Teil1: IRDA

1. Eigenschaften von IrDA + Verwendung/Applikationen

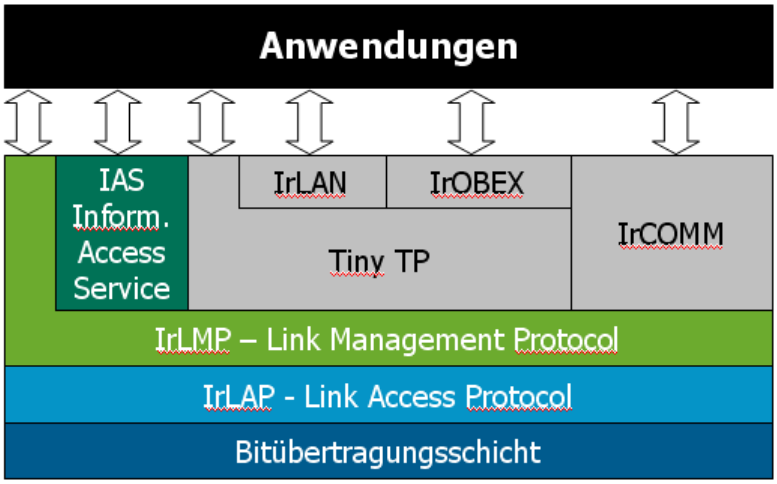
Merkmale

- Kompletter IRDA Protokollstack (IRPHY, Framer, IRLAP, IRLMP, IAS, TINYTP, IRCOMM, IROBEX)
- Primary und Secondary Funktion (skalierbar)
- Datenraten von 9,6 kBit/s - 16 MBit/s (skalierbar)
- Wiederverwendbare IP
- Automatisch konfigurierbare IP
- Einfache Systemintegration
- leichte Bedienung über API
- Geringer Ressourcenverbrauch
- Synthesefähige VHDL (=Hardwarebeschreibungssprache) Beschreibung
- C-Code auf zahlreiche Mikrocontrollerarchitekturen portierbar
- Kleine Reichweite (nur innerhalb von Gebäuden anwendbar) es muss Sichtverbindung zw. 2 Geräten sein.
- Große Abhörsicherheit
- Weltweit erprobte universelle, schnurlose Datenverbindung
- Über 150 Millionen Geräte
- Breite Palette an unterstützte HW, SW-Plattformen, sowie Betriebssystemen
- Bei Punkt-zu-Punkt-Verbindungen im Einsatz
- Rückwärtskompatibilität zwischen Versionen
- Enger Sendekegel, damit wenig Interferenz mit anderen Geräten
- Robuster Betrieb
- Anteile von Infrarot befinden sich im Sonnenlicht -> Störung so stark dass nur innerhalb von Gebäuden Irda funktioniert.
- Unempfindlich gegenüber elektromagnetischen Störungen (Maschinen, Funksender)

Anwendungsbereiche

- Portable High Speed Systeme
- Portable Low Power Mikrosysteme
- Einsatz in System-on-Chip Lösungen, sowie als separater Schaltkreis
- Notebooks, PDAs
- Drucker
- Handys, Pager
- Modems
- Digitalkameras
- LAN Access Devices
- Medizintechnik
- im industriellen Umfeld
- Uhren
- Integriert in Windows, MacOS, Linux, OS/2, PalmOS, WindowsCE, Symbian,...

2. Erklären Sie den IrDA-Protocol Stack



Bitübertragungsschicht:

Hier findet die optische Übertragung statt. Der entsprechende Standard spezifiziert die Darstellung der Bits, Übertragungsgeschwindigkeiten und optische Charakteristika.

- Darstellung und Kodierung der Datenbits
- Bestimmung der Übertragungsparameter (SIR, MIR, FIR, VIR oder UFIR)
- Zugriff auf Infrarot-Medium
- Abfrage der Sendebereitschaft am Infrarot-Medium
- Unzuverlässiges Senden/Empfangen von Datenpaketen

IrLAP - Link Access Protocol (= Sicherungsschicht):

- Bereitstellung einer zuverlässigen Vollduplex-Verbindung zwischen zwei Geräten
- Zugriffssteuerung für den Infrarotkanal
- Erkennung von IrDA-Geräten innerhalb des Empfangsbereichs
- Aushandeln der Rollenverteilung *primary-secondary*
- Aushandeln von Kommunikationsparametern
- Beginnen und Beenden von Kommunikationsverbindungen

Zugriffskontrolle

- *Keine Kollisionserkennung*:
  - Werden Datenpakete von mehreren Sendern gleichzeitig versendet, kommt es zu Kollisionen. à Datenverfälschung
- *daher Master/Slave-Prinzip*:
  - Regelung des Zugriffs
  - IrLAP unterscheidet *primary* und *secundary*
  - bei Kontaktaufnahme à Rollenverteilung
  - Primary = der, der den ersten Verbindungswunsch anzeigt
  - Primary regelt Zugriff auf Ir-Kanal

IrLAP-Zustände

Normal Disconnect Mode NDM:
- Zustand nicht verbundener Geräte
- Abfrage von Geräten in Reichweite
- nur Broadcast-Nachrichten möglich

Normal Response Mode NRM
- Gerät in zuverlässiger Verbindung mit anderem Gerät
- höhere Protokolle können Daten austauschen
- fehlerhafte Pakete werden erneut angefordert

- IrLAP benutzt eine HDLC-Weiterentwicklung
- Infrarot-Übertragung ist sehr fehleranfällig
  - daher CRC (Cyclic Redundancy Check)
  - nach fünf 1-Bits wird ein 0-Bit eingefügt
  - Flags für Erkennung von Rahmen-Anfang/Ende enthalten sechs 1-Bits
- Größe eines Datenblocks: 64 -2048 Bytes

IrLMP:

- Stellt mehrere logische Kanäle über eine physikalische Verbindung her, während auf der Ebene von IrLAP nur eine einzige Verbindung zwischen 2 Geräten existiert.
- IrLMP tauscht Geräteinformationen aus, sowie installierte Dienste und stellt sie in eine kleine Datenbank
- Verhüllen der Rollenverteilung *Primary-Secondary*

LSAP, LSAP-SEL

- *Damit eine Anwendung mehrere logische Verbindungen aufbauen kann, werden LSAP's (**Logical Service Access Point**) eingeführt.*
- *Ein LSAP repräsentiert einen Dienst oder einen logischen Kommunikationskanal zu einer Anwendung.*
- *Identifizierung erfolgt über eine Nummer, dem LSAP-Selector (LSAP-SEL)*

IAS – Information Access Service:

- Suchdienste - Auskunft über verfügbare Dienste anderer Kommunikationspartner (wie gelben Seiten)
- Verarbeitung lokaler Suchanfragen und Speichern der Ergebnisse

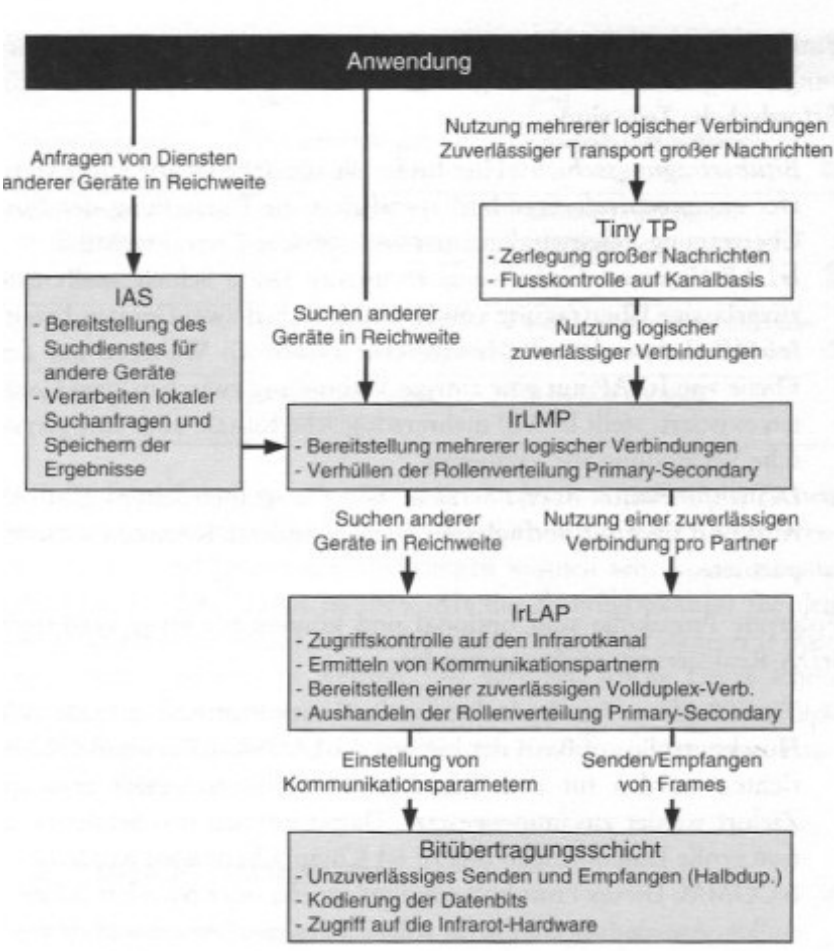
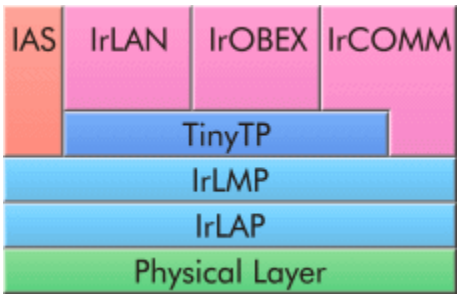


Abbildung mit den Vorgeschriebenen Protokollschichten incl. Tiny TP.

Tiny TP ist zwar optional wird aber von IrDa dringend empfohlen da es wichtige Funktionen für den Datentransport übernimmt.
Anwendungen, die auf diesen Protokollstapel aufbauen, können folgende Dienstleistungen in Anspruch nehmen:

- Suchen anderer Geräte in Kommunikationsreichweite (über IrLMP)
- Abfragen welche Dienste die Geräte anbieten (IAS)
- Nutzen dieser Dienste indem Kommunikationsverbindungen aufgebaut werden.(über TinyIP)

3. Welche optionalen IrDA-Protokolle gibt es? Erklärung



Folgende Protokolle sind optional und können bei der konkreten IrDa Realisierung weggelassen werden:

TinyTP – Tiny Transport Protocol

- Flusskontrolle auf Basis der logischen IrLMP-Kanäle
- Große Nachrichten werden für Transport zerteilt und am Zielort wieder zusammengesetzt
- Damit können pro Sendeoperation große Datenmengen (bis zu 64 Kbyte) übertragen werden.

Infrared LAN

Über dieses Protokoll kann sich ein Gerät über Infrarot an ein existierendes Lokales Netzwerk binden.

IrOBEX – Infrared Object Exchange Protocol

Das IrOBEX entspricht einem reduziertem http es dient z.B. zum Austausch von komplexen Objekten wie vCards, Texten oder Grafiken („APPLIANCES").

COM-Schnittstelle – IrCOMM

IrCOMM emuliert serielle und parallele Schnittstellen. Hier können

- Anwendungen über Infrarot drucken,
- Modems über Infrarot genutzt werden,
- Kommunikationsprotokolle benutzt werden, die eine serielle Schnittstelle benutzen (z.B. TCP/IP über PPP)

So kann mit Anwendungen mit herkömmlichen Kommunikationsschnitstellen (COM-Ports…) kommuniziert werden.

IrTRAN-P:

- für den Austausch von Bildern zwischen Digitalkameras, Drucker und PCs

IrMC:

- Rahmenwerk für mobile Kommunikation mit IrDA. Keine Protokollschicht im eigentlichen Sinn, sondern eine Sammlung von Formatspezifikationen für den Austausch von Daten wie sie in der Mobilkommunikation vorkommen.
  - Kalendereinträge, Texte, Nachrichten
  - 3G-Smartphones

IrJetSend:

- zur Einbindung des Hewlett-Packard JetSend Protokolls in die IrDA Plattform (beispielsweise HP-Taschenrechner)

4. Erklären Sie die RZI-Modulation, Warum wäre ohne RZI bei langen 1-Folgen keine Synchronisation möglich?

Ist die Modulation welche in der Bitübertragungsschicht verwendet wird.

RZI – Return Zero Inverted

- bei 0 Bits ... kurzer Ir-Impuls
- bei 1 Bits ... kein Impuls
- bei langer 1-Folge ist keine Synchronisation mehr möglich, daher muss nach fünf 1 eine 0 eingefügt werden

Zur Erreichung der hohen Datenübertragungsgeschwindigkeiten verwenden FIR und VFIR andere Modulationsverfahren als das standardmäßige Return to Zero Inverted (RZI).

Hab einen sehr guten link gefunden allerdings ist dort nur NRZI beschrieben, bin mir nicht sicher ob es dazupasst bzw. ob es NRZI richtig erklärt:

http://lexikon.izynews.de/de/dir/default_fr.aspx?u=http%3a%2f%2flexikon.izynews.de%2flex%2fIrDA

5. Datenraten IrDA, Reichweite

Infrarot-Kommunikation von Industriekonsortium definiert, dass ca. 150 Organisationen umfasst.

