

Security Achitectures for Mobile IPv6

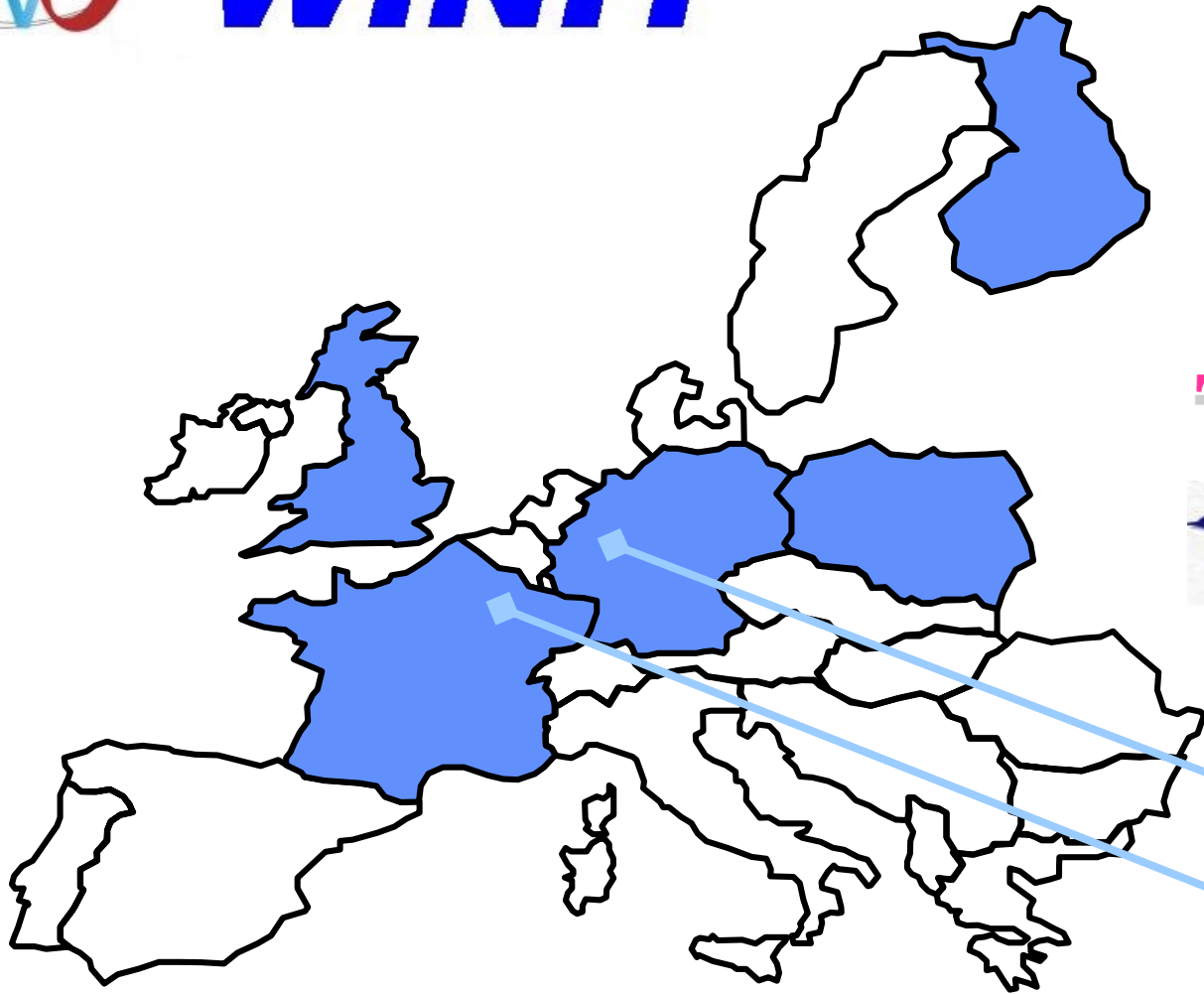
Euro6IX/ 6NET Workshop, Limerick, Ireland
Wednesday June 5th 2002

Thomas Scheffler
T-Systems Nova GmbH
Berkom

thomas.scheffler@t-systems.com

- Work in the 6WINIT Project
- Security Analysis of Mobile IPv6
- Possible Security Architecture
- Implementation
- Outlook

