Wbone:
WLAN Roaming Based on Deep Security

Zagreb, May 22nd, 2003

Carsten Bormann <cabo@tzi.de>
Niels Pollem <np@tzi.de>
with a lot of help from TERENA TF Mobility

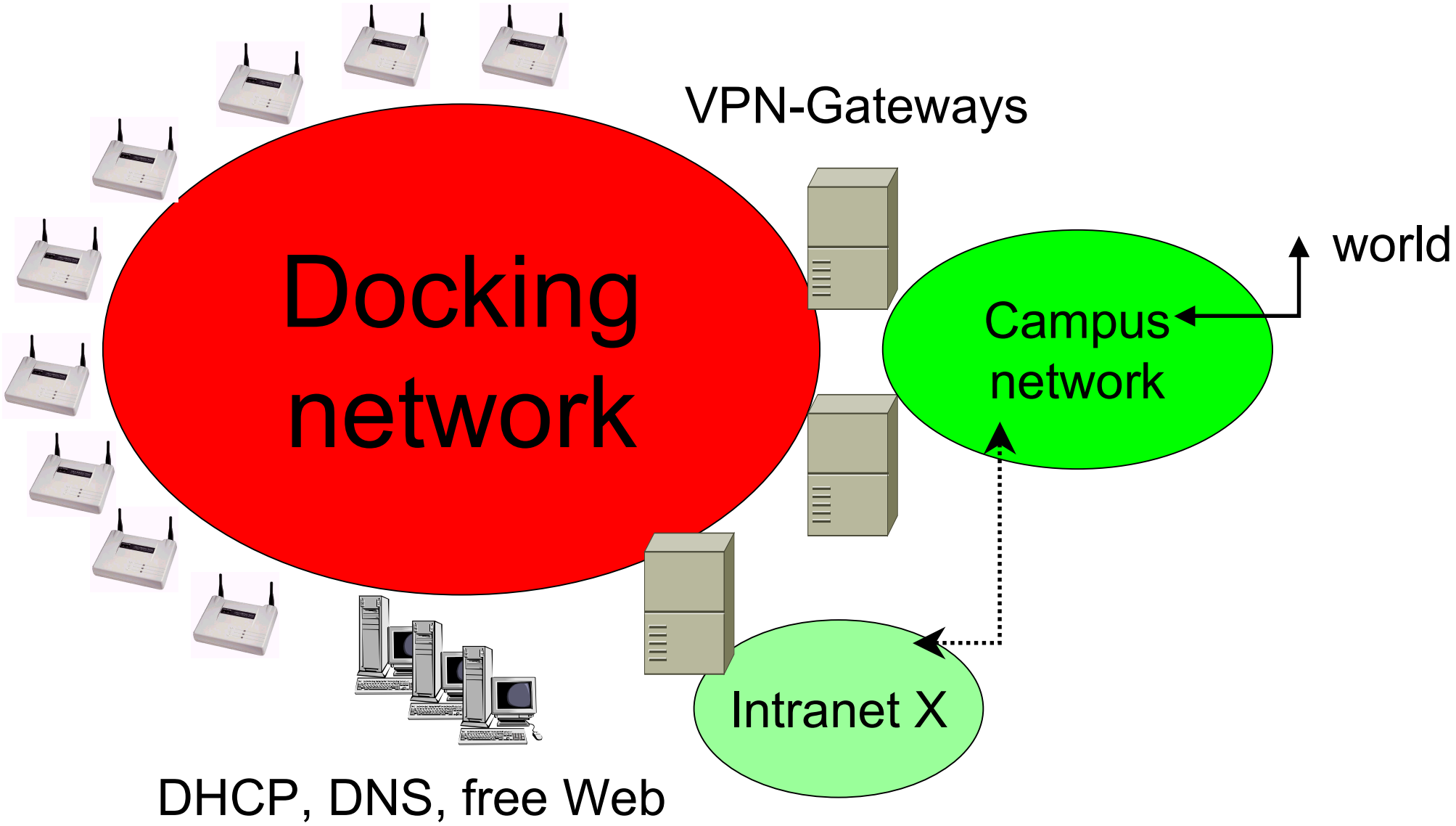
WLAN Security: Requirements

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

Security is rarely easy

WLAN Security: Approaches

- AP-based Security: AP is network boundary
  - WEP (broken), WEP fixes, WPA, …
  - 802.1X (EAP variants + RADIUS) + 802.11i
- Network based Security: deep security
  - VPNs needed by mobile people anyway
  - SSH, PPTP, IPsec
    - Allow development of security standards
    - Some VPN technologies are IPv6 enabled
  - AP-based security not needed anymore!


