ENABLING EFFICIENT AND OPERATIONAL MOBILITY IN LARGE HETEROGENEOUS IP NETWORKS

ENABLE
Enabling Efficient and Operational Mobility in Large Heterogeneous IP Networks

Projektvorstellung

Information Society Technologies

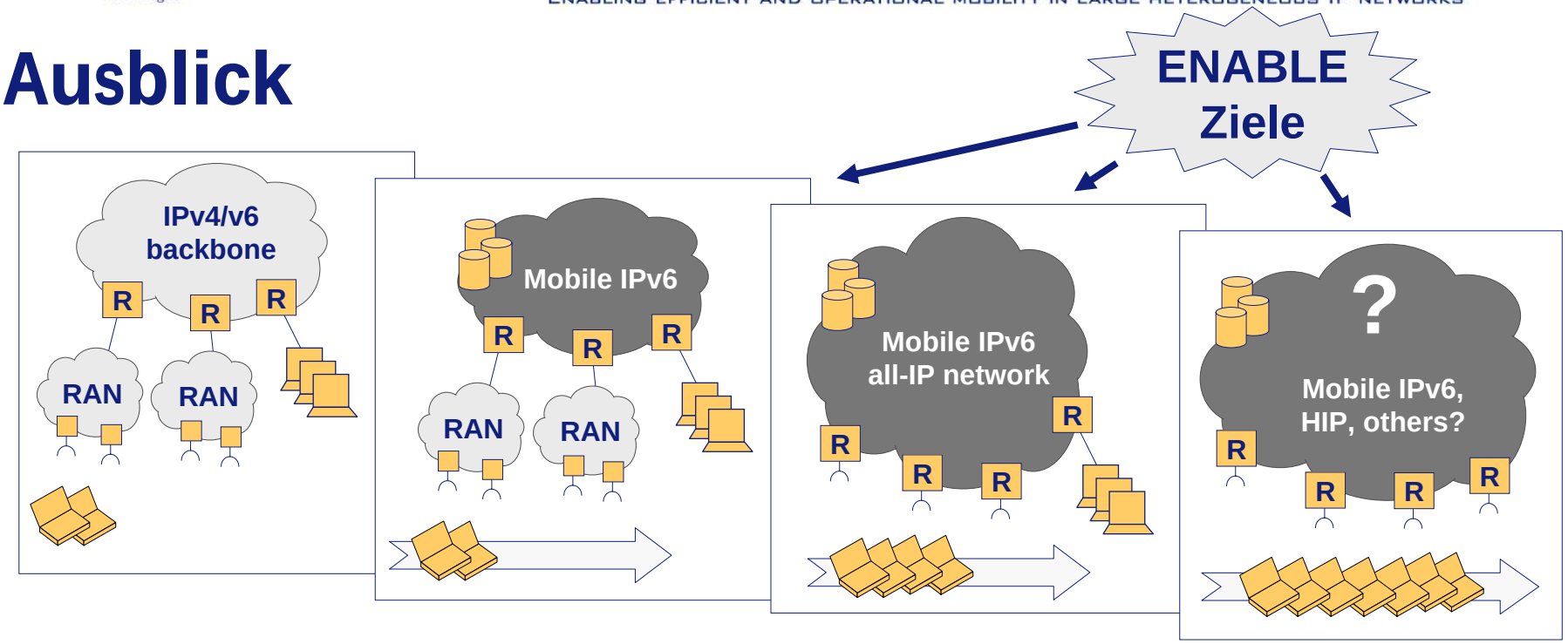
Das ENABLE Projekt

- Dauer: 2 Jahre
- Budget: 3.792 Mio € (406 Mannmonate)
  - EU-Beihilfe: 2.449 Mio €
- Projekt Partner:
  - Koordinator:
    - Telecom Italia
  - Partner:
    - Consulintel (Spanien)
    - Georg-August-Universität Göttingen
    - Siemens AG
    - University of Murcia (Spanien)
    - Industrieanlagen-Betriebsgesellschaft mbH (IABG)
    - Waterford Institute of Technology (Irland)
    - Brunel University (England)
    - Huawei (China)

