Unwire! - Wireless Lan

v.1.03 [24.03.2003]

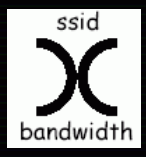
I. Was ist Wireless Lan und was ist es nicht?

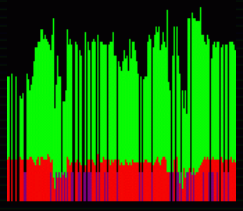
II. Adapter & Antennen: die Hardware zum Funken

III. Standard-Dschungel: Frequenzen, Geschwindigkeiten & (In)Kompatibilitäten

IV. Sicherheit: WEP und wie man Netze schützen kann

V. Horchen und Malen: Wardriving & Warchalking





Unwire! - Wireless Lan

I. Was ist Wireless Lan und was ist es nicht?

einige Synonyme (nicht immer richtig bzw. eindeutig):

~> WLan
~> WaveLan
~> Funk-Lan/ -Netz
~> Wireless Ethernet
~> usw.

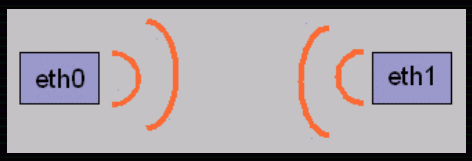
andere Drahtlose (Daten) Verbindungen:

~> Packet Radio
~> Infrared Data Association [IRDA]
~> Bluetooth
~> Global Standard for Mobile Communications [GSM]
  ~> General Packet Radio Service [GPRS]
  ~> High Speed Circuit Switched Data [HSCSD]
~> Universal Mobile Telecommunications Systems [UMTS]
~> ...

Unwire! - Wireless Lan

I. Was ist Wireless Lan und was ist es nicht?

~> im wahrsten Sinne des Wortes "Ethernet"
~> physical layer ist nicht Draht oder Glasfaser sondern der "Äther"
~> an der prinzipiellen Funktionsweise ändert sich nichts
~> eine WLan Karte wird als "normale" Netzwerkkarte behandelt



Durch die Eigenschaften von drahtlosen Netzwerken, sind natürlich andere Infrastruckturen bzw. Topologien als bei drahtgebundenen Netzwerken möglich.

Unwire! - Wireless Lan

I. Was ist Wireless Lan und was ist es nicht?

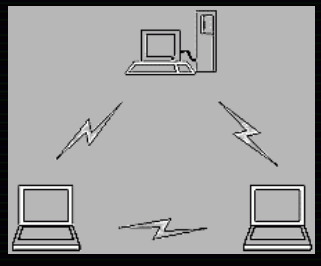
Infrastrukturen / Topologien

Ad-hoc [Peer-to-Peer]

~> einfachste Variante
~> vergleichbar mit Linien- oder vollvermascher Topologie

\+ quasi unbegrenzte Anzahl von Teilnehmern
\+ preiswerter und einfacher Aufbau
\+ sehr flexibel

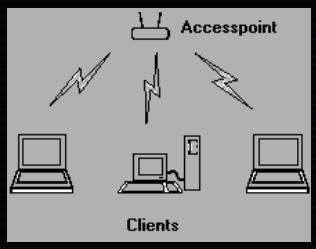
\- mit steigender Anzahl von Teilnehmern sinkt die Bandbreite
\- geringe Reichweite (jeder muss jeden erreichen können)



Unwire! - Wireless Lan

I. Was ist Wireless Lan und was ist es nicht?

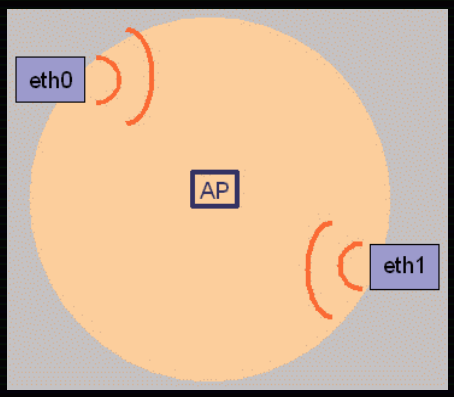
Infrastrukturen / Topologien



Access Point

~> vergleichbar mit Stern - Topologie

+ Anzahl von Teilnehmern wird durch Access Point bestimmt
+ höhere Reichweite
~> besteht Verbindung zum AP, erreicht man das gesamte Netz



