Westfälische Wilhelms-Universität Münster

Sichere WLANs an UNI und UKM – 2007

Dieter Frieler

27.10.2006

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Übersicht

0 Einleitung
1 Stand bisher
2 Ziele
3 Umsetzung
4 WPA / WPA 2
5 Praxis: Windows XP
6 Support
7 Ausblick

Stand bisher

Eingestzte Dienste

- Offene und unverschlüsselte Funkzelle:
  Funk-Hoer1
- Authentifizierung durch „VPN“ (PPTP) oder Cisco-VPN (IPSec)
- Einige wenige WEP verschlüsselte Funkzellen
  - Nur für angemeldete Geräte (Datenbank, MAC-Filter)
  - kleine Benutzergruppen

Stand bisher

Nicht eingesetzt

- WEP
  - Authentifizierung:
    - Ein(!) von allen Geräten geteilter Schlüssel der veröffentlicht werden muss
    - Nur Geräteauthentifizeirung, keine Benutzerauthentifizierung
    - Keine Server Authentifizierung
  - Verschlüsselung
    - Wegen Designfehler leicht zu knacken

Ziele

Unsere Ziele

– Ein sichereres (verschlüsseltes) FunkLAN

– Höhere Abdeckung erreichen

– Roamingfähigkeit erhalten

– Support vereinfachen / verbessern

– Auf besondere Anforderungen besser reagieren zu können (besondere Funkzellen, Gäste aus anderen Hochschulen)

– *Class of Service*

– *Versorgung ausserhalb von Uni-Gebäuden*

Umsetzung

Abgeschlossen 2005

- Austausch veralteter Hardware
  - 50 Orinoco AP-1000 durch AP-4000 ersetzt
- Softwareupdates auf noch nicht so alter Hardware
  - ca. 80 AP-2000
- Anschaffung neuer Hardware
  - 200 Proxim AP-4000

Proxim AP-4000

Besonderheiten

- Unterstüzt 802.11b, 802.11g und 802.11a
- Anschlussmöglichkeiten für externe Antennen
- Bis zu 16 SSIDs gleichzeitig, mit jeweils eigenen Sicherheitseigenschaften und eigenen VLANs
- Abspeichern der Konfiguration auf Netzwerkserver
- Unterstützt SNMP und Traps
- Class of Service
- Alle zur Zeit gängigen Verschlüsselungsmethoden
- Roaming zwischen Access-Points
- WDS (Punkt-zu-Punkt Kopplungen)
- MESH-Protokoll (Bildung von Maschen bei hoher Dichte)

Umsetzung

Bis Ende 2006

- Weitere Hardware angeschafft (insgesamt sind 300 Access-Points installiert)
- Zeitplan:
  - Bis 27.09.06: Vorbereitende Maßnahmen abschliesen (Infrastruktur, Netzplanung, EMS)
  - Bis 07.11.06: Einführung der neuen Zelle „uni-ms“
  - 13.11.06: Bekanntgabe des neuen Dienstes
  - 20.11.06: Abkündigung „Funk-Hoer1“ zum 01.01.07
  - 01.01.07: Abschaltung „Funk-Hoer1“

