Chapter 15. modems

Table of Contents

Een inleiding over oude en hedendaagse modems.

15.1. over modems

Over modems is heel wat te zeggen, modems hebben een essentiële rol gespeeld in de ontwikkeling van internet.

15.1.1. modulatie-demodulatie

Per definitie is een modem een modulator-demodulator. Modulatie is het encoderen van digitale informatie (zoals bits) over een analoog signaal (zoals het geluid over een telefoonverbinding). Demodulatie is het terug omzetten van dit analoge signaal naar (hopelijk dezelfde) bits.

Een modem is dus een interface tussen de computer en het telefoonnetwerk, en laat toe dat twee computers (digitaal) met elkaar praten over de (analoge) telefoon.

15.1.2. pariteit

Pariteit is een eenvoudige controle op fouten tijdens de transmissie.

15.1.3. baud

Het moduleren van digitale informatie gebeurt in **symbolen**. Een symbool is een eenheid van digitale informatie die gecodeerd (gemoduleerd) is in een analoog signaal. Zo een eenheid van digitale informatie is bijvoorbeeld een bit (deze kan 0 of 1 zijn). Maar het kan evengoed een koppel bits zijn (mogelijke symbolen zijn dan 00, 01, 10 en 11).

Indien een modem 300 symbolen per seconde kan zenden of ontvangen, spreken we van een **modulatie rate** of **baud rate** van 300.

15.1.4. bit rate

De **bit rate** van de modem hangt af van de gebruikte symbolen. In het geval dat elk symbool slechts 1 bit bevat, is de bit rate gelijk aan de baud rate. Bevat elk symbool twee bits, dan is de bit rate het dubbel van de baud rate.

15.1.5. bits per seconde

De **bit rate** kan je meten in bits per seconde (**bit/s** of **bps**) of ook in kilo- mega- giga- en terabits per seconde (ook geschreven als Mbit/s, Mbps, Gbit/s, Gbps, Tbit/s, Tbps). In tegenstelling tot de kibi vs kilo discussie bij harde schijven, is hier een kilo altijd gelijk geweest aan 1000 en een mega altijd aan 1000 kilo (enzoverder).

15.1.6. seventies V. standaarden

De bandbreedte (soms ook snelheid genoemd) in bits per seconde hangt af van de gebruikte standaard. De **V.21** standaard van 1962 liet toe om 300 bit/s te halen met een baud rate van 300 (m.b.v. FSK). De **V.22** standaard uit 1976 haalde 1200 bit/s gebruik makend van 600 baud (m.b.v. PSK).

15.1.7. eighties V. standaarden

De jaren 80 zagen een evolutie van 2400 bit/s over 600 baud (de V.22bis standaard) naar 9600 bit/s over 2400 baud. Deze laatste werd in 1989 bereikt met de **V.32** standaard.

15.1.8. nineties V. standaarden

1991 zag de 14.4 kbit/s, dit werd verdubbeld in 1994 en verdrievoudigd in 1996 om vanaf 1998 een tijdje te blijven staan op de veelgebruikte **V.90** standaard van 56 kilobits per seconde.

Nadien zijn we overgeschakeld op andere technologiën zoals DSL en DOCSIS.

15.2. over DSL

15.2.1. DSL

DSL is een verzamelnaam voor verschillende **digital subscriber loop** implementaties zoals SDSL, IDSL, ADSL, ADSL2 etc.

Typisch aan DSL is dat je een **DSL-splitter** nodig hebt om de lage voice-tonen (die naar de klassieke telefoon moeten) te scheiden van de hoge tonen (boven 25kHz) die DSL gebruikt voor data, en die naar de xDSL modem moeten.

In tegenstelling tot wat sommige mensen denken, maakt de DSL technologie geen gebruik van het echte **pots** netwerk, maar enkel van de **local loop**.

15.2.2. ADSL

Asynchronous DSL werkt ook over de telefoonlijn, of beter over het klassieke koperpaar tot aan de centrale (de **local loop**). **adsl** is veel sneller dan de 'normale' modems. **adsl** gebruikt andere frequenties dan de voice-modems, en werkt enkel op korte afstand (maximum 5km) van de **DSLAM** in de telefooncentrale. Die **dslam** splitst wederom de stem van de rest, en daar waar de stem over het **pots** netwerk

verder gaat, gaat het **adsl** signaal over het datanetwerk van de telefoonmaatschappij (of isp) om zodoende het internet te bereiken.

