

Draadloze verbindingen

Door:
Dave Ligthart
Edwin Croes
Leon Meijer
Robin Harmsen

Inhouds Opgave

INHOUDS OPGAVE	2
INLEIDING	4
WIFI	5
WAT IS WIFI?	5
DE STANDAARDEN	5
ROAMING	6
BEVEILIGING	7
<i>MAC-filtering</i>	7
<i>WEP-encryptie</i>	7
<i>WPA-encryptie</i>	7
<i>Een VPN</i>	7
DE ZWAKTES VAN WEP	8
<i>Hoe gaat de encryptie in zijn werk</i>	9
<i>Hoe gaat de decryptie in zijn werk</i>	9
<i>Het opvangen van pakketten en het achterhalen van de keystream</i>	10
<i>Het maken en gebruiken van een woordenboek</i>	10
<i>Het aanvallen volgens de manier van Fluhrer, Mantin en Shamir</i>	10
<i>Het in de praktijk kraken van een WEP-key</i>	11
<i>Welke maatregelen zijn er tegen deze zwaktes?</i>	11
SOORTEN APPARATEN	12
BLUETOOTH	13
<i>PAN en piconet</i>	13
<i>Frequency</i>	13
<i>Snelheid en bereik</i>	13
<i>Profielen en stack</i>	13
<i>Toepassingen</i>	14
BLUETOOTH PROTOCOL STACK	14
<i>Protocol lagen</i>	15
BLUETOOTH BASIS PROTOCOLLEN	15
<i>Baseband</i>	15
<i>Link Manager Protocol</i>	16
<i>Logical Link Control en Adaption Protocol</i>	16
<i>Service Discovery Protocol</i>	16
CABLE REPLACEMENT PROTOCOL	17
<i>RFCOMM</i>	17
TELEPHONY CONTROL PROTOCOL	17
<i>Telephony Control (binair)</i>	17
<i>Telephony Control (AT opdrachten)</i>	17
AANGENOMEN PROTOCOLLEN	17
<i>PPP</i>	17
<i>TCP/IP – UDP/IP</i>	17
<i>OBEX protocol</i>	18
<i>WAP</i>	18
BLUETOOTH MODELLEN	19
<i>Bestandsverzending</i>	19
<i>Internetbrug</i>	19
<i>LAN Toegang</i>	20
<i>Synchronisatie</i>	20
<i>Headset</i>	21

WIMAX	22
WAT IS HET?	22
WIMAX ZAL WAARSCHIJNLIJK DE DOORBRAAK IN BREEDBAND EN DRAADLOOSE NETWERK TOEPASSINGEN WORDEN.	22
BIJLAGE BLUETOOTH	23
VERKLARENDE WOORDENLIJST	23
BRONNEN	24

Inleiding

Deze Opdracht is gedaan door Leon, Robin, Edwin en Dave. We hebben gekozen voor het onderwerp Wireless omdat dit een snel ontwikkelende technologie is die ons allen erg aanspreekt. Het neemt namelijk een hoop voordelen met zich mee t.o.v. andere manieren om een netwerk te bouwen. Deze voordelen zijn: geen draden meer waardoor je met je laptop gemakkelijk in de tuin of op het balkon kan gaan zitten. Waar geen breedband verbinding is kan je toch internet zonder (telefoon-)tikken krijgen.

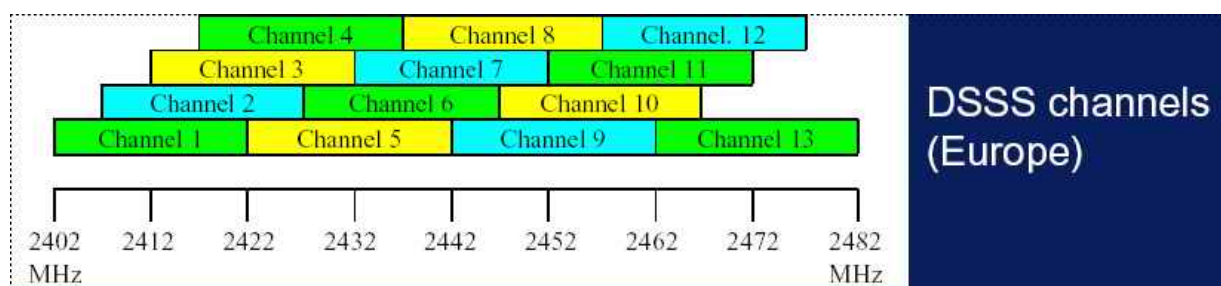
We vonden dat Bluetooth een onderdeel van wireless verslag moest worden omdat het ook draadloos gaat en omdat het concept ongeveer hetzelfde is. We hopen dat we alles een beetje goed hebben kunnen uitzetten zodat het een duidelijk en prettig te lezen verslag is.

WiFi

Wat is WiFi?

WiFi is de afkorting van Wireless Fidelity, vergelijkbaar met Hi-Fi (high Fidelity) voor de audio-wereld. Met het begrip WiFi geeft een fabrikant aan dat zijn producten voldoen aan de normen voor draadloze apparatuur, vastgelegd in de internationale technische standaard IEEE 802.11b. Het WiFi logo betekent dat een product is getest en gecertificeerd door de WECA (Wireless Ethernet Compatibility Alliance), en dat het kan samenwerken met WiFi apparatuur van andere leveranciers. In Europa kan WiFi op 13 verschillende kanalen binnen de 2.4Ghz band werken. Daarvan zijn er maar 3 volledig gescheiden kanalen: channel 1, channel 7 en channel 13.

Channel	Frequency (Mhz)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472



De standaarden

Er zijn momenteel drie standaarden. Dat zijn: de A, B en G standaard. Officieel moet je hier 802.11 voor zetten, zodat je respectievelijk 802.11a, 802.11b en 802.11g krijgt.

