

## Gebruik van draadloze netwerken aan de K.U.Leuven

Draadloze netwerken worden steeds populairder. Meer en meer gebruikers (zowel personeel als studenten) beschikken immers over een draagbare computer of PDA. Deze gebruikers zijn vragende partij voor draadloze netwerk oplossingen, met als belangrijkste voordelen een verhoogde mobiliteit en gebruiksgemak. Ook aan de K.U.Leuven is er een toenemende vraag naar draadloze netwerken, bv. voor leslokalen, vergaderzalen, conferentie -ruimten, bibliotheken, alma's, enz.

De aard van draadloze netwerken zorgt echter voor specifieke beveiligingsproblemen, waar een oplossing voor gevonden dient te worden. Belangrijkste probleempunt is het gebruikte transmissie -medium, dat zich uitermate leent voor af luisterpraktijken. Verder is er de zwakke beveiliging voorzien in de bestaande 802.11 standaarden voor draadloze netwerken, nl. het WEP encryptie protocol. Ongelukkigerwijs is aangetoond dat dit protocol zware gebreken vertoont, en via publiek verkrijgbare software tools (zoals *AirSnort*) makkelijk te kraken is.

Dit document gaat in op verschillende types van toepassing voor draadloze netwerken, en toont aan hoe deze binnen de K.U.Leuven context op een veilige manier toegepast kunnen worden (rekening houdend met de zwakke punten in de bestaande standaarden). We starten met een kort overzicht van de gebruikte technologie, en de vereisten waaraan een wireless access point moet voldoen. Hierna zoomen we in op de toepassingsgebieden, en stellen we oplossingen voor die een veilig gebruik van draadloze netwerktechnologie moet toelaten.

### ***Draadloze netwerk technologie***

Op dit ogenblik zijn er twee standaarden voor draadloze communicatie, nl.

- 802.11b            11 Mbps, 2.4 Ghz
- 802.11a            54 Mbps, 5 Ghz

De 802.11b standaard is de meest gebruikte, en wordt door courante wireless access points ondersteund. De 802.11a standaard ondersteunt hogere bandbreedten, maar dit is gekoppeld aan een kleiner bereik (m.a.w. het bereik van een 802.11a access point is kleiner dan dit van een 802.11b access point). Verder mogen 802.11a access points enkel binnenshuis gebruikt worden.

Naast deze twee standaarden is er een nieuwe standaard in ontwikkeling (802.11g), die naar verwachting eind 2003 gefinaliseerd zal zijn. De 802.11g standaard is backward compatible met de 802.11b standaard, maar voorziet eveneens in hogere snelheden tot 54Mbps. Deze standaard zal tevens werken in de publieke frekwentieband van 2.4Ghz (m.a.w. outdoor toepassingen zijn hier wel toegelaten).

Gezien de komst van de 802.11g standaard is het onverstandig om te investeren in 802.11a technologie (deze zal wellicht vrij snel van de markt verdwijnen). Verder is het aangewezen om bij aankoop van nieuwe access points erop toe te zien dat er een upgrade pad bestaat van 802.11b naar 802.11g technologie (bij de betere access points kan dit mits vervanging van de radio module en/of een firmware upgrade).

Omwille van de zwakke beveiliging van het WEP protocol zijn vele leveranciers voor de dag gekomen met eigen, niet-standaard, beveiligingsmechanismen. Deze niet-standaard mechanismen vereisen meestal dat leverancier-specifieke drivers en/of client-software gebruikt worden. Het lijkt ons onverstandig te steunen op dergelijke niet-standaard mechanismen. Een mogelijke uitzondering vormen punt-tot-punt verbindingen – hier gaat het om pure backbone verbindingen, waar een eventueel gebruik van leverancier-specifieke oplossingen geen impact heeft op eindgebruikers.

Vele leveranciers voorzien ook allerlei snuffjes op hun access points, zoals een ingebouwde DHCP server, ingebouwde adresvertaler, enz. Dergelijke features zullen we niet gebruiken in onze scenarios. Onze enige vereiste op dit vlak is dat het access point zich gedraagt als een normale repeater. Verder dienen de access points te voorzien in standaard *enterprise features*, zoals: bescherming van de beheer-toegang via access-list en paswoord, logging faciliteiten via syslog, tijd synchronisatie via ntp, monitoring faciliteiten via snmp.