ADSL heeft typisch een veel grotere download bandbreedte dan upload. Een adsl modem synchroniseert met een bepaalde sync rate, de gebruiker bereikt door overhead maximaal 80-85 procent van deze sync rate.

15.2.3. SDSL

Synchronous DSL is nagenoeg identiek aan ADSL, behalve dat de up en download hetzelfde is.

15.2.4. DSLAM

Een DSLAM is een **DSL Access Multiplexer** die verscheidene DSL lijnen verbindt met het internet. Je kan pas ADSL nemen als jouw telefooncentrale over een DSLAM beschikt.

De bandbreedte die je haalt tussen je xDSL modem en je lokale DSLAM wordt beperkt door de afstand tot aan de centrale:

```
 300m --> 25 Mbit/s
 600m --> 24 Mbit/s
 900m --> 23 Mbit/s
1200m --> 22 Mbit/s
1500m --> 21 Mbit/s
1800m --> 19 Mbit/s
2100m --> 16 Mbit/s
4500m --> 1.5 Mbit/s
```

15.2.5. local loop

Met de **local loop** bedoelen we de laatste paar kilometer draad van de telefooncentrale tot aan uw woning. In heel wat landen is de (oude) publieke telefoonmaatschappij de eigenaar van deze laatste kilometer tot aan uw huis. Sommige landen hebben een wetgeving die verplicht om deze **local loop** te delen met concurrenten.

15.2.6. ATM

ATM is ontwikkeld in de jaren 80 met realtime audio en video over het netwerk als doel. ATM werkt met zeer kleine cellen om **jitter** te voorkomen. Het is immers onaanvaardbaar dat packetjes te laat komen tijdens een telefoongesprek.

Naast een DSLAM (in dezelfde telefooncentrale) staat soms een ATM verbonden met een ISP.

15.2.7. IP-DSLAM

Een IP-DSLAM is een DSLAM die rechtstreeks IP spreekt met routers (in tegenstelling tot de normale DSLAM die ATM gebruikt om daarna via een ATM-IP router te verbinden met IP).

15.2.8. IDSL

IDSL is DSL over ISDN. Het grote verschil met SDSL en ADSL is dat er bij IDSL geen gebruik wordt gemaakt van het klassieke voice-telefoonnetwerk. Alle data gaat over het ISDN netwerk. Nadeel is dan weer dat je niet tegelijk kan internetten en telefoneren (als je enkel over ISDN beschikt).

15.2.9. multiplexen

Multiplexen wil zeggen dat meerdere digitale signalen (die komen van meerdere kabels) worden samengezet op 1 enkel signaal (een enkele kabel). Multiplexen laat dus toe dat meerdere digitale signalen een (duur) kanaal (of een enkele kabel) delen. De multiplexer is een toestel dat meerdere signalen groepeert, de demultiplexer haalt de originele signalen er weer uit. Deze toestellen worden ook een **muxer** en een **demuxer** genoemd.

15.2.10. ADSL2+

ADSL2+ gebruikt een groter spectrum om de downloadsnelheid van ADSL te verdubbelen tot 24Mbit/s.

15.2.11. VDSL

VDSL is een nog snellere variant van DSL, met downloads tot 52Mbit (en tot 100Mbit sinds 2006).

15.3. over kabelmodems

15.3.1. DOCSIS

DOCSIS is een internationale standaard om dataverkeer mogelijk te maken over de bestaande kabel-TV netwerken (zonder de TV uitzendingen te verstoren).

DOCSIS maakt gebruikt van kabelmodems die dienst doen als bridge en als modem om internet toegang te leveren via het (coax) kabelnetwerk.

In Europa wordt door de PAL/NTSC verschillen eigenlijk de **EuroDOCSIS** standaard gebruikt (die ongeveer 25 procent sneller is dan de equivalente DOCSIS standaard).

15.3.2. CMTS

Te vergelijken met de DSLAM bij DSL, verbinden de kabelmodems van de klanten zich met een CMTS in de centrales van het (TV-)kabelnetwerk. Een CMTS heeft (duizenden) coax kabels aan de ene kant, en ethernet interfaces aan de internet kant.

