ENABLING EFFICIENT AND OPERATIONAL MOBILITY IN LARGE HETEROGENEOUS IP NETWORKS

ENABLE QoS Services for Large-Scale Operational IP Mobility Networks

Xiaoming Fu
University of Göttingen, Germany
Email: fu@cs.uni-goettingen.de

Ivano Guardini, Marco Marchisio
Telecom Italia Lab, Italy
Email: {ivano.guardini,marco.marchisio}
@telecomitalia.com

Information Society Technologies

Table of content

- Introduction to IST ENABLE project – Enabling Efficient and Operational Mobility in Large Heterogeneous IP Networks
- Motivation
  - problem statement and related works
  - reference network scenario
- ENABLE QoS concept
  - protection of MIPv6 signalling
  - QoS differentiation of data traffic, including admission control
  - Push and pull models, and authorization
- Conclusions

Overview of IST ENABLE project

- FP6 Specific Targeted Research Project
  - 24 months (01.01.06-31.12.07), EC contribution 2.7 M€
  - Addressing operational issues with Mobile IPv6, e.g. bootstrapping, firewall traversal, IPv4 interworking, service authorization, multihoming, QoS and mobility optimization; also investigate emerging mobility solutions like HIP, MOBIKE, SHIM6, NETLMM/PMIP.
- Consortium (9 partners)
  - Telecom Italia Lab (IT)
  - University of Göttingen (DE)
  - Siemens (DE)
  - IABG (DE)
  - Consulintel (ES)
  - University of Murcia (ES)
  - TSSG, Waterford Institute of Technology (IE)
  - Brunel University (UK)
  - Huawei Technologies (CN)

Motivation

- Mobile IPv6 traffic receives simply best effort services
  - However mobile users may have stronger desire to receive high quality
  - This includes both data traffic and control/signaling traffic
- QoS in wired networks well addressed
  - Both control plane (signaling/resource reservation, admission control) and data plane (marker and classifier, traffic shaper, scheduler/dropping)
- In mobile networks, the following issues need to be changed
  - Signaling: reserve QoS resources for MIPv6 flows (incl. admission control)
  - Classification and marking: identify and mark the data traffic to receive certain service
    - Including preemption for MIPv6 signaling traffic: marking appropriately

QoS & MIPv6: problem statement

- Preemption of MIPv6 signaling
  - it is necessary to avoid that the BU, BA, BRR, HoT, CoT, HoTI and CoTI messages get lost in case of network congestion
  - Like preemption of RSVP messages for reliable signaling
- QoS differentiation of data traffic
  - There needs to be dynamic admission control in the edge of the network
  - QoS policies on data traffic must be effective in Bi-directional Tunneling (BT) and in Route Optimization (RO)
  - QoS policies on data traffic must be updated as the mobile node changes its point of attachment to the network
- Authorization of QoS resource usage
  - In conjunction with admission control/QoS session setup

Reference network scenario

- Considering that QoS in IP networks is a very wide problem space, firstly we concentrate a simplified scenario:
  - single administrative domain including multiple heterogeneous access networks
    - 2-3G, WiMAX, WiFi, etc.
  - QoS differentiation achieved through the DiffServ approach
    - a limited number of QoS classes is pre-configured within the domain
    - traffic conditioning (packet classification, DSCP marking, policing and shaping) is performed by the edge routers located between the access segment and the core network
- Other scenarios (multi-domain cases, other QoS solutions) are under further investigation

Preemption of MIPv6 signalling (I)

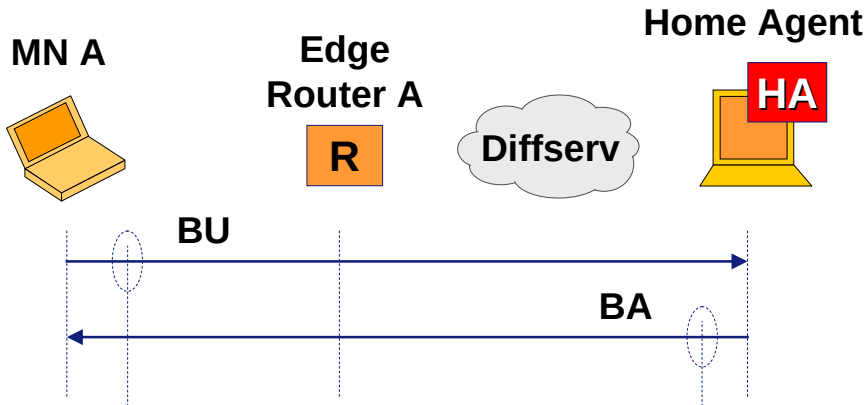
- MIPv6 signalling should be mapped on a QoS class providing high probability of traffic delivery to destination
  - e.g. the low “Low Latency Data” class
    - DSCP = 011000
      - the same marking typology suggested for any other kind of peer-to-peer signalling (e.g. SIP, H323)
      - Assured Forwarding (AF) PHB
  - or Expedited Forwarding (EF) PHB
    - DSCP = 101110 "low loss, low latency, low jitter, assured BW, e2e service"

