ENABLING EFFICIENT AND OPERATIONAL MOBILITY IN LARGE HETEROGENEOUS IP NETWORKS

Deployment of MIPv6 in operational networks

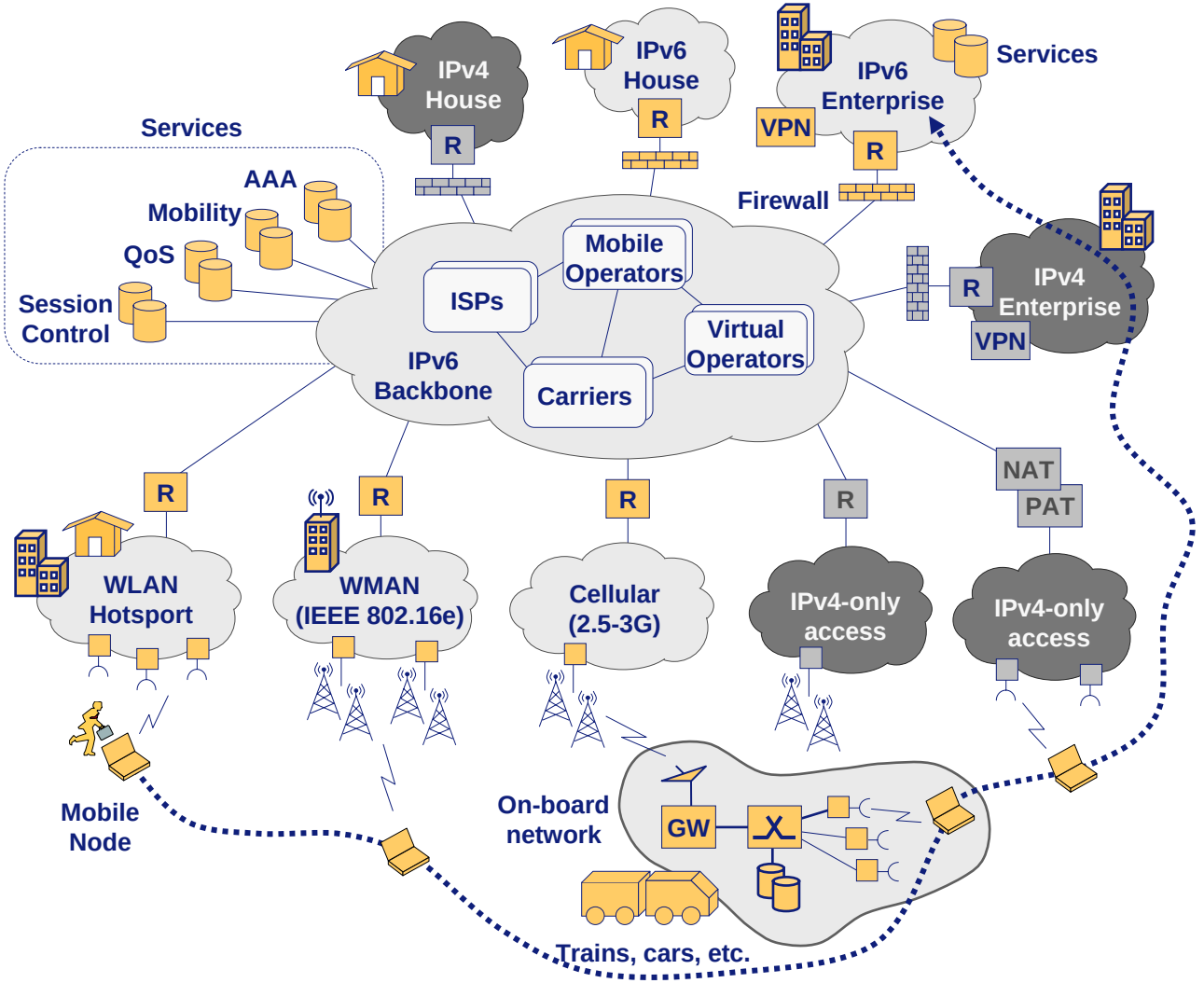
Presentation at the University of Passau, 02.05.2006

Wolfgang Fritsche, IABG

Information Society Technologies

Overview of Mobile IPv6 (MIPv6)