Projektziele

- Entwicklung von leistungs- und funktionsfähiger Mobilität als Service in großen IPv6 Netzwerken unter Berücksichtigung des Übergangs IPv4/IPv6
  - Forschung und Beisteuerung in den diversen Standardisierungsforen (IETF, 3GPP, etc.)
  - Validierung durch Experimente (Prototypen, Tests, etc.)
- Forschungsschwerpunkte
  - Verbesserung von Mobile IPv6 um **transparente Mobilität** in **großen funktionsfähigen Netzen** mit **mehrfachen administrativen Domains**, **heterogenen Zugängen** und einer schnell **wachsenden Anzahl von Benutzern zu ermöglichen**
  - Verbesserung der Grundfunktionalität von Mobile IPv6 um **„Premium“ Dienste** (fast handover, QoS, etc.)
  - Analyse von Zielen und von Designgrundregeln für eine **langfristige Entwicklung über Mobile IPv6 hinaus**

Ausblick



Today

Dedicated RANs optimized for specific services

- cellular (2.5-3G)
- Wireless LAN
- WMAN (WiMAX)

Step 1

Integration of heterogeneous RANs to offer efficient and cost-effective ubiquitous mobility

- MIPv6 is the key

Step 2

Smooth migration to an all-IP network architecture

- all services over IP
- MIPv6 with fast handover support

Step 3

Fully mobile Internet

- tremendous growth in the number of terminals
- MIPv6 might suffer its age

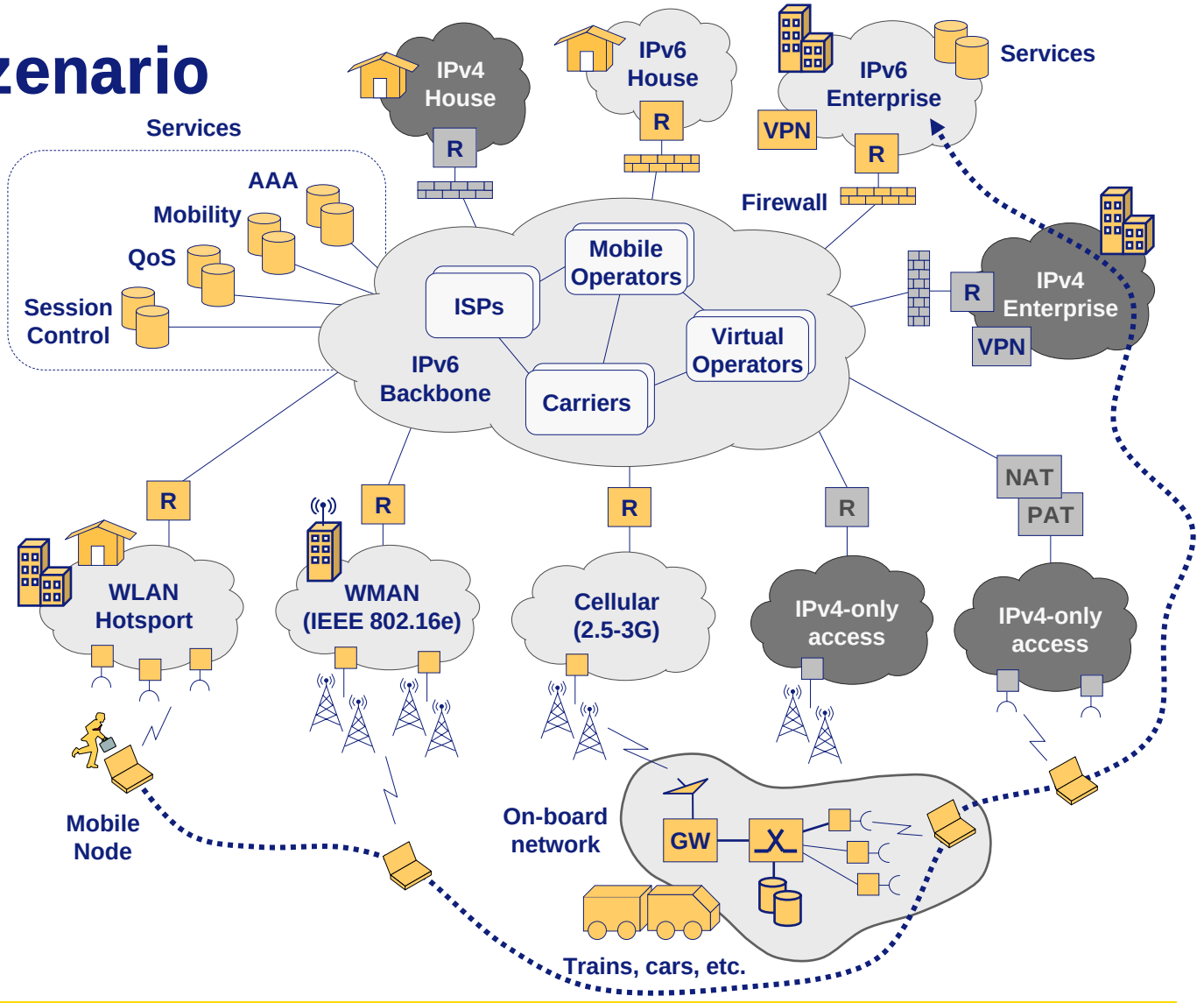
Forschungsschwerpunkte (I)

