

An introduction to Network Access Security

Torino, IT • March 4th, 2005

Carsten Bormann <cabo@tzi.de>



Overview

- ▶ Network Access Security: Traditions
- ▶ WLAN Security
- ▶ WLAN Roaming

Overview

- ▶ Network Access Security: Traditions
- ▶ WLAN Security
- ▶ WLAN Roaming

Bad, bad world out there

The old world

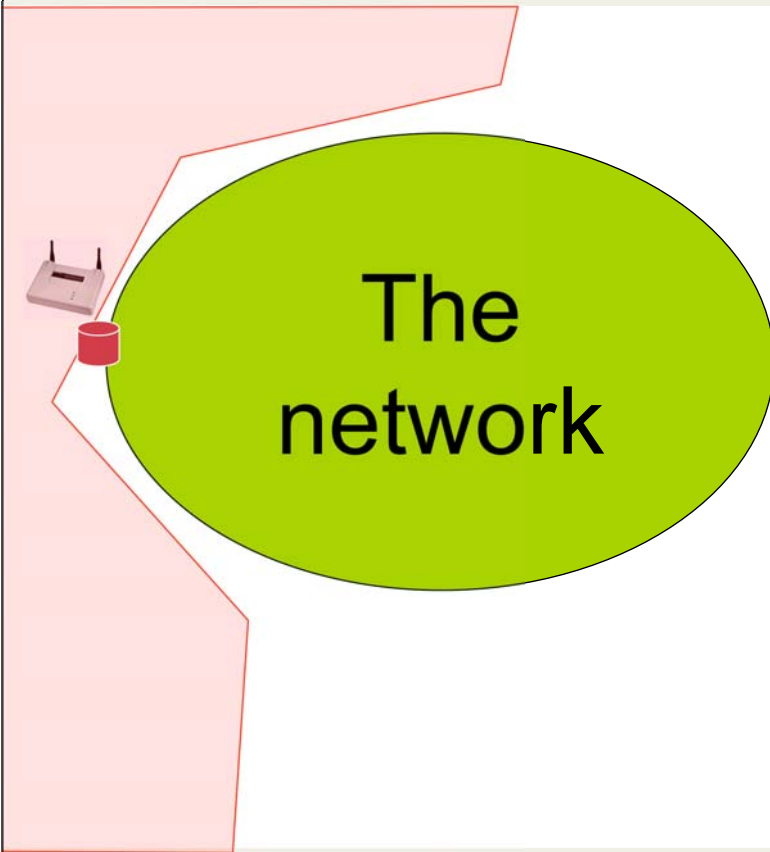
Modem



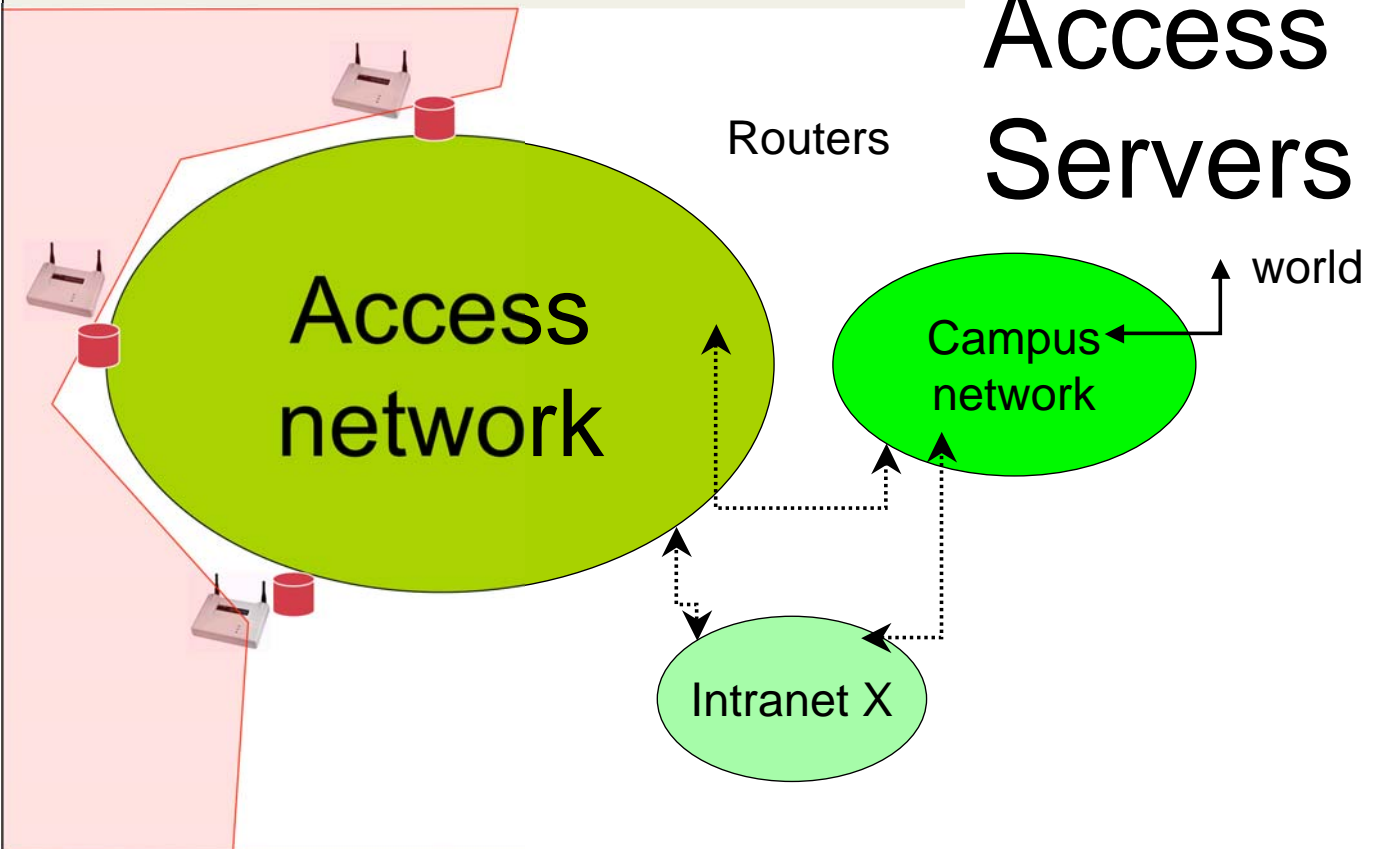
User DB

The Host

Access Servers

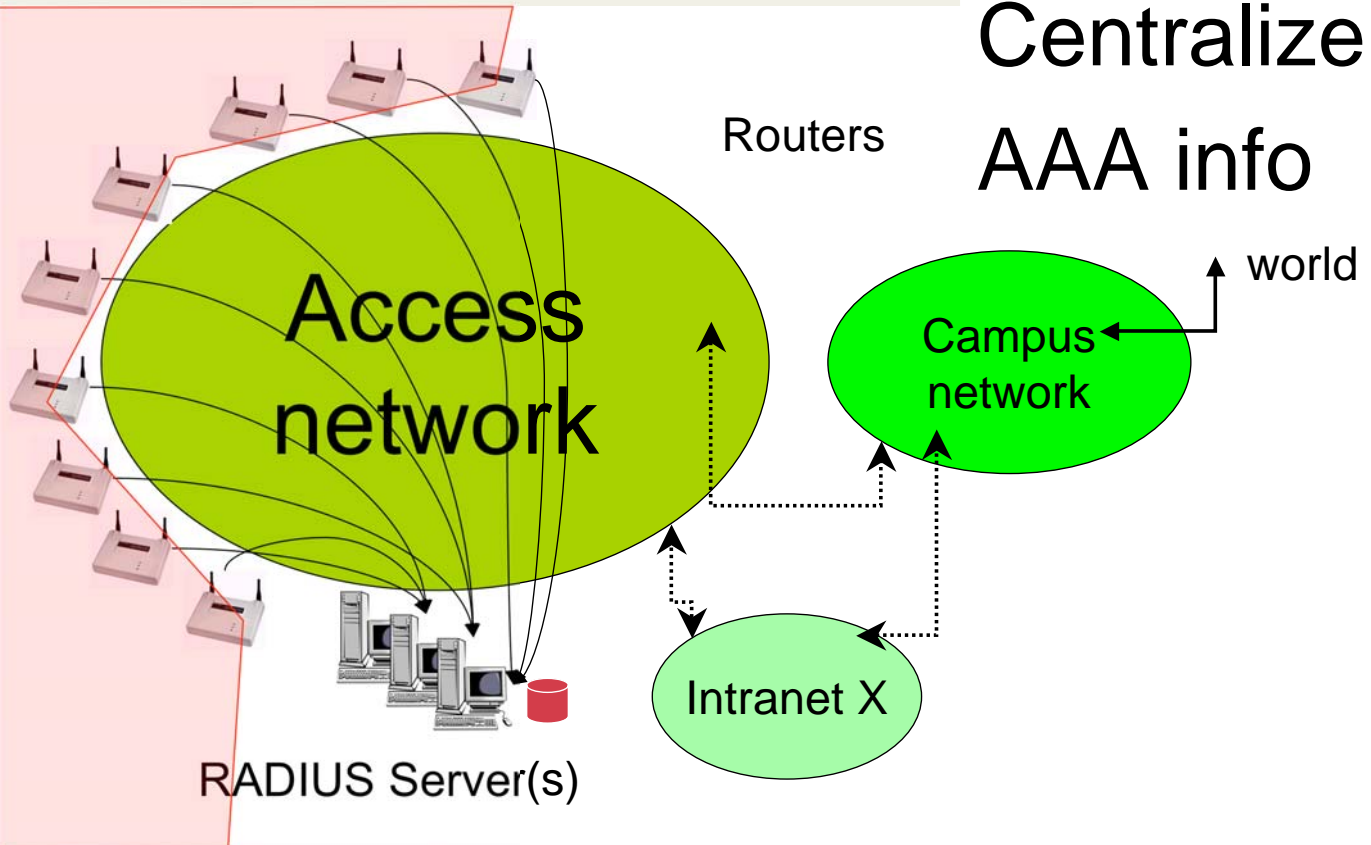


Access Servers



Centralize AAA info

Routers



Elements of traditional Network Access Security

- ▶ Handle Network Access Security at L2
 - PPP and attendant authentication protocols (PAP, CHAP, EAP)
 - Mainly user/password based
- ▶ RADIUS as “backend protocol”
 - Access devices (PEPs) stay dumb
 - RADIUS server is PDP
- ▶ NAIs and RADIUS proxying
 - Network Access Identifier: cabo@tzi.de
 - Use part after @ to identify home RADIUS server

802.1X: Network Access Security for Ethernet

- ▶ Before 802.1X:
Everyone can attach to a switch and get network access
- ▶ 802.1X: Run EAP over the LAN
 - Supplicant: Client trying to obtain access
 - Authenticator (PEP): Switch
 - Authentication Server (PDP): RADIUS server
- ▶ Switch can make decisions such as VLAN assignment based on information returned from RADIUS server

What is being protected?