15.4. over bandbreedte

Tot slot nog een kleine vergelijking van bandbreedtes van de besproken modems in kilobytes per seconde.

```
Modem 300/300 bit/baud  -->  0.03kB/s
Modem 2400/600 bit/baud -->  0.24kB/s
Modem 9600/2400         -->  0.96kB/s
Modem 14.4 (V.32 bis)   -->  1.4 kB/s
Modem 56k (V.90)        -->  6.6 kB/s

ISDN BRI                -->   16 kB/s
IDSL                    -->   18 kB/s
SDSL                    -->  290 kB/s

ADSL                    -->  1024/  128 kB/s
ADSL2+                  -->  3072/  448 kB/s
DOCSIS v1               -->  4750/ 1125 kB/s
EuroDOCSIS v1           -->  6000/ 1125 kB/s
DOCSIS v2               -->  4750/ 3375 kB/s
EuroDOCSIS v2           -->  6000/ 3375 kB/s
DOCSIS v3               --> 20000/15000 kB/s
EuroDOCSIS v3           --> 25000/15000 kB/s

ter info : GPON FTTH    --> +300000 kB/s
```

Chapter 16. draadloos

Table of Contents

Een inleiding op draadloze netwerken en protoocols.

16.1. wireless

Wireless is veel trager dan bijvoorbeeld utp kabels, maar meestal wel snel genoeg (sneller dus) dan gangbare thuis-internet verbindingen.

Wireless ofte draadloos wil zeggen dat we alles bekijken wat golven van energie gebruikt om (data) te communiceren. Eerst eens kijken wat een golf is.

Een golf (voor zover we die gebruiken bij datacommunicatie) beweegt zich voort in de lucht (of in een ander medium) met een bepaalde frequentie en amplitude. We laten voor het gemak de lichtgolven en elektromagnetische golven even buiten beschouwing.

16.2. frequentie

Frequentie wordt uitgedrukt in **Hertz**. Een golf met een frequentie van 440 Hertz ontvang je 440 keer in zijn geheel per seconde. Tussen haakjes, 440Hz is de basisfrequentie voor het stemmen van instrumenten (ook wel kamertoon genoemd).

De meeste golven in deze cursus hebben echter een veel hogere frequentie, daarom gebruiken we onder andere kHz, MHz, GHz en THz (voor elke orde van 1000).

Heinrich Hertz (1857-02-27 - 1894-01-01) was een Hamburgs natuurkundige die vooral bezig was met elektromagnetisme en lichtgolven. Hij was de eerste om het bestaan van **VHF** en **UHF** aan te tonen.

16.3. spectrum

UHF en VHF zijn onderdelen van het volledige radiospectrum, gaande van 3 Hz tot 300 Ghz.

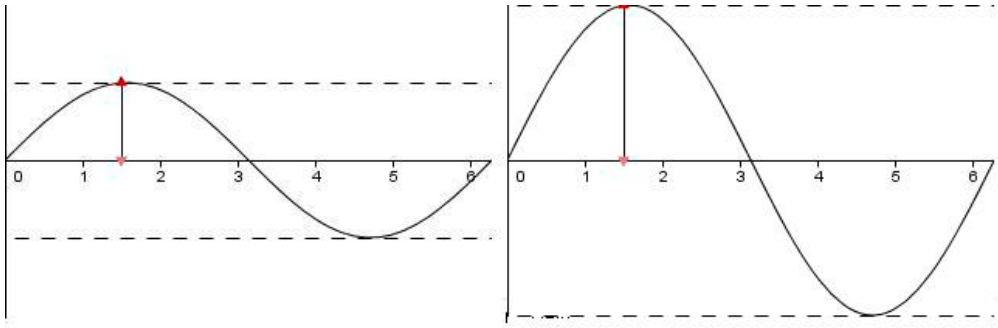
`http://nl.wikipedia.org/wiki/Radiospectrum`

De AM-radio uitzendingen (de langegolf) zitten bijvoorbeeld in de LF band (Low Frequency). FM en (analoge)TV uitzendingen gebruiken de VHF (30-300Mhz). Een toontje hoger zitten UHF-TV, GSM, onze microgolfoven, wireless LAN en Bluetooth. UHF golven zijn tussen de 10 centimeter en 1 meter lang, en overbruggen moeiteloos afstanden tot 100km. UHF wordt ook opgevangen door satellietschotel antennes.

Het spectrum is bepaald door de **ITU** (http://www.itu.int).