IRV6 WINIT



..... T-Systems

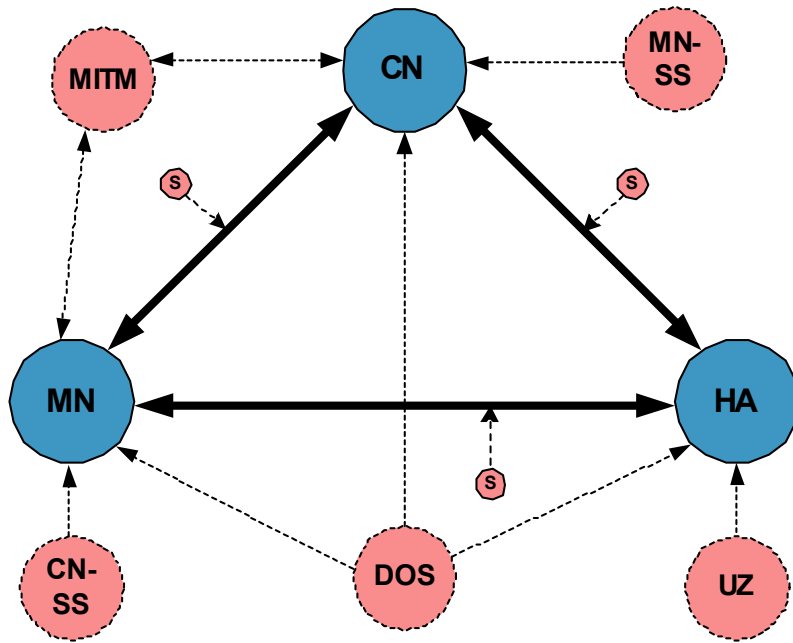
Validate introduction of Wireless Internet in Europe

- Based on IPv6 + GPRS and UMTS/3GPP
- Both personal and terminal mobility
- Full range of IPv6 Facilities
- Procedures for IPv6-2-3G Nets
 - Including IPv4/IPv6 network and application integration
- Investigate problems providing a trans-national wireless delivery service
- Early IPv6-ready applications testing
- Implement handsets and edge devices

Validate the feasibility of running real applications

Mobile Scenarios are designed to provide freedom for the user to roam about - they are susceptible to to by their very design

- distinguishing between legitimate and illegitimate use
- authentication, authorisation and accounting of use across administrative domains
- denial of service
- creating, distributing and enforcing policies
- eavesdropping



Tread	Possible Solution	Abbr.
Man in the Middle	Authentication of Control Messages	MITM
Eavesdropping	Line Encryption	S
Manipulation of Binding Cache (DoS)	Authentication of Control Messages	DOS
ICMP Attack	Access Lists for ICMP Requests on Router	DOS
Unauthorised Access	User Authentication, Access Lists, AAA	UZ
Session Stealing	Authentication of Control Messages	MN-SS CN-SS
Profiling	-	

Security Analysis of Mobile IPv6



Company / Project	Open Source	Draft Status	Security	Platform	Further Support
Ericsson/Telebit	No	13	No	Telebit Router	Yes
Microsoft	No	12	Status not clear	Windows	Yes
MIPL	Yes	15	Yes	Linux	Yes
Lancaster	Yes	5	No	Linux	No
Monarch	Yes	3	No	BSD	No
NEC	Yes	13	Yes	BSD	Yes
Cisco	First version planned for 4/2002				

- Currently most MIPv6 Implementations do not support secure control messages.
- A number of security issues is left to other protocols
- Scalability issues due to lack of 'Global PKI'

Proposed Architecture for 'Closed Systems'