- The key problem is how to achieve correct classification of MIPv6 signalling, in order to distinguish it from data traffic
  - Reliable MIPv6 signaling to satisfy the prerequisite for QoS-ensured MIPv6 forwarding
  - Alike preemption for RSVP signaling messages

Preemption of MIPv6 signalling (II)

- Signalling messages sent by HA can be marked by HA itself
  - the HA is a "trusted" node
- Signalling messages transmitted by the mobile node should be marked by the edge router
  - all the messages including a Mobility Header must be protected (BU, BA, BRR, BE, HoT, CoT, HoTI and CoTI)
  - optionally, MIPv6-specific ICMP signalling could also be protected
    - Home Agent Address Discovery Request (ICMP Type = 150)
    - Home Agent Address Discovery Reply (ICMP Type = 151)
    - Mobile Prefix Solicitation (ICMP Type = 152)
    - Mobile Prefix Advertisement (ICMP Type = 153)

For example: BU and BA messages



Mobility Header	Binding Update (Alternate CoA option)
	ESP header in transport mode
Destination Options Header	Home Address Option (Home Address)
IPv6 Header	Src: Care-of Address Dst: HA Address -: -

Mobility Header	Binding Acknowledgement
	ESP header in transport mode
Routing Header (Type 2)	Home Address
IPv6 Header	Src: HA Address Dst: Care-of Address -: -

Classification of MIPv6 signalling

- The following signalling messages must be classified and marked by the edge routers
  - Binding Update (BU)
    - the ESP header is present (transport mode)
    - a Destination Options Header containing the Home Address Option is present
    - the destination address is the Home Agent address
      - this check is used in order not to confuse BU messages with data packets sent by mobile node in in Route Optimization and protected by IPsec ESP
  - Home Test Init (HoTI)
    - it is not easily identifiable by the edge router (being ciphered)
      - the only possibility is to protect all the IPsec ESP traffic (tunnel mode) sent to the HA, but this solution is possible only if the same solution is not used to protect also the traffic data in Bi-directional Tunneling
  - Care-of Test Init (CoTI) and Care-of Test (CoT)
    - CoTI or CoT Mobility Headers are present in the message