16.4. amplitude

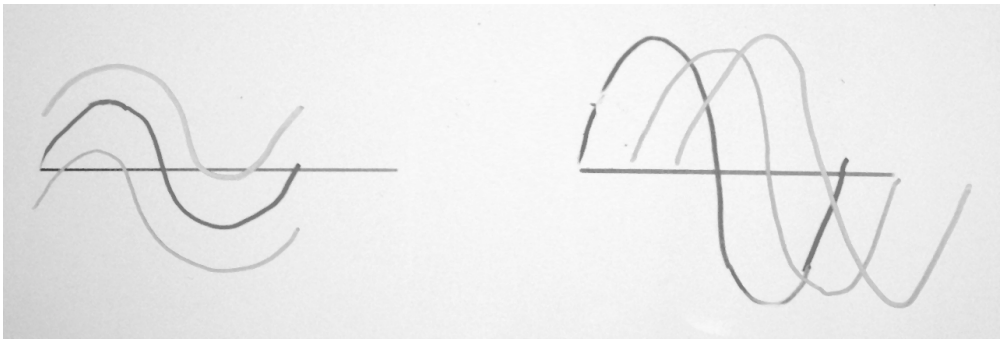
Amplitude is de grootte van de golf.



Een geluidsgolf is bijvoorbeeld sterker (of groter) als hij vertrekt bij uw mond, dan wanneer hij aankomt bij iemands oor (toch als je zonder versterkers in een open ruimte spreekt). Bij geluidsgolven wordt deze amplitude gemeten als luchtdruk (in **pascal** dus).

16.5. fase

De fase van een golf kan uitgedrukt worden in graden, waarbij 360 graden gelijk is aan 1 golflengte. Verschillende golven kunnen met elkaar in fase zijn, of niet.



Sommige mensen zetten bass-luidsprekers per ongeluk in tegenfase.

16.6. golflengte

De **golflengte** is de lengte in meter van een golf, te meten van top tot top (of eender welk ander puntenkoppel met dezelfde fase).

16.7. IEEE 802.11

De **IEEE 802.11** standaarden beschrijven draadloze radiogolf communicatie voor computers in een WLAN (wireless local area network). De gebruikte frequenties zijn 2.4, 3.6 en 5GHz.

De meest gebruikte van deze standaarden zijn de 802.11a, 802.11b en 802.11g.

16.7.1. 802.11a

De **IEEE 802.11a** standaard dateert al uit 1999 en werkt op de 5GHz band. De theoretische maximum bandbreedte die je met deze standaard haalt, is 54Mbit/s (net zoals modems wordt er teruggevallen op lagere snelheden bij het handshaken).

Deze standaard gebruikt 12 kanalen.

16.7.2. 802.11b

De **IEEE 802.11b** standaard (ook uit 1999) is beperkt tot maximaal 11Mbit/s, maar is wel al tien jaar beschikbaar in de praktijk. Bijkomend voordeel op de 802.11a is dat deze de 2.4GHz band gebruikt i.p.v. de 5GHz (deze laatste wordt makkelijker geabsorbeerd door muren).

Nadeel is dan weer dat de 2.4GHz band een vrije band is, er is dus interferentie mogelijk met andere draadloze toestellen (en ook met microgolfovens).

16.7.3. 802.11g

In 2003 kwam men op de proppen met de **IEE 802.11g** standaard. Deze werkt ook in het 2.4GHz spectrum, maar wel aan maximaal 54Mbit (in de praktijk 22Mbit bruikbare data).

Al sinds januari 2003 (dus nog voordat de standaard er was) zijn er triband (ondersteuning voor a,b en g) producten op de markt.

16.7.4. 802.11n

Sinds eind 2009 is er een nieuwe standaard, de **802.11n** met een theoretische bandbreedte van 600Mbit/s. De toestellen zijn al wel sinds twee jaar te koop.

`http://en.wikipedia.org/wiki/IEEE_802.11n-2009`

16.7.5. kanalen

Een band zoals bijvoorbeeld de 2.4GHz band wordt de een IEEE 802.11 standaard steeds onderverdeeld in **kanalen**. De 2.4Ghz band beschikt eigenlijk over alle frequenties van 2.400 Ghz tot en met 2.499 GHz. Vanaf het eerste kanaal op 2.412 GHz is er om de 5Mhz een nieuw kanaal. Alle kanalen zijn 22MHz breed, er is dus overlapping.

