AUTOMOTIVE | INFOCOM | TRANSPORT & ENVIRONMENT | AERONAUTICS | SPACE | DEFENCE

Secure and mobile applications with IPv6

IABG-Presentation at the Luxembourg IPv6 event

Luxembourg, 12.07.2005

Industrieanlagen-Betriebsgesellschaft mbH
Einsteinstraße 20
D-85521 Ottobrunn

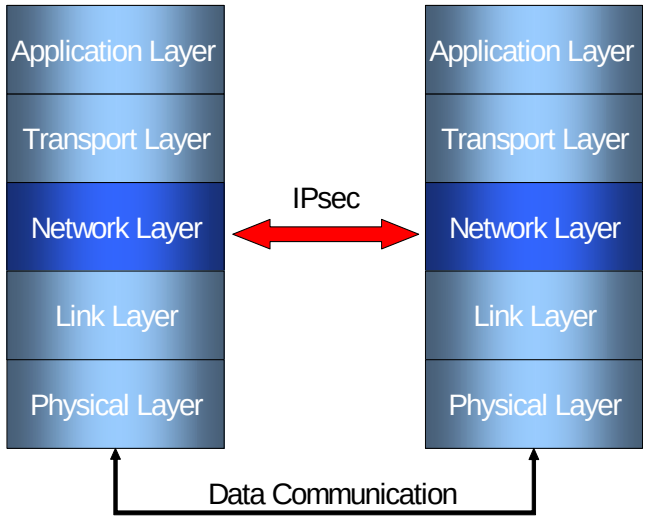
Agenda

- IPv6 security – facts & fiction
- IPv6 privacy – facts & fiction
- IPv6 mobility
- INSC: IPv6 in joint NATO operation
- IPv6 over satellite

IPv6 security-facts & fiction

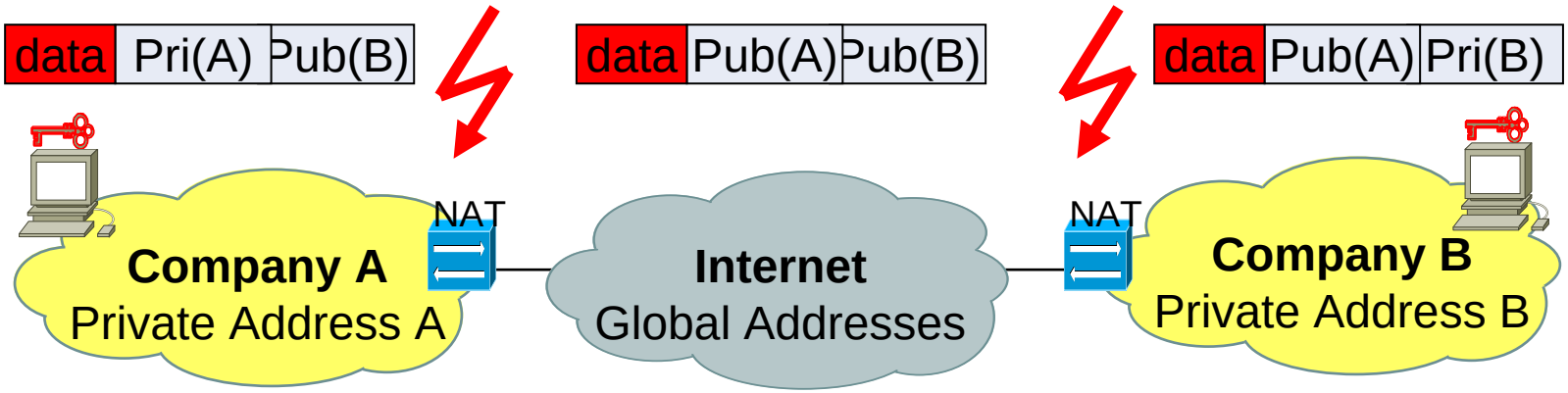
IPsec

- **Is IPsec for IPv6 more secure than IPsec for IPv4?**
  - Clear answer: NO!
- **There cannot be a major difference, as**
  - The IPsec functionality is on the same protocol layer
  - The IPsec protocol specification is the same
  - The algorithms / cryptography to be used are the same



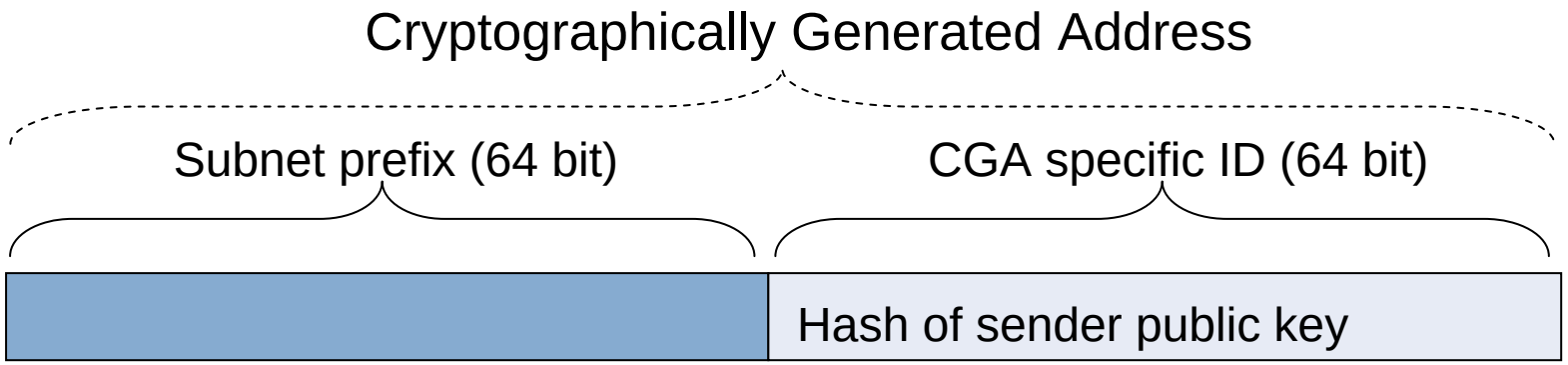
IPsec ctnd.

