



ENABLING EFFICIENT AND OPERATIONAL MOBILITY IN LARGE HETEROGENEOUS IP NETWORKS

Provision of HA reliability for operational MIPv6 service deployment



“Research and Deployment Possibilities based on MIPv6”
workshop at
IST Mobile & Wireless
Communications Summit 2007

Budapest, July 5th 2007

W. Fritsche, K. Mayer (IABG)
M. La Monaca (Telecom Italia)
P. Garcia Segura (UMU)



Agenda

- Overview of ENABLE
- HA reliability approach of mip6 DT
- HA reliability work in ENABLE
- Conclusions

Overview of ENABLE

Overview of ENABLE project

- ENABLE at a glance
 - Research project funded by the European Commission
 - 8 European and one Chinese partner
 - Duration: 2006 - 2007
 - Budget: 3,792 M€
- Goal of ENALBE
 - Enable deployment of efficient and operational mobility as a service in large scale IPv6 network environments
 - 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>

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

Motivation for HA reliability

- A HA is a single point of failure within the MIPv6 service.
- HA could fail for various reasons
 - Crash of HA system
 - DoS attacks to HA
 - No route to HA available
 - Administratively stopped for maintenance reasons
 - ...
- In order to increase availability and reliability of HA functionality, HA redundancy can be added.
- Mip6 Design Team is working on HA reliability solutions covering MN and MR registrations (*Note: This presentation mainly focuses on MNs*)

HA reliability approach of mip6 DT

Core approach of HA reliability (I)

- Introduction of redundancy for HA functionality
- Redundant HA Set consists of
 - One Active HA
 - One or more Standby HAs
- Provision of reliability by Redundant HA Set
 - All HAs (Active and Standby) are available at MN bootstrapping
 - Active HA serves MNs for a home address/prefix
 - Switch to Standby HA in case Active HA fails
 - Switch between HAs should be transparent to applications
- Two modes for HA reliability
 - One mode completely transparent for MN (HA Virtual Switch)
 - One mode requiring to inform the MN about HA switch (HA Hard Switch)

Core approach of HA reliability (II)

- State synchronization
 - Information hold for MNs must be synchronized between Active and Standby HAs
 - ❑ Binding Cache Information hold for MNs
 - ❑ Security and AAA state information hold for MNs
- Secured Message Exchanges
 - Messages exchanged between HAs have to be secured
- Failure Detection
 - Redundant HAs must actively check for failure of Active HA
 - In Hard Switch mode a MN will be notified about HA failure
- Two WG drafts on this item
 - Protocol between HAs
 - ❑ Home Agent Reliability Protocol (draft-ietf-mip6-hareliability-01.txt)
 - Protocol between HA and MN
 - ❑ Mobility Header Home Agent Switch Message (draft-ietf-mip6-ha-switch-03.txt)