`http://en.wikipedia.org/wiki/List_of_WLAN_channels`

Het is aan te raden om enkel de kanalen 1, 6 en 11 te gebruiken als het bereik van de access points elkaar overlapt. Het gebruik van de kanalen 1, 4, 8 en 11 kan voor problemen zorgen (als je ze onverstandig plaatst).

`http://www.cisco.com/en/US/docs/wireless/technology/channel/deployment/guide/Channel.html`

16.7.6. bonding

Producten die kanalen samen gebruiken (bonding) om 108Mbit aan te bieden, zijn niet beschreven in een standaard en zijn zeker niet met alle draadloze clients compatibel.

16.7.7. bandbreedte?

In de praktijk wordt door de asynchroniteit van deze standaarden en de overhead van de lagen een veel lagere doorvoer van data gehaald dan de geadverteerde 54Mbit (of 11Mbit).

16.8. WiMAX

WiMAX is de marketing naam voor de **IEEE 802.16** standaard om mobiele draadloze toegang te voorzien met een bereik van enkele kilometer en een

bandbreedte tussen 1 en 20Mbit. Steden zoals Leuven, Gent en Aalst beschikken over een WiMAX netwerk (van Clearwire).

Praktijkervaring leert dat de technologie nog in de kinderschoenen staat (of dat clearwire het aantal stations duidelijk onderschat). Er zijn (of waren) plannen bij Clearwire om heel België te dekken met WiMAX (maar vandaag is er nog geen verbinding in Antwerpen bijvoorbeeld).

16.9. Wi-fi

Dit is een handelsmerk, meestal gebruikt voor WLAN (Wireless LAN) toestellen.

16.10. Access Point

Een **Wireless Access Point** is een toestel dat draadloze verbindingen toelaat van client devices (wireless pc-cards etc). Meestal is de **access point** verbonden met een bekabeld netwerk.

Deze toestellen kunnen meestal verschillende draadloze WLAN (of Bluetooth) standaarden aan, en kunnen een kanaal kiezen.

16.11. hotspot

Een **hotspot** is een plaats waar draadloos internet beschikbaar is. Zowel laptops, netbooks als pda en smartphones kunnen gebruik maken van hotspots.

Beveiliging van hotspots (of wireless in het algemeen) is een heel groot onderwerp...

16.12. draadloze beveiliging

Het grote verschil met bekabelde netwerken, is dat je geen firewall in de lucht kan hangen om je draadloze netwerk te beveiligen.

16.12.1. per ongeluk

Heel wat software zoekt automatisch een netwerk, heel wat draadloze toestellen (modems) staan standaard open voor deze automatische zoekopdrachten. Het is dus perfect mogelijk dat je per ongeluk op een ander zijn draadloos netwerk surft.

16.12.2. MAC beveiliging

Je kan de meeste **access points** beveiligen door enkel bepaalde MAC-adressen toe te laten. Maar zoals jullie weten is het MAC-adres een essentieel onderdeel van elk ethernet frame, en door elke sniffer gewoon te lezen.

MAC filtering beschermt je wel tegen 'per ongeluk'.

16.12.3. IP beveiliging

Je kan de draadloze DHCP server afzetten, en enkel werken met (enkele) toegelaten vaste ip-adressen.

16.12.4. WEP

WEP staat voor **Wired Equivalency Privacy/Protocol** en is een verouderde standaard om draadloze netwerken te beveiligen.

De WEP standaard dateert uit 1997, sinds 2001 zijn er tools te vinden om WEP te kraken. Als reactie hierop werd WPA ontworpen.

WEP bestaat (of bestond) in een 40bit en een 128bit standaard (danku USA). Een grotere sleutel wil zeggen dat er meer pakketjes moeten gesnift worden alvorens je de key kan berekenen (kraken). Een goeie crack-tool genereert zelf binnen enkele minuten de nodige trafiek om de WEP-sleutel te achterhalen. Sinds 2007 is publiek aangetoond dat dit ook binnen de enkele seconden kan.

`http://eprint.iacr.org/2007/120.pdf`

16.12.5. WPA

WPA staat voor **Wi-Fi Protected Access** en is ontworpen als reactie op de zwakke WEP beveiliging. WPA is ondertussen zelf vervangen door WPA2. WPA beveiliging met een simpele passphrase (pre-shared key) kan binnen de minuut gekraakt worden. WPA2 (dat AES gebruikt) is wel veilig als je een goeie 64-hex string gebruikt.