## **Toepassingen voor draadloze netwerken**

### **Wireless access point (KULeuvenNet)**

Een eerste type toepassing zijn de *wireless access points*. De bedoeling hier is om eindgebruikers (die beschikken over een draagbare computer met wireless lan kaart) aan te sluiten op het K.U.Leuven netwerk en Internet. Uit gesprekken met gebruikers komen een aantal typische scenarios naar voren:

- Tijdelijke opstellingen tijdens congressen, conferenties, enz. Bedoeling is om de deelnemers de mogelijkheid te bieden om via een draagbare computer het Internet te raadplegen. Deze draadloze netwerktoegang wordt voorzien in aanvulling op een mail-room.
- Permanente opstellingen in burelen, vergaderzalen, auditoria en publieke ruimten. K.U.Leuven gebruikers moeten hier via hun draagbare computer toegang hebben tot het K.U.Leuven netwerk (uiteraard op een veilige manier). Verder moet het mogelijk zijn dat bezoekers deze draadloze netwerktoegang kunnen gebruiken om toegang te krijgen tot het Internet (mits toelating van K.U.Leuven).
- Opstellingen voor specifieke doeleinden. Een concreet voorbeeld is de communicatie met mobiele robots via een draadloos netwerk. Het gaat hier typisch om toepassingen waar de *client* niet geïmplementeerd is op een standaard personal computer.

In eerste instantie kan er dus een onderscheid gemaakt worden tussen tijdelijke en permanente opstellingen.

- Bij tijdelijke opstellingen (congressen, conferenties) lijkt het aangewezen om het gebruiksgemak te laten primeren. Typische gebruikers hier zijn over het algemeen geen informatica-specialisten, en omwille van het tijdelijk karakter van deze opstellingen is het aangewezen om eventuele problemen zoveel mogelijk te vermijden. Een mogelijkheid is om vrijelijk Internet toegang te voorzien. Toegang tot Internet is dan anoniem, maar de kans op misbruiken is beperkt – het gaat immers om een tijdelijke opstelling (van enkele dagen tot een week).
- Bij permanente opstellingen hebben we een andere situatie – hier staat het wireless access point permanent opgesteld, en is de kans op misbruiken dus groter. Een toegangscontrole-

systeem is hier aangewezen (zie verder). Bij dit toegangscontrolesysteem moeten voorzieningen aanwezig zijn om ook niet-K.U.Leuven gebruikers te authenticeren.

Verder maken we best ook onderscheid tussen toegang tot Internet en toegang tot KULeuvenNet. Gezien het gevaar voor sniffing is het aangewezen om voor toegang tot KULeuvenNet enkel beveiligde verbindingen te gebruiken. In geen geval mogen authenticaties (login/paswoord) onversleuteld over het wireless netwerk verstuurd worden. Voor de toegang tot Internet zou het best zijn dat courante VPN oplossingen ondersteund worden (dit om bezoekers de mogelijkheid te geven om via een VPN toepassing aan te sluiten op hun thuisbasis).

Opstellingen voor speciale doeleinden (zoals het hoger vermelde controle-netwerk voor mobiele robots) dienen geval per geval onderzocht te worden. We stellen voor dat de beveiliging hiervan door KULeuvenNet gekeurd wordt (in opdracht van de K.U.Leuven beveiligingscommissie).

### **Wireless access point (thuisgebruik)**

Voor thuisgebruik is de kostprijs van een wireless access point een belangrijke factor. Het is hier belangrijk dat eindgebruikers zich bewust zijn van de gevaren die deze technologie met zich meebrengt. De meeste access points voor thuisgebruik voorzien in hun standaard instellingen immers geen beveiliging (dit betekent dat een buur probleemloos de draadloze netwerktoegang kan misbruiken – zonder dat de thuisgebruiker zich hiervan bewust is).

Gezien meer en meer personeelsleden via hun thuiscomputer toegang wensen tot het K.U.Leuven netwerk (via een VPN oplossing), is het aan te bevelen dat de K.U.Leuven richtlijnen opstelt voor een minimale beveiliging van draadloze thuisnetwerken. Met het oog op gebruikers-ondersteuning is het tevens aan te bevelen dat LUDIT via de PC-shop standaard oplossingen aanbiedt voor een draadloos thuisnetwerk.