De A en B standaard zijn er al een tijdje. De A standaard heeft een snelheid van maximaal 54Mbit/sec. De frequentie van de A standaard is 5Ghz. Deze frequentie is gevoeliger voor obstakels en weersomstandigheden, waardoor het bereik meestal een helft, maar vaak een derde is van de B standaard. Omdat het

signaal nadat het minder wordt overschakelt op een lagere snelheid, is de B standaard meestal beter.

De B standaard werkt op 2.4Ghz. Deze frequentie is minder gevoelig voor obstakels en weersomstandigheden. Vat dit niet te zwaar op, want last van obstakels heb je al vrij snel, echter niet zo snel als met de A standaard. De B standaard kent 4 snelheden: 11, 5.5, 2 en 1 Mbit. Als het signaal goed is, zit je op 11 Mbit. Hoe minder het signaal, hoe minder de snelheid. De B standaard is op dit moment de meest gebruikte standaard.

Nu is er ook nog de G standaard. Dit is eigenlijk de opvolger van de B standaard en de A standaard tegelijk: het combineert het beste van de twee werelden, en het slechtste is verbeterd. Het werkt op 2.4 Ghz, dus dat scheelt al in de kwaliteit van het signaal. Verder is de snelheid van de G standaard 54Mbit. Nog een groot voordeel van de G standaard, is dat er op de meeste nieuwe G hardware WPA security zit. Dit is de verbeterde versie van WEP.

Er wordt ook nog aan andere 802.11 standaarden gewerkt:

- 802.11d** Extensions to Operate in Additional Regulatory Domains
- 802.11e** MAC Enhancements for Quality of Service
- 802.11f** Recommended Practice for Inter Access Point Protocol
- 802.11g** Standard for Higher Rate (20+ Mbps) Extensions in the 2.4GHz Band
- 802.11h** SMa - Spectrum Managed 802.11a
- 802.11i** MAC Enhancements for Enhanced Security
- 802.11j** 4.9 GHz - 5 GHz Operation in Japan
- 802.11k** Radio Resource Measurement Enhancements
- 802.11m** **Onbekend**
- 802.11n** Standard for Enhancements for Higher Throughput

Roaming

Simpel gezegd is roaming het proces van het verplaatsen van een verbinding van het ene accesspoint naar het andere. Als een netwerk uit meerdere accesspoints bestaat is het natuurlijk indenkbaar dat je zo'n sterk mogelijk signaal wilt hebben. Roaming zorgt ervoor dat het accesspoint met het beste bereik gekozen wordt om op verder te gaan. Als er op een ander accesspoint moet worden overgesprongen moet er wel kunnen doorgedaan met het netwerken. De enige problemen die hier wel op willen treden is packet loss bij het overgaan op een ander accesspoint.

Beveiliging

Bij een draadloos netwerk is beveiliging heel belangrijk. Als een netwerk niet beveiligd is, is het namelijk niet moeilijk om van buiten af op het netwerk te komen en dan kan een eventuele kraker verkeerde dingen doen. Er zijn verschillende beveiligingen en elke heeft zo zijn voordelen en nadelen.

MAC-filtering

Mac-filtering is een beveiliging die alleen de opgegeven mac-adressen op het netwerk toelaat. Hierdoor zouden alleen de devices binnen de netwerk omgeving op het netwerk kunnen. Het voordeel van deze techniek is dat het buitenstaanders enigszins tegen houdt. Het grote nadeel van deze techniek is dat het niet moeilijk is om een mac-adres te faken. De verstuurde pakketten kunnen worden opgevangen door buitenstaanders en hier zijn de mac-adressen gewoon uit te lezen. Op het moment dat dat mac-adres van het netwerk gaat, hij wordt bijvoorbeeld uitgezet, dan kan de aanvaller met dat zelfde mac-adres het netwerk op.

WEP-encryptie

Een andere en betere manier is om WEP-encryptie te gebruiken. WEP staat voor Wired Equivalent Protocol. Deze versleutelt de pakketten zodat het voor de buitenstaanders niet te lezen is. De encryptie is in te stellen op 64-bit, 128-bit en soms zelfs al 256-bit. Deze manier schrikt veel aanvallers af maar als een aanvaller echt het netwerk in wil komen dan kan hij gebruik maken van bepaalde zwaktes die WEP heeft. Deze zijn te lezen in het volgende hoofdstuk.

WPA-encryptie

WPA-encryptie is de opvolger van WEP. WPA staat voor WiFi Protect Access. Ook WPA encrypt de pakketten. WPA maakt gebruik van TKIP (Temporal Key Integrity Protocol) en heeft alle zwakke punten van WEP verbeterd. Het enige nadeel is dat WPA nog niet op alle devices is toegepast. Ook zijn er mensen die claimen dat WPA ook een zwakte heeft. Deze zwakte zou zijn dat gebruikers een makkelijk te raden key instellen.

Een VPN

Een VPN is een Virtual Private Network en versleuteld ook alle pakketten. Door gebruik te maken van een VPN over WEP is ook WEP weer wat veiliger gemaakt waardoor je weer een veilig netwerk hebt. Een VPN is net als WPA moeilijk te kraken.

De zwaktes van WEP

De WEP-encryptie is niet waterdicht. WEP heeft namelijk de volgende zwakke punten:

- **WEP maakt gebruik van een gedeelde key**
Elk van devices die met elkaar praten, heeft dezelfde key gedefinieerd. Hierdoor is de veiligheid van de key niet gewaarborgd.
- **Geen per-packet authenticatie**
Er wordt niet bij elk pakket gekeken of deze geldig is of niet, waardoor het makkelijker wordt om pakketten op het netwerk te spoofen.
- **WEP is kwetsbaar voor aanvallen van buitenaf**
Het is mogelijk om zonder WEP-key toch pakketjes het netwerk op te sturen die worden geaccepteerd.
- **Er is geen gebruikers identificatie en authenticatie**
Een gebruiker hoeft zich niet te identificeren en er is ook geen authenticatie procedure waardoor je als een buitenstaander toch het netwerk kan bereiken.
- **RC4 is kwetsbaar voor zogeheten "plain-text" aanvallen**
Aangezien WEP gebruikt maakt van het RC4 algoritme is dit ook voor WEP een zwakte.