16.12.6. ramen en muren

Om te verhinderen dat je (corporate) netwerk ook op de parking beschikbaar is, kan je speciale verf op de muur plaatsen (of een film op de ruiten) om radiogolven bewust te absorberen.

16.13. wardriving

wardriving is het zoeken naar draadloze (onbeveiligde) netwerken met een laptop of netbook, meestal al rijdend. Meestal worden tools zoals **kismet** of **kismac** gebruikt, soms ook **netstumbler**, maar er bestaan heel wat meer tools. **wardriving** brengt deze netwerken in kaart (door te luisteren). Het effectief gebruiken van (onbeveiligde) draadloze netwerken behoort niet tot het **wardriven**. (netstumbler gaat dus iets verder dan nodig om netwerken in kaart te brengen)

16.14. bluetooth

Bluetooth is een draadloos protocol dat gebruikt maakt van een **master** om te communiceren met een **slave**. Een **bluetooth** toestel kan een verbinding hebben met maximaal zeven **slaves**. Enkel de **master** kan data sturen (of data opvragen).

Heel wat toestellen hebben standaard **bluetooth** geactiveerd. Scannen naar **bluetooth** toestellen in je woonkamer kan wel eens verrassende resulaten opleveren als er toevallig mensen passeren op straat:

```
root@mac:~# hcitool scan
Scanning ...
00:22:XX:XX:XX:XX HTC Hero grijs
00:16:53:0B:1C:75 Mercedes
00:16:53:08:EB:6E Julie
00:16:X8:4X:52:95 W810i
00:16:XX:XX:XX:8X n/a
00:16:XX:XX:XX:8X Steven Nokia 6021
00:19:4X:75:85:53 Johnneke
00:1X:XX:X2:9X:7X Nokia 6021
00:21:XX:XX:XX:XX Nokia 3120 classic
00:26:5X:7X:2X:88 David
18:86:XX:18:XX:39 Nokia 6300
X8:7X:33:XX:8X:X2 Nokia 6303 classic
X8:7X:33:XX:93:X2 Nokia 6303 classic
```

Chapter 17. VPN

Table of Contents

Dit hoofdstuk gaat over **vpn** an andere manieren om een verbinding te leggen met een netwerk of met internet.

17.1. Verbinden met internet

Je kan je LAN rechtstreeks verbinden met internet door een **router** te plaatsen tussen de LAN en internet.

Als deze router **snat** is, dan heb je in de LAN private ip-adressen en maakt je LAN geen deel uit van het internet (de ip adressen zijn verborgen).

Je kan ook verschillende protocols (typisch http en https) via een **proxy server** toegang geven tot internet. Een proxy server is in zijn oorsprokelijke essentie een **cache** van het internet (of het www). Tegenwoordig zitten er ook filters op proxy servers. Een proxy server kan in je LAN staan, of zelf een (snat) router zijn.

Grote organisaties hebben een **dmz** met een inner en een outer firewall om hun LAN op een veilige manier te scheiden van het boze-internet-vol-hackers-en-crackers.

Van thuis uit kan je op het internet via **dial-up**, **isdn**, **dsl**, **docsis**, **ftth**(half miljoen in Nederland (200Mbit), 10 miljoen in USA, binnen 2 jaar 40 miljoen in China, proefprojecten in Belgie in Sint-Truiden) en andere.

17.2. PPP

In de jaren 90 maakten ISP's gebruik van **ppp** om dial-up internet toegang te voorzien. Maar PPP kan veel meer, het laat toe om IP pakketten te versturen over het pstn, seriele kabels, radio, glasvezel en meer. Daarenboven kan PPP ook dienen om SNA, IPX, Appeltalk, NetBEUI en andere netwerklaag protocols te gebruiken in de plaats van IP.

`http://en.wikipedia.org/wiki/Point-to-point_protocol`

PPP zit op laag 2 en ondersteunt authenticatie (PAP, CHAP), versleuteling, compressie en multilink.

17.3. VPN

Een **vpn** is een verbinding vanuit een LAN (of van thuis uit) naar de 'afgeschermde' LAN van een organisatie, en dit via een bestaand netwerk (vandaag meestal het internet).

Protocols zoals PPTP (Microsoft), L2F(Cisco) en L2TP(open source) zijn specifiek gemaakt voor dit doel.