VPN-Gateways
Docking network
Campus network
world
Intranet X
DHCP, DNS, free Web

“Standard Architecture” (DE)

- all Access Points in one Layer-2 VLAN (RFC 1918) – docking network
  - use specific SSID (“Uni-Bremen”) for access (explicit!)
- little infrastructure in docking network
  - DHCP, DNS, “free services” (internal Web)
- one VPN-Gateway each for target networks
  - Campus Network, workgroups, possibly w/ Firewalls ➔ decentralize
  - SSH, PPTP, IPsec ➔ clients for all platforms
  - Gateway Cheap hardware (PC w/ Linux)
- “standard” = used in many German universities

WLAN Access Control: Why VPN based?

- Historically, more reason to trust L3 security than L2
  - IPSec has lots of security analysis behind it
- 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 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!
- Easy to accommodate multiple security contexts
  - with Cisco 1200 and other products (to be shipped)

- Most of all: It just works™

WLAN Access Control: Why Web-based filtering is better

- No software (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 Greenspot etc.
- Privacy isn't that important anyway (use TLS and SSH)
- Accountability isn't that important anyway

- Most of all: It just works™

Users want to roam between institutions

- TERENA TF Mobility: Roam within Europe's NRENs
  - 802.1X with RADIUS (AP-based)
  - Access to VPN gateways (network-based)
  - Web-based authentication (network-based)
- Here: Bremen Approach (Wbone)
- http://www.terena.nl/mobility

DFN
Deutsches Forschungsnetz

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

Minimize admin overhead

- Very little admin work to enable roaming per user
  - (preferably none)
  - both for home network and even more so for visited network
- **No** admin work required per roaming occurrence

- Minimize the complexity of additional systems required
  - (consider architecture at the involved institutions)
  - must integrate with existing AAA systems, e.g., RADIUS
  - no n^2 work required when scaling system

- No regulatory entanglement

Good usability

- Available to most current WLAN (and wired) users
  - standards-based; low-cost
- No additional software required to enable roaming
  - (software may be required for local use beforehand)
  - consider both Laptop and PDA usage
- Enable all work
  - IPv4 and IPv6
  - Access to home institution networks
  - Enable use of home addresses while roaming
- Enable local work in visited network
  - SLP, authorization issues/user classes?

Security requirements

- Allow use only for approved [by who] NREN users
  - Legal binding to some common terms of use
- Provide accountability
- Nice to have: Provide reasonable basic (“like in wired access”) security for individual user [cannot fulfill in all environments]
  - Confidentiality of traffic
    - (not necessarily with respect to current position!)
  - Integrity/guard against data manipulation and session hijacking
- Allow real security (e2e) on top (e.g., highlight the limitations of NATs)