- Verbesserung der Skalierbarkeit von Mobile IPv6
  - **Dynamische Veränderung** von Konfigurationsdaten auf Terminals und HAs
  - **Lastverteilung** zwischen mehreren HAs
- Verbesserung der Ausfallsicherheit
  - Entwicklung eine Lösung zur **HA-Ausfallsicherung** (kein „single point of failure“)
- Steuern von Mobilen Diensten
  - **Service Authorization** basieren auf einer AAA Infrastruktur
- Bereitstellung von „Premium“ Netzwerkdiensten
  - Fast Handover, QoS, etc.
- Integration von Mobile IPv6 in reelle Netzwerke
  - Koexistenz mit **Middleboxes** (Firewalls, etc.)
  - Einsatz von Mobile IPv6 in **ausschließlich IPv4 Netzwerken**

Forschungsschwerpunkte (II)

- Analyse von Protokollen und von Architekturen für langfristige Netzwerkentwicklung
  - **Skalierbarkeit** mit einer hohen Anzahl von Terminals
  - Optimierte Unterstützung für **Terminals mit sehr begrenzten Verarbeitungs- und Speicherkapazitäten** (z.B. Sensoren)
  - Der Einsatz von **Mobile IPv6 ist eventuell nicht ausreichend**, daher müssen mögliche langfristige Alternativen oder Weiterentwicklungen sorgfältig ausgewertet werden.
    - Host Identity Protocol (HIP)
    - IKEv2 Mobility and Multihoming (MOBIKE)
    - NETwork based Localized Mobility Management (NETLMM)
    - ...

