NSIS Working Group
Internet-Draft
Expires: August 21, 2008

L. Cordeiro
M. Curado
Univ. Coimbra
P. Neves
PTIn
S. Sargento
Univ. Aveiro
G. Landi
CPR
X. Fu
Univ. Goettingen
February 18, 2008

# Media Independent Handover Network Signalling Layer Protocol (MIH NSLP)
draft-cordeiro-nsis-mih-nslp

## Status of this Memo



## Copyright Notice

Abstract

This memo defines the Media Independent Handover Network Signalling Layer Protocol (MIH NSLP) for the transport of messages from the IEEE 802.21 standard using the Next Steps in Signalling (NSIS) framework. The MIH NSLP is responsible for the transport of MIH messages to remote entities reporting on link layer information, in order to support seamless mobility in heterogeneous environments. A usage example of the MIH NSLP is also provided.

Table of Contents

## 1. Introduction

In order to improve the handover between heterogeneous access networks, the IEEE 802.21 standard is being defined to provide Media Independent Handover services (MIH). IEEE 802.21/MIH makes available link layer information to the upper network layers, both locally and remotely. Although the standard defines the guidelines to transport the MIH protocol messages to remote entities, namely the need to be reliable and to guarantee security of the messages exchanged, it does not specify a transport mechanism. [1] describes a possible design for the MIH transport mechanism; however it requires a multitude of new protocol elements and is also limited in several technical constraints such as message size and protocol discovery.

The IETF NSIS WG is finalizing the base protocols to offer flexible and extensible signalling services for a variety of application, including the General Internet Signaling Transport (GIST) for support secure, reliable, congestion-controlled data transport, as well as other features desired for signalling. Given the potential of NSIS to perform Quality of Service (QoS) signalling for real-time applications in wired and wireless scenarios, which is also often desired by the applications using MIH, we propose to use GIST to transport MIH messages. Therefore, this document defines a Media Independent Handover NSIS Signalling Layer Protocol (MIH NSLP) to support seamless mobility in heterogeneous network environments through the integration of MIH and NSIS.

This document is structured as follows. Section 3 presents the motivation for the development of a MIH NSLP. Section 4 details the MIH NSLP and Section 5 shows an example of the use of the MIH NSLP in a mobility scenario.

## 2. Terminology and Abbreviations

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",

"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [2].

The following additional terms are used:

- E2E: End-to-End
- QoS: Quality of Service
- MIH: Media Independent Handover





- MIH NSLP: Media Independent Handover NSIS Signaling Layer Protocol, uses NSIS as the transport protocol for MIH messages.
- NSIS: Next Steps in Signaling
- GIST: General Internet Signaling Transport
- WLAN: Wireless Local Area Networks
- WiMAX: Worldwide Interoperability for Microwave Access
- UMTS: Universal Mobile Telephone Service
- MBMS: Multicast and Broadcast Multimedia Services
- DVB: Digital Video Broadcast
- SAP: Service Access Point
- MICS: Media Independent Command Services
- MIES: Media Independent Event Services
- MIIS: Media Independent Information Services
- MIHF: Media Independent Handover Function
- MIHU: Media Independent Handover User

- ASN: WiMAX Access Service Network
- AN: Access Network
- CSN: WiMAX Connectivity Service Network
- CN: Core Network
- MS: Mobile Station
- TCP: Transmission Control Protocol
- UDP: User Datagram Protocol
- BS: WiMAX Base Station
- SS: WiMAX Subscriber Station





- AP: WiFi Access Point
- SF: WiMAX Service Flow
- HA: MIP Home Agent
- CoA: MIP Care of Address
- AAA: Authentication, Authorization and Accounting
- ASN-GW: WiMAX Access Service Network Gateway
- MIH Registration Server: responsible to handle the MIHF ID into network address mapping.

## 3. Problem Statement

With the current evolution of network technologies we envision that, in a near future, there will be a heterogeneous landscape of different technologies such as WLAN, WiMAX, UMTS/MBMS and DVB, providing ubiquitous network access to users. The wide availability

of co-located technologies and the growing trend of users' mobility, require the seamless support of mobility and service continuity. Nevertheless, due to the large number of new access technologies, it is very difficult to provide seamless mobility across these technologies.