Umsetzung

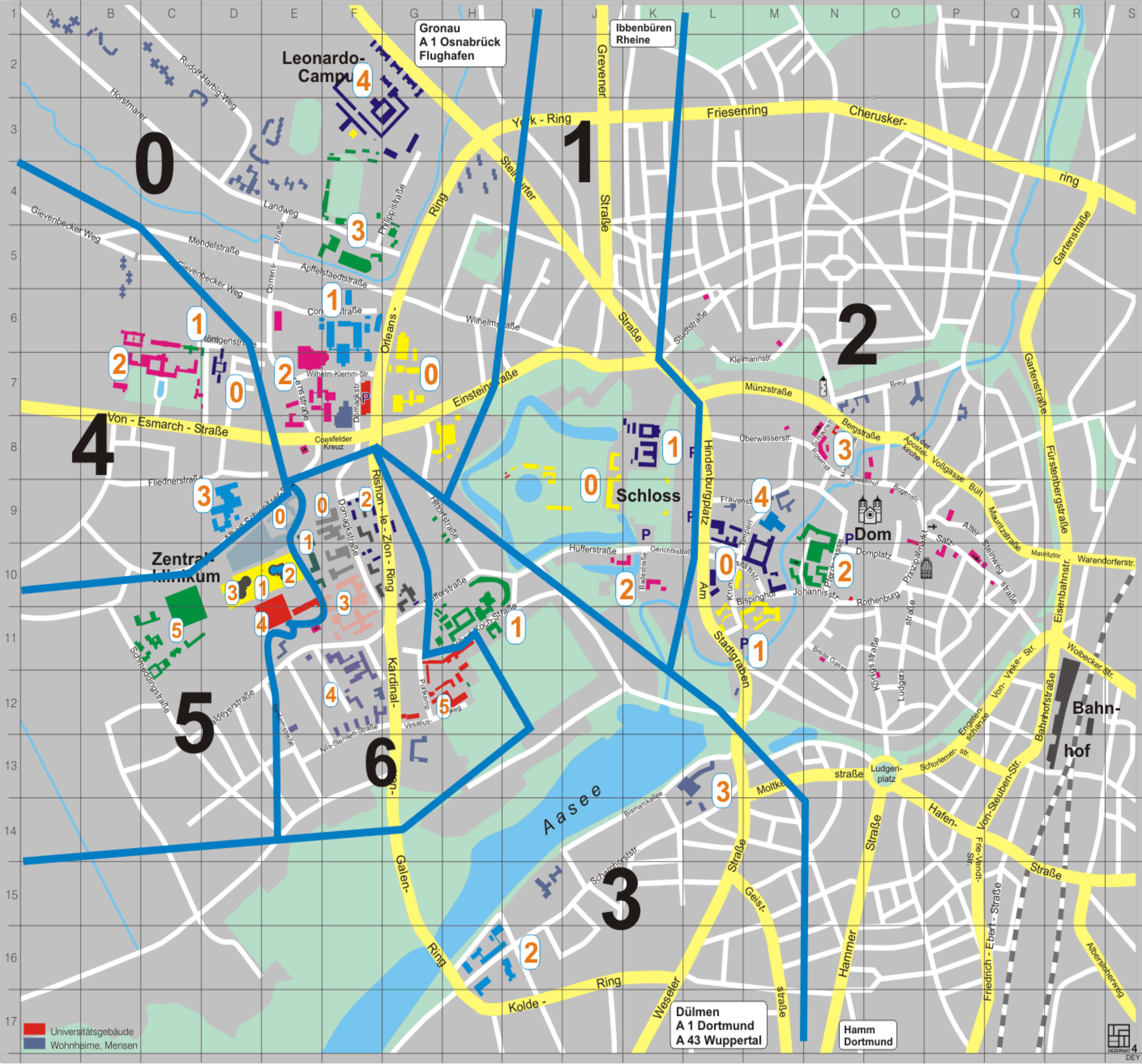
Erneuerung der Netzstrukturen

- Einbindung in das neue hierachische Netzkonzept
- 32 kleine Broadcast-Domains
- Neue Server für DHCP und RADIUS Dienste