Er zijn vier verschillende aanvallen die zijn uit te voeren op een netwerk met WEP-key beveiliging. Al deze aanvallen maken gebruik van de zwaktes van WEP.

- **Een passieve aanval**
Hier wordt verkeer ontsleutelt gebaseerd op statistische gegevens.
- **Een actieve aanval om gegevens te versturen op het lan vanuit ongeautoriseerde stations**
Hier worden pakketten gegenereerd en het netwerk opgestuurd waar dus ook gevaarlijke dingen in kunnen staan.
- **Een actieve aanval om verkeer te ontsleutelen**
Bij deze aanval wordt de brute-force methode toegepast om de pakketten te ontsleutelen.
- **Een aanval gebaseerd op een woordenboek**
Een systeem verzameld een bepaalde tijd pakketten, die achteraf real-time ontsleutelt worden met behulp van een woordenboek.

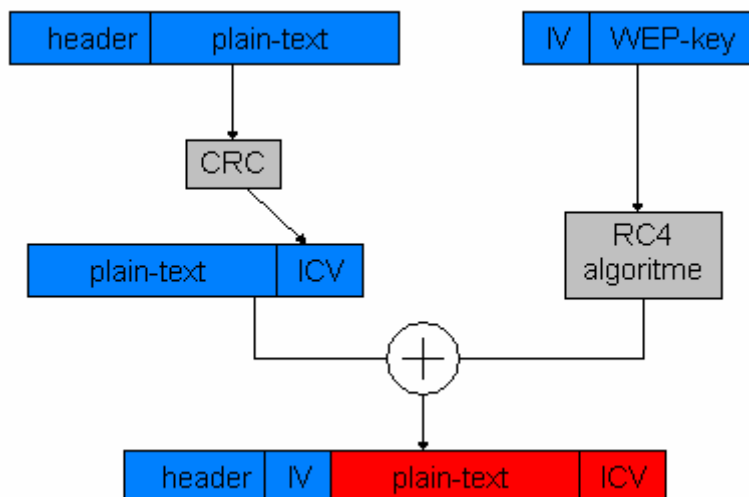
Hoe gaat de encryptie in zijn werk

Een WEP-encrypted pakketje wordt in een paar stappen gemaakt. Over plain-text, het gewone leesbare pakket, wordt een integriteits test algoritme (CRC) gedaan die een Integrity Check Value (ICV) oplevert. De ICV wordt achter de plain-text geplaatst.

De geheime WEP-key van 40-bit wordt samengevoegd met een initialisatie vector (IV, een nummer gegenereerd door de device) van 24-bit. De uitkomst wordt ingevoerd in een "pseudo-random number generator" (PRNG) ingevoerd en de uitkomst levert een keystream op. RC4 is het algoritme wat hiervoor wordt gebruikt.

Er wordt een exclusive OR (XOR) gedaan met de plain-text+ICV en de keystream. Dit is het geëncrypte gedeelte. Voor het geëncrypte gedeelte wordt de IV gezet die wel gewoon te lezen is.

Het totaal pakket wat wordt verzonden is de header, de IV en het geëncrypte gedeelte. Zie ook het figuur hieronder.



Hoe gaat de decryptie in zijn werk

Aangezien het grootste deel al is uitgelegd in de encryptie van het pakket is het niet moeilijk om de decryptie te beschrijven.

Eerst wordt de IV uit het pakket gelezen. Hier wordt samen met de WEP-key weer een keystream van gemaakt. Er wordt een XOR gedaan met de keystream en met het geëncrypte gedeelte. Nu zijn de plain-text en de ICV weer leesbaar.

Als de decryptie is voltooid wordt er door middel van het integriteits test algoritme met de ICV, gekeken of de plain-text niet corrupt is. In de figuur hieronder is het encrypten en decrypten simpel weergegeven.

```

"WIRELESS" = 574952454C455353
RC4("foo") = 0123456789ABCDEF
encryptie   ----- XOR
              566A1722C5EE9EBC
RC4("foo") = 0123456789ABCDEF
decryptie   ----- XOR
              "WIRELESS" = 574952454C455353

```

Het opvangen van pakketten en het achterhalen van de keystream

Op het moment dat er pakketten zijn opgevangen en er zijn twee pakketten aanwezig met dezelfde IV, dan is er een mogelijkheid om de keystream eruit te halen. Een voorwaarde is wel dat de inhoud van een van de pakketten bekend is.

Stel je hebt een pakket P1 en een pakket P2. Beiden zijn geëncrypt. P3 is P1 alleen dan niet geëncrypt en hetzelfde geldt voor P4 en P2. Dan bestaat er het volgende: $P1 \text{ XOR } P2 = P3 \text{ XOR } P4$. Op het moment dat je XOR uitvoert op P1 en P2 vervalt de keystream. Als nu de inhoud van P1 of P2 bekend is (als je dus P3 of P4 weet) dan kun je de keystream achterhalen en de andere pakketten met dezelfde IV decrypten. De keystream krijg je door P1 te XORen met P3.

Het maken en gebruiken van een woordenboek

Met een woordenboek wordt hier een bestand bedoeld waar voor elke IV een keystream bekend is. Deze keystream is te achterhalen door de manier van hierboven uit te voeren. Als je voor elke IV die er is de keystream achterhaalt en deze in een file zet, kun je alle pakketten ontsleutelen met de juiste keystream of zelf pakketten versleutelen en versturen.