- ▶ Scarce Network Resources
 - Dialin pool etc.
- ▶ Network Security
 - Often, Network Access Security was the only Network Security!
 - No longer an option in Internet times
 - Privileged IP addresses
 - Access behind firewall

Overview

- ▶ Network Access Security: Traditions
- ▶ WLAN Security
- ▶ WLAN Roaming

WLANs are different

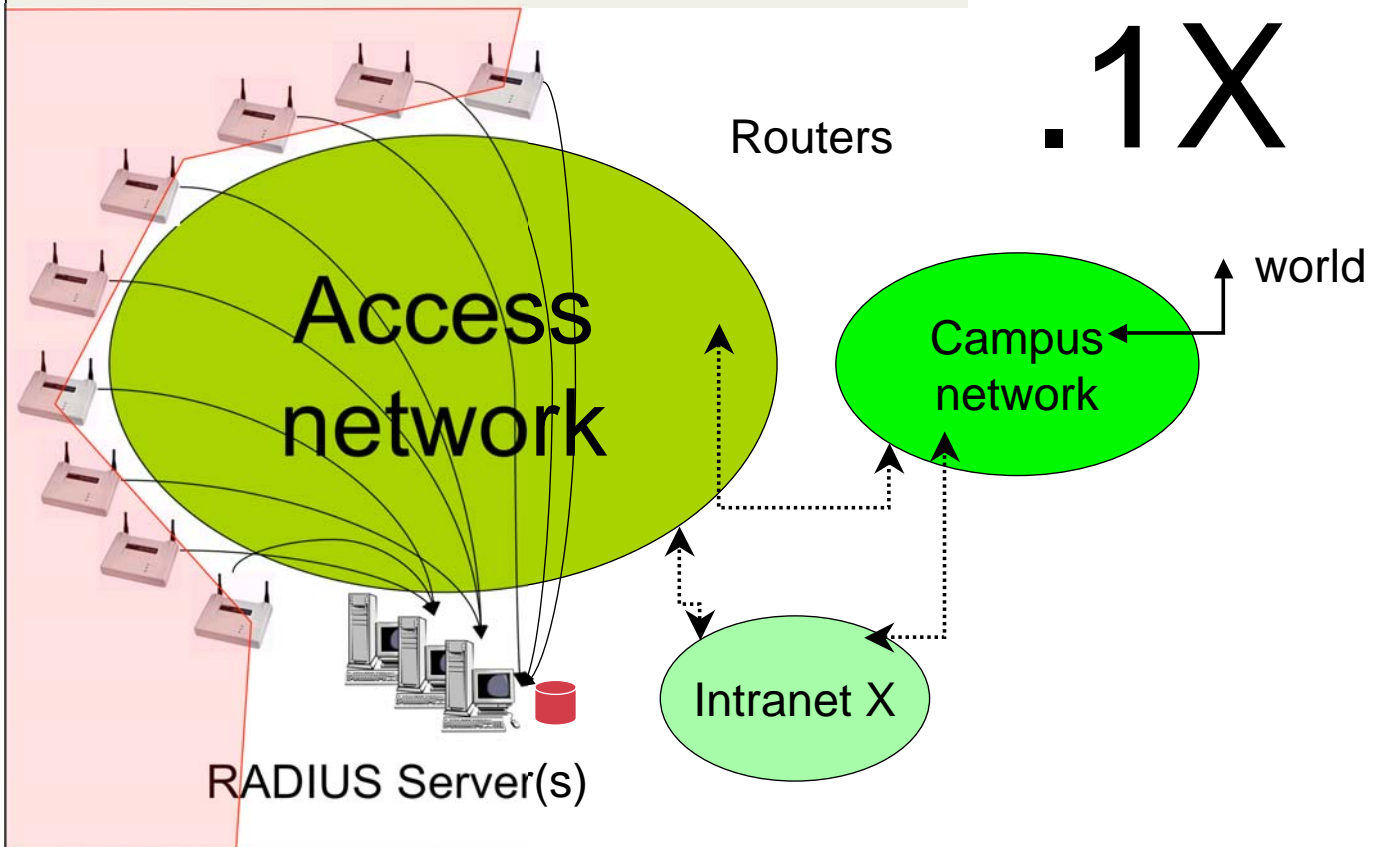
- ▶ WLANs are radio-based
 - Everyone can hear everything
 - Requirement for confidentiality
- ▶ No “line” any more
 - Rogue devices can insert/modify information
- ▶ Less requirement for protection of access resources
 - WLAN is “fast”
 - ISM band radio cannot be protected anyway

WLAN Security: Requirements

- ▶ **Confidentiality (Privacy):**
 - Nobody can understand foreign traffic
 - Insider attacks as likely as outsiders'
- ▶ **Accountability:**
 - We can find out who did something
 - Prerequisite: **Authentication**