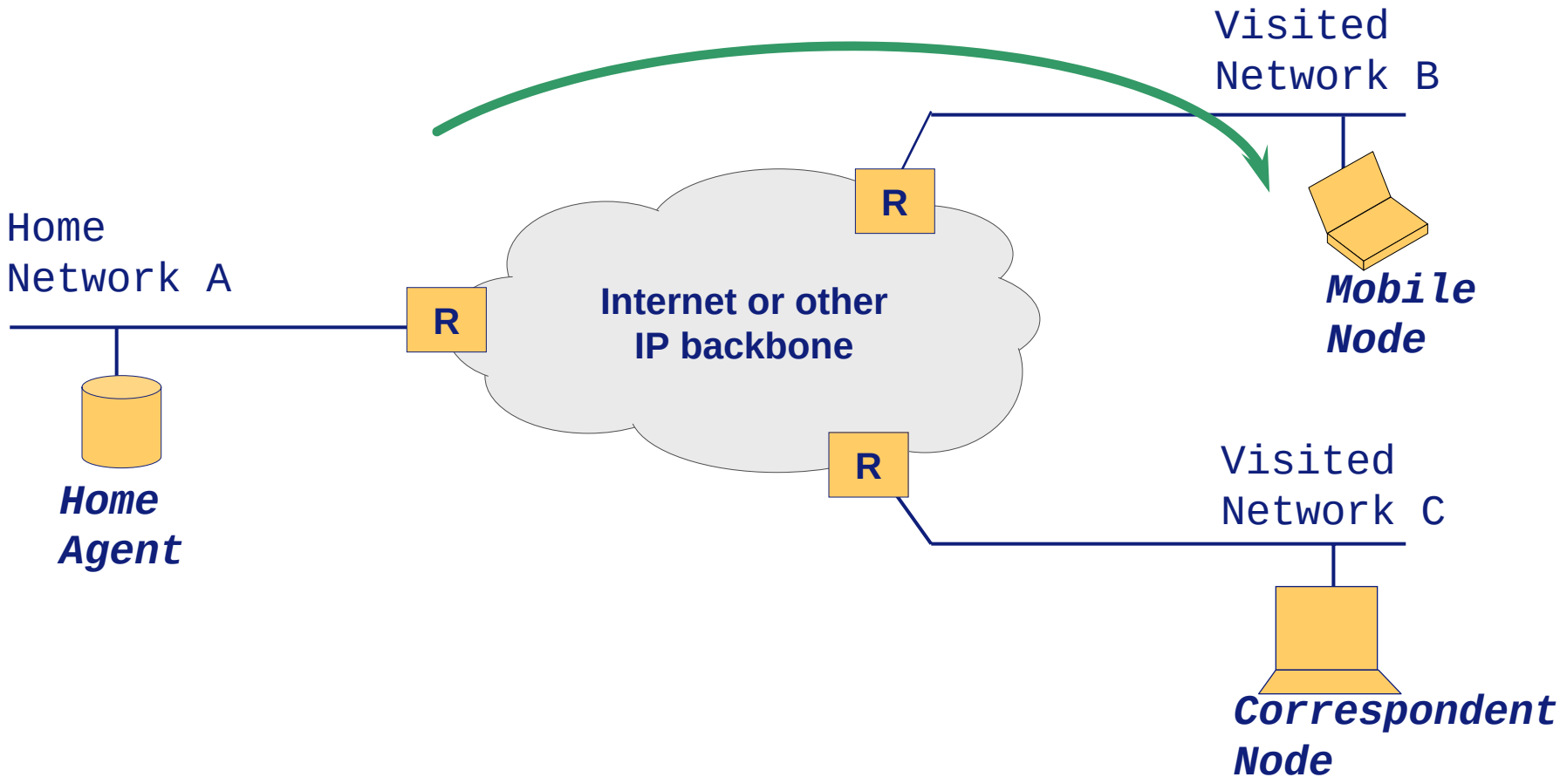
Mobility in today's Internet



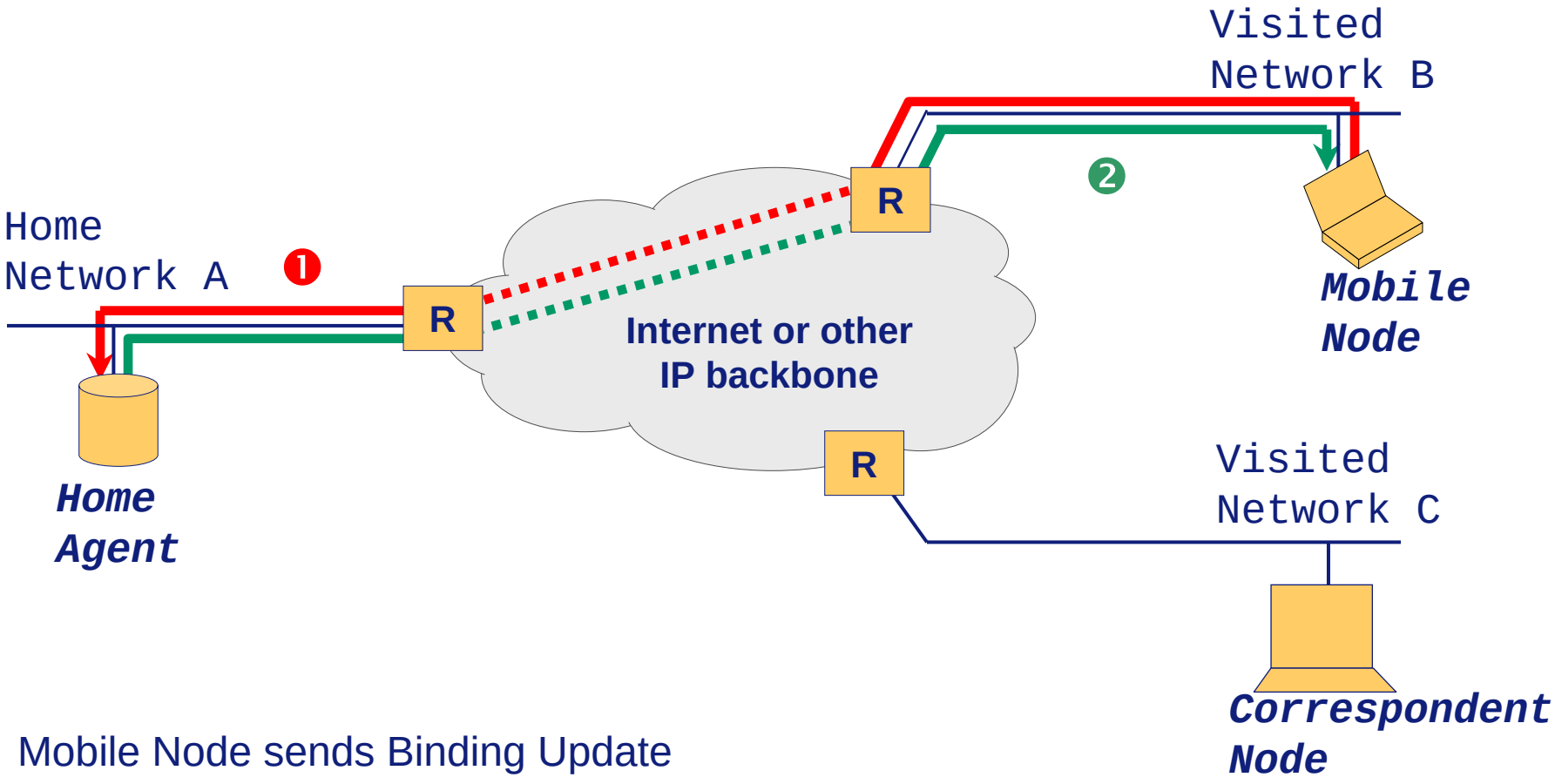
Rationale for Mobile IPv6 (MIPv6)