### **Wireless bridge (KULeuvenNet backbone)**

Een ander type toepassing is de *wireless bridge*. De bedoeling hier is om punt-tot-punt verbindingen te realiseren via draadloze netwerktechnologie. Binnen KULeuvenNet wensen we dit soort technologie te gebruiken voor het verlengen van Ethernet segmenten via een draadloze verbinding (bv. voor het voorzien van backup verbindingen).

Het gaat hier dus om backbone verbindingen, waar potentieel gevoelige gegevens over getransporteerd worden. Beveiliging is hier dus cruciaal. Omdat bij dit type verbindingen geen eindgebruikers betrokken zijn, laten we de mogelijkheid open om gebruik te maken van leverancier-specifieke beveiligingsoplossingen (bij gebrek aan bruikbare standaarden).

Voor wireless bridges stellen we volgende vereisten:

- Ondersteuning voor vlans via het 802.1q multiplexing protocol
- Degelijke encryptie op de wireless link (via leverancier-specifieke oplossing, via standaard oplossing wanneer deze beschikbaar komt)
- Mag enkel geïnstalleerd worden door KULeuvenNet

## **Draadloze netwerken binnen de K.U.Leuven**

### **Richtlijnen**

Voor gebruik aan de K.U.Leuven dienen *enterprise class* access points ingezet te worden. Dit betekent dat het access point moet voldoen aan de volgende voorwaarden:

- Bescherming van de beheertoegang via access-lists en paswoord
- Logging faciliteiten via syslog
- Tijd synchronizatie via het NTP protocol
- Monitoring faciliteiten via het SNMP protocol

Access points worden aangesloten op het bedrade netwerk *buiten* de centrale K.U.Leuven firewall. Er wordt tevens een afzonderlijk IP subnet voorzien voor het draadloze netwerk. Installatie van access points mag enkel gebeuren met medewerking van KULeuvenNet. Toegang tot het interne K.U.Leuven netwerk is beperkt tot volgende protocols:

- http en https voor webtoegang
- smtp (e-mail) toegang tot publieke smtp servers op het K.U.Leuven netwerk (in principe enkel via de centrale anti-virus cluster, uitzonderingen zijn mogelijk indien goedgekeurd door de beveiligingscommissie).
- pop en imap (e-mail) toegang via ssl
- ssh toegang
- vpn toegang via de centrale vpn-cluster (gebruik van een eigen vpn-oplossing is mogelijk mits goedkeuring door de beveiligingscommissie).

Toegang tot het interne K.U.Leuven netwerk is dus beperkt tot een aantal beveiligde toepassingen. Een volledige toegang tot KULeuvenNet (bv. voor gebruik van SAP, toegang tot netwerkschijven) is enkel mogelijk via VPN. Toegang via het draadloze netwerk naar Internet is onderworpen aan dezelfde beperkingen die gelden voor andere netwerken binnen KULeuven (o.a. blokkering van filesharing programma's, verplicht gebruik van de centrale anti-viruscluster, enz).

Toegang tot het draadloze netwerk dient gecontroleerd te worden via een login mechanisme. M.a.w. enkel geauthenticeerde gebruikers krijgen toegang tot het draadloze netwerk. De authenticatie van gebruikers dient op een veilige manier te gebeuren.

### **Aanbevelingen**

Als standaardoplossing stelt KULeuvenNet momenteel een Cisco Aironet 1100 of 1200 enterprise class access point voor. In dit geval biedt KULeuvenNet tevens de nodige ondersteuning voor configuratie en installatie van het draadloze netwerk. Wanneer een afdeling opteert voor een afwijkend type access point (dat tevens voldoet aan de richtlijnen), kan KULeuvenNet geen ondersteuning bieden bij configuratie en installatie. In dit geval dient de afdeling eveneens aan te tonen dat de configuratie van het access point voldoet aan de richtlijnen.

KULeuvenNet biedt tevens een standaard oplossing voor een gecontroleerde toegang tot het draadloze netwerk (gebaseerd op de bestaande KotNet login procedure). Afdelingen mogen een eigen netwerk login systeem implementeren, mits grondige motivatie, en op voorwaarde dat dit goedgekeurd wordt door de beveiligingscommissie.

Het standaard netwerk login mechanisme wordt in detail besproken in appendix A.