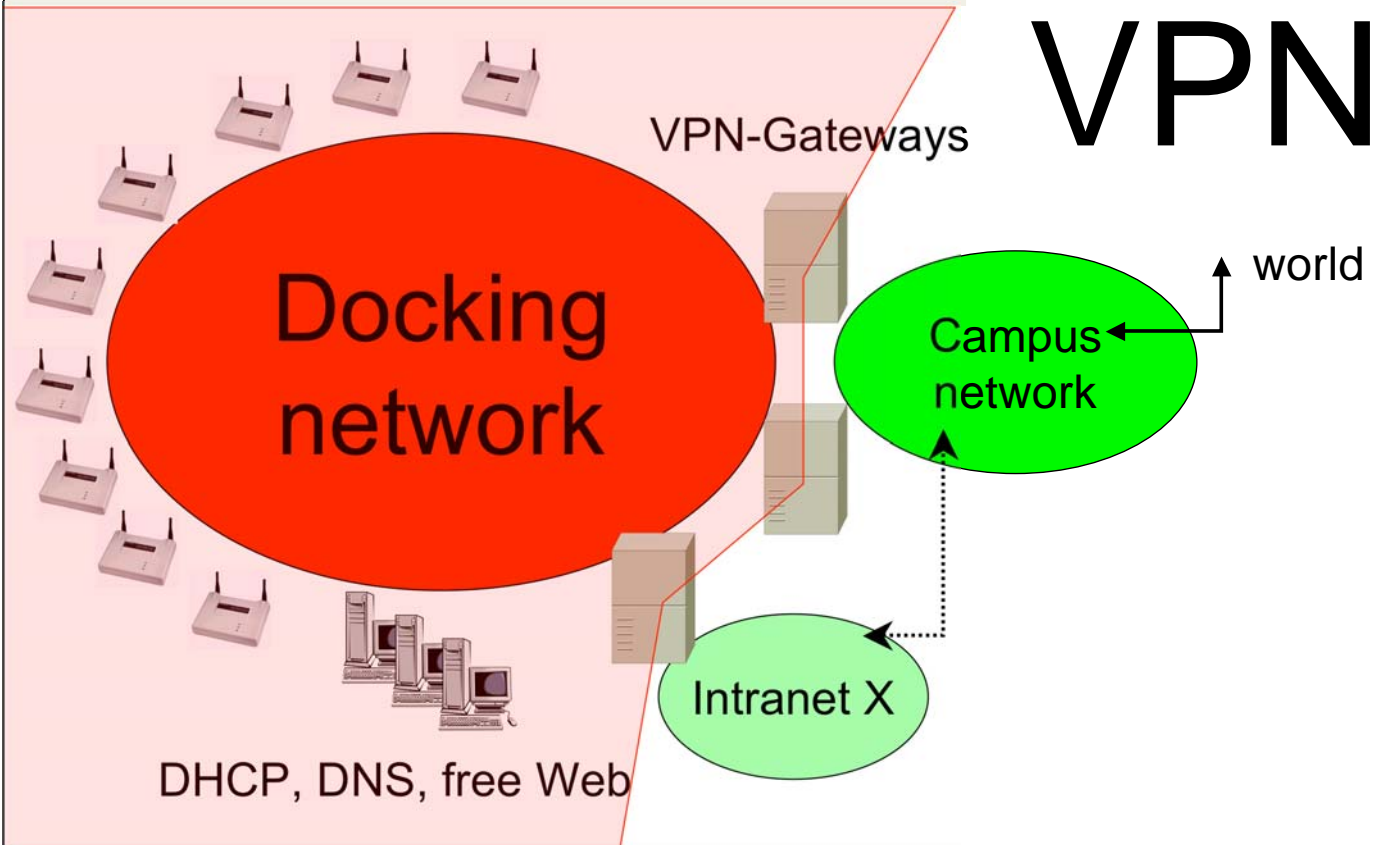
WLAN Security: Approaches

- ▶ **AP-based Security:** AP is network boundary
 - WEP (broken), WEP fixes
 - **802.1X** (EAP variants + RADIUS) + 802.11i (“WPA Enterprise”)
- ▶ **Network based Security:** deep security
 - **VPNs** needed by mobile people anyway
 - SSH, PPTP, IPsec
 - Alternative: **Web-diverter** (temporary MAC/IP address filtering)
 - No confidentiality at all, though