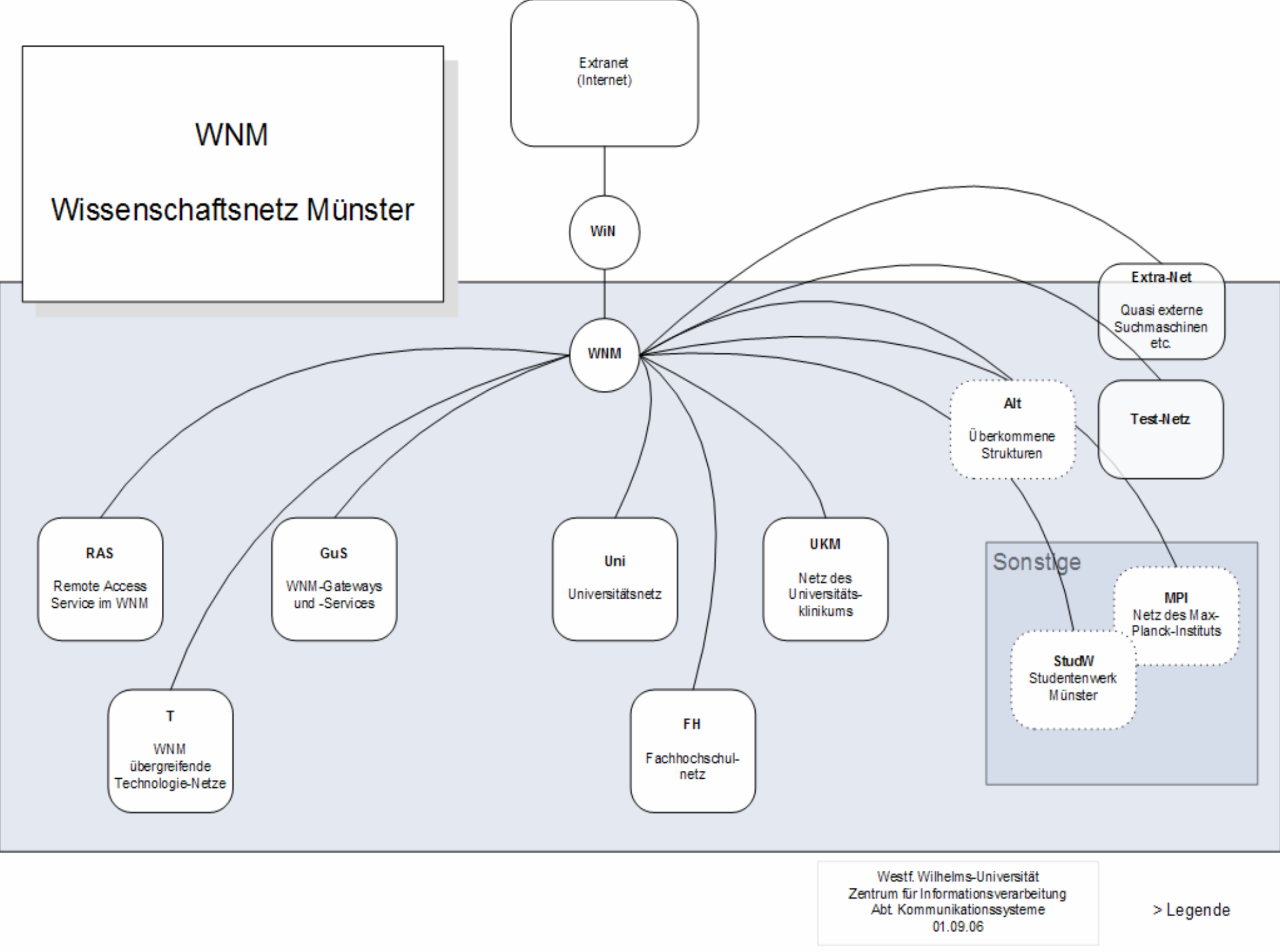
Automatisierte Methoden mittels EMS

- Testen von automatischen Netzmanegment Methoden auf dem EMS-System für das FunkLAN
  (Noch nicht abgeschlossen)