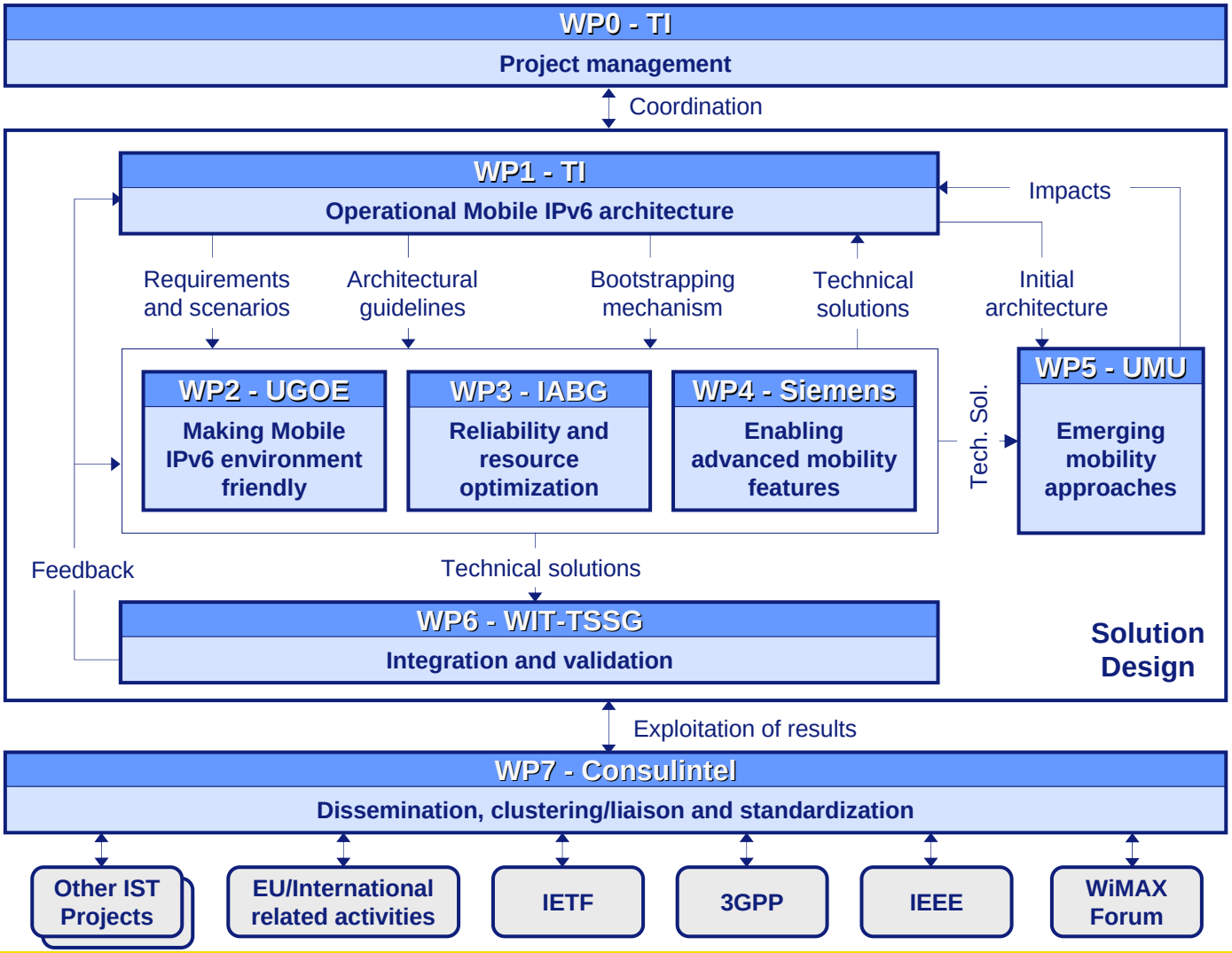
ENABLE
Referenz Szenario



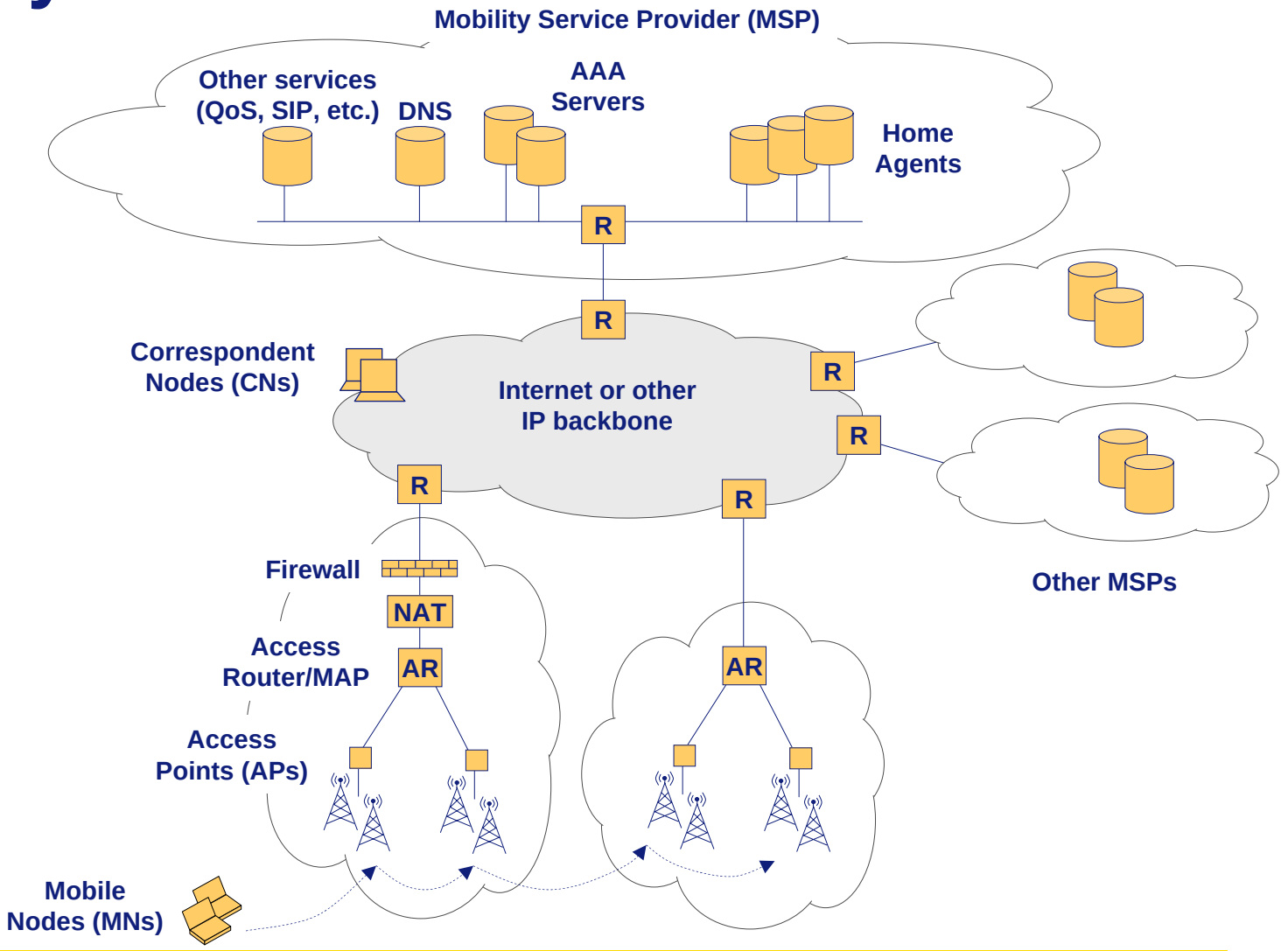
Erwartete Auswirkungen

- Das heutige Mobile IPv6 verhindert es, das ENABLE Referenz Szenario umzusetzen.
- ENABLE soll die Probleme in enger Zusammenarbeit mit der IETF schließen,
  - um sicherzustellen, dass die entwickelten Lösungen in Übereinstimmung mit den architektonischen Grundregeln der Internet-Gemeinschaft sind und vielleicht standardisiert werden.
- Die Forschung in ENABLE erhöht die Fähigkeiten einer zukunftssicheren Mobilitätsinfrastruktur zur Benutzung von der zukünftigen Anwendungen wie pervasive peer-to-peer, audio/video conferencing over IP, emergency services, etc.
- ENABLE trägt auch zur Entwicklung eines langfristigen Ausblicks zum in Zukunft völlig mobilen Internet bei.

Work Packages



ENABLE System Architektur



Veröffentlichungen

- Resultate und Ergebnisse der Projektarbeit sollen publiziert werden:
  - Paper, Journale und Publikationen
  - Präsentationen auf unterschiedlichen Events und Konferenzen
  - Testvorführungen und Miteinbeziehung der externen Benutzer
  - Kooperation mit anderen vergleichbaren Projekten
  - Standardisierungstätigkeiten

ENABLE

- Projekt Webseite:
  - http://www.ist-enable.org

- Projekt-, Bachelor- und Masterarbeiten in ENABLE
  - Xiaoming Fu

Enabling efficient and operational mobility in large heterogeneous IP networks

Firewall traversal for MIPv6: Problem Statement

Mobilkommunikation II

Prof. Dr. Dieter Hogrefe

WS 06/07

Information Society Technologies

Inhalt

- Firewalls: Funktions- und Arbeitsweise
- Mögliche Firewall Platzierungen und daraus resultierende Probleme
  - Firewall beschützt MN's Netzwerk
  - Firewall beschützt HA's Netzwerk
  - Firewall beschützt CN's Netzwerk
- Zusammenfassung