1994: IrDA SIR V1.0 bis 115,2 kbit/s
1995: IrDA FIR V1.1 bis 4 Mbit/s
1999: IrDA VFIR bis 16 Mbis/s

Datenrate	Spezifikation	Modulation
2,4 -115,2 kbps	SIR	RZI
0,576 Mbps	FIR	RZI
1,152 Mbps	FIR	RZI
4 Mbps	FIR	4PPM
16 Mbps	VFIR	HHH (1,13)

Die entsprechende Empfangsdiode bei IrDA ist so ausgelegt, dass sie Reichweiten von etwa einem Meter ermöglicht - theoretisch. Das große Problem an der Infrarottechnik ist nämlich die Tatsache, dass die Übertragung empfindlich auf äußere Einflüsse wie Umgebungslicht und reflektierende Gegenstände reagiert. Unter direkter Sonnenlichteinstrahlung ist man daher schon über 10 cm Reichweite froh, während unter Kunstlicht auch gerne mal mehr als ein Meter drin ist.

6. Erklären Sie die Aufgaben des IrLAP

Siehe Frage: Erklären Sie den IrDA-Protocol Stack

7. Wie läuft die Kontaktaufnahme zweier IrDA-Geräte ab?

Werden Datenpakete mehrere Pakete versendet so kommt es zu Kollisionen bei denen der Inhalt verfälscht wird und somit die Nutzdaten nicht mehr verwendbar sind. Daher wird mit Hilfe des Master/Slave Verfahrens der alleinige Zugriff auf den IR-Kanal geregelt.
IrLAP unterscheidet hierfür im NRM zwischen Primary und Secondary (NRM (S)). Üblicherweise ist das Gerät welches um eine Verbindung ansucht der Master und das antwortende Gerät Slave. Senden Beide gleichzeitig einen Verbindungswusch so entscheidet der Zufall.

8. Wie wird bei IrDA der Zugriff auf den IR-Kanal geregelt?

Nach Rollenvergabe regelt Primary den Zugriff auf den IR-Kanal und kann unaufgefordert senden. Ein Secondary darf nur senden wenn er vom Primary aufgefordert wird, und dann auch nur für einen best. Zeitraum. Anschließend muss er dass Senderecht an Primary zurückgeben.
Gibt es ein Primary und mehrere Secondary so wird das Senderrecht nacheinander vergeben. Diese Art der Verbindung wird Point to Multipoint genannt.
Ein Primary muss im Rahmen der Kommunikation mehr Aufgaben bewältigen als das Secondary, daher können mache Geräte wie z.B. Digitalkameras oder Drucker nur als Secondary betrieben werden. Kommen 2 Geräte in Reichweite welche nur Secondary sein können so ist eine Kommunikation unmöglich.

Während im Zusand von NRM der Zugriff auf den IR-Kanal strikt geregelt ist wurde im Zustand von NDM noch nicht ausgehandelt wer Primary oder Secondary ist. Hier muss das Verfahren *Media Access Control Rules* verwendet werden um Kollisionsfrei auf den IR-Kanal zugreifen zu können.

Pakete im NDM Zustand werden mit der festen Datenrate von 9600 Bit/s versendet
Eine laufende Kommunikation im Zustand NRM hat Vorrang gegenüber der Kommunikation im Zustand NDM. Will ein Gerät im Zustand NDM ein Paket versenden so muss es mindestens 500ms den IR-Kanal abhören bevor es sendet.

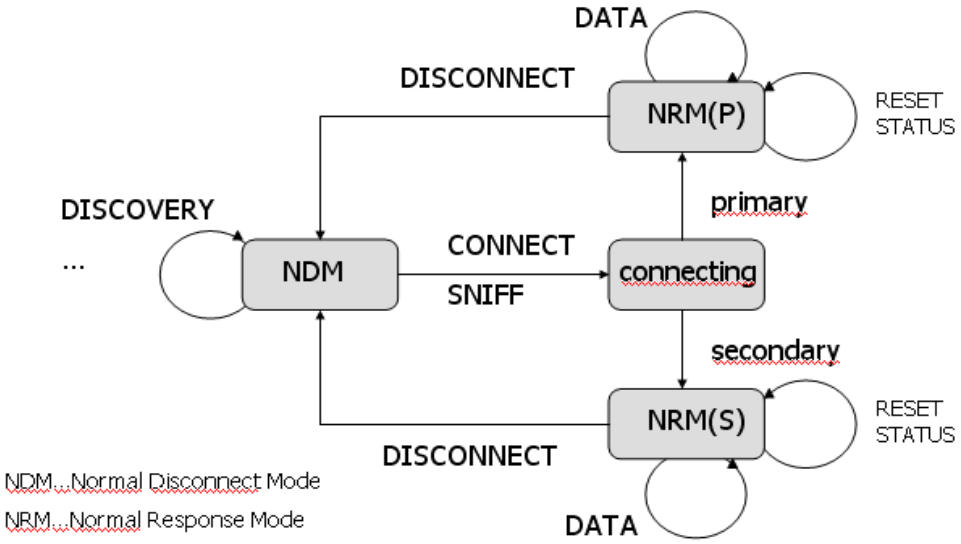
9. Woran unterscheiden sich der Normal Disconnect und der Normal Response Mode?

IrLap unterscheidet 2 Zustände in welchem sich ein Gerät befinden kann:

Normal **D**isconnect **M**ode auch als Contention Mode bezeichnet: Diesen Zustand nehmen Geräte ein die nicht miteinander verbunden sind. Hier kann ein Gerät nur feststellen welche Geräte sich in der Kommunikationsbereich befinden (discovery).Die Übertragung von Nutzdaten ist bis auf folgende Ausnahme unmöglich: Es kann eine Broadcast Nachricht an alle gesendet werden, wobei dies nicht zuverlässig ist.

Normal **R**esponse **M**ode auch als Connection Mode bezeichnet. Geräte in diesem Zustand haben eine zuverlässige Verbindung zu einem anderen Gerät aufgebaut. Höhere Protokollschichten können jetzt Daten mit anderen Geräten austauschen. Die Kommunikationspartner werden bei der Verbindungsaufnahme zwischen den Partnern ausgehandelt. IrLap stellt sicher dass fehlerhafte Pakete erkannt und neu angefordert werden. Erst wenn Fehler von der IrLAP Schicht nicht behoben werden können werden höhere Schichte informiert.

10. Zeichnen Sie das IrDA- Zusatandsdiagramm



11.Erklären Sie das Link Management bei IrDA

Das Link Management wird durch das Infrared Link Management Protocol (IrLMP) geregelt. Die Rolle des Geräts innerhalb von IrLAP wird verborgen. Sowohl Primary als auch Secondary können Dienste anbieten, die vom jeweils anderen Gerät genutzt werden können. Die Asymmetrie zwischen Primary und Secondary ist für höhere Protokollschichten oder Anwendungen damit verdeckt.

IrLAP stellt zwischen Geräten lediglich eine Verbindung zur Verfügung. Für Anwendungen sind jedoch oft mehrere logische, parallel nutzbare Kanäle erforderlich. IrLAP stellt ein sehr rudimentäres Discovery zur Verfügung, bei dem nur die Geräteadressen von Geräten in Reichweite ermittelt werden. IrLMP bringt über andere Geräte wesentlich mehr in Erfahrung, beispielsweise einen Gerätenamen und die installierten Dienste. IrLMP stellt diese Informationen in einer kleinen Datenbank zur Verfügung.

12.Wozu führt man LSAPs ein?

Damit eine Anwendung mehrere logische Verbindungen zu anderen Geräten aufbauen kann, wird mir IrLMP das Konzept der logischen Dienstzugangspunkte (Logical Service Access Point, LSAP) eingeführt. Ein LSAP repräsentiert einen Dienst (z.B. einen Druckdienst) oder einen logischen Kommunikationskanal zu einer Anwendung. Ein LSAP wird über eine Nummer identifiziert, dem LSAP-Selector, kurz LSAP-SEL. LSAP-SELs bestehen aus sieben Bits und stammen aus dem folgenden Nummernkreis.

13.Warum lässt sich IrDA nicht ohne große Schwierigkeiten auf Point-to-Multipoint-Betrieb umstellen?

Da IrDA ein Master – Slave Prinzip verfolgt und dies sich eigentlich auf 2 Endgerät beschränkt, wo jeder eine der beiden Rollen zugeteilt bekommt gibt es natürlich ein Problem das ganze auf Master – MultiSlave zu portieren. Hier muss der Master einiges mehr an Management übernehmen und somit ist es nicht so einfach zu handlen.

14.Beschreiben Sie das IAS

Information Access Service ist ein spezieller Dienst. IAS kann mit den „gelben Seiten" verglichen werden. Statt einen Dienst mit einer Nummer zu identifizieren, nutzt man ein Verzeichnis, in dem man die entsprechende Dienstnummer nachschlagen kann. Mit IAS werden Informationen über zugreifbare Dienst eines Geräts für andere Geräte zugänglich gemacht. IAS ist wie ein anderer Dienst über eine LSAP-SEL zugreifbar, hierzu ist die LSAP-SEL 0 reserviert.

Das zugrunde liegende Protokoll zum Austausch von IAS-Daten wird IAP (Information Access Protocol) genannt. Eine IAS-Datenbasis besteht aus einer beliebigen Anzahl von Class-Objekten, die über einen Namen zugreifbar sind. Jede Klasse besteht aus einer Tabelle mit Attributen und Werten. Ein Objekt mit dem Namen „Device" muss in jeder Datenbasis genau einmal vorhanden sein und enthält Informationen über das Gerät, beispielsweise den Gerätenamen. Zu jedem Dienst gibt es eine weitere Klasse.

15.Wozu dient IrCOMM?

IrCOMM emuliert serielle RS-232-Schnittstellen oder parallele Centronics-Schnittstellen über eine Infrarotverbindung. Viele existierende Anwendungen und Systemprogramme sind speziell auf serielle bzw. parallele Schnittstellen zugeschnitten und ein späterer Einbau der IrDA-Funktionalität würde Modifikationen erfordern. Mit IrCOMM können diese Anwendungen ohne Änderung für die Infrarotkommunikation genutzt werden. Hiermit erschließen sich viele Möglichkeiten.

Beispielsweise:

- Können Anwendungen über Infrarot drucken
- Können Modems über Infrarot genutzt werden
- Können Kommunikationsprotokolle verwendet werden, die eine serielle Schnittstelle benutzen

Die Verwendung von IrCOMM erzeugt jedoch einige Probleme. Auf eine einzelne serielle oder parallele Schnittstelle kann immer nur eine Anwendung zu einer Zeit zugreifen. Damit wird die Möglichkeit von IrLMP mehrere logische Kanäle parallel zu verwenden nicht genutzt.

16.Wozu dient IrOBEX?

IrOBEX oder kurz OBEX stellt einen sehr komfortablen Mechanismus zur Verfügung, um komplexe Datenstrukturen zwischen zwei Geräten zu transferieren. Dieser Mechanismus ist auch unter dem Namen Beamen bekannt.

17.

a) Welches Protokoll ist bei IrDA für die Einrichtung logischer Kanäle zuständig?
IrLMP (Infrared Link Management Protocol)

b) In welche OSI-Schicht gehört dieses Protokoll?
Schicht 3, Vermittlungsschicht

c) Ist für dieses Protokoll wichtig, welcher Teilnehmer Primary und welcher Secondary ist?
Nein, Zuteilung erfolgt im LAP

d) Wenn ja, warum? Wenn nein, warum nicht?
Weil beide Dienste anbieten können, die vom jeweils anderen Gerät genutzt werden können.

e) Kann eine IrDA-Anwendung auch mehrere logische Verbindungen aufbauen? Wenn ja, wie? Wenn nein, wieso nicht?
Ja durch das LSAP. Jede Verb. Bekommt eindeutige Nr, die LSAP Set Nr.

f) Wie können mit IrDA logische Kanäle identifiziert werden?
Mit Hilfe von IAS ?

Teil2: Bluetooth

18.Eigenschaften von Bluetooth

- Es unterstützt eine Datenrate von 1 Mbit/s
- Es können Entfernungen bis zu 10 m überbrückt werden
- Geräte in Kommunikationsreichweite werden automatisch verbunden
- Ein Gerät kann gezielt nach installierten Diensten eins anderen Geräts suchen
- Es stehen mehrere zuverlässige logische Kanäle zwischen zwei Geräten zur Verfügung
- Nachrichten können unzuverlässig via Broadcast an mehrere Geräte gleichzeitig versendet werden.
- Zwischen zwei Geräten können Audiokanäle mit reservierter Bandbreite eingerichtet werden
- Es können Dienstgüte-Parameter eingestellt werden
- Es ist ein Transportprotokoll mit Flusskontrolle und Segmentierung langer Nachrichten vorhanden
- Es können serielle Schnittstellen emuliert werden
- Dienste zur Authentifzierung und Verschlüsselung sind integriert

19.Vergleichen Sie Bluetooth mit IrDA. Wo sind die wesentlichen Unterschiede und Gemeinsamkeiten?