Westfälische
Wilhelms - Universität
Münster

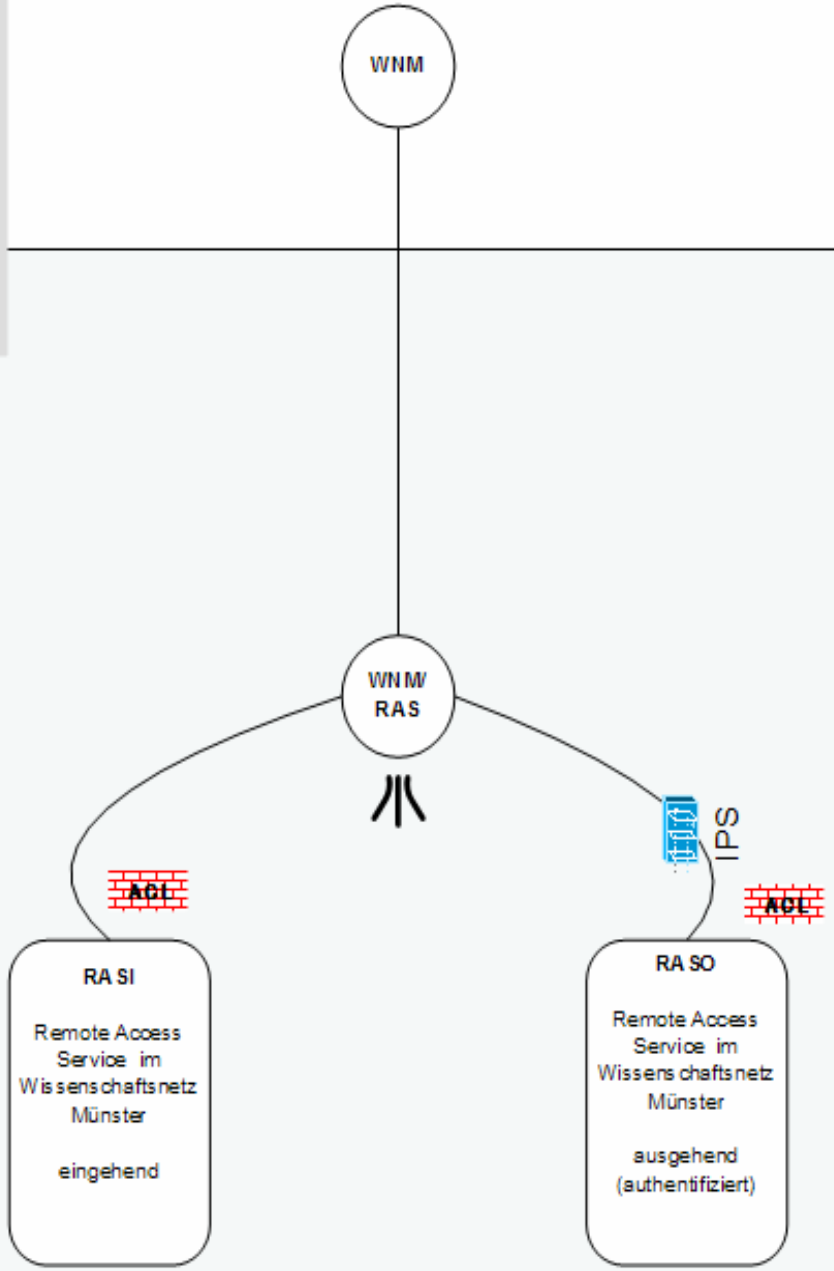


Stand: Juni 2000


WNM
Wissenschaftsnetz Münster
Extranet
(Internet)
WiN
WNM
Extra-Net
Quasi externe
Suchmaschinen
etc.
Test-Netz
Alt
Überkommene
Strukturen
RAS
Remote Access
Service im WNM
GuS
WNM-Gateways
und -Services
Uni
Universitätsnetz
UKM
Netz des
Universitäts-
klinikums
Sonstige
MPI
Netz des Max-
Planck-Instituts
StudW
Studentenwerk
Münster
T
WNM
übergreifende
Technologie-Netze
FH
Fachhochschul-
netz
Westf. Wilhelms-Universität
Zentrum für Informationsverarbeitung
Abt. Kommunikationssysteme
01.09.06
> Legende