Firewalls: Funktions- und Arbeitsweise

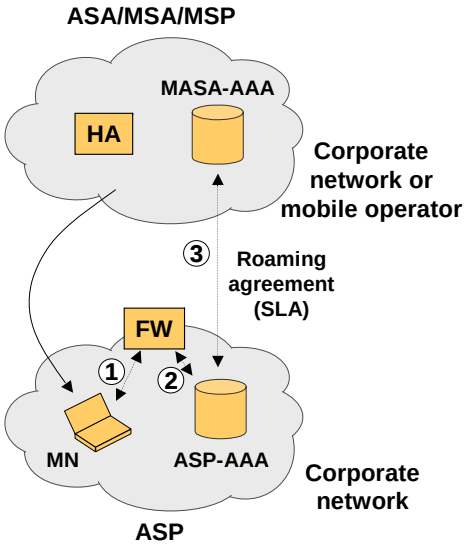
- Firewall entscheiden anhand eines 5-Tupels ob Pakete erlaubt oder verworfen werden:
  - { Source IP address, Destination IP address, Protocol type, Source port number, Destination port number }
- Die am meisten verbreitete Art von Firewalls ist der Stateful Packet Filters (SPF), welcher das Netzwerk von nicht verlangtem Datenpaketen beschützt.
- SPFs erlauben oder verwerfen Pakete anhand von Informationen aus einer lokalen Zustandstabelle, welche von der Firewall verwaltet wird.

Mögliche Firewall Platzierungen und daraus resultierende Probleme

- Mobile IPv6 definiert MN, HA, CN.
- Diese Entitäten können in einem Netzwerk liegen, welches von einer Firewall beschützt wird.
- Daher drei grundlegende Szenarien
  - Firewall beschützt MN's Netzwerk,
  - Firewall beschützt HA's Netzwerk,
  - Firewall beschützt CN's Netzwerk.
- Diese Platzierungen bringen mehrere Problem mit sich:

Firewall beschützt MN's Netzwerk (I)

- Problem 1
  - Viele Firewalls verwerfen IPsec Pakete da sie aufgrund der Verschlüsselung nicht feststellen können, ob diese angefordert oder berechtigt sind.
  - Bindung Updates und Binding Acknowledgements können daher verworfen werden.
- Problem 2
  - MN und CN wollen Route Optimization benutzen.
  - Home Test Nachricht des RRT muss mit IPsec verschlüsselt sein.
  - Die Firewall verwirft die Home Test Nachricht und verhindern somit die RRT Prozedur.

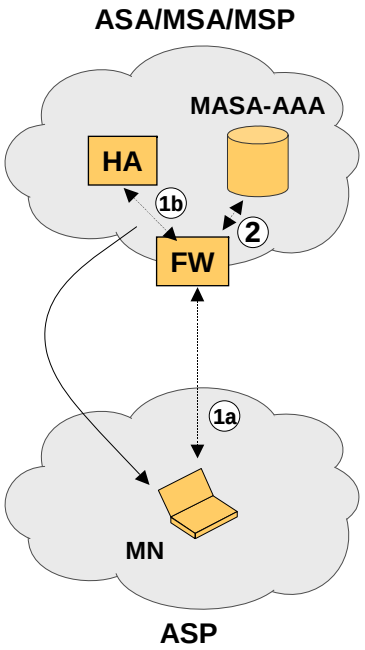


Firewall beschützt MN's Netzwerk (II)

- Problem 3
  - Annahme: MN hat das Binding Update erfolgreich zum HA geschickt.
  - Anschließender Datenverkehr wird vom HA gesendet.
  - Da für diese Art von Verkehr keine States in der Firewall existieren, werden die Pakete verworfen.
- Problem 4
  - Firewalls können CN's an der Kommunikation hindern,
    - weil ankommende Pakete aufgrund nicht existierende States in der Firewall verworfen werden.
- Problem 5
  - Wenn der MN in ein anderes Netzwerk roamt und dieses durch eine Firewall beschützt wird, werden alle neu ankommenden Pakete verworfen, da für diese keine States existieren.