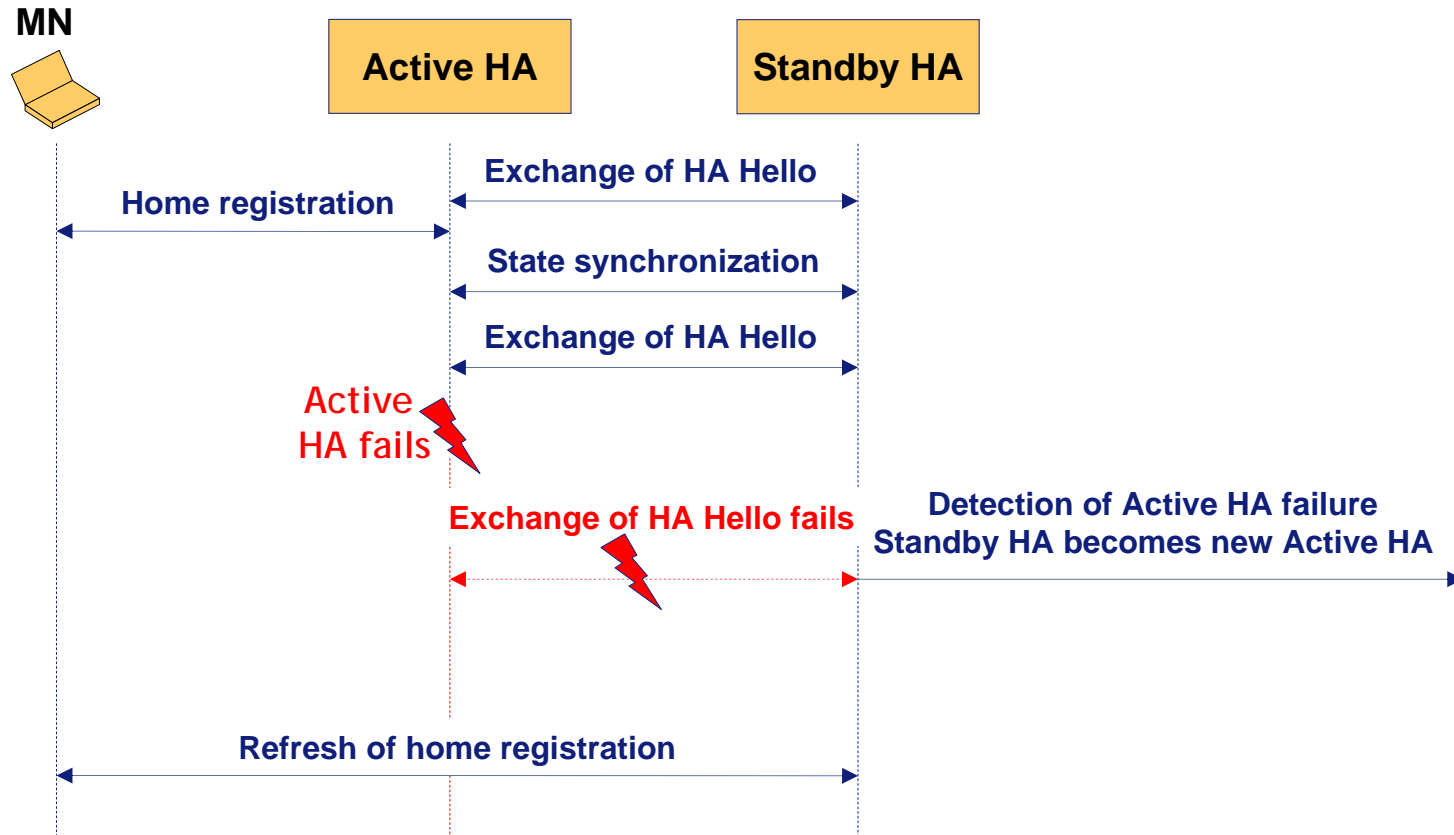
New MHs and Mobity Options

- The core functionality of the HA reliability functionality makes use of the following new MHs ...
 - Home Agent Hello Message
 - ❑ Solicited and unsolicited Home Agent Hello Messages
 - State Synchronization Message
 - ❑ Requests and Replies
 - Home Agent Control Message
 - ❑ SwitchOver Requests and SwitchOver Replies
 - ❑ SwitchBack Requests and SwitchBack Replies
 - Home Agent Switch Message
- ... and of the following new Mobility Options
 - Binding Cache Information Option
 - AAA Information Option
 - New subtypes (Home Agent Address, Home Address) for the IP Address Option