RAS

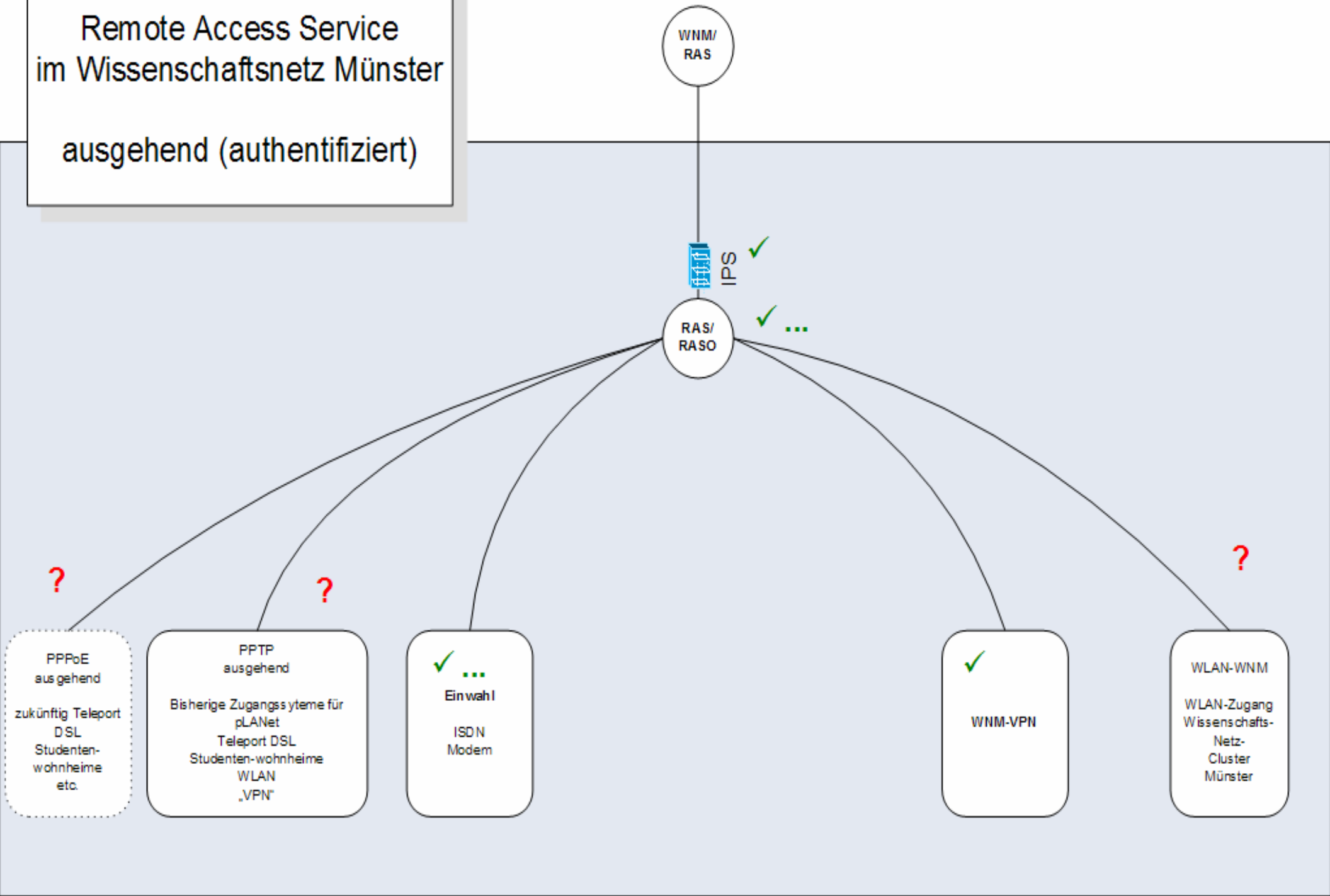
Netzzone für Remote Access Service im Wissenchaftsnetz Münster



Netzzone RASO

Remote Access Service im Wissenschaftsnetz Münster

ausgehend (authentifiziert)