## **Draadloze netwerken voor thuisgebruik**

### **Richtlijnen**

Wanneer het draadloze thuisnetwerk gebruikt wordt om via VPN toegang te krijgen tot het interne K.U.Leuven netwerk, dienen volgende richtlijnen gevolgd te worden:

- Gebruik van een niet voor de hand liggende SSID (dit is een string die het draadloze netwerk identificeert). Deze SSID mag niet door het access point verspreid worden (non-broadcast SSID).
- Gebruik van een niet voor de hand liggende WEP encryptie sleutel (bij voorkeur 128 bit WEP of hoger).
- Toegang tot de configuratie-interface van het access point dient beschermd te worden met een paswoord (verschillend van het *factory-default* paswoord).

Wanneer het access point gebruikt wordt bij een multi-user KotNet aansluiting (voor aansluiting van meerdere studenten), is het gebruik van adresvertaling op het access point (NAT) verboden.

### **Aanbevelingen**

LUDIT zal via de PC-shop een standaard access point voor thuisgebruik aanbieden. Hierbij zal tevens een gebruiksgids aangeboden worden voor de configuratie van SSID en WEP encryptiesleutel.

### **Conclusie**

Het gebruik van draadloze netwerken stelt specifieke beveiligingsproblemen, eigen aan het medium. De in dit document voorgestelde richtlijnen laten een veilig gebruik van deze technologie aan de K.U.Leuven toe.

- Voor gebruik binnen de K.U.Leuven stelt LUDIT/KULeuvenNet standaard oplossingen voor, zowel wat betreft het access point als wat betreft de gecontroleerde toegang tot het draadloze netwerk. Er wordt sterk aangeraden om, waar mogelijk, van deze standaard oplossingen gebruik te maken.  
Afdelingen kunnen, indien gewenst, hun eigen draadloze netwerkoplossing uitwerken, mits deze op technisch- en beveiligingsvlak voldoet aan de richtlijnen (de beoordeling hiervan gebeurt door KULeuvenNet, in opdracht van de beveiligingscommissie – bij betwisting zal de beveiligingscommissie een uitspraak doen).
- Voor thuisgebruik wordt een standaard oplossing aangeboden door LUDIT (via de PC-shop). Dit is de enige oplossing die door LUDIT wordt ondersteund. Thuisgebruikers wordt sterk aanbevolen om de door LUDIT aangeboden oplossing te gebruiken.

## Appendix A - Netwerk login voor wireless access points

Bij inzetten van wireless access points is het belangrijk voor ogen te houden dat deze bedoeld zijn voor de modale eindgebruiker (weze het een K.U.Leuven gebruiker of een bezoeker). M.a.w. toegang tot het netwerk moet zo eenvoudig mogelijk zijn – complexe oplossingen gebaseerd op instellen van WEP encryptiesleutels, SSID's, registratie van MAC-adressen, enz. zijn om deze redenen te verwerpen. Binnen KULeuvenNet hebben we reeds ervaring met een gebruiksvriendelijk web-gebaseerd toegangscontrolesysteem, nl. de KotNet login.

We voorzien daarom voor draadloze netwerken een netwerk login systeem, gebaseerd op het bestaande KotNet login systeem.

- Het draadloze netwerk is vrij toegankelijk (zonder WEP-encryptie, met een publiek beschikbare SSID). Elke gebruiker kan dan ook probleemloos aansluiten op het wireless access point. Vanuit het netwerk wordt via DHCP een ip adres aan de machine van de gebruiker toegekend.
- Initieel heeft het ip adres van de gebruiker enkel toegang tot een beperkt aantal systemen (met name deze systemen die de netwerk-login ondersteunen). Om de volledige netwerk toegang te activeren, moet de gebruiker via een beveiligde webpagina inloggen met zijn/haar intranet userid en paswoord. Na een geslaagde authenticatie wordt het netwerk voor deze gebruiker toegankelijk gemaakt.
- Na login is de toegang tot Internet vrij (onderworpen aan dezelfde beperkingen als andere KotNet aansluitingen).
- Na login is de toegang tot KULeuvenNet beperkt tot volgende protocols: *http/https* naar geregistreerde K.U.Leuven webservers, *imap/pop* via *ssl*, *smtp* naar de centrale anti-virus cluster. Verder worden ook *ssh* en *ipsec* toegelaten. M.a.w. gebruikers kunnen websites raadplegen en hun e-mail consulteren. Is een meer uitgebreide toegang tot het K.U.Leuven netwerk nodig (bv. SAP, toegang tot netwerk bestandensysteem), dan dient men gebruik te maken van de centrale VPN infrastructuur.