- Don’t aggravate security issues of visited networks

Security non-requirements

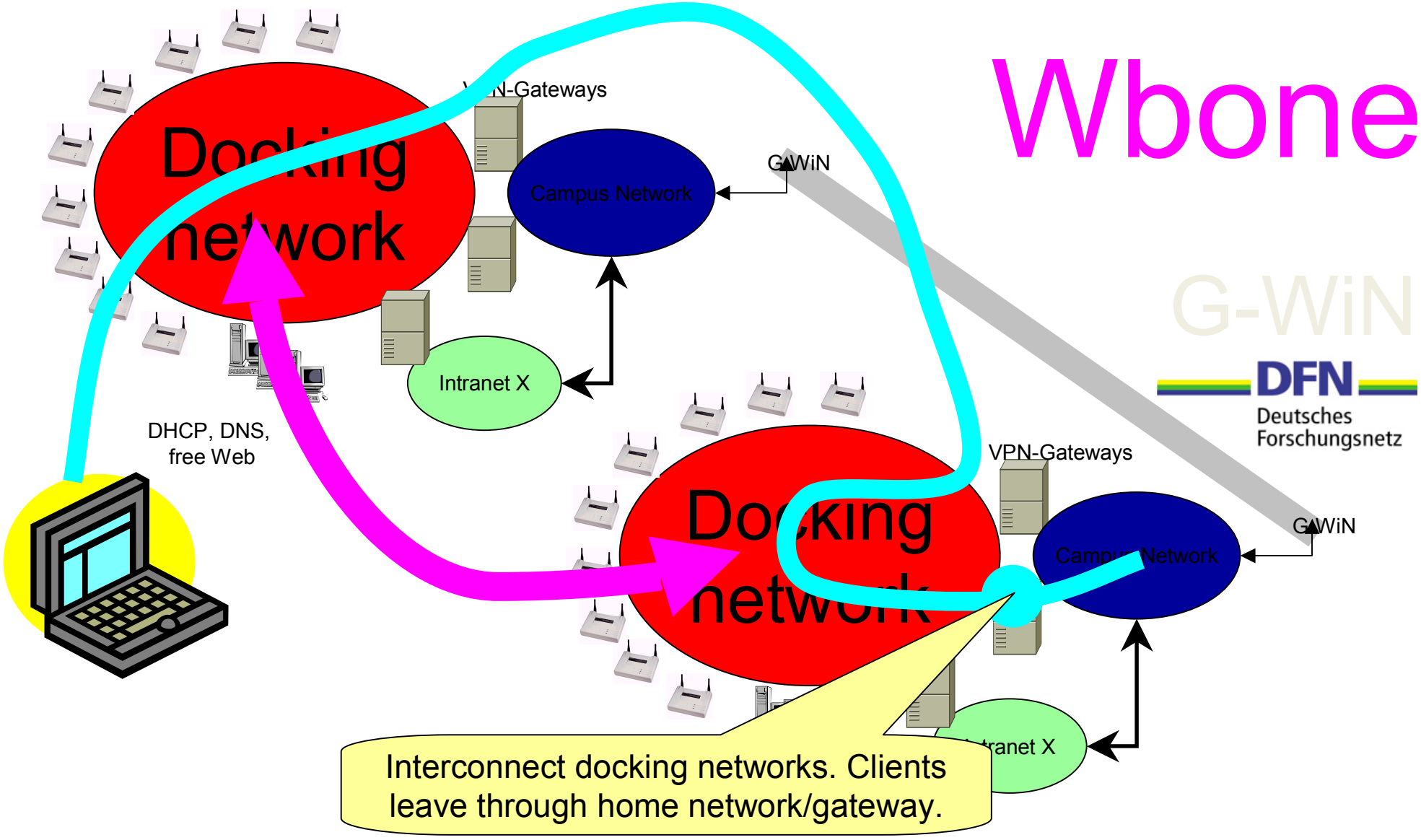
- No need to “protect” WLAN
  - ISM spectrum can’t be protected anyway
- Hard to reliably conceal positioning information

Bremen:
One State … Five Universities

Universität Bremen → shared programs
Hochschule Bremen
Hochschule für Künste
Hochschule Bremerhaven
International University Bremen