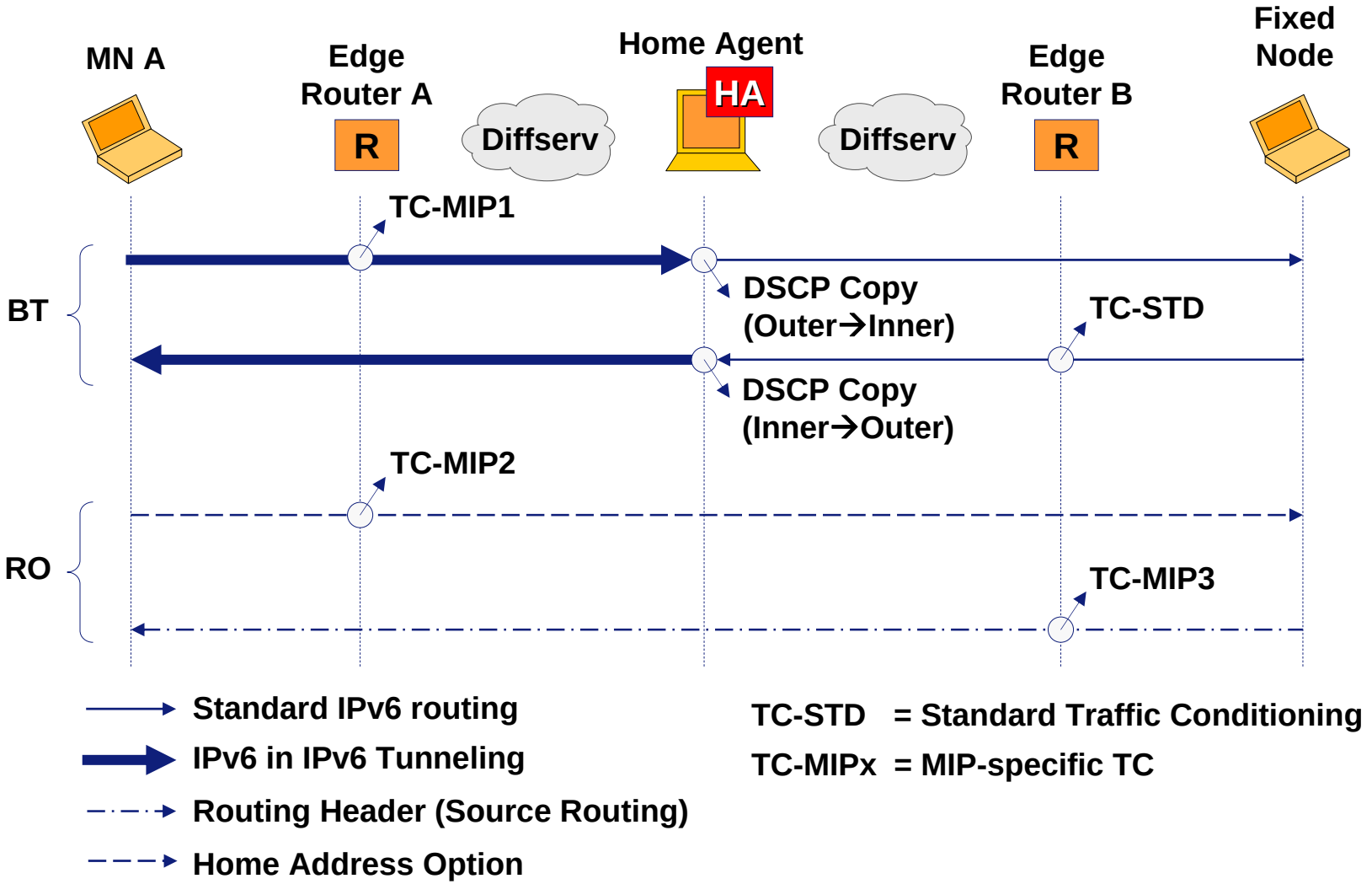
MIPv6 signalling preemption: conclusions

- BA, BRR, BE and HoT messages can be marked by HA
- CoT and CoTI messages can be marked with static rules pre-configured on the edge routers of the domain
- Classification of BU messages requires to check that the destination is a HA
  - automatic installation of a classification rule in the NAS during the authentication phase (after HA allocation to the MN)
    - ❑ possible only if the edge router works as NAS
  - manual installation of a classification rule for each HA
- HoTI messages classification is an open issue