Aufgabe	IrDA	Bluetooth
Zugriffskontrolle, Verbindungsauf-, -abbau, zuverlässige Verbindung	IrLAP	Baseband, LMP
Verschlüsselung und Authentifizierung	nein	LMP
Mehrere logische Kanäle	IrLMP	L2CAP
Segmentation and Reassembly	TinyTP	L2CAP
Kanalkennung	LSAP-SEL	CID
Protokollkennung	nein	PSM
Suche von Geräten vor Verbindungsaufbau	IrLMP	werden automatisch verbunden
Service Discovery	IAS	SDP
Kreditbasierte Flusssteuerung	TinyTP	L2CAP
Einstellung von Dienstgüte-Parametern	nein	L2CAP

Eigenschaft	IrDA	Bluetooth
Schnittstellenemulation	IrCOMM (RS 232 und Centronics)	RFCOMM (nur RS-232)
Netzwerkschnittstelle	IrLAN	über RFCOMM
Objektaustausch	OBEX	OBEX

20. Vergleichen Sie Bluetooth mit WLAN. Wo sind die wesentlichen Unterschiede und Gemeinsamkeiten?

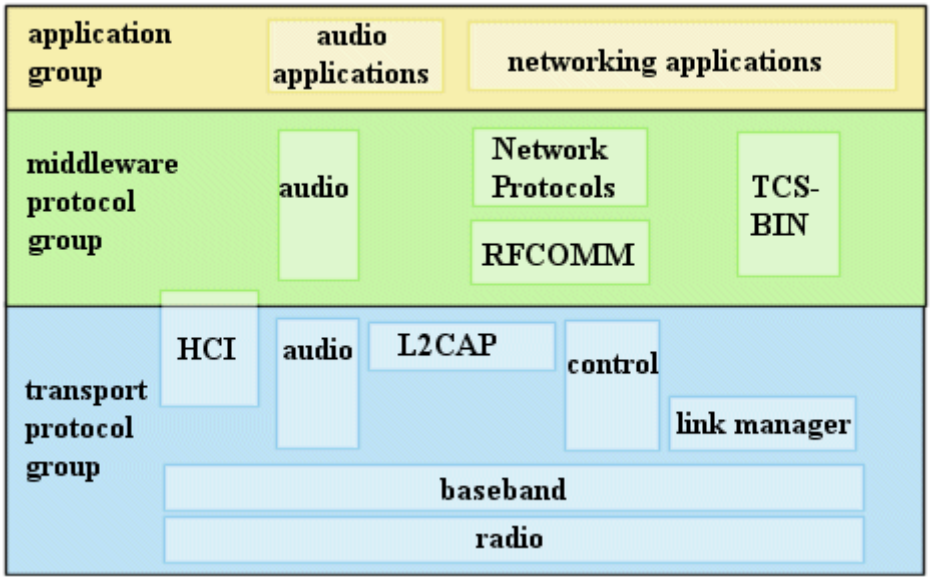
Unterschiede:
Zugriffsmethode auf Medien
CDMA-Frequency Hopping

BT-PAN: niedr. Bandbreite, Übertragung codiert, abhörsicher (Frequ.hop), kürzere Reichweite, begrenzte Anzahl an Verbindungen zu einem BT-Spot (7Slaves, 1 Master > Scatternet)

WLAN-LAN: höhere Bandbreite, Übertragung=plaintext, höhere Reichweite

Gemeinsamkeiten:
elektromagn Wellen/Übertragung, Roaming möglich

21. Welche Aufgaben haben die Bluetooth Protokoll-Schichten zu erfüllen?



1. Baseband und Radio
- Bereitstellen von synchr. und asynchr. Verbindungen
- Aushandeln der Rollenverteilung Master- Slave
- Aufbau von Verbindungen
- Einrichten von Betriebsmodi
- Kodieren der Datenbits
- Frequency-Hopping
- Zugriff auf Funk-HW
- Fehlerkorrektur

2. LMP – Link Management Protocol
- Link-Konfiguration zw. BT-Geräten
- Authentifikation und Verschlüsselung (Austausch von Keys)
- Abgleich von Uhren
- Einrichten von einfachen Dienstgüte-Parametern
- Steuert Stromspar-Mechanismen
- Steuert Verbindungsstatus von BT-Geräten

3. L2CAP - Logical Link Control and Adaption Protocol

- Verbindungsorientierte und verbindungslose Daten-Services
- Zerlegung großer Nachrichten
- Bereitstellung mehrerer logischer Kanäle
- Einrichten von zusätzlichen Dienstgüte-Parametern

4. SDP - Service Discovery Protocol
- Bereitstellung des Suchdienstes für anderes Gerät
- Verarbeiten lokaler Suchanfragen und Speichern der Ergebnisse

5. Protokoll für Kommunikations-Schnittstelle (RFCOMM)
- Serielles Leitungs-Emulations-Protokoll
- Emuliert RS-232 – Signalisierung über Bluetooth
- Stellt Datentransport für höhere Schichten zur Verfügung, welche seriell übertragen

6. TCS BIN – Telephony Contol Binary
- Bitorientiertes Protokoll
- Definiert Signalisierung für den Aufbau von Sprach- und Datenverbindungen über Bluetooth
- Definiert mobility management: dient zur Verbindung ganzer Gruppen von TCS-Geräten
- Basiert auf ITU-T Spezifikation Q.931

7. Telephony Control–AT-commands
- Umsetzung des AT-Befehlssatzes für Modems und Mobiltelefonen der ITU-T auf Bluetooth
- Entsprechend ITU-T V.250
- Zusätzlich FAX-Service-Kommandos

22.Welchen OSI-Schichten entsprechen Baseband und Bluetooth Radio?

Bluetooth Radio: Schicht 1, Bitübetragungsschicht
Baseband: Schicht 2, Sicherungsschicht

23.Link Management Protocol

siehe Frage 21

24.Wozu dient L2CAP?

Logical Link Control and Adaption Protocol
Dieses Protokoll stellt mehrere logische Kanäle zur Verfügung und segmentiert große Nachrichten für den Transport.

Siehe auch Frage 21

25.Wozu dienen SDP, RFComm, Telephony Control Protocol?

SDP - Service Discovery Protocol:
Dieses Protokoll ermöglicht, Dienste anderer Bluetooth-Geräte zu suchen.

RFCOMM:
Damit können serielle Schnittstellen emuliert werden.

Telephony Control Protocol Binary:
Dieses Protokoll stellt Funktionen zur Anrufsteuerung bereit, wie sie bei Telefonen benötigt werden.

Mehr Info: ebenfalls Frage 21

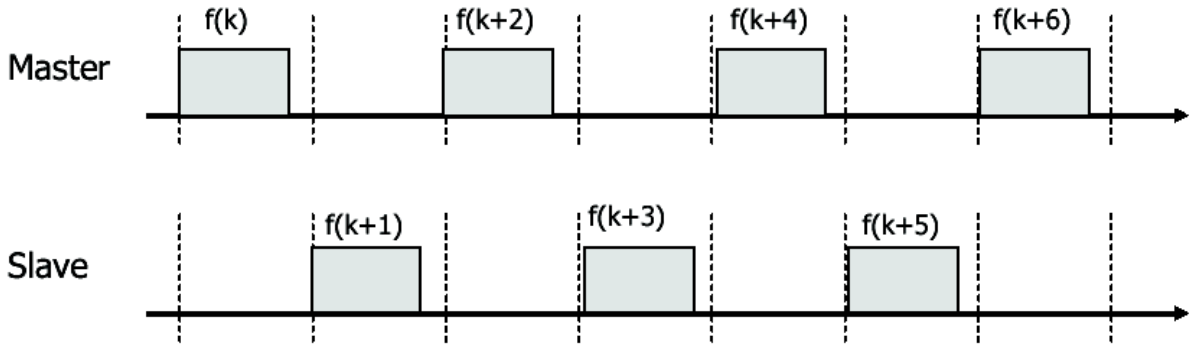
26.Erklären Sie das Frequency Hopping

Generell wechselt hier die Trägerfrequenz frequentiv und diskret. Die Sequenz der Frequenzwechsel wird durch Pseudozufallszahlen bestimmt.

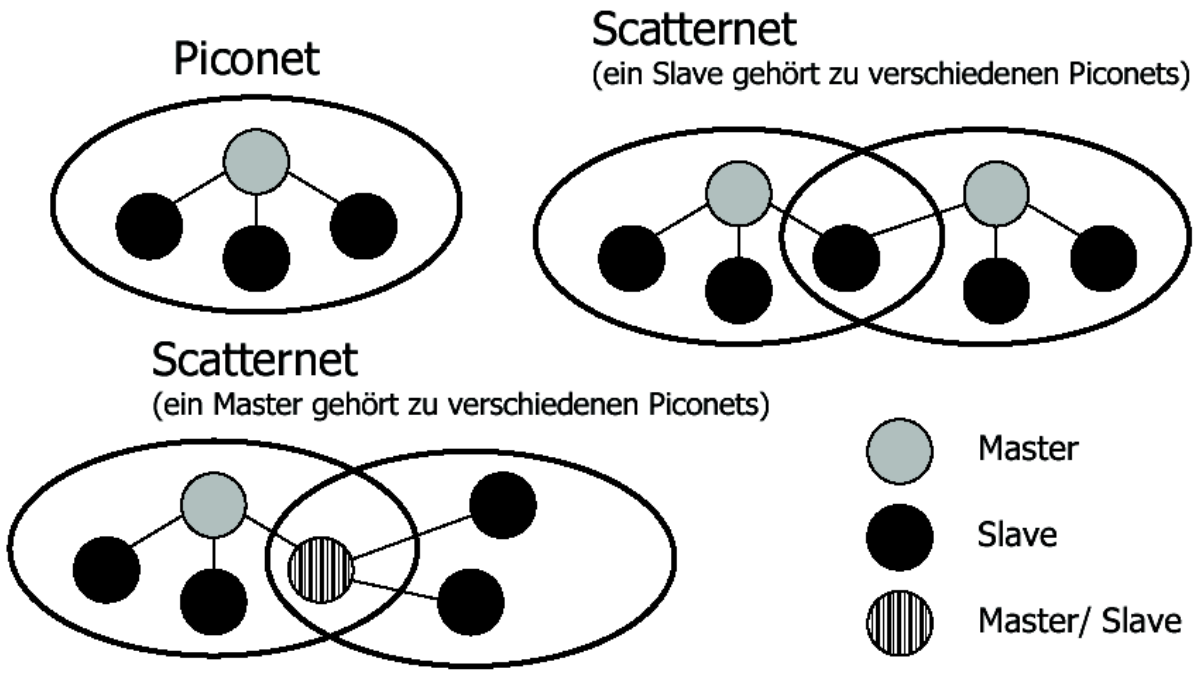
Slow Hopping:
Hierbei wird minimal 1 bit pro Frequenzsprung übertragen, also z.b. 3 Bits bevor die Frequenz wechselt.

Fast Hopping:
Hier wird maximal 1 bit pro Frequenzsprung übertragen, es können aber durchaus auch 3 Frequenzsprünge innerhalb eines Bits stattfinden.

Aus den Folien:
Regelmäßiger Wechsel zw. den 79 Kanälen
*1600 Wechsel/s = 625 µs Slo*t



27.Welche Konfigurationen von Master und Slaves sind bei Bluetooth möglich? Wie heißen sie?



28.Angenommen ein Bluetooth-Gerät A kann Verbindung mit 3 weiteren Bluetooth-Geräten (B, C und D) aufnehmen.

a) Welche Konfigurationen sind prinzipiell vorstellbar, wenn alle Geräte beteiligt sind? Benennen Sie diese.

b)Wenn Gerät B und C miteinander nur über A verbunden sind, können dann Daten von B nach A übertragen werden?
Wenn nein, warum nicht?
Wenn ja, welche Schichten werden durchlaufen zur Übertragung einer vCard?

Schichten zur Übertragung einer vCard:

- OBEX
- RFCOMM
- L2CAP
- Baseband

bekommen wir vom chris!

Teil3: WLAN

29.Wo setzt man WLANs ein?

- Mobilität des Personals oder einzelner Mitarbeiter steigern
- Vorhandenes Netzwerk nachrüsten
- Netzwerk hinzufügen oder erweitern
- Mitarbeiter zu neuen Standorten hinzufügen, Mitarbeiter versetzen oder ändern
- Mitarbeiterproduktivität erhöhen
- Netzwerkleistung verbessern
- Betriebsabläufe ausweiten
- Vorhandene drahtlose Hardware und/oder Software aktualisieren
- In kostengünstiges Netzwerk investieren

30. Wo verwendet man IEEE 802.11 a, b, g?

Ein WLAN nach 802.11a ist unter folgenden Voraussetzungen geeignet:

- Erweiterter Durchsatz von bis zu 54 Mbit/s nötig
- Es werden Bandbreite und Geschwindigkeit für große Grafik-, Audio-, Daten- und Videodateien benötigt
- Jeder einzelne Access Point(Zugangspunkt) soll viele Benutzer haben, wie z.B. in einem Unternehmen.
- Störungen durch andere drahtlose Geräte sollen verringert werden

Ein WLAN nach 802.11b ist unter folgenden Voraussetzungen geeignet:

- Datenraten bis zu 11 Mbit/s reichen aus
- Reichweite im Gebäude ist wichtig
- Durchdringen von Wänden erforderlich
- Vorhandenes 802.11b-WLAN soll erweitert werden
- WLAN-Zugriff für Handheld-PCs erforderlich
- Geringe Anzahl an Benutzern pro Zugangspunkt

Ein WLAN nach 802.11g ist unter folgenden Voraussetzungen geeignet:

- Erweiterter Durchsatz von bis zu 54 Mbit/s nötig
  Ein 802.11b-Netzwerk ist bereits vorhanden
- Es werden Bandbreite und Geschwindigkeit für große Grafik-, Audio-, Daten-und Videodateien benötigt
- Geringe Anzahl an Benutzern pro Zugangspunkt
- Reichweite im Gebäude ist wichtig
- Durchdringen von Wänden erforderlich

31. Erklären Sie den Ad hoc- Modus!

Bei einem Ad-Hoc-Netzwerk (Peer-to-Peer-Netzwerk) handelt es sich um ein unabhängiges lokales Netzwerk, das nicht an eine verkabelte Infrastruktur angeschlossen ist, und bei dem alle Stationen direkt miteinander verbunden sind (man spricht dabei von einer Mesh-Topologie).