In order to optimize the handover process, the IEEE is currently defining the 802.21 standard, focused on Media Independent Handover services (MIH). The main goal of the IEEE 802.21 standard is to provide link layer information to the upper layers, optimizing the handover process between heterogeneous access networks. The Media Independent Handover Function (MIHF) is the core component of the 802.21 standard. It provides a set of well defined and standardized Service Access Points (SAP) with both the link layer (MIH_LINK_SAP) and the upper layers (MIH_SAP) that will use this information (MIH users). A set of services is provided through these interfaces in order to facilitate the communication process:

- Media Independent Command Service (MICS): allows higher layers to configure, control and get information from the lower layer.

- Media Independent Event Service (MIES): allows higher layers to receive indications from link layers.

- Media Independent Information Service (MIIS): provides a framework and corresponding mechanisms by which a MIHF entity obtains static





network information.

Events and commands can be local and/or remote. Local events are generated from the link layer and propagated towards the MIH users within the local device. Remote events are propagated towards a MIH user connected to a peer MIHF.

Several network elements might be interested to receive notifications from the lower layers, and therefore the MIH protocol has been defined to propagate the MIH services towards the peer MIHFs.

Figure 1 illustrates the distribution of the MIHF entities across the network components.

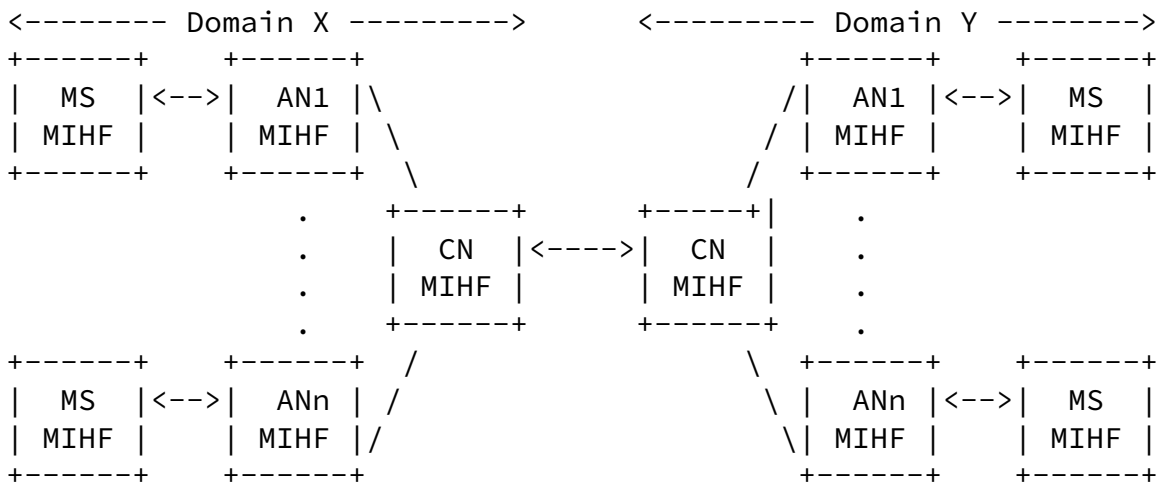


Figure 1: MIHF Communication Model

The MIHFs might be spread in several network elements inside the same domain, or even across different domains. In Figure 1 we illustrate two different domains (domain X and domain Y). Each domain is composed by the Core Network (CN), responsible for the overall management and control of the network, connected to several Access Networks (AN). Each AN provides connectivity to the Mobile Stations (MS), using wired/wireless access technologies (e.g. WiMAX, DVB, WiFi, UMTS). As depicted in Figure 1, each one of these entities - CN, AN and MS - is a potential candidate to host the MIHF entity. Therefore, MIH messages SHALL be able to reach all the MIHFs in the network, independently of their location.

However, no specific transport mechanism is defined to carry the MIH protocol messages between remote MIHFs. Only the guidelines to transmit the MIH messages across the network are defined in the MIH standard. The transport protocol used MUST be reliable, guaranteeing





the correct delivery of the messages to the peer MIHF, and provide security over the exchanged messages.

The Transmission Control Protocol (TCP) is able to satisfy the reliability requirement posed by the MIH protocol. It provides error control and flow control, guaranteeing the in-order delivery of the packets. However, although TCP offers reliability, it does not guarantee fast-packet delivery due to its retransmission mechanism.

In what concerns the User Datagram Protocol (UDP), it assures fast-packet delivery, but it does not guarantee the correct packet delivery, and therefore is unreliable.

As a result, a reliable, secure and fast-delivery solution to transport MIH protocol messages between peer MIHFs is required. Although a new fast-delivery solution can be designed, other existent solutions can be envisioned.