Een andere manier van een woordenboek gebruiken is een brute-force aanval aan de hand van een woordenboek. Als de gebruiker een ASCII WEP-key heeft ingesteld, zal het meestal een bestaand woord zijn. Door elke entry in een woordenboek langs te gaan en te proberen op een pakketje kan de WEP-key gevonden worden, maar succes is niet gegarandeerd.

Het aanvallen volgens de manier van Fluhrer, Mantin en Shamir

Om te beginnen eerst een stukje over hoe RC4 werkt: RC4 bestaat uit twee delen: een key scheduling algoritme en een output generator. In WEP gebruikt het key scheduling algoritme een 64-bit (40-bit geheime sleutel met een 24-bit IV) sleutel of een 128-bit (104-bit geheime sleutel met een 24-bit IV) sleutel om een RC4 state array, S , op te zetten, wat een permutatie is van $\{0, \dots, 255\}$. De output generator gebruikt S om een pseudorandom reeks te genereren.

De aanval maakt alleen gebruik van het eerste woord van de uitkomst van de pseudorandom reeks, dus daar kunnen we ons op richten. De vergelijking van de eerste output byte is wordt gegeven door $S[S[1]] + S[S[1]]$. Hierdoor hangt de eerste byte alleen maar af van drie waarden van de state array ($S[1]$, $S[S[1]]$, $S[S[1]] + S[S[1]]$).

Om de aanval toe te passen, zoeken we naar IV's die de key setup algoritme in een staat zet die informatie lekt over de key. Gebruik makend van de terminologie van Fluhrer en anderen, verwijzen we deze key lekkende gevallen

als opgelost. Elk opgelost pakket lekt informatie over maar één key byte, en deze moet goed worden geraden voordat een pakket informatie geeft over een latere key byte.

Het gaat er dus om dat elke key byte goed wordt geraden. Een programma dat deze aanval implementeert is AirSnort. Als je precies wilt weten hoe de aanval in zijn werk gaat, kun bij onze bronnen kijken.

Het in de praktijk kraken van een WEP-key

Als je in de praktijk een WEP-key wilt kraken heb je niet zo heel veel kennis nodig over de zwaktes van WEP. Het enige wat je nodig hebt is de juiste hardware en software. De benodigdheden zijn:

- Computer (het liefst een laptop)
- Een draadloze netwerk kaart (met een Prism of Orinoco chipset)
- AirSnort
- De juiste configuratie van het operating system en drivers

Het makkelijkst is om een laptop te gebruiken. Doe hier de draadloze netwerk kaart in. Als je geen zin hebt om veel moeite te doen dan kun je Knoppix gebruiken. Hier zijn de drivers al pre-installed en ook AirSnort staat er al op. Doe de cd in de laptop en boot ervan. Eenmaal in Knoppix moet je even je wireless kaartje instellen en dan kun je AirSnort starten. Je hebt wel super-user rechten nodig! Als je eenmaal AirSnort hebt aangezet kun je beginnen met wachten.

Airsnort heeft ongeveer 2000 interessante pakketten nodig om de key te kunnen kraken. Deze interessante pakketten zijn de pakketten die informatie lekken over de key.

Welke maatregelen zijn er tegen deze zwaktes?

Om aan deze WEP-key zwaktes te ontsnappen, zijn er verschillende manieren. Er zijn bijvoorbeeld netwerkkaartjes die de zwakke IV's niet gebruiken, zodat er geen informatie meer wordt gelekt. Deze manier lost alleen het Fluhrer en anderen probleem op.

Een andere manier is om WEP te vervangen voor WPA. Dit is natuurlijk niet makkelijk als je netwerk device alleen WEP heeft. Als je device WPA heeft gebruik deze dan.

Maar de beste en makkelijkste oplossing voor iedereen is toch het gebruik maken van een VPN. Hierdoor is het voor een eventuele kraker niet meer leuk omdat hij dan eerst het VPN moet kraken wat erg lang kan duren (lees vele jaren).

Soorten Apparaten

USB adapter netwerk kaart

PCI netwerk kaart

PCMCIA netwerk kaart

Acces point

Wireless bridge

Repeater

De netwerk adapter van het draadloze netwerk bestaan in 3 soorten (PCMCIA voor de laptop, PCI voor in de pc en USB variant voor in de USB poort). Deze zorgen er voor dat de computer met het netwerk kan communiceren. Dit doet het apparaat door het digitale signaal van de computer om te zetten in een analoog radio signaal. Het verzonde signaal kan dan weer door een anderen draadloze netwerk kaart of acces point worden opgevangen en vertaalt naar digitaal signaal of worden door gestuurd naar een andere netwerk node.

De wireless bridge en de Repeater lijken in principe wel op elkaar. Wat de wireless bridge doet, is het verbinden van een wireless netwerk met een andere netwerk wat op zichzelf ook weer een wireless netwerk kan zijn maar ook een bedraad netwerk. De repeater herhaalt het signaal waardoor de afstand waarover het signaal komt extra verkomt. Het nadeel van een repeater is dat hij de snelheid van het netwerk halveert waardoor het niet verstandig is om deze meerdere keren in het netwerk te gebruiken.

Bluetooth

Bluetooth is een communicatiesysteem voor apparaten die op korte afstand met elkaar communiceren. Het ultieme doel is om apparaten die conform de Bluetooth-specificatie zijn gemaakt te laten samenwerken.

PAN en piconet

Naast de al bekende WAN en LAN is er nu ook PAN. PAN staat voor Personal Area Network. Wanneer een netwerk wordt opgezet via Bluetooth, wordt dit PAN genoemd, aangezien het bereik niet groot is. Een netwerk van Bluetooth apparaten wordt een piconet genoemd. Een piconet bestaat uit maximaal 8 Bluetooth-apparaten.