Die Konfiguration eines WLAN im Ad-Hoc-Moduswird bei der Errichtung eines Netzwerks verwendet, bei dem keine drahtlose Infrastruktur besteht oder bei dem bestimmte Dienste nicht benötigt werden (bspw. gemeinsamer Drucker), wie etwa bei einer Messe oder der Zusammenarbeit von Mitarbeitern an einem anderen Standort.

32. Erklären Sie den Infrastrukturmodus!

In einem Infrastrukturnetzwerk sind die WLAN-Clients über einen drahtlosen Zugangspunkt (Access-Point) mit dem Unternehmensnetzwerk verbunden, und sie verfahren dann so, wie es ein verkabelter Client tun würde.

Die meisten drahtlosen LANs in Unternehmen werden im Infrastrukturmodus betrieben; sie greifen für die Verbindung zu Druckern und Dateiservern auf das verkabelte Netzwerk zu.

33. Was ist WiFi?

WiFi steht für „Wireless Fidelity". - Das Wi-FiCERTIFIED* Logo stammt von der Wi-Fi Alliance. Das Wi-FiCERTIFIED Logo zeigt, dass das Produkt strengen Prüfungsanforderungen hinsichtlich der Interoperabilität genügt, so dass sichergestellt ist, dass Produkte unterschiedlicher Hersteller zusammen eingesetzt werden können.

34.Was sind die Schwierigkeiten bei der Planung eines WLAN-Netzes für ein größeres Gebäude?

Von den 14 zur Verfügung stehenden Kanälen überschneiden/überlagern sich nur 3 Kanäle nicht. – In großen Gebäuden besteht die Schwierigkeit also darin, die einzelnen Zellen so anzuordnen, dass es möglichst zu keinen Frequenzüberlagerungen kommt, sodass die einzelnen Frequenzbereiche einander nicht stören. (Die einzelnen Zellen müssen jeweils ein paar Kanäle Abstand zueinander haben!)

Bei der Planung eines WLAN-Netzes für ein größeres Gebäude stellt ebenfalls die Sicherheit einen wesentlichen Aspekt dar. – So empfiehlt es sich, bei Gebäuderändern keine Rundstrahler zu verwenden, da Informationen ansonsten in (firmenfremde) Bereiche gelangen können, für welche sie nicht bestimmt sind.

35. Roaming

- Netz soll homogen verfügbar sein
- auch während einer Bewegung des Teilnehmers

Funktionsweise:

- Mobile Station erkennt abnehmende Feldstärke
- Suche nach neuem Access Point
  Passive Scanning, Active Scanning mittels Frames
- Registrierung an geeignetem Access Point
- neuer Access Point gibt Netzwerk den Zellwechsel bekannt

Probleme dabei:

- vollständige Vernetzung durch Distribution-System
- keine unverbundenen Netzteile erlaubt
- mögliche Lösung mittels Mobile IP

36. Wie funktioniert DSSS? = Direct Sequence Spread Spectrum

- Bandspreizung nach CDMA-Verfahren (Code Division Multiple Access)
- bedingt bessere Bandbreitennutzung
- relativ störunempfindlich
- Jedes Bit wird vor seiner Übertragung mit einer 11-bit Baker Sequenz gespreizt.
- 802.11 sieht im ISM-Band 14 Kanäle vor

http://de.wikipedia.org/wiki/DSSS

37.Zugriff auf das Funkmedium

Mac Schicht regelt den Zugriff der Clients untereinander (ARP Tables) – das heißt wenn 2 oder mehrere Clients gleichzeitig an einen weiteren Client eine Message senden kann dieser die Nachricht nicht mehr lesen.

Darum gibt es 2 Möglichkeiten:

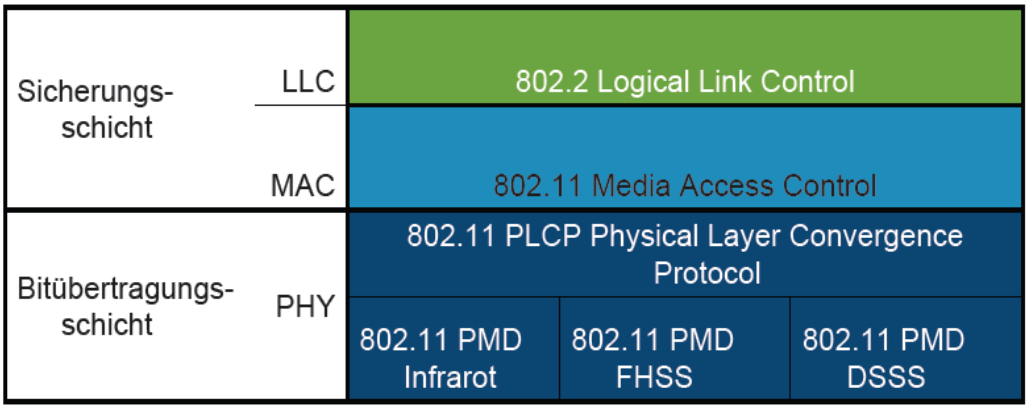
- Kollisionen weitgehend zu vermeiden
- Mechanismen die Kollisionen erkennen und nötige Schritte dafür einleiten

Stichwort: CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)
Hier werden Kollisionen vermieden. Client hört das Medium ab – findet eine Übertragung statt wartet er bis diese beendet wurde (und noch ein bißchen länger) und beginnt dann (soweit Medium frei) mit der Übertragung. Sollte eine andere Station schneller gewesen sein wartet beginnt der Vorgang von neuem solange bis der Client senden konnte (d.h. Backoff)

(Quelle: www.netlexikon.de):
Es wird dem Prinzip „Listen before talk" gefolgt, welches zwar Kollisionen nicht ausschließen, aber dennoch minimieren kann. - Hier der prinzipielle Ablauf dieses Vorgangs:

1. Zuerst wird das Medium abgehört ("Carrier Sense")
2. Ist das Medium für die Dauer eines IFS (InterFrame Spacing) frei, wird gesendet
3. Ist das Medium belegt, wird auf einen freien IFS gewartet und zur Kollisionsvermeidung zusätzlich um eine zufällige "Backoff-Zeit" verzögert
4. Wird das Medium während der Backoff-Zeit von einer anderen Station belegt, bleibt der Backoff-Timer so lange stehen und wird nach Freiwerden des Mediums weitergezählt

38.WLAN Protocol Stack



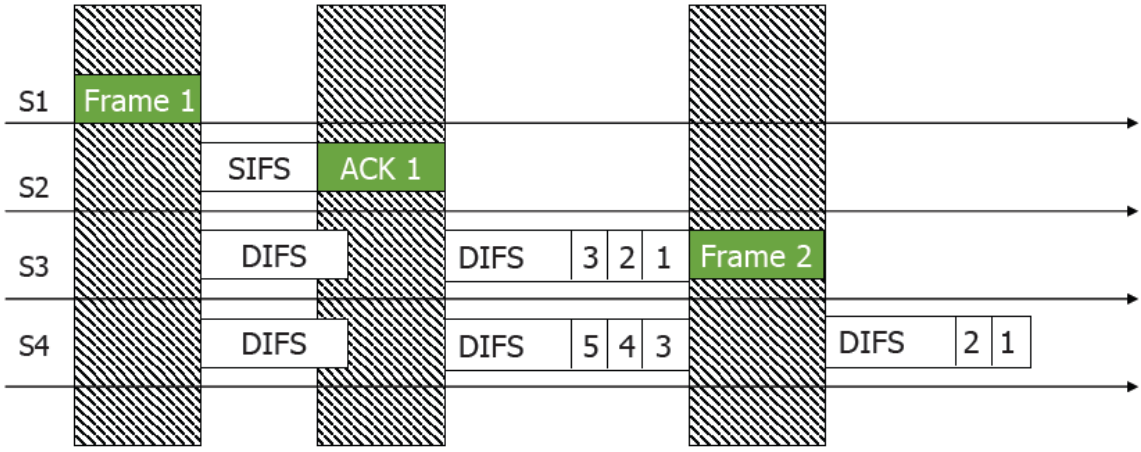
39. Was ist ein Interframe Space? Welche Arten gibt es?

Ein Interframe Space dient zur Zugriffsregelung auf das Medium. Je kürzer dieser Interframe Space ist, umso schneller versucht die Station das freie Medium zu belegen.

Es gibt 3 verschiedene Interframe Spaces welche, je kürzer diese sind, eine höhere Priorität des Clients repräsentieren.

*Die Kurzbe*zeichnung **IFS** steht für "InterFrame Spacing" (auch InterFrame Gap). Ein Mechanismus, der zur Realisierung von CSMA/CA verwendet wird.
Man unterscheidet

- SIFS (Short ~): Die Zeit, die vor dem Senden eines Bestätigungspaketen (ACKs), "Clear to Send"-Paketen (CTSs) oder einer Antwort auf Polling vergangen sein muss
- PIFS (Point Coordination Function ~): Die Zeit, die vor dem Senden von PCF Informationen durch den Access Point vergangen sein muss
- DIFS (Distributed Coordination Function ~): Die Zeit, die vor dem Senden eines normalen Datenpakets vergangen sein muss



40. In einem Adhoc-Netz befinden sich 3 Stationen S1, S2 und S3. S2 und S3 wollen beide jeweils einen Frame an S1 senden. Es wird CSMA/CA mit Bestätigung verwendet.
a) Zeichnen Sie ein entsprechendes Diagramm, bei dem S2 sofort sendet und S3 eine Zufallszahl 1 für die Wartezeit wählt.
b) Die erste Quittung von S1 an S2 wird durch einen Fehler nicht zugestellt. Verändern Sie das Diagramm entsprechend. S2 wählt dabei eine Zufallszahl 2 für die Wartezeit aus.

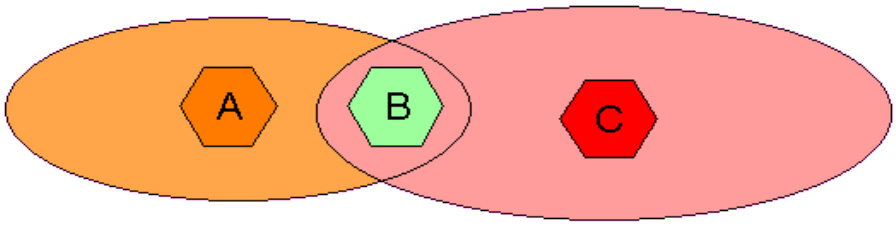
S1		***SIFS***	***ACK***			***SIFS***	***ACK***
S2	***Frame***						
S3		***DIFS***		***DIFS + 1***	***Frame***		

S 1		***SIFS***	***ACK (bad)***			***SIFS***	***AC K***			***SIF S***	***AC K***
S 2	***Fram e***			***DIFS + 2***		***DIF S***		***DIFS + 1***	***Fram e***		
S 3		***DIF S***		***DIFS + 1***	***Fram e***						

Je höher IFS - desto höher Priorität

41. Was ist das Hidden Terminal Problem?
a) Erklärung + Skizze
b) Was für zusätzliche Frames müssen eingeführt werden um das Problem zu beheben?
c) Was für einen Einfluß haben diese Frames auf die Belegung des Mediums?
d) Welchen Nachteil hat das Verfahren?

Sender A und C sehen sich nicht, Empfaenger B sieht beide:



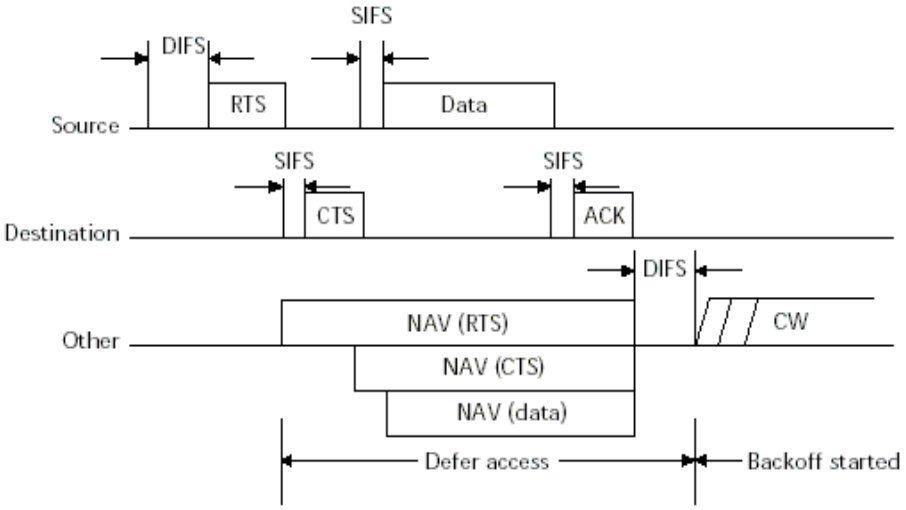
Problem:
So nun will A was schicken, keiner sendet was, also fängt er an. C will aber auch, bemerkt aber nicht, dass A gerade sendet (hockt ja hinterm Berg) Also schickt der auch los. Ende der Geschichte: B bekommt A+C auf einmal.

Lösung:
Austausch von **RTS-(Request to send) und CTS-(Clear to send) Rahmen**, da auch der Empfaenger (hier ja B) sein CTS schickt, sieht auch A dass da gleich was abgeht und er nicht schicken soll.

Zur Behebung des Hidden-Terminal-Problems:

Also wenn A etwas an B senden will schickt jener sobald er meint das Medium ist frei und er darf senden ein RTS Package zu B. Dieser Antwortert innerhalb des SIFS mit einem CTS. Dieses CTS Package hört auch C und weiß somit das er nicht senden darf. Danach startet der eigentlicht Datentransfer zw. A & B welcher mit einem ACK beendet wird. Sobald C merkt, dass das Medium frei ist lässt er sein DIFS & Contention Window ablaufen und sendet dann sein RTS Package.