- Evolvement of the mobile Internet
  - Growing number of mobile Internet users
  - Growing diversity of mobile Internet devices (PDA, cellphone, smartphone, …)
  - Increasing heterogenity of access networks (GSM, 3G, WLAN, WiMax, …)
  - Efficient support of mobility in the Internet required
- Importance of transparency
  - Mobility support should be transparent to users and applications
- MIPv6 approach
  - MIPv6 offers this transparent mobility support by influencing the routing of IP packets

Mobile IPv6 example

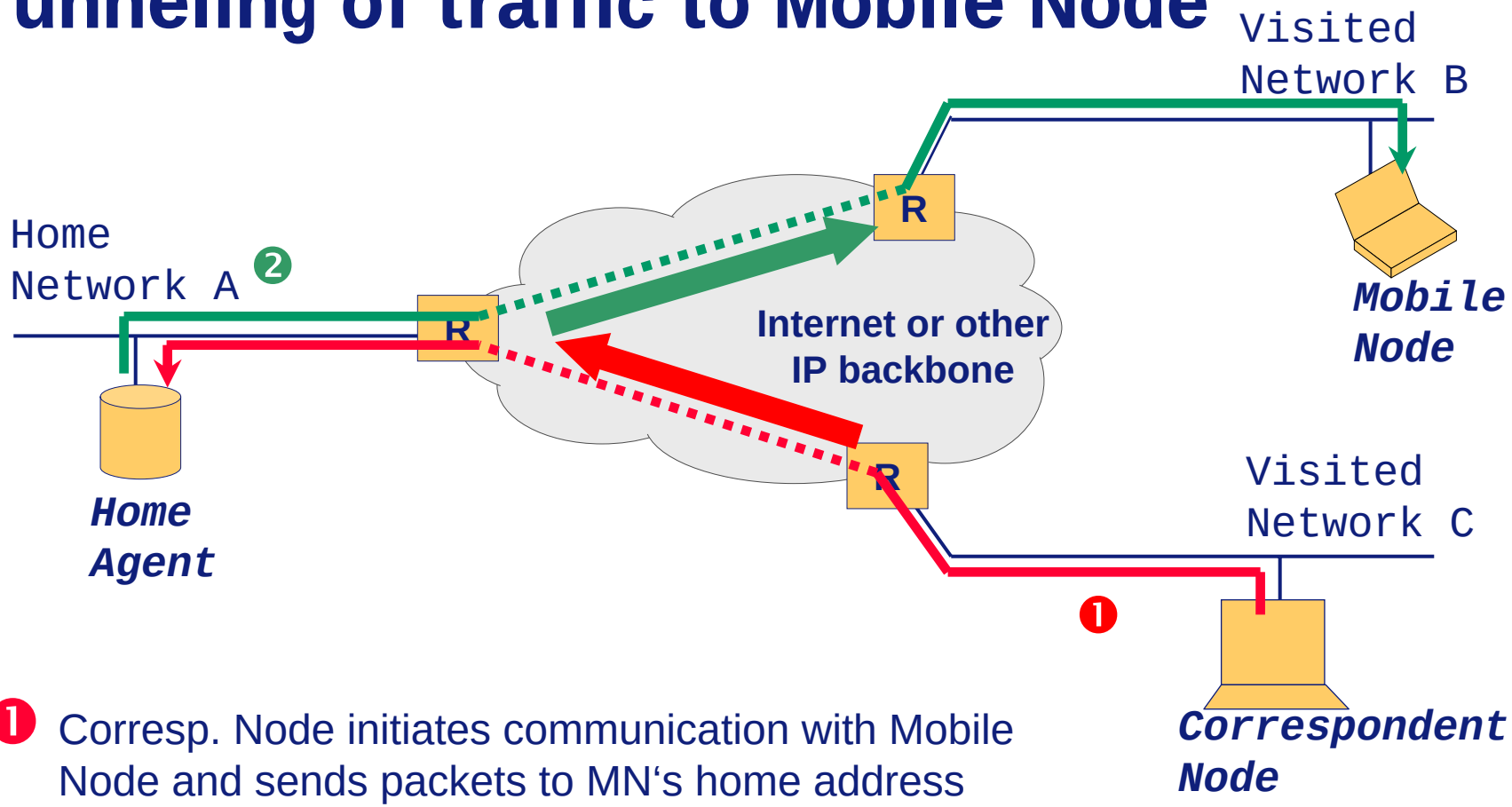


Mobile Node registers at Home Agent



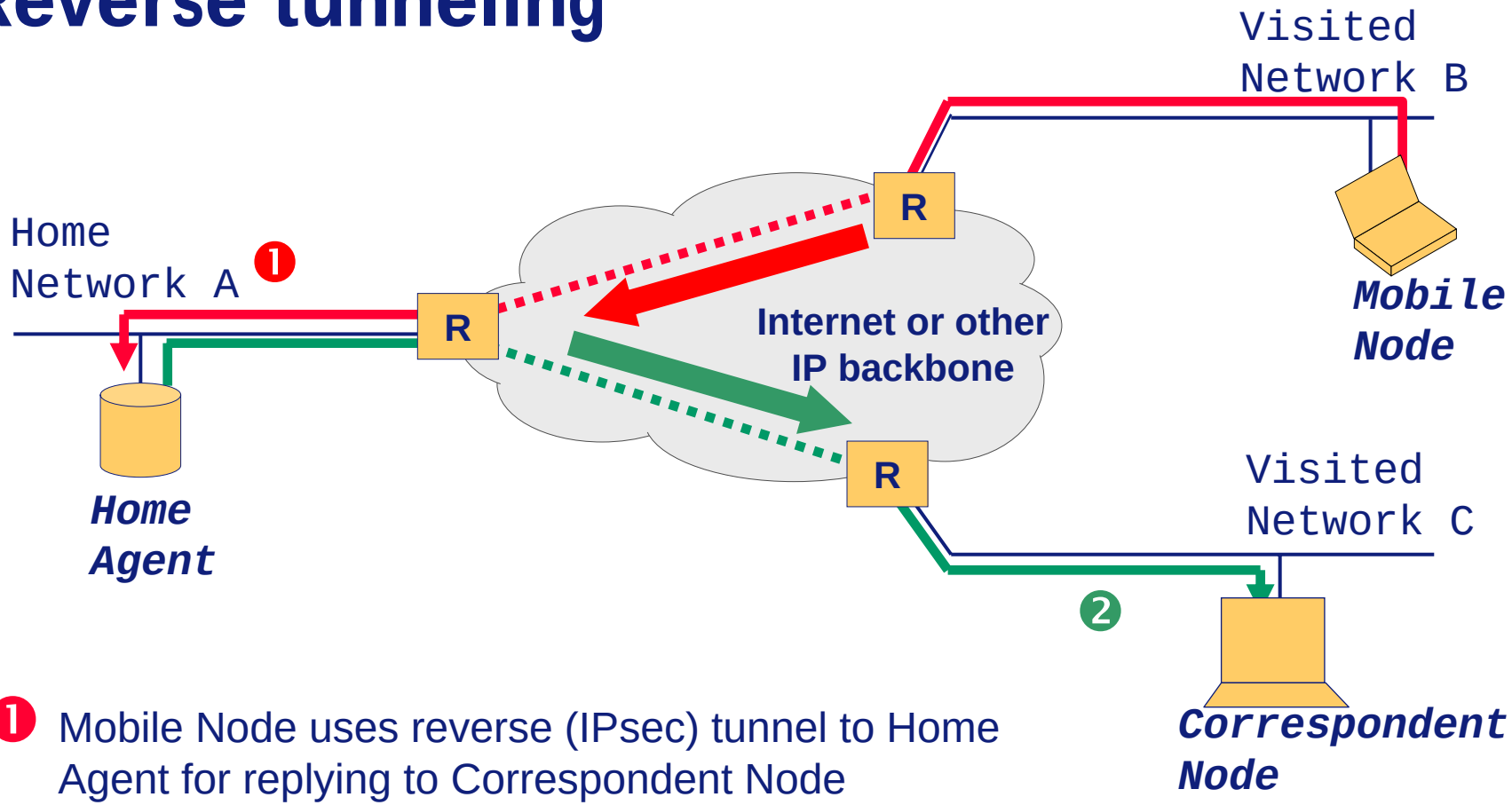
1. Mobile Node sends Binding Update
2. Home Agent replies with Binding Acknowledgement

Tunneling of traffic to Mobile Node



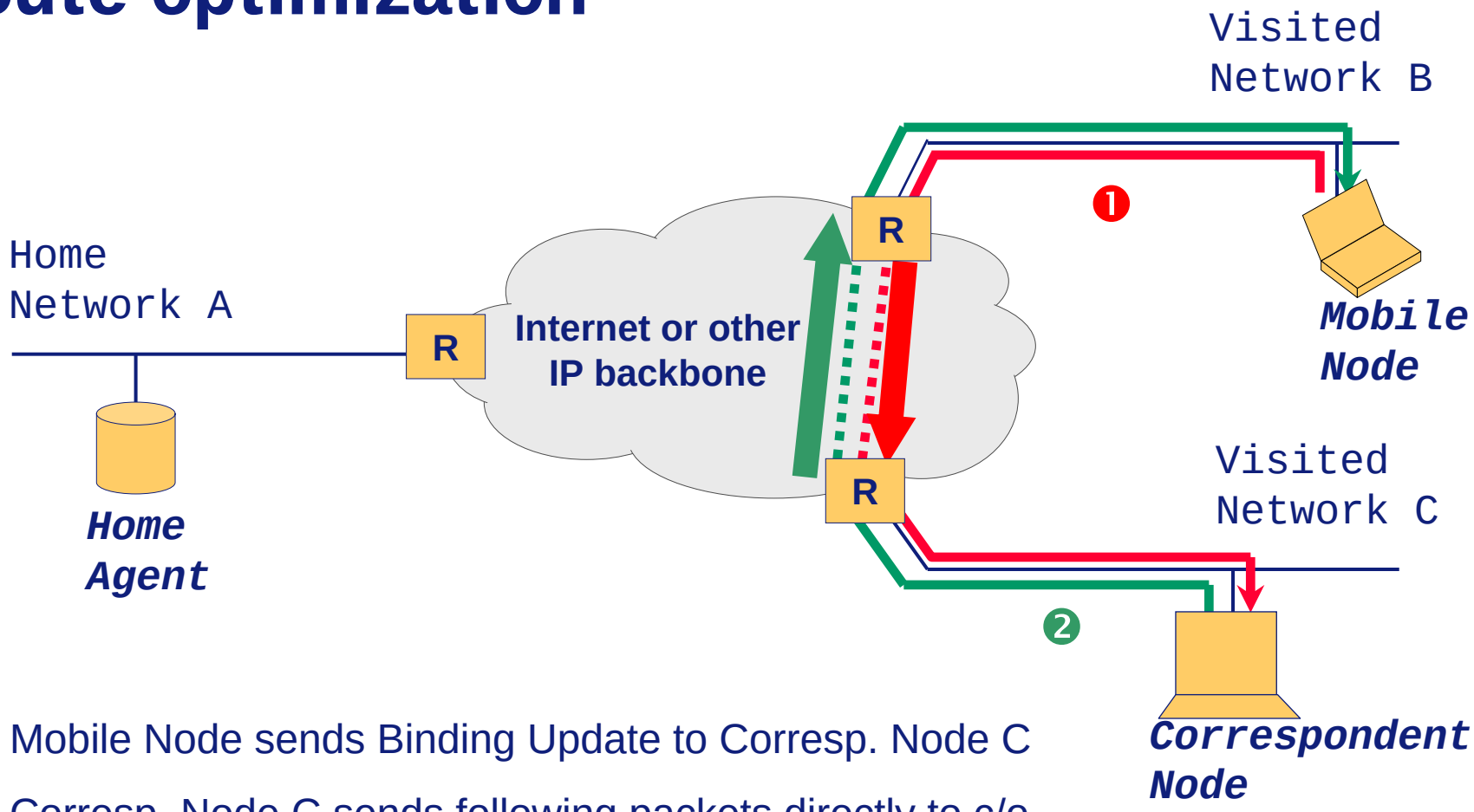
1. Corresp. Node initiates communication with Mobile Node and sends packets to MN's home address
2. Home Agent intercepts packets and forward them to the Mobile Node (proxy functionality)