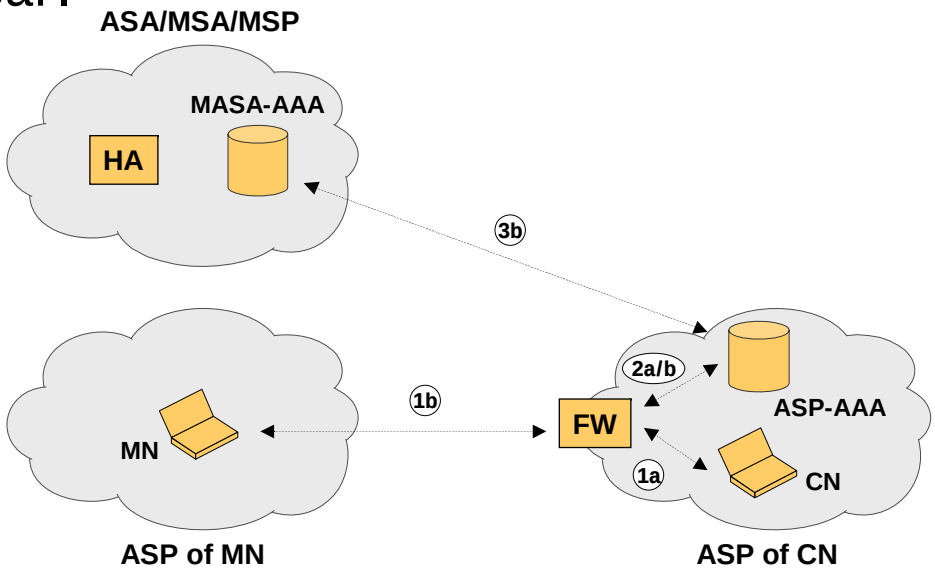
Firewall beschützt HA's Netzwerk

- Problem 1
  - Firewall beschützt den Home Agent und verwirft IPsec Pakete.
  - IPsec verschlüsselte MIPv6 Signalisierungsnachrichten (Binding Update, HoT) werden von der Firewall verworfen.
  - Dies hindert den MN daran Bindung Updates zu senden und Route Optimization zu benutzen.
- Problem 2
  - Firewall verwirft Verbindungsaufbauanfragen vom CN und MN, da für diese keine States existieren.



Firewall beschützt CN's Netzwerk (I)

- Problem 1
  - Care of Test Init Nachricht wird mit der CoA des MN's als Herkunftsadresse gesendet.
  - Dieses Paket entspricht keinem Eintrag in der Firewall und die CoTI Nachricht wird verworfen.
  - Daher kann die RRT Prozedur nicht beendet werden und Route Optimisation ist nicht einsetzbar.



Firewall beschützt CN's Netzwerk (II)

- Problem 2
  - Annahme: Bindung Update zum CN war erfolgreich.
  - Die Firewall wird weiterhin Pakete die von der CoA kommen verwerfen, da diese keinem Eintrag in der Firewall entsprechen.

Forschung in ENABLE

- Forschungsschwerpunkt von WP2 in ENABLE ist es, die Mobile IPv6 Signalisierung in Gegenwart von Firewalls zu ermöglichen.
- Dynamische Konfiguration von Firewalls um Ende-zu-Ende Kommunikationsszenarien das Durchschreiten dieser Firewalls zu ermöglichen.
- Es gibt mehrere mögliche „Middlebox traversal“ Lösungen:
  - Application Layer Gateways (ALGs)
  - Middlebox Communication - MIDCOM
  - NSIS und NAT/FW NSLP
  - Policy Based Networks (PBN)
  - VPN Ansätze
- Diese Ansätze werden momentan innerhalb von ENABLE analysiert und eine Lösung für „Mobile IPv6 Firewall Traversal“ entwickelt.

Zusammenfassung

- Firewalls können – abhängig von ihrer Platzierung – den Einsatz von Mobile IPv6 unmöglich machen.
- Mögliche Firewall Platzierungen:
  - Firewall beschützt MN's Netzwerk
  - Firewall beschützt HA's Netzwerk
  - Firewall beschützt CN's Netzwerk
- Probleme resultieren großenteils daher das,
  - viele Firewalls IPsec Pakete verwerfen da sie aufgrund der Verschlüsselung nicht feststellen können, ob diese angefordert oder berechtigt sind.
  - Stateful Packet Filter (SPF) das Netzwerk vor nicht angeforderten Datenpaketen beschützen und daher Pakete die keinem Eintrag in der Zustandstabelle entsprechen, verwerfen.