Das Verfahren erzeugt zusätzlichen Verwaltungsaufwand. Dadurch sinkt der Nutzdaten-Durchsatz.
Damit die Belegung des Mediums für einen bestimmten Zeitraum erfolgt, enthalten RTS und CTS ein Feld, das eine Wartezeit für alle anderen Stationen vorgibt: Net Allocation Vector. Erst nach NAV bewerben sich die anderen Stationen wieder.



42.Wie behebt man das Hidden Terminal Problem? Erklärung

siehe oben, Frage 41

43.Prinzip PCF-Verfahren

= Point Coordination Function

Wird dann verwendet wenn man das Chaos auf normalen Medien verhindern will und den einzelnen Clients eine minimale Bandbreite und eine maximale Antwortzeit garantieren will/muss. (wichtig bei zeitkritischen abläufen)

Vorgang:

Voraussetzung für den Einsatz dieses Verfahrens ist vorerst ein Coordinator, auch Point Coordination Station genannt und dies ist so gut wie immer ein Access Point.

Zweite Voraussetzung um ein PCF zu initieren ist, dass das Medium frei ist.

Treffen diese beiden Dinge zu dann sendet die PCS ein Coordination Frame welches den Start des PCF Verfahrens einleitet (CFStart). Danach erhalten alle einen NAV***(!? Kürzel?)*** und warten bis sie von der PCS "angesprochen" werden. Die PCS geht nun jede Station durch und fragt dort an (POLL) erhält das Frame und die Station geht wieder in den "wait" Modus. So geht die PCS jede Station in ihrer Reichweite durch. Nachdem sie alle Station abgeklappert hat sendet sie wieder ein Coordination Frame welches besagt, dass das PCF abgeschlossen ist (CFEnd). Nun herscht wieder das koordinierte Chaos auf dem Medium.

44.Was für Probleme gibt es bei VoWLAN?

- Einigung auf den verwendeten Standard (a, b, g ...)
- Gute Planung der WLAN Zellen (ähnlich GSM oder UMTS), dadurch muss Handover funktioneren und das auch über verschiedene Kanäle
- Abdeckung, Reichweite vs Durchsatz
- Störungen am Funkkanal durch ander Geräte (Mikrowellen usw)
- Verwendetes Protokoll (TCP, UDP oder proprietäres) und Komprimierung – dies ist wichtig für den Bandbreitenbedarf
- Geräte die Zeitverzögerungen erzeugen – dies wirkt sich unangenehm für den telefonierenden Menschen aus

Teil4: WMAN, WiMax

45.Was gibt es für globale, drahtlose Standards? Klassifizieren Sie diese.

WPAN -> 9 Meter (30 feet) -> 110 – 480 Mbps
- UWB

WLAN –> 90 Meter (300 feet) -> 11 – 54 Mbps
- Wi-Fi

WMAN / Mobile WMAN -> 1,6 – 9,6 km (1 – 6 miles) -> 30 – 75 Mbps
- WiMax

WWAN -> 1,6 – 8 km (1 – 5 miles) -> 348 Kbps – 2,4 Mbps
- WCDMA / UMTS
- CDMA2000
- Edge

46.Welche Anwendungen gibt es für WMAN?

- Wireless MAN dient dem drahtlosen Breitband-Zugang ergänzend zu Kabel, DSL und Standleitungs-Diensten
- Extra für Außenanwendung, große Reichweiten und "Carrier Class"- Anwendungen entwickelt.
- hoher Durchsatz, skalierbar bis 1000 Teilnehmer, Dienstgüte, Mikrowellen (keine Sichtverbindung notwendig)
- für lizenziertes und lizenzfreie Funkspektren
- breiter Markt: von Ballungsräumen bis zu ländlichen Gebieten, wo es schlechte Verkabelung gibt
- Breitband über Hotspots hinaus

47.Was unterscheidet stationären, nomadischen und mobilen „ Broadband Wireless Access"?

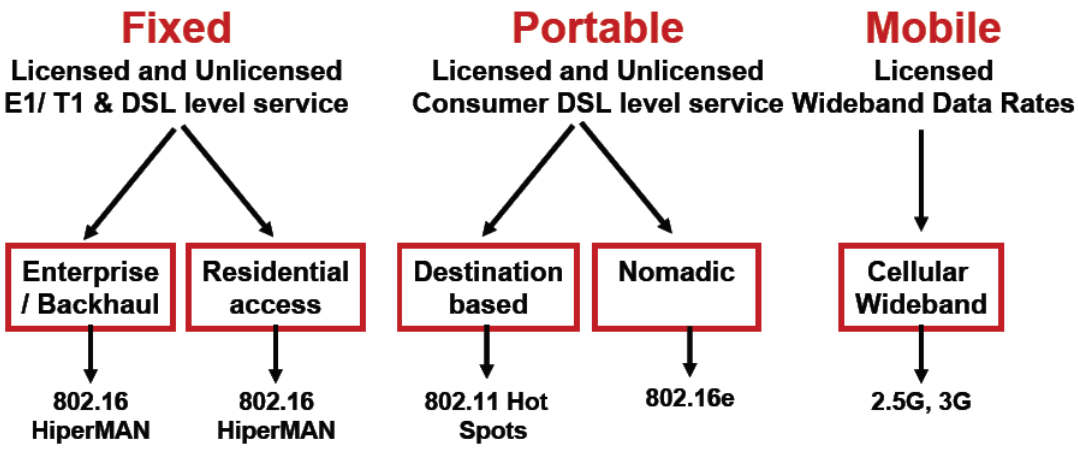
Wireless Platforms

Stationär:
Fixed Wireless ist ein "high-speed symmetrical service", das wie der Name schon sagt nur innerhalb einer bestimmten Reichweite vom Sender aus funktioniert, das heißt man ist an seinen Platz gebunden, wenn man Broadband Access haben will

Portable/Nomadic:
Der Service, der dem wireless subscriber Portability liefert. Das wird durch ein portables HandSet erreicht, das leicht in Taschen etc. getragen werden kann, wenn sich der Subscriber von einem Ort zum anderen bewegt.

Ein Portabler Zugang kann (ca. innerhalb eines 3-12 Meilen Radius) solange verwendet werden, bis kein Signal mehr von ihm erreicht wird (kann auch an den nächsten Zugang weitergeleitet werden, wenn vorhanden - auch zwischen Städten, etc.. solange, das Service dort aktiviert ist)

Mobile:
It's a ad hoc peer-to-peer technology enables first responders to instantly self-deploy a broadband communications network just by turning on their radios - no towers or infrastructure is needed.
Public Safety and Emergency Response Personnel, Fire, Police and EMS professionals usually use it.



48. Was bedeutet Line of Sight und Non Line of Sight?

LOS…Line of Sight
NLOS…Non Line of Sight

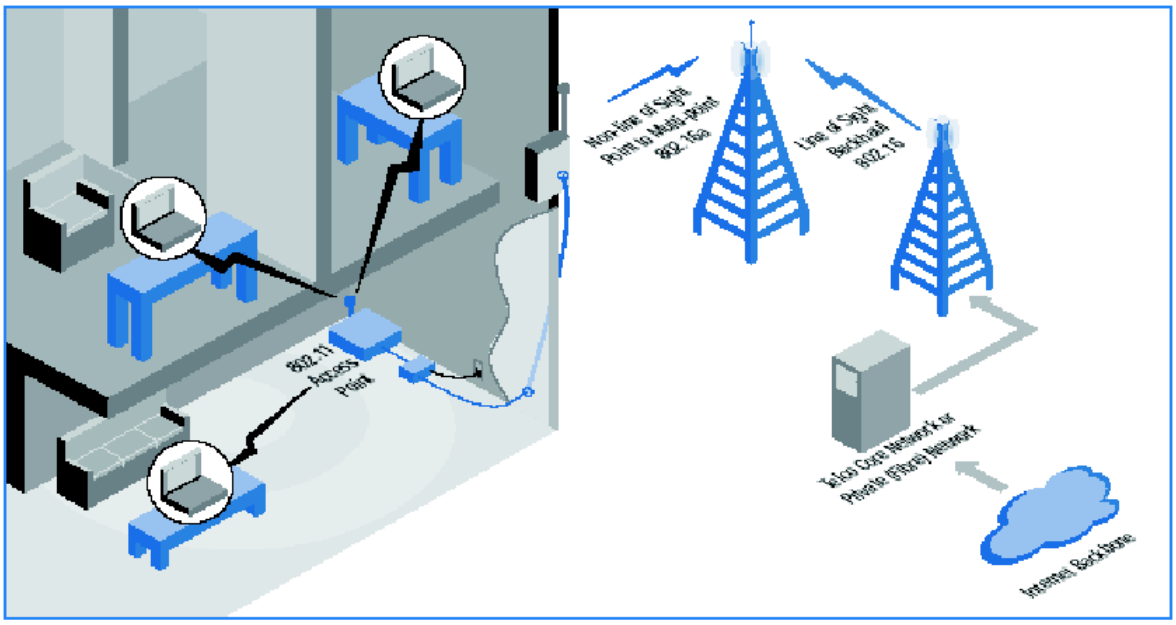
49.Wo liegen die Haupteinsatzbereiche von WiMax?

- **Datentransport**:
  - Verbindung von Mobilfunkbasisstationen
  - Anbindung von Hotspots
- **Broadband on Demand**
  - T1/E1 für Geschäftskunden
  - Für Events, Messen etc.
- **Privatkunden**
  - Ergänzung zu Kabel und DSL (< 4km)
- **Gebiete ohne Breitbandzugang**
  - Ländliche Gebiete
- **Breitband abseits von Hotspots**

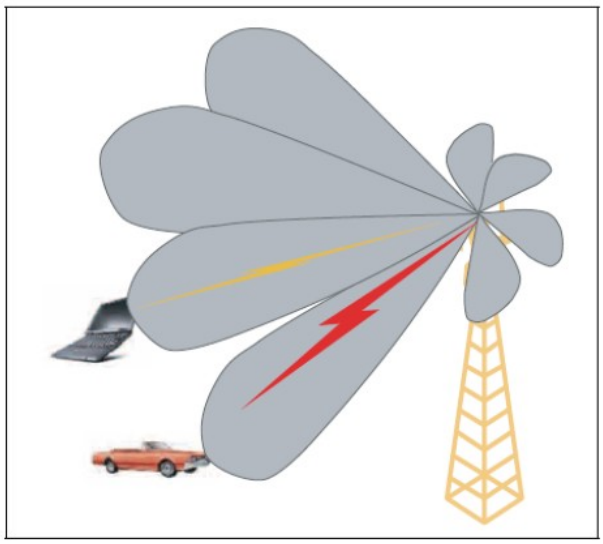
50.Welche Vorteile bietet 802.16?

- **Hoher Datendurchsatz bei großen Reichweiten (bis zu 50 km)**
  - Mehr bps/Hz bei höheren Reichweiten
- **Skalierbare Systemkapazität**
  - Einfaches Hinzufügen neuer Kanäle zur Maximierung der Kapazität einer Zelle
  - Flexible Kanalbandbreiten ermöglichen Band-Allokationen sowohl für das lizenzierte als auch lizenzfreie Spektrum
- **Funkbereichsabdeckung**
  - Standardbasierende Technologien (Mesh-Netzwerke, aktive Antennen, MIMO) um Performance bei fehlender Sichtverbindung zu verbessern
- **Dienstgüte/QoS**
  - Verbindungsorientierter MAC unterstützt Sprache und Video
  - Unterscheidung der Dienstgüte in Klassen:
  - E1/T1 für Business
  - „best effort" für Konsummarkt
- **Investitionsrisiko**
  - WiMAX zertifiziertes, interoperables Equipment reduziert Risiko für Betreiber
  - Betriebskosten können bei erprobten, standardisiertem Equipment stark reduziert werden

51.Architektur-Zeichnung von WiMax, Definitionen.



52. Was sind intelligente Antennen?



WiMax wird intelligente Antennen unterstützen.

Antennen können gerichtet und nachgeführt werden ohne mechanische Veränderung der Antenne

53.Welche Reichweiten und welche Bitraten lassen sich maximal mit 802.16 erzielen?

Reichweiten: ein paar Häuserblöcke
Bitraten: bis 75 mbps

54.Welches Frequenzspektrum wird verwendet?

10 – 66 Ghz

55.Welche Modulation verwendet 802.16 in der Bitübertragungsschicht?

- Gray coded single carrier QAM
  - QPSK
  - 16QAM
    - Verpflichtend für Downlink, optional für Uplink
  - 64QAM
    - Verpflichtend für Downlink und Uplink

Teil5: SIP

56.Grundzüge von SIP.

Das ***Session Initiation Protocol (SIP)*** ist ein IETF standardisiertes Protokoll zur einfachen Einleitung, Verwaltung und Koordination von Multimedia-Sitzungen über das Internet (IP -Telefonie, Video-Konferenz, Telelearning). Die Geschichte des SIP seit 1996 ist eng verbunden mit dem *Multicast Backbone (MBone)*, einem Netz zur Verteilung von Audio- und Videoströmen und für Mehrpunktkonferenzen, das auf dem Internet aufsetzt. Schnell zeigte sich, dass mit S IP nicht nur MBone-Sessions signalisiert werden konnten, sondern SIP auch für VolP genutzt werden konnte, um Anwender „anzurufen". Die Internet Engineering Task Force (IETF) standardisierte SIP schließlich im März 1999 unter dem RFC2543. Dieser wurde im Juni 2002 durch den RFC 3261 aktualisiert. Das *Session Initiation Protocol* (SIP) RFC3261 ist ein Signalisierungs-Kontroll-Protokoll der Applikationsschicht, mit dem Multimedia-Sitzungen eingerichtet, unterhalten und beendet werden können. Das *Session Description Protocol (SDP)* RFC2327 ist für die Beschreibung und den Austausch von Merkmalen von Multimediaverbindungen vorgesehen.