Met bovenstaand login-systeem heeft men na authenticatie vrije toegang tot Internet (binnen de geldende KotNet beperkingen), en is de toegang tot het interne K.U.Leuven netwerk beperkt tot een aantal veilige toepassingen. Is een volledige toegang tot het interne K.U.Leuven netwerk nodig, dan kan dit gerealiseerd worden via een VPN oplossing.

### Wireless netwerk toegang voor bezoekers

Het hierboven voorgestelde netwerk-login mechanisme veronderstelt dat elke gebruiker beschikt over een userid en paswoord. Dit zal echter niet altijd het geval zijn. Het is niet de bedoeling om al deze tijdelijke gebruikers rechten te geven op het K.U.Leuven netwerk – we wensen hier immers geen accounts die toegang geven tot K.U.Leuven informatie, wel accounts die een netwerk login mogelijk maken.

- **Tijdelijke accounts**  
Een oplossing is om *tijdelijke accounts* te voorzien, die door geregistreerde beheerders aangemaakt kunnen worden. Deze geregistreerde beheerders omvatten bv. de lokale netwerkbeheerders en campus services. Het gaat hier om strikt tijdelijke accounts, met een

bepaalde geldigheidsduur. Doelpubliek voor dergelijke accounts zijn gasten, die behoefte hebben aan netwerktoegang, maar die geen toegang mogen hebben tot de interne toepassingen aan de K.U.Leuven (bv. SAP, Toledo, enz).

Implementatie van dergelijke tijdelijke accounts vergt een uitbreiding van de bestaande registratieprocedures via CWIS. Het moet namelijk mogelijk zijn om accounts te koppelen aan een gebruikerscategorie. Deze categorie bepaalt dan de toegangsrechten tot interne K.U.Leuven toepassingen. Dergelijke uitbreiding op de CWIS registratieprocedures wordt momenteel binnen LUDIT onderzocht.

- **Netwerk accounts**

In afwachting van het beschikbaar komen van registratieprocedures voor tijdelijke accounts, voorziet KULeuvenNet in *netwerk accounts* voor draadloze netwerken. Hierbij wordt een login naam gekoppeld met elk geïnstalleerd draadloos netwerk. Bij deze netwerk login naam hoort een *paswoord van de dag*, dat toegang verleent tot het draadloze netwerk.

De beheerder van het draadloze netwerk (geregistreerd bij KULeuvenNet) kan via een beveiligde webpagina een lijst met dag-paswoorden opvragen voor zijn draadloos netwerk.

Om misbruik tegen te gaan kan een beheerder enkel de dag-paswoorden voor de volgende 10 dagen opvragen.

Dit systeem van tijdelijke/netwerk accounts is interessant om externe bezoekers netwerktoegang te geven via een permanent opgesteld draadloos netwerk. We denken hier bv. aan gastdocenten, sprekers op een seminarie, deelnemers aan een cursus of conferentie.

## Appendix B – implementatie van het netwerk login systeem

Het netwerk-login systeem wordt geïmplementeerd m.b.v. router access lists. Voor wireless netwerken gebruiken we twee acl's

- **incoming access lists wlan-in**

deze blokkeert alle niet-ingelogde gebruikers, en laat enkel verkeer door dat nodig is voor de login-procedure (dns, dhcp, toegang tot de login webserver). Gebruikers dienen in te loggen via een formulier op een ssl-beveiligde webpagina. Hierbij geven ze hun login naam op (intranet userid, tijdelijk account of netwerk account), en het bijhorende paswoord. Bij een geslaagde netwerk login wordt de router access list uitgebreid met een permit-regel, die het ip-adres van de ingelogde gebruiker toegang verleent tot KULeuvenNet en Internet.

```
ip access-list extended wlan-in

! permit dns access to KULeuvenNet dns servers + dhcp broadcast
permit udp 10.0.0.0 0.0.255.255 134.58.126.0 0.0.1.255 eq domain
permit tcp 10.0.0.0 0.0.255.255 134.58.126.0 0.0.1.255 eq domain

! permit dhcp broadcast
permit udp any eq bootpc any

! web-access permitted to KULeuvenNet/LUDIT (for net-login)
permit tcp 10.0.0.0 0.0.255.255 134.58.126.0 0.0.1.255 eq www
permit tcp 10.0.0.0 0.0.255.255 134.58.126.0 0.0.1.255 eq 443
permit tcp 10.0.0.0 0.0.255.255 134.58.10.0 0.0.0.255 eq www
permit tcp 10.0.0.0 0.0.255.255 134.58.10.0 0.0.0.255 eq 443

! permit icmp (for debugging purposes)
permit icmp any 134.58.0.0 0.0.255.255
permit icmp any 10.0.0.0 0.0.255.255

! logged-in users are added below
permit ip host <user-ip-address> any
```