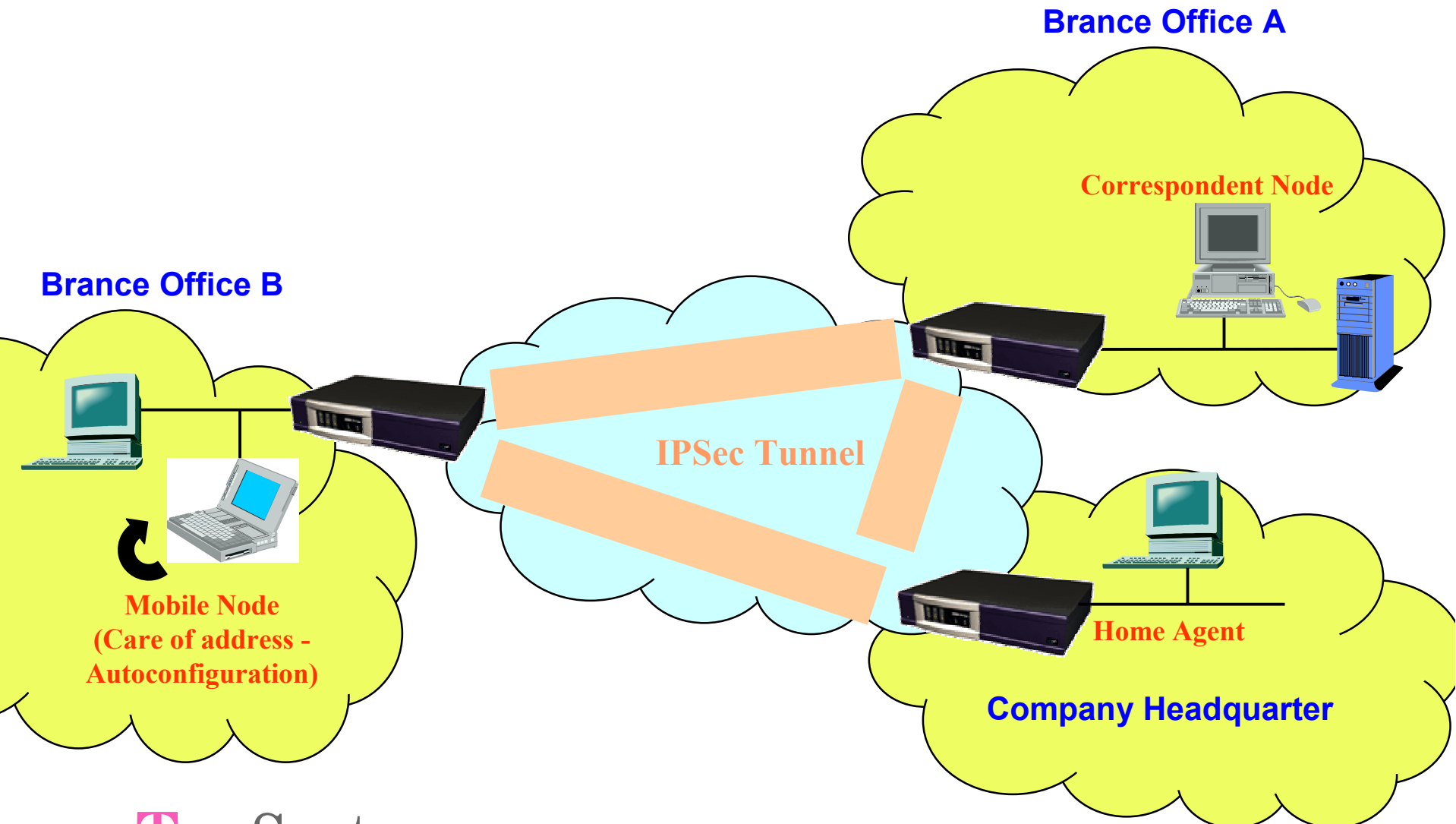
What is a closed system

- One administrative domain
- Users/machines are known in advance
- Single use policy
- Dedicated software environment