To address seamless mobility support, media independent handovers together with fast/local mobility approaches are not sufficient. When users move while accessing real-time services, resources need to be reserved in advance in the new network to guarantee that the services maintain their quality. Next Steps in Signalling (NSIS) [3] QoS signalling protocol is an emergent QoS signalling and reservation protocol with capabilities to be used in mobile environments. NSIS decomposes the overall signalling protocol suite into a generic (lower) layer and specific upper layers for each specific signalling application. In the lower layer, General Internet Signalling Transport (GIST) [4] offers transport services to higher layer signalling applications for two purposes: sending and receiving signalling messages between neighbour hops (NSIS entities), and exchanging control and feedback information. Above this layer, there is the NSIS Signalling Layer Protocol (NSLP) layer [5], which generically stands for any protocol within the signalling application layer.

NSIS is very well suited for heterogeneous wired and wireless networks and is able to interact with mobility protocols for seamless handovers. Therefore, to enable the support of seamless mobility, MIH can be integrated with NSIS and cooperate in the handover process. To provide a clean cooperation with low overhead (both in messages exchanged and time), and since MIH protocol messages require a transport protocol, we propose and define a MIH NSLP to use NSIS as a transport protocol for MIH messages.

## 4. Media Independent Handover NSLP Specification

In order to use the NSIS framework to transport MIH messages, a





specific NSLP, the Media Independent Handover NSLP, is developed in

this document. The MIH NSLP allows the distribution of MIH messages across different networks. The following describes the procedure to transport MIH messages within the MIH NSLP, followed by the specification of the MIH NSLP architecture.

## 4.1. MIH NSLP Architecture

The MIH NSLP is responsible for the transport of MIH Messages using the GIST protocol. Figure 2 details the architecture of NSIS usage as the MIHF transport protocol.

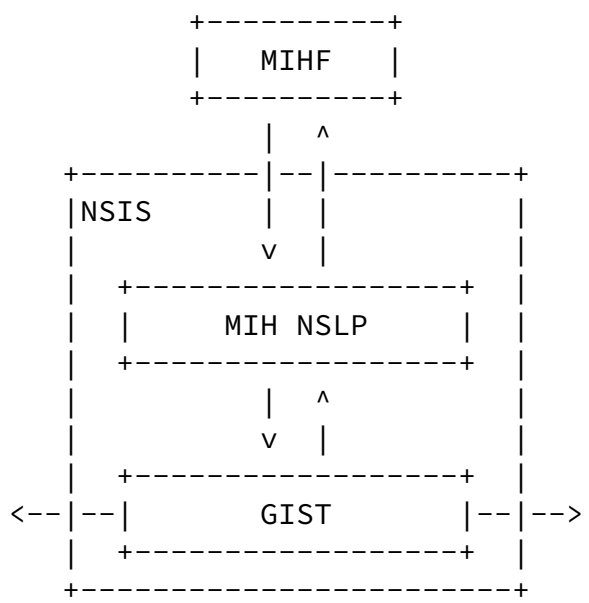


Figure 2: MIH NSLP architecture

This figure shows the interaction between the MIH NSLP, the MIHF and the GIST protocol.

The MIH NSLP interface with MIHF handles the MIHF MIH Message exchange. This interface is compliant with the MIH_NET_SAP defined in [6].

The MIH NSLP interface with GIST handles message transport. This interface is specified in [4].

The MIH NSLP is split in six different functionalities as follows:

o Interface with MIHF

- Interface with GIST
- Message transport (and retransmission if acknowledge is required)
- Message reception
- Message interception
- MIH Registration Server (only active through an election process - out of scope)
  - Registration
  - DeRegistration
  - Request
  - Messages retransmission

These functionalities are described in the next sections.

## 4.2. MIH Message Transport

As specified in [6], MIHF entities need to propagate MIH messages towards peer MIHF entities. The MIH standard does not include the specification of a transport protocol, at layer 3, and only the requirements for this protocol are defined. These requirements can be summed up to reliability and security over the MIH exchanged messages, requirements that are met by the GIST protocol.

Figure 3 shows an example of the NSIS usage to transport MIH Messages.