Frequency

Eén van de belangrijkste eigenschappen van Bluetooth is *frequency-hopping*. De frequentie wisselt 1600 keer per seconde over 79 kanalen in Europa/VS, en 23 kanalen in Japan. Alle bluetooth apparaten maken gebruik van de vrije 2.4 GHz band, net als Wifi. Door dit frequency-hopping is bluetooth minder storingsgevoelig (het heeft minder last van andere apparaten die op dezelfde frequentie werken) en is veiliger. Het is veiliger omdat alleen beide apparaten het synchronisatieschema kennen. Een bluetooth chip kan 7 verbindingen gelijktijdig hebben.

Snelheid en bereik

De maximale snelheid van Bluetooth bedraagt 1 Mbit. Dat is aanzienlijk langzamer dan Wifi, maar snel genoeg voor pda's en mobiele telefoons. Wanneer veel dataoverdracht nodig is (bijvoorbeeld voor grote bestanden) is WiFi een betere keuze. In de bluetooth specificatie staan drie classificaties voor het bereik van een bluetooth zender.

- **Klasse A**
100 meter, 100 mW
- **Klasse B**
10 meter, 2,5 mW
- **Klasse C**
1 meter, 1 mW

Profielen en stack

Door middel van gemeenschappelijke profielen kunnen Bluetooth apparaten met elkaar communiceren. Met een profiel wordt eigenlijk een protocol stack bedoeld. Voor het verzenden van een visitekaartje gebeurt bijvoorbeeld het volgende: vCard -> OBEX -> RDCOMM -> L2CAP -> Baseband. Het ontvangende apparaat moet al deze protocol stacks ook geïmplementeerd hebben om het kaartje goed binnen te krijgen.

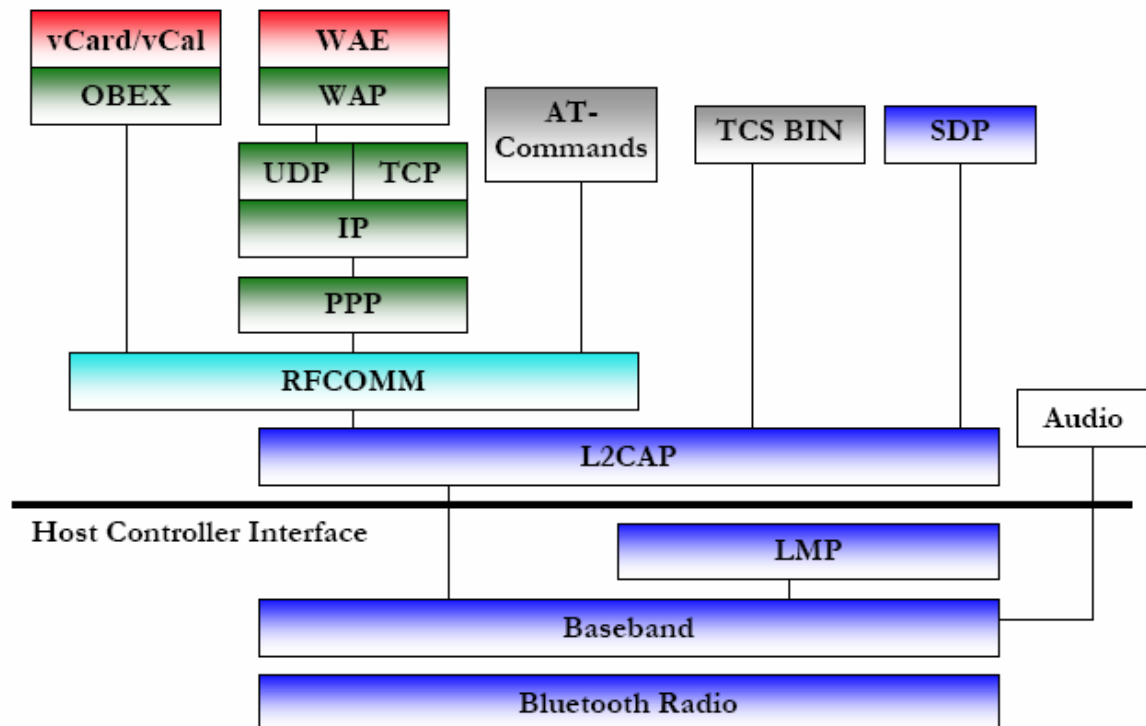
Toepassingen

Steeds meer nieuwe kleine draagbare apparaten zijn momenteel voorzien van Bluetooth. Daarbij moet vooral gedacht worden aan de volgende apparaten:

- Mobiele telefoon
- PDA
- Laptop
- Digitale (video)camera
- Printers
- Toetsenborden

Bluetooth protocol stack

In het onderstaande figuur ziet u een overzicht van de Bluetooth protocol stack.



Zoals in het figuur te zien is bestaat Bluetooth uit specifieke protocollen als LMP en L2CAP, maar ook uit algemene protocollen zoals UDP, TCP en OBEX (Object Exchange Protocol).

Bij het ontwerpen van apparaten met Bluetooth is het hoofddoel dat zo veel mogelijk bestaande protocollen uit de hogere lagen worden hergebruikt.

Daardoor werken Bluetooth applicaties snel en worden beter ondersteund door andere apparaten.

Protocol lagen

De Bluetooth protocol stack kan onderverdeeld worden in vier lagen. De protocollen behoren als volgt in de volgende lagen:

Bluetooth basis protocollen	Baseband, LMP, L2CAP, SDP
Kabel vervang protocol (Cable Replacement Protocol)	RFCOMM
Telefoon beheer	TCS Binary, AT-opdrachten
Aangenomen protocollen	PPP, UDP/TCP/IP, OBEX, WAP, vCard, vCal, IrMC, WAE

Naast de bovenstaande protocollagen, staat in de specificatie ook een Host Controller Interface (HCI). Deze heeft een opdracht interface naar de baseband controller, link manager en heeft toegang tot de hardware status en control registers.

Aangezien de Bluetooth specificatie open is, kunnen er aanvullende protocollen aan worden toegevoegd (bijvoorbeeld HTTP of FTP). Deze worden bovenop de bestaande hogere protocollen toegevoegd.