57.Welche Dienste kann man mit SIP realisieren?

- **User location**: Ermitteln des Endgerätes für die gewünschte Kommunikation
  - Büro, Heim, unterwegs
- **Callset-up**: Läuten und Übertragen der Ruf-Parameter für Anrufer und Angerufenen
- **User availability**: Bestimmung der Erreichbarkeit des Kommunikationspartners
  - Callstate: ready, on anothercall
  - Willingness: beschäftigt, in Besprechung
- **User capabilites**: Ermitteln des Mediums und dessen Konfiguration
  - Text, Video, Sprache oder eMail
  - Ermitteln der verfügbaren Teilnehmer
- **Instantmessaging**
  - text chat, voicechat

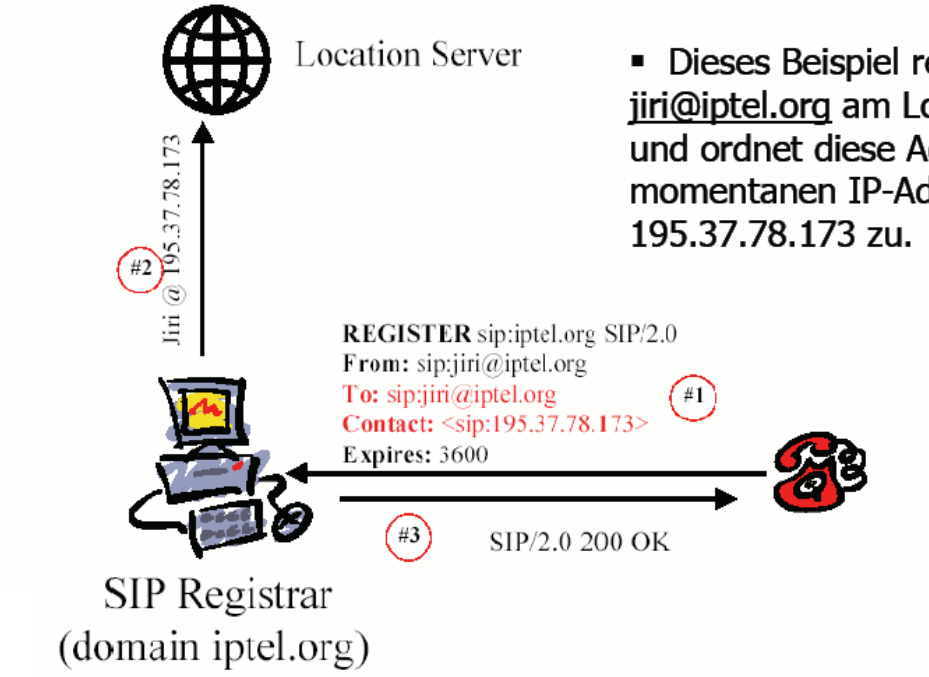
58. SIP-Adressierung

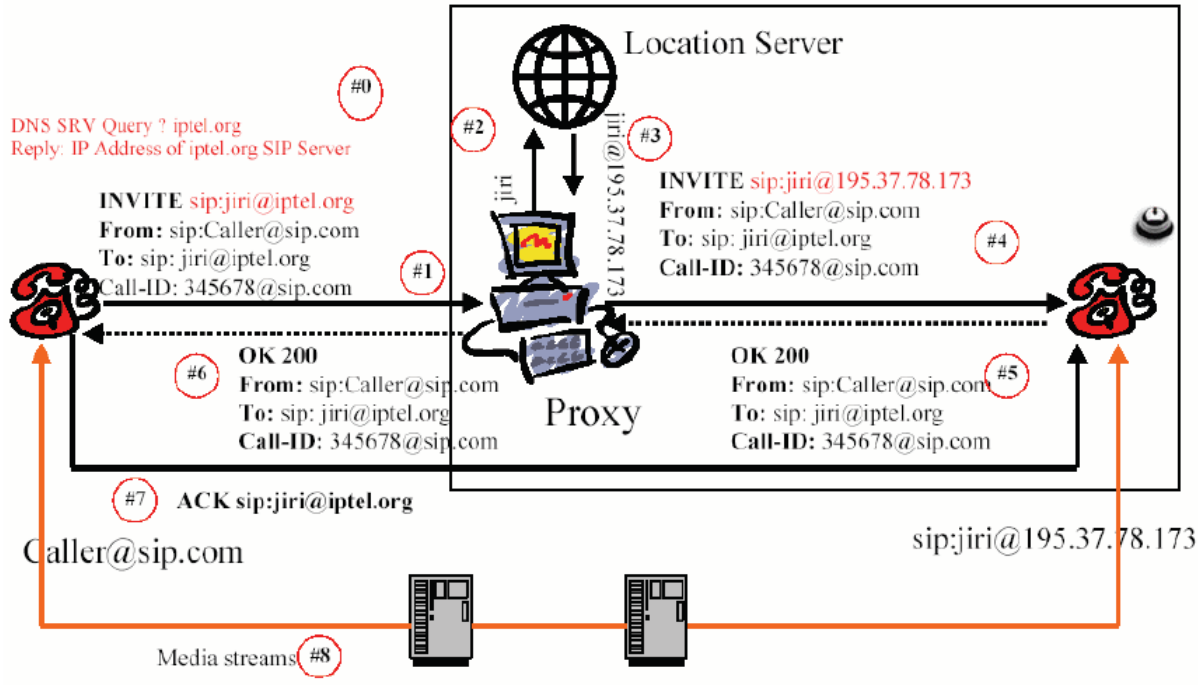
- SIP Adressen sind global erreichbar
- Adresse muss Host enthalten
- Adresse kann Usernamen, Port-Nr., Parameter enthalten
- Adresse kann in Web-Seiten, emails ... eingebunden werden
- der Adressraum ist unbegrenzt

Format von URLs wird verwendet:
sip:hans@muster.org
sip:voicemail@muster.org?subject=callmesip:sales@hotel.xy; geo.position:=48.54_-123..84_120
Adresse ist äquivalent zu nicht-SIP-URLs wie mailto:, http:, ...

59. Wie läuft ein Verbindungsaufbau mit SIP typischerweise ab?

Zuerst muss ein Teilnehmer registriert werden, dann kann eine Verbindung aufgebaut werden, dann erfolgt ein Verbindungsaufbau über einen Proxy:





Generell: Registrar, Proxy und Redirect Server sind unabhängige Komponenten und können alle auf demselben Rechner implementiert sein.

In diesem Beispiel möchte Caller (sip:Caller@sip.com) eine SIP Verbindung mit Jiri (sip:jiri@iptel.org) aufbauen.

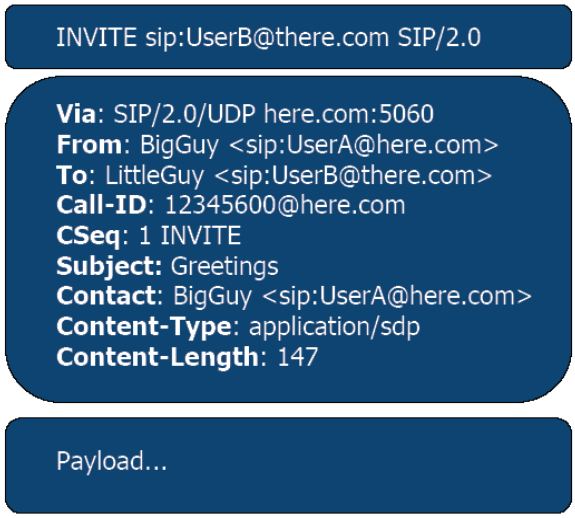
1. *Caller sendet eine INVITE Nachricht für Jiri an den SIP Proxy*
2. *Der Proxy leitet die Nachricht weiter and den Location Server*
3. *Er erhält als Antwort, dass Jiri unter der Adresse sip:jiri@195.37.78.173 erreichbar ist*
4. *Der Proxy sendet jetzt die INVITE Nachricht an sip:jiri@195.37.78.173.*
5. *Die INVITE Nachricht kommt bei Jiri an und er schickt ein OK 200 zurück an den Proxy*
6. *Dieser schickt die OK 200 Meldung an Caller*
7. *Die Nutzverbindung für die Daten wird direkt zwischen den beiden User-Agents mit einem ACK von Caller an Jiri aufgebaut.*
8. *Die Media-Streams können übertragen werden*

60. SIP – Request

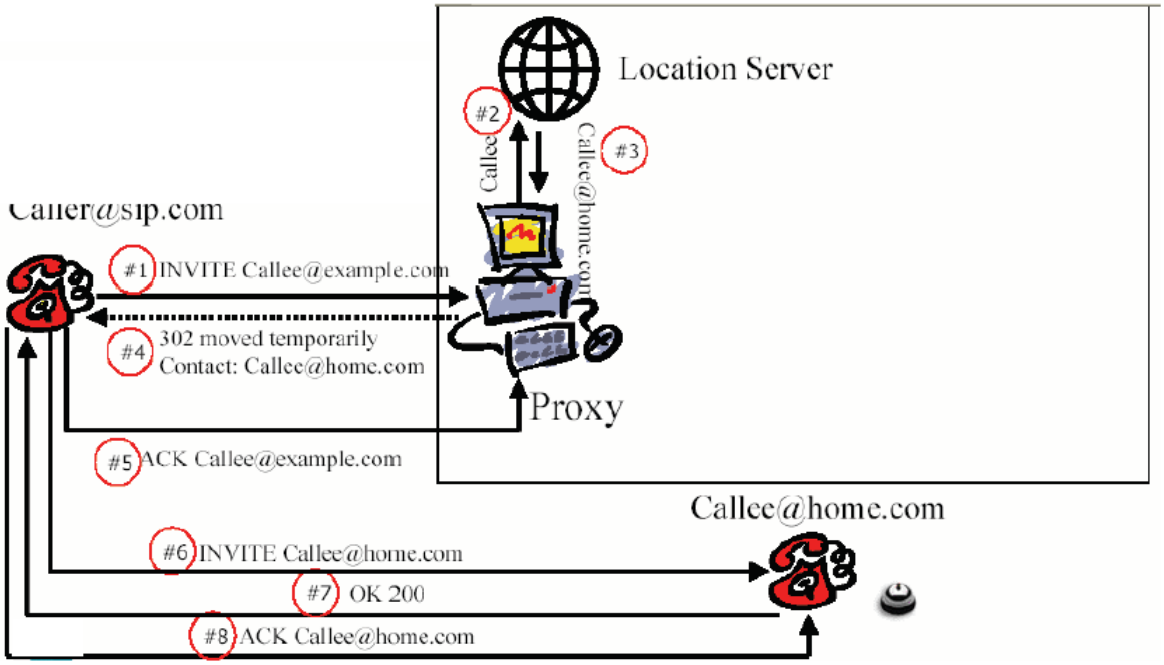
SIP-Requests(„Methods")

- INVITE öffnet Verbindungen („media sessions")
- ACK bestätigt Verbindungsaufbau (immer gemeinsam mit INVITE)
- BYE beendet Verbindungen
- CANCEL löscht anstehendes INVITE
- OPTIONS fragt nach vorhandenen Optionen
- REGISTER verknüpft permanente Adresse mit dzt. Ort im Netzwerk

Bsp.: **MessageStructure: RequestMethod (INVITE-Request)**



61. SIP-Redirect Modus



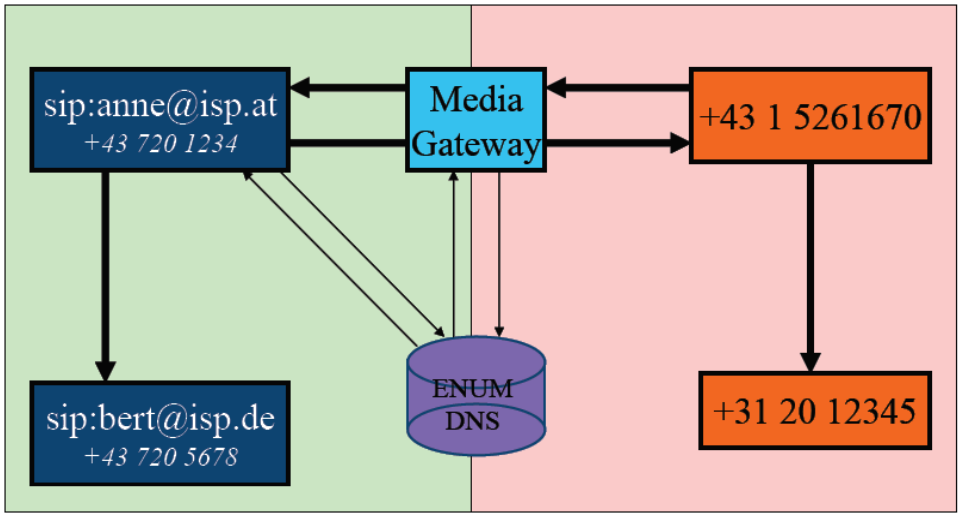
1. *Caller sendet eine INVITE Nachricht für Calle an den SIP Proxy*
2. *Der Proxy leitet die Nachricht weiter an den Location Server*
3. *Da Callee nicht mehr beim Registrar example.com, sondern bei home.com*
4. *angemeldet ist, sendet dieser ein sogenanntes „Redirect" als Antwort, welches besagt, dass Callee jetzt unter der Adresse sip:Callee@home.com erreichbar ist*
5. *Der Proxy sendet jetzt eine 302 removed temporarily Nachricht an Caller*
6. *Caller sendet daraufhin eine ACKnoledge Nachricht an den Proxy*
7. *Caller sendet nun ein INVITE an Calle@home.com*
8. *Die SIP Antwort 200 OK wird an Caller gesendet*
9. *Ein ACK kommt von Caller an Callee zurück*

62.Wie wird der Übergang vom Internet ins Telefonnetz mit sip realisiert?