- **However, IPsec deployment will be easier in IPv6 due to the disappearance of NAT boxes**
  - NAT boxes modify IP packets and break therefore the end-to-end transparency
  - This modification also breaks end-to-end IPsec
  - Workarounds are complex and costly and often not possible at all



Cryptographically Generated Addresses

- **IPv6 addresses, which carry hashed information about public key in the identifier part**
- **Benefits**
  - Certificate functionality without requiring a key management infrastructure
  - Solution for securing IPv6 Neighbor Discovery (resolve chicken-egg problem of IPsec)



The side benefit of large address space

- **IPv6 uses 2^{64} addresses on a link instead of usually less than 28 for IPv4**
- **Attacks based on simply scanning a whole network**
  - would need years for performing it
  - would thereby consume a massive bandwidth on the scanned link
  - are therefore no longer appropriate
- **However**
  - one needs to take care about the addressing of server (use of arbitrary identifiers)
  - one needs to secure neighbor discovery messages

Viruses, worms and spam

- **Viruses, worms and spam are today some of the most annoying penetrations**
  - They infect user equipment
  - Consume significant network / computation resources
  - Have a large scale distribution
- **Can IPv6 prevent me from that?**
  - NO, as viruses, worms and spam are an application level problem, and have to be defended there
  - In the same way IPv4 cannot help here
  - However, IPv6 could make their fast distribution more complex (network scanning for vulnerable systems is more complex in IPv6)

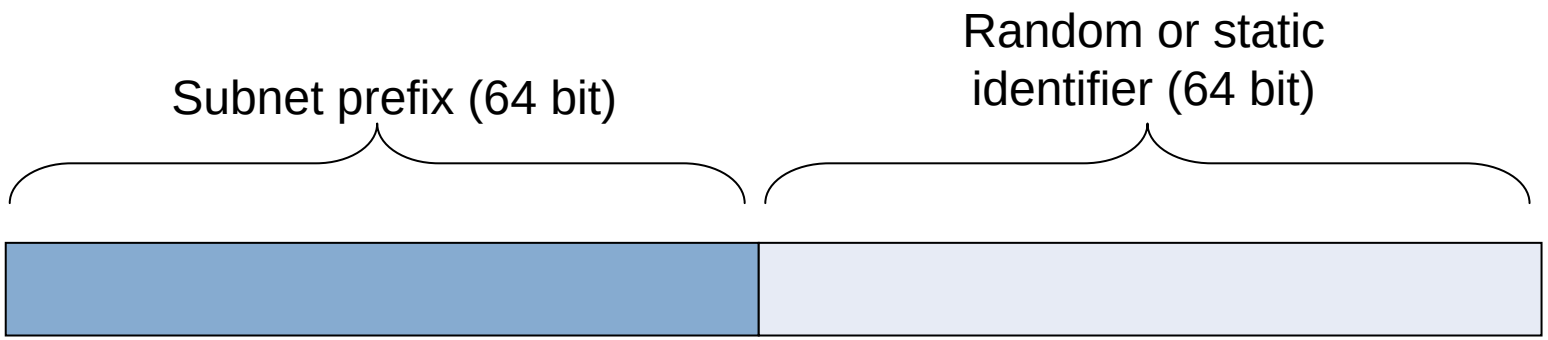
IPv6 security products

- **The main security product manufacturer support meanwhile IPv6 for IPsec, firewalling, IDS, …**
- **However, some of these products are just copies from IPv4 and don't reflect IPv6 specifica, e.g.**
  - Extended use of ICMPv6 requires different firewalling policies
  - Reflect the increased use of IP Multicast instead of Broadcast on local links
  - Make use of IPv6 address aggregation for more effective ingress filtering
  - Discard fragmented packets sourced from / destined to intermediate systems
  - Efficient support of tunneling, which will be intensively used during IPv6 transition
- **Further work is required here**

IPv6 privacy - facts & fiction

Tracability of (mobile) users

- **In stateless IPv6 address autoconfiguration identifiers can be derived from HW (static part in address)**
- **Does this mean that I‘m trackable (location, sites visited, …)?**
  - IPv6 supports also random identifiers for privacy reasons
  - These random identifiers are default setting in some operating systems



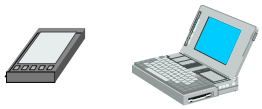
Disappearance of NATs

- **Without NAT boxes my home / company devices will have public addresses**
- **Does this mean that I‘m easily reachable from outside and therefore also more affected by attacks?**
  - NO, as NAT boxes do not give any security or privacy.
  - A (host) firewall can effectively shield parts which should not be reachable from outside.
  - Even more, a firewall can provide application layer security, a NAT box can not

