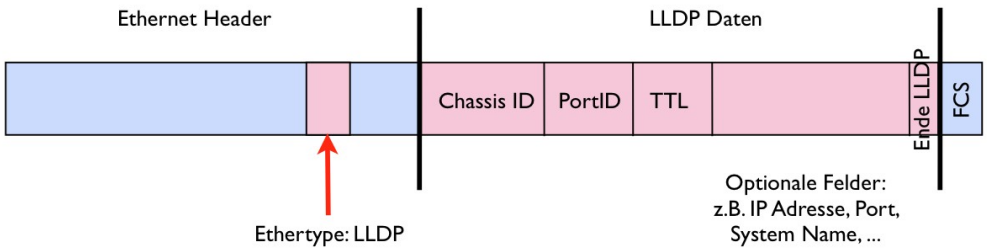
1.6. Topologie Erkennungsdienst

Ein Hersteller von Systemen mit netzwerkbasierter Feldbusschnittstelle bietet eine automatische Topologieerkennung an. Hiermit lässt sich die Netztopologie aus dem laufenden Netz auslesen, wie in folgender Abbildung gezeigt. Damit dieser Dienst mit Geräten unterschiedlicher Hersteller funktioniert, basiert die Kommunikation unter den Geräten auf Basis eines internationalen Standards, nämlich dem in IEEE 802.1AB standardisierten Protokoll LLDP (Link Layer Discovery Protocol)



Frage 1.6.1: Über das sogenannte Link Layer Discovery Protokoll (LLDP) finden sich die in der folgenden Abbildung gezeigten Informationen. Welcher Protokollschicht ordnen Sie LLDP zu? Wie weit wird die per LLDP ausgetauschte Information kommuniziert? Können Protokolle auf Schicht 3 passiert werden? Begründen Sie Ihre Entscheidung.

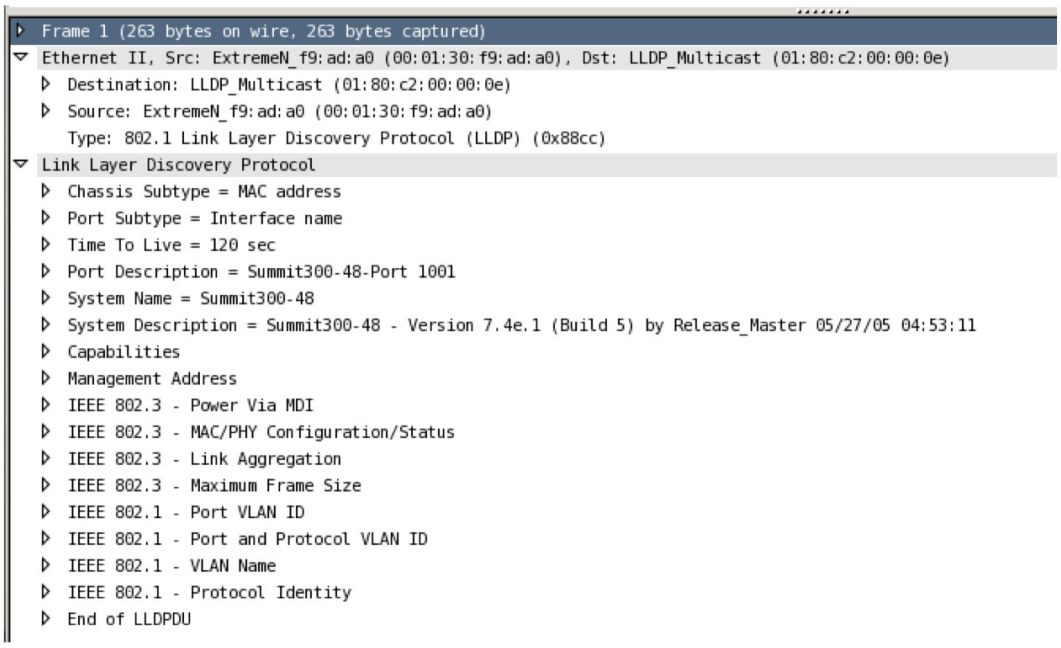




Frage 1.6.2: Die Topologie soll netzweit erkannt werden, auch über VLANs und über Router hinweg. Wie lässt sich dies erreichen? Welche Information wird benötigt? Wie lässt sich die Kompatibilität zwischen Geräten unterschiedlicher Hersteller gewähr-leisten? Hinweis: Verwenden Sie lokale Verzeichnisse auf den Geräten.

Frage 1.6.3: Wenn Geräte ausfallen, bzw. aus dem Netz entfernt werden, muss die Topologie aktualisiert werden. Wie lässt sich verhindern, dass veraltete Informationen in den Geräten vorgehalten werden?

Frage 1.6.4: Die folgende Abbildung zeigt einen mit einem Netzwerk-Analyse-Programm dekodierten LLDP Rahmen. Identifizieren und interpretieren Sie die obligatorischen und optionalen Felder im Rahmen.

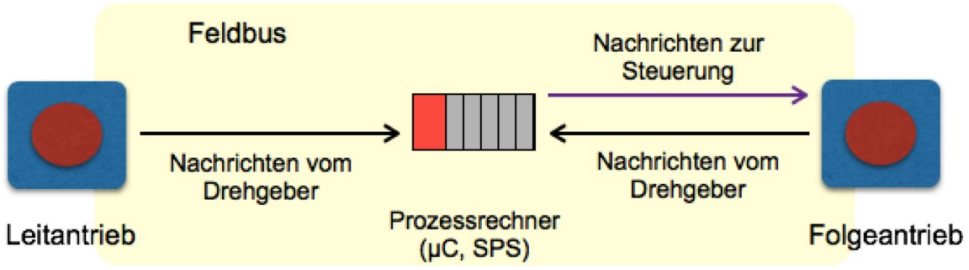


Frage 1.4.5: Der in Abbildung dekodierte Rahmen enthält ein Feld TTL (= Time to Live), das auf 120 s gesetzt ist. Welche Funktion könnte dieses Feld haben? Wie wird die Information aus dem TTL-Feld in den Geräten vermutlich verwendet?

Frage 1.4.6: Der Systemhersteller bietet beim Austausch von Geräten im Feld ein besonderes Leistungsmerkmal: die automatische Übernahme der Konfigurations-parameter des ausgetauschten Gerätes. Wie könnte er dieses Leistungsmerkmal realisieren?

1.7. Echtzeit Anwendung

Ein Antrieb soll als Folgeantrieb auf einen Leitantrieb synchronisiert werden, so dass zwischen beiden Antrieben Gleichlauf hergestellt wird. Hierbei werden Winkelfehler und Drift durch einen Prozessrechner am Folgeantrieb ausgeregelt. Zur Synchronisation stehen dem Prozessrechner von beiden Antrieben Impulse der jeweiligen Drehgeber zur Verfügung. Folgende Abbildung zeigt die Anordnung.



Zur Kommunikation sind beide Antriebe und der Prozessrechner an einen Feldbus ange-schlossen. Es sei angenommen, dass sich der Leitantrieb mit 3000 Umdrehungen pro Minute bewegt.

Frage 1.8.1: Traditioneller Feldbus mit 1 Mbit/s Übertragungsrate und 100 Bit Nachrichtenlänge. Welche Zykluszeit lässt sich hiermit für die 3 Geräte erzielen? Wie viele Nachrichten pro Umdrehung erhält der Prozessrechner vom Leitantrieb.

Lösung: (1) Dauer einer Umdrehung: 20 ms, (2) Dauer der Übertragung einer Nachricht: 100 µs, (3) mit insgesamt 3 Geräten und 2 Nachrichten pro Gerät (Abfrage und Antwort) beträgt der Buszyklus 3 x 2 x 100 µs = 600 µs, (4) pro Umdrehung erhält der Prozessrechner also 20 ms / 600 µs = 33 Nachrichten pro Umdrehung.

Frage 1.8.2: Es wird ein Ethernet basierter Feldbus eingesetzt mit 100 Mbit/s Übertragungsrate und 64 Bytes Nachrichtenlänge. Die zyklische Abfrage (Buszyklus) wird beibehalten. Welche Zykluszeit ist realisierbar? Wie viele Nachrichten vom Leitantrieb erhält der Prozessrechner pro Umdrehung?

Lösung: (1) Dauer einer Umdrehung: 20 ms, (2) Dauer der Übertragung einer Nachricht: ca. 5 µs, (3) mit insgesamt 3 Geräten und 2 Nachrichten pro Gerät (Abfrage und Antwort) beträgt der Buszyklus 3 x 2 x 5 µs = 30 µs, (4) pro Umdrehung erhält der Prozessrechner also 20 ms / 30 µs = 666 Nachrichten pro Umdrehung.

Frage 1.8.3: Der Ethernet basierte Feldbus wird über eine Strecke geführt, an der insgesamt 10 Geräte (mit integrierten Switches) in einer Linientopologie betrieben werden. Zur Kommunikation werden die MAC-Adressen verwendet. Die Strecke transportiert auch regulären Verkehr aus dem Netzwerk. (1) Lässt sich in dieser Umgebung ein fester Buszyklus einrichten? Wenn nicht, beschreiben Sie eine Alternative für die Kommunikation zwischen den Antrieben und ihrem Prozessrechner. (2) Welche Effekte ergeben sich an den Knotenpunkten (Ethernet-Switches) durch die Bearbeitungs-zeit, sowie durch Wechselwirkung mit anderem Verkehr (bei Rahmenlängen bis zu 1500 Bytes)? (3) Wie können Sie diese Wechselwirkungen reduzieren? (4) Wie viele Nachrichten pro Umdrehung erhält der Prozessrechner in einem realistischen Szenario?

Lösung: (1) Nein, Antwortzeiten lassen sich nicht garantieren. Alternative: Leitantrieb und Folgeantrieb kommunizieren ihre Meldungen in festen Intervallen. Der Prozessrechner greift nach Bedarf steuernd ein. (2) Bearbeitungszeit: ca. 5 µs pro Knoten (für MAC Weiterleitung), Wechselwirkung mit anderem Verkehr: Laufzeitschwankungen um 120 µs pro Paket von 1500 Bytes an jedem Knoten, je nach Verkehrsaufkommen auch mehrere Pakete pro Knoten. (3) Wechselwirkungen verringern: Priorität für Prozessdaten einreichten, z.B. durch VLAN oder ein anderes Verfahren zur Verkehrstrennung, Anzahl der Knoten reduzieren, Länge der Pakete einschränken, (4) realistisches Szenario: VLAN für Prozessdaten, 2 Knoten zwischen Antrieb und Prozessrechner: 2 x 5 µs = 10 µs Bearbeitungszeit, 2x 120 µs = 240 µs Laufzeit-schwankungen, somit kann der Antrieb mit einiger Sicherheit alle 250 µs eine Meldung beim Prozessrechner abliefern, d.h. ca. 20 ms / 250 µs = ca. 80 Nachrichten pro Umdrehung.

Frage 1.8.4: Ab welchen Entfernungen (Länge des Feldbusses) spielen Laufzeiteffekte durch die Signalausbreitung jeweils eine Rolle?

Lösung: Mit einer Ausbreitungsgeschwindigkeit von ca 200 * 106 m/s durchläuft das Signal in einer µs ca 200 m. (1) Für den traditionellen Feldbus mit 1 Mbit/s beträgt die Dauer der Übertragung eines Bits 1 µs. Damit Sendung und Empfang höchstens 1/4 Bit versetzt sind, sollte der Bus nicht länger als 50 m sein. (2) Für den Netzwerk basierten Transport kann man auf Synchronität im Sinne von Nachrichten auf einem gemeinsamen Medium verzichten. Der Bus wird bidirektional betrieben, an den Knoten sind Bearbeitungszeiten eingeplant. Hier gehen die Latenzen insgesamt in die Berechnung der möglichen Reaktionszeiten ein.

Frage 1.8.5: Zeitsynchrone Steuerung. Welche Reaktionszeit ist für die winkelgenaue Steuerung (mit 1 Grad Genauigkeit) eines Antriebs mindestens erforderlich, der mit 3000 Umdrehungen pro Minute läuft? Welchen Vorteil bringen synchrone Uhren in den Controllern (Antriebe, Feldbusklemmen, bzw. Prozessrechner)?

Frage 1.8.6: Uhrenvergleich: Damit die Uhren synchron bleiben, müssen sie durch ein geeignetes Protokoll von Zeit zu Zeit nachgestellt werden. Hierzu übernimmt ein Gerät die Zeitbasis (Master-Clock), alle anderen Geräte werden nach dieser Uhr gestellt (Slave Clocks). Das Stellen der Uhren erfolgt durch Versand von Nachrichten nach einem geeigneten Protokoll. Hierbei ist der Gangunterschied der Uhren festzustellen und ausserdem die Laufzeit der Nachricht zwischen den Geräten zu berücksichtigen. Beschreiben Sie ein Verfahren, mit dem sich die Uhr eines Gerätes nach der Uhr in einem anderen Gerät stellen lässt. Hinweis: Gehen Sie schrittweise vor: (1) ohne Berücksichtigung der Laufzeit, (2) mit Berücksichtigung der Laufzeit.

2. Weitverkehrsnetze

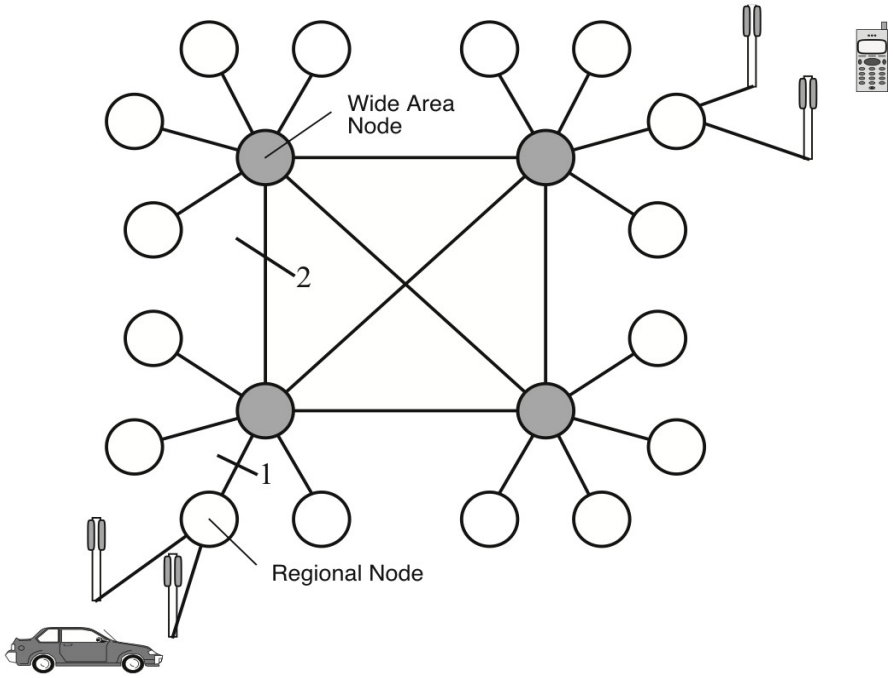
In diesem Kapitel wird der Aufbau und die Funktionsweise von Weitverkehrsnetzen erläutert. Als Basis dienen das Internet und die Telefonnetze. Grundsätzlich ist der Aufbau privater Weitverkehrsnetze z.B. für die Anbindung von Umspannwerken an eine Leitwarte ähnlich. Die verwendeten Technologien und die Methoden zur Auslegung der Netze sind gleich. Zur Überwachung von Betriebs-mitteln in den Verteilnetzen bzw. zum Auslesen von Informationen beim Endkunden lassen sich öffentliche Netze unmittelbar verwenden.

2.1. Datentransport

Über ein Netz mit der in folgender Abbildung gezeigten Topologie soll pro Teilnehmer in der Hauptverkehrsstunde folgender Verkehr übertragen werden:

- 2 Telefonanrufe pro Teilnehmer (mit 64 kbit/s) mit jeweils 100 s Dauer
- 2 SMS von jeweils 1000 Bits pro Teilnehmer

Im Netz befinden sich völlig gleichmäßig verteilt insgesamt 40 Millionen Teilnehmer.



Frage 2.1.1: (1) Berechnen Sie den Verkehr in Mbit/s für alle Telefongespräche. (2) Berechnen Sie den Verkehr in Mbit/s für alle SMS Nachrichten. (3) Berechnen Sie den gesamten Verkehr im Netz in Mbit/s. Hinweis: Oben angegebene Werte (2 Telefonate, 2 SMS) sind Mittelwerte pro Stunde und pro Teilnehmer.

Lösung: Verkehrsmenge (als Datenrate in bit/s):

Telefonanrufe: $40*10^6$ * 2/3600s * 64.000 bit/s * 100s = 142222 Mbit/s = (142,2 Gbit/s)

SMS: $40*10^6$ * 2/3600s * 1000 bit = 22,2 Mbit/s

Verkehrsmenge insgesamt: 142,244 Gbit/s (aus (1) + (2))

Frage 2.1.2: Berechnen Sie überschlägig die an folgenden Schnittstellen insgesamt zu übertragenden Datenraten: Schnittstelle [1] (vom regionalen Knoten zum Weitverkehrsknoten), Schnittstelle [2] zwischen den Weitverkehrsknoten.

Lösung:

- Verkehr pro regionaler Knoten: 1/16 des Gesamtverkehrs (bei Vernachlässigung des lokalen Verkehrs am regionalen Knoten) = Verkehr an Schnittstelle [1]:
- Berechnung für Schnittstelle [1]: 142244 /16 Mbit/s = 8890 Mbit/s
- Verkehr an Schnittstelle [2]: pro Weitverkehrsknoten fließt Verkehr aus 4 regionalen Knoten zu. Dieser Verkehr fließt über 3 Schnittstellen ab. An Schnittstelle [2] ergibt sich somit 4/3 des Verkehrs von Schnittstelle [1].
- Berechnung für Schnittstelle [2]: 4*8890/ 3 Mbit/s = 11854 Mbit/s

2.2. Paketvermittlung

In dem in Aufgabe 2.1 gezeigten Netz sollen die Telefonanrufe und SMS-Nachrichten nun individuell an einzelne Teilnehmer zugestellt werden. Hierzu werden über dem Übertragungsnetz, das in Aufgabe 2.1 für das Verkehrsaufkommen insgesamt ausgelegt wurde, Knoten zur Paketvermittlung aufgestellt. Die Paketvermittlungsstellen (=Router) werden als Regionale Knoten und Weitverkehrsknoten eingerichtet.

Frage 2.2.1: Erläutern Sie die Funktionsweise einer Paketvermittlungsstelle (eines Routers). Hinweis: Verwenden Sie die Begriffe Netzadressen und Routing-Tabellen.

Lösung: Funktionsweise: (1) Nachricht annehmen (speichern), (2) Zieladresse lesen, (3) Zielport aus der Routing-Tabelle entnehmen, (4) Nachricht an den passenden Ausgangsport geben.

Frage 2.2.2: Welche Inhalte enthält die Routing-Tabelle einer Paketvermittlungsstelle? Wie werden diese Inhalte gefüllt?

Lösung: (1) Inhalte der Routing-Tabelle: Zieladresse, Zielport. (2) Füllen der Routing-Tabellen: Die Inhalte werden entweder statisch konfiguriert (Administrator) oder automatisch durch Routing-Protokolle erstellt.

Frage 2.2.3: Welche Rolle spielt die Netzhierarchie (d.h. die hierarchische Vergabe von Netzadressen) für die Größe der Routing-Tabellen? Verwenden Sie als Beispiel das Netz in der Abbildung aus Aufgabe 2.1.

Lösung: Die regionalen Knoten haben folgende Möglichkeiten: [1] Die weiter zu leitenden Nachricht ist lokaler Verkehr für einen anderen direkt angeschlossenen Teilnehmer, oder [2] die Nachricht ist für einen Teilnehmer im Weitverkehrsnetz. Die Weitverkehrsknoten haben jeweils drei andere Weitverkehrsknoten zum Weiterleiten der Nachricht.

Wenn man die Netzadressen nach einem hierarchischen Schema vergibt (z.B. wie im Postnetz mit Postleitzahlen, bzw. wie in der folgenden Aufgabe 4 zu sehen), bleiben die Routing-Tabellen kurz.

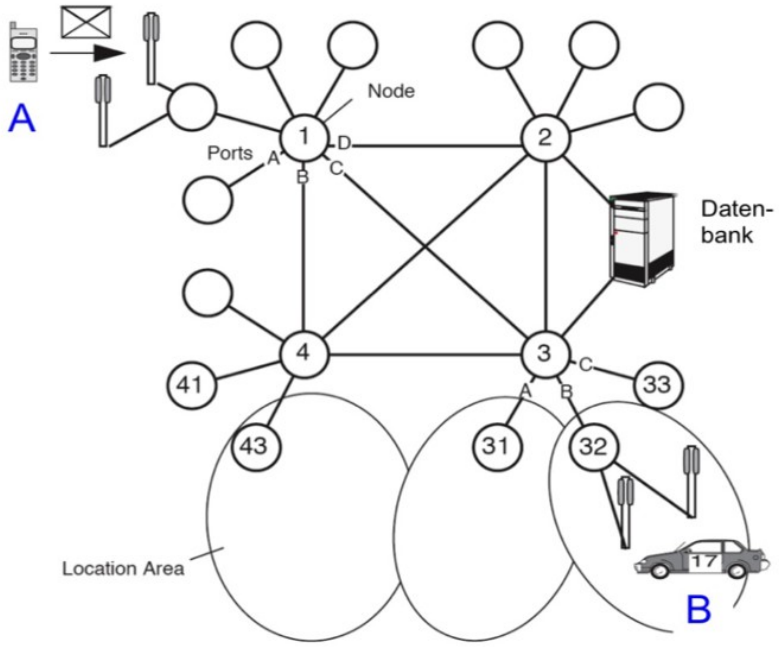
Beispiel: Regionale Knoten: nur Ausscheidung lokal und Weitverkehr. Weitverkehrs-knoten: Analyse der ersten Ziffer der Zieladresse und weiterleiten an den passenden Port.

Bei zufällig verteilten Netzadressen werden die Routing-Tabellen lang, da jede Adresse vollständig analysiert (und somit eingetragen) werden muss. Beispiel: lokale MAC-Adressen (= Geräteadressen) im LAN (lokalen Netz bei Ethernet).

Frage 2.2.4: Erläutern Sie das Funktionsprinzip eines Telefongesprächs über das Internet (Voice over IP). Hinweis: Hierbei soll ein kontinuierlicher Datenstrom (Telefongespräch) mit Hilfe einzelner Pakete übertragen.

2.3. Mobilkommunikation

Folgende Abbildung beschreibt ein Mobilfunknetz auf abstrakte Weise.



Teilnehmer A (Alice) ist am regionalen Knoten 11 angeschlossen und hat dort die Anschlussnummer 12. Alice ist somit zu erreichen unter der Telefonnummer 11-12. Bob hält sich gerade am regionalen Knoten 32 auf und hat die Anschlussnummer 17. Bob ist also zu erreichen unter der Nummer 32-17. Das Netz arbeitet mit Paketvermittlung.

Frage 2.3.1: Alice möchte Bob eine Nachricht (SMS) schicken. Welche Nummer wählt sie? Auf welche Weise transportiert das Netz die Nachricht zu Bob?

Lösung: (1) Alice wählt die Nummer 32-17. (2) Die Netzknoten analysieren die Nummer als Netzadresse: Knoten 1 schaut nach der ersten Stelle von 32-17: Alle Nachrichten zum Knoten 3 schickt er über Port C weiter (diesen Port ermittelt er aus seiner Routing-Tabelle, die Netzadressen in Ports übersetzt). (3) Knoten 3 schaut nach der ersten und zweiten Ziffer „32“ und gibt die Nachricht über Port B an Knoten 32 weiter. (4) Knoten 32 stellt die Nachricht an Anschluss 17 durch.

Frage 2.3.2: Bob bewegt sich im Netz. Er besucht einen Bekannten und befindet sich nun am Knoten 43 mit der Anschlussnummer 17. Wie kann Alice Bob erreichen? Sind die Netzadressen für mobile Teilnehmer im Netz eine geeignete Methode? Beschreiben Sie einen Mechanismus zur Adressierung mobiler Teilnehmer im Netz.