Durch Enum
*t**E**lephone **NU**mber **M**apping* ist eine Anwendung des Domain Name Systems zur Übersetzung von Telefonnummern in Internet-Adressen

seine Folien:

- Abbildung Telefonnummer ->URI nötig
- Domains bilden Namen auf IP-Adressen ab
- ENUM bildet Telefonnummern auf URI's ab und zwar mit genau diesem DNS
- eine ENUM Eintrag wäre zB
- +43 664 4213465 -> sip:mah@nic.at43.at



63.a) Nennen Sie 5 der wichtigsten SIP-Befehle, die bei einem SIP-Verbindungsaufbau vorkommen.
b) Geben Sie eine gültige SIP-Adresse an

- INVITE öffnet Verbindungen („media sessions“)
- ACK bestätigt Verbindungsaufbau (immer gemeinsam mit INVITE)
- BYE beendet Verbindungen
- CANCEL löscht anstehendes INVITE
- OPTIONS fragt nach vorhandenen Optionen
- REGISTER verknüpft permanente Adresse mit dzt. Ort im Netzwerk
- Der SIP-RequestCOMET (extendedmethod) zeigt Erfüllung bzw. nicht-Erfüllung an.

Sip:MobCom@test.net

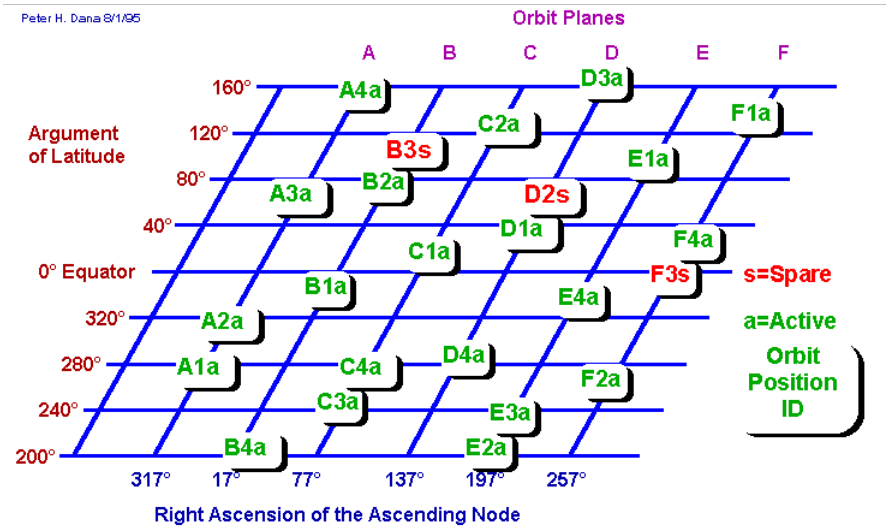
Teil6: Satellitennavigation, GPS

64. Was sind Orbitalebenen und wie sind sie bei GPS angeordnet?

Orbitalebene:
Eine imaginäre, riesige Fläche, die von der Umlaufbahn eines Erdsatelliten beschrieben wird. Sie reicht durch den Erdmittelpunkt.
Die 24 GPS-Satelliten sind in *sechs Orbitalebenen*, den sogenannten ‚Abstandskäfigen' angeordnet. Jede Orbitalebene enthält vier Satelliten. Die Bahnen sind so gelegt, dass von jedem Punkt der Erde zu jeder beliebigen Zeit mindestens vier Satelliten gleichzeitig sichtbar sind. Dies ist die Mindestanzahl die ein terrestrischer Empfänger benötigt, um eine dreidimensionale Ortsbestimmung ausführen zu können.

Seine Folien:

- Es gibt 6 Orbitalebenen mit normalerweise je 4 Satelliten
  - im Abstand von 60°
  - Neigung 55° gegen die Äquatorebene
  - Das ergibt 5-8 sichtbare Satelliten von jedem Punkt der Erdoberfläche aus.



Simplified Representation of Nominal GPS Constellation

65. GPS-Dienste

- Navigationsdienste
- Vermessungswesen
- Geodätische Kursbestimmung
- Astromomie
- Studien zur Plattentektonik
- Telekommunikation
- Forschung
- Messungen in der Atmosphäre

66.Wodurch werden die Messergebnisse bei GPS verfälscht?

- Signal- und Phasenverschiebungen in der Ionosphäre und Troposphäre: Das Signal verlangsamt sich beim Durchgang durch die Atmosphäre
- Signalstreuung, Reflexionen: treten durch Gebäude, Felsen usw. auf. Die Signallaufzeit wird erhöht und Fehler entstehen.
- Fehler beim Empfängertakt: Der Empfängertakt ist nicht so stabil wie der Sendertakt im Satelliten (Atomuhr) > Zeitfehler
- Ephemeriden-Fehler: Ungenauigkeiten in der übermittelten Position des Satelliten gegenüber der tatsächlichen Position.
- Anzahl sichtbarer Satelliten: Hindernisse können die Sichtbarkeit der Satelliten beeinflussen > weniger Positionsdaten zur Verfügung
- Geometrische ungünstige Satelliten-Positionen: sehr spitze/stumpfe Winkel entstehen > Abschattung von Satelliten
- Gezielte Signalbeeinträchtigung: oft werden hochgenau Daten aus militärischen Gründen gezielt verschlechtert.

67.Satelliten-Signale, Modulation?

2 Trägersignale:

- L1 (1575,42 MHz), für Navigation-Message und SPS-Signale
- L2 (1227,60 MHz), für Messung der ionosphärischen Delays durch PPS-fähige Empfänger

Modulation (durch binäre Datenströme):

- C/A-Code (Coarse/Acquistion): L1 wird moduliert, C/A-Code = Pseudozufallsfolgen mit Wiederholfrequenz von 1 MHz, jeder Satellit erhält eigene Pseudozufallsfolge > Identifikation anhand dieser möglich, Verwendung bei SPS
- P-Code (Precise): L1 und L2 werden moduliert, P-Code = sehr lange Pseudozufallsfolge, hat eine Periode von 7 Tagen, kann verschlüsselt werden
- Y-Code: = verschlüsselter P-Code, Basis für PPS
- Navigation Message: moduliert L1 und L2, enthält Positionsdaten, Taktkorrekturdaten, …

68.Grundprinzip DGPS

- Grundidee: Fehler eines unbekannten Ortes mit den berechneten Fehlern eines bekannten Ortes zu korrigieren.
- Korrekturwerte werden von einem Referenzempfänger aus der Differenz der Daten des tatsächlichen Ortes mit den empfangenen Ortsdaten ermittelt.
- Der Referenzempfänger muss alle sichtbaren Satelliten mitverfolgen.
- Referenzempfänger misst Pseudoentfernung (exakte Entfernung + Messfehler + Abweichung Lokalzeit/Systemzeit) zu jedem Satelliten > Referenzempfänger sendet

Benutzer für jeden Satelliten den Korrekturwert > Benutzer ermittelt seine Pseudoentfernung und zieht den Korrekturwert ab

69.GPS-Fehlerquellen

- SV (space vehicle) Clock
- SV Ephemeries
- Selective Availability
- Troposphere
- Ionosphere
- Pseudo-Range Noise
- Receiver Noise
- Multipath
- RMS Error

70.Erklären Sie WAAS?

Wide Area Augmentation System
Referenzempfänger misst Pseudoentfernung zu jedem Satelliten > Übermittlung der Korrekturdaten zur Masterstation > Übermittlung der Korrekturdaten zu einem geostationären Satelliten (Immarsat 3) > Benutzer ermittelt seine Pseudoentfernung und zieht Korrekturwerte (die er vom geostationären Satelliten erhält) ab.

71.Worin unterscheidet sich WAAS von DGPS?

Benutzer erhält die Korrekturwerte nicht direkt von Referenzempfänger sondern von einem geostationären Satelliten (Immarsat 3).

72.Beispiel Positionsbestimmung:

Ein Fahrzeug möchte seine Geschwindigkeit ermitteln. Das Positionsbestimmungsverfahren erlaubt keine direkte Geschwindigkeitsmessung. Daher werden 2 Positionsmessungen im Abstand von 3s durchgeführt.
a) Berechnen Sie die aktuelle Geschwindigkeit, wenn 2 Positionen p1=(0, 0) und p2=(108m, 108m) gemessen wurden. Kartesisches Koordinatensystem mit 0-Punkt in p1, Höhe nicht berücksichtigt.
b) Das Verfahren hat eine Genauigkeit von 30m. Geben Sie das Intervall der möglichen Geschwindigkeiten an, die zu den Messungen p1 und p2 führen könnten.
c) Durch welchen Umstand könnte trotz einer hohen Ungenauigkeit trotzdem eine relativ genaue Geschwindigkeitsmessung möglich sein?

Bem.: Es kommen keine Beispiele, bei denen Gleichungssysteme gelöst werden müssen.

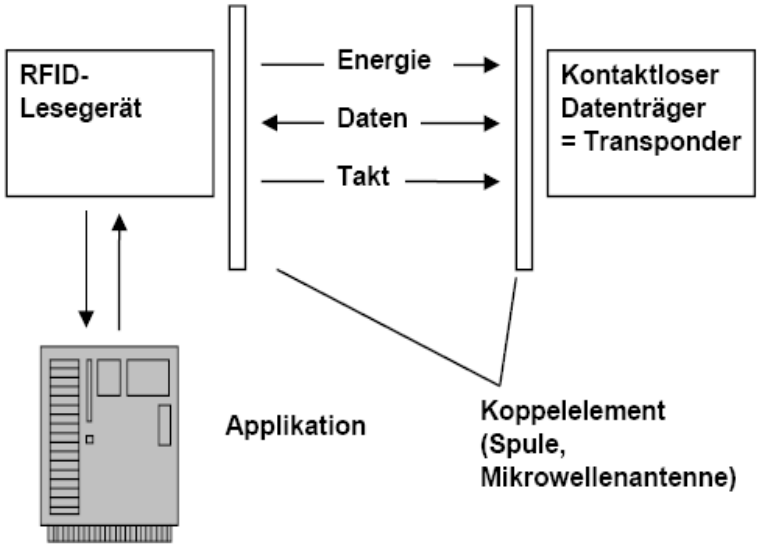
- 183,29 km/h
- 81,46 km/h – 285, 11 km/h
- ???

73.Erklären Sie RFID

= Radio Frequency Identification
- Dient zur automatischen, drahtlosen Identifikation von Objekten
- Kontaktlose Kommunikation über elektromagnetische Wellen
- Gehört zu den Auto-ID Systemen
- Anwendung zb.: Lager/Logistik, Fahrzeugidentifikationen (Schranken), Autodiebstahlsicherung, Zugangssysteme, Eintrittskarten, Mautsysteme, Ski-Pass, Sport, Post-Dienste, Bibliotheken, …

- Vorteile: kontaktlose Übertragung, größere Datenmengen speicherbar, geringere Empfindlichkeit (Nässe, Verschmutzung, Verschleiß), hohe Auslesegschwindigkeit (ca. 500 Tags/Sec), reduzierte Fehleranfälligkeit, keine Sichtverbindung notwendig, gleichzeitiges Lesen und Schreiben von vielen Etiketten möglich
- Nachteile: große Abhängigkeiten von äußeren Einflüssen (Metall, Umwelteinflüsse), Daten für Menschen nicht ohne Hilfsmittel erfassbar

Aufbau:

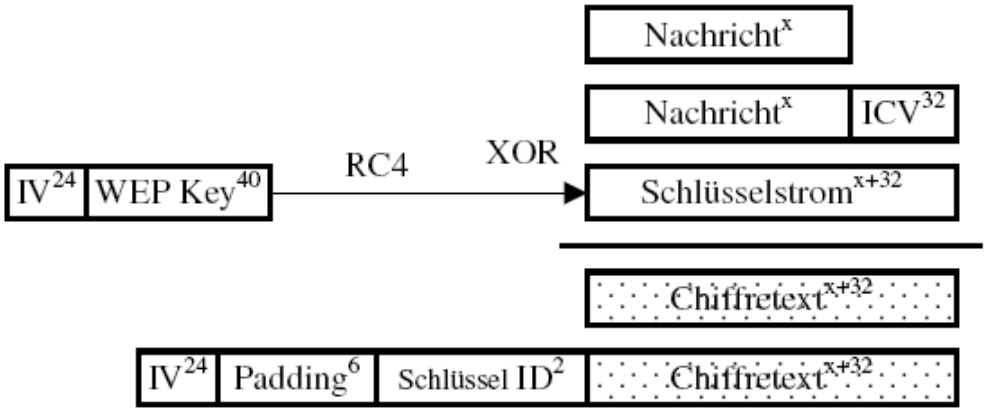


74.WEP Ver-/Entschlüsselung

= Wired Equivalent Privacy

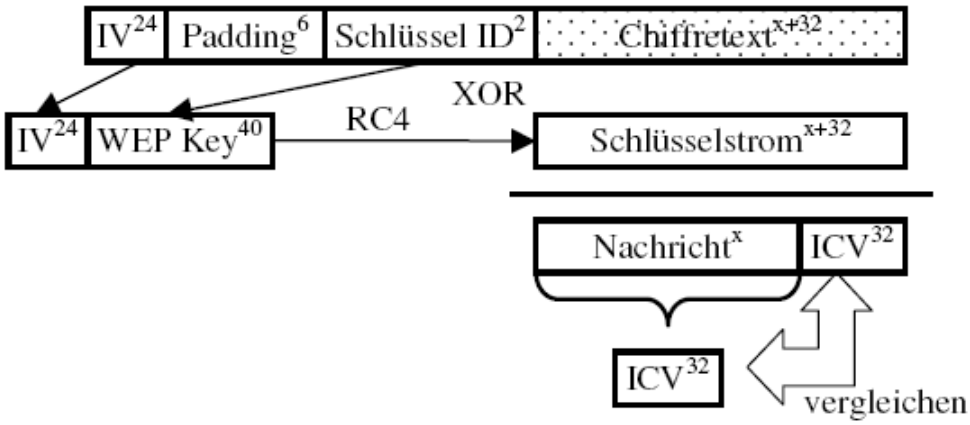
Ziele:
Vertraulichkeit, Zugangskontrolle, Datenintegrität