IPv6 mobility

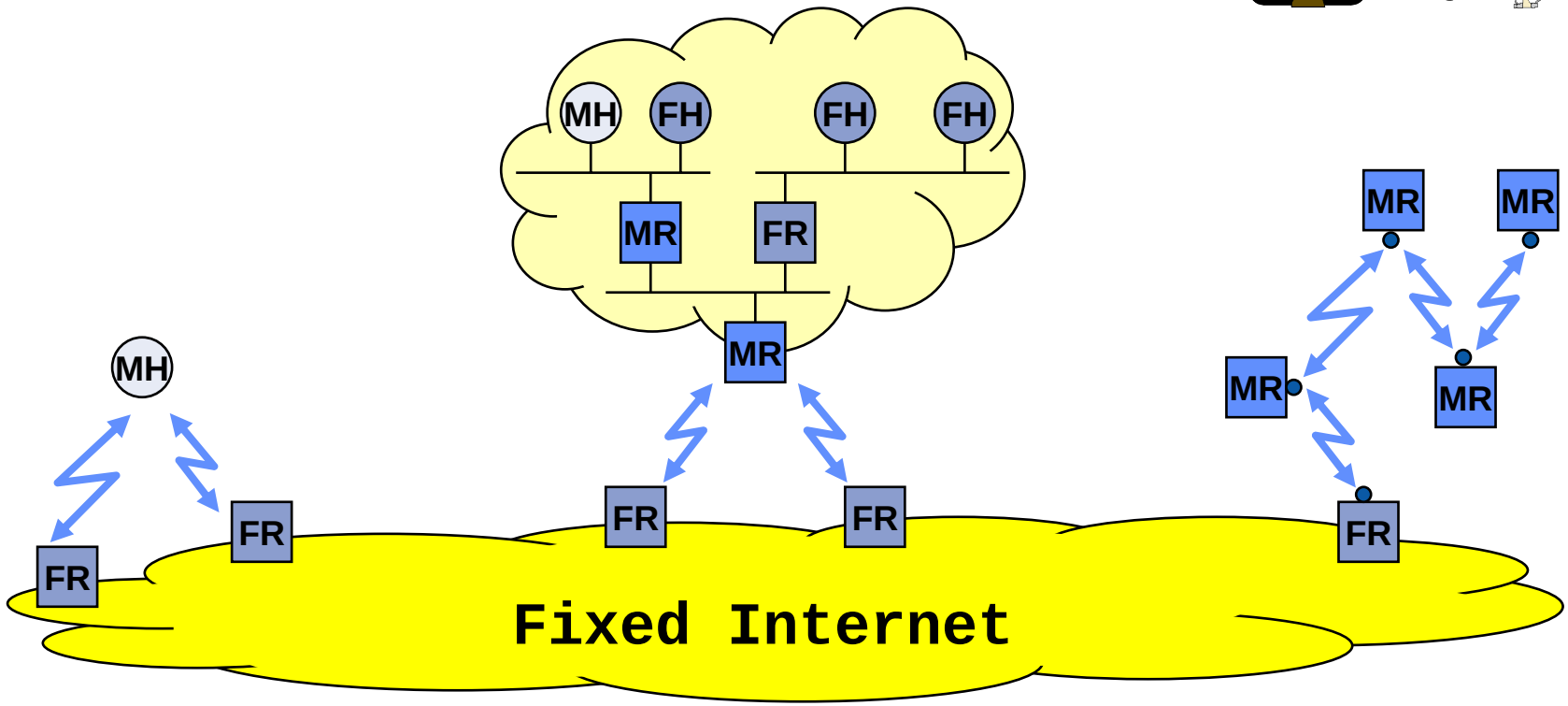
Mobility – Variety of scenarios

Host Mobility



Network Mobility

MANET



FH Fixed Host

FR Fixed Router

MH Mobile Host

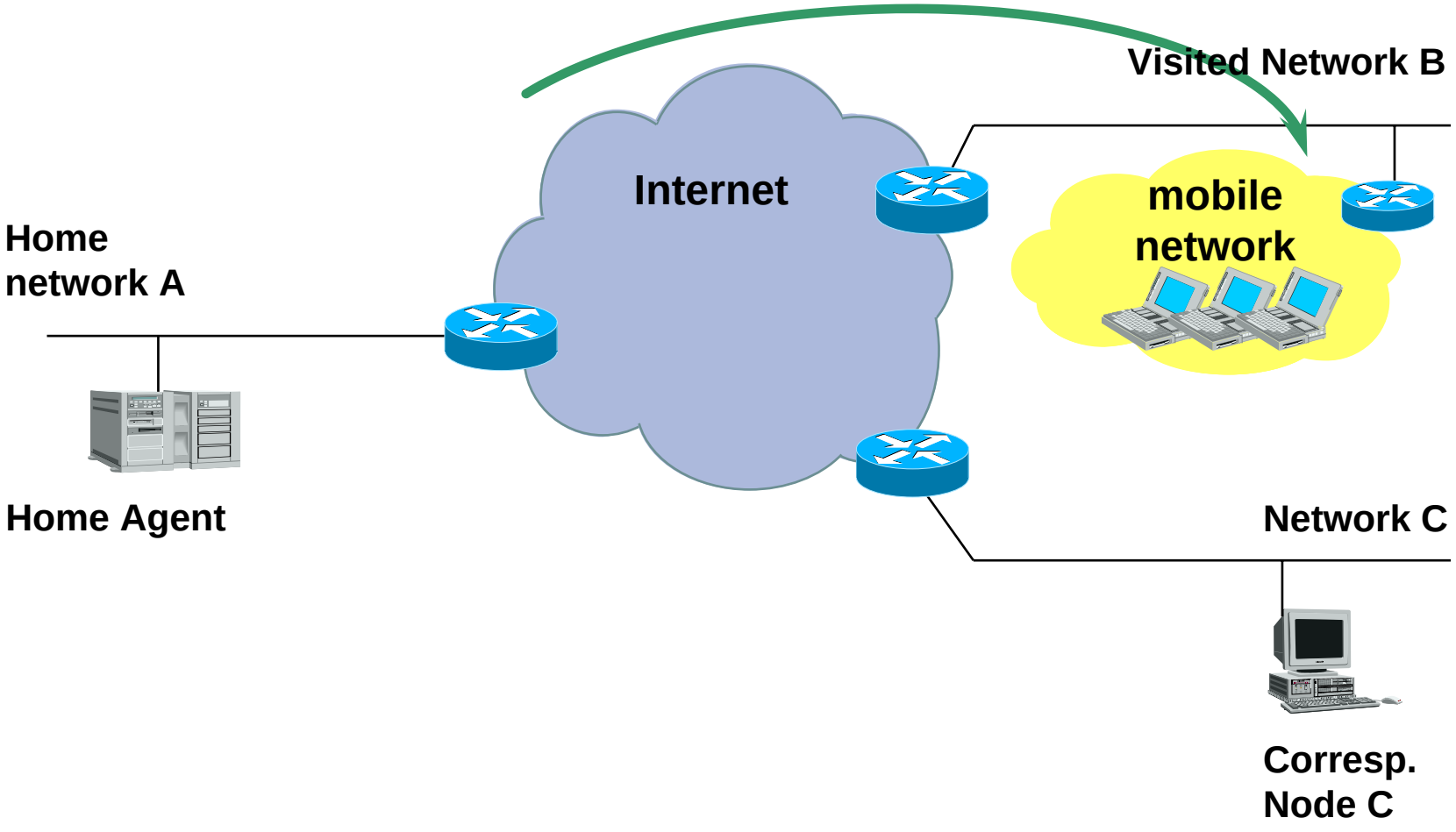
MR Mobile Router

FR Fixed MANET Router

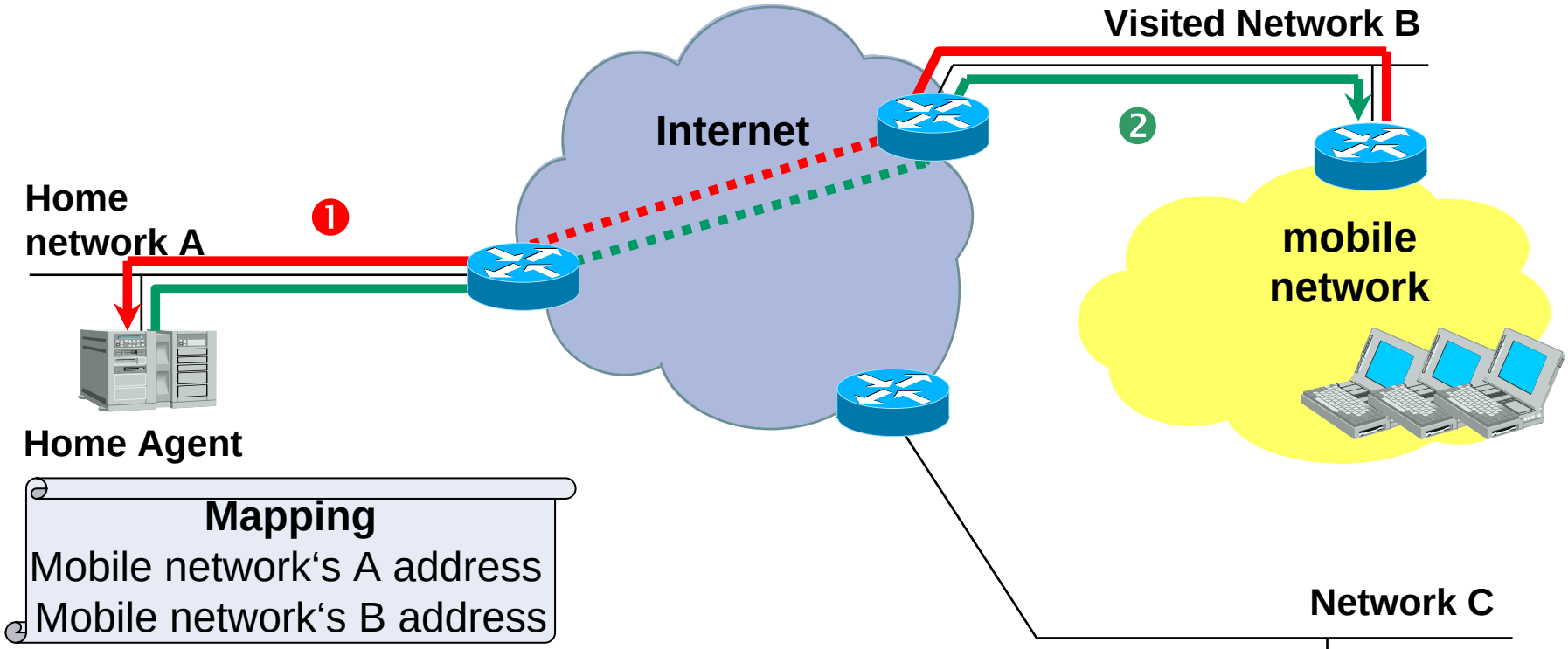
MR Mobile MANET Router

IABG

Network mobility – An example



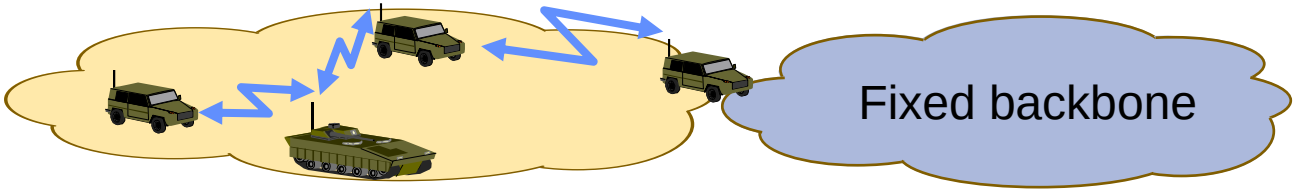
Network mobility – Home registration



1. Mobile Router sends Binding Update
2. Home Agent replies with Binding Acknowledgement

MANET – Overview

- In MANETs there is no fixed infrastructure
- MANET nodes have both, host and router functionality
- MANETs can (but don't have to) be connected to a fixed backbone via a MANET gateway
- MANETs can (but don't have to) have an aggregated address prefix
- MANETs need their own routing protocol for setting up connectivity between the different MANET nodes
- There are different kinds of MANETs
  - Proactive MANET: Route will be calculated in advance
  - Reactive MANET: Route will be calculated on demand
  - Hybrid MANET: Combination of proactive and reactive MANET