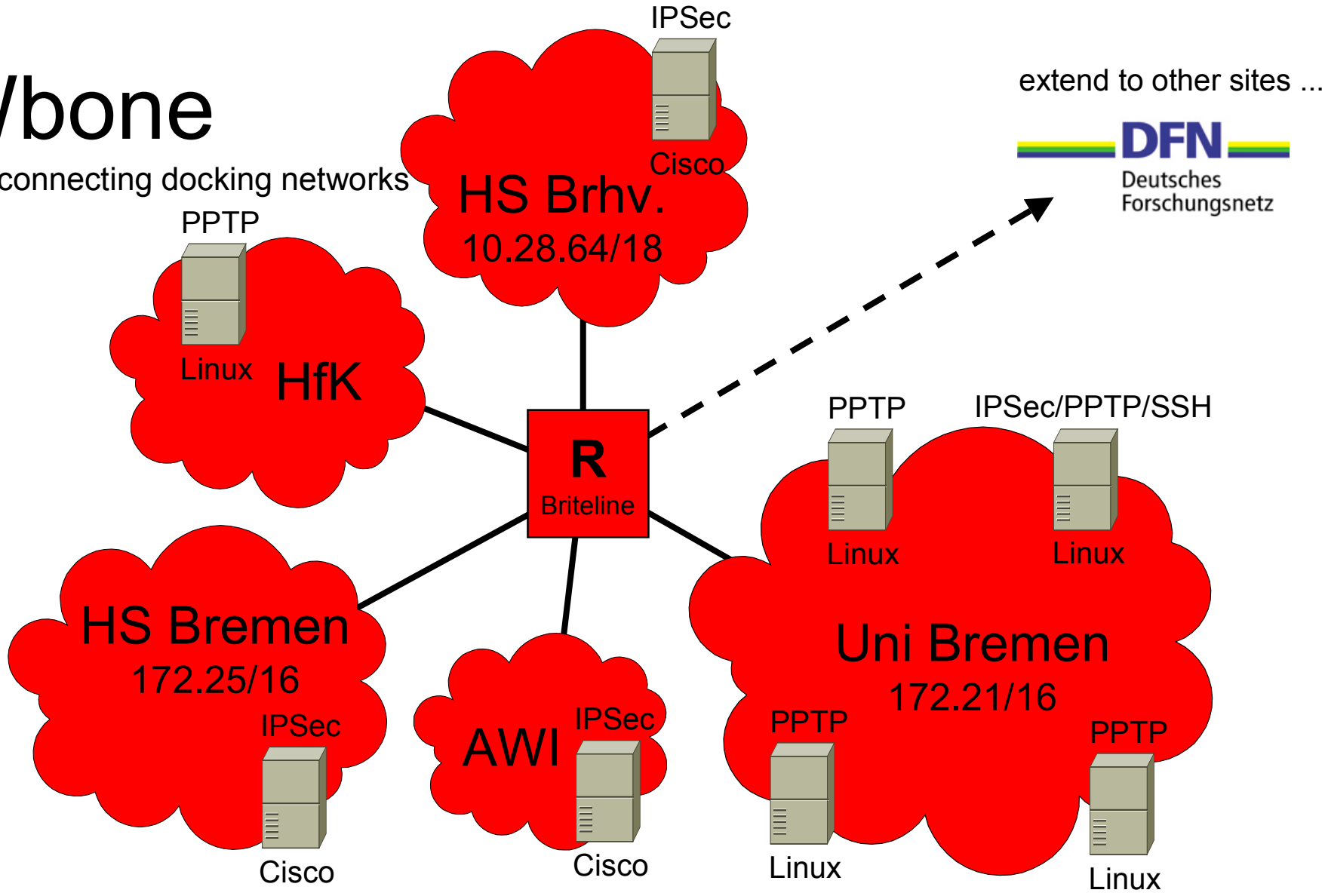
Wbone: VPN-based solution(s)

- Security (for 802.11): VPN-based (local) solution
  - widely adopted in Germany → interconnect
  - requires routing, address space coordination
- Bremen: create early user experience
  - by chance, different RFC 1918 networks used for docking networks
  - so, simply connect them via state‘s backbone
  - users can connect to home gateway from any site


Wbone
Docking network
VPN-Gateways
Campus Network
G-WiN
Intranet X
DHCP, DNS,
free Web
G-WiN
DFN
Deutsches
Forschungsnetz
Docking network
VPN-Gateways
G-WiN
Interconnect docking networks. Clients
leave through home network/gateway.