Bluetooth basis protocollen

Baseband

De BaseBand en de Link Control zorgen voor de fysieke RF verbinding tussen Bluetooth apparaten, zodat een piconet gevormd wordt. Omdat het Bluetooth RF systeem een frequency-hopping systeem heeft moeten de datapakketten in *time slots* verzonden worden op gedefinieerde frequenties. Deze laag zorgt voor de synchronisatie met de verschillende verbonden Bluetooth apparaten.

Er zijn 2 verschillende soorten fysieke lagen. De eerste is SCO, wat staat voor Synchronous Connection Oriented. Deze is point-to-point, waardoor een master en slave gevormd wordt. Dit datalink type wordt gebruikt voor tijd kritieke toepassingen als een voice headset. Niet aangekomen of incorrecte pakketjes worden niet herverzonden. De tweede is ACL, ofwel voor Asynchronous Connectionless Link. Over een ACL verbinding kan alleen data. Voor een SCO verbinding is een ACL verbinding noodzakelijk.

Type	Symmetric (SCO) (Kbps)	Asymmetric (Kbps) Downlink	(ACL) (Kbps) Uplink
1 channel, using FEC	108,8	108,8	108,8
1 channel	172,8	172,8	172,8
3 channels, using FEC	256,0	384,0	54,4
3 channels	384,0	576,0	86,4
5 channels, using FEC	286,7	477,8	36,3
5 channels	432,6	721,0	56,7

Table 1 Possible Bitrates

Alle audio-en datapakketten kunnen worden voorzien van verschillende niveau's FEC en CRC foutcorrectie, en kunnen worden versleuteld.

Audio data kan worden verzonden naar 1 of meer Bluetooth-apparaten. Audio wordt direct van en naar de Baseband verzonden, zodat het niet gaat door L2CAP. Daardoor is audio relatief eenvoudig binnen Bluetooth. Elk Bluetooth-apparaat kan audio ontvangen en verzenden door een audiolink te openen.

Link Manager Protocol

Het Link Manager Protocol is verantwoordelijk voor het opzetten van een verbinding tussen Bluetooth-apparaten. Dit omvat ook de beveiligingsaspecten zoals authenticatie en encryptie.

Verder zorgt LMP voor de stroommodus en de verbindingstatus van een Bluetooth-apparaat binnen een piconet.

Logical Link Control en Adaption Protocol

Met de Bluetooth Logical Link Control en het Adaption Protocol (L2CAP) kunnen hogere lagen gebruik maken van de Baseband.

L2CAP die *connection-oriented* en *connectionless* data services voor de hogere lagen protocollen, met mogelijkheid voor protocol multiplexing en segmentatie. De maximale grootte van L2CAP datapakketten is 64 kilobytes, die doorgegeven kunnen worden aan hogere lagen.

Service Discovery Protocol

Het ontdekken van services is een zeer belangrijk onderdeel van Bluetooth. Een overzicht van services die een Bluetooth apparaat biedt, is de basis voor het gebruiken van Bluetooth. Via SDP kan apparaatinformatie en de services/profielen (inclusief de eigenschappen) van een ander apparaat worden gevraagd. Daarna kan een verbinding worden gemaakt tussen 2 of meer Bluetooth apparaten.

Cable Replacement Protocol

RFCOMM

RFCOMM emuleert een seriële verbinding en is gebaseerd op de ETSI 07.10 specificatie. Het emuleert de zeer bekende RS-232 control en data signalen. RFCOMM kan weer gebruikt worden door hogere lagen protocollen, zoals OBEX. Dankzij de seriële emulatie is het eenvoudig om software die gebruik maakt van RS-232 compatible te maken met Bluetooth.

Synchronisatie tussen een bijv. een PDA en een PC gebeurt doorgaans via een seriële RS-232 kabel, een USB kabel, infrarood of Bluetooth. Aangezien de aansturing van de hardware via RS-232, infrarood en Bluetooth gelijk is, is softwareontwikkeling makkelijker en kan bestaande software gebruik maken van Bluetooth.

Telephony Control Protocol

Telephony Control (binair)

TCS (binair) is een bit-georiënteerd protocol waarin alle signalen voor data-en spraakoproepen zijn vastgelegd.

Telephony Control (AT opdrachten)

Er zijn AT-opdrachten gespecificeerd zodat een mobiele telefoon en een modem gebruikt kunnen worden.

Aangenomen protocollen

PPP

In de Bluetooth specificatie is PPP ontwikkeld om gebruik te worden via RFCOMM voor het maken van point-to-point verbindingen. PPP is het point-to-point protocol, waarmee IP pakketten van/naar de PPP laag naar een LAN kunnen worden gebracht.

TCP/IP – UDP/IP

Deze protocollen worden gebruikt voor het wereldwijde internet. Het is het meest gebruikte protocol in de wereld. TCP/IP wordt ondertussen ook gebruikt door printers, handheld computers en mobiele telefoons.

TCP/IP/PPP wordt gebruikt voor alle scenario's waar een internet brug nodig is, zoals bij WAP.

OBEX protocol

OBEX is ontwikkeld door de Infrared Data Association (IrDA) voor het uitwisselen van objecten op een eenvoudige manier. OBEX biedt ongeveer dezelfde functionaliteit als http, maar dan in een lichtere vorm. Het model is onafhankelijk van het transportmechanisme. OBEX is een betrouwbaar protocol. Met OBEX is ook *folder-listing* mogelijk, oftewel: een ander Bluetooth apparaat kan de door de inhoud van een gegevensmap bladeren.