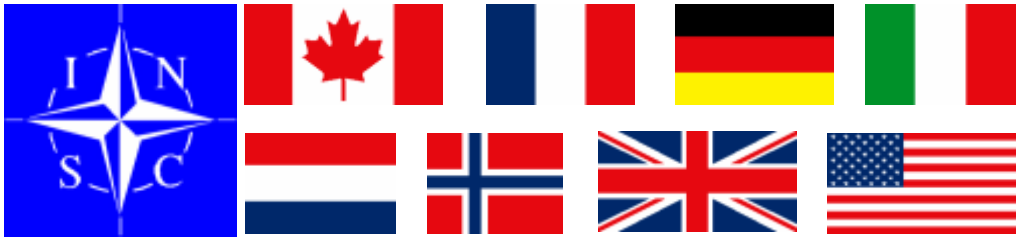


INSC

Interoperable Networks for Secure Communication

INSC - Overview

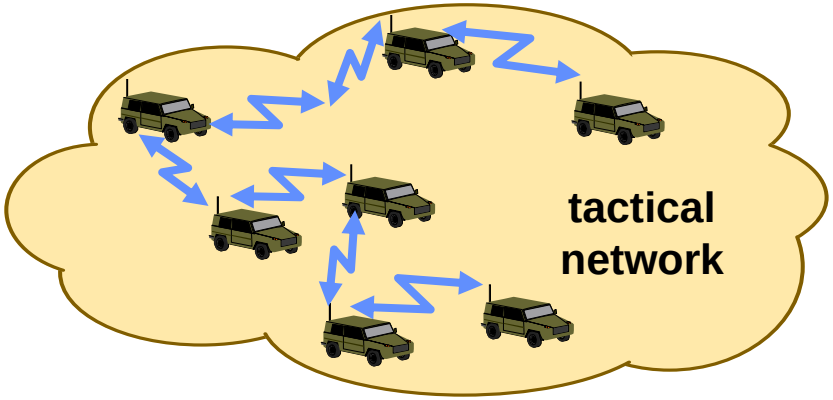
- Goal of INSC
  - Collaborative research on interoperable, manageable, secure, mobile military networks
  - Focus on IPv6
- Partners
  - 8 NATO partners plus NATO



- Phase 1
  - Begin: March 2001
  - End: February 2004
- Phase 2
  - Begin: March 2004
  - End: Summer 2006

INSC – German field tests done in autumn 2004

- Use of MANET technology to connect distributed military vehicles
- Extensive trial done with 10 vehicles in German military training area (38 x 10 km)
- Vehicles equipped with amplified WLAN technology and OLSR node
- Different operational scenarios (vehicle chase, patrol, airborne relay, …) and different applications (video, audio, remote data base access, …) performed

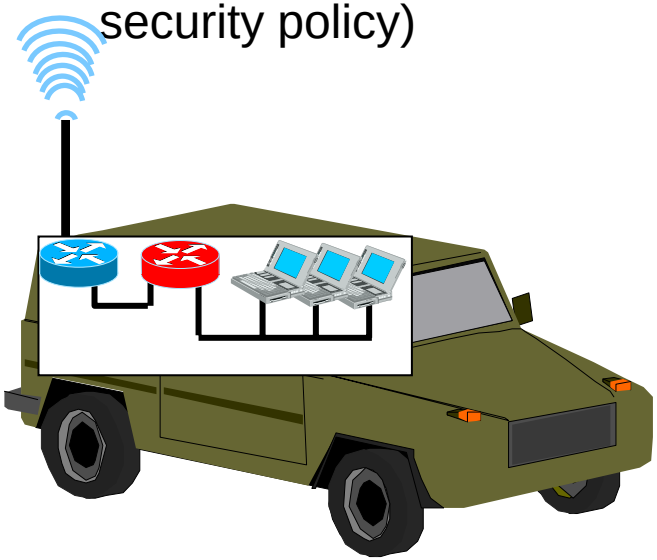


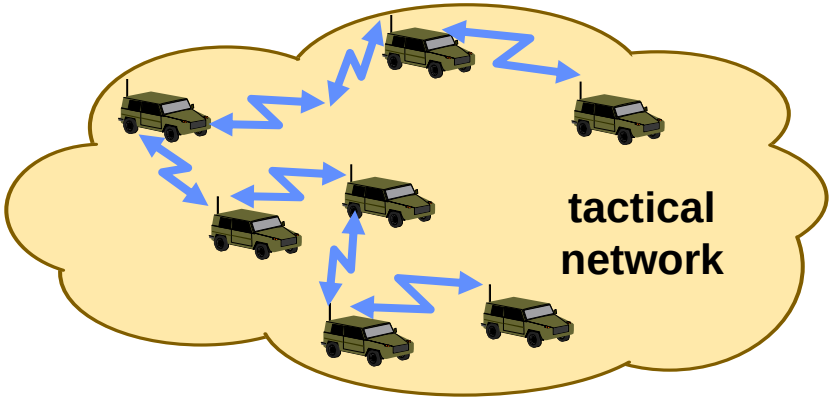
INSC – German field test 2005: Overview

- Use of 20 vehicles in total
- Vehicles will have on-board network (connecting e.g. terminals, sensors, actuators, …)
- Communication of on-board network will be secured
- Vehicles‘ router will be based on embedded PC platform
- Use of network mobility technology to increase range and resilience of MANET area
- Satellite technology will be used to connect
  - tactical network as whole
  - vehicles (planned for 2006)