Reverse tunneling



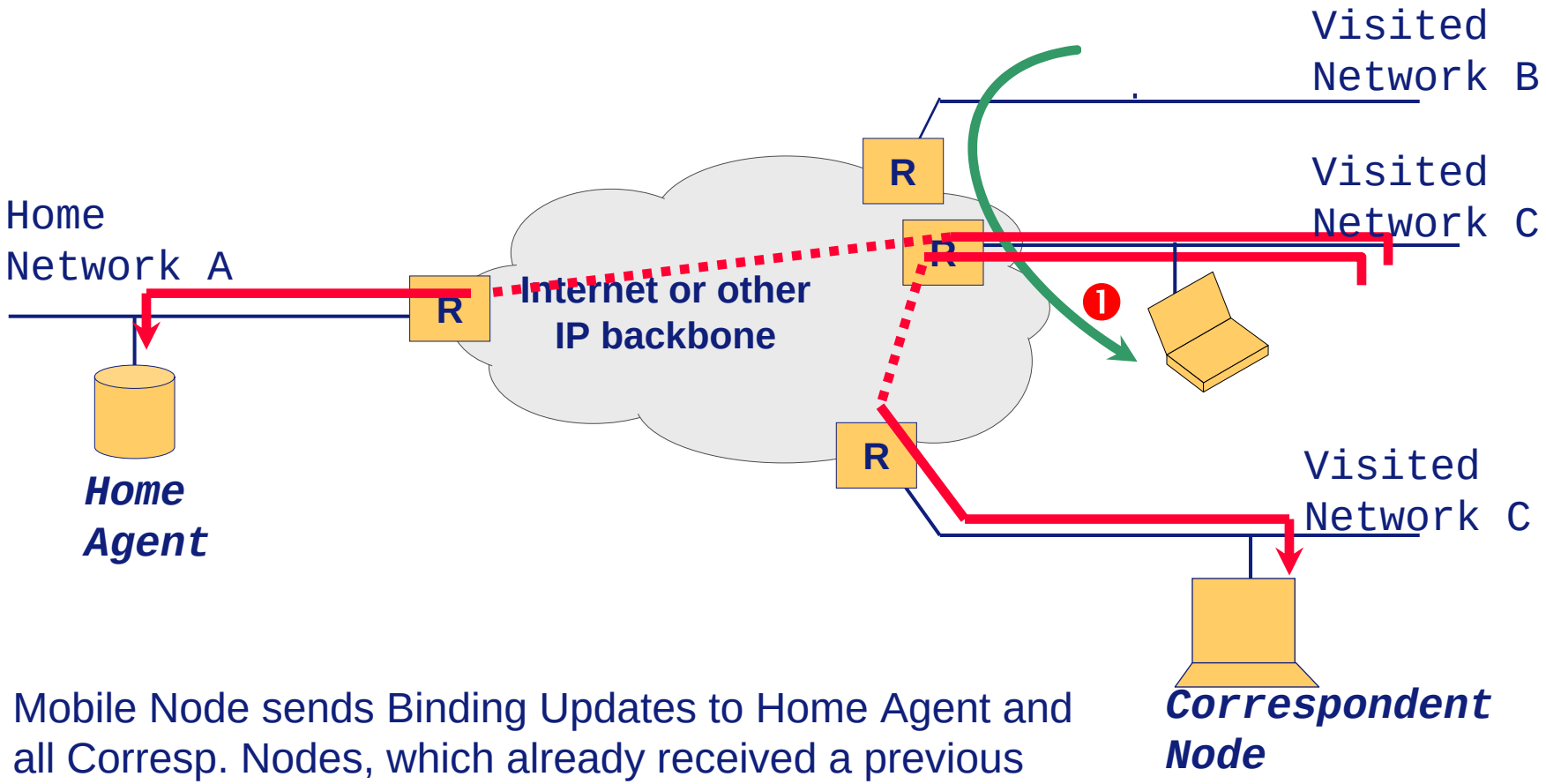
1. Mobile Node uses reverse (IPsec) tunnel to Home Agent for replying to Correspondent Node
2. Home Agent decapsulates packet from Mobile Node and forwards it to Correspondent Node

Route optimization



1. Mobile Node sends Binding Update to Corresp. Node C
2. Corresp. Node C sends following packets directly to c/o address of Mobile Node

Roaming



1. Mobile Node sends Binding Updates to Home Agent and all Corresp. Nodes, which already received a previous Binding Update from this Mobile Node