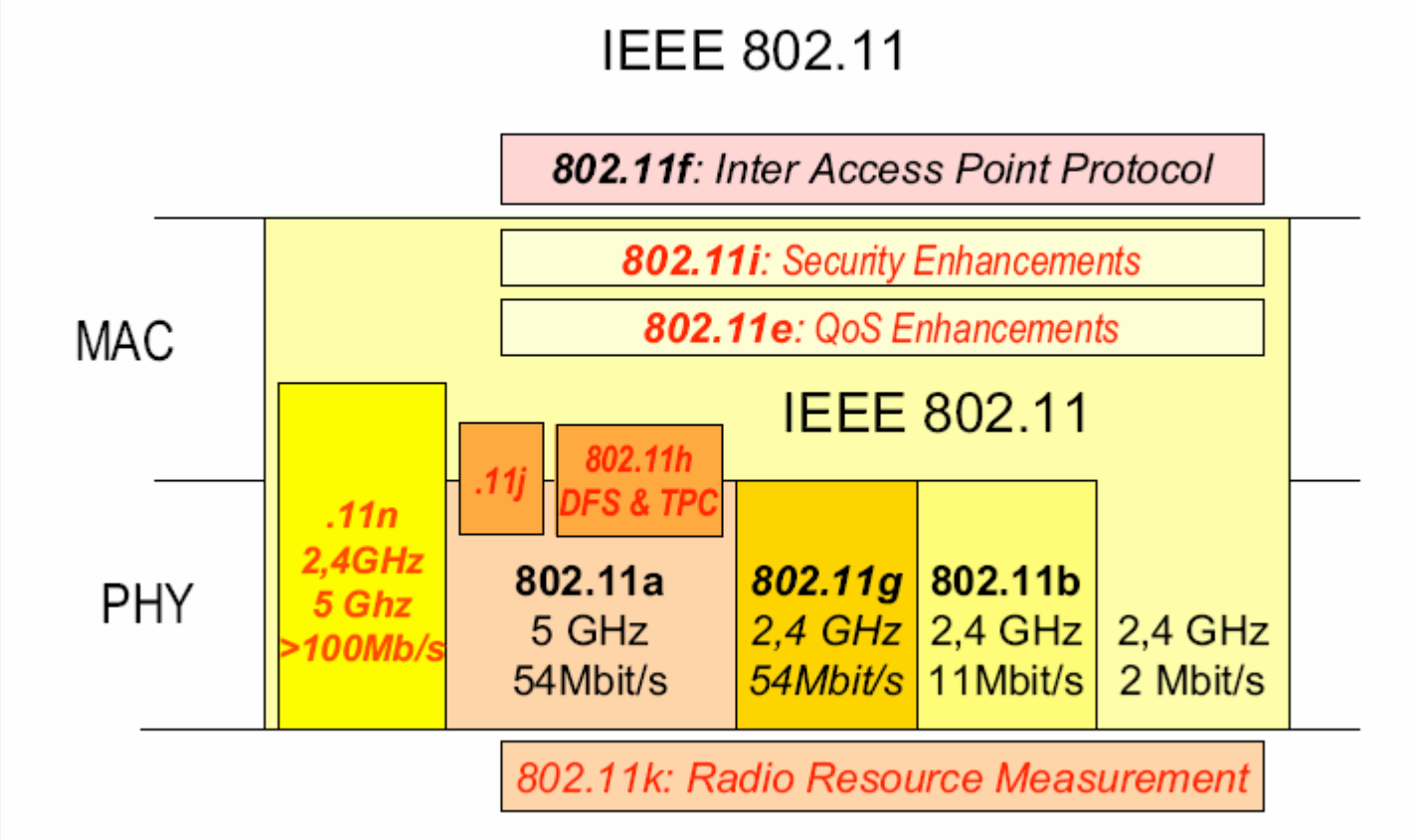


Umsetzung

- Einführung „uni-ms“
  - Auf allen Access-Points wird „uni-ms“ zusätzlich eingeführt. „Funk-Hoer1“ bleibt wie gewohnt erhalten
  - „uni-ms“ ist eine WPA/ WPA2 gesicherte Funkzelle

WPA / WPA2

Normierungen:



WPA / WPA2

- Wi-Fi Protected Access
- Verbesserte Verschlüsselungsverfahren TKIP und CCMP (AES)
- Schlüsselmanagment
- WPA-Enterprise:
  - Benutzerauthentifizierung mit EAP (802.1x)
- WPA-PSK
  - Pre-shared Key

WPA-PSK

- Passwort muss gut gewählt sein.
  Brute-Force-Cracker schon im umlauf
- Ein Schlüssel der allen Nutzern bekannt sein muss
  -> nur für kleine Benutzergruppen