Lösung: (1) Bob hat nun eine andere Netzadresse, nämlich die 43-17. Um ihn dort erreichen zu können, müsste Alice wissen, dass er sich jetzt unter dieser Adresse aufhält. Ein Verfahren, bei Wechsel des Standorts allen Bekannten die neue Adresse zu schicken, ist im Mobilnetz nicht praktikabel (diese Methode funktioniert bei einem Umzug in eine andere Wohnung). (2) Netzadressen sind folglich für die Erreichbarkeit mobiler Teilnehmer im Netz nicht geeignet. (3) Als Alternative werden Namen bzw. logische Adressen verwendet: Bob erhält z.B. eine eindeutige logische Adresse „0172 12 34 56 7“, bzw. „Bob@mobile-network.de“. Unter diesem Eintrag findet sich in der Datenbank seine aktuelle Netzadresse.

Frage 2.3.3: Wie werden die aktuellen Aufenthaltsorte mobiler Teilnehmer im Netz verwaltet? Beschreiben Sie einen Mechanismus, der den Aufenthaltsort eines Teilnehmer automatisch aktualisiert.

Lösung: Wenn sich ein Teilnehmer durch das Netz bewegt, nimmt das Mobiltelefon jeweils Kontakt zu der Basisstation mit der größten Feldstärke auf. Nach der Kontaktaufnahme meldet sich das Mobiltelefon in der Datenbank mit seiner aktuellen Netzadresse an. Der Datenbankeintrag enthält die logische Adresse und die aktuelle Netzadresse. Diese Aufenthaltsverwaltung (engl. Mobility Management) für bewegliche Teilnehmer (engl. roaming subscribers) mit der Aktualisierung der Netzadressen am Aufenthaltsort (engl. location updates) geschieht automatisch durch ein hierfür vereinbartes Protokoll im Netz.

Frage 2.3.4: Bob hat auf der Fahrt zu seinem Bekannten (Anschluss 43-17) sein Mobiltelefon (dt. Händi) ausgeschaltet. Er schaltet sein Mobiltelefon erst wieder ein, als er wieder zuhause ist (Anschluss 32-17). Wie kann ihn die Nachricht (SMS), die Alice ihm während seines Aufenthaltes bei seinem Bekannten geschickt hat, später noch erreichen? Beschreiben Sie eine geeignete Methode, Nachrichten an zeitweise nicht erreichbare Teilnehmer zuzustellen. Wie würde man für Telefonanrufe an Bob vorgehen?

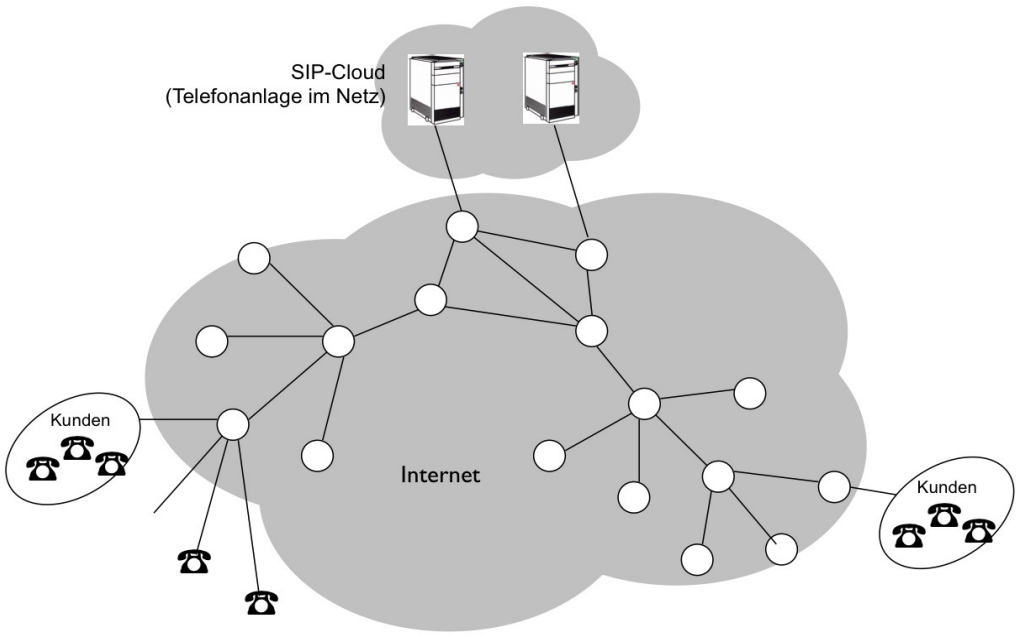
Lösung: (1) Man verwendet einen Speicher (engl. Mailbox) für Nachrichten. Wenn Bob unter seiner in der Datenbank zuletzt gespeichertem Aufenthaltsort nicht erreichbar ist, wird die Nachricht in der Mailbox aufbewahrt. Sobald Bob sein Mobiltelefon wieder eingeschaltet hat und dieses sich in der Datenbank anmeldet, wird die Mailbox abgefragt. Dort für Bob aufbewahrte Nachrichten werden an seine aktuelle Adresse verschickt. (2) Für Telefonanrufe würde man genauso vorgehen: Anrufbeantworter im Netz (Voice Mailbox).

Frage 2.3.5: Im Unterschied zu einem festen Telefonanschluss bzw. festen Internet-Anschluss sind die Teilnehmer über Funk angebunden. Welche Anforderungen bzgl. der Sicherheit gegen Missbrauch und bezüglich der Vertraulichkeit der Verbindungen ergeben sich hieraus?

Frage 2.3.6: In Netz findet sich eine anschauliche Erklärung über die Funktion eines Mobilfunknetzes. Schauen Sie sich diese bitte an und vergleichen Sie die dort gezeigte Struktur mit der Struktur des oben gezeigten Netzes.

2.4. Telefonanlage im Internet

Ein Dienstanbieter bietet als Alternative zu Nebenstellen-Telefonanlagen für Firmen eine Telefonnanlage im Internet an. Als Hardware bei den Kunden sind hierfür nur SIP-Telefone erforderlich, die über den Internet-Anschluss der Firma arbeiten. Die Konfiguration und Bedienung erfolgt per Web-Browser. Als Vorteile werden die bessere Skalierbarkeit und geringere Kosten im Vergleich zur eigenen Telefonanlage angeführt. Der Dienstanbieter betreibt selbst kein Telekommunikationsnetz, sondern mietet nur Server-Kapazität für sein Dienst-angebot.



Verkehrsaufkommen

Der Dienstanbieter bedient insgesamt 1 Million Anschlüsse bei Geschäftskunden, von denen jeder in der Hauptverkehrsstunde 7,2 Anrufe generiert. Die Dauer eines Anrufs beträgt im Mittel 200 Sekunden. Für die Verbindungssteuerung per SIP werden pro Anruf 3 Nachrichten von jeweils 10 kBytes verschickt. Für die Sprachübertragung werden alle 20 ms Sprach-aufzeichnungen in ein RTP-Paket verpackt. Zur Kodierung wird ein G.711 Codec verwendet (Abtastrate von 8000 Samples/s, jeweils mit 8 bit kodiert). Die Umverpackung (Overhead) für die Sprachübertragung beträgt 12 Bytes für den RTP-Paketkopf (Header), 8 Bytes für den UDP-Paketkopf und 20 Bytes für den IP-Paketkopf, sowie 30 Bytes für den Ethernet-Header (inkl. VLAN Tag).

Frage 2.4.1: Bemessung des SIP-Servers (Call Servers): Welche Transaktionsrate ergibt sich insgesamt? Wie groß ist der Durchsatz des Signalisierungsverkehrs?

Lösung: Transaktionsrate: 10^6 * 7,2 pro Stunde / 3600 Sekunden pro Stunde = 2000 tps Transaktionen pro Sekunde

Durchsatz Signalisierungsverkehr: 2000 1/s * 3 * (10 * 1024) Bytes * 8 bit/Byte = 492 Mbit/s

Frage 2.4.2: Sprachverkehr, Overhead: Welche Paketgröße wird verwendet (IP-Pakete)? Wie groß ist der Anteil der Nutzinformation?

Lösung: Paketgröße: 200 Bytes (= Nutzdaten plus Verpackung)

Nutzdaten: 20 ms * 64 kbit/s / 8 bit/Byte = 160 Bytes pro Paket

Verpackung: 12 Bytes (RTP) + 8 Bytes (UDP) + 20 Bytes (IPv4) = 40 Bytes

Anteil der Nutzinformation: 160/200 = 80%

Frage 2.4.3: Sprachverkehr insgesamt: Welche Paketrate ergibt sich insgesamt? Wie groß ist der gesamte Datenstrom (IP-Pakete)?

Lösung: Paketrate (Bemessungsgröße für Media Server):

1/ 20 ms = 50 Pakete/s pro Anruf

Anzahl gleichzeitiger Anrufe: 2000 tps * 200 s = 400 000 Anrufe

Paketrate insgesamt: 20 * 10^6 Pakete pro Sekunde

Datenstrom insgesamt: 200 Bytes * 8 bit/Byte * 20 * 10^6 1/s = 32 Gbit/s

Frage 2.4.4: Ein Kunde nimmt das Angebot für 100 Anschlüsse in Anspruch. Welcher zusätzliche Verkehr im Netzwerk des Kunden ergibt sich auf Schicht 2 (Ethernet)?

Lösung: 100 Anschlüsse / 10^6 Anschlüsse = Anteil von 10^{-4}

32 Gbit/s * 10^{-4} = 3,2 Mbit/s

mit zusätzlichen Overhead 30 Bytes für Ethernet-Rahmen: 230/200 = 1,15: 3,68 Mbit/s

Frage 2.4.5: Die Sprachübertragung im Netzwerk des Kunden konkurriert nun mit regulärem Datenverkehr. Welche Auswirkungen ergeben sich für den Sprachverkehr?

Lösung: Lastabhängige Laufzeitschwankungen; Einbussen der Sprachqualität

Frage 2.4.6: Beschreiben Sie Maßnahmen, mit denen der Kunde die Qualität der Sprachübertragung verbessern kann.

- separates Netzwerk aufbauen für Sprachverkehr
- VLAN für Sprachverkehr konfigurieren
- Verkehrsklassen mit Priorität für Sprachverkehr einführen (QoS, DiffServ)
- Netz überdimensionieren

Sicherheit

Im Vergleich zur klassischen Telefonie ist die Kommunikation über IP-basierte Protokolle und Netzwerke (Ethernet) relativ ungeschützt. Geben Sie eine realistische Einschätzung der Lage. Unterscheiden Sie hierbei bitte folgende Bereiche: (1) Im Netzwerk des Kunden (Ethernet, Lokales Netz), (2) mobile Anwendungen (Apps), (3) Im Internet.

Frage 2.4.7: Welche Bedrohungen bestehen? Welche Schutzmassnahmen gibt es hierfür für die Bereiche (1) und (2)?

Lösung: (1) Im lokalen Netz des Kunden:

- Mithören der Anrufe (beispielsweise durch ARP-Poisoning)
- Ausspionieren von Anruflisten, Passwörtern, Aktivitäten, Anwesenheit, ...
- Schutzmassnahmen: Arbeitsrecht, Betriebsrat, Vorgesetzte, betriebliche Richtlinien
- ...

(2) für mobile Anwendungen (Apps):

- Diebstahl des Endgerätes (Smartphone), dadurch Diebstahl personenbezogener Daten (Telefonbuch, Adressbuch, Kalender, Anruflisten, Dokumente), ...
- Schutzmassnahme; Löschen der Daten durch Fernzugriff
- Belauschen von Konversationen und Ausspionieren des Bildschirms unterwegs
- Schutzmassnahme: betriebliche Richtlinien (Verhalten in der Öffentlichkeit)
- ...

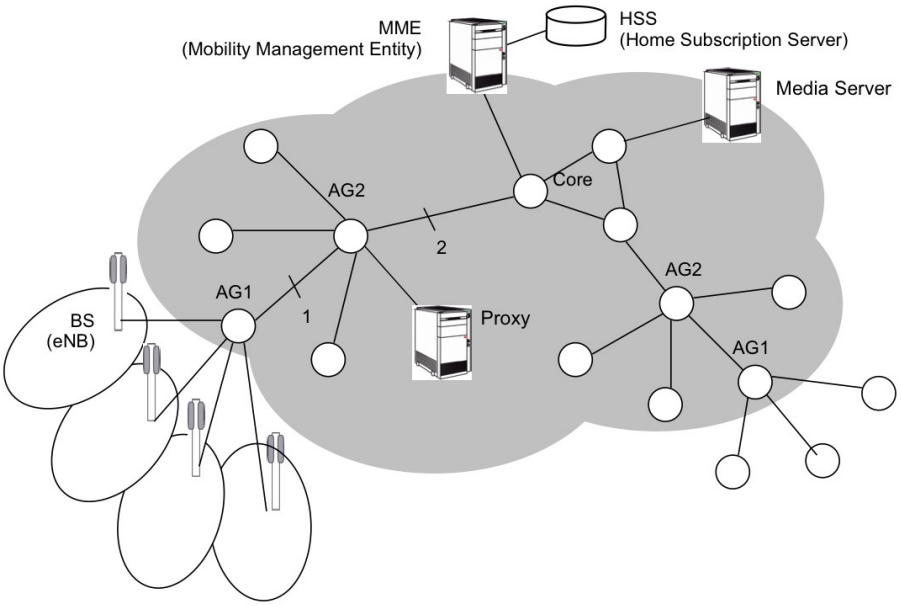
Frage 2.4.8: Welche Bedrohungen bestehen und welche Schutzmassnahmen gibt im Internet (Bereich (3))?

Lösung: (3) Im Internet:

- Mithören der Kommunikation bei ungesicherten Verbindungen, Ausspähen von Daten
- Schutzmassnahme: VPN (verschlüsselte Verbindung, Tunnel) zum Betrieb und zwischen den Standorten
- ...

2.5. Der superschnelle mobile Pauschaltarif

Unter der Bezeichnung „Allnet-Flat“ bietet ein Mobilnetzbetreiber einen netzübergreifenden monatlichen Pauschaltarif an. Das eigene Netz wird nach dem neuesten Mobilfunk-Standard mit Übertragungsgeschwindigkeiten von bis zu 50 Mbit/s (download) beworben. Unter den Vertragsleistungen findet sich der Satz: „Ab einem Datenvolumen von 200 MB wird die Bandbreite im laufenden Monat auf maximal 64 kbit/s (download) und maximal 16 kbit/s (upload) beschränkt.“



Frage 2.5.1: Wie viele Teilnehmer kann eine Funkzelle aufnehmen, unter der Annahme, dass alle Teilnehmer den Pauschaltarif nutzen und bereits ihr freies Kontingent von 200 MB erreicht haben und gedrosselt werden? Welche Datenmenge (GB) kann eine Funkzelle in der Hauptverkehrsstunde übertragen? Nach wie vielen Stunden wären die Kontingente von jeweils 200 MB für die in der ersten Frage errechnete Anzahl an Teil-nehmern erreicht? Welchen Zweck verfolgt dieser Pauschaltarif?

Lösung:

- Eine Funkzelle sendet mit maximal 50 Mbit/s. Im Verhältnis zu 64 kbit/s kann die Funkzelle 781 Teilnehmer aufnehmen.
- In einer Stunde überträgt die Funkzelle 50 Mbit/s * 3600 s / 8 bits/Byte = 22,5 GB.
- Für 781 Teilnehmer mit jeweils 200 MB ergibt sich eine Datenmenge von insgesamt 156,25 GB. Diese Datenmenge kann die Funkzelle in 6,9 Stunden übertragen.

- Pauschale monatliche Einnahmen pro Teilnehmer werden bei einer hohen Teilnehmerzahl interessant. Da die Funkzelle als gemeinsames Übertragungsmedium ihre Kapazität unter allen Teilnehmern aufteilt, muss man hierfür die Datenrate pro Teilnehmer einschränken.

  Bemerkung zu den Konventionen bei der Schreibweise von Einheiten: Kilo, Mega und Giga in Kombination mit Bytes (kB, MB und GB) werden üblicherweise als 2-er Potenzen interpretiert, d.h. 1 kByte = 2^{10} Bytes = 1024 Bytes anstelle von 1000 Bytes. O.g. Berechnung wäre somit streng genommen um einen Faktor $(1000/1024)^3$ zu korrigieren, d.h. 21 GB statt 22,5 GB. Im Rahmen der Abschätzung spielt diese Genauigkeit allerdings keine Rolle.

Frage 2.5.2: Im Knoten AG1 werden jeweils 20 Basisstationen (BS) aggregiert. Jede Basisstation stellt 3 Funkzellen bereit. Das Netz enthält insgesamt 10 Knoten AG2, die jeweils 10 Knoten AG1 aggregieren. Welche Datenraten müssen die mit (1) und (2) bezeichneten Leitungen transportieren? Welche Datenrate ergibt sich am Media-Server? Welche Paketrate muss der Media-Server verarbeiten, wenn ein Paket 512 Bytes Daten enthält? Wie viele Teilnehmer-Sessions bedient der Media-Server gleichzeitig? Welche Verbesserung ließe sich durch Proxy-Server an den Knoten AG2 erzielen, die von den Nutzern vom Media-Server abgefragte Inhalte speichern und bei wiederholten Abfragen an dessen Stelle bereit stellen?

Lösung:

- Datenrate pro Basisstation (mit 3 Funkzellen): 150 Mbit/s. An Leitung (1) ergeben sich 20 * 150 Mbit/s = 3 Gbit/s. An Leitung (2) ergeben sich 10 * 3 Gbit/s = 30 Gbit/s.
- Der Medienserver muss eine Datenrate von 10 * 30 Gbit/s = 300 Gbit/s bedienen.
- Paketrate: mit 8 * 512 = 4096 bit/Paket erhält man aus der Datenrate am Server eine Paketrate von 300 Gbit/s / 4096 bit/Paket = 73,2 Millionen Pakete/s.
- Gleichzeitige Sessions: 300 Gbit/s insgesamt geteilt durch 64 kbit/s pro Nutzer = 4,7 Mio. Sessions (bzw. Teilnehmer)
- Verbesserung: Datenrate und Transaktionsrate am Media-Server werden drastisch reduziert. Die Proxies an AG2 müssen nur 1/10 der Datenrate und der Transaktionsrate des Medien-Servers bedienen.

Frage 2.5.3: Mobilitätsverwaltung. Es wird angenommen, dass das Netz ca. 5 Millionen Teilnehmer bedienen kann. Jeder Teilnehmer verursacht in der Hauptverkehrs-stunde 1,8 Einträge (Location Updates) im zentralen Register (MME - Mobility Management Entity). Jeder Eintrag wird mit einer Nachricht der Länge 2000 Bytes kommuniziert. Welche Transaktionsrate muss das MME bedienen? Welche Datenrate hat der Anschluss des MME? Welchen Zweck verfolgt die Mobilitätsverwaltung? Welchen Zweck verfolgt die mit der Mobilitätsverwaltung kombinierte Authentifizierung der Teilnehmer (im HSS)?

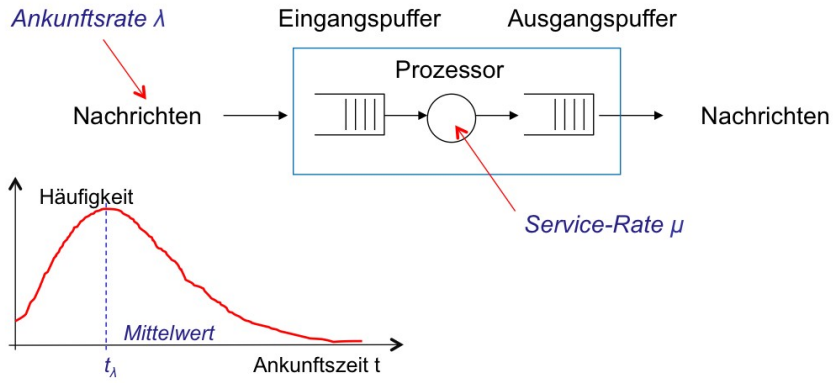
Lösung:

- Transaktionsrate: 5 Mio Teilnehmer * 1,8 Transaktionen / 3600 Sekunden = 2500 Transaktionen pro Sekunde
- Datenrate: 2500 Transaktionen/s * 8 * 2000 bit = 40 Mbit/s.
- Mobilitätsverwaltung: Teilnehmer bleiben im Netz erreichbar.
- Authentifizierung: Schutz vor Manipulationen durch Dritte (nur Teilnehmer mit Vertrag z.B. für den Pauschaltarif können das Netz nutzen).

3. Auslegung der Kommunikationsinfrastruktur

3.1. Verkehrstheorie

Folgende Abbildung zeigt als abstraktes Szenario einen Prozessor, der eingangsseitig mit Nachrichten versorgt wird, und diese nach Verarbeitung ausgangsseitig weiter gibt. Diese Anordnung ist recht universell und trifft auf eine Vielzahl von Prozessen zu, die eingehende Transaktionen verarbeiten. Ein Beispiel wäre die Kasse in einem Supermarkt.



Im Fall der Kasse im Supermarkt entspricht der Prozessor dem Kassierer, der Kunden bedient. Die Kunden (Nachrichten) treffen zufällig an der Kasse ein. Erstellt man eine Häufigkeitsverteilung über den Ankunftszeiten (ein Histogramm), erhält man eine mittlere Ankunftsrate $\lambda = 1/t_\lambda$, beispielsweise 5 Kunden pro Minute. Dieser Mittelwert unterliegt jedoch Schwankungen, wie in der Abbildung gezeigt: Einige Kunden kommen schneller an, andere benötigen deutlich länger.

Der Prozessor kann eine gegebene Menge an Transaktionen (Nachrichten, Kunden) pro Zeiteinheit bearbeiten: Er besitzt eine mittlere Service-Rate μ, beispielsweise 6 Kunden pro Minute. Als Systemauslastung ρ (engl. system utilization) bezeichnet man das Verhältnis der der Ankunftsrate (engl. arrival rate) zur Service-Rate:

$$\rho = \frac{\lambda}{\mu} \qquad (3.1.1)$$

Damit keine der Transaktionen (Nachrichten, Kunden) verloren geht ist eingangsseitig ein Puffer vorgesehen, der sich einfach als Warteschlange interpretieren lässt.

Frage 3.1.1: Wie gross ist die Systemauslastung in oben gegebenen Beispiel? Der Filialeiter möchte eine Systemauslastung von mindestens 100% erzielen. Er begründet seine Forderung damit, dass die Kassenbedienung ja schliesslich 6 Kunden pro Minute bedienen kann. Kann er seine Forderung durchsetzen? Was geschieht, wenn sich die Systemauslastung 100% nähert? Begründen Sie Ihre Aussage.

Lösung: Die Systemauslastung beträgt $\rho = \lambda/\mu = 5/6 = 83\%$. Die Forderung nach annähernd 100% Systemauslastung wäre nur dann zu erfüllen, wenn die eingehenden Transaktionen in einem exakten Zeitraster mit Schrittweite t_λ ankommen. Da diese Zeit jedoch nur ein Mittelwert darstellt, und einige Kunden deutlich später ankommen, gibt es nach Öffnung des Marktes an der Kasse zeitliche Lücken, die die Kassenbedienung nicht wieder aufarbeiten kann, da der Mittelwert ja eingehalten wird, und daher auch einmal Kunden in kürzeren Intervallen eintreffen.

Es bildet sich eine Warteschlange. Die Länge der Warteschlange ist abhängig von der Systemauslastung: Je höher die Systemauslastung, desto länger die Schlange. Dieses Verhalten deckt sich mit der praktischen Erfahrung an Kassen im Supermarkt. Nähert sich die Systemauslastung 100%, werden die Warteschlangen endlos.

Frage 3.1.2: Warteschlangen. Unter der Voraussetzung, dass die Ankunftszeiten der ankommenden Transaktionen Poisson-verteilt sind, lässt sich die Länge N (= Anzahl wartender Transaktionen) der Warteschlange in Abhängigkeit der Systemauslastung ρ berechnen. Es ergibt sich:

$$N = \frac{\rho}{1-\rho} \qquad (3.1.2)$$

Berechnen Sie die Länge der Warteschlange für Systemauslastungen von 80%, 90%, 95% und 98%.