Operational requirements

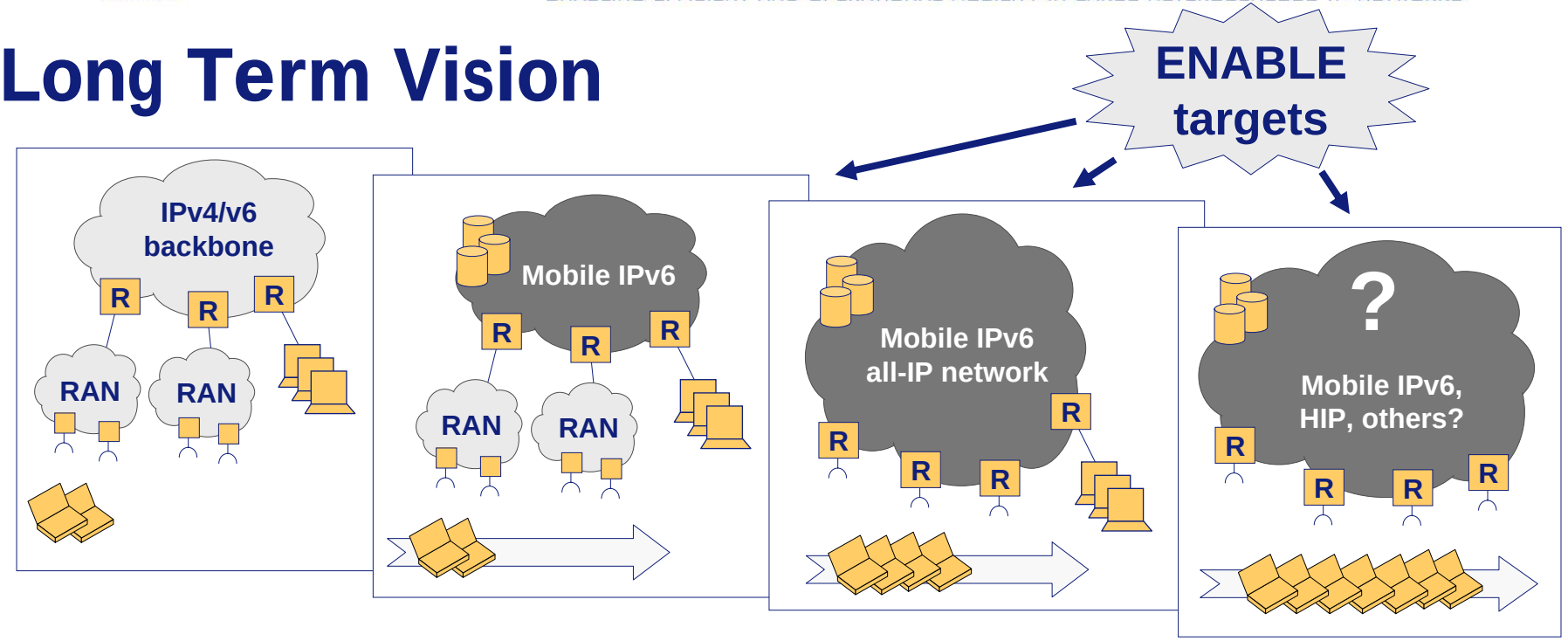
Requirements for operational deployment of MIPv6

- Improvement of Mobile IPv6 scalability
  - **Dynamic provisioning** of configuration data on terminals and HAs
  - **Load-sharing** across HAs
- Improvement of reliability
  - Solutions for **HA failover** (no single point of failure)
- Control of mobility service
  - **Service authorization** based on a AAA infrastructure
- Enable offering of "premium" network features
  - **On-demand and secure activation** of fast handovers, QoS, etc.
- Integration of Mobile IPv6 in real-life environments
  - Coexistence with **middle-boxes** (firewalls, VPN concentrators, etc.)
  - Deployment of **Mobile IPv6 in IPv4-only accesses**

Overview of ENABLE project

- ENABLE at a glance
  - Research project funded by the European Commission
  - 8 European and one Chinese partner
  - Duration: 2006 – 2007
- Goal of ENALBE
  - Enable deployment of efficient and operational mobility as a service in large scale IPv6 network environments
  - Taking into account also the transition from current IPv4 networks
  - Research and contribution to standardization fora (IETF, 3GPP, etc.)
  - Validation through laboratory experiments (prototypes, testing, etc.)
- More information
  - ENABLE project web site http://www.ist-enable.org