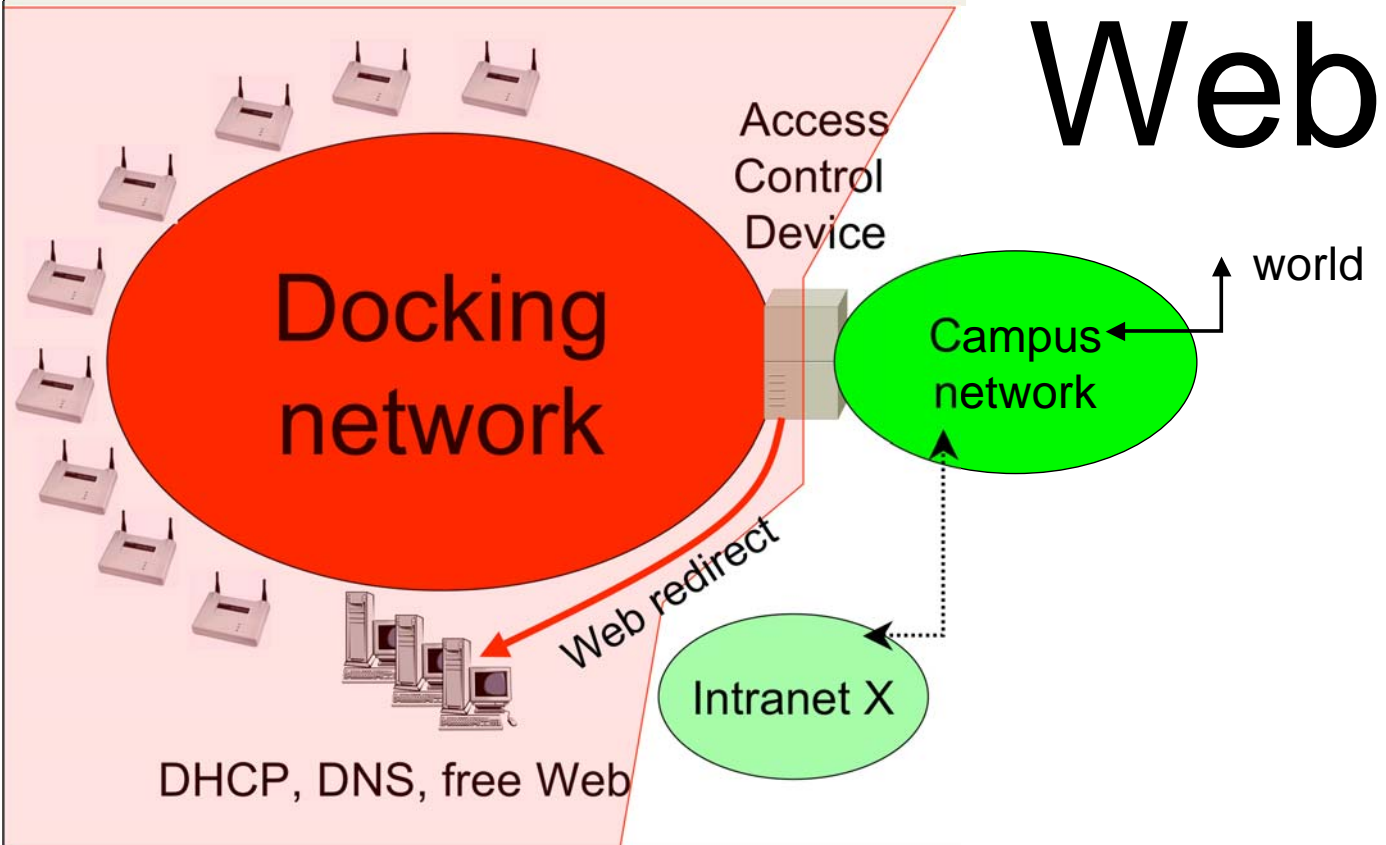
WLAN Access Control: Why 802.1X is better

- ▶ 802.1X is taking over the world anyway
- ▶ The EAP/XYZ people are finally getting it right
 - Only 5 more revisions before XYZ wins wide vendor support
- ▶ Available for more and more systems (Windows 2000 up)
- ▶ Distribute hard crypto work to zillions of access points
- ▶ Block *them* as early as possible
 - More control to visited site admin, too!
- ▶ Most of all: It just works™



WLAN Access Control: Why VPN is better

- ▶ Historically, more reason to **trust L3** security than L2
 - IPsec has lots of security analysis behind it
- ▶ Can use cheap/dumb/untrustworthy APs
- ▶ **Available** for *just about everything* (Windows 98, PDA etc.)
- ▶ Easy to accommodate **multiple security contexts**
 - Even with pre-2003 infrastructure
 - Data is secure in the air and up to VPN gateway
- ▶ Most of all: It just works™



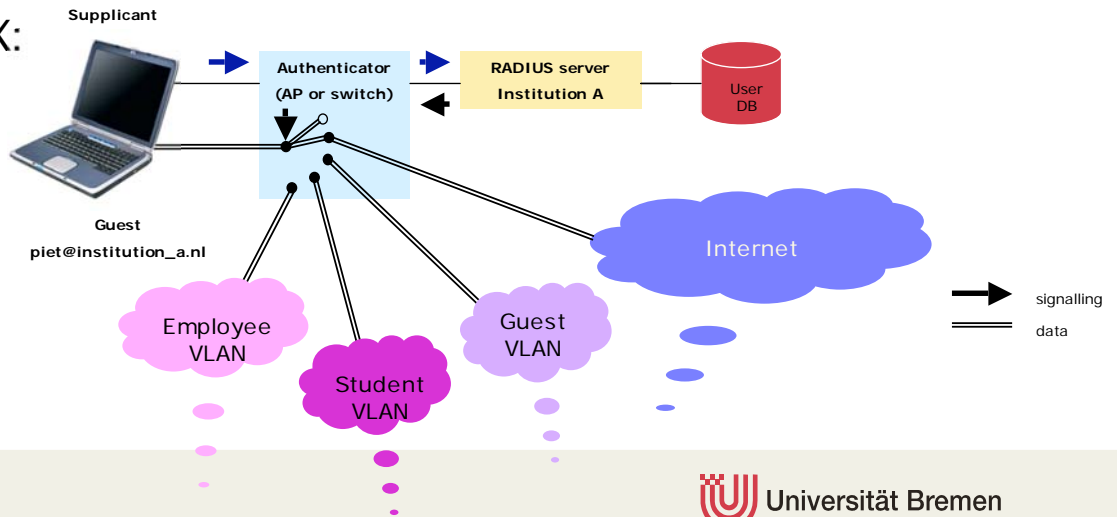
WLAN Access Control: Why Web-based filtering is better