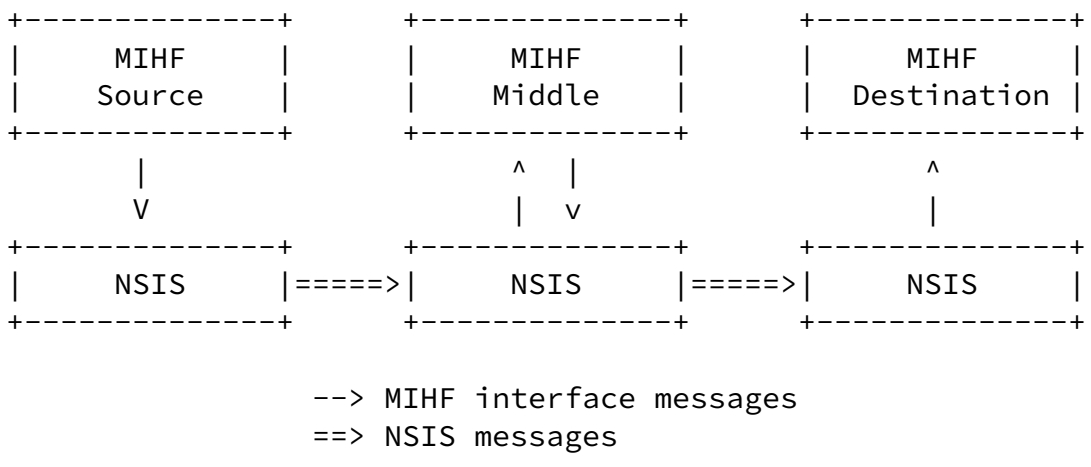

Figure 3: NSIS usage to transport MIH Messages

This figure presents the interaction between the MIHF and the NSIS framework and the transport of MIH Messages between a Source and a Destination MIHF. In this scenario, the Middle MIHF also intervenes by receiving the message exchanged due to the intercept NSIS feature. The processing of these intercepted messages is out of the scope of this document.

To be able to transport the MIH Messages, NSIS requires the destination network address of the MIHF Destination. However, MIH entities only handle MIHF Identifiers (ID) to identify the remote MIHF. Therefore, there is the need to perform the mapping between the MIHF ID and the correspondent network addresses, which is under NSIS responsibility.

The main functionality of the MIH NSLP is to handle the mapping between MIHF ID and network addresses, since GIST is able to provide all the required functionalities required by the MIH specification for MIH Message transport. The mapping procedure is described in the next sub-section.

Figure 4 shows the procedure to send MIH Messages to the remote MIHF when the remote MIHF IP Address is available, either through the cache mechanisms or resorting to the mapping procedure.

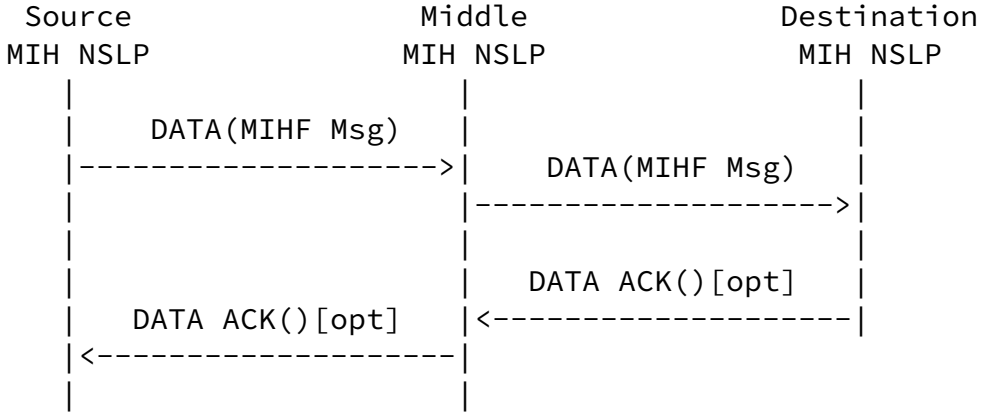

Figure 4: Message transport between two MIH NSLP

In this figure the MIHF Message needs to be sent from the Source MIH NSLP to the Destination MIH NSLP. To send the MIHF Message, the MIH NSLP creates a MIH NSLP DATA message with the MIHF Message as one of its components.

During the message exchange, the DATA message is intercepted in the





Middle MIHF. According to the MIH NSLP architecture, this feature could be useful for several scenarios. However, this feature is out of scope of this document. If no specific action is defined in the Middle MIHF entity, the MIH NSLP MUST forward the DATA message to the Destination MIH NSLP.

When a DATA message reaches the destination, the MIHF Message is forwarded to the local MIHF for processing. The MIH Message information is transparent to the MIH NSLP. The MIHF processing is defined in [6].