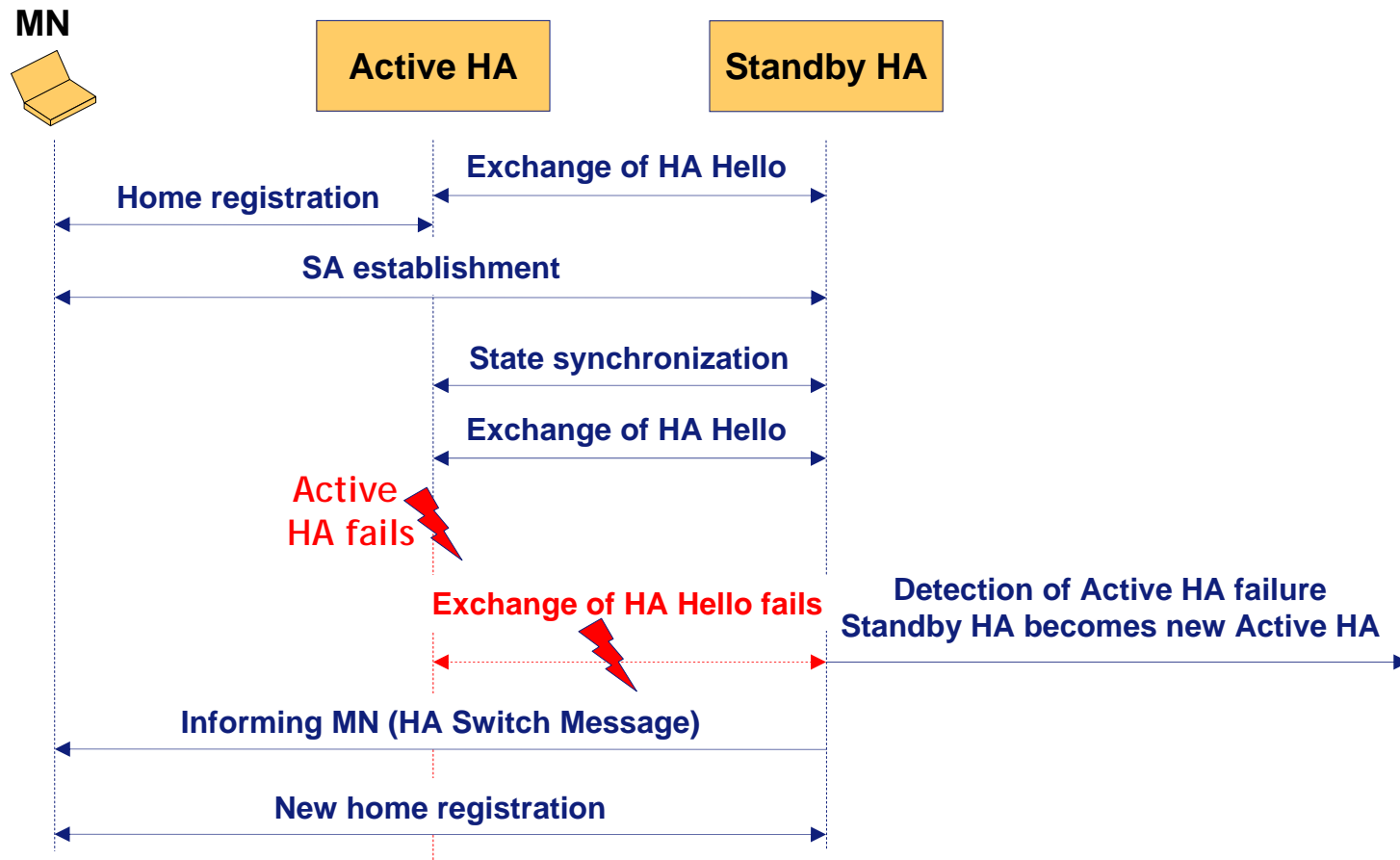
Failure detection

- Failure detection is done using a Hello mechanism between all HAs of the redundant HA set (Active HA and Standby HA(s))
 - This mechanism is similar as the one defined by MIPv6 for multiple HAs on a link based on RAs
 - However, frequency and processing of RAs cannot be controlled by HA reliability functionality
 - In case only HA functionality fails, ICMP may still work, consequently RAs wouldn't detect this failure
 - Therefore an own Hello mechanism has been defined for HA reliability
- The Active HA sets the A flag in its HA Hello Message
- HA Hello Messages are sent either unicast or multicast
- If a HA Hello Message is not received from a HA peer within a configurable amount of time, it is considered to have failed