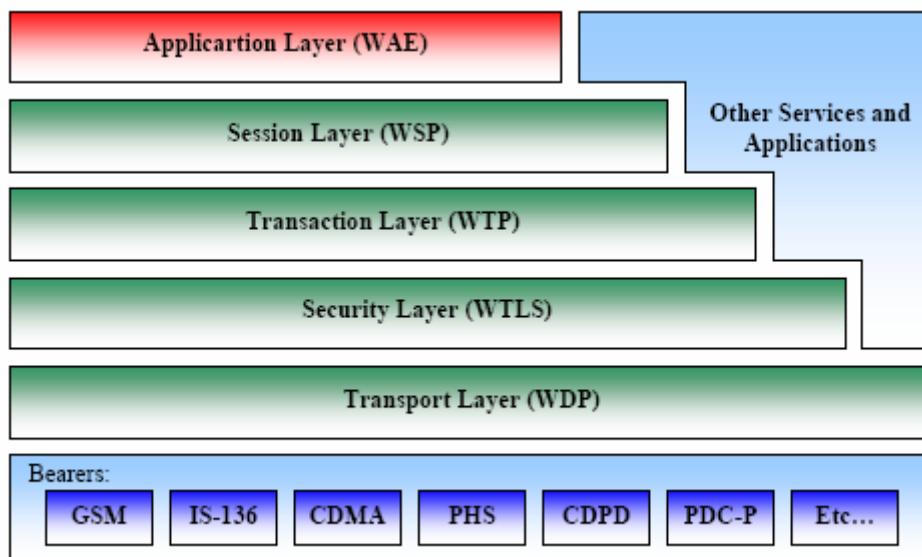
RFCOMM wordt gebruikt voor het uitwisselen via OBEX. In de toekomst zal dat ook kunnen via TCP/IP.

Bij OBEX zijn een aantal formaten vastgelegd:

vCard	Visitekaartje
vCalendar	Persoonlijke kalenderitems
vMessage	Berichten
vNote	Notities

WAP

WAP zit tegenwoordig op vrijwel alle nieuwe mobiele telefoons. WAP staat voor Wireless Application Protocol. Mobiele telefoons kunnen via het WAP internetten. Het doel is om internetgegevens naar mobiele telefoons en andere draadloze apparaten te brengen.



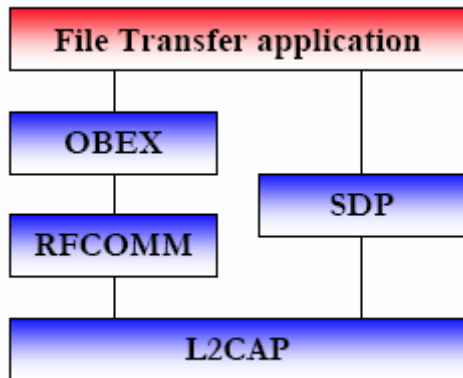
Bovenstaande figuur toont het WAP Framework.

Waar HTML wordt gebruikt bij HTTP, wordt WML (Wireless Markup Language) gebruikt bij WAP. Op mobiele telefoons is dan ook een WAP/WML browser aanwezig. Voor BMP-afbeeldingen wordt bij WAP wBMP gebruikt. WMLScript wordt gebruikt voor scripting.

Bluetooth modellen

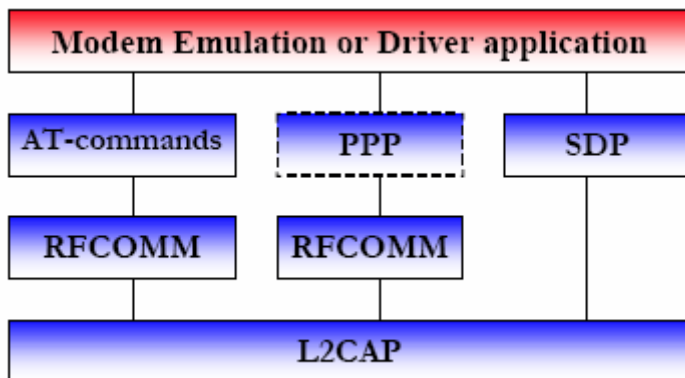
Bestandsverzending

Met het *file transfer usage model* kan data van het ene apparaat (bijv PC, smartphone of PDA) worden verzonden naar een ander. Met het model kunnen bestanden als .xls, .doc en .jpg worden verzonden, maar ook het verkrijgen van een lijst van de inhoud van een map is mogelijk.



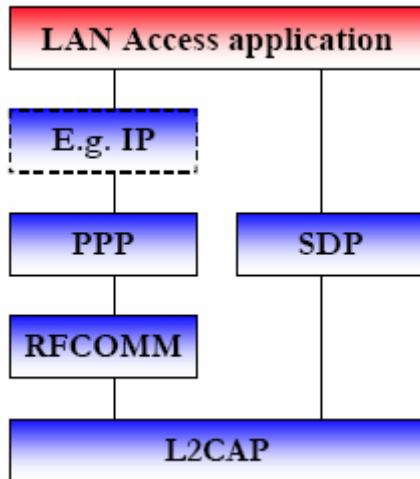
Internetbrug

Met dit model kan een mobiele telefoon of draadloos modem zich gedragen als een modem op de PC. Hierdoor kan gebruik gemaakt worden van fax-en inbelverbindingen, net als op de PC. De AT-opdrachten zijn nodig om de mobiele telefoon of modem te besturen.



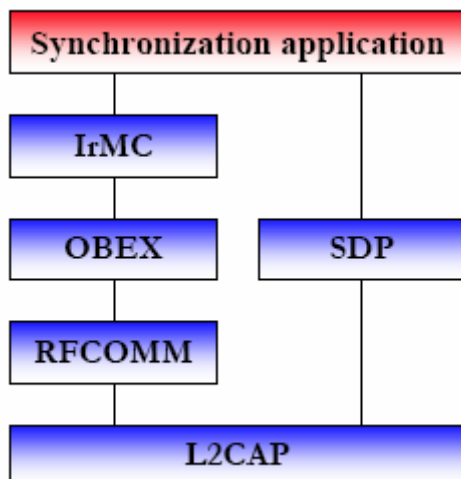
LAN Toegang

In dit model gebruiken meerdere data terminals (DT's) een LAN access point (LAP) en een draadloze verbinding met een Local Area Network (LAN). Eenmaal verbonden, kunnen de DT's gebruikt worden alsof ze zijn verbonden via een LAN of inbelverbinding.