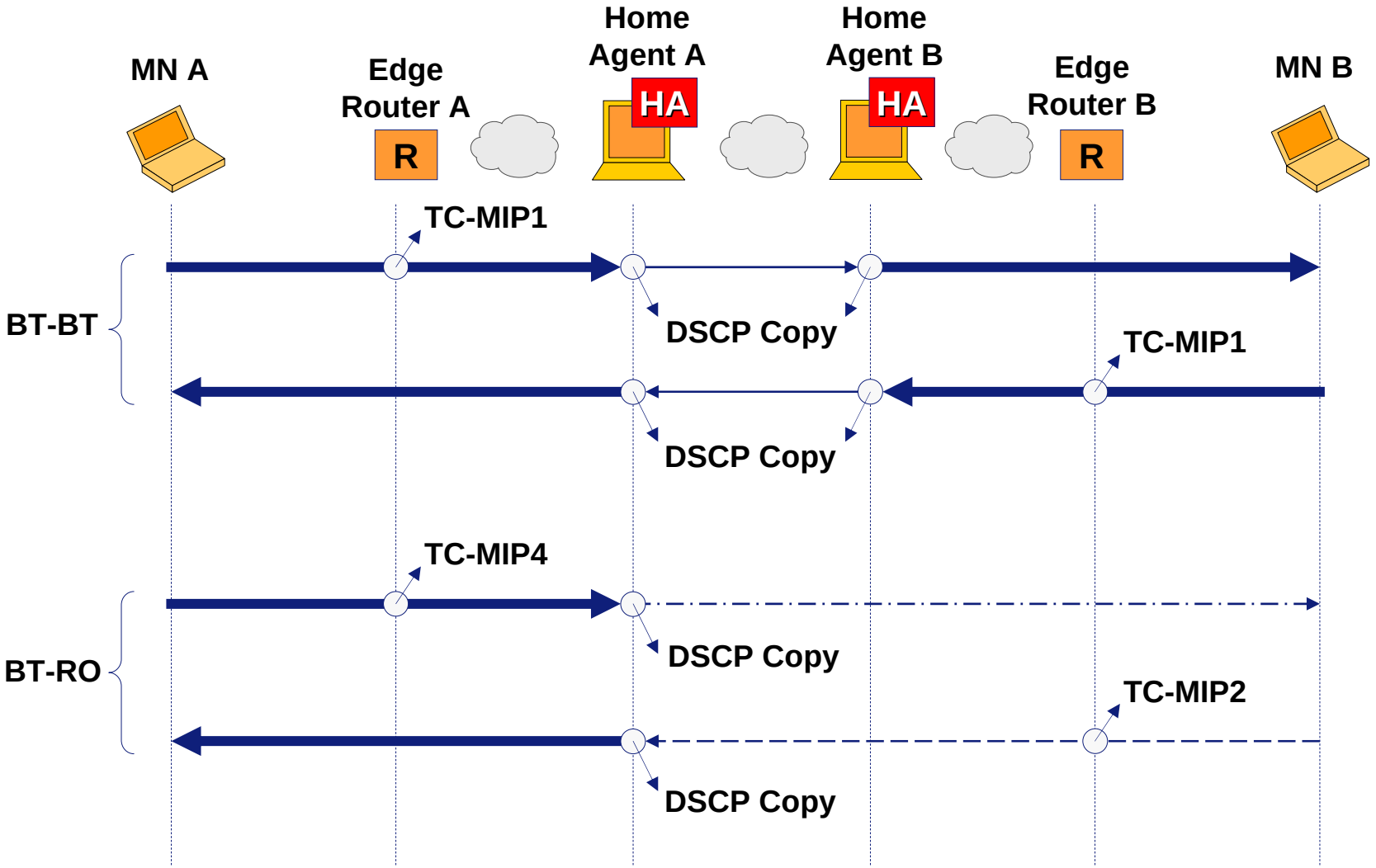
QoS differentiation of data traffic

- Aspects of the problem
  - classification of data traffic
    - in Bi-directional Tunneling and Route Optimization
  - enforcement of QoS policies on the edge routers
    - initial configuration of QoS policies at network attach or service activation
    - re-configuration of QoS policies based across mobile node movements
    - release of QoS reservations at the end of the session
    - Involved authorization issues