Verschlüsselung:
Zuerst wird über die eigentliche Nachricht M, mittels CRC-32 c(), der 32 Bit lange ICV gebildet und an die Nachricht angehängt. So entsteht der zu verschlüsselnde Klartext P = _M|c(M)_. Danach wird zufällig ein IV v gewählt. An v wird der geheime Schlüssel k angehängt. Aus diesem String wird dann mit der Stromchiffre RC4 ein Schlüsselstrom RC4(v,k) erzeugt. Als nächstes wird der zu verschlüsselnde Klartext mit dem Schlüsselstrom zum Chiffretext C XORed C = P Å RC4(v,k). Diesem Chiffretext werden noch der IV, ein 6 Bit Padding pad und die Schlüs[illegible] ch als IV-Feld bezei



Auffüllen der restlichen 6 Bit der Schlüssel ID zu einem Byte. Durch hintereinander Hängen der einzelnen Teile ergibt sich der über das Netzwerk zu übermittelnde Text S = v|pad|id|C.

Entschlüsselung:
Der Empfänger kann mit Hilfe des IV und der Schlüssel ID die Verschlüsselung rückgängig machen. Mit der Schlüssel ID kann er aus den vier möglichen geheimen Schlüsseln, den zu verwendenden Schlüssel bestimmen. Zusammen mit dem IV kann er den Schlüsselstrom berechnen.
C Å RC4(v,k)
= [P Å RC4(v,k)] Å RC4(v,k)
= P Å [RC4(v,k) Å RC4(v,k)]
= P
Dann berechnet der Empfänger die CRC-32 Prüfsumme für die erhaltene Nachricht und vergleicht diese mit der angehängten Prüfsumme. Nur wenn die berechnete Prüfsumme mit der angehängten Prüfsumme übereinstimmt wird das Paket akzeptiert.



WEP ist die Abkürzung für Wired Equivalent Privacy und bezeichnet den Algorithmus, nach welchem die zu übertragende Datenpakete verschlüsselt werden, falls diese Option aktiviert wurde.
Dabei wird das Datenpaket, wie in der Abbildung zu sehen, dergestalt verändert, dass die Bestandteile Data und CRC mit einer Pseudozufallszahl durch xor verknüpft werden und zusätzlich ein IV, der zur Generierung der Zufallszahl verwendet wurde, im Klartext übertragen wird.

Ziele:
- Vertraulichkeit
- Zugangskontrolle
- Datenintegrität

RC4 Algorithmus siehe Dokument „seminar_mobsec"!

75. Welche Sicherheitslücken gibt es bei WEP?

- Open System Authentification ist leider Standardeinstellung. (Jeder Station wird ohne Passwortabfrage Zugang gewährt)
- 40 Bit WEP-Schlüssel ist zu klein.
- IV-Raum ist zu klein und wiederholt sich nach einigen Stunden.
- Wenn ein Klartext bekannt ist, kann der dazugehörige Schlüsselstrom durch XOR ermittelt werden. Damit sind verschlüsselte Texte, die den gleichen IV verwenden, entschlüsselbar!
- CRC-32-Prüfsumme ist linear und leicht berechenbar, daher für Angreifer bei Kenntnis des IVs und der Pseudozufallsfolge nachvollziehbar.

76. Lösungsansätze dazu

- Kurze Nutzungszeiten und automatisches Schlüsselmanagement (Jedoch Interoperabilitätsprobleme)
- Sicherheit in höheren Schichten nutzen: Firewalls, SSH, SSL, VPN nutzen.
- *Counter Mode CBC-MAC* (CCMP)
    - AES (Advanced Encryption Standard) als Verschlüsselung
    - *Cipher Block Chaining Message Authentication Code* (CBC-MAC) zur Integritätssicherung

Standardisierte Verbesserungen:

- Temporal Key Integrity Protocol (TKIP)
- Weitgehende Nutzung vorhandener HW
- IV auf 48 Bit erweitert
- Message Integrity Check (MIC) mit 64-Bit-Schlüssel
- Sequenznummer gegen Replay (48 Bit)
- Verschlüsseln mit „Per Packet" Schlüssel (Aus Basisschlüssel, Sequenznummer, MAC-Adresse ...)

77. Angriff auf WLAN – Anmeldung ohne Schlüssel

Man benötigt einen erfolgreichen Anmeldeversuch eines anderen Teilnehmers, da man damit sowohl die vom Access Point gelieferte Challenge als auch die benötigte Antwort der teilnehmenden Station erhält.
Außerdem erhält man durch dieses Paar (verschlüsselter Text, unverschlüsselter Text) und das Lösen der Gleichung C = P xor RC4(IV,K):

RC4(IV,K) = C xor P

eine 128 Bytes lange PRGA Ausgabe, deren zugehöriger IV ja sowieso bereits als Klartext vorliegt. Somit haben wir unter mehrfacher Verwendung desselben IVs die passende RC4 Ausgabe, um WEP Pakete mit 128 Bytes an Daten zu versenden, ohne damit irgendwelche Aufmerksamkeit zu erregen.

78. Angriff auf WLAN – Wiederholung des bereits verwendeten IV

Mehrfache Verwendung von IVs bedeutet gleichzeitig auch mehrfache Verwendung derselben Zufallsfolge. Sei im Folgenden die Pseudozufallsfolge PZF = RC4(IV,K). Die Verschlüsselung zweier Nachrichten P1 und P2 bedeutet:

C1 = P1 xor PZF
C2 = P2 xor PZF

Das heißt also, dass wir zwei verschlüsselte Nachrichten haben über die wir Folgendes aussagen können:

C1 xor C2 = (P1 xor PZF) xor (P2 xor PZF) = P1 xor P2

Haben wir also zwei verschlüsselte Nachrichten C1 und C2 erhalten, so wissen wir wenigstens P1 xor P2. Oft enthalten Nachrichten aber soviel Redundanz, dass man allein daraus auf beide Nachrichten schließen kann. Es gibt bekannte Methoden, die – zumindest für englische Texte – nach zwei Texten suchen, die – mit xor verknüpft – das gewünschte P1 xor P2 ergeben.
Gelingt es, auf diese Weise die Texte zu entschlüsseln, so hat man neben den beiden gewonnenen Nachrichten auch wieder eine Pseudozufallsfolge (Mit zugehörigem IV) gefunden, die man möglicherweise für das eigene aktive Senden verwenden kann.
Wie wahrscheinlich es ist, dass zwei Pakete mit demselben IV verschlüsselt werden, lässt sich dadurch abschätzen, dass eine Station, die konstant pro Sekunde 400 Pakete mit einer Größe

von 1500 Bytes verschickt, die zur Verfügung stehende Zahl von 2^24 möglichen IVs innerhalb von weniger als zwölf Stunden verbraucht hat. Hat bis dahin der Schlüssel nicht geändert, werden in der Folge also die gleichen Zufallsfolgen verwendet.
Erschwerend kommt hier noch hinzu, dass viele Implementierungen bei einer (Re-) Initialisierung der WLAN Karte den IV auf 0 setzen und dann bei jedem zu versendenden Paket um 1 inkrementieren. Dies hat zur Folge, dass niedrige Werte mit höherer Wahrscheinlichkeit auftreten als höhere.

79. Angriff auf WLAN – IP Umleitung

Oftmals fungiert ein WLAN Access Point auch als IP Router mit Internetanschluss, d.h. es werden auch IP Pakete über den AP geschickt. Da der Empfänger aller Wahrscheinlichkeit nach keine Möglichkeit hat, die WEP Verschlüsselung zu entziffern, wird dies vom AP erledigt und das unverschlüsselte Paket übers Internet verschickt.
Die Idee hinter dieser Attacke ist nun, dass man die Adresse der Empfänger IP derart ändert, dass das Paket auf einem Rechner ankommt, den der Angreifer selbst unter Kontrolle hat. Dort kann das vom AP bereits entschlüsselte Paket gelesen werden.

80. Angriff auf WLAN – Entschlüsselungswörterbuch

Gelingt es dem Angreifer – durch welche Methode auch immer – den Klartext zu einem Nachrichtenpaket zu ermitteln, so hat er auch die zugehörige Zufallszahlenfolge gewonnen. Wenn er nun lange genug auf dem Netzwerk mithört und fleißig entschlüsseln versucht, so kann er sich quasi nebenher ein nach IVs indiziertes Entschlüsselungswörterbuch aufbauen, das selbst im ungünstigen Fall in seiner Größe 38GB nicht überschreitet.
Allerdings braucht der Angreifer hierfür – je nach Netzlast – mitunter gehörig Geduld und ist außerdem darauf angewiesen, dass sich der Schlüssel in der Zwischenzeit nicht ändert. Unpraktisch wird der Angriff jedoch, wenn die Größe der IVs zunimmt, da damit das Wörterbuch – wollte man alle Vektoren aufnehmen – sehr schnell sehr viel größer werden würde.

81. Ein mobiles Endgerät möchte sich authentifizieren. Im entsprechenden Netz wird 802.11x mit EAP und einem RADIUS-Server eingesetzt. Wie läuft der Authentifizierungsvorgang ab. Wie wird der Zugriff auf das LAN kontrolliert?

802.11X ist eine sicherere Methode der Authentifizierung. Sie ist nicht speziell für WLAN gedacht, sonder für alle Ethernet Netze. Sie funktioniert folgendermaßen: Die Station stellt einen Anmeldeantrag beim Access Point. Dieser aktiviert den Port der Station und setzt ihn in den unautorisierten Zustand. Dann schickt der AP der Station eine Identitätsanfrage nach dem Extensible Authentication Protocol EAP. Die Antwort der Station auf diese Anfrage wird an den Server weitergeleitet. Dieser sendet dann eine Autorisierungsanfrage – im Falle von IEEE 802.1X nach dem Kerberos V Protokoll – über den AP an die Station, die entsprechend darauf antworten muss. Akzeptiert der Server die Antwort der Station, dann setzt der AP den Port der Station auf autorisiert, andernfalls schließt sie ihn.

82. Wozu dienen link keys bei Bluetooth? Welche Arten kann man unterscheiden? Erklärung.

Werden zur Verschlüsselung und zur Authentisierung verwendet. Man unterscheidet:

- initialization key
- unit key
- combination key
- master key

Master Key
Wird generiert, wenn der Master zu mehreren Geräten gleichzeitig Information senden möchte. Er überschreibt den aktuellen link key für eine Sitzung.

Initialization Key
Er wird während der Initialisierung genutzt. Wenn sich zwei Geräte zum ersten Mal begegnen und eine Verschlüsselung erwünscht ist, müssen sie einen gemeinsamen Schlüssel vereinbaren. Dazu wird der init key mittels einer Funktion (E22) aus einer geheimen PIN, der Device Adresse des Gerätes und einer Zufallszahl generiert. Standardmäßig ist die PIN 0000. Die Device Adresse ist aus einer unverschlüsselten Kommunikation bekannt.

Unit Key
Er wird generiert, wenn ein Bluetooth Gerät das erste Mal benutzt wird. Er setzt sich aus einer 128 Bit Zufallszahl und der 128 Bit Geräte Adresse zusammen.

Combination Key
Bei höherer Sicherheitsstufe während Initialisierung. Zufallszahl wird von beiden Geräten erzeugt. Danach wird mit dem Algorithmus E21, der auch den unit key erstellt, der Schlüssel erzeugt. Nachdem die Zufallszahlen geheim ausgetauscht wurden, erzeugen beide Geräte den combination key.

Encryption Key
Wird erzeugt, wenn der Link Manager die Verschlüsselung aktiviert. Er wird bei jeder neuen Verschlüsselungsanforderung neu berechnet. Der Schlüssel wird aus dem aktuellen link key, einer 96 Bit Chiphering Offset Number COF und einer 128 Bit Zufallszahl durch einen weiteren Algorithmus E3 generiert.

83. Wie kann man bei Bluetooth den Pin herausfinden?

- Ist der PIN zu kurz, kann der link key durch eine brute-force-Attacke herausgefunden werden:
- Angreifer belauscht Initialisierungsphase und bekommt so Zufallszahl und ausgetauschte Verifikationsdaten für die *init keys*.
- Angreifer wählt nun selbst einen PIN aus führt Initialisierung und Verifikation offline durch
- Dann vergleicht er die berechneten Funktionswerte mit den belauschten Daten.
- Bei Übereinstimmung hat er den richtigen PIN. Die weitere Kommunikation kann entschlüsselt werden.