  Einsatzort: SOHO und Privat

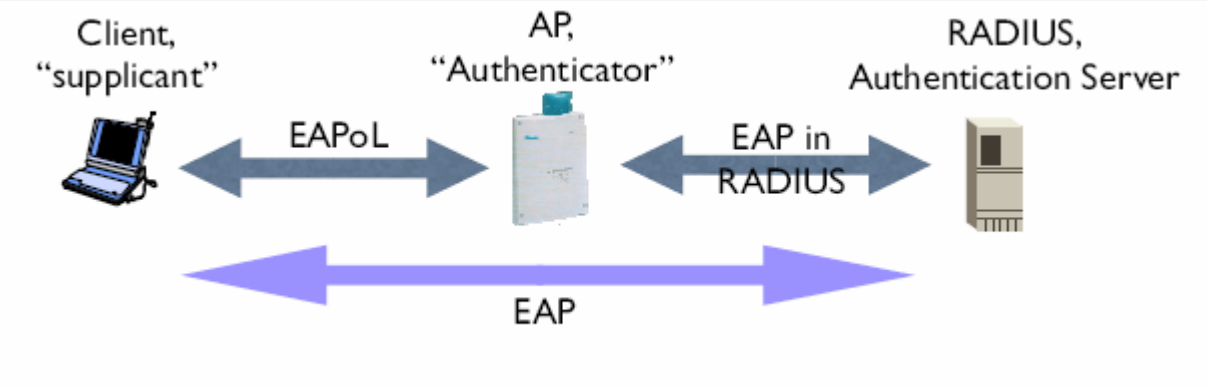
WPA-Enterprise

3 Teile

- Authentifizierung
- Schlüsselaustauschverfahren / Schlüsselmanagment
- Verschlüsselung