Long Term Vision



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

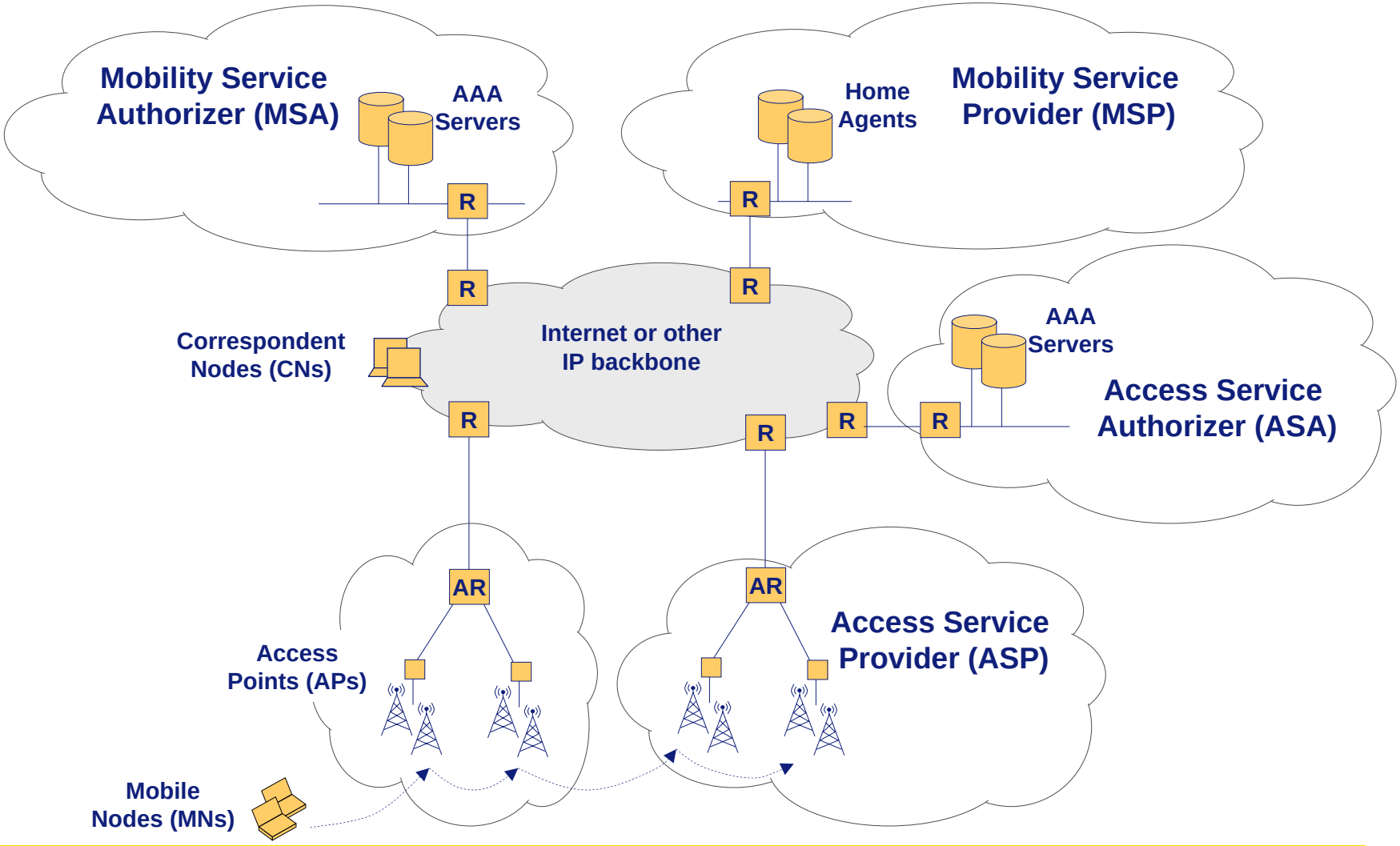
Fully mobile Internet

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

Bootstrapping

- Goal
  - Addressing the operational requirement for dynamic provisioning of configuration data on terminals and HAs and MIPv6 service authorization
- Configuration data
  - HA address
    - Required on MN
    - Used for registering Binding Updates with HA
  - MN‘s Home Address
    - Required on MN
    - Used for communication with other nodes
    - Could change if home network will be renumbered
  - Keying Material
    - Required on MN and HA
    - Used to set up a security association (IPsec) between MN and HA

Service entities involved in bootstrapping



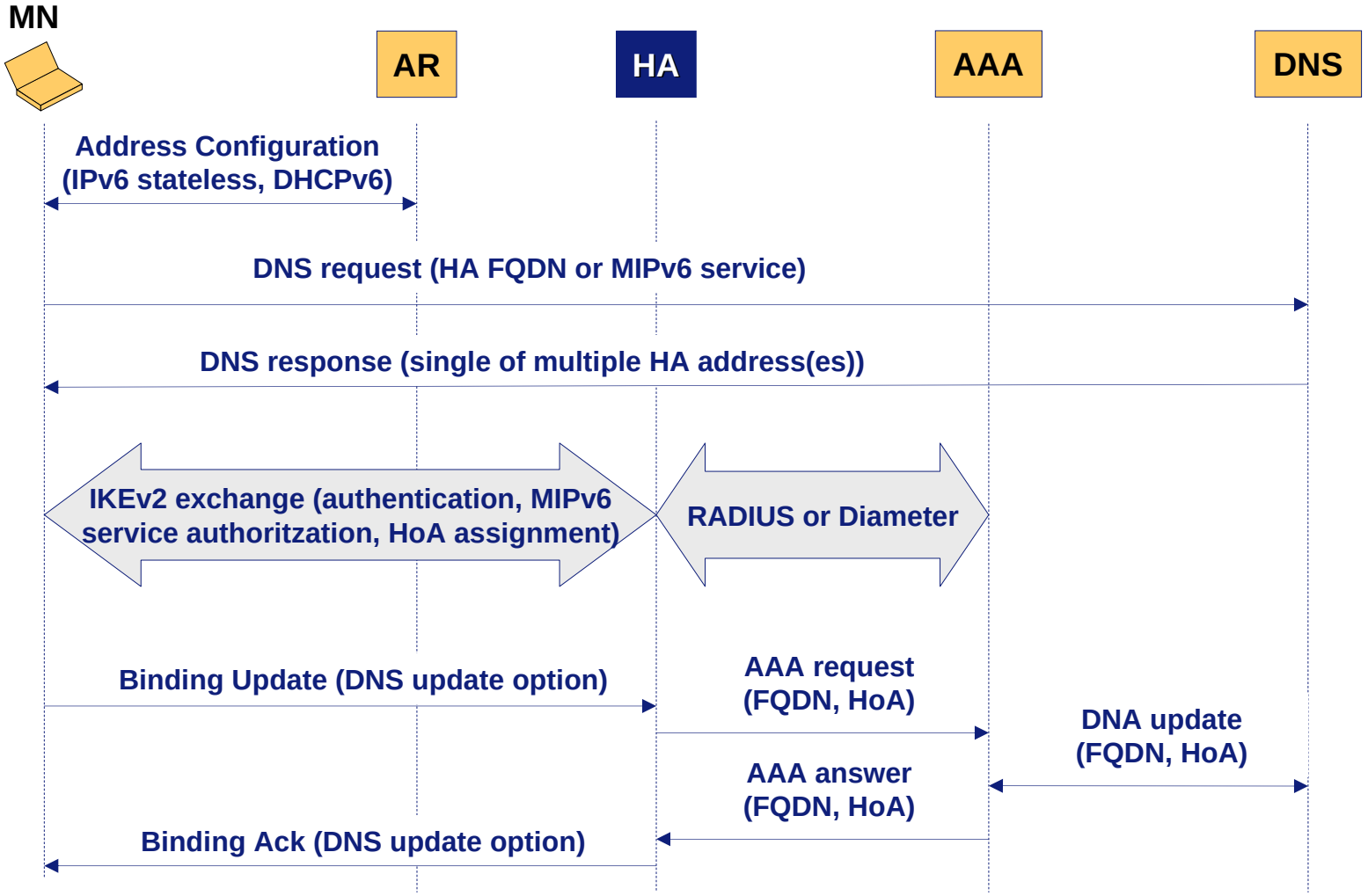
Bootstrapping architectures investigated by IETF