INSC – German field test 2005: Vehicle with on-board network

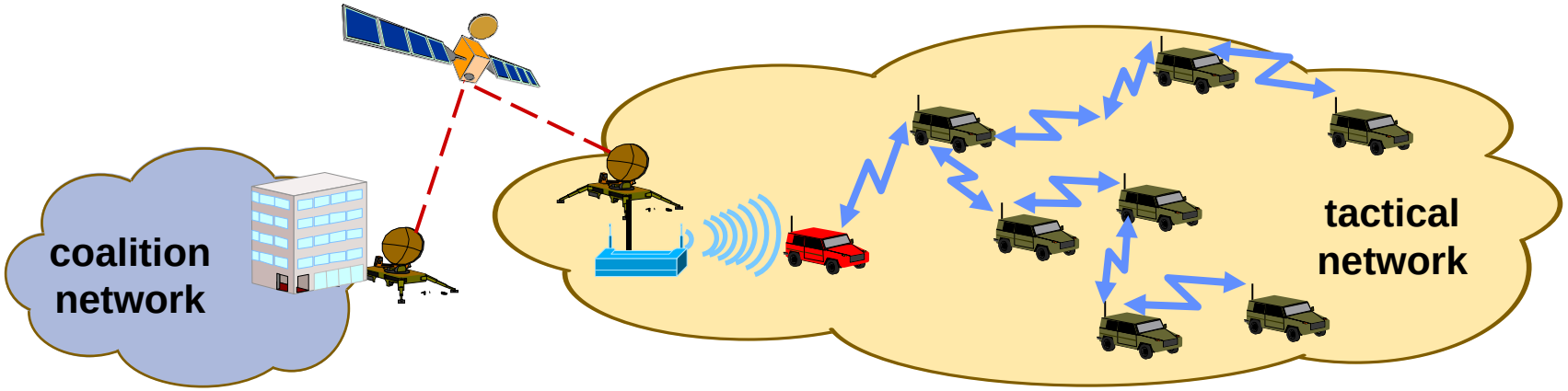
- Goal: Increase functionality of military vehicle
- Use of MANET technology to connect vehicle on-board network 
- On-board router runs OLSR protocol and connects on-board network (using OLSR HNA)
- On-board network is secured via IPsec gateway
- Mobile on-board router and IPsec gateway could be integrated (depends on security policy)





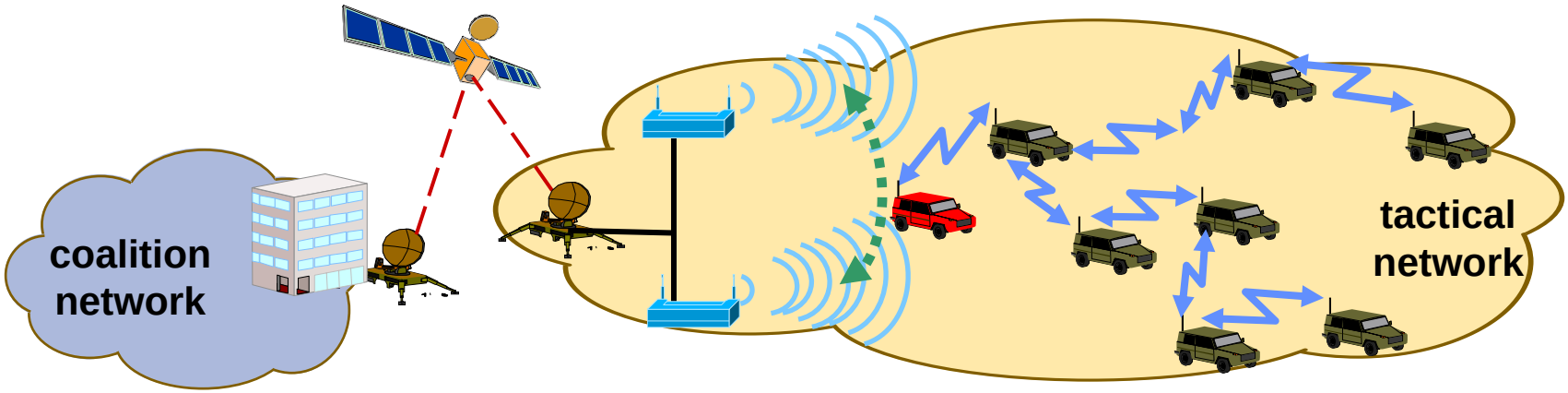
INSC – German field test 2005: Connection of tactical network

- Goal: Increase flexibility of tactical network connection
- Connection of the tactical network to the INSC coalition network via hub & spoke satellite network (IABG Teleport used as hub station)
- Forward link uses native IPv6 over DVB-S (ULE); return link terrestrial, alternatively SCPC
- Connection of MANET via MANET gateway  (two WLAN interfaces, one in ad-hoc mode, one in infrastructure mode)



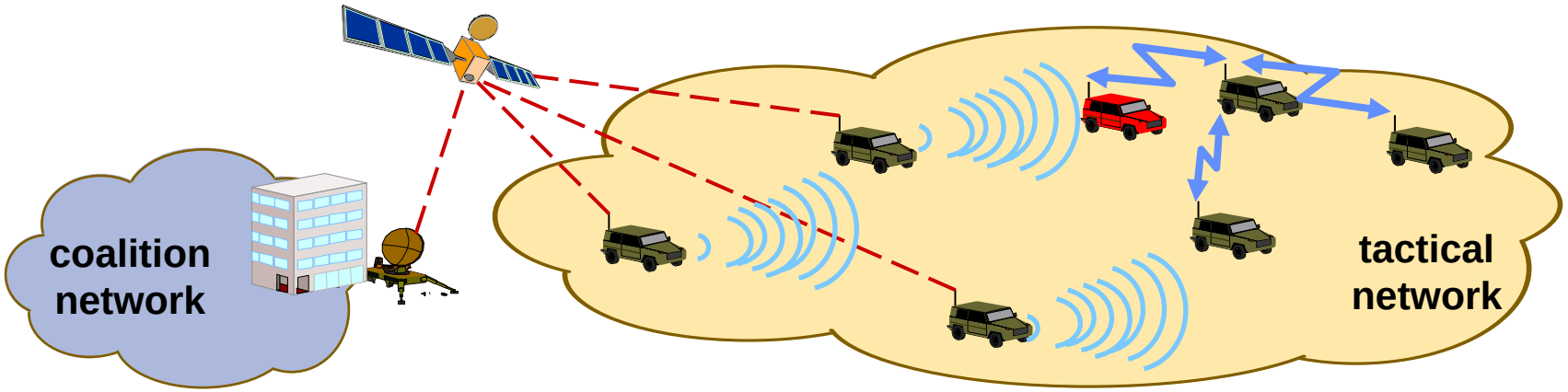
INSC – German field test 2005: Roaming of MANET gateway

- Goal: Increase range and resilience of tactical network connection
- MANET uses different, distributed wireless access points for its connection to the satellite network
- MANET gateway roams between these different access points
- For this purpose NEMO functionality is installed on the mobile on-board router
- There can be different vehicles acting as MANET gateway