- **outgoing access list wlan-out**

deze access list zorgt ervoor dat enkel veilige diensten op KULeuvenNet aangesproken kunnen worden, nl. http/https, pop/imap over ssl, smtp naar anti-virus cluster, ssh, ipsec (onderworpen aan dezelfde gebruiksregels als andere KotNet aansluitingen).

```
ip access-list extended wlan-out

! permit traffic from KULeuvenNet/LUDIT (netlogin)
permit tcp 134.58.126.0 0.0.1.255 eq www any
permit tcp 134.58.10.0 0.0.0.255 eq www any
permit tcp 134.58.126.0 0.0.1.255 eq 443 any
permit tcp 134.58.10.0 0.0.0.255 eq 443 any

! permit ntp to KULeuvenNet ntp servers
permit ip 134.58.255.0 0.0.0.255 any

! permit smtp traffic to anti-virus cluster
permit tcp 134.58.240.0 0.0.0.255 eq smtp any

! http/https permitted
permit tcp 134.58.0.0 0.0.255.255 eq 80 any
permit tcp 134.58.0.0 0.0.255.255 eq 443 any
```

```
! ssl based traffic permitted (pop/imap)
permit tcp 134.58.0.0 0.0.255.255 eq 993 any
permit tcp 134.58.0.0 0.0.255.255 eq 994 any
permit tcp 134.58.0.0 0.0.255.255 eq 995 any

! permit ssh
permit tcp 134.58.0.0 0.0.255.255 eq 22 any

! permit ipsec
permit udp 134.58.0.0 0.0.255.255 eq 500 any
permit 50 134.58.0.0 0.0.255.255 any
permit 51 134.58.0.0 0.0.255.255 any

! permit icmp (for debugging purposes)
permit icmp any any

! deny other traffic from KULeuven
deny ip 134.58.0.0 0.0.255.255 any
deny ip 10.0.0.0 0.255.255.255 any

! deny all smtp that doesn't use the cav-cluster
deny tcp any eq 25 any

! other traffic permitted
permit ip any any
```

## Appendix C – werken met netwerk accounts

KULeuvenNet voorziet een geauthenticeerde webpagina, waar geregistreerde beheerders (netwerkbeheerders en campus services) *paswoorden van de dag*, geassocieerd met het netwerk account voor een draadloos netwerk, kunnen opvragen. Op deze webpagina wordt volgende informatie gevraagd:

- intranet userid en paswoord van de beheerder
- aantal te tonen paswoorden (maximum 10)
- draadloos netwerk (te kiezen uit een lijst van locaties, waarvoor de beheerder bevoegd is).

Op basis van deze informatie wordt een lijst van dag-paswoorden getoond, die op de aangegeven dagen gebruikt kunnen worden. KULeuvenNet registreert wie deze dagpaswoorden opgevraagd heeft (zodat deze persoon gecontacteerd kan worden in geval van problemen).

Hieronder volgt een voorbeeldje van een gegenereerde dag-paswoord lijst.

```

| Lijst met dag-paswoorden
|
| Subnet:                10.0.73.0/24 - Aula Pieter De Somer
|
| Ogevraagd door:      Herman Moons (u0012638)
|
| LOGIN      PASWOORD      GELDIG OP
| -----
| WLAN-PDS   Ax22fk9t      zon 04-mei-2003
| WLAN-PDS   3uikZ99P      maa 05-mei-2003
| WLAN-PDS   ksw8NM23      din 06-mei-2003
| WLAN-PDS   F4Wru8vb      woe 07-mei-2003
|
| Gebruik van deze login/paswoord combinaties is strikt beperkt
| tot gasten van de K.U.Leuven. Personeel en studenten van de
| K.U.Leuven moeten steeds gebruik maken van hun intranet userid
| en bijhorend paswoord.

```