- Split scenario
  - Mobility Service Authorizer (MSA) is different from Access Service Authorizer (ASA)
  - Assignment of Home Agent done using DNS
- Integrated scenario
  - Mobility Service Authorizer (MSA) is the same as Access Service Authorizer (ASA)
  - Assignment of Home Agent done using DHCPv6

Steps of the split scenario

- Getting network access
  - Using DHCPv6 or IPv6 stateless address autoconfiguration
- Home Agent assignment done by DNS request from MN
  - Requesting for a FQDN of a HA (e.g. ha.service-provider.com)
  - Requesting for a MIPv6 service (e.g. mip6.ipv6.service-provider.com)
- Setting up an IPsec security association between HA and MN
  - Use of Internet Key Exchange version2 (IKEv2) for this purpose
  - For this purpose the HA may contact a PKI or AAA for MN authentication and service authorization
- Assignment of a Home Address to MN
  - Done within the IKEv2 exchange
  - MN could propose a Home Address
- Update of the MNs DNS entry with the new Home Address
  - Triggering of DNS update within Binding Update from MN to HA
  - HA updates DNS directly or further delegates this to AAA

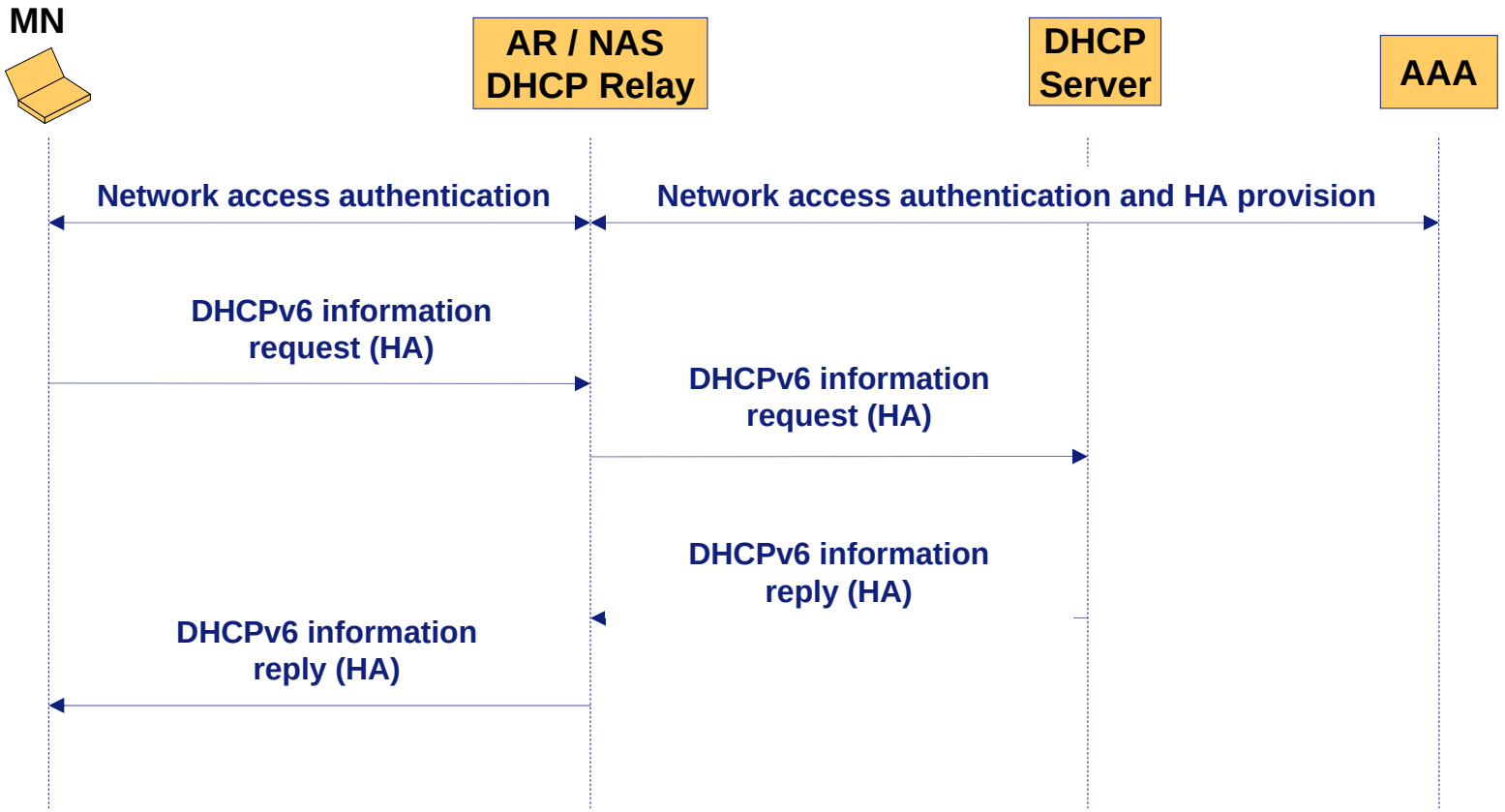
Example message flow for split scenario



Steps of the integrated scenario

- Getting network access
  - Using DHCPv6 or IPv6 stateless address autoconfiguration
- Home Agent assignment done by DHCPv6 request from MN
  - HA is provided by the Mobility Service Provider
    - AAA of Mobility Service Provider provides HA to DHCPv6
    - DHCPv6 finally assigns HA to MN
  - HA is provided by Access Service Provider
    - Direct assignment of HA to MN by DHCPv6
- Remaining steps identical to split scenarion
  - Setting up an IPsec security association between HA and MN
  - Assignment of a Home Address to MN
  - Update of the MNs DNS entry with the new Home Address

Example message flow of integrated scenario



Contact

Wolfgang Fritsche

Manager Advanced IP Services

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

This work has been partially supported by the European Commission FP6 IST ENABLE project.