- ▶ No client software needed (everybody has a browser)
- ▶ Ties right into existing user/password schemes
- ▶ Can be made to work easily for guest users
 - It's what the hotspots use, so guest users will know it already
 - May be able to tie in with hotspot federations
- ▶ Privacy isn't that important anyway (use TLS and SSH)
- ▶ Accountability isn't that important anyway

- ▶ Most of all: It just works™

Another Requirement: Multiple User Groups

- ▶ Easy do to with VPN
 - Give each user group a VPN gateway
- ▶ Can be done with Web Redirector
- ▶ 802.1X:



These Three Are Here To Stay

- ▶ 802.1X
 - Secure SSID
 - RADIUS
 - ▶ Web-diverter
 - Open SSID
 - RADIUS
 - ▶ VPN-based
 - Open SSID
 - RADIUS not very useful
- } RADIUS backend
- } Docking net (open SSID)

Overview

- ▶ Network Access Security: Traditions
- ▶ WLAN Security
- ▶ WLAN Roaming

Roaming: High-level requirements

Objective:

Enable NREN users to use Internet (WLAN and wired) everywhere in Europe

- ▶ with minimal administrative overhead (per roaming)
- ▶ with good usability
- ▶ maintaining required security for all partners

- ▶ <http://www.terena.nl/mobility>



Inter-NREN WLAN Roaming

Big assumptions:

- ▶ Every NREN user is equal when it comes to network access (no user profiles)
- ▶ AUPs are “close enough”

- ➔ Authentication, not Authorization problem



Roaming Solutions

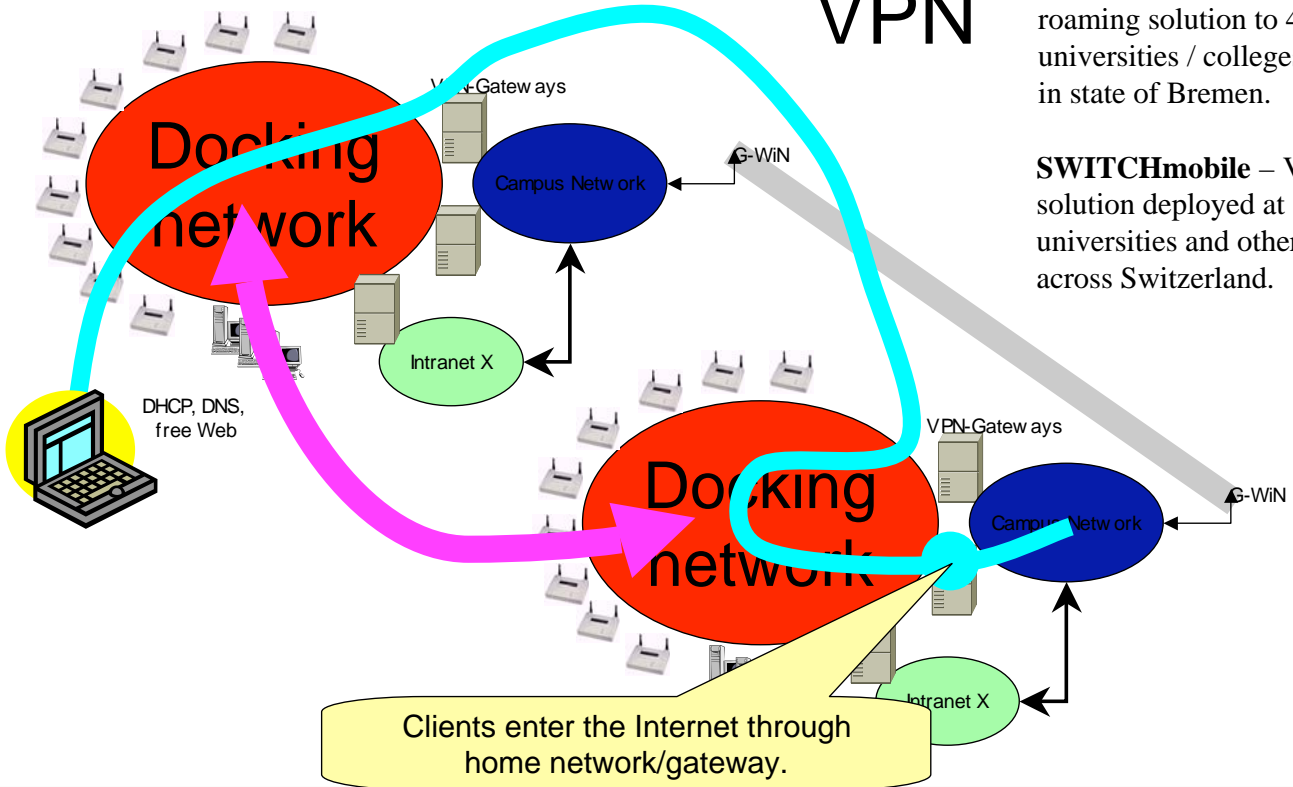
- ▶ RADIUS backend: build **RADIUS hierarchy**
 - Use NAI to authenticate to existing authenticators
 - Nicely solves problem for .1X and Web
 - ➔ Klaas Wierenga
- ▶ VPN approach:
allow access to all VPN gateways from all docking networks
 - Users can connect to home gateway from any site
 - Technical approach:
Controlled Address Space for Gateways (**CASG**)



VPN

Wbone – VPN roaming solution to 4 universities / colleges in state of Bremen.