Synchronisatie

Met dit model kunnen apparaten met elkaar PIM-informatie (Personal Information Management) synchroniseren. PIM wordt gebruikt voor adresboeken, kalender, berichten en notities.

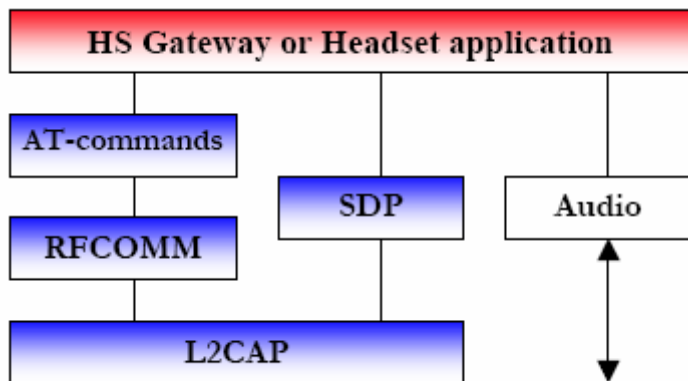


Headset

In Nederland is een headset voor in de auto verplicht wanneer rijdend gebeld wordt. Er zijn setjes op de markt die werken met kabels, maar ze zijn er ook die draadloos via Bluetooth werken!

Door een draadloze headset wordt de vrijheid en bewegingsmogelijkheden van de gebruiker vergroot.

De audiostream is rechtstreeks verbonden met de Baseband. De headset moet AT-opdrachten kunnen verwerken en resultaatcodes kunnen ontvangen. Daardoor kan via de headset een inkomend telefoontje beantwoord worden.



WiMAX

Wat is het?

Naast de WiFi standaarden is er nu ook een nieuwe draadloos netwerk standaard genaamd WiMAX (802.16)

802.16a, of wel WiMAX, is een draadloos netwerk standaard dat grotere afstand en bandbreedte aan kan dan de WiFi familie. (802.11)

De eerste versie van de 802.16 standaard, die door de IEEE in 2002 werd geaccepteerd is, opereert in de 10to66 GHz frequency band en moest een line-of-sight hebben.

De 802.16a extensie, gemaakt in Maart 2003, heeft geen line-of-sight meer nodig en werkt op lagere frequenties (2 tot 11 GHz), welke vrij zijn om te gebruiken.

802.16a kan ongeveer 70Mbit per over een afstand van 50 kilometer aan. En dat met duizende gebruikers op een basis station.

Ter vergelijking, de meeste gebruikte WiFi standaard (802.11b), kan 11Mbit per seconden aan over een afstand van 300 meter in open gebied.

Aan andere 802.16 standaarden wordt nog gewerkt:

802.16b — Quality of service

802.16c — Interoperability, with protocols and test-suite structures

802.16d — Fixing things not covered by 802.11c, which is the standard for developing access points

802.16e — Support for mobile as well as fixed broadband

WiMAX zal waarschijnlijk de doorbraak in breedband en draadloose netwerk toepassingen worden.

De grotere afstand en hogere bandbreedte van WiMAX geeft een ISP de mogelijkheid om breedband internet toegang direct naar de huizen brengen zonder dat ze zich zorgen hoeven te maken over de problemen die kunnen ontstaan bij het leggen van fysieke verbindingen lijnen over de "laatste km".

Naast dat het makelijker is is het ook goedkoper voor de ISPs. Een auto om de installatie te doen kost bijv al €400. met WiMAX heb je dit niet omdat je een access point hebt of afstand.

WiMAX is nog niet beschikbaar op dit moment, maar de standaard zal in Januari vast gelegd worden volgens Intel.

Intel wil ook graag het eerste bedrijf zijn dat WiMAX gebaseerde producten op de markt brengt. De productie van chips voor WiMAX apparatuur zullen in de eerste helft van 2004 starten, Intel hoopt WiMAX commercieel beschikbaar te hebben in 2005.

WiMAX zal in het begin niet meteen beschikbaar zijn voor laptops en handhelds, WiMAX zal eerst gebruikt worden om de problemen van de laatste kilometer te overwinnen.

Bijlage Bluetooth

Verklarende woordenlijst

Term	Betekenis
ACL	Asynchronous ConnectionLess
API	Application Programming Interface
CRC	Cyclic Redundancy Check
DT	Data Terminal
FEC	Forward Error Correction
FTP	File Transfer Protocol
GAP	Generic Access Profile
GOEP	Generic Object Exchange Profile
HCI	Host Controller Interface
HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IrDA	Infrared Data Association
IrMC	Ir Mobile Communications
LAN	Local Area Network
LAP	LAN Access Point
LMP	Link Manager Protocol
L2CAP	Logical Link and Control Adaptation Protocol
OBEX	Object Exchange Protocol
PDA	Personal Digital Assistant
PIM	Personal Information Management
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephony Network
RFCOMM	Serial Cable Emulation Protocol
SCO	Synchronous Connection-Oriented
SDAP	Service Discovery Application Profile
SDP	Service Discovery Protocol
TCP/UDP	Transport Control Protocol/User Datagram Protocol
TCS Binary	Telephony Control Specification – Binary
WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WML	Wireless Markup Language

Bronnen

<http://www.bluetooth.org>

<http://www.bluetooth.com>

<http://standards.ieee.org/wireless/>

<http://airsnort.shmoo.com>

http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

<http://www.cs.rice.edu/~astubble/wep/>

http://www.cs.rice.edu/~astubble/wep_attack.pdf

<http://forum.wirelessnederland.nl>

<http://www.wi-lan.com/>