Routing of data traffic: mobile-fixed



Routing of data traffic: mobile-mobile



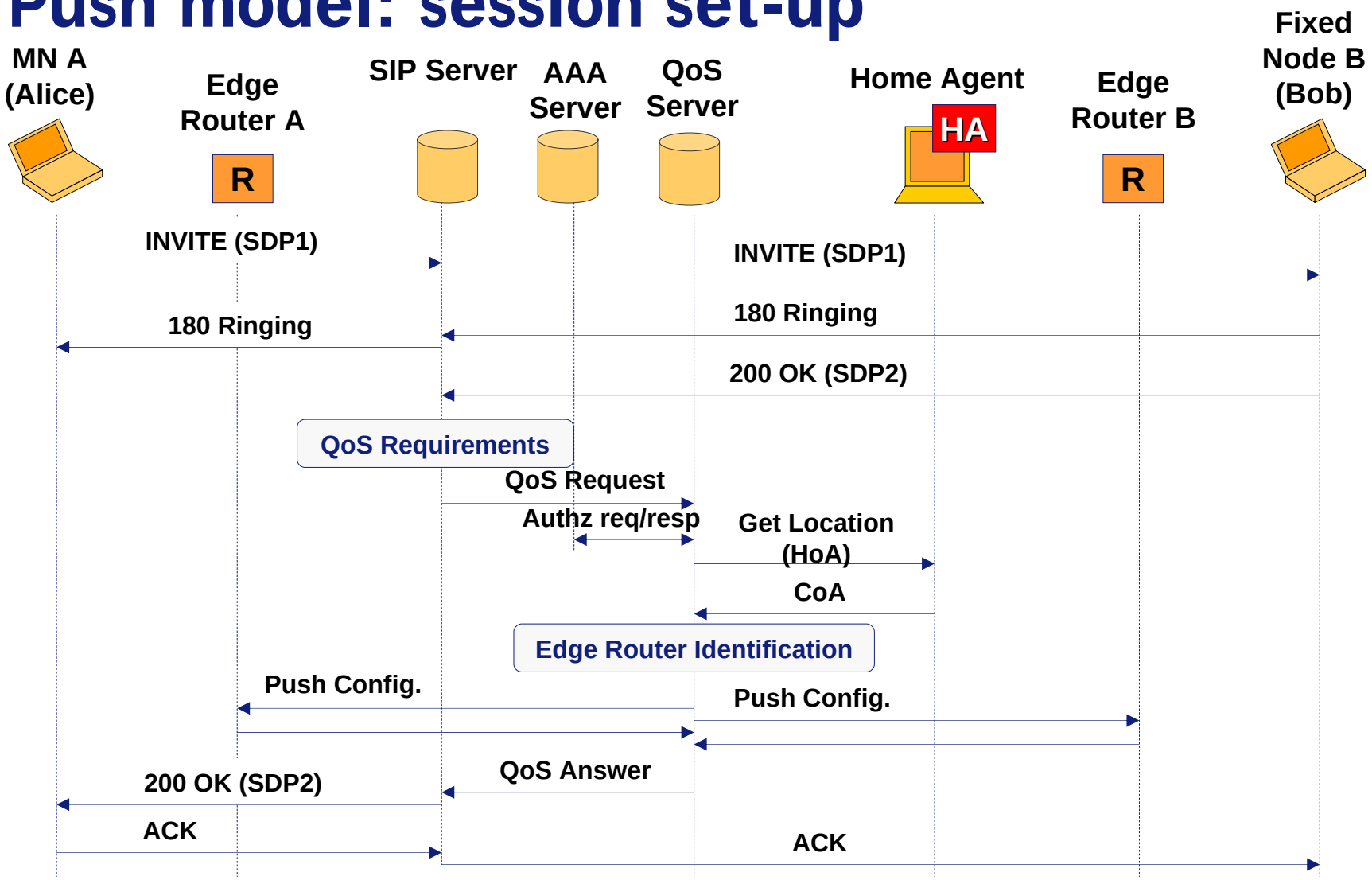
Technical options (I)

- "Push" model (network-based)
  - MN demands (e.g. via SIP) session set-up with the QoS requirements and this acts as trigger for the resources reservation in the network
  - the QoS server identifies the edge routers and installs immediately the QoS reservatopm state (e.g. reservation enforcement)
  - Authorization process takes place usually between the QoS server and the AAA server in the QoS domain (upon session requests).