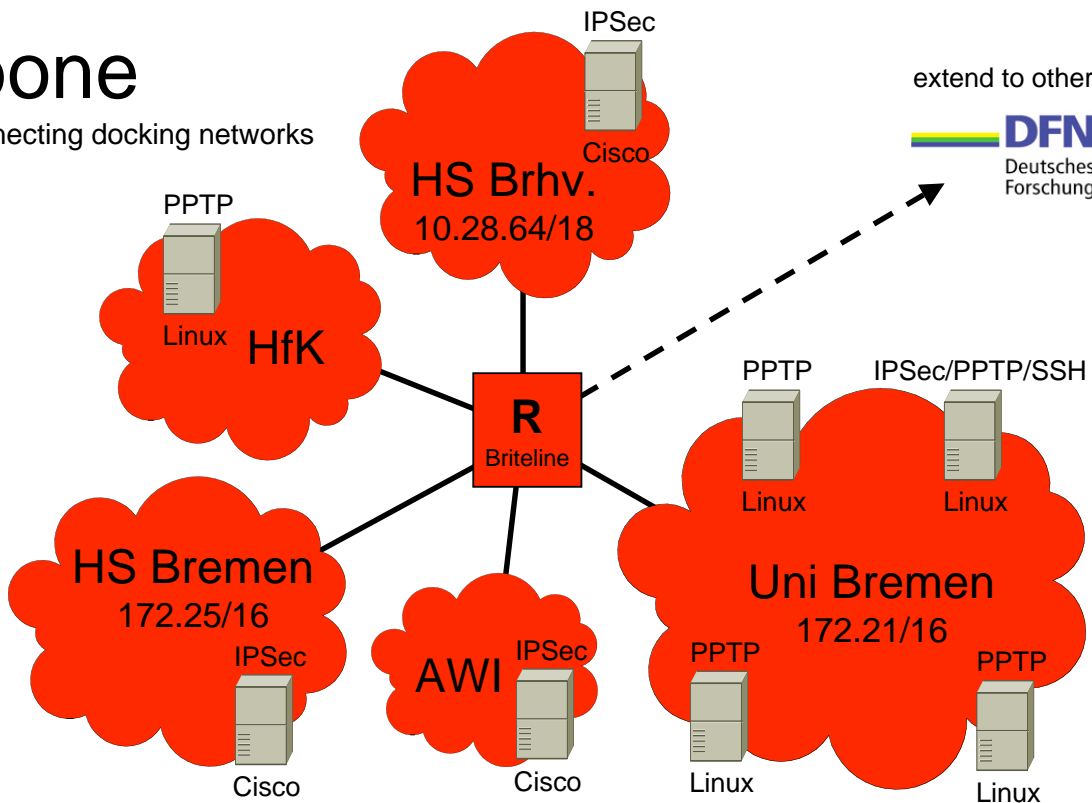
SWITCHmobile – VPN solution deployed at 14+ universities and other sites across Switzerland.



Wbone

interconnecting docking networks

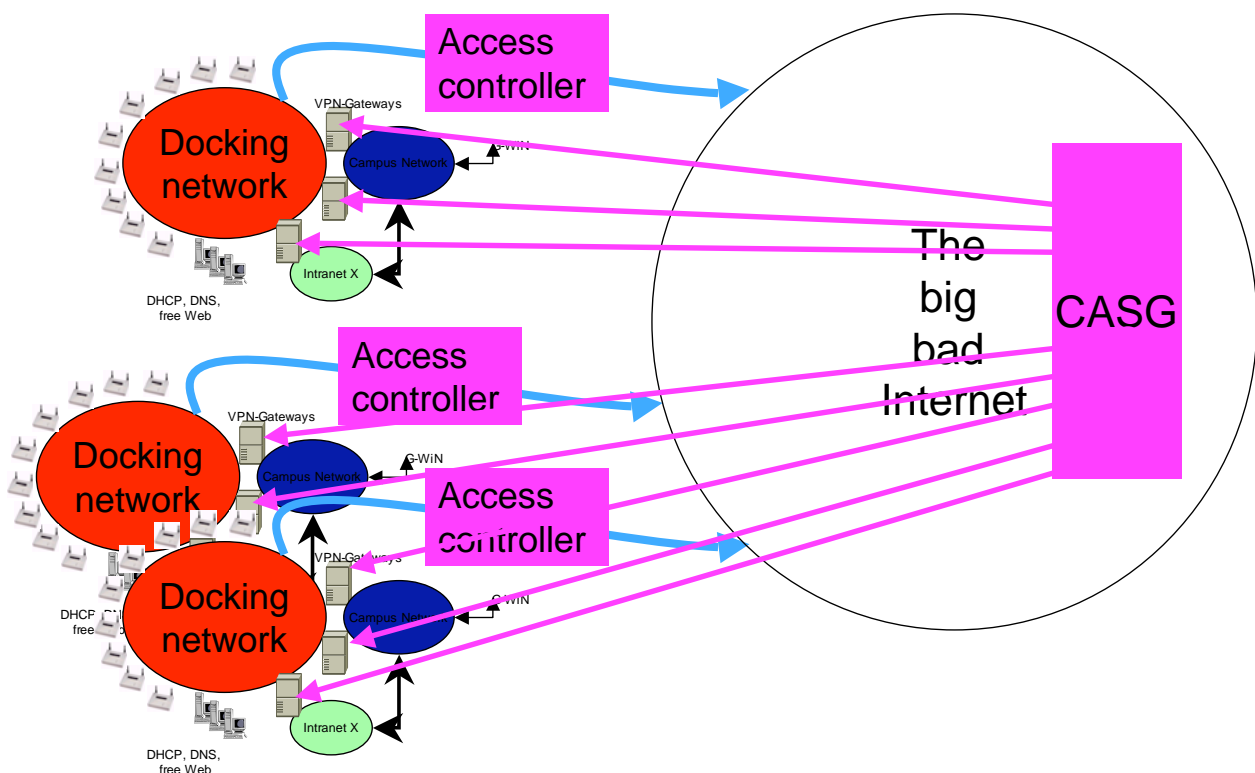
extend to other sites ...