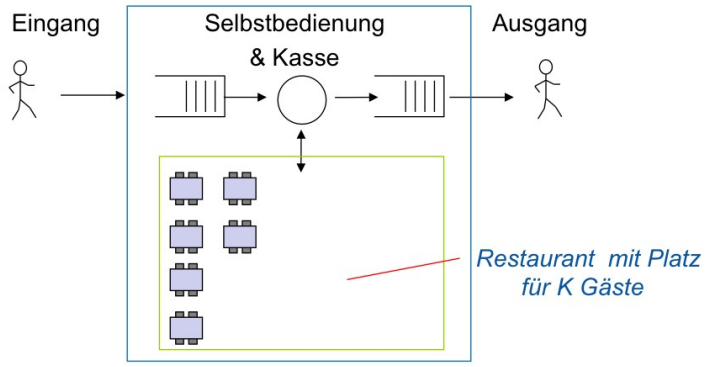
Lösung: Man erhält N = 4, 9, 19 und 49 für die oben genannten Systemauslastungen.

Frage 3.1.3: Am späten Nachmittag steigt die Ankunftsrate im Supermarkt auf 17 Kunden pro Minute. Wie reagiert der Filialleiter? Wie viele Kassen raten Sie ihm zu öffnen? Begründen Sie Ihre Empfehlung?

Frage 3.1.4: Multi-Prozessorsystem. In einem Smart-Grid soll eine Transaktionsrate (= Ankunftsrate) von 10000 Transaktionen pro Sekunde verarbeitet werden. Der Prozessor besteht aus einzelnen Servern, die in Lastaufteilung arbeiten (engl. load sharing). Ein einzelner Server kann 2000 Transaktionen pro Sekunde bedienen. Das Gesamtsystem soll bei einer Systemauslastung von 80% betrieben werden. Wie viele Server möchten Sie verwenden? Hinweis: Bei einem Multi-Prozessorsystem mit m Prozessoren, die jeweils mit einer Service-Rate von μ arbeiten, beträgt die Service-Rate insgesamt μ_{ges} = m μ.

3.2. Transaktionsverarbeitung

Folgende Abbildung zeigt ein Selbstbedienungsrestaurant. Unter einer Transaktion wird hierbei die Verarbeitung eines Gastes verstanden, d.h. der Gang von der Selbstbedienungstheke zur Kasse, die anschliessende Verweildauer im Restaurant-Bereich zur Einnahme der Speisen bis zum Räumen des Platzes.



Frage 3.2.1: Die mittlere Aufenthaltsdauer eines Gastes (Dauer der Transaktion) beträgt 10 Minuten. Der Restaurantbereich fasst K = 200 Gäste. Wie viele Gäste pro Minute (bzw. pro Stunde) muß die Kasse bedienen können? Benennen Sie folgende Größen: (1) die Transaktionsrate (= Ankunftsrate), (2) die Service-Rate bei gegebener Systemauslastung.

Lösung: Bei vollbesetztem Restaurant werden im Mittel 200 Gäste / 10 Minuten = 20 Gäste pro Minute ausgetauscht. Diese Transaktionsrate entspricht der Ankunftsrate. Damit an der Kasse keine unnötig langen Warteschlangen entstehen, sollte die Kasse in der Hauptbetriebszeit mehr als 20 Gäste pro Minute bedienen können. Bei einer Systemauslastung von 80% sollte die Kasse beispielsweise 25 Gäste pro Minute bedienen können.

Frage 3.2.2: Anzahl paralleler Sessions. Im Beispiel aus 3.2.1 besteht ein Zusammenhang zwischen der Transaktionsrate und der Anzahl paralleler Transaktionen (bzw. Sessions = Anzahl K der Plätze im Restaurantbereich). Erläutern Sie diesen Zusammenhang.

Lösung: Transaktionsrate [1/s] * Dauer der Transaktion [s] = Anzahl paralleler Transaktionen

Statt Transaktionen ist auch der Begriff „Sessions“ im Sinne von in Bearbeitung befindlichen Transaktionen gebräuchlich. Beispiel:

- Transaktionsrate: 20 Gäste pro Minute
- Dauer der Transaktion: 10 Minuten
- Anzahl gleichzeitig in Bearbeitung befindlicher Transaktionen (Sessions): 200 Gäste

Frage 3.2.3: Server für Bankautomaten. Ein Server kann eine Rate von 200 Transaktionen pro Sekunde an Bankautomaten im Netz bedienen (Transaktion = Geld abheben). Eine Transaktion dauert im Mittel 2 Minuten. Für die Dauer einer Transaktion muss der Server einen Kundendatensatz von 512 Bytes im Arbeitsspeicher halten. Wie viele parallele Transaktionen muss der Server bedienen können? Wie viel Arbeitsspeicher benötigt der Server?

Lösung: (1) Transaktionsrate [1/s] * Dauer der Transaktion [s] = Anzahl paralleler Transaktionen

(2) Arbeitsspeicher: Anzahl paralleler Transaktionen * Bytes/Transaktion = Bytes.

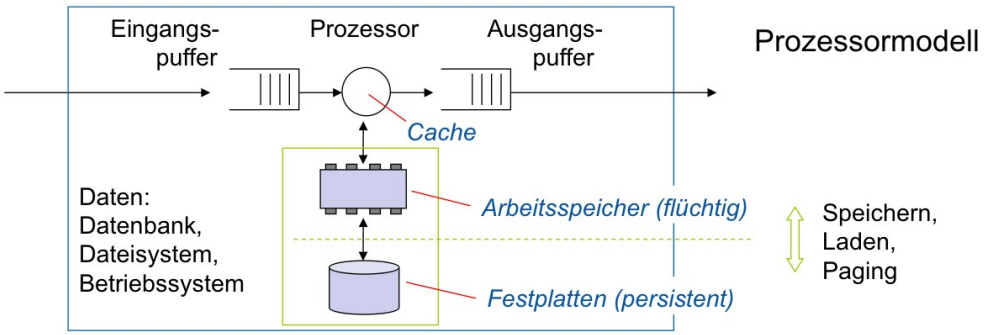
Mit den Zahlen aus dem Beispiel: (1) 24000 parallele Transaktionen (Sessions), (2) 12 MBytes.

Frage 3.2.4: Telefonanlage. Eine Telefonanlage soll 2000 Anrufe gleichzeitig bedienen. Die Dauer eines Anrufs beträgt 2 Minuten. Welche Transaktionsrate muss die Telefonanlage unterstützen? Wie viel Arbeitsspeicher wird benötigt, wenn zu jedem Anruf (zur Abrechnung) ein Kundendatensatz von 512 Bytes im Arbeitsspeicher gehalten werden muss?

Lösung: (1) Transaktionsrate [1/s] = Anzahl paralleler Transaktionen / Dauer der Transaktion [s] = 17 Anrufe pro Sekunde. Während also 2000 Teilnehmer gleichzeitig sprechen, legen pro Sekunde 17 Teilnehmer auf und 17 andere Teilnehmer starten pro Sekunde einen Anruf.

(2) Arbeitsspeicher: 2000 Anrufe * 512 Bytes = 1 MByte.

Frage 3.2.5: Prozessmodell. Für einen Prozess bzw. für einen Prozessor wird in die folgender Abbildung gezeigte Abstraktion verwendet.



Erläutern Sie folgende Begriffe: (1) Transaktion, (2) Transaktionsrate, (3) Dauer einer Transaktion, (4) Anzahl paralleler Transaktionen, (5) erforderliche Daten im Arbeitsspeicher pro Transaktion (6) Menge an parallel verfügbaren Daten im Arbeitsspeicher insgesamt, (7) Ankunftsrate, (8) Servicerate, (9) Systemauslastung, (10) Eingangspuffer und Ausgangspuffer.

Frage 3.2.6: Transaktionsverarbeitung. Der in Frage 3.2.5 gezeigte Prozessor verarbeitet Prozess-daten. Pro Sekunde stellt er als Client 10000 Anfragen an die Server, die ihn über das Netz mit Informationen versorgen. Zu jeder Anfrage schickt er eine Empfangsbestätigung und schickt die gewonnene Information zur Visualisierung weiter an einen anderen anderen Prozessor. Die Dauer einer Transaktion beträgt 2 Sekunden, pro Transaktion müssen 2 kBytes Daten im Arbeitsspeicher gehalten werden. Wie viele parallele Transaktionen bedient der Client und wie viel Arbeitsspeicher wird hierfür benötigt?

3.3. Verkehrsmodelle

Unter einem Verkehrsmodell versteht man alle Annahmen, die über ein geplantes Angebot bekannt sind. Hierunter fallen:

- Anzahl der Teilnehmer bzw. Geräte im Netz
- Anzahl der Transaktionen pro Teilnehmer in der Hauptbetriebsstunde [1/h] bzw. [1/s]
- Dauer einer Transaktion [s]
- Datensatz im Arbeitsspeicher pro Transaktion [Bytes]
- Nachrichten pro Transaktion, die über das Netz kommuniziert werden
- Datenmenge einer Nachricht [bit], die über das Netz kommuniziert wird.

Unter der Hauptbetriebsstunde (bzw. Hauptverkehrsstunde) versteht man hierbei die Tageszeit, für die die Anlage ausgelegt werden soll.

Frage 3.3.1: Eine Telefonanlage soll auf folgendes Verkehrsmodell ausgelegt werden:

- 1 Million Teilnehmer
- 3,6 Anrufe pro Teilnehmer in der Hauptverkehrsstunde
- 200 Sekunden Anrufdauer (Dauer einer Transaktion)
- 1 kByte Daten pro laufender Transaktion in der Anlage.

Welche Transaktionsrate muss die Anlage bedienen können? Wie viele parallele Transaktionen muss die Anlage bedienen können? Welcher Arbeitsspeicher wird hierfür benötigt?

Lösung: (1) 1000 Transaktionen pro Sekunde, (2) 200 000 parallele Transaktionen, (3) 200 MBytes.

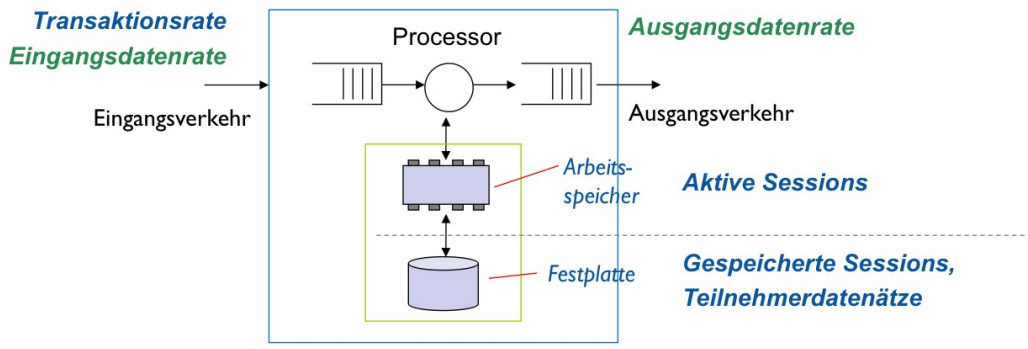
Frage 3.3.2: Datenrate. Im Datenmodell aus Aufgabe 3.3.1 werden pro Transaktion 4 Nachrichten über das Netz ausgetauscht (jeweils gesendet und empfangen). Eine Nachricht ist 512 Bytes lang. Welche Datenrate muss die Anlage bedienen können?

Lösung: (1) Bits pro Transaktion = 4 Nachrichten * 512 Bytes * 8 bit/Byte = 16384 bits pro Transaktion.

(2) Datenrate = Bits pro Transaktion [bit] * Transaktionen pro Sekunde (Transaktionsrate) [1/s]

Im Beispiel: 16384 bit * 1000 1/s = 16,384 Mbit/s (= 16,384 * 10^6 bit/s).

Frage 3.3.3: Prozessormodell. Folgende Abbildung zeigt das Prozessormodell.



Erläutern Sie die Begriffe (1) Transaktionsrate und (2) Datenrate. Was bedeuten diese Größen für die Auslegung des Systems? Wonach richtet sich die Wahl des Prozessors (CPU)? Wie viel Arbeitsspeicher bzw. persistenter Speicher wird benötigt?

Frage 3.3.4: Datenrate und Paketrate. Der oben beschriebene Prozessor soll als Paketfilter eingesetzt werden. Ein Strom von Daten (Sprachpaketen einer Voice over IP Anwendung) soll nach bestimmten

Kriterien gefiltert bzw. nach bestimmten Inhalten abgesucht bzw. abgehört werden. Es liegt folgendes Verkehrsmodell vor:

- 1 Million Teilnehmer
- 3,6 Anrufe pro Teilnehmer in der Hauptverkehrsstunde
- 200 Sekunden Anrufdauer (Dauer einer Transaktion)
- jeweils 20 ms pro Paket
- 256 Bytes Paketgröße (inklusive Overhead).

Berechnen Sie (1) die Paketrate pro Transaktion (Anruf), (2) die Anzahl Pakete pro Transaktion (Anruf), (3) die Transaktionsrate, (4) die Anzahl paralleler Transaktionen, (5) die Paketrate insgesamt, (6) die Datenrate insgesamt. (6) Worauf ist das Paketfilter auszulegen?

Lösung: (1) 50 Pakete pro Sekunde pro Transaktion, (2) Anzahl Pakete pro Transaktion = Paketrate der Transaktion [1/s] * Dauer der Transaktion [s] = 50 1/s * 200 s = 10 000 Pakete pro Anruf, (3) Transaktionsrate 10^6 * (3,6/3600) 1/s = 1000 1/s (Anrufe pro Sekunde), (4) Anzahl paralleler Transaktion (Sessions) = Transaktionsrate [1/s] * Dauer der Transaktion [s] = 1000 1/s * 200 s = 200.000 parallele Transaktionen, (5) 200.000 parallele Transaktionen * 50 Pakete/s = 10 Millionen Pakete/s, (6) Datenrate insgesamt = Paketrate insgesamt [1/s] * Daten [bit] pro Paket: $10*10^6$ 1/s * 256 * 8 bit = 20,48 Gbit/s. (6) Auslegungsgrößen für das Paketfilter: Paketrate insgesamt = Transaktionsrate des Filters.

3.4. Redundanz

Um die Systemverfügbarkeit zu erhöhen, werden einzelne Systemkomponenten mehrfach vorgesehen. Bei einem Teilausfall ist somit ein anderer Teil des Systems überlebensfähig. Das Prinzip beruht auf der Verbundwahrscheinlichkeit für einen Systemausfall. Beispiel:

- Die Wahrscheinlichkeit, dass die Komponente 1 ausfällt, beträgt $P_1 = 0{,}01 = 1\%$.
- Die Wahrscheinlichkeit, dass die Komponente 2 ausfällt, beträgt $P_2 = 0{,}01 = 1\%$.
- Sofern die Ausfälle beider Komponenten voneinander unabhängig sind (im Sinne statistisch unabhängige Zufallsprozesse), beträgt die Wahrscheinlichkeit, dass beide Komponenten zur gleichen Zeit ausfallen: $Pges = P_1\ P_2 = 10^{-4} = 0{,}01\ \%$.

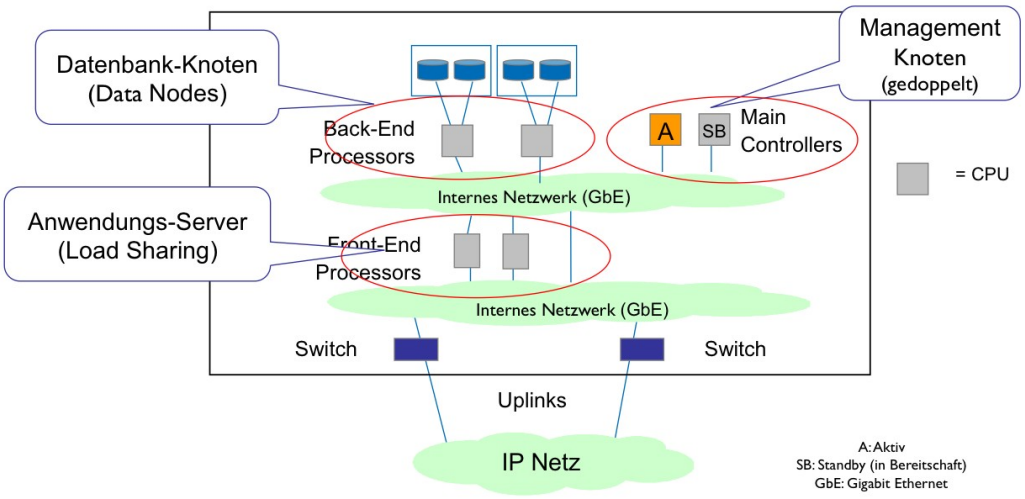
Während eine Komponente eine Verfügbarkeit von $P_1^{-1} = 99\%$ besitzt, besitzt das Gesamtsystem somit eine Verfügbarkeit von 99,99%.

Frage 3.5.1: Ein fairer Würfel wirft mit einer Wahrscheinlichkeit $P_6 = 1/6$ die Zahl 6. Die Zahl 6 soll vermieden werden. Wir groß ist die Wahrscheinlichkeit: (1) mit einem Würfel keine Zahl 6 zu werfen? (2) mit 2 Würfeln zugleich nicht die Zahl 6 zu werfen? Wie viele Würfel wären erforder-lich, damit mit einer Wahrscheinlichkeit von 99,999% bei einem Wurf nicht alle Würfel zugleich die Zahl 6 werfen?

Frage 3.5.2: Würfelwette. Wenn Sie mit N Würfeln spielen und mit einem Wurf mindestens ein Würfel eine 6 zeigt, gewinnen Sie. Im anderen Fall gewinnt der Gegner. Es wird unter zwei Spielern abwechselnd gewürfelt. Wie viele Würfel nehmen Sie, damit das Spiel interessant ist?

Frage 3.5.3: Folgende Abbildung zeigt ein System zur Transaktionsverarbeitung. Die Knoten haben unterschiedliche Aufgaben:

- Anwendungsprozessoren (Vorverarbeitung, z.B. Protokollstack bedienen, Informationen extrahieren bzw. verpacken)
- Datenbank-Knoten: Informationen verarbeiten, speichern, bzw. extrahieren
- Management-Knoten: Überwachung des Systems auf Funktionsfähigkeit, ggf. Umschaltvorgänge auslösen bzw. Alarme generieren
- persistenter Speicher zum Aufbewahren der Daten.



Wo sind Komponenten mehrfach vorhanden und können redundant genutzt werden? Was bedeutet hierbei der Begriff Lastaufteilung (engl. Load-Sharing)? Wie verhält sich das System im Fehlerfall (Ausfall jeweils einer Komponente)? Was geschieht bei Ausfall eines der Management-Knoten? Wie funktioniert das Umschalten bzw. Ausweichen auf eine redundante Komponente innerhalb des Systems?

Frage 3.5.4: Ein Server soll für eine Systemverfügbarkeit von 99,999% ausgelegt werden. Welcher Ausfallzeit entspricht diese Forderung in einem Jahr als Bezugsintervall? Wie viele Komponenten bzw. Teilsysteme sind sind erforderlich, wenn eine Komponente eine Verfügbarkeit von 99% hat?

Bei der Betrachtung der gesamten Systemverfügbarkeit war die statistische Unabhängig-keit der Teilprozesse vorausgesetzt, d.h. die Fehlerursachen der Komponenten sind voneinander unabhängig. Welche Fehlerfälle widersprechen dieser Forderung? Wie können Sie das System gegen solche Fehler absichern?

4. Sichere Kommunikation

4.1. Bedrohungen und Massnahmen

Unter sicherer Kommunikation versteht man, dass Informationen, die zwischen zwei Teilnehmern A (Alice) und B (Bob) über Kommunikationsnetze ausgetauscht werden, folgenden Ansprüchen genügen:

- Vertraulichkeit (engl. Confidentiality): Informationen sollten nicht unerwünscht an Dritte gelangen (Beispiele: Briefgeheimnis, Fernmeldegeheimnis, Schutz personenbezogener Daten, firmenvertrauliche Daten)
- Integrität (engl. Integrity): Unversehrtheit. Die kommunizierte Information sollte nicht verfälscht sein.
- Verfügbarkeit (engl. Availability): Anwendungen und Dienste sollten für autorisierte Nutzer jederzeit verfügbar sein.

Hierbei geht man davon aus, dass die Kommunikation über das Netz grundsätzlich nicht sicher ist. Als Bedrohungen unterschiedet man:

- Passive Angriffe: Passive Angriffe sind dadurch gekennzeichnet, dass der Angreifer nicht in die Kommunikation eingreift. Er bleibt passiv. Beispiele: Mithören, Passwörter ausspionieren, Daten kopieren, Identitätsdiebstahl, Verhaltensmuster und Nutzerprofile erstellen. Die Gefahr passiver Angriffe besteht darin, dass sie schwer erkennbar sind und unbemerkt bleiben.
- Aktive Angriffe: Ein aktiver Angreifer greift in die Kommunikation ein. Er hinterlässt hierdurch Spuren. Beispiele: Manipulation von Daten, Verbindungen entführen, Geräte manipulieren (zum Mitschneiden von Daten, durch Einführen von Schadsoftware, durch Vandalismus), unter falscher bzw. vorgetäuschter Identität agieren, Übertölpeln von Nutzern (z.B. zum ausspionieren von Passwörtern), Boykott von Anlagen (Denial-of-Service).

Hinweis: Im englischen Sprachgebrauch bezeichnet man die auf oben genannte Weise definierte Sicherheit im Sinne von Schutz gegen äußere Einflüsse als „Security“. Mit dem Begriff „Safety“ bezeichnet man die Betriebssicherheit bzw. funktionale Sicherheit eines Systems im Sinne von Gefahren für Leben und Umwelt, die von dem System ausgehen.

Frage 4.1.1: Nennen Sie Angriffe auf die Vertraulichkeit? Welche Schutzmaßnahmen gibt es hierfür?

Lösung: Angriffe: Mithören, „Datendiebstahl“. Schutzmaßnahmen: Zugangskontrolle, Authentifizierung, Autorisierung, Verschlüsselung der Information.

Frage 4.1.2: Nennen Sie Angriffe auf die Integrität? Welche Schutzmaßnahmen gibt es hierfür?

Lösung: Angriffe: Identitätsdiebstahl, manipulierte Daten. Schutzmaßnahmen: Sichere Passwörter, Prüfsummen, Signatur.

Frage 4.1.3: Nennen Sie Angriffe auf die Verfügbarkeit? Welche Schutzmaßnahmen gibt es hierfür?

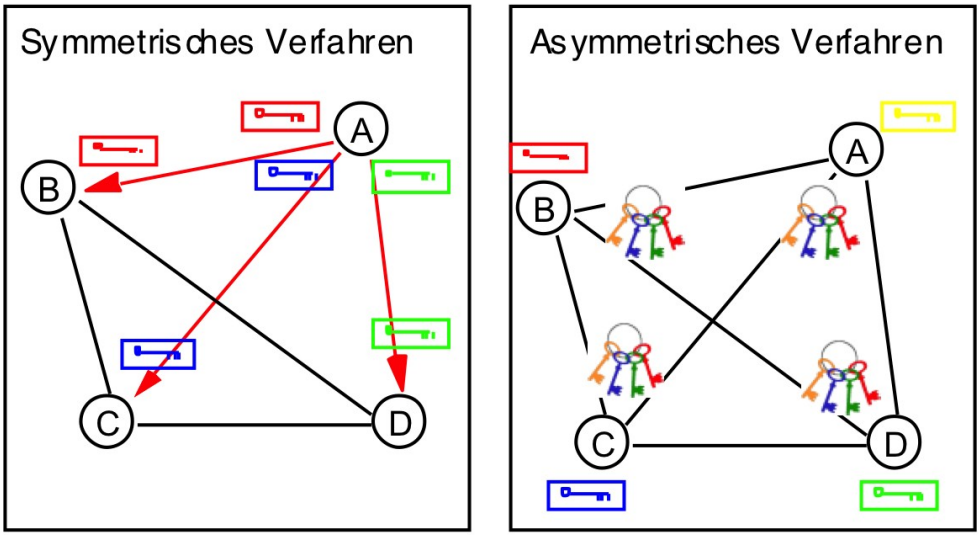
Lösung: Angriffe auf die Systemverfügbarkeit: Überflutung (Denial-of-Service), schädliche Software. Schutzmaßnahmen: Lastabwehr, Paketfilter, Redundante Systeme, Erkennung von Schadsoftware, kontinuierliche Behebung der Lücken im System, Kapselung der Systeme, rollenbasiertes Sicherheitsmodell (Rollen, Rechte und Pflichten werden definiert und eingefordert).