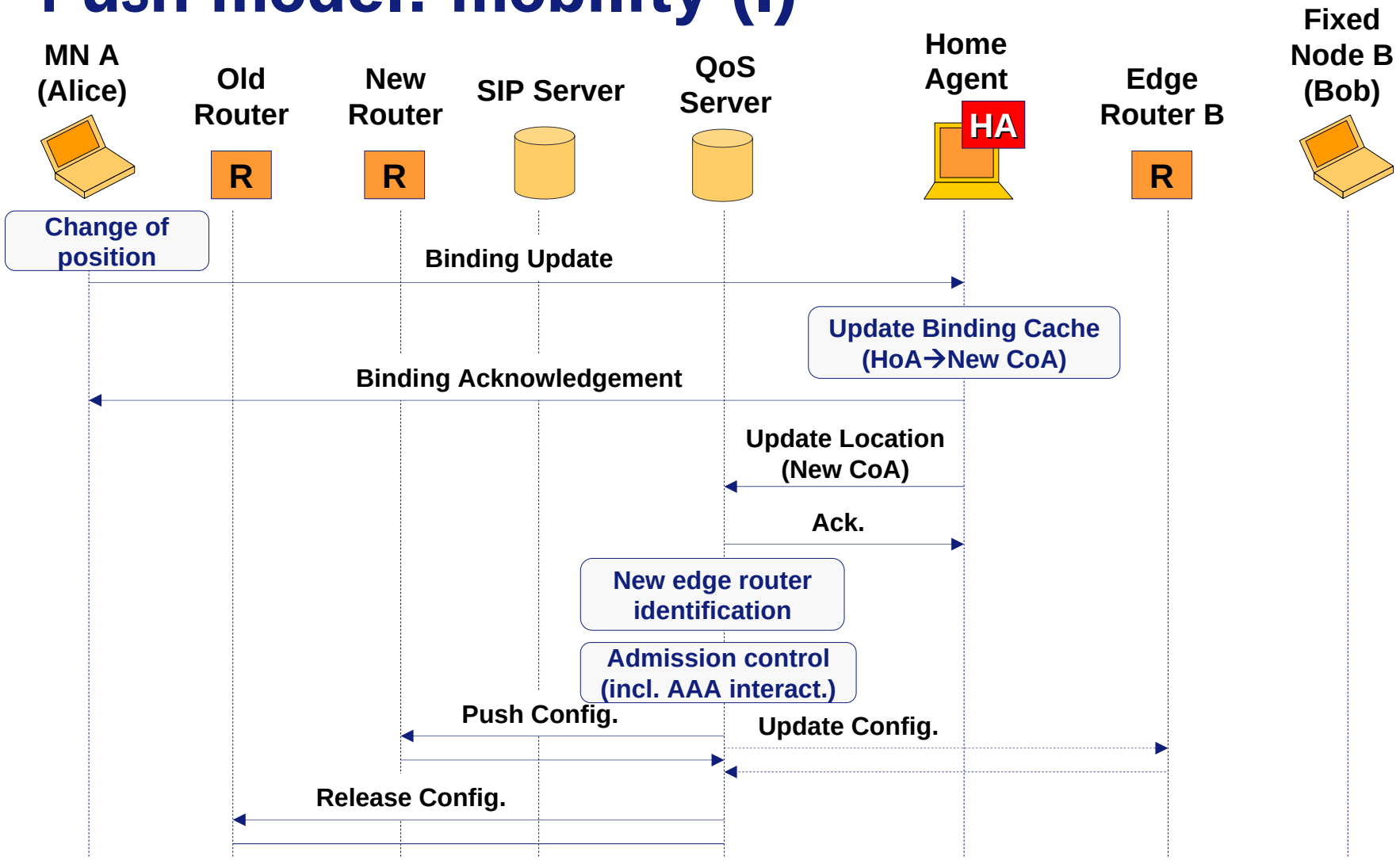
Technical options (II)

- "Pull" model (participation of the mobile terminal)
  - MN initializes access control with the AAA server
    - If successful, AAA server issues the MN with an Authorization Token
    - This might involve cross-domain message exchange: in case of multiple domains, Home AAA server will be contacted and eventually it issues the authorization token
  - MN inserts the Authorization Token in the subsequent reservation request (e.g. RSVP, NSIS)
  - When the edge router receives the reservation request, it contacts the AAA server to verify the token, then the edge router performs local admission control
    - The admission control can be also done with central entity e.g. QoS server/BB
  - If this succeeds, the reservation request is forwarded to next admission control entity in the data forwarding chain

Push model: session set-up



Push model: mobility (I)