- höhere Kosten als Ad-hoc
- weniger flexibel als Ad-hoc

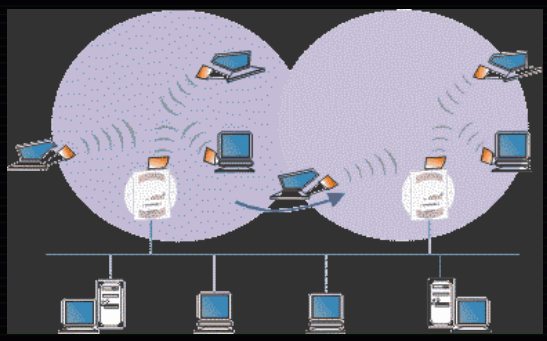
Unwire! - Wireless Lan

I. Was ist Wireless Lan und was ist es nicht?

Infrastrukturen / Topologien

Infrastruktur-Modus

~> managed
wenn mehrere Funkzellen vorhanden sind, besteht die Möglichkeit des Roaming
[ohne Verbindungsabbruch von Funkzelle zu Funkzelle "hüpfen" (GSM)]
~> Bridge
Brücke zwischen zwei drahtgebundenen Netzen
~> Repeater
Reichweitenerhöhung



Unwire! - Wireless Lan

II. Adapter & Antennen: die Hardware zum Funken

Adapter

PC Cards [PCMCIA] →

PCI to PCMCIA Adapter + PC Card

PCI Adapter →

Compact Flash Adapter →

USB Adapter

*ich bevorzuge keine Netgearprodukte, aber die haben schöne Bilder auf ihren Webseiten

Unwire! - Wireless Lan

II. Adapter & Antennen: die Hardware zum Funken

Antennen

jeder WLan Adapter hat eine interne/externe Antenne →
~> in der Regel sehr klein
~> geringe Reichweite

Abhilfe schaffen externe Antennen

Unwire! - Wireless Lan

III. Standard-Dschungel: Frequenzen, Geschwindigkeiten & (In)Kompatibilitäten

IEEE 802.11 [1997]	Standard für lokale drahtlose Netzwerke Definition eines gemeinsamen MAC-Protokolls [Media Access Control] Definition physikalischer Übertragungsverfahren [PHY] bis 2 Mbit/s Frequenzband 2,4 - 2,48 GHz
IEEE 802.11a [1999]	bis 54 Mbit/s im 5 GHz Frequenzband [18 Kanäle] 200 / 1000 mW
IEEE 802.11b [1999]	Weiterentwicklung von 802.11 bis 11 Mbit/s im 2,4 GHz Frequenzband [11 / 3 Kanäle] ~ 100 mW
IEEE 802.11g [i.A.]	bis 54 Mbit/s im 2,4 GHz Frequenzband abwärtskompatibel zu 802.11b
IEEE 802.11c+d	6/2001 MAC Verbesserung für Bridges PHY-Änderungen für Zulassung in unterschiedlichen Regionen

Die Standards IEEE 802.11e [quality-of-service], f [Inter Access Point Protokoll (IAPP)], h [Leistungskontrolle, dynamische Frequenzwahl] und i [höhere Sicherheit, Authentifizierung] sind in Arbeit.

Unwire! - Wireless Lan

III. Standard-Dschungel: Frequenzen, Geschwindigkeiten & (In)Kompatibilitäten

Mittlerweile sind Funknetze mit Hardware unterschiedlicher Hersteller möglich.
[Hersteller haben erkannt das Interoperabilität gar nicht so schlecht ist.]

Problme gibt es manchmal noch mit:

1.) Roaming zwischen Zellen unterschiedlicher Hersteller [IEEE 802.11f]
2.) Verschlüsselung mit Hardware unterschiedlicher Hersteller [Cisco]
3.) unterschidliche Reichweiten und Geschwindigkeiten
    ~> Einigung auf gemeinsame Geschwindigkeit
    ~> schlechte Karten können Netz ausbremsen

22 MBit/s Karten?
    ~> Karten in Richtung 802.11g [aber nicht 100%ig]
    ~> Standard 802.11g noch nicht verabschiedet
    ~> Texas Instruments nutzt eigenes Modulationsverfahren
    ~> Abwärtskompatibilität zu 802.11b Karten und Kompatibilität zu 802.11g Geräten ist nicht garantiert (vermutlich wird auf 11 MBit/s runtergeschalten)

Unwire! - Wireless Lan

IV. Sicherheit: WEP und wie man Netze schützen kann

Funknetzwerke erfordern besondere Sicherheitsmaßnahmen.
Warum? Sollte klar sein.

WEP [Wired Equivalent Privacy]

~> ist im IEEE Standard integriert
~> häufig kann man lesen das WLan unsicher wäre ~> FALSCH!
WEP wird als unsicher betrachtet, nicht WLan
~> Warum ist WEP schlecht? Wie können WEP verschlüsselte Daten gelesen werden?
Wird seltenst erklärt.