Frage 4.1.4: Welches Diebesgut wird bei einem Datendiebstahl entwendet? Wie fällt der Verlust auf? Welcher Unterschied bestehen zu einem materiellen Diebstahl? Um welche Art von Angriff handelt es sich?

4.2. Symmetrische und asymmetrische Schlüssel

Die Vertraulichkeit einer Kommunikation lässt sich durch Verschlüsselung der zwischen A und B ausgetauschten Informationen gewährleisten. Hiebei geht man davon aus, dass Nachrichten zwischen A und B zwar jederzeit mitgehört oder abgefangen werden können, dass jedoch der Inhalt dem Angreifer unzugänglich bleibt, sofern er sie nicht entschlüsseln kann.

Unter der Voraussetzung, dass die eingesetzten Verfahren zur Verschlüsselung sicher sind, setzt die Fähigkeit zur Entschlüsselung die Kenntnis des passenden Schlüssels voraus. Folgende Abbildung zeigt die Kommunikationsbeziehungen zwischen vier Parteien A, B, C und D über ein Netz.



Im linken Teil der Abbildung werden symmetrische Schlüsselpaare verwendet: Damit A mit B kommunizieren kann, benötigen beide den gleichen symmetrischen Schlüssel. Wenn A mit C verschlüsselt kommunizieren möchte, verwenden beide ein anderes Schlüsselpaar.

Im rechten Teil der Abbildung werden asymmetrische Schlüsselpaare eingesetzt: Hier erhält jeder Kommunikationspartner einen privaten Schlüssel, den er vor allen anderen geheim halten muss. Als Gegenstück des privaten Schlüssels dient ein passender öffentlicher Schlüssel, den jeder wissen darf. Öffentliche Schlüssel der jeweiligen Kommunikationspartner bewahren die Teilnehmer an einem Schlüsselbund auf.

Frage 4.2.1: Symmetrische Schlüssel. Bei der Verwendung symmetrischer Schlüsselpaare muss für jede Kommunikationsbeziehung ein eigenes Paar verwendet werden. Wie viele Schlüsselpaare werden für 3 Kommunikationspartner benötigt? Wie viele Schlüsselpaare werden für 4 Kommunikationspartner benötigt? Verallgemeinern Sie auf N Kommunikationspartner. Wie viele Schlüsselpaare wären für N=1000 Kommunikationspartner nötig?

Lösung: Die Anzahl K der Schlüsselpaare entspricht der Anzahl der Kanten und Diagonalen des N-Ecks aus N Kommunikationspartnern, d.h. der Anzahl der möglichen Kommunikationsbeziehungen.

1. Durch Abzählen ermittelt man: N=2: k=1; N=3, k=3; N=4, k=6; N=5, k=10. Eine Gleichung, die hierzu passt, wäre k= N*(N-1)/2.
2. Interpretation: Die Anzahl der Kanten k eines voll vermaschten Graphen mit N Knoten beträgt k= N*(N-1)/2. Geometrie: Die Zahl der Diagonalen und Kanten eines N-Ecks entspricht k.

Für N = 1000 wären somit annähernd $N^2/2 = 500\,000$ Schlüsselpaare erforderlich. Der Aufwand steigt gemäß der Beziehung $k(N) \simeq N^2/2$ quadratisch mit der Anzahl der Kommunikationspartner.

Frage 4.2.2: Asymmetrische Schlüssel. Bei der Verwendung asymmetrischer Schlüsselpaare verwendet jeder Kommunikationspartner einen geheimen, privaten Schlüssel, sowie einen passenden öffentlichen Schlüssel. Wie viele Schlüsselpaare werden für 4 Kommunikationspartner benötigt? Verallgemeinern Sie auf N Kommunikationspartner. Wie viele Schlüsselpaare wären für N=1000 Kommunikationspartner nötig?

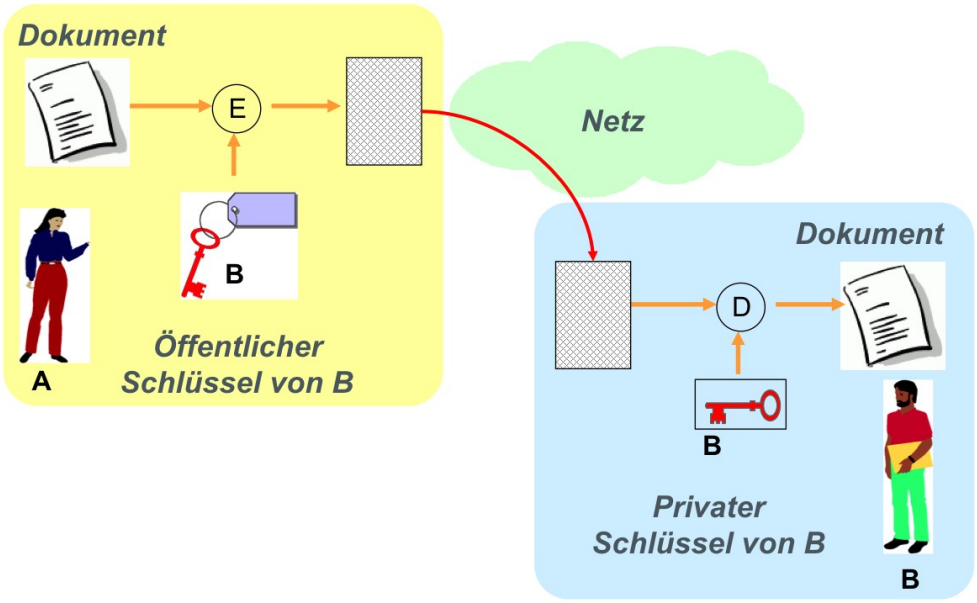
Lösung: Hier entspricht die Anzahl der Schlüsselpaare einfach der Anzahl der Kommunikationspartner, d.h. k(N) = N. Der Aufwand wächst somit linear mit der zahl der Kommunikationspartner.

Frage 4.2.3: Schlüsselmanagement. Die symmetrischen Schlüsselpaare bzw. die privaten Schlüssel müssen geheim gehalten werden, und können somit nicht über das Netz kommuniziert werden. Wie gelingt die Verteilung der Schlüssel in beiden Fällen? Welches Verfahren hat diesbezüglich Vorteile? Wie lässt sich ein kompromittierter Schlüssel zurück rufen bzw. beseitigen?

Frage 4.2.4: Rechenaufwand. Asymmetrische Verfahren sind sehr rechenaufwändig im Vergleich zu symmetrischen Verschlüsselungsverfahren, haben jedoch den Vorteil des einfachen Schlüsselmanagements. Wie lassen sich beide Verfahren so kombinieren, dass die vorteilhaften Seiten genutzt werden können?

4.3. Verschlüsselung

In folgender Abbildung schickt Alice ein verschlüsseltes Dokument an Bob.



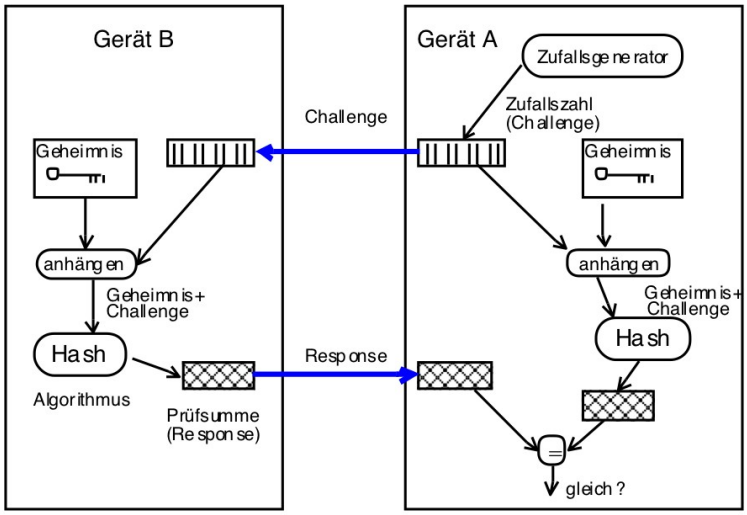
Sie verwendet hierzu ein asymmetrisches Schlüsselpaar. In der Darstellung bedeuten „E“ die Verschlüsselung (engl. Encryption) und „D“ die Entschlüsselung (engl. Decryption). Die Art der Verschlüsselungsverfahren ist hierbei nicht weiter relevant. „E“ und „D“ sind derart beschaffen, dass eine Verkettung beider Verfahren wieder Klartext erzeugt.

Frage 4.3.1: Weshalb verwendet Alice den öffentlichen Schlüssel von Bob? Hätte sie seinen privaten Schlüssel verwenden können? Hätte Sie ihren privaten Schlüssel verwenden können?

Lösung: Wenn Bob seinen privaten Schlüssel geheim hält, kann außer ihm das mit seinem öffentlichen Schlüssel verschlüsselte Dokument niemand öffnen. Wenn Alice ihren privaten Schlüssel verwendet, kann jeder mit ihrem öffentlichen Schlüssel das Dokument wieder her stellen. Der Inhalt wäre so nicht geschützt.

Frage 4.3.2: Wie geht Bob vor, wenn er Alice seinerseits ein verschlüsseltes Dokument schicken möchte? Skizzieren Sie den Ablauf und erläutern Sie Ihren Vorschlag.

Frage 4.3.3: Folgende Abbildung zeigt ein Verfahren, mit dem ein Gerät (Gerät A) die Identität eines anderen Gerätes (Gerät B) überprüfen kann. Solche Verfahren werden beispielsweise eingesetzt, um die Zugangsberechtigung eines Mobiltelefons (Gerät B) durch das Netz (Gerät A) zu überprüfen. Ein andere Beispiel wäre z.B. ein Gerät A (z.B. Mobiltelefon) bekanntes Bluetooth Gerät B (z.B. Bluetooth-Sprechgarnitur bzw. -Freisprecheinrichtung).



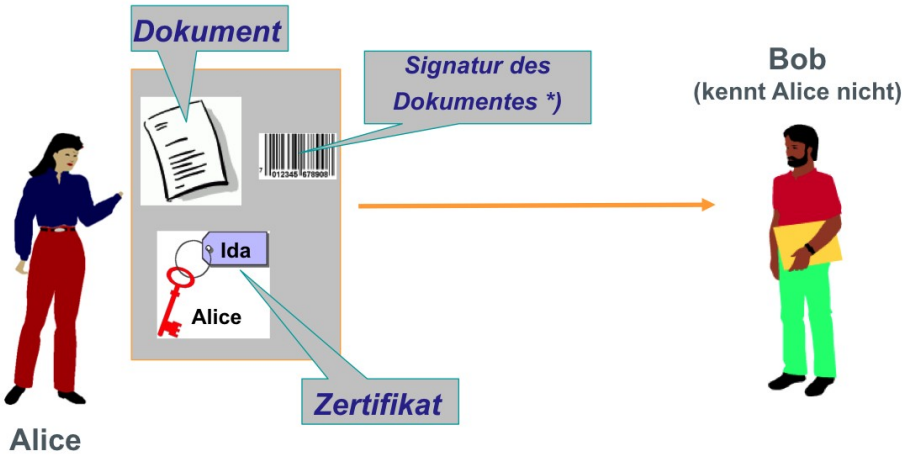
Erläutern Sie das Verfahren. Wodurch wird der Identitätsnachweis für Gerät B erbracht? Warum wird das Geheimnis (geheimer Schlüssel) nicht über das Netz übertragen? Wie gelangt das Geheimnis auf beide Geräte.

Lösung: Identitätsnachweis durch Kenntnis des Geheimnisses. Verbreitung des Geheimnisses: muss vorher geladen werden, z.B. SIM-Karte, Bluetooth-Pairing, separater Kommunikationskanal (SMS).

Frage 4.3.4: Das in Frage 4.3.3 gezeigte Verfahren ist für einen sicheren Identitätsnachweis nicht ausreichend: Das Netz (bzw. Gerät A) muss seine Identität gegenüber dem Mobiltelefon (Gerät B) nicht nachweisen. Wie könnte man das Verfahren für einen beiderseitigen Identitätsnachweis erweitern? Wie ist der gegenseitige Identitätsnachweis in anderen Fällen gelöst, z.B. beim Home Banking? Hinweis: Wechselseitige Identitätsnachweise sind üblich, z.B. bei einer Fahrkartenkontrolle durch einen uniformierten Bediensteten (Uniform als Nachweis) bzw. durch einen Ausweis des Bediensteten (bzw. Polizeimarke etc).

4.4. Signatur

Wenn man über ein Netz ein Dokument austauschen möchte, z.B. einen Kaufvertrag, möchte man den Vertragspartner gerne eindeutig identifizieren und gewährleisten, dass das Dokument unverfälscht übertragen wurde. Folgende Abbildung zeigt die Situation, dass Bob mit Alice einen Vertrag abschliessen möchten. Alice ist jedoch Bob unbekannt, er kann sie daher nicht aus der Kom-munikationsbeziehung heraus identifizieren.



Daher erbringt Alice eine Nachweis über Ihre Identität und über den Ursprung des Dokumentes. Der Nachweis iwird dadurch erbracht, dass Alice mit dem Dokument ein Zertifikat schickt, das beglaubigt, dass ihr der ebenfalls mitgeschickte öffentliche Schlüssel gehört. Dieses Zertifikat kann Bob nachprüfen. Mit ihrem geheimen (privaten) Schlüssel signiert (= verschlüsselt) Alice eine Prüfsumme des Dokuments. Bob kann aus dem Dokument ebenfalls eine Prüfsumme berechnen. Die von Alice geschickte signierte Prüfsumme entschlüsselt er mit dem öffentlichen Schlüssel von Alice. Stimmen beide Prüfsummen überein, ist der Identitätsnachweis für Alice (sie besitzt den zugehörigen privaten Schlüssel) und der Ursprungsnachweis über das Dokument erbracht.

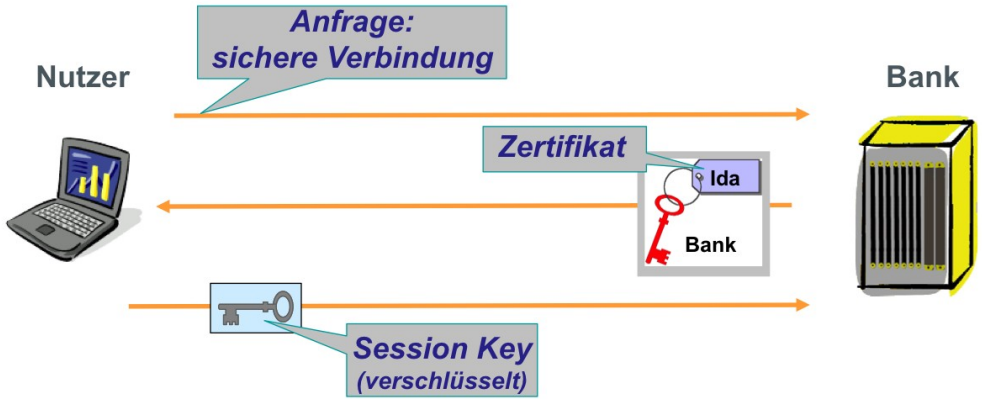
Frage 4.2.1: Identitätsnachweise. Im praktischen Leben kommt es vor, dass man seine Identität nachweisen muß. Nennen Sie einige typische Situationen. Nennen Sie die Mittel, mit denen die Identität hierbei nachgewiesen wird.

Lösungsbeispiel: Polizeiliche Kontrolle (Personalausweis), Einreise in ein Land (Reisepass), Zugang zum Betriebsgelände (Firmenausweis), Zugang zum Home Banking (Benutzerkennung und Passwort), Smartphone (Fingerabdruck bzw. Zugangscode), Zugang zum Mobilfunknetz (SIM-Karte), Zugang zum Firmennetz (VPN-Token), Internet-Zugang mit DSL- bzw. Kabelmodem (Benutzerkennung und Passwort), Apps installieren (Signatur wird überprüft), …

Allgemeine Mittel zum Identitätsnachweis: (1) Kenntnis einesGeheimnisses („ich weiss etwas“), (2) Ausweis, physikalischer Schlüssel bzw. Token („ich habe etwas“), (3) biometrische Merkmale („ich bin es“), sowie (4) Kombinationen hieraus.

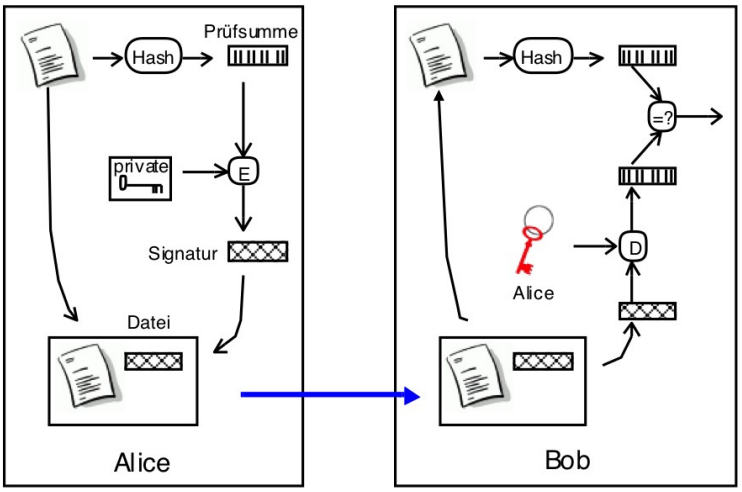
Frage 4.2.2: Notarielle Beglaubigung, bzw. beglaubigte Dokumente. Wichtige Verträge, wie z.B. Kaufverträge für Grundstücke, Testamente etc werden notariell beglaubigt. Andere Dokumente, wie z.B. Zeugniskopien werden von der ausstellenden Stelle bzw. einer Vertrauensperson beglaubigt bzw. zertifiziert. Erläutern Sie die Funktionsweise einer Beglaubigung. Worauf beruht das Vertrauen in ein beglaubigtes Dokument? Wie lässt sich die Beglaubigung nachprüfen?

Frage 4.2.3: Home Banking (SSL, HTTPS). Folgende Abbildung zeigt den Ablauf des Aufbaus einer sicheren Verbindung mit Hilfe eines Web-Browsers. Beschreiben Sie den Ablauf. Worauf beruht die Sicherheit der Verbindung? Wodurch ist gewährleistet, dass Sie beim Home Banking nicht auf einem vorgetäuschten, manipulierten Server landen, der nur Ihre Kontonummer und Transaktionsnummern ausspähen möchte?



Lösung: (1) Ablauf: Der Nutzer entnimmt dem Zertifikat den öffentlichen Schlüssel der Bank. Mit dem öffentlichen Schlüssel verschlüsselt er einen zufälligen, symmetrischen Session Key, den er der Bank übermittelt. Der Session Key wird nun für den Austausch verschlüsselter Nachrichten verwendet. (2) Vertrauensbeziehung: Beruht nur auf dem Zertifikat. Wenn der Browser das Zertifikat akzeptiert, gehen Sie einem potentiellen Betrüger ins Netz.

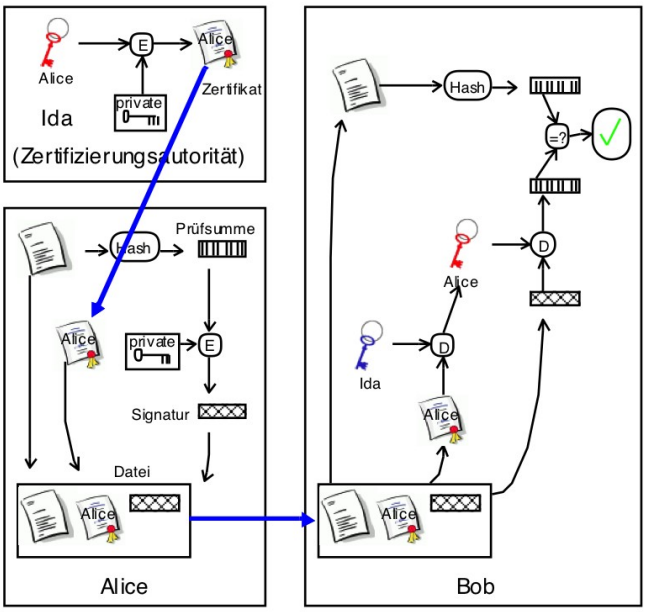
Frage 4.2.4: Signatur. Folgende Abbildung zeigt die Übergabe eines Dokumentes von A nach B.



Erläutern Sie den Ablauf bei A. Erläutern Sie den Ablauf bei B. Woher bekommt Bob den öffentlichen Schlüssel von Alice? Woher weiss er, dass dieser Schlüssel echt ist?

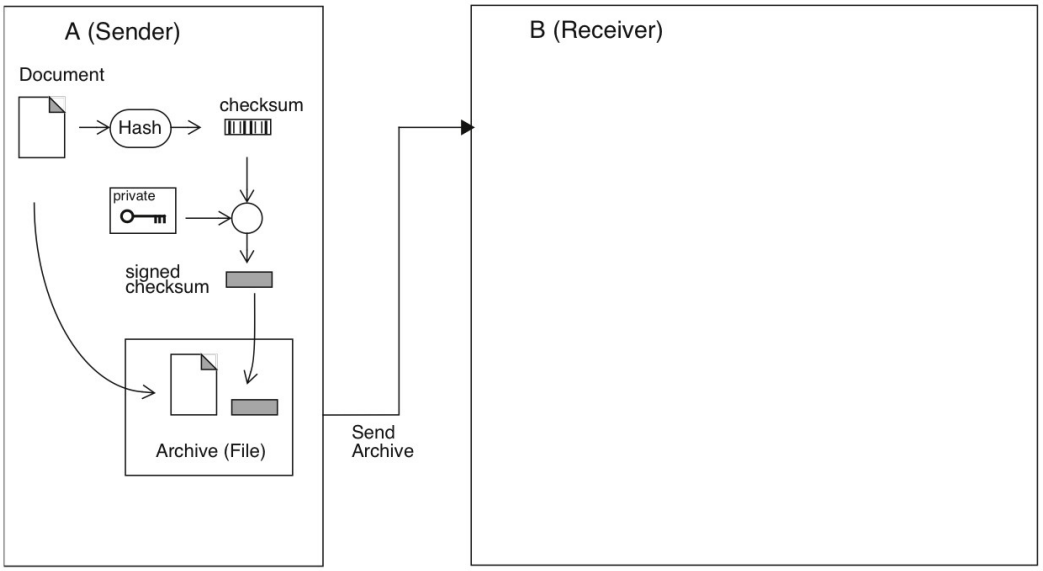
Hinweis: Der Block „Hash“ kennzeichnet die Bildung einer Prüfsumme fixer Länge, bzw. einer Zahl, die das Dokument repräsentiert. Diese Prüfsummen sind deutlich kürzer als das ursprüngliche Dokument (z.B. mit 128 bzw. 160 Bits Länge). Das Dokument kann aus der Prüfsumme nicht rekonstruiert werden. Kleinste Änderungen im Dokument verursachen Änderungen der Prüfsumme.

Frage 4.2.5: Zertifikat. Folgende Abbildung zeigt ein Verfahren zur Übergabe eines Dokumentes von A nach B. Das Verfahren besitzt Ähnlichkeit mit dem Verfahren aus Frage 4.2.4.



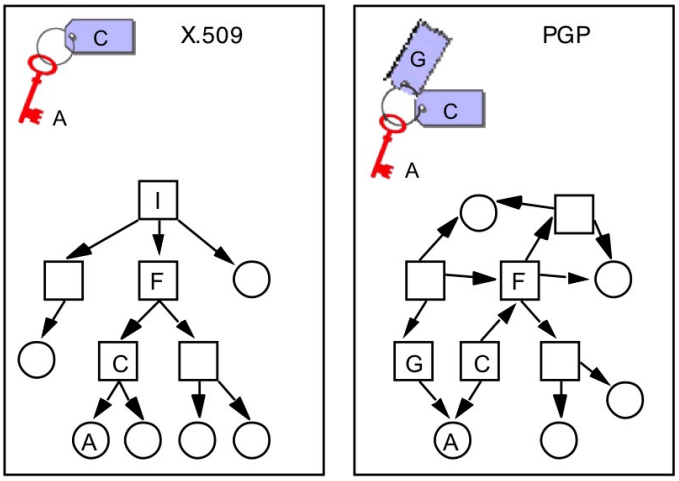
Erläutern Sie die Unterschiede zum Verfahren aus Frage 4.2.4. Erläutern Sie den Ablauf bei A. Erläutern Sie den Ablauf bei B. Woher bekommt Bob den öffentlichen Schlüssel von Alice? Woher weiss er, dass dieser Schlüssel echt ist?