The CASG

```
inetnum: 193.174.167.0 - 193.174.167.255
netname: CASG-DFN
descr: DFN-Verein
descr: Stresemannstrasse 78
descr: 10963 Berlin
country: DE
admin-c: MW238
tech-c: JR433
tech-c: KL565
status: ASSIGNED PA
mnt-by: DFN-LIR-MNT
changed: poldi@dfn.de 20040603
source: RIPE
```

- ▶ Separate docking networks from controlled address space for gateways (CASG)
- ▶ Hosts on docking networks can freely interchange packets with hosts in the CASG
 - Easy to accomplish with a couple of ACLs
- ▶ All VPN gateways get an additional CASG address
 - With some Cisco concentrators, this may require plumbing



Implications of the CASG model

All AAA issues stay local

- ▶ VPN Gateways decide locally whom they admit
- ▶ Guest user uses **home** IP address
 - Home is contact point of any incident enquiries
 - Can use IP address for (weak) authentication

- ▶ Remaining problem:
CASG plumbing

The CASG Pledge

- ▶ I will gladly accept any packet
 - There is no such thing as a security incident on the CASG
- ▶ I will not put useful things in the CASG
 - People should not be motivated to go there except to authenticate or use authenticated services

- ▶ I will help manage the prefix space to remain stable

Good **eduroam** Citizens

- ▶ 802.1X
 - Secure SSID
 - RADIUS
 - ▶ Web-based captive portal
 - Open SSID
 - RADIUS
 - ▶ VPN-based
 - Open SSID
 - No RADIUS
- } RADIUS backend
- } Docking net (open SSID)

How can I help... as a home institution

Implement the other backend:

- ▶ As a RADIUS-based site
 - Implement a CASG VPN gateway (or subscribe to an NREN one)
 - Provide the right RADIUS for all frontends
- ▶ As a VPN site
 - Run a RADIUS server
- ▶ Help the users try and debug their roaming setup while at home (play visited site)

How can I help... as a visited institution

Implement the other frontend:

- ▶ As a docking network site
 - Implement the other docking approach:
 - CASG access or Web-diverter
 - Implement a 802.1X SSID (“eduroam”) in addition to open SSID
- ▶ As an 802.1X site
 - Implement an open SSID with CASG access and Web-diverter
- ▶ Your local users will like it, too
 - Maybe too much...

Fun little issues

- ▶ 1/3 of Bremen’s 432 Cisco 340 APs can't do VLANs
 - Ethernet interface hardware MTU issue
- ▶ Some client WLAN drivers are erratic in the presence of multi-SSID APs
- ▶ Can't give university IP addresses to roamers
 - Too many university-only services are “authenticated” on IP address
 - Address pool must be big enough for flash crowds
- ▶ CASG space is currently allocated on a national level
 - So there will be a dozen updates before CASG is stable

Security objectives reached?

▶ Privacy/Confidentiality

- VPN, .1X: very good
 - Home site is revealed, though
 - .1X: Home site can make some ID information available for visited site
- Web: mediocre
 - Authentication information visible at Web redirector
 - Data visible (if not protected by VPN)

▶ Authentication/Accountability

- VPN, .1X: very good
 - More information is visible to visited site admin in 802.1X
- Web: mediocre
 - Hijacking too easy

Conclusions

- ▶ It is possible to create a fully interoperable solution
- ▶ It's not that hard:
 - especially when you use TF mobility's deliverables to guide you
- ▶ Integration approach also provides an easy upgrade path
 - E.g., add 802.1X to docking-only site

Conclusions

- ▶ It is possible to create a full, interoperable solution
- ▶ It's not that hard:
 - especially when you use TF mobility deliverables to guide you
- ▶ Integration approach also provides an easy upgrade path
 - E.g., add IEEE 802.1X to docking only site

GO for it

<http://www.terena.nl/mobility/>