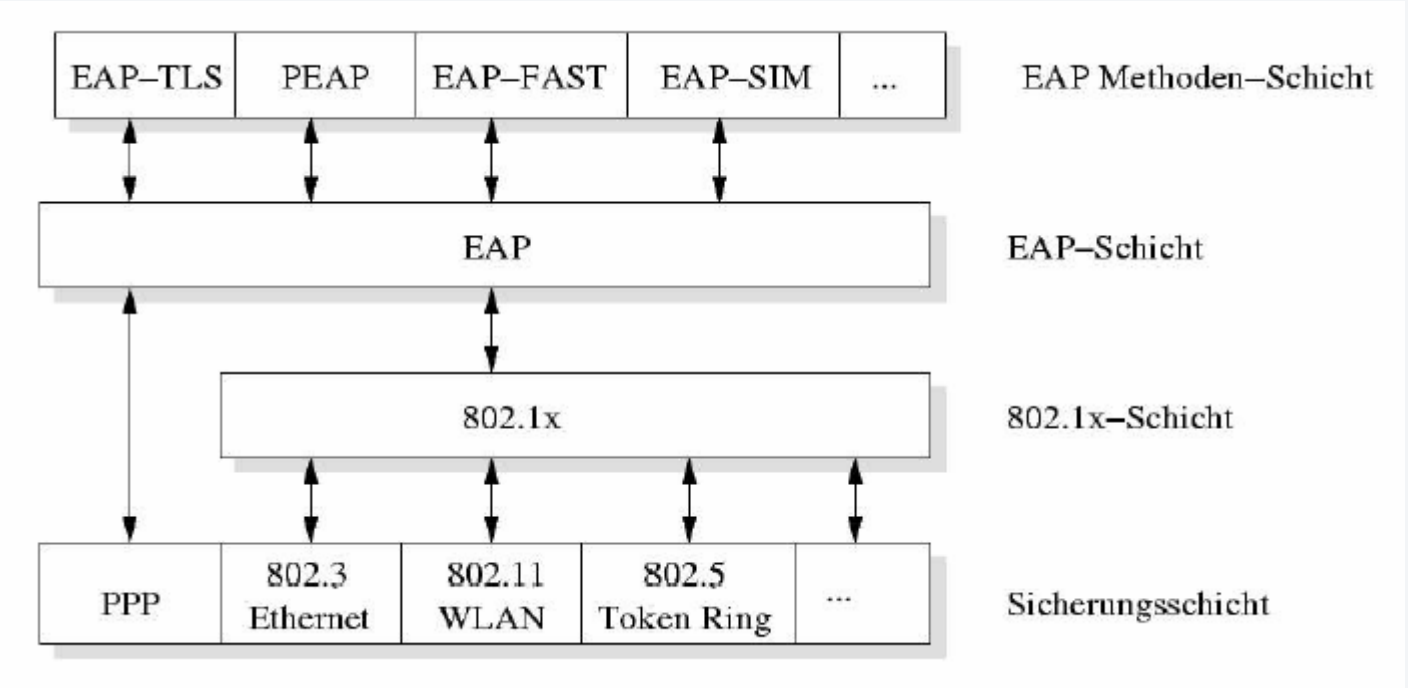
Authentifizierung

EAP und RADIUS



Die Authentifizierung findet zwischen Client und RADIUS statt
Der Access-Point dient lediglich als Proxy:
Vom Client empfangene EAP Nachrichten in RADIUS bzw. vom RADIUS Server empfangene EAP Nachrichten in EAPOL kapseln und entsprechend weiterleiten

EAP-Methoden



Schlüsselmanagment

- Temporärer Schlüssel wird aus der EAP-Accept Message gebildet (256Bit)
- Mit diesem Schlüssel werden weitere Schlüssel generiert und ausgetauscht (jeweils 128Bit).
- Regelmässiger Wechsel der Schlüssel
- Nur einmal Benutzung von Schlüsseln
- Für Broadcasts gib es Gruppenschlüssel

Verschlüsselung

- TKIP
  - Verbesserung des WEP-Verfahren
  - Auch mit alter Hardware möglich
  - Im Standard als Option vorgesehen
- CCMP (AES)
  - Von Grund auf neu konzeptiertes Verfahren
  - Basiert auf AES mit 128Bit Schlüssel
  - Verschlüsselung MAC-Ebene
  - Quell und Zieladresse werden mit einbezogen
  - Gilt als sicher

Clienten

Client	98/ ME	XP/ 2K	OS X	Li nux	Pckt PC	TLS	PEAP	TTLS	License
Win Builtin	✗	✓	✗	✗	✗	✓	CHAP v2	✗	Builtin
OSX Builtin	✗	✗	✓	✗	✗	✓	✓	✓	Builtin
SecureW2	✗	✓	✗	✗	✓	✗	✗	✓	Free
Odyssey	✓	✓	✗	✗	✓	✓	✓	✓	$$
AEGIS	✓	✓	✓	✓	✓	✓	✓	✓	$$
wpa_supp	✓	✓	✗	✓	✗	✓	✓	✓	Free
Xsupplicant	✗	✗	✗	✓	✗	✓	✓	✓	Free

Praxis: Windows XP

Kurze Vorführung

Anleitung unter :

http://www.uni-muenster.de/ZIV/Content--netz_funk_lan_Anleitungen.html

Offene Organisatorische Punkte

- ZIV intern
  - Schulung ZIV-Line, NOC-Dienst, Benutzerber.
  - Erstellung und Pflege weiterer Anleitungen
  - Webseiten noch nicht erstellt
- Von wem und wieviel Support für welche Betriebssysteme
- Garantierte Empfangsqualität für alle Endgeräte an welchen Stellen?

FunkLAN Support

- Häufige Fehlerursachen:
  - Treiberprobleme bei nicht Windows-Treibern
  - Umschaltung zwischen Profilen wenn der Kunde auch ein Heim-Funknetz betreibt
  - Netzabdeckung noch nicht flächendeckend
- Erschwernisse:
  - Nutzer kann nicht erkennen welcher AP nicht funktioniert
  - Mitarbeiter kann nicht erkennen welchen AP der Kunde nutzen will
- Verbesserung:
  - Bei WPA wegfall der VPN-Komponente

Ausblick

- Abschaltung „Funk-Hoer1“
- Einführung spezieller Funkzellen und Suffix-Accounts
- Anzahl der Access-Points drastisch (bis zu 3000 Stück) erhöhen
- VOIP über drahtlose Clienten
- DFN-Roaming

Fragen ?