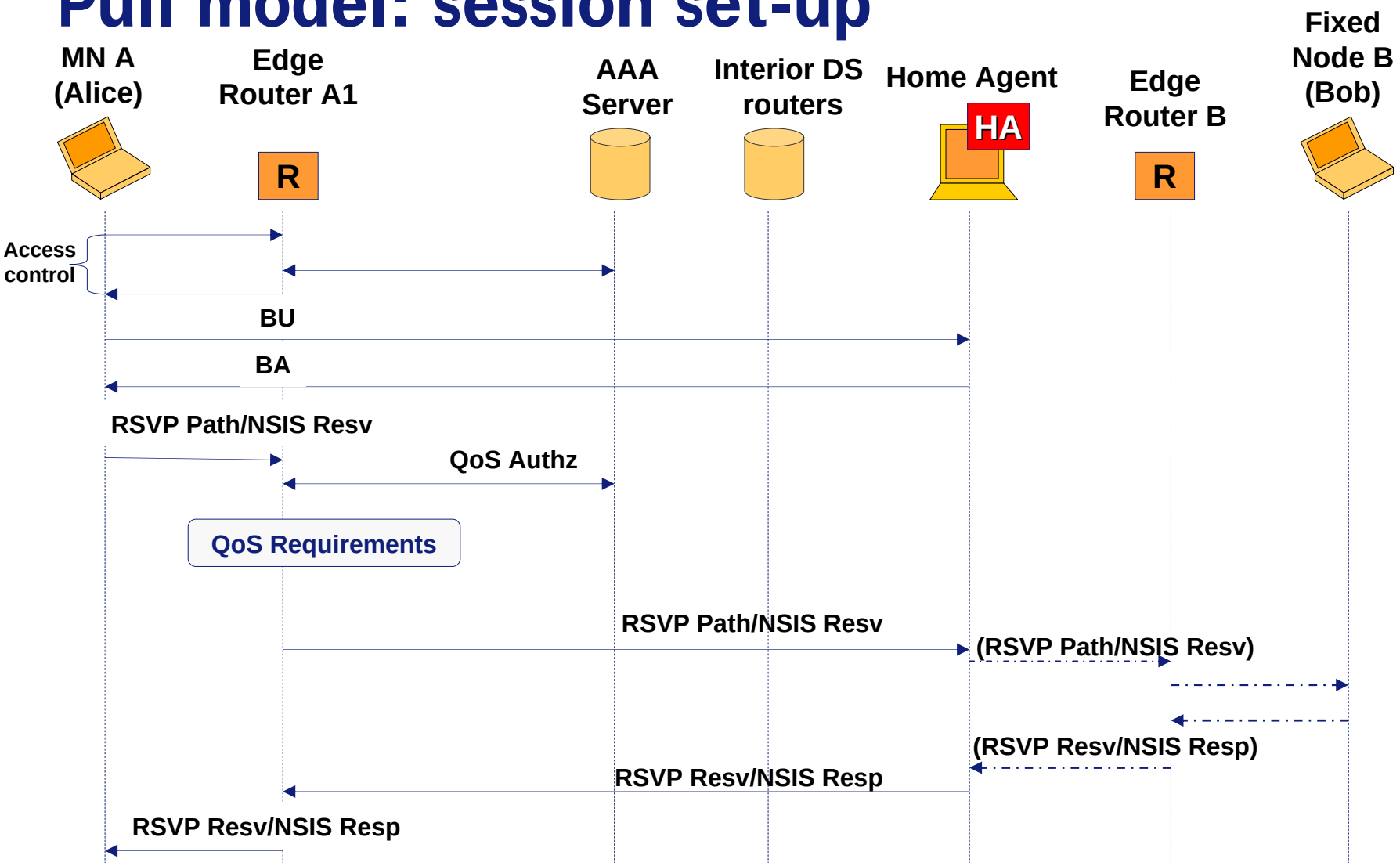
Push model: mobility (II)

- When mobile node movement causes an access router/topology change, the QoS server must repeat the admission control for each active flow
  - it is possible that in the new access network visited by mobile node there are no enough resources
- If the admission control is not passed, the QoS server sends a notification message to the call control platform
  - Then the SIP server can
    - release the communication in progress
    - force a media renegotiation (e.g. quality reduction with a new audio/video codec that generates lower bit-rate)