Frage 4.2.6: Dokument mit Ursprungsnachweis. Alice schickt Bob ein Dokument in der in in folgender Abbildung gezeigten Weise. Wie geht Bob nach empfang des Dokumentes vor? Ergänzen Sie die Abläufe und erläutern Sie das verfahren. Wurde das Dokument verschlüsselt übertragen?

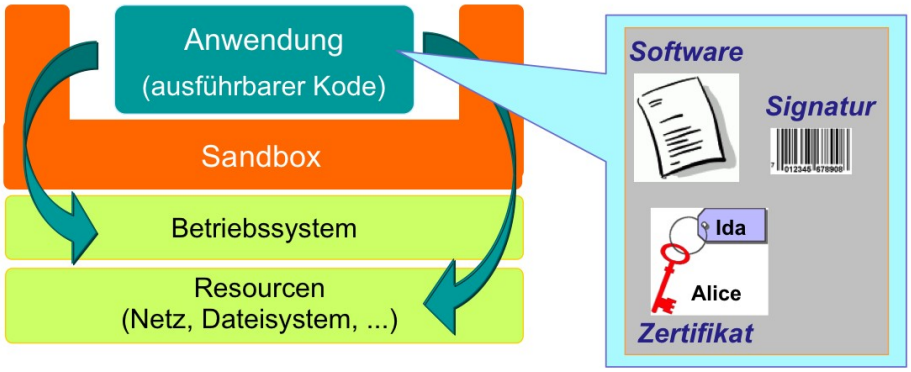


Frage 4.2.7: Alice möchte ein Dokument verschlüsselt übertragen. Skizzieren Sie die Abläufe nach dem oben gezeigten Schema. Zusatzfrage: Wie geht Alice vor, um ein verschlüsseltes und von ihr signiertes Dokument zu übertragen?

Frage 4.2.8: Vertrauensbeziehungen. Folgende Abbildung zeigt zwei gängige Methoden zur Erstellung und Prüfung von Zertifikaten: (1) nach dem Standard X.509, sowie (2) nach dem Standard PGP (pretty good privacy, OpenSource Projekt). Welche Vertrauensbeziehungen werden verwendet? Welche Unterschiede bestehen diesbezüglich zwischen beiden Verfahren? Was wären ggf. Vorteile bzw. Nachteile beim praktischen Einsatz?



Frage 4.2.9: Signierte Apps. Beim Laden und Installieren von Software (Apps) können Schädlinge auf das Zielsystem (Smartphone, Rechner, Prozessrechner) gelangen. Folgende Abbildung zeigt ein Verfahren, dass die zu installierende Software signiert. Ziel dieser Methode ist es, nur vertrauenswürdige Anwendungen zu installieren und nur vertrauenswürdigen Anwendungen den Zugriff auf die Betriebsmittel und Daten (z.B. E-Mails, Kontakte, Dokumente) zu gewähren.



Erläutern Sie den Ablauf des Verfahrens. Worauf beruht das Vertrauen? Was wird mit dieser Methode gewährleistet? Erkennt und verhindert diese Methode zuverlässig die Installation von Schadsoftware?

4.5. E-Mail Verschlüsselung

E-Mail wird meist ungeschützt im Klartext übertragen.

Frage 4.3.1: Welche Bedrohungen gibt es für diese Art des Austauschs von E-Mail?

Lösung:

- Passiver Angriff: Mithören, Ausspionieren der Informationen, Datendiebstahl.
- Aktiver Angriff: Eingriff in die Kommunikation, Manipulation von Daten, vortäuschen falscher Identitäten, Zustellung von Schadsoftware, Störung, Belästigung, ...

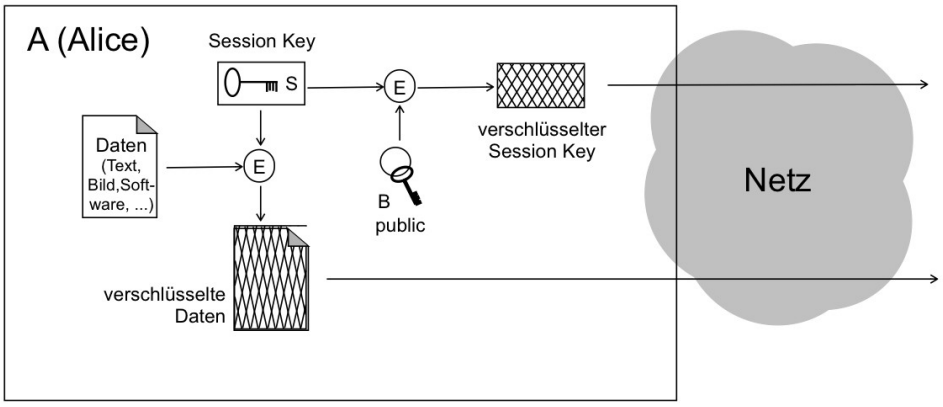
Frage 4.3.2: Wie können Sie sich vor diesen Bedrohungen schützen?

Lösung:

- Passiver Angriff: Schutz der Vertraulichkeit durch Verschlüsselung der Inhalte

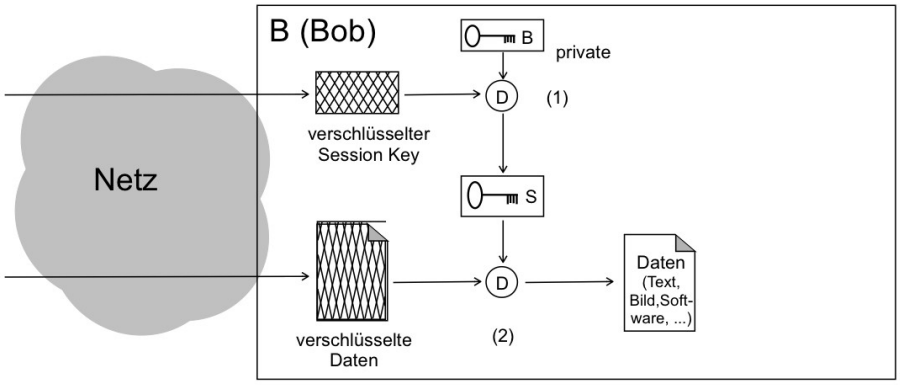
- Aktiver Angriff: Schutz vor Manipulation der Daten durch Signaturen, hierdurch ebenfalls Identitätsnachweis und Ursprungsnachweis der Inhalte

In dem in folgender Abbildung gezeigten Szenario möchte Alice per E-Mail vertrauliche Informationen an Bob schicken.



Frage 4.3.3: Wie kann Bob die empfangenen Dateien entschlüsseln (Skizze)?

Lösungsbeispiel (Skizze):



- Bob entschlüsselt den Session Key S mit Hilfe seines privaten Schlüssels B
- Das verschlüsselte Dokument lässt sich nun mit Hilfe des Session Keys S entschlüsseln.

Frage 4.3.4: Woher kennt Alice den öffentlichen Schlüssel von Bob (Schlüssel B public)? Wie kann Alice sichergehen, dass dieser Schlüssel Bob‘s korrekter öffentlicher Schlüssel ist? Erläutern Sie einige Möglichkeiten.

Lösung:

- Bob und Alice kennen sich und haben diesen Schlüssel auf einem sicheren Weg ausgetauscht.
- Bob und Alice kennen sich nicht. Bob schickt ihr den Schlüssel z.B. per E-Mail. Alice kann den Schlüssel bzw. eine Prüfsumme des Schlüssels (Fingerprint) von Bekannten überprüfen lassen.
- Bob schickt einen von einer vertrauenswürdigen Instanz signierten Schlüssel. Zum Erhalten der Signatur hat Bob dieser Instanz einen Identitätsnachweis erbracht. In diesem Fall kann Ali-

ce die Signatur des Schlüssels mit Hilfe des ihr bekannten öffentlichen Schlüssels der vertrauenswürdigen Instanz prüfen.

Frage 4.3.5: Wie kann Bob ein vertrauliches Dokument an Alice schicken?

Lösung: Wie Skizze zu Frage 4.3.1, jedoch mit B (Bob) anstelle von A (Alice) und mit dem öffentlichen Schlüssel von Alice (A public) anstelle des Schlüssels B public.

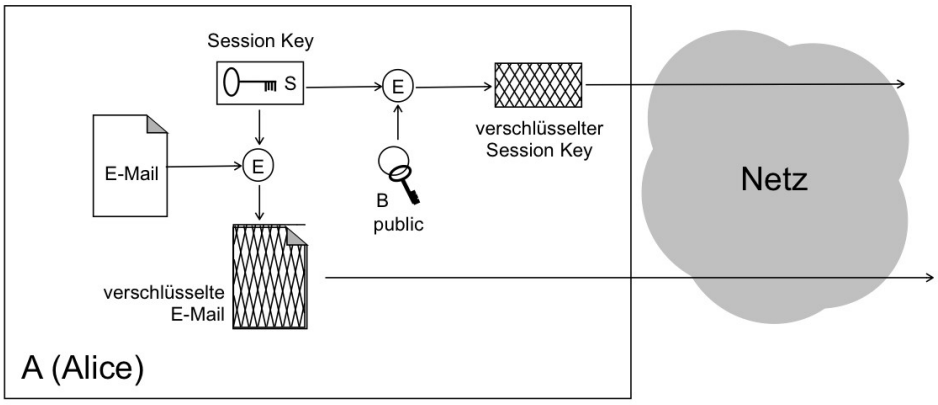
Frage 4.3.6: Wie kann Alice sicher sein, dass dieses Dokument wirklich von Bob stammt und nicht manipuliert wurde? Was kann Bob zum Nachweis der Unversehrtheit des Dokumentes und zum Nachweis des Ursprungs des Dokumentes tun? Wie kann Alice diese Eigenschaften prüfen?

Lösung:

- Da jeder den öffentlichen Schlüssel von Alice haben kann, ist die Verschlüs-selung mit Hilfe dieses Schlüssels nicht als Ursprungsnachweis hinreichend.
- Bob schickt zusätzlich eine Signatur des Dokumentes mit. Die Signatur erzeugt Bob mit Hilfe einer Prüfsumme des Dokumentes, die er durch einen Hasch-Algorithmus erzeugt. Diese Prüfsumme signiert er (verschlüsselt er) mit seinem privaten Schlüssel B private. Die Signatur (= mit B private verschlüsselte Prüfsumme) schickt Bob zusätzlich mit dem verschlüsselten Dokument.
- Alice prüft die Signatur des Dokuments. Hierzu erzeugt Sie aus dem Klartext des Dokumentes per Hash-Algorithmus eine Prüfsumme. Diese Prüfsumme vergleicht Sie mit der Prüfsumme, die Bob mitgeschickt hat. Die von Bob geschickte Prüfsumme entschlüsselt sie hierzu mit dem von ihr überprüften öffentlichen Schlüssel von Bob. Stimmen beide Prüfsummen überein, ist das Dokument unversehrt und stammt von Bob.

4.6. E-Mail Verschlüsselung mit PGP

Alice möchte an Bob eine verschlüsselte E-Mail senden. Sie verwendet dazu einen öffentlichen Schlüssel von Bob, wie in der folgenden Abbildung gezeigt.



Frage 4.4.1: Erläutern Sie die Funktion des Verfahrens in einigen Stichworten. Was wird als E-Mail über das Netz verschickt?

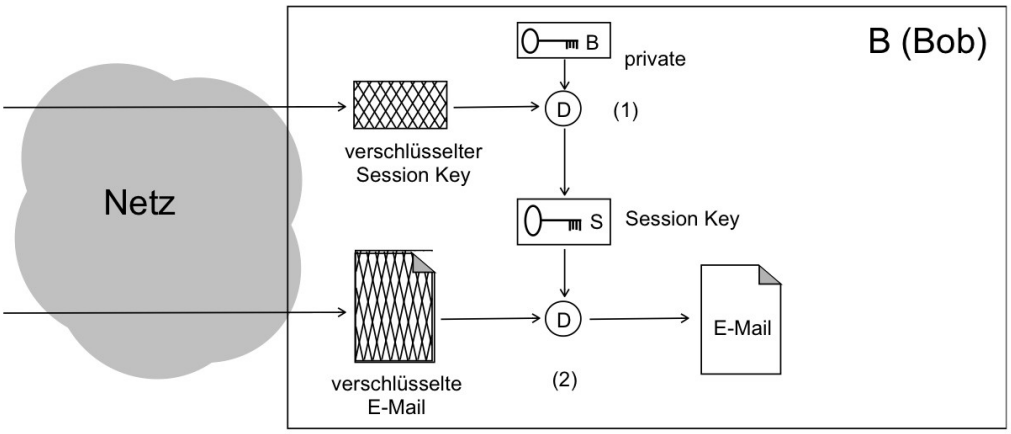
Lösung:

- Die ursprüngliche E-Mail (Text und ggf. Anlagen) werden mit einem Session-Key verschlüsselt. Dieser Session Key ist zum Entschlüsseln der Nachricht erforderlich und muss daher ebenfalls mit der Nachricht übertragen werden.

- Zur Übertragung wird der Session Key mit dem öffentlichen Schlüssel des Empfängers (Bob) verschlüsselt. Zum Entschlüsseln ist der zugehörige private Schlüssel erforderlich, den der Empfänger unter Verschluss hält.

Frage 4.4.2: Skizzieren Sie, wie Bob als Empfänger die E-Mail von Alice entschlüsseln kann (passender Vorgang zur Abbildung oben). Kann Bob sicher sein, dass die Nachricht tatsächlich von Alice kommt?

Lösung (Skizze):



Bob kann nicht sicher sein, dass die Nachricht tatsächlich von Alice stammt. Sein öffentlicher Schlüssel ist jedem zugänglich.

Frage 4.4.3: Alice hat die Angewohnheit, im cc der E-Mail ihre eigene E-Mail-Adresse anzugeben, damit sie eine Kopie der Nachricht zum Einsortieren in ihre Ablage empfangen kann. Was ist erforderlich, damit Alice Kopien ihrer verschlüsselt gesendeten Nachrichten lesen kann?

Lösung:

- Die gesendete Nachricht kann nur mit dem privaten, d.h. geheimen Schlüssel des Empfängers gelesen werden.
- Die Kopie der Nachricht müsste also entweder unverschlüsselt an Alice selbst gesendet werden (wenig konsequent), oder mit dem öffentlichen Schlüssel von Alice verschlüsselt werden. Diese Funktion kann das E-Mail Programm eigenständig leisten.

Frage 4.4.4: Bob möchte eine signierte E-Mail an Alice schicken. Skizzieren Sie den Ablauf auf Senderseite und Empfängerseite. Wozu dient die Signatur? Ließe sich auch eine verschlüsselte E-Mail an Alice signieren?

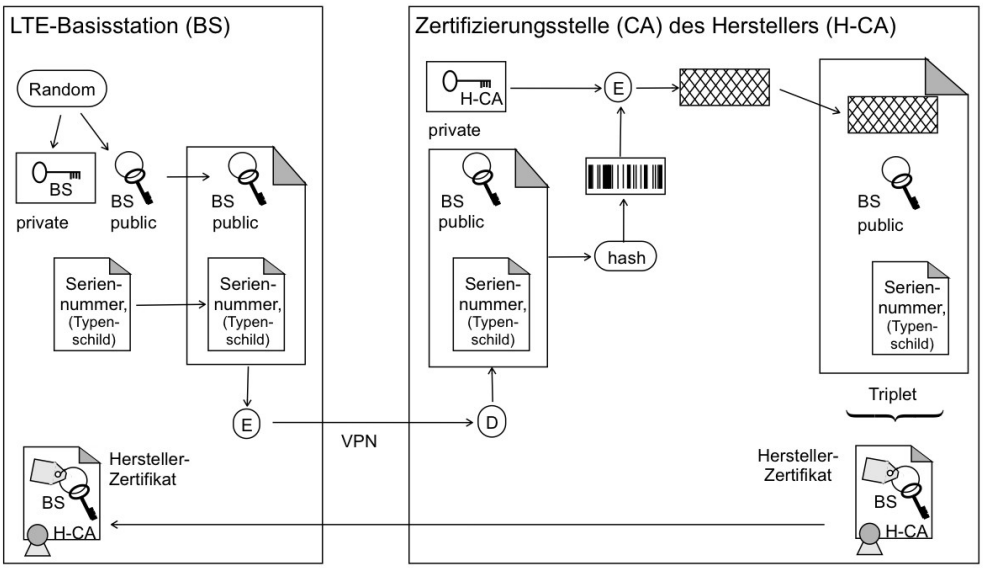
Lösung: Skizze: siehe z.B. Aufgabe 4.2, Skizze zu Frage 4.2.3. Die Signatur dient als Urspungsnachweis des Dokuments: Sofern Bob seinen privaten (geheimen) Schlüssel sicher aufbewahrt, kann Alice darauf vertrauen, das er die E-Mail geschickt hat.

4.7. Einsatz von Zertifikaten bei der Inbetriebnahme

Die aktuelle Generation Mobilfunk setzt durchgehend auf IP-basierte Transportnetze (mit Aggregation des Verkehrs im Zugangsnetz über Ethernet), ohne spezielle mobilfunkspezifische Protokolle und Schnittstellen in den unteren Protokollschichten.

Der Aufbau der Infrastruktur, speziell die individuelle Konfiguration der zahlreichen Basis-stationen (eNB bzw. allgemein BS), ist zeitintensiv und personalintensiv. Daher wird ein weitgehend auto-

matisierter Prozess angestrebt. Diese Methoden sind auch für Kommunikationsanwendungen in den Energieversorgungsnetzen (Smart Grids) einsetzbar.



(a) Ablauf in der Fabrik des Herstellers

Frage 4.5.1: Erläutern Sie Abläufe bei der Fabrikation der Basisstation beim Hersteller

Lösung:

(1) Die Basisstation (BS) erzeugt ein zufälliges asymmetrisches Schlüsselpaar (privater und öffentlicher Schlüssel).

(2) Den öffentlichen Schlüssel gibt die BS zusammen mit der Seriennummer (und anderen herstellerspezifischen Informationen auf dem elektronischen Typenschild) an die Zertifizierungsstelle des Herstellers (H-CA).

(3) Die Zertifizierungsstelle signiert Schlüssel und Typenschild (inkl. Seriennummer) und gibt diese Information zusammen mit der Signatur als Herstellerzertifikat zurück an die Basisstation (Zertifikat = Triplet aus öffentlichem Schlüssel, Typenschild (inkl. Seriennummer) und Signatur der CA).

Frage 4.5.2: Was ist das Ergebnis der Prozedur? Welche Informationen verbleiben auf der Basis-station?

Lösung:

- Privater Schlüssel (gesichert z.B. auf HSM)
- Seriennummer (auf elektronischem Typenschild)
- Herstellerzertifikat

Frage 4.5.3: Die Übertragung des öffentlichen Schlüssels und der Seriennummer (Typenschild) an die Zertifizierungsstelle des Herstellers geschieht über ein VPN. Wie wäre eine solche Übertragung technisch zu lösen?

Lösung:

(1) Durch eine verschlüsselte Verbindung zwischen BS und H-CA.

(2) Schlüssel: z.B. Token bzw. UID/Passwort des Mitarbeiters der Produktion, bzw. automatisch generierter Schlüssel (Session Key).

Frage 4.5.4: Weshalb wird die in Frage 4.5.3 genannte Information über ein VPN übertragen? Welche Gefährdung besteht, wenn die in Frage 1.3 genannte Information bzw. das Hersteller-Zertifikat in falsche Hände gerät?

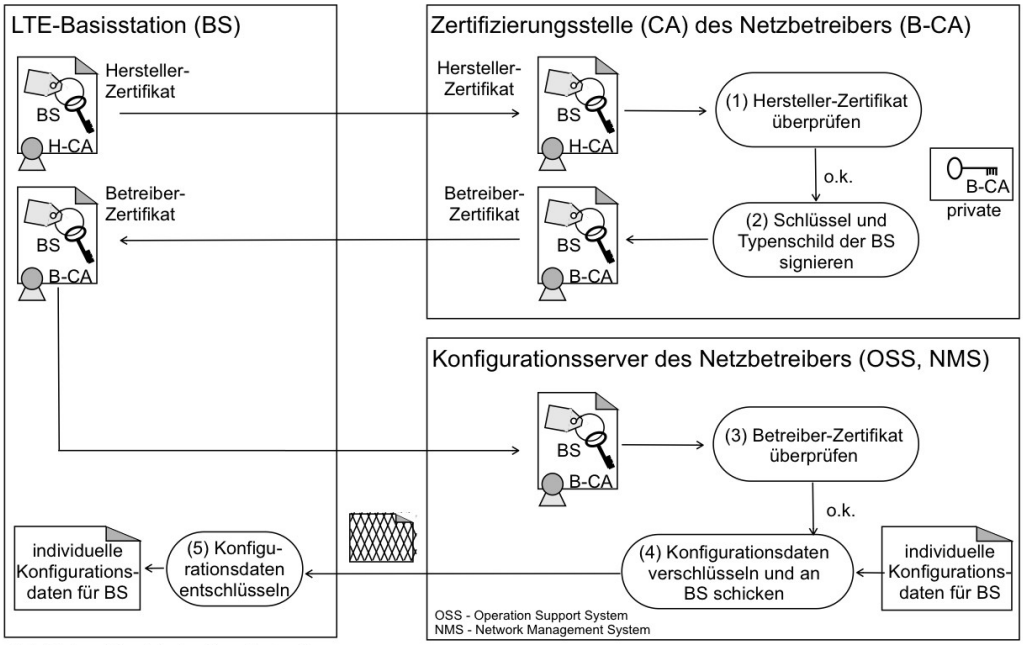
Lösung:

(1) Begründung für VPN: Offenlegung von Fabrikationsprofilen ist unerwünscht (wie viele BS wann und wo gefertigt wurden, mit welchen Seriennummern und Schlüsseln). Ausserdem wird auf diese Weise sichergestellt, aus welcher Quelle die Anfrage nach einem Zertifikat stammt.

(2) Gefahren: Versuche, mit Hilfe der Seriennummern (Typenschilder) und öffentlichen Schlüssel Basisstationen bzw. Hersteller-Zertifikate zu fälschen. Z.B. Versuch, der H-CA manipulierte Daten unter zu schummeln, mit der Bitte um Signatur. Gefährdung: Gering einzustufen, wenn die eingehenden Daten beim H-CA mit Fertigungsdaten aus anderen Quellen verglichen werden und der Produktionsprozess dokumentiert ist.

(3) Hersteller-Zertifikat: kann veröffentlicht werden, da für auf dem Zertifikat basierende Abläufe ein passender privater Schlüssel existieren muss.

Im Anschluss an die Fertigung in der Fabrik des Herstellers werden die Bassistationen (BS) im Netz des Betreibers installiert und in Betrieb genommen. Hierzu wird jeder Basisstation eine IP-Adresse zugeordnet, sowie die Koordinaten der Zertifizierungsstelle und des Konfigurationsservers des Netzbetreibers. Der weitere Ablauf finden sich in der folgenden Abbildung.



(b) Ablauf im Netz des Betreibers

Frage 4.5.5: Erläutern Sie Abläufe bei der Inbetriebnahme beim Netzbetreiber.

Lösung:

(1) Die Basisstation gibt das Herstellerzertifikat an die Zertifizierungsstelle des Netz-betreibers (B-CA). Diese überprüft das Zertifikat (ebenfalls möglich: Überprüfung der Informationen aus dem Typenschild gegen eine vorher bereitgestellte Datenbasis). Nach erfolgreicher Überprüfung stellt die B-CA ein Betreiber-Zertifikat aus und übermittelt dieses an die BS.

(2) Die BS schickt das Betreiber-Zertifikat an den Konfigurationsserver des Netzbetreibers. Der Konfigurationsserver überprüft das Zertifikat. Nach erfolgreicher Überprüfung wählt der Konfigurationsser-

ver die für die BS vorgesehene Konfigurationsdaten aus (inkl. Software) und übermittelt diese in verschlüsselter Form an die BS.

Frage 4.5.6: Was ist das Ergebnis der Prozedur? Welche Informationen verbleiben auf der Basisstation?

Lösung: Die Lösung ist auch als Diagramm (Skizze) darstellbar.