~> Funknetze können beliebig sicher gemacht werden ~> Kompetenz des Admins

Unwire! - Wireless Lan

IV. Sicherheit: WEP und wie man Netze schützen kann

Warum ist WEP schlecht?

Bevor WEP in der Luft zerrissen wird, es hat auch Vorteile:

~> jede Karte nach IEEE 802.11x hat die Möglichkeit Daten WEP zu verschlüsseln
~> extrem einfach zu benutzen
~> nach der Treiberinstallation steht WEP sofort zur Verfügung
unter Linux genügt ein Befehl Beispiel: iwconfig eth*x* key s:*XXXXX*
unter Windows wenige Mausklicks und tippen eines Passworts
~> verhindert Dateneinsicht im Vorbeigehen/fahren

Nachteile:

~> Verschlüsselung wird mit Hilfe des Treibers realisiert
teilweise erhebliche Geschwindigkeitseinbußen
~> Schwächen in RC4 Verschlüsselung [Basis von WEP]
~> Shared Secret [beide Teilnehmer müssen den geheimen Schlüssel kennen]

Unwire! - Wireless Lan

IV. Sicherheit: WEP und wie man Netze schützen kann

Wie können WEP verschlüsselte Daten gelesen werden?

Wie funktioniert WEP?

~> zwei Verschlüsselungstiefen 64/128 Bit
Schlüssel: 24 Bit langer Initialisierungsvektor [IV] + 40 bzw. 104 Bit geheimer Schlüssel
~> mittels RC4-Algorithmus wird aus IV + geheimer Schlüssel ein Schlüsselstrom erzeugt
~> Teilnehmer verwenden unterschiedliche IV's
Verhindert das immer der gleiche RC4 Schlüssel benutzt wird
[geheimer Schlüssel ist gleich]

Übertragung:

~> bilden einer Prüfsumme des Paketes [Integritäts Check]
erkennen von Datenveränderungen
~> Schlüsselstrom wird erzeugt
~> (unverschlüsselte Daten mit Prüfsumme) XOR (Schlüsselstrom) = verschlüsselte Daten
~> IV wird im Klartext gesendet dann die verschlüsselten Daten
~> Empfänger generiert aus IV und geheimen Schlüssel den RC4 Schlüsslstrom
Schlüsselstrom XOR verschlüsselte Daten = unverschlüsselte Daten
Prüfsumme bilden, vergleichen Paket OK

Unwire! - Wireless Lan

IV. Sicherheit: WEP und wie man Netze schützen kann

Wie können WEP verschlüsselte Daten gelesen werden?

Schwachpunkt ist der Initialisierungsvektor:

verknüpft man zwei Pakete einer Sitzung mit den gleichen IV's
(die also mit identischen RC4 Schlüsseln verarbeitet sind) XOR
erhält man den geheimen Schlüssel

~> gesucht werden zwei Pakete mit gleichem IV
IV ist 24 Bit lang
bei Paketgröße 1500 Byte / 11 MBit / voll ausgelastet
wiederholt sich der IV nach spätestens 5 Stunden (max 24 Gbyte)
~> nicht alle Hersteller nutzen vollen 24 Bit Adressbereich
schnellere Wiederholung des IV's
~> einige Hersteller setzen IV Zähler bei Reset auf 0 und zählen hoch
bei mehreren Teilnehmen lauschen ~> schnellerer Erfolg
~> weiterhin ist bekannt, dass es so genannte schwache IV's gibt
enthalten mit 5% Wahrscheinlichkeit Hinweise auf ein Bit des Schlüssels
nach 8,5 GByte liegen ausreichend schwache IV's zur Ermittlung des Schlüssels vor
~> wenn Passwort nicht HEX sondern ASCII, reduziert dies die möglichen Kombinationen,
so dass man mit 1,3 - 2,8 GB Daten dabei ist

Unwire! - Wireless Lan

IV. Sicherheit: WEP und wie man Netze schützen kann
weitere Probleme ...

~> Karte mit prism-2-Chipsatz und Linux wlan-ng Treiber erlaubt ohne Netzanmeldung Paketmitschnitt
~> geeignete Tools scannen die Daten nach schwachen IV's und liefern nach ausreichender Anzahl von Paketen den WEP-Schlüssel innerhalb einer Sekunde

Schwachstelle der XOR Funktion

~> orginal Daten und verschlüsselte Daten sind einer Person bekannt
(aufwendig, aber bei finanziellen Angelegenheiten könnte sich der Aufwand lohnen)
durch die XOR Funktion ist es möglich, die Daten durch andere zu ersetzen
das Paket wird als korrekt anerkannt (Prüfsumme nicht vergessen)
hierbei ist es nicht notwendig den Schlüssel zu kennen, weil ja
Schlüsselstrom = verschlüsselte Daten XOR unverschlüsselte Daten und mit
Schlüsselstrom XOR modifizierte unverschlüsselte Daten = verschlüsselte Daten
hat man es dann

eins noch ...