17.4. L2TP

Het **l2tp** (Layer 2 Tunneling Protocol) maakt gebruik van IpSec en PPP om een beveiligde tunnel te maken over een bestaand netwerk. Dit laatste is vandaag vaak het internet, maar het kan ook een ander IP-netwerk zijn, of zelfs X-25, Frame Relay

en ATM. Omdat l2tp een tunnel maakt over deze WAN protocols wordt l2tp zelf ook gezien als een WAN protocol.

L2TP maakt gebruik van IpSec voor versleuteling en authenticatie.

17.5. IpSec

IpSec is een onderdeel van ipv6 standaard en 'backported' naar ipv4 om versleutelde tunnels met authenticatie te maken. IpSec ondersteunt ook het **onderhandelen** van methodes en sleutels om een beveiligde verbinding op te zetten.

IpSec zit op de internetlaag en heeft dus geen enkele invloed op (de configuratie van) applicaties. Dit in tegenstelling tot TLS en SSL (denk https) en ssh (putty) die zich op de applicatielaag bevinden.

Wanneer twee LAN's via IpSec vebonden zijn over het internet, dan zijn vanzelf **alle** transfer tussen alle applicatie op die twee LAN's versleuteld en authenticated.

IpSec kan werken in **tunnel mode** of niet. Het kan dus zowel een individuele computer verbinden met een andere computer, als twee routers op verschillende LAN's.

17.6. PPTP

Microsoft heeft lang gegokt op **pptp** en stak dit standaard in alle Windows versies vanaf Win95 OSR2 (wel beperkt tot twee verbindingen).

PPTP maakt gebruik van GRE (Cisco Generic Routing Encapsulation) om PPP packetten te encapsulaten in IP. Daarbinnen kon dus alles ziten. Nadeel van PPTP is dat het werkt met DES (single, niet triple) voor MS-CHAP authenticatie. In Windows 2008 kan je ook MS-CHAPv2 gebruiken met TLS beveiliging.

17.7. GRE

Naast TCP en UDP kan je op laag 4 ook **GRE** (Genreal Routing Encapsulation) vinden. 'General' omdat er anders veel encapsualtie implementaties moeten zijn (ip, ipx, appletalk, sna, ...) tot de tweede macht. Vandaar dat Cisco een algemeen protocol maakte om laag 3 in laag 3 te tunnelen.

```
IP -- GRE -- IP
IP -- GRE -- IPX
```

17.8. SSL

SSL (Secure Socket Layer), ontwikkeld door Netscape, is een veel gebruikt tunneling protocol inde transportlaag. Denk maar aan https bijvoorbeeld.

Omdat andere bedrijven enkele terkortkomingen aan SSL verbeterden, werd in 1996 bij de standaardisatie gekozen om na SSLv3 dit TLS (Transport Layer Security) te noemen.

SSL kan werken met RSA voor sleutels; DES, 3DES, voor encryptie en zowel SHA als MD5 hashes voor controle. Voordat SSL data kan verzenden is worden er 9 handshake pakketjes uitgewisseld tussen client en server.

17.9. WPS

http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup#Security

Daniel wees me in een mail op **WPS** (Wi-fi Protected Setup) en de eenvoud om wireless **wpa2** toch te kraken als WPS aan staat. Hij schreef hetvolgende:

Toen ik na de laatste les netwerken op zoek was achter Kismet kwam ik via wat surfen terecht op deze interessante info:

WPA is blijkbaar zeer goede beveiliging voor wifi netwerken maar er bestaat een technologie op zowat alle wifi toestellen genaamd WPS die toelaat om zonder de WPA-key in te voeren toestellen op het netwerk te laten inloggen.

Deze WPS maakt gebruikt van een Pin code bestaande uit 8 cijfers, waarbij het achtste cijfer een hash is van de eerste 7. Deze is dan ook veel minder veilig dan WPA, het is namelijk mogelijk om de WPS-Pin te kraken met nauwelijks 11000 mogelijke combinaties. Uit deze WPS-Pin kan dan de WPA-key afgeleid worden. WPS staat standaard aan op zowat elke ISP-box.

Ik besloot dit dan maar eens te proberen (op mijn eigen Telenet-box uiteraard) en zowaar: ik had m'n WPA-key na een uur en tien minuten. Dit met een standaard Telenet-paswoord van 12 random karakters, wat normaal gezien perfect veilig zou moeten zijn, op een zeer recente Telenet-box. De box heeft een lockout van 5 minuten na te veel attempts, maar zelfs met deze lockout zou je alle 11000 combinaties kunnen proberen in minder dan 48 uur.