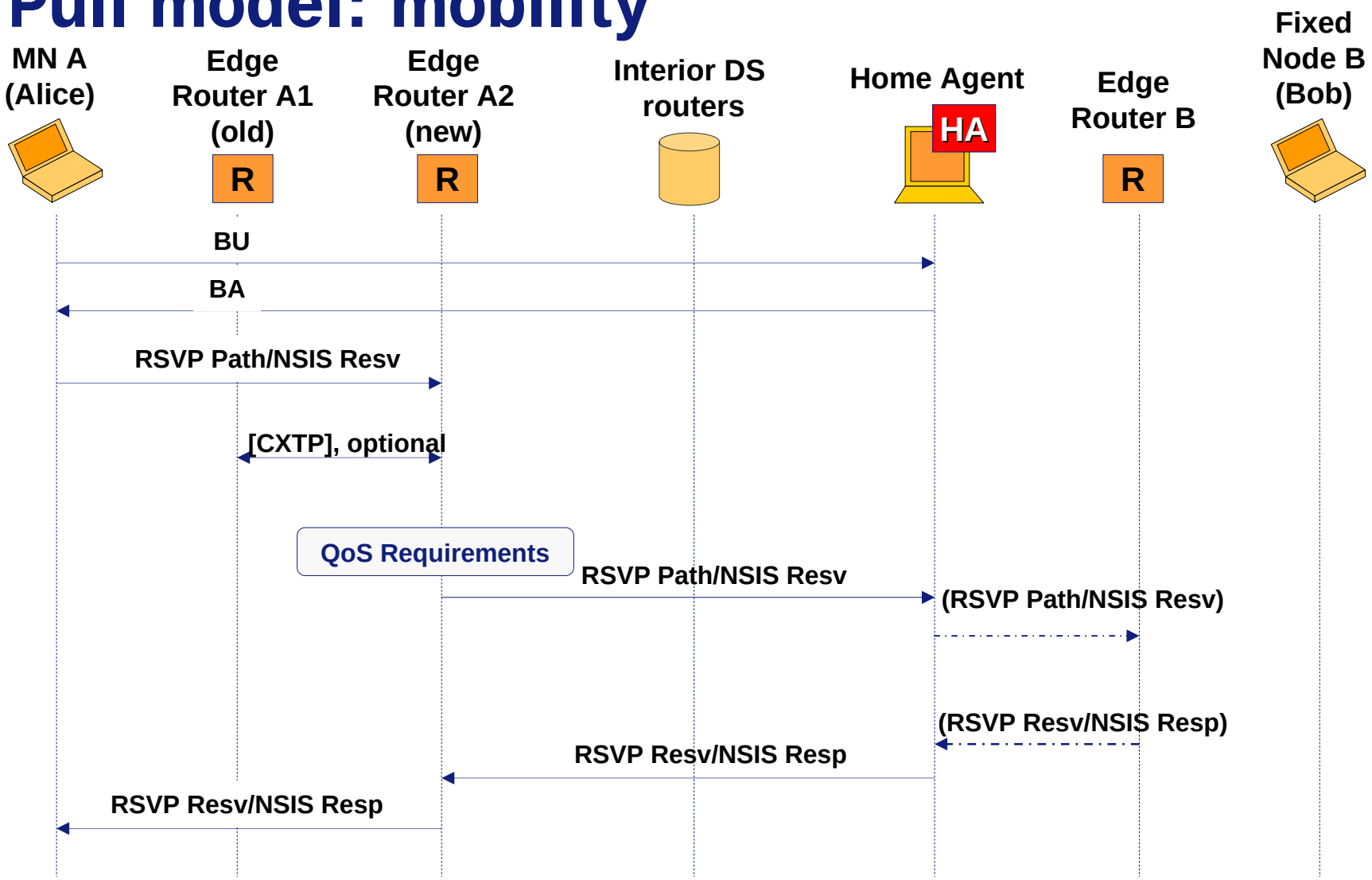
Pull model

- There is no central entity managing the QoS resources for all sessions
- Hop-by-hop way
  - Can use either RSVP or NSIS
  - In the simple case, let's firstly consider single domain
- Admission control is per-request/flow but data plane can be per-class
- Authorization token can be derived during the L7 signaling or the access control phase, by contacting the AAA server
  - We assume that the MN need to have an authorization token with an AAA server in order to obtain desired QoS

Pull model: session set-up



Pull model: mobility



QoS provisioning for data traffic: other issues

- Details for session releases
- Details for session renegotiation in case of lack of resources in the new point of attachment
- Details for optimization:
  - Less message messages
  - Context transfer
  - Details
- Details for multi-domain case

Conclusions

- Premium services (e.g. QoS) are desired for IP mobility networks
  - Changed IP address, changed routing path
  - Influenced by the classic IP protocol and Mobile IP protocol design
- ENABLE QoS Framework intends to offer the operational QoS services for IP mobility networks
- It includes signaling preemption, admission control/signaling and marking for MIPv6 traffic, as well as bootstrapping
- Further open issues are being investigated
  - Admission control details
  - Maybe a better IP mobility framework is desired: issues like locator/identifier split, better routing and addressing coordination, alnative to routing headers?
  - Middlebox configuration in general is a universal problem, not just QoS
  - These two orthognal issues (mobility support and middlebox traversal for IP networks) may eventually result in evolutions to the Internet architecture