Optionally, a DATA ACK message can be sent to the Source MIH NSLP when the DATA message arrives to the Destination MIH NSLP. This feature can be requested by the Source MIH NSLP and SHOULD depend on the transfer attributes requested to GIST (reliable and/or secure).

A MIHF response to the received MIH Message is treated as a new request by the MIH NSLP. The MIH NSLP does not handle states for the MIH Messages.

## 4.3. Mapping between MIHF ID and Network Addresses

In order to map all MIHF ID into network addresses a MIH Registration Server is required. This MIH Registration Server is responsible for handling the mapping between MIHF ID and network addresses of MIHF entities. For this purpose one entity MUST be elected as a MIH Registration Server. The election of this entity is out of scope of this document because it depends on specific deployment scenarios characteristics. In the example described in Section 5 an appropriate choice would be the CN entity. The knowledge of the MIH Registration Server MUST be known to all MIHF entities involved.

With the usage of the MIH Registration Server, when a MIH NSLP needs to send a MIH Message to a remote MIHF, it queries the MIH Registration Server in order to receive the appropriate network address. Figure 5 and Figure 6 highlight the MIH NSLP message exchange to perform a MIHF ID mapping to a network address.

Figure 5 describes the procedure that a MIH NSLP performs when it is ready to transport MIH Messages.





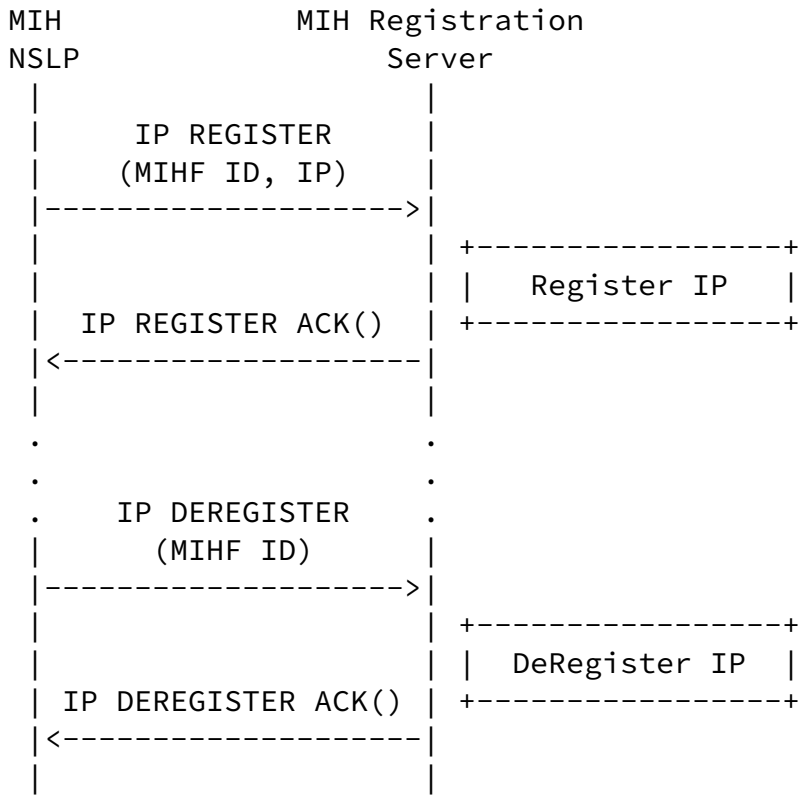


Figure 5: MIH NSLP registration/deregistration in a MIH Registration Server

This registration procedure is composed by four MIH NSLP messages, the IP REGISTER, the IP REGISTER ACK, IP DEREGISTER and the IP DEREGISTER ACK. The IP REGISTER message is sent by the MIH NSLP to the MIH Registration Server to register its MIHF ID and IP Address in the MIH Registration Server. To confirm the registration of the MIH NSLP, the MIH Registration Server sends an IP REGISTER ACK to the MIH NSLP with the result of the registration. The registration result can be:

- Successful: the registration process was successful;
- Warning due to duplicate MIHF ID: the received MIHF ID already exists with a different IP Address;
- Warning due to duplicate IP Address: the received IP Address already exist with a different MIHF ID;
- Internal failure: an error occurred not related to the request received.

After a successful/warning registration procedure the MIH Registration Server is able to map this MIHF ID to the appropriate IP





Address and the MIH NSLP is ready to transport MIH Messages. The MIH NSLP actions to a warning and failure registration are implementation dependent.