Aktion (1): Das Hersteller-Zertifikat enthält einen Hinweis auf die Zertifizierungsstelle des Herstellers (H-CA), deren öffentlicher Schlüssel der Zertifizierungsstelle des Betreibers (B-CA) bekannt ist. Mit diesem öffentlichen Schlüssel wird die im Hersteller-Zertifikat enthaltene Signatur entschlüsselt (siehe Triplet in Bild 1). Entspricht dieser entschlüsselte Text der in der B-CA selber erstellten Prüfsumme (aus BS-Schlüssel und Seriennummer/Typenschild), ist das Hersteller-Zertifikat gültig.

Aktion (2): Bildung einer Prüfsumme (aus BS-Schlüssel und Seriennummer/Typenschild) und Signatur dieser Prüfsumme (mit privatem Schlüssel der B-CA). Siehe Bild 1.

Frage 4.5.7: Bei der Systemkonfiguration: Wie wird das Betreiber-Zertifikat überprüft (Aktion (3) in der Abbildung)? Wie werden die Konfigurationsdaten für die Basisstation verschlüsselt (Aktion (4) in der Abbildung)? Wozu werden die Konfigurationsdaten für die Basisstation verschlüsselt? Wie werden die Konfigurationsdaten auf der Basisstation entschlüsselt (Aktion (5) in der Abbildung)?

Lösung: Die Lösung ist auch als Diagramm (Skizze) darstellbar.

Aktion (3): Das Betreiber-Zertifikat enthält einen Hinweis auf die Zertifizierungsstelle des Betreibers (B-CA), deren öffentlicher Schlüssel dem Konfigurationsserver des Betreibers bekannt ist. Mit diesem öffentlichen Schlüssel wird die im Betreiber-Zertifikat enthaltene Signatur entschlüsselt (siehe Triplet in Bild 1). Entspricht dieser entschlüsselte Text der im Konfigurationsserver selber erstellten Prüfsumme (aus BS-Schlüssel und Seriennummer/Typenschild), ist das Betreiber-Zertifikat gültig.

Aktion (4): Mit dem öffentlichen Schlüssel der BS. Wozu: Vermeidung von Profilen über den Netzausbau, sowie Daten-Diebstahl (von Software und Konfigurationsdaten für die BS).

Aktion (5): Mit dem privaten Schlüssel der BS.

Frage 4.5.8: Identitätsnachweis für den Konfigurationsserver: Was wäre der Zweck eines solchen Nachweises gegenüber der Basisstation? Wie wäre das Verfahren zu realisieren?

Lösung:

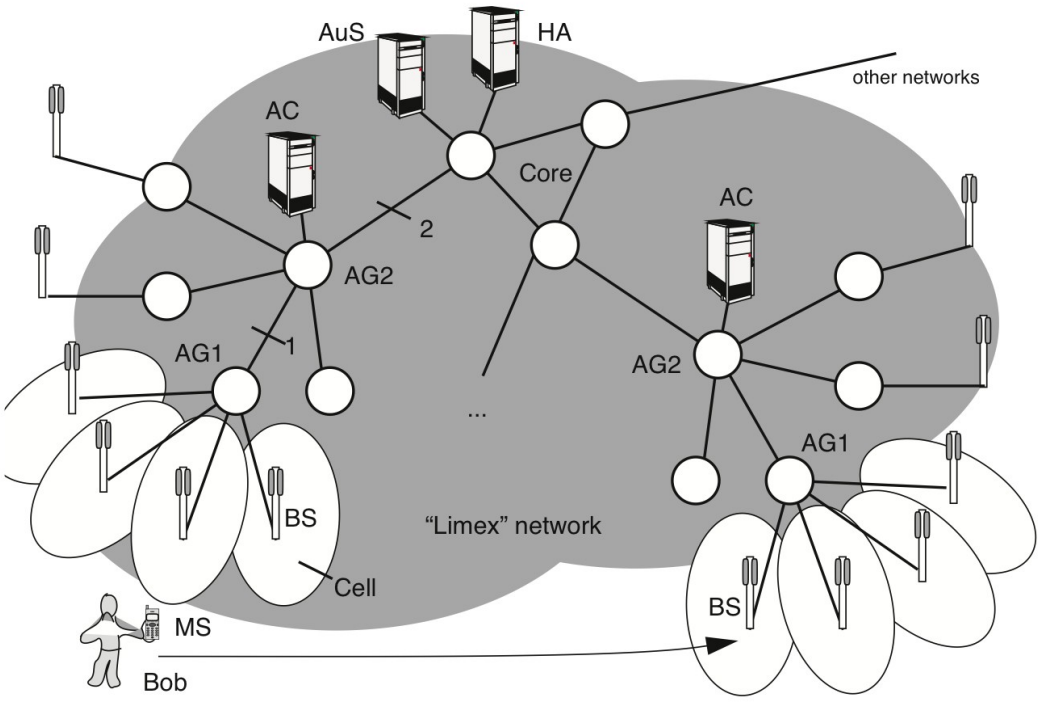
(1) Zweck eines Identitätsnachweises für den Konfigurationsserver: Vermeidung von fehlkonfigurierten bzw. manipulierten Basisstationen. Die BS sendet nur Daten an vertrauens-würdige Konfigurationsserver und akzeptiert nur Konfigurationsdaten von vertrauenswürdigen Konfigurationsservern.

(2) Realisierungsmethode: Mit Hilfe eines Zertifikates des Konfigurationsservers, das an die Basisstation geschickt wird. Die BS kann das Zertifikat mit Hilfe des öffentlichen Schlüssels der Zertifizierungsstelle überprüfen.

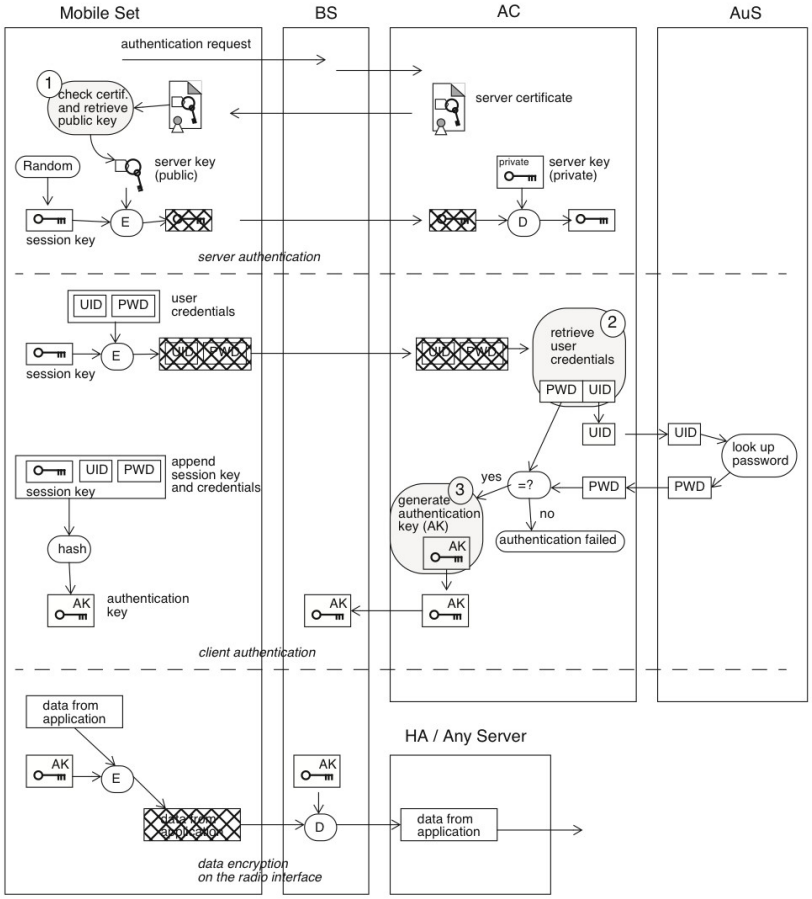
4.8. Authentifizierung von Endgeräten und Servern im Netz

In einem Mobilfunknetz sind folgende Aufgaben unter den Netzkomponenten aufgeteilt:

- Mobilitätsverwaltung: HA (Home Agent, registriert den Aufenthaltsort der Teilnehmer)
- Datenbank für Schlüssel: AuS (Authentification Server, bewahrt die Schlüssel der Teilnehmer auf)
- Zugangsberechtigung: AC (Access Controller, überprüft die Zugangsberechtigung der Teilnehmer auf Anfrage)



Der Betreiber den Netzes möchte nur im Internet gängige Verfahren und Protokolle verwenden. Die Überprüfung der Zugangsberechtigung soll nach folgendem Schema erfolgen.



Frage 4.6.1: Erläutern Sie die Rollen der gezeigten Netzelemente: Endgeräte (Mobile Set), Basisstation (BS, Base Station), Zugangscontroller (AC, Access Controller), Datenbank (AuS, Authentification Server).

Frage 4.6.2: Folgende Abläufe sind in der Abbildung unvollständig:

(1) Überprüfung des Server-Zertifikates auf dem Endgerät (check certificate and retrieve public key).

(2) Anfrage der Nutzerkennung (retrieve user credentials)

(3) Authentisierungsschlüssel erzeugen (generate authentication key).

Ergänzen Sie diese Abläufe (Skizze mit Erläuterungen).

Frage 4.6.3: Wie liessen sich diese Verfahren in Energienetzen einsetzen? Diskutieren Sie Anwendungsfälle, sowie den Schutz, den diese Verfahren bieten.

Frage 4.6.4: Was muß beim Einsatz öffentlicher Mobilfunknetze als Kommunikationsmedium in der elektrischen Energieversorgung beachtet werden? Welche Anwendungen eignen sich hierfür, welche Anwendungen sind nicht geeignet?

5. Klausuraufgaben

5.1. Logische Adressierung

Sie haben im privaten IP-Netz zuhause oder am Arbeitsplatz einen eigenen Web-Server installiert, auf den Sie aus dem öffentlichen IP-Adressraum heraus zugreifen möchten. Anwen-dungen hierfür wären beispielsweise die Abfrage von Zählerständen (Smart Meter) bzw. Systemzuständen für Telematik-Anwendungen (Heimautomatisierung, Gebäudeautomati-sierung) von unterwegs bzw. von einer Leitstelle aus.

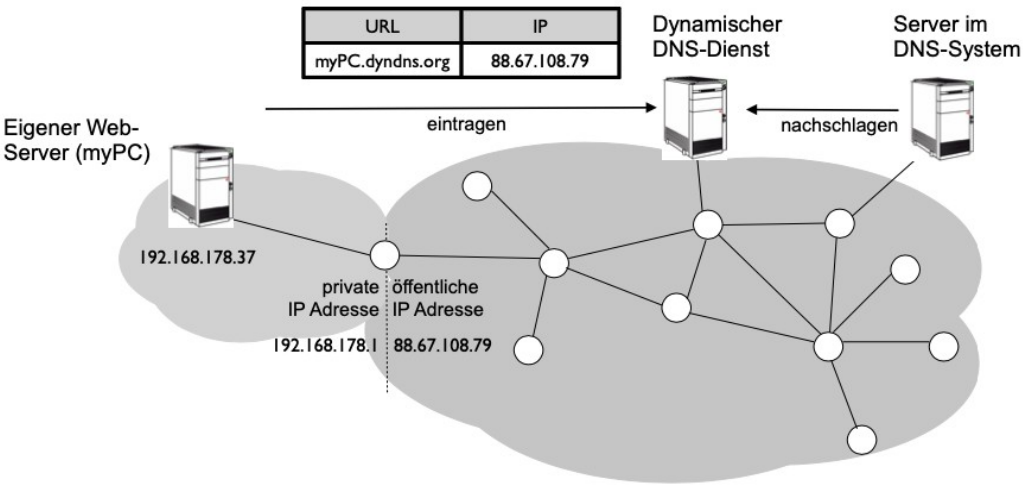
Frage 5.1.1: Können Sie den Web-Server für eine HTTP-Anfrage von unterwegs aus erreichen? Begründen Sie Ihre Entscheidung.

Lösung: Nein. Der private Adressraum ist vom öffentlichen Adressraum aus nicht sichtbar.

Frage 5.1.2: Umgekehrt können Sie vom heimischen Server aus auf Dienste im öffentlichen Adressraum zuzugreifen, z.B. auf Webseiten. Wie funktioniert das? Was könnte der Server tun, um auf diese Weise von aussen zugänglich zu werden?

Lösung: Der Server kann auf bekannte URLs bzw. IP-Adressen im öffentlichen Bereich zugreifen, da diese Adressen eben bekannt sind. Wenn der Server sich zuerst an einem Gerät im öffentlichen Bereich meldet, kann dieses Gerät ab diesem Zeitpunkt auf die nun bekannte Adresse des Servers zugreifen. Technisch wird das bei IPv4-Adressen mit Hilfe einer Übersetzung der privaten Adressen in Ports der öffentlichen Adresse des Routers (z.b. der FritzBox!) zum öffentlichen Netz gelöst. Bei IPv6-Adressen macht der eigene Server erst seine Adresse bekannt, der Zugriff kann anschliessend ohne Übersetzung geschehen.

Der Router (z.B. eine FritzBox!) als Schnittstelle zwischen dem privaten Netz und dem öffentlichen Netz erhält vom Netzbetreiber eine öffentliche IP-Adresse. Diese öffentliche IP-Adresse ist jedoch nicht fest vergeben, sondern wird täglich ausgetauscht. Damit das private Netz trotz wechselnder öffentlicher IP-Adressen erreichbar ist, bieten Anbieter dynamische DNS-Einträge an, wie in folgender Abbildung gezeigt.



Frage 5.1.3: Beschreiben Sie die Funktion des angebotenen Dienstes.

Lösung: Statt der täglich wechselnden IP-Adressen wird als Koordinate ein Eintrag im DNS-System verwendet, der sich nicht ändert. Hierzu bietet der Anbieter des dynamischen DNS-Dienstes z.B. eine untergeordnete Domain wie z.B „myPC.dyndns.org“ zu seiner Domain „dyndns.org“ an.

Frage 5.1.4: Wie erfolgt die Aktualisierung der öffentlichen IP-Adressen?

Lösung: Im dynamischen DNS-Server wird die zur privaten Domain gehörige dynamische, d.h. wechselnde öffentliche IP-Adresse des privaten Netzes eingetragen. Die private Domain wird im DNS-System bekannt gemacht Auf diese Art kann diese IP-Adresse über den konstanten Domain-Namen nachgeschlagen werden.

Frage 5.1.5: Sicherheit. Welche Sicherheitsrisiken gehen Sie ein durch die Nutzung des dynamischen DNS-Eintrags?

Lösung:

(1) Der Anbieter der dynamischen DNS kann ein Nutzerprofil von Ihnen anlegen mit allen Daten, die er für die Erteilung der Eintrags von Ihnen abfragt.

(2) Ausserdem kann er Statistik führen über die eintreffenden DNS-Abfragen zu Ihrer Domain, sowie über die Ihnen zugeteilten IP-Adressen.

(3) Der Anbieter hat keine Kenntnis der auf Ihrem Server angebotenen und Informa-tionen, deren Nutzung und deren Nutzer.

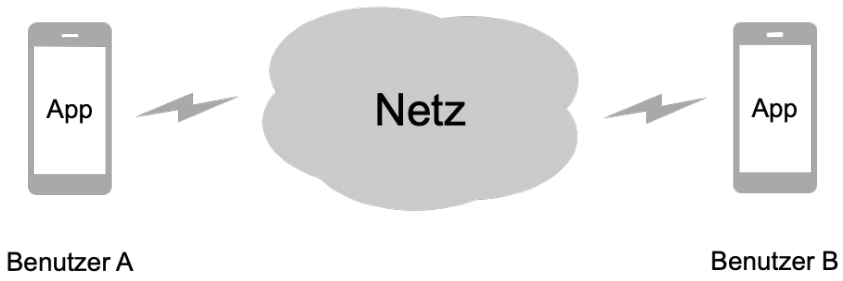
(4) Durch den Web-Server im eigenen Netz wird ihr eigenes Netz leichter von aussen sichtbar und angreifbar.

Frage 5.1.6: Als Alternative zum eigenen Web-Server mit dynamischen DNS-Eintrag könnten Sie Ihren Web-Server mit eigener Domain bei einem Web-Hoster realisieren. Bewerten Sie diese Alternative bzgl. der Sicherheitsrisiken.

Lösung: (1) Dem Web-Hoster muss man vertrauen können. Da der Web-Server auf seiner Infrastruktur läuft, hat er Zugang zu sämtlichen Informationen bzgl. der Nutzung des Servers, d.h. Nutzer, Browser-Typ, Ursprung der Anfragen, alle abgefragte Inhalte, Informationsmengen etc. Ein Anbieter eines dynamischen DNS-Eintrags besitzt vergleichsweise wenig Informationen über die Nutzung des Web-Servers. (2) Der Web-Server hat durch die Unterbringung beim Web-Hoster keinen Einfluss auf das eigene Netz.

5.2. Sichere Nachrichtenübermittlung

Für den technischen Support ist der Einsatz eines Kommunikationsdienstes für Kunden und Mitarbeiter auf Basis von Smart Phones vorgesehen.



Für die sichere Kommunikation mittels Kurznachrichten aus einer App über das Netz sollen folgende Anforderungen gelten:

- Authentizität: Die Identität des jeweiligen gewünschten Gesprächspartner ist sichergestellt (durch einen Identitätsnachweis)
- Vertraulichkeit: Die Kommunikation über das Netz ist vor Einblicken Dritter geschützt (kann also nicht belauscht werden).

Frage 5.2.1: Wie können Sie die erste Anforderung (Authentizität) bei der Kommunikation sicherstellen? Skizzieren Sie bzw. beschreiben Sie ein Szenario für die Kommunikation zwischen A (Alice) und B (Bob). Wodurch wird der Nachweis der Identität erbracht? Hinweis: Verwenden Sie Methoden der asymmetrischen Verschlüsselung.

Lösung:

- Identitätsnachweis durch Signatur, d.h. Verschlüsseln mit dem privaten Schlüssel.
- Die Nachricht kann von jedem.der den öffentlichen Schlüssel von Alice hat, gelesen werden. Hiermit ist jedoch sichergestellt, dass die Nachricht mit Hilfe des privaten Schlüssels von Alice erstellt wurde. Sofern Alice Ihren privaten Schlüssel geheim hält, ist hiermit der Nachweis der Identität erbracht.

Frage 5.2.2: Wie können Sie die zweite Anforderung (Vertraulichkeit) sicher stellen? Skizzieren Sie bzw. beschreiben Sie ein Szenario für die Kommunikation. Hinweis: verwenden Sie einen symmetrischen Session Key. Erzeugen und kommunizieren Sie den Session Key in geeigneter Weise.

Lösung:

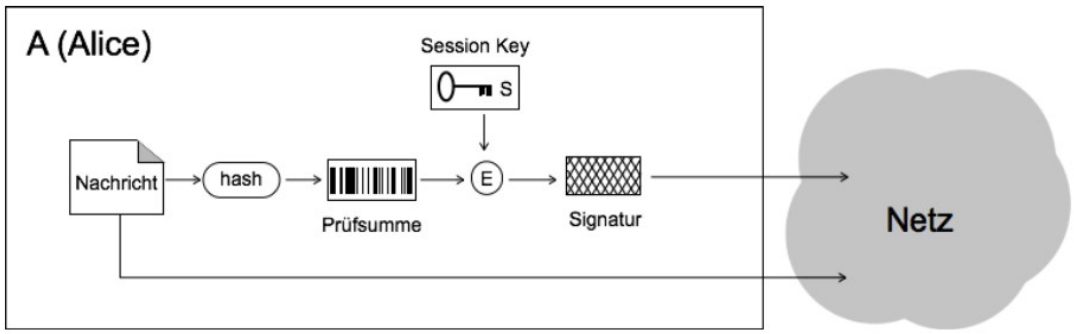
- Prinzip: Verschlüsselung mit dem öffentlichen Schlüssel des Empfängers: Die Nachricht kann nur von jemandem geöffnet werden, der im Besitz des zugehörigen privaten Schlüssel ist.
- Session Key: Dient als Nachricht. Eine von A erzeugte Zufallszahl wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und über das Netz an B kommuniziert.
- Nachrichten werden anschliessend mit dem Session Key verschlüsselt. A und B sind im Besitz des Session Keys.

Frage 5.2.3: Folgenlosigkeit. Für den Informationsaustausch per Kurznachrichten ist es unerwünscht, dass sich die Kommunikation durch einen Mitschnitt (gespeicherte Daten der Kommunikation) u.U. lange Zeit später entschlüsseln lässt, z.B. wenn einer der Schlüssel später einmal kompromittiert wird (durch Unachtsamkeit bzw. Bruch des Verschlüsselungsverfahrens). (1) Welcher der o.g. Kategorien ordnen Sie diese Anfor-derung zu? (2) Beschreiben Sie eine Methode, wie sich die Konversation im Anschluss an die Session vergessen lässt (d.h. nicht mehr rekonstruieren lässt, sofern beide Gesprächspartner der Methode folgen).

Lösung:

- Kategorie: Vertraulichkeit
- Methode: Der Session Key wird nach dem Informationsaustausch zwischen A und B sowohl von A als auch von B gelöscht. Hierfür sorgt die von A und B verwendete App.

Frage 5.2.4: Abstreitbarkeit. Im Gegensatz zu vertraglichen Dokumenten, bei denen Dritten gegenüber die Identität der Vertragspartner im Zusammenhang mit der vertrag-lichen Vereinbarung jederzeit nachgewiesen werden kann, ist diese Eigenschaft bei einer informellen Kommunikation eher unerwünscht. Alice möchte nicht, dass Bob ihre Aus-sagen über einen gemeinsamen Bekannten (bzw. über Arbeitskollegen) Dritten gegen-über nachweisen kann. Sie möchte solche Behauptungen von Bob abstreiten können. Ebenso möchte Bob seine Aussagen im Gespräch mit Alice Dritten gegenüber abstreiten können.



Alice und Bob verwenden hierzu das in der Abbildung oben gezeigte Schema. (1) Skizzieren Sie den Ablauf bei Bob. (2) Erläutern Sie das Verfahren. (3) Erläutern Sie, warum bei diesem Verfahren zwar zwischen Alice und Bob ein Identitätsnachweis vorhanden ist, jedoch Aussagen von Alice an Bob Dritten gegenüber von Alice abgestritten werden können (und umgekehrt). Hinweis: Welcher Schlüssel wird verwendet?

Lösung:

- Ablauf: Gegenstück zur Abbildung: Bob liest den signierten Session Key mit Hilfe des öffentlichen Schlüssels von A.
- Identitätsnachweis: Durch die Signatur des Session Keys.
- Nachrichten: werden entweder unverschlüsselt übertragen oder mit dem Session Key verschlüsselt übertragen. Unverschlüsselte Nachrichten können manipuliert sein. Verschlüs-selte Nachrichten können sowohl von A als auch von B manipuliert sein, da beide im Besitz des Session Keys sind. Somit kann A Aussagen von B abstreiten, und umgekehrt.

Frage 5.2.5: Verbindungsdaten. Auch wenn alle o.g. Anforderungen an den sicheren Austausch von Nachrichten durch die eingesetzte App erfüllt sind, bleibt nicht geheim, dass Alice und Bob miteinander über das Netz kommunizieren. (1) Welche Meta-Daten der Kommunikation (die sogenannten Verbindungsdaten) verbleiben im Netz? (2) Welche Bedrohung geht von diesen Daten aus?

Lösung:

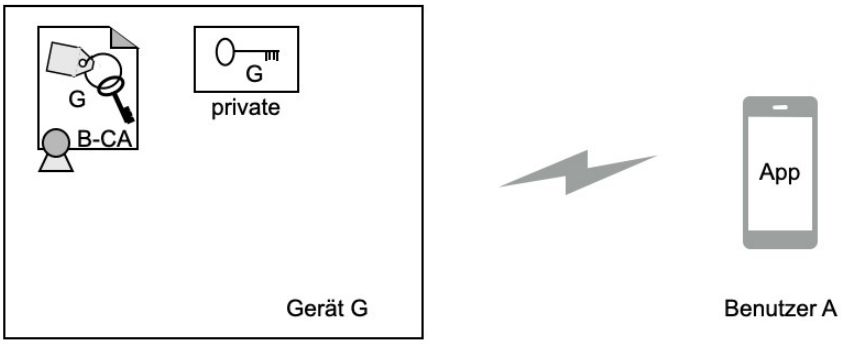
- Zeitpunkt und Dauer des Informationsaustauschs, Netzadressen von A und B. Alle Daten, die beim sogenannten Einzelverbindungsnachweis auf der Telefonrechnung stehen. Bei mobilen Apps ggf. auch Standort und Spuren des Browsers bzw. der App.
- Es können Kommunikationsprofile über die Gesprächspartner von A bzw. B erstellt werden. Die kompletten Beziehungsgeflechte lassen sich erstellen und analysieren.