~> Daten ins Internet sind unverschlüsselt ~> IP Adresse im Paket auf IP im iNet ändern
(wenns geht, die des eigenen Rechners) ~> Daten kommen unverschlüsselt an

Unwire! - Wireless Lan

IV. Sicherheit: WEP und wie man Netze schützen kann

Lösungen für höhere Sicherheit

Verbesserung der WEP Verschlüsselung in Arbeit
~> RC4 Packet Keying
unterschiedliche Schlüssel für jedes Datenpaket
beide Seiten verwenden 128 Bit temporal Key [TK]
TK wird mit Adresse des Senders verknüpft [jeder Sender hat anderen Schlüsselstrom]
Packet Keying wird sich per Firmware und Treiber Update auf vorhandenen Karten einsetzen lassen

~> Cisco [Aironet-Serie]:
gegenseitige Authentisierung mit LEAP [Lightweight Extensible Authentication Protocol]
unidirektionale, unumkehrbare Hash-Schlüssel
dynamische benutzer- und sitzungsbasierte WEP Schlüssel
IV wird bei jeder Sitzung geändert

Nachteil: funktioniert nur in reinen Cisco Netzen

~> IEEE arbeitet an verbesserten WEP-Standard
AES [Advanced Encryption Standard] ist im Gespräch

Unwire! - Wireless Lan

IV. Sicherheit: WEP und wie man Netze schützen kann

Lösungen für höhere Sicherheit

WEP bzw. IEEE bietet momentan keine professionelle Lösung

IPSec

~> Hardware preiswert (alter Rechner)
~> Software für Linux kostenlos (freeswan), Windows nicht wirklich
~> Lösung: Server Linux ; Windowsclients mit PGP Net (freeware), SSHSentinel (129€)
~> kaum Geschwindigkeitsverluste
~> kompletter Datenstrom ist verschlüsselt
~> RSA Authentifikation, Shared Secret Authentifikation
~> 3DES, AES
~> simple Firewallregeln:

```
iptables -A FORWARD -i ipsec+ -j ACCEPT
iptables -A FORWARD -o ipsec+ -j ACCEPT
iptables -A FORWARD -j DROP
```

~> Alles was unverschlüsselt ist, kommt nach /dev/null

~> MAC/IP Adressen Erkennung (auch ohne IPSec)

Projekt:
WLan IPSec Router

Unwire! - Wireless Lan

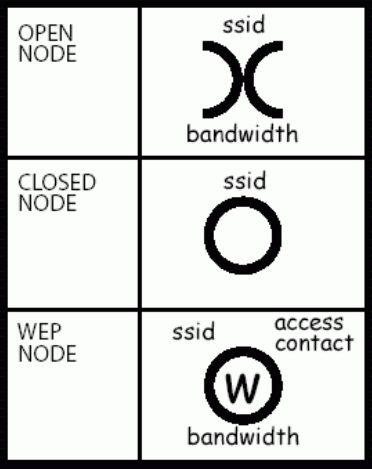
V. Horchen und Malen: Wardriving & Warchalking

~> Wardriving
Laptop, WLan Karte und Antenne
Auto, Bus, S-Bahn, Fahrad oder zu Fuß
GPS Receiver ~> Kartographie (wo kann man kostenlos surfen)
angepasste Linux Distribution ~> WarLinux

Motivation?
~> Spass am Gerät :-)
~> animiert Menschen dazu, Netze zu sichern [erschreckend viele offene Netze]
~> Datenschutz
Patientendaten in Berlin [2000/2001]
Kundendaten
Kreditkartendaten
~> Missbrauch von Daten,
~> verschlüsseln von Daten [Erpressung]

~> Warchalking

Symbole werden mit Kreide an geeignete Stellen gezeichnet um nachkommenden Interessierten Hinweise zu geben.



Unwire! - Wireless Lan

Slides als pdf & sxi im Netz unter http://st23.de

Quellen:

http://www.google.de
http://www.glossar.de
http://www.1stwave.de
http://www.bsi.de
http://www.netgear.de
http://www.alternate.de
http://www.3sat.de

http://www.lancom-systems.de
http://www.zdnet.de
http://www.wardriving.com
http://www.staticusers.net
http://www.warchalking.org

FAQ Wireless Standards 03/2003
PC Professionell Jahresarchiv 2002

Dank an Kathe für die Bugreports.