Home Agent Virtual Switch mode



Home Agent Hard Switch mode



HA reliability work in ENABLE

Operational design assumptions for HA reliability

- For economical reasons Standby HAs have to serve multiple Active HAs
- In an operational deployment all HAs are likely to be placed in a secure environment
 - they can communicate securely with each other without any additional security protocol
- Redundant HAs are likely to be placed on a single link („Local Recovery“)
 - Providing redundancy over different links („Global Recovery“) will take too long due to changes required in routing
 - IP Multicast can be used for e.g. HA failure detection or state synchronization
- Establishing and maintaining more than 2 SAs for a MN via the air interface may not be acceptable by mobile operator
- In case an Active HA fails and returns to operation later, it is not necessary to take back its previously registered MNs
 - It can also continue to serve as Standby HA

Binding Cache information to be synchronized

- Information to be synchronized from Binding Cache includes
 - HoA of registered MNs
 - CoA corresponding to the MN's HoA
 - Lifetime value, indicating the remaining lifetime of a Binding Cache entry
 - Flags, indicating e.g. whether the Binding Cache entry represents a home registration
 - Maximum Sequence Number received within previous BUs
- All in all for MIPv6 42 octets would need to be synchronized for Binding Cache entries
 - To increase efficiency, for the Hard Switch mode knowing the CoAs of MNs registered with an Active HA might be sufficient

Authent. Protocol inform. to be synchronized

- Auth. Protocol specific information to be synchronized
 - Shared-key-based mobility SA
 - ❑ SPI
 - 4 octets
 - ❑ MN-HA key and corresponding lifetime and name
 - 128 (default) + 32 + 64 octets
 - ❑ algorithms for authentication and replay protection
 - 1 octet
 - 1 bit specifying the replay protection mechanism (i.e. timestamps/BU seq. numbers)
 - 7 bits specifying the selected authentication algorithm
- Total = 229 octets
- This information is synchronized only when MNs bootstrap / are relocated / or a MN-HA key expires

IPsec information to be synchronized

- The following information must be synchronized
 - Security Policy Database (SPD) and selectors
 - ❑ About 16 bytes need to be synchronized for every sent/received IP packet
 - ❑ About 162 bytes need to be synchronized on each policy creation
 - Security Association Database (SAD)
 - ❑ About 36 bytes need to be synchronized for every sent/received IP packet
 - ❑ About 297 bytes need to be synchronized on each SA creation
 - IKEv2 Security Association (IKEv2 SA)
 - ❑ About 3004 bytes need to be synchronized on each sent/received IKEv2 message
 - ❑ About 1084 bytes need to be synchronized on each IKE_SA creation
- Synchronizing IPsec information may easily result in unacceptable overhead

AAA information to be synchronized

- The Diameter connection itself including TCP/SCTP/TLS/IPsec state may be synchronized
 - Alternatively it may be disconnected after HA failure
- There are also plenty of AVPs to be synchronized
 - User-Name
 - Session-Id
 - IKEv2-PSK AVP
 - IKEv2-PSK-Lifetime AVP
 - IKEv2-PSK-Name AVP
 - MN-HA-Key AVP
 - MN-HA-Key-Lifetime AVP
 - MN-HA-Key-Name AVP
 - ...
- There may also be the requirement to synchronize accounting information
- It's difficult to assess the overhead for synchronization of AAA information

Conclusion

Conclusion

- An operational HA service provision has to be reliable
 - This requires deployment of multiple HAs and their synchronization to a certain extent
- The Virtual Switch mode would be preferable from an end-user point of view, however
 - Synchronizing accounting information seems difficult to achieve
 - Synchronizing per packet IPsec state seems difficult to achieve
 - Using the Authentication Protocol without synchronization of accounting information seems possible
- The Hard Switch mode is simpler from a synchronization point of view
 - More than 2 simultaneous SAs between MN and HAs via the air interface seems difficult to get deployed by mobile operators
 - Also here the usage of the Authentication Protocol may be an option

Further information

- Visit ENABLE project website www.ist-enable.com
- Contact

Wolfgang Fritsche

Head of Internet Competence Center

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.