Frage 5.2.6: Diskussion: Ließen sich die Meta-Daten (Verbindungsdaten) als Spuren verwischen? Wie beispielsweise? Wäre der Aufwand hierfür gemessen an den Bedro-hungsszenarien zu rechtfertigen?

Lösung: Anonymisierungsdienste wie Tor (Netz von Servern mit zufälligen Pfaden) bieten ansatzweise das Verwischen von Spuren als Dienst an. Jedoch verlässt sich der Nutzer dann auf den Dienstanbieter. Ausserdem begibt sich ein Nutzer in ein professionell kriminelles Milieu. Mit vertretbarem Aufwand nicht realisierbar.

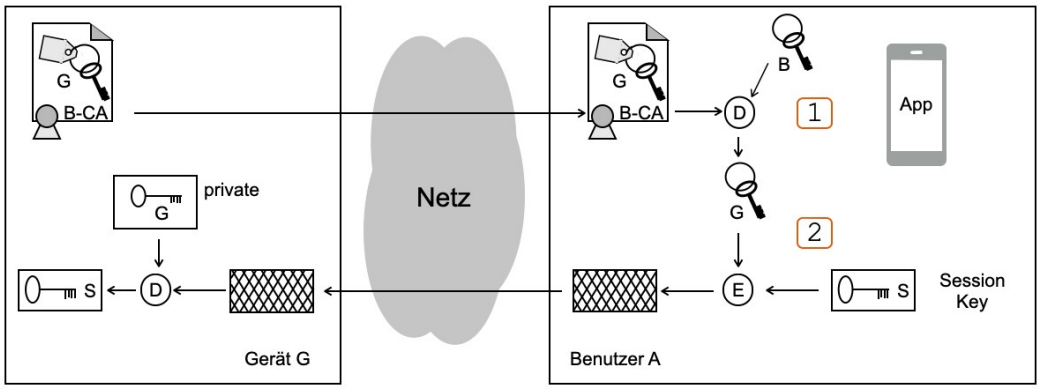
5.3. Sicherer Systemzugang mit App

Ein Gerät (z.B. Schaltschrank, Maschine, Zugangstür) soll einen Zugriff nur für autorisierte Benutzer bieten. Die Benutzer sind mit einem mobilen Gerät ausgestattet, das den Zugriff per App gestattet. Als Kommunikationsschnittstelle soll ein Nahbereichs-Funk-Standard eingesetzt werden (z.B. Bluetooth, WLAN, NFC, …).



Hierzu wird das Gerät G mit einem privaten Schlüssel und einen Zertifikat ausgestattet, das der Betreiber B des Gerätes ausgestellt hat, wie in der Abbildung gezeigt.

Frage 5.4.1: Identitätsnachweis G. Wie kann die App (bzw. Benutzer A) sicher sein, mit dem korrekten Gerät zu kommunizieren? Wie kann Benutzer A eine verschlüsselte Nachricht an Gerät G schicken? Worauf beruht das Vertrauen des Benutzers A? Erläutern Sie den unten dargestellten Ablauf.



Lösung:

Ablauf: (1) Gerät G schickt bei Kontaktaufnahme durch A sein Zertifikat an A. A überprüft das Zertifikat. (2) Hierauf erzeugt A einen Session-Key, den es verschlüsselt an Gerät G schickt. Funktion siehe Skript (z.B. SSL, On-line Banking). Wenn Gerät G den Schlüssel korrekt auspacken kann, ist es im Besitz des privaten Schlüssels G.

Die Überprüfung des Zertifikates erfolgt mit Hilfe des in A gespeicherten Root-Zertifikates B, welches zuvor auf dem Gerät A installiert wurde. Das Zertifikat von G ist zuvor durch Signatur des Schlüssels G bei der Zertifizierungsinstanz B (B-CA) erstellt worden, wie in folgender zusätzlicher Abbildung dargestellt (sowie in zahlreichen Übungen im Skript).

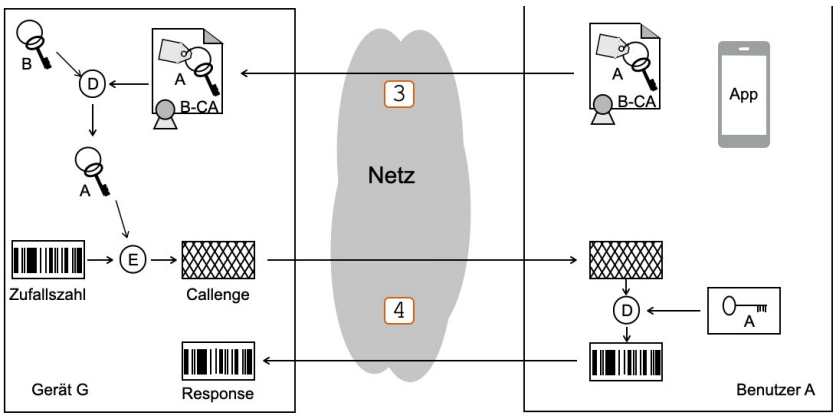
Frage 5.4.2: Worauf ist bei der Ausstattung des Gerätes G beim Hersteller bzw. beim Betreiber zu achten? Wie erfolgt die Ausstattung in der Praxis? Welche Rolle spielt das Betriebssystem des Gerätes? Hinweis: Welche Informationen sind geheim?

Lösung: Der geheime Schlüssel darf das Gerät niemals verlassen und muss sicher im Gerät abgelegt werden. Auf das Betriebssystem ist hierbei kein Verlass. In der Praxis bieten sich speziell geschützte Chips (TPM) bzw. Chipkarten an (siehe SIM-Karte).

Frage 5.4.3: Identitätsnachweis A. Bevor das Gerät G Zugriff für den Benutzer A auf Daten und Funktionen gewährt, muss es dessen Identität überprüfen. Beschreiben Sie hierzu eine Möglichkeit. Skizzieren Sie den Ablauf der Kommunikation. Bewerten Sie Ihre Wahl.

Lösungsbeispiele: (1) Passwort und Benutzerkennung (wie beim Home-Banking). Die sichere Übertragung ist mit Hilfe des Session-Keys möglich. Setzt jedoch die Einrichtung und Pflege dieser Daten auf dem Gerät voraus, daher wenig praktikabel. (2) Zertifikat A: gleicher Ablauf wie oben mit Zertifikat von A:

Gerät G muss hierbei prüfen, ob A tatsächlich im Besitz des passenden privaten Schlüssel ist. Dies kann z.B. durch Übermittlung einer verschlüsselten Zufallszahl geschehen (Challenge-Response-Verfahren, siehe Skript).



Frage 5.4.4: Zugriff für Werkspersonal. Der Zugriff ist nun abgesichert, was leider auch Abfragen zur Konfiguration im Werk des Herstellers bzw. Betreibers erschwert. Wie kann autorisiertes Werkspersonal auf das Gerät zugreifen?

Lösung: Das Werkspersonal benötigt eine App mit Zertifikat des Herstellers bzw. Betreibers. Das Gerät kann das Zertifikat überprüfen. Wenn dem überprüften Zertifikat keine besondere Rolle zugewiesen ist (besondere Zugriffsrechte für hinterlegte Schlüssel), erhält das Personal Basisrechte für die Kommunikation mit den Gerät. Umgekehrt können in der App für das Werkspersonal die Schlüssel der Geräte hinterlegt sein, auf die sie Zugriff haben. So lassen sich Geräte automatisch identifizieren, um Fehler zu vermeiden.

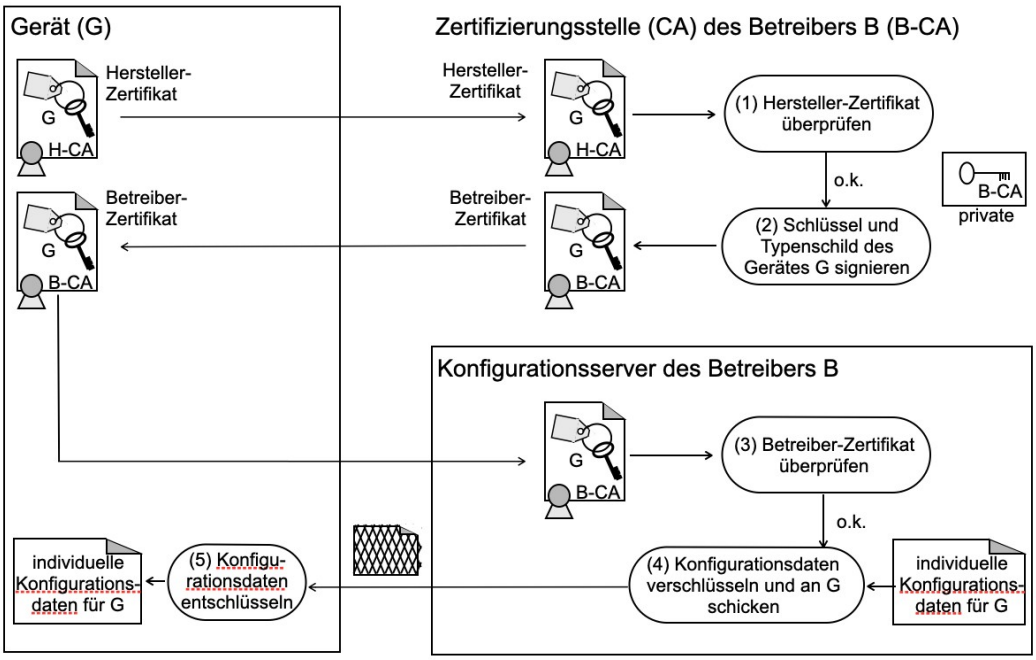
Frage 5.4.5: Austausch der Zertifikate. Betreiber B hat Geräte vom Hersteller H gekauft, auf denen Zertifikate des Herstellers H hinterlegt sind. Diese Zertifikate von H sollen durch Betreiberzertifikate von B ausgetauscht werden. Skizzieren Sie einen Ablauf hierzu und erläutern Sie ihr den Ablauf.

Lösung: Der Betreiber liest die Herstellerzertifikate aus (siehe Frage 2.1), überprüft die Zertifikate (siehe Frage 2.1) und stellt dann neue Zertifikate aus, indem er den öffentlichen Schlüssel des Gerätes G in seiner Zertifizierungsstelle signieren lässt (siehe Frage 2.1). Hierbei lassen sich auch weitere Infor-

mationen in das Zertifikat einschließen, wie z.B. die Seriennummer des Gerätes, Kenngrößen, Baujahr etc, wie sie auf Typenschildern zu finden sind. Abbildung siehe Lösungen zu Frage 2.6.

Frage 5.4.6: Sichere Software-Updates. Mit Hilfe der Betreiberzertifikate soll das Gerät mit Software bzw. mit Daten bespielt und konfiguriert werden, Skizzieren Sie einen Ablauf hierzu und beschreiben Sie den Ablauf.

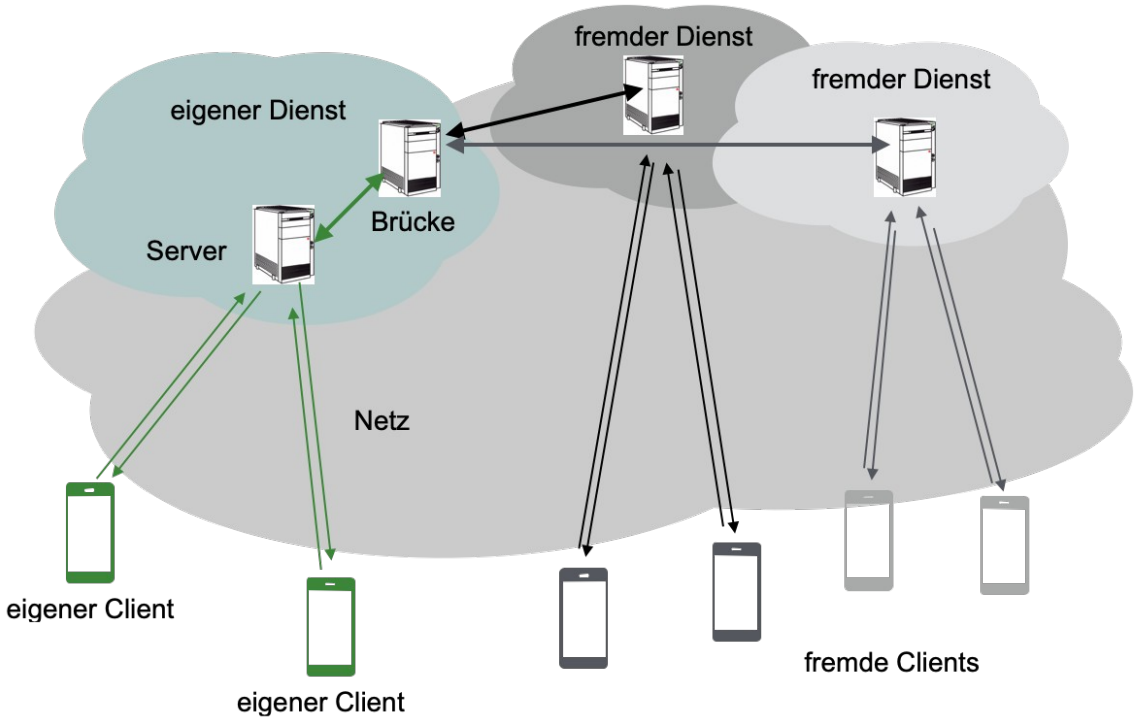
Lösung: siehe Abbildung unten. der Konfigurationsserver des Herstellers überprüft das Geräte-Zertifikat, verschlüsselt (und signiert) die Konfigurationsdaten bzw. Installationsdateien, und überträgt diese dann an das Gerät. Details siehe Skript.



(b) Ablauf im Netz des Betreibers B

5.4. Kurznachrichten- und Konferenzdienst

Ein eigener Kurznachrichtendienst (Chat-Server) soll wie in folgender Abbildung gezeigt realisiert werden. Neben Kurznachrichten mit Gruppenfunktionen besteht auch die Möglichkeit des Austausches per Sprache und Video (individuell oder in Art einer Web-Konferenz). Benutzer verwenden auf ihren Endgeräten (Smartphones, Tablets, Laptops etc.) passende Client-Apps zu den Servern. Die eigenen Server kooperieren mit Servern fremder Dienste, so dass sich deren Clients (fremde Clients = Clients mit anderen Apps) in die Chats oder Konferenzen einbinden lassen.



Der Dienst soll insgesamt 10 Millionen Clients erreichen, hiervon 1 Million eigene Clients. Die fremden Clients sollen über Brücken-Server zu den Chat-Servern der fremden Dienste angebunden werden, wobei die Brücke jeweils einzelne Transaktionen bedient (d.h. die fremden Clients verursachen den gleichen Verkehr wie die eigenen Clients). Für die Transaktionen wird folgendes Verkehrsmodell verwendet:

- 10,8 **Kurznachrichten** pro Teilnehmer in der Hauptverkehrsstunde mit 10 kBytes pro Kurznachricht
- 1,8 Anrufe bzw. **Sprachnachrichten** pro Teilnehmer in der Hauptverkehrsstunde von 100 Sekunden Dauer mit einer Datenrate von 64 kbit/s
- 0,45 **Video-Anrufe** pro Teilnehmer in der Hauptverkehrsstunde für Web-Konferenzen mit einer Dauer von 30 Minuten mit einer Datenrate von 256 kbit/s

Frage 5.5.1: Kurznachrichten. Welche Transaktionsrate ergibt sich für Kurznachrichten insgesamt? Welche Datenrate ergibt sich für diese Transaktionen am Server? Welchen Anteil hiervon müssen (a) der Server und (b) die Brücke zu den anderen Diensten bearbeiten?

Lösung:

(1) Der Dienst erreicht über die Brücken insgesamt 10 Millionen Teilnehmer. Somit errechnet sich die Transaktionsrate zu (10^7 * 10,8) / 3600 s = 30 * 10^3 1/s = 30.000 Transaktionen pro Sekunde.

(2) Hieraus folgt eine Datenrate von 10 * 1024 * 8 bit * 30.000 1/s = 2,46 Gbit/s. Diese Datenrate muss der Chat-Server bedienen.

(3) Der Server muss alle diese Transaktionen bearbeiten; die Brücke 9/10 der Transaktionen.

Frage 5.5.2: Sprache und Video. Welche Transaktionsraten ergeben sich für die genannten Dienste? Welche Transaktionsrate ergibt sich zusammen mit den Kurznachrichten (Frage 1.1)? Wie viele aktive Sessions bearbeitet der Server für Sprache und Video?

Lösung:

(1a) Sprache: Anteil 1,8/10,8 = 1/6 an den Kurznachrichten oben, somit 5.000 1/s; (1b) Video: Anteil 0,45/10,8 = 1/24 der Kurznachrichten oben, somit 1.250 1/s.

(2) Insgesamt trägt der Anteil von Sprache und Video an der Transaktionslast nicht auf, man erhält 36250 1/s. Der Anteil von Sprache und Video hieran beträgt 6250/36250 < 20%.

(3a) Aktive Sessions für Sprache: Aus dem Produkt der Transaktionsrate [1/s] mit der Dauer der Transaktion [s] erhält man 5.000 1/s * 100 s = 500.000 parallele Transaktionen bzw. Sessions. (3b) Für die Videos errechnet man 1250 1/s * 30 * 60 s = 2.250.000 Sessions.

Frage 5.5.3: Paketraten für Sprache und Video. Sprache und Video sollen in Paketen übertragen werden, die insgesamt jeweils 20 ms Audiodaten oder Videodaten beinhalten. Welche Paketrate insgesamt ergibt sich für Sprache? Welche Paketrate insgesamt ergibt sich für Video? Welche Netto-Datenraten ergeben sich insgesamt für Sprache und Video (Overhead durch Paketköpfe nicht mitgerechnet)?

Lösung:

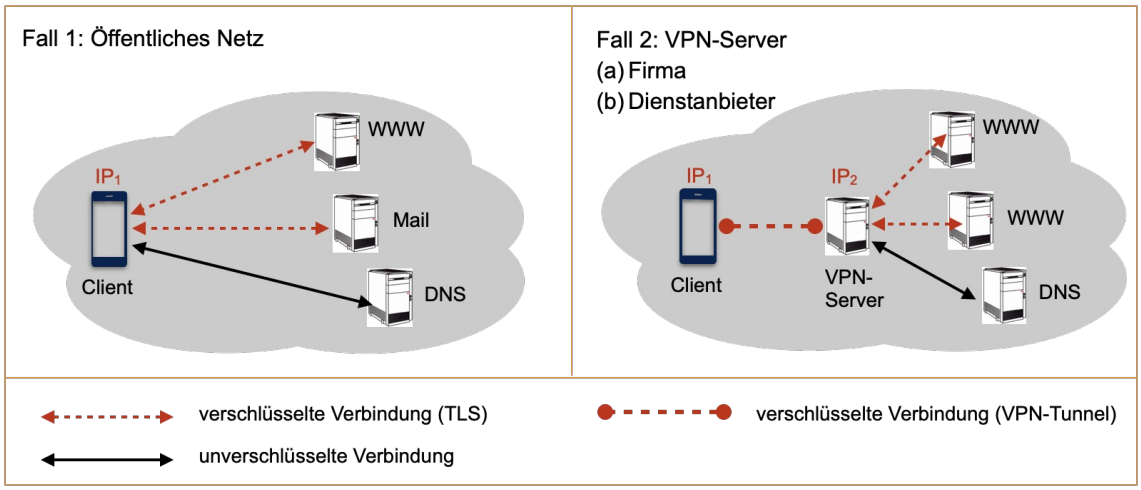
(1) Sprache: Alle 20 ms wird ein Paket verschickt, die Paketrate pro Session beträgt somit 50 1/s. Es sind 500.000 Sessions aktiv (siehe Frage 1.2). Die Paketrate insgesamt beträgt somit 25 Millionen Pakete/s.

(2) Video: Die Paketrate pro Session beträgt ebenfalls 50 1/s. Bei 2.250.000 Sessions erhält man insgesamt eine Paketrate von 112,5 Millionen Pakete/s.

(3) Netto-Datenraten: Sprache 500.000 Sessions * 64 kbit/s = 32 Gbit/s; Video 2.250.000 Sessions * 256 kbit/s = 576 Gbit/s.

5.5. Sichere Verbindungen

Der Zugang von einem Client zu Servern im Netz kann entweder direkt erfolgen, wie in Fall 1 in der Abbildung links dargestellt, bzw. indirekt über einen VPN-Server, wie in Fall 2 in der Abbildung rechts. In beiden Fällen erhält der Client eine öffentliche IP Adresse.



Frage 5.6.1: Transport Layer Security (TLS). Verbindungen zu Web-Servern sollen über verschlüsselte Verbindungen mit Hilfe von HTTPS erfolgen. Hierbei sollen sich Web-Server mit Hilfe von Zertifikaten ausweisen. Beschreiben Sie den Nutzen der Zertifikate (einschließlich der Verschlüsselung). Welcher Schutz wird hierdurch gewährt? Hinweis: Stichworte genügen.

Lösung: Zertifikate: (a) Identitätsnachweis für den Server => Integrität, (b) Durch den übermittelten öffentlichen Schlüssel des Servers kann eine verschlüsselte Verbindung aufgebaut werden bzw. ein Schlüssel übertragen werden => Vertraulichkeit der Inhalte.

Frage 5.6.2: Verbindungsdaten. Welche Informationen verbleiben im Netz, auch wenn die Inhalte der Kommunikation verschlüsselt werden? Welche Gefahren ergeben sich hierdurch für den Client?

Lösung: Zieladressen, Quelladressen und die Zeitpunkte der Abfragen verbleiben im Netz. Hieraus lassen sich Kommunikationsprofile der Clients erstellen (mit wem wird wann und wie oft kommuniziert).

Frage 5.6.3: Unverschlüsselte DNS-Anfragen (DNS: Domain Name System, Auflösung der Domain-Namen in IP-Adressen). Welche Gefahren gehen von unverschlüsselten Anfragen aus? Welche Ärgernisse sind außerdem mit DNS-Anfragen verbunden?

Lösung: (1) Verbindungsdaten und die angefragten Domains (= Inhalte der Anfrage) sind sichtbar: Auch hierüber lassen sich Nutzerprofile erstellen. (2) Werbung auf Web-Seiten, die weitere DNS-Anfragen verursachen.

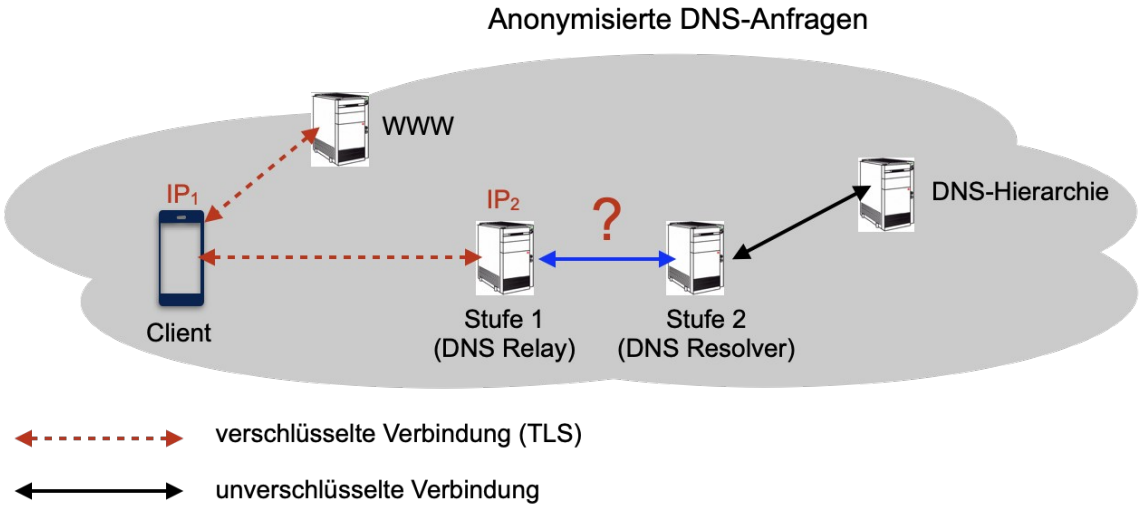
Frage 5.6.4: VPN-Server im Firmennetz (Fall 2a). Beim Zugang ins Firmennetz wird eine Verbindung eingesetzt, die als Tunnel jede Kommunikation mit dem VPN-Server verschlüsselt. Somit wird der Client über diesen Tunnel Teil des Adressraums des Firmennetzes (in der Abbildung ist dieser private Adressraum nicht dargestellt, sondern nur öffentliche IP-Adressen IP_1 und IP_2). Beschreiben Sie die Eigenschaften der VPN-Verbindung. Wie unterscheidet sich der VPN-Tunnel von TLS? Wie werden über die VPN-Verbindung Dienste im öffentlichen Netz erreicht?