INSC – Tests planned for 2006: Satellite access to the vehicle

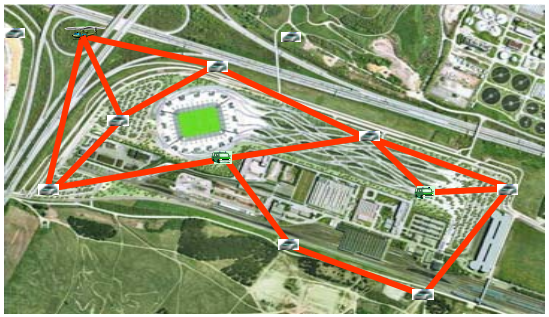
- Goal: Increase flexibility of tactical network connection
- Vehicles with their on-board network are connected directly via satellite to the coalition network using DVB-S / RCS as satellite technology
- Vehicle will have a DVB-S / RCS terminal (e.g. NERA, EMS) on-board
- Only restricted vehicle mobility (nomadic vehicles)
- Satellite connected vehicle can act as access router for MANET gateways 



INSC – Further possibilities for using this technology

- Police has raised their interest in this technology
  - Approach interesting for German Security Agency
  - One possible application scenario is the world soccer championship 2006 in Germany
  - Police would also use „handheld“ devices
  - Trials with IABG are planned

- Car manufacturer look into this technology
  - Support of roaming between different wireless networks (NEMO)
  - Car-2-car communication (MANET)



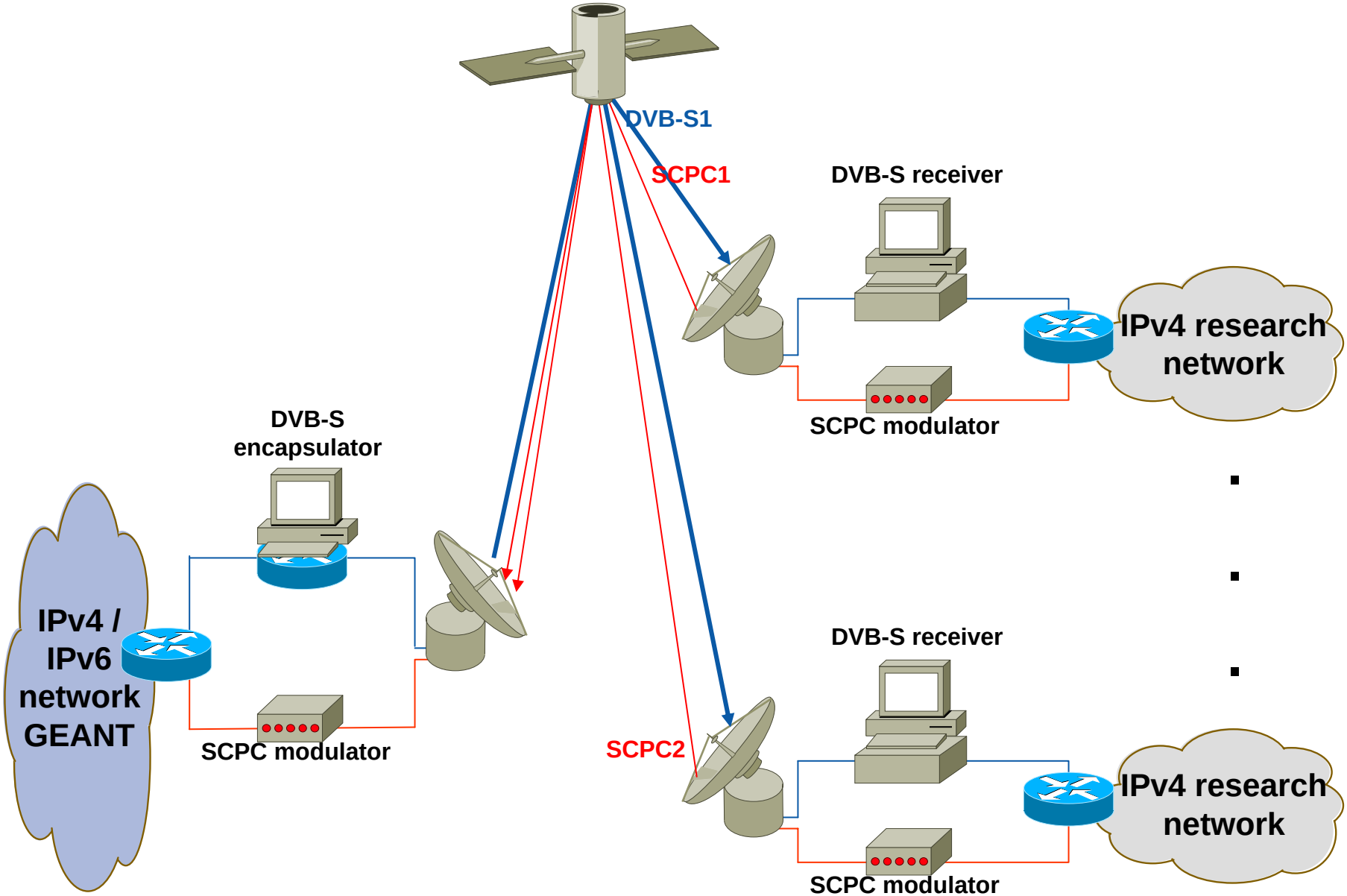
IPv6 over satellite

Background of SILK project

- In 2001, NATO Networking Panel decided to put in Regional Network for Newly Independent States (NISs) of the Southern Caucasus and Central Asia
- Wanted to connect existing NRENs into GEANT
- Start with own resources – $2.5 M for 3 years
- Allow to be extensible by others
- Information under http://www.silkproject.org