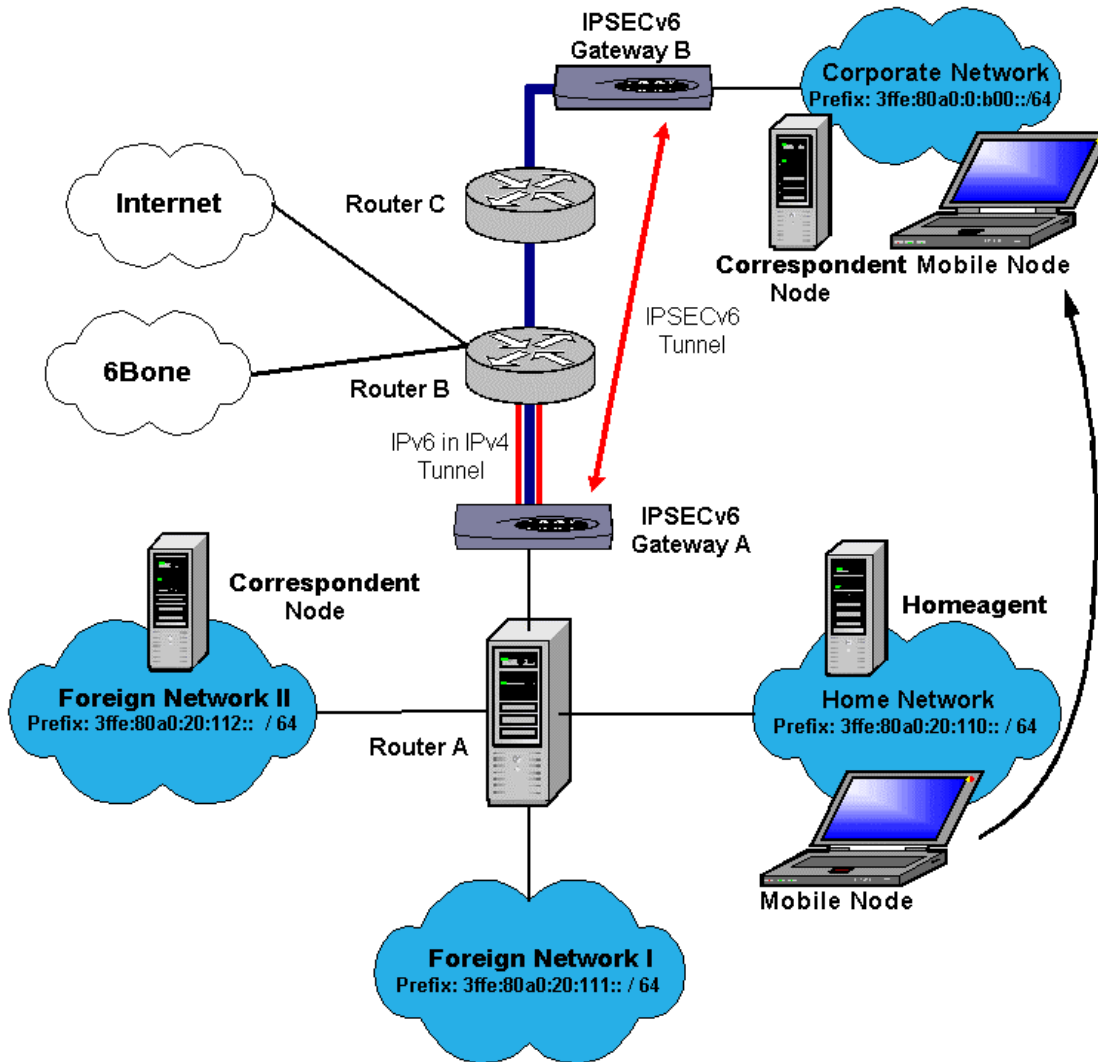
Characteristics of an closed system

- Authentication of users can used predefined tokens (MAC,...)
- Firewalling keeps out the rest
- Threads from within
 - Illegitimate use
 - Playful users
- No need to be 100 per cent standards compliant

Proposed Architecture for 'Closed Systems'



Lab Setup and Findings



Security Gateways:

- FreeSWAN (IABG)

Mobile IPv6:

- MIPL

Findings:

- Authentication of Binding Updates not yet possible (MIPL freezes)
- No implementations for Draft 16/17 (Reverse Routability)
- Solution for small installations
- Critical components are missing
 - PKI
 - AAA
 - Policy Server
- All hosts need to support Mobile IP!

Things to do:

- Interworking (eg. FreeSWAN/MIPL, 6WIND Edge Device)
- Status of standardisation (New Drafts)
- Integration of MIP and IPsec Gateway on one Machine
- Thorough testing and validation of security
- Integration with AAA and PKI
- Securing Open Mobile IPv6 Installations

Thank you for your interest!



Thomas Scheffler

T-Systems Nova GmbH
Berkom
Next Generation Networks
Goslarer Ufer 35
10589 Berlin

Tel. +49 30 3497 2274
Fax +49 30 3497 2275
thomas.scheffler@t-systems.com