Wbone

interconnecting docking networks



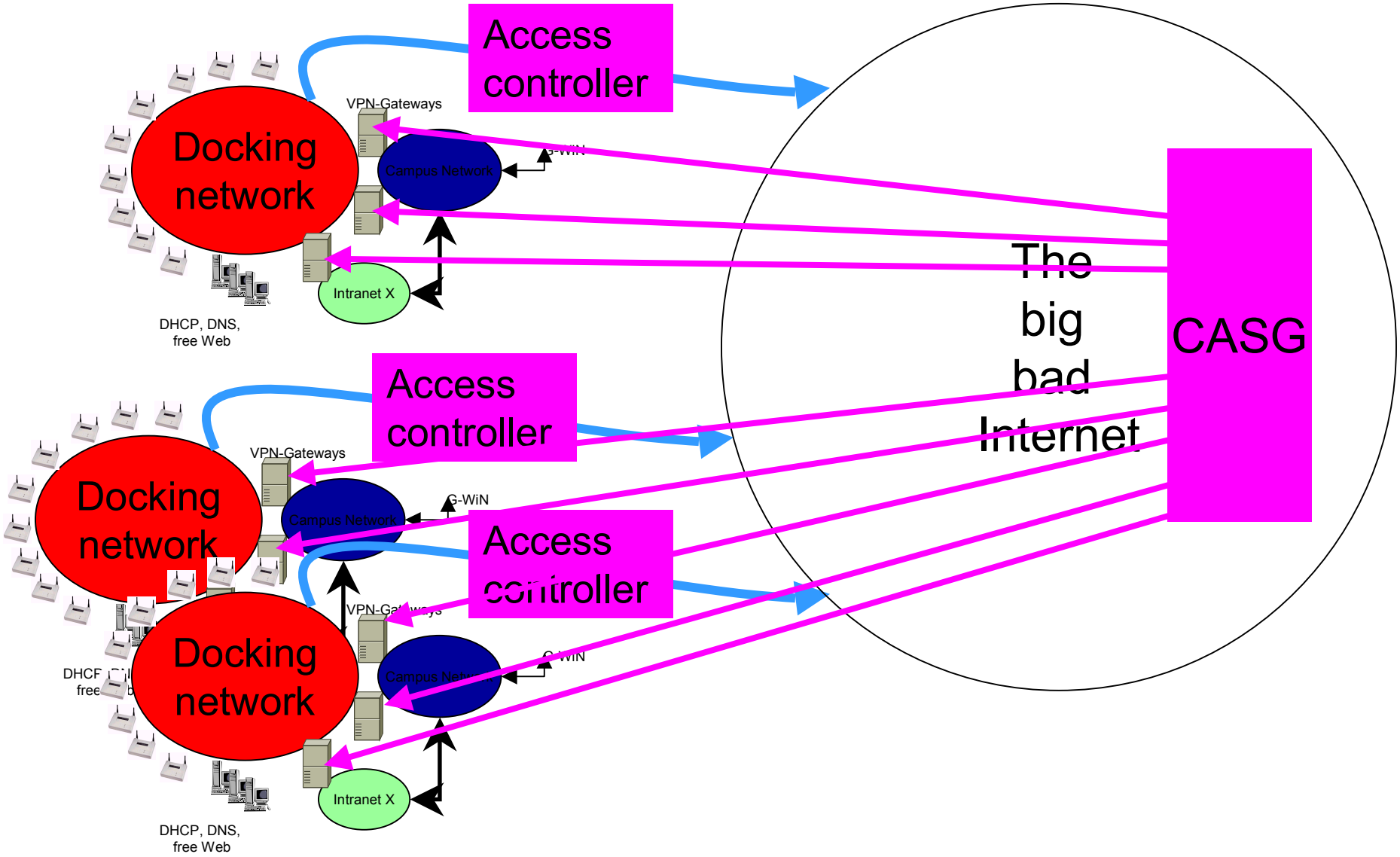
Wbone:
the user experience is there ...

- no need for users to change their configuration
  - that's the way it's supposed to be
  - staff and students can roam freely, 1800 registered daily!
- now, make it scale
  - address coordination, DNS
  - OSPF, GRE, VRF
    - routable addresses vs. RFC 1918

Wbone: Moving to Europe

- Scale private address architecture to European level?
  - Do all this in **public, routable address space** instead!
- Separate docking networks from controlled address space for gateways (CASG*)
  - Docking networks allow packets out to and in from CASG
    - Need to add access control device (such as router with ACL)
  - Nicely solve the transit problem in the processe

*) née “relay network” (Ueli Kienholz)


Access controller
Docking network
VPN-Gateways
Campus Network
Intranet X
DHCP, DNS, free Web
The big bad Internet
CASG
Access controller
Docking network
VPN-Gateways
Campus Network
Access controller
Docking network
Intranet X
DHCP, DNS, free Web

CASG allocation

- Back-of-the-Envelope: 1 address per 10000 population
  - E.g., .CH gets ~600, Bremen gets ~60
- Allocate to minimize routing fragmentation
  - May have to use **some** tunneling/forwarding
- VPN gateway can have both local and CASG address

Interoperability?

- Both Web and .1X can use RADIUS hierarchy
  - VPN gateways can actually do it, too
- VPN sites probably want to add Web-based filtering
  - Helps Web and .1X users connected to RADIUS hierarchy
- Web-based sites usually call CASG access
  - By using RADIUS hierarchy, .1X users share
- .1X sites with Cisco 1200 can add "docking VLAN"
  - CASG access and Web-based filtering to accommodate visitors

YES

but lots of political problems

Political problem

- It makes **a lot of sense** for an NREN to force one variant
  - Fictional examples: FI: All Web, NL: all .1X, DE: all VPN
- Opening backdoors for other NRENs at the same time?
  - may make you seem less convincing :-)
- Let's do **the right thing**™ anyway…