Lösungsbeispiele: (1) Der Tunnel stellt eine Punkt-zu-Punkt-Verbindung zwischen Client und VPN-Server dar. Unabhängig von der Wahl der Kommunikationsverbindung und der Verschlüsselung werden alle Anwendungen über diesen Kanal geführt, einschließlich der IP-Verbbindung im privaten Adressraum des Firmennetzes. (2) TLS unterstützt Anwendungsprotokolle zwischen dem Client und verschiedenen Servern, z.B. HTTPS. VPN tunnelt als Punkt-zu-Punkt-Verbindung Anwendungen zwischen Client und VPN-Server. (3) Im öffentlichen Netz repräsentiert der VPN-Server den Client, der Client (bzw. dessen IP-Adresse) bleibt daher bei solchen Anfragen verborgen. Für den VPN-Server lassen sich wiederum Verbindungsdaten sammeln, einschließlich der DNS-Anfragen (sofern im Firmennetz kein eigener DNS-Proxy verwendet wird).

Frage 5.6.5: VPN-Server eines Dienstanbieters (Fall 2b). Anstelle der Firma stellt den VPN-Server ein Dienstanbieter zur Verfügung. Ein Firmennetz gibt es hierbei nicht. Welchen Zweck verfolgt ein solches Angebot (bitte mit Begründung)? Welche Einschränkungen bestehen? Welche Gefahren sind mit der Nutzung eines solchen Servers verbunden?

Lösung: (1) Auch hier bleibt im öffentlichen Netz die IP-Adresse des Clients verborgen, der VPN-Server arbeitet als dessen Stellvertreter. Die Verbindung vom Client zum VPN-Server ist als Tunnel realisiert, alle Anfragen zum VPN-Server bleiben im Netz verborgen. Zweck: Verbergen der eigenen Identität bei Anfragen im Internet, Umgehung von Sperren für Web-Seiten und Streaming-Angebote (letztere mit Sperren für ausländische IP-Adressen). (2) Einschränkungen: VPN-Server lassen sich in schwarzen Listen sperren; DNS-Anfragen sind weiterhin lesbar; Sperren von Web-Seiten an DNS-Servern bleiben möglich. (3) Gefahren: Man muss dem Dienstanbieter vertrauen, da der VPN-Tunnel hier endet und der Anbieter alle Anfragen mitlesen und mitschreiben kann.

Frage 5.6.6: Anonymisierte DNS-Anfragen (Abbildung unten). Folgende Abbildung zeigt eine Anordnung zur zweistufigen Bearbeitung von DNS-Anfragen: Stufe 1(Relay) nimmt die Anfrage des Client entgegen und übernimmt die Anfrage im DNS-System, Stufe 2 (Resolver) löst die Anfrage auf, kennt aber den Client nicht. Damit die Client-Anfrage im Netz nicht lesbar ist, muss diese vom Client verschlüsselt werden. (1) Erläutern Sie das Funktionsprinzip. (2) Welche Aufgabenteilung zwischen Stufe 1 (Relay) und Stufe 2 (Resolver) wäre wünschenswert? Wo muss die Client-Verschlüsselung somit enden? Begründen Sie Ihre Aussagen. (3) Welche Vorteile bringen anonymisierter DNS-Abfragen?



Lösung: (1) Funktionsprinzip: Im einfachsten Fall kennt Stufe 1 die Frage und den Fragesteller, verbirgt aber dessen Identität bei der Weitergabe der Frage. Stufe 2 kennt die Antwort auf die Frage, kann aber den Fragesteller nicht identifizieren. Vom übergeordneten DNS-System aus sind die Anfragen anonym, nicht jedoch für den Server auf Stufe 1 (Relay): Dieser kennt Frage und Fragesteller. Dieses System wäre somit vergleichbar einem VPN. Es gibt eine bessere Aufgabenteilung.

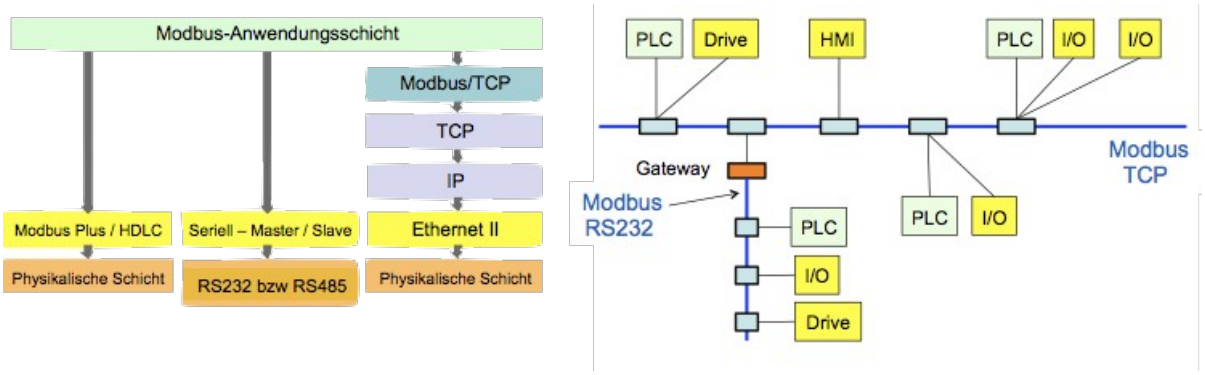
(2) Aufgabenteilung: Stufe 1 (Relay) sollte den Client kennen (IP-Adresse IP_1 des Fragenden), jedoch nicht dessen Frage (Inhalt der DNS-Anfrage). Der Stufe 2 (Resolver) sollte die Identität des Fragenden verborgen sein (in Art einer anonymen Anfrage). Stufe 1 sollte daher verschlüsselte Anfragen des Clients entgegen nehmen und diese verschlüsselt an die Stufe 2 weitergeben, jedoch mit der eigenen IP-Adresse IP_2 als Absender. Stufe 2 entschlüsselt die Anfragen für das DNS-System und verschlüsselt die Antworten für die Stufe 1. Stufe 1 leitet die verschlüsselten Anfragen weiter an den Client.

(3) Vorteile: DNS-Anfragen reduzieren sich auf deren Verbindungsdaten: die angefragten Inhalte bleiben verborgen. Einen Schutz gegen Werbung bietet das Verfahren nicht: alle diesbezüglichen Anfragen werden über die beiden Stufen geführt. Anonymität gegen Betreiber von Web-Seiten bietet das Verfahren ebenfalls nicht, da diese ihre Clients auf Anwendungsschicht identifizieren (auch ohne Anmeldung durch Cookies, Browser-Informationen, Click-Muster, …). Verborgen bleibt nur die IP-Adresse des Clients.

Hinweis: Die Anonymität setzt eine strikte Arbeitsteilung zwischen den Betreibern der Relays und Resolver voraus. Kooperieren diese (indem sie Verbindungsdaten austauschen), ist die Anonymität gebrochen.

5.6. Kopplung von Anlagen

Eine Anlagensteuerung soll mit Hilfe eines Feldbusses aufgebaut werden. Hierzu soll Modbus eingesetzt werden, sowohl als serieller Bus (RS232) als auch im Netzwerk. Folgende Abbildung zeigt die Protokollschichten (links), sowie die vorgesehene Konfiguration (rechts).



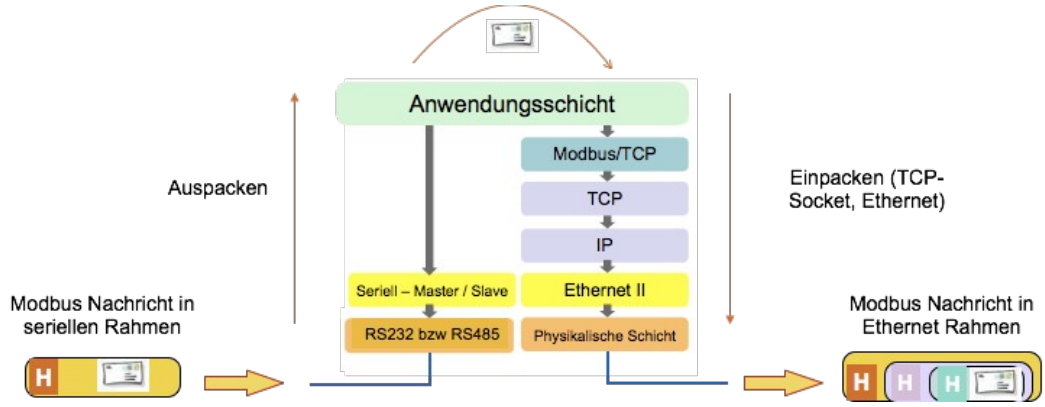
Hierbei bedeuten: (1) PLC: Programmable Logic Control (programmierbare Steuerung, engl. für SPS), (2) HMI: Human Machine Interface (Bedienterminal), (3) I/O: Input/Output (An-schaltung digitaler und analoger Eingänge bzw. Ausgänge), (4) Drive: Antrieb.

Frage 5.7.1: Welche Unterschiede gibt es zwischen der seriellen Kommunikation und der Kommunikation über das Netzwerk?

Lösung: (1) Seriell: üblicherweise Punkt zu Punkt Verbindung (keine Netzadressen), bzw. mit Busmaster und Slaves über ein gemeinsames Medium (unter Verwendung von Geräte-adressen). Die Kommunikation ist als auf die Verbindung zwischen zwei Geräten bzw. zwischen Geräten um Bussegment lokal begrenzt. (2) Netzwerk: zwischen Geräten im lokalen Netz (unter Verwendung von MAC-Adressen im Ethernet) bzw. zwischen Geräten im IP-Netz (unter Verwendung von IP-Adressen) im privaten bzw. öffentlichen Weitverkehrsnetz.

Frage 5.7.2: Gateway. Für die Kommunikation zwischen dem Netzwerk (Modbus TCP) und dem seriellen Zweig (Seriell – Master/Slave) wird ein Gateway eingesetzt. Skizzieren Sie die Protokollschichten des Gateways. Erläutern Sie die Funktion der Schichten im Gateway. Was geschieht mit einer Nachricht, die das Gateway passiert? Wie können Geräte im Netzwerk erreicht werden? Hinweis: Verwenden Sie die Protokollschichten in der Abbildung oben und entpacken bzw. verpacken Sie die Nachrichten beim Durchgang durch das Gateway.

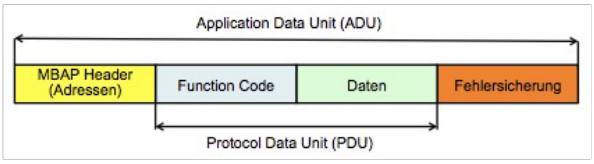
Lösung: Das Gateway vermittelt Nachrichten zwischen beiden Segmenten.



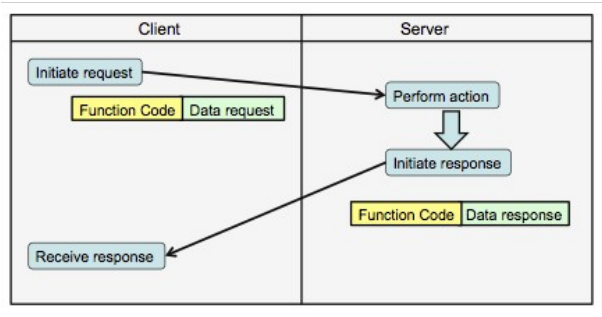
Jedes Segment hat unterschiedliche Protokollschichten, bis auf die Anwendungsschicht: (1) Physikalische Schicht: serieller Bus bzw. RS232 Schnittstelle, Ethernet Medium z.B. Fast Ethernet, (2) Rahmenprotokoll (bei Ethernet inklusive MAC-Adressen als lokale Netzadressen), (3) Netzwerkprotokoll (IP-Adressen), ab (4) Anwendungsprotokolle (TCP-Sockets). Das Gateway verpackt die Modbus-Nachricht auf Anwendungsebene zwischen den Protokoll-schichten um.

Da im seriellen Zweig keine Netzwerkadressen (Ethernet, IP) verwendet werden, muss die Anwendungsschicht diese erzeugen, damit die Nachricht die korrekten Adressaten erreicht. Das kann beispielsweise mit Hilfe der Modbus Geräteadressen geschehen (nach Konfiguration des Gateways).

Frage 5.7.3: In der Modbus Spezifikation findet sich folgende Protokollbeschreibung.



- PDU: unabhängig von den genutzten Protokollschichten
- ADU: Anpassung an die genutzten Protokollschichten
- Function Code (1 Byte): Definition der auszuführenden Aktion



Modbus Request PDU

- mb_req_pdu = {function_code, request_data}

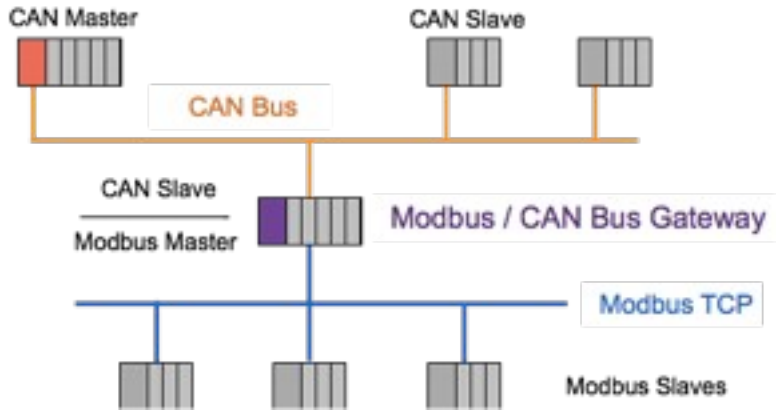
Modbus Response PDU

- mb_rsp_pdu = {function_code, response_data}

Welche Funktionen haben PDU und ADU bei der Kommunikation zwischen den Geräten? Wie werden PDU und ADU im Gateway verwendet? Was geschieht bei einer Anfrage des Clients an den Server? Wozu dient der Function Code?

Lösung: (1) Die ADU enthält die Modbus Geräteadressen, sowie eine Fehlersicherung (durch eine Prüfsumme). Der Kopf der ADU (MBAP Header) enthält die Geräteadresse (Ziel-adresse). Letztere wird benötigt, um den Anwendungsrahmen zu schützen. (2) Das Gateway wertet die in der ADU enthaltenen Informationen aus, unabhängig von der PDU. (3) Die Nachrichtenformate (Zweck der Nachricht, Fehlermeldungen etc) sind in die PDU kodiert. Dieser Teil ist unabhängig von der Kommunikation im seriellen Segment bzw. im Netz. (4) Client und Server verwenden auf Anwendungsebene nur die PDU. (5) Function Code: Zweck der Nachricht (z.B. Lesen bzw. Schreiben bestimmter Datenbereiche, Fehlermeldungen, …). Der Funktion Code lasst sich auf Korrektheit überprüfen (ungültige Codes).

Frage 5.7.4: CAN-Bus Gateway. Ein Hersteller bietet Gateways zwischen unter-schiedlichen Bussystemen an, wie z.B. das unten gezeigte CAN-Bus zu Modbus Gateway. Worin bestehen die Unterschiede zu dem Gateway aus Frage 3.2? Wie erfolgt die Kommunikation zwischen den unterschiedlichen Bussystemen? Beschreiben Sie die Funktionsweise des CAN-Bus Gateways.



Lösung: Im Unterschied zu Frage 3.2 erfolgt die Verbindung auf Anwendungsebene. In der gezeigten Konfiguration ist CAN Bus das überlagerte Netz. Das Modbus / CAN Bus Gate-way terminiert den CAN Bus als CAN Bus Slave, verhält sich also buskonform. Im unterlagerten Bus (Modbus) verhält sich das Gateway ebenfalls buskonform als Master (Client). Auf diese Weise kann das Gateways Anfragen des CAN Masters (Clients) als Modbus Master (Client) an Modbus Slaves (Server) weiter geben. Die unterschiedlichen Nachrichtenformate werden auf Anwendungsebene ineinander übersetzt. Hierzu ist eine Konfiguration des Gateways durch den Administrator erforderlich.

Frage 5.7.5: Modbus arbeitet mit 8-Bit Server-Adressen (Slave-Adressen). Ein Modbus Segment ist bereits mit 3 Geräten (Slaves) in Betrieb. Ein weiteres Gerät soll mit zufällig gewählter Adresse mit ihn Betrieb genommen werden. Wie groß ist die Wahrscheinlichkeit, dass es keine Konflikte (Kollisionen) mit einer der bereits existierenden Geräte-adressen gibt?

Lösung: In der Realität würde man in diesem Fall die Adressen manuell überprüfen und so Konflikte vermeiden. Rechnerisch ermittelt man die Lösung aus $P(n)=(1-1/M)^{n-1}$, wobei n die Anzahl der Geräte insgesamt darstellt, M die Anzahl möglicher Adressen (M = 256). Für n = 4 ermittelt man P(4) = 0,988.

Frage 5.7.6: Für ein Modbus Segment sollen alle Adressen zufällig vergeben werden. Wie viele Geräte können auf diese Art betrieben werden, wenn die Wahrscheinlichkeit für Konfliktfreiheit (keine Kollisionen) größer als 0,999 sein soll? Halten Sie die zufällige Adressvergabe für praktikabel? Wäre die zufällige Adressvergabe mit dieser Vorgabe für die Kollisionsfreiheit für 16-Bit Adressen praktikabel?

Lösung: Mit 8-Bit Adresse ist das Verfahren nicht praktikabel, die Vorgabe lässt sich bereits mit 2 Geräten nicht erzielen. Mit 16-Bit Adressen könnten bis zu 14 Geräte mit zufälligen Adressen versorgt werden. Bei dieser überschaubaren Größe macht das Verfahren gegenüber der manuellen Vergabe wenig Sinn. Die Lösung ermittelt sich rechnerisch z.B. per Rekursion aus P'(n) = (1 - (n-1) / M) P'(n-1) mit P'(2) = (1 - 1/M).

Englisch - Deutsch

Admission control	Zulassungskontrolle
Air Interface	Funkschnittstelle
Application layer	Anwendungsschicht, Verarbeitungsschicht
Basic Services (BS)	Basisdienste
Bearer Service	Trägerdienst
Block Error Rate	Blockfehlerrate
Broadcast	Rundsendung
Call Control	Rufsteuerung
Call Drop Rate	Verbindungsabbruchrate
Call Forwarding (CF)	Rufumleitung
Carrier	Verbindungsnetzbetreiber
Cell Identity (CID)	Zellkennung
Circuit switched domain	Leitungsvermittelte Domäne
Circuit switching	Leitungsvermittlung
Confidentiality	Vertraulichkeit
Content Provider	Inhalteanbieter
Control Plane	Steuerungsebene
Core Network	Kernnetz
Credentials	Beglaubigung, Zeugnis
Data Link Layer	Sicherungsschicht
Delay, Latency	Verzögerung, Laufzeit
Downlink	Abwärtsstrecke
Echo Canceller	Echokompensator
Expedited Forwarding	beschleunigtes Weiterleiten
Fading	Schwund
Firewall	Brandschutzmauer, Paketfilter
Frame Error Rate	Rahmenfehlerrate
Frequency Division Multiple Access	Frequenzvielfachzugriff
Handover, Handoff	(Verbindungs-)Übergabe, Weiterreichen
Integrity	Unversehrtheit (von Daten bzw. Systemen)
Jitter	Laufzeitschwankungen
Line of Sight	Sichtverbindung
Local Area Network	Lokales Rechnernetz
Location Area (LA)	Aufenthaltsbereich
Mobile Termination	Mobilfunk-Netzabschluss
Mobility Management	Mobilitätssteuerung
Multicast	Vielfachsendung

narrowband	schmalbandig
Network Layer	Vermittlungsschicht
Packet Loss	Paketverlust
Packet Switching	Paketvermittlung
Penetration Loss	Wanddämpfungsverlust
Physical Layer	Physikalische Schicht
Power Control	Leistungsregelung
Presence Service	Erreichbarkeitsdienst
Processing Gain	Prozessgewinn
Pseudo Noise Sequence	Pseudozufallsfolge
Push Service	Zustelldienst
Quality of Service	Dienstgüte
Release	Ausgabe (eines Normenpaketes oder Softwarepaketes)
Resource Management	Administration der Betriebsmittel
Resources	Betriebsmittel
Routing	Verkehrslenkung
Scrambling	Verwürfelung
Sensitivity	Empfindlichkeit
Service Provider	Dienstanbieter, Diensterbringer
Session	Sitzung
Session Layer	Sitzungsschicht
Session Management	Sitzungssteuerung
Short Message	Kurznachricht
State Event Diagram	Zustandsübergangsdiagramm
Subframe	Teilrahmen
Sublayer	Teilschicht
Subscription	Vertragsabschluss, Subskription, Diensteinschreibung
Supplementary Services (SS)	Zusatzdienste
Terminal Equipment	Endgerät
Time Division Multiple Access	Zeitvielfachzugriff
Traffic Model	Verkehrsmodell
Transcoding	Umcodierung
Transport Layer	Transportschicht
Uplink	Aufwärtsstrecke
User Equipment	Teilnehmerausrüstung
User Plane	Nutzerebene

Abkürzungen

AAA	Authentication, Authorization, Accounting
AG	Access Gateway
AP	Access Point
API	Application Programming Interface
CDMA	Code Division Multiple Access
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
LAN	Local Area Network
MAC	Medium Access Control
MSISDN	Mobile Subscriber ISDN Number
OSPF	Open Shortest Path First
RFC	Request For Comments (IETF)
RTP	Real Time Transport Protocol
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
UDP	User Datagram Protocol
UML	Unified Modeling Language
URL	Universal Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WWW	World Wide Web
XML	Extended Markup Language

Literatur

(1) R. Hoheisel, H. Jansen, R. Kochranke, G. Siegmund et al: Informationstechnik, Telekommunikation, Neue Netze, Europa-Lehrmittel; 7 Auflage, 2015, ISBN-13: 978-3808536278

(2) Gerd Siegmund, SDN – Software Defined Networking: Neue Anforderungen und Netzarchitekturen für performante Netze, VDE VERLAG GmbH, 2018, ISBN-13: 978-3800745111

(3) Andrew S. Tanenbaum, Computer Netzwerke, Pearson Studium; Auflage: 5., überarbeitete Auflage (2012); ISBN 978-3-86894-137-1

(4) Bruce Schneyer, Secrets & Lies: IT-Sicherheit in einer vernetzten Welt, dpunkt.verlag/Wiley; Auflage: 1. Aufl. (2001), ISBN-13: 978-3898641135

(5) Gerd Siegmund, Technik der Netze, Band 1 und 2, Band 1: Klassische Kommunikationstechnik: Grundlagen, Verkehrstheorie, ISDN/GSM/IN - Band 2: Neue Ansätze: SIP in IMS und NGN; VDE-Verlag; Auflage: 6., vollst. neu bearbeitete und erweiterte Auflage (2010); ISBN-13: 978-3800732203

(6) Harald Orlamünder, Paketbasierte Kommunikationsprotokolle: Hüthig Telekommunikation; Auflage: 1 (2005) ISBN-13: 978-3826650468

(7) Franz-Josef Banet, Anke Gärtner, Gerhard Teßmar, UMTS: Netztechnik, Dienstarchitektur Evolution, Hüthig Telekommunikation; Auflage: 1 (2004), ISBN-13: 978- 3826650345

Anhang A – Protokollschichten