SILK Countries

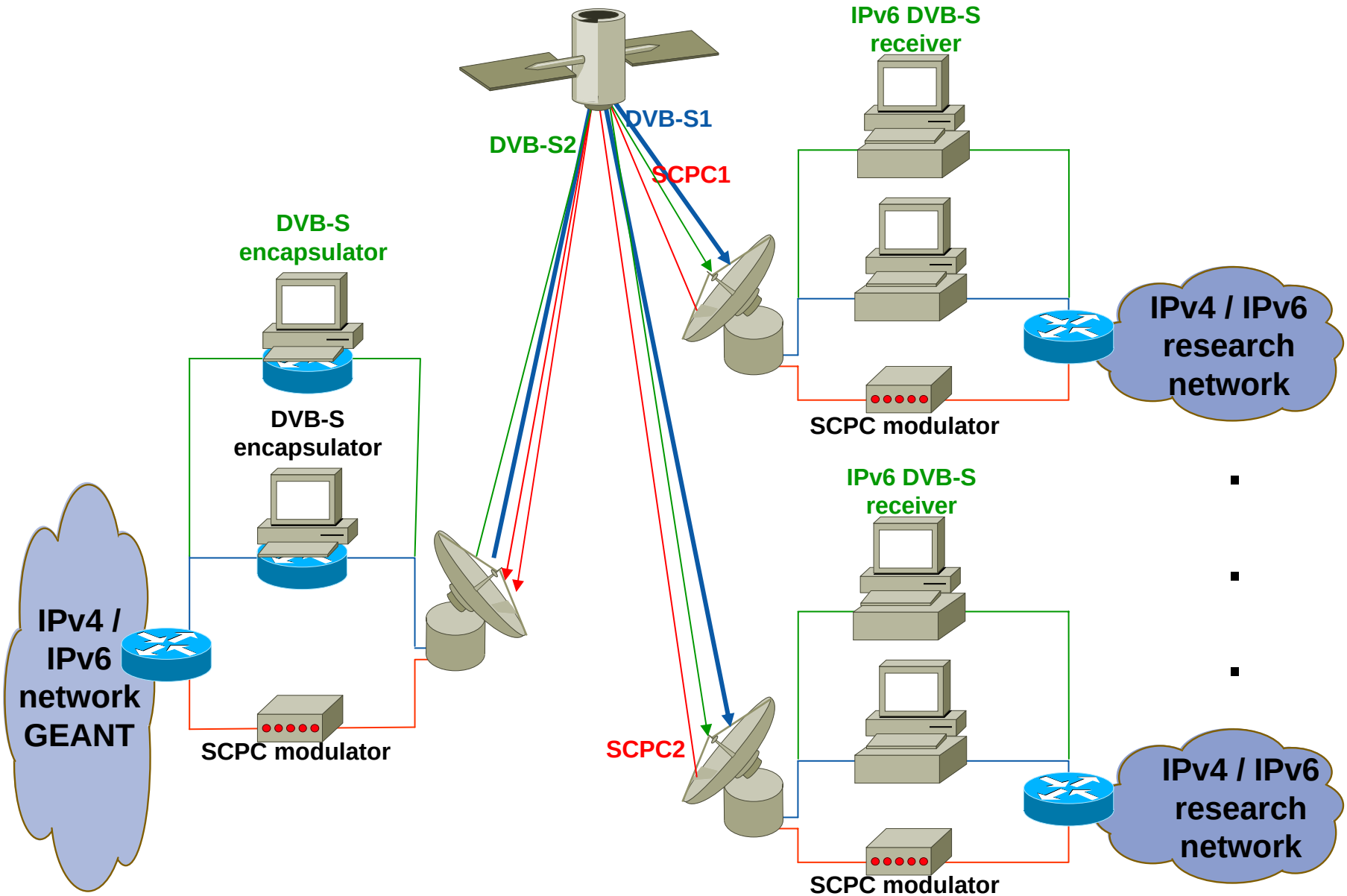
Current network architecture



Two alternative solutions to provide IPv6

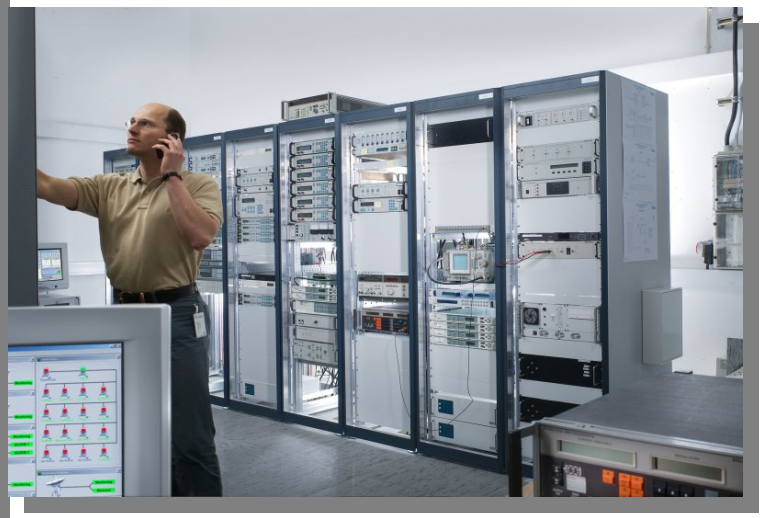
- SILK NRENs want also experience with IPv6
  - Provided it will not interfere with IPv4 services
- Use of IPv6 tunneling
  - Could be done with existing DVB-S equipment
  - Use of Ethernet bridging or IPv6 over IPv4 tunnel
  - Will be done by SILK project itself (using EC funding)
- Integration of native IPv6
  - Use of additional IPv6 capable DVB-S equipment based on ULE
  - Use of extra satellite bandwidth for IPv6
  - Will be provided to SILK by ESA / IABG

Network architecture with native IPv6 support



Equipment used in SILK

Tunnel solution on IABG Teleport



- Local access to IPv6 ISPs
- Transmit IPv6 tunneled on DVB-S
- Transmit IPv6 native on SCPC
- First commercial customers

Contact

Wolfgang Fritsche

Manager Advanced IP Services

Phone: +49 89 6088-2897
Email: fritsche@iabg.de
Web: www.iabg.de