The IP DEREGISTER message is sent to the MIH Registration Server when the MIH NSLP intends to stop functions. This message includes the MIHF ID that is to be removed from the registry. After the registry deregistration the MIH Registration Server send an IP DEREGISTRATION ACK to the MIH NSLP notifying it of the registration result. The deregistration result can be:

- Successful: the deregistration process was successful;
- Warning due to unknown MIHF ID: the received MIHF ID does not exists;
- Internal failure: an error occurred not related to the request received.

Figure 6 describes the procedure that a MIH NSLP performs to map a MIHF ID to an IP Address.

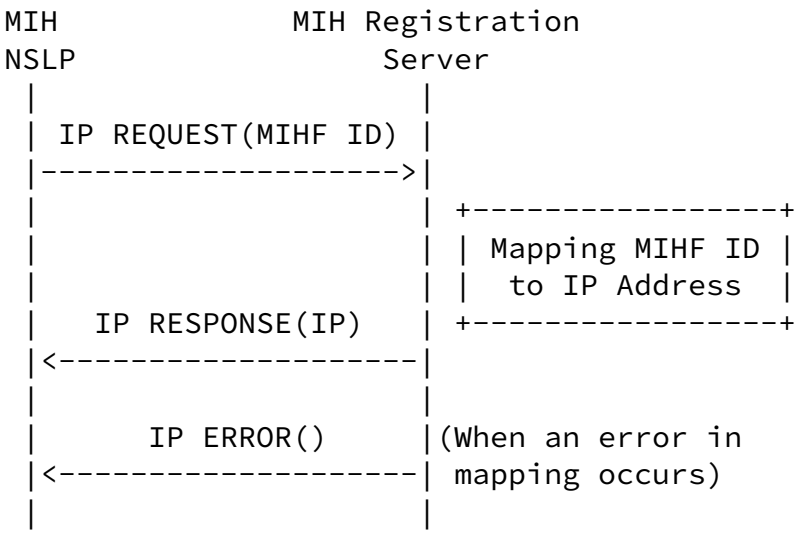


Figure 6: MIH NSLP mapping procedure

In this figure there are two MIH NSLP messages, the IP REQUEST and the IP RESPONSE. The IP REQUEST message is sent from the MIH NSLP that requires the mapping to the MIH Registration Server with the MIHF ID that needs to be mapped to an IP address. After the MIH Registration Server mapping, an IP RESPONSE message is sent from the MIH Registration Server to the requesting MIH NSLP. This message includes the IP address that resulted from the mapping of the request





MIHF ID.

In the MIHF ID mapping process some errors MAY occur. When an error happens the MIH Registration Server entity MUST send an IP ERROR message to the requesting MIH NSLP stating the error. The possible errors are:

- Unknown MIHF ID: there is no reference to the requested MIHF ID;
- Unknown IP Address: there is no IP Address associated to the requested MIHF ID;

- Internal Error: an error occurred not related to the MIHF ID or the IP Address.

When IP REGISTER, IP DEREGISTER and IP REQUEST messages are sent, a timer MUST be set to prevent the case of starvation due to a failure in receiving the respective responses. These cases can occur when:

- The MIH Registration Server cannot be reached;

- The MIH Registration Server fails to respond.

If a timer expires, the IP REGISTER, IP DEREGISTER or IP REQUEST message MUST be retransmitted until a maximum of three times. Each time the timer expires the timer period SHOULD be doubled.

For the IP REGISTER ACK, IP DEREGISTER ACK, IP RESPONSE and IP ERROR messages there is no need for timers. In the case these messages fail to arrive to the MIH NSLP, the retransmission procedure will force the resend of the appropriate response message.

## 5. Mobility Scenario Example

This section will present an example (including a picture) of the use the Mobility NSLP to transport MIH messages in the mobility context - controlled by the CSN.

This section presents a sample mobility scenario, where the exchange of MIHF messages among different network nodes allows the efficient management of control plane functionalities, such as data plane configuration and resource reservation for the traffic flows involved in the handover.

The example scenario is shown in Figure 7. It consists of a Mobile Node (MN) with two network interfaces (ETH and WiFi) which is connected to a Wi-Fi Access-Point attached to a WiMAX fixed





Subscriber Station (serving SS). The MN moves and, since the radio signal becomes lower, the user decides for the ETH connection and plugs in the cable. The ETH network is connected to another WiMAX fixed Subscriber Station (target SS), located in the same Access

Service Network of the serving SS. Both the stations are connected to Base Stations (BS) controlled by the same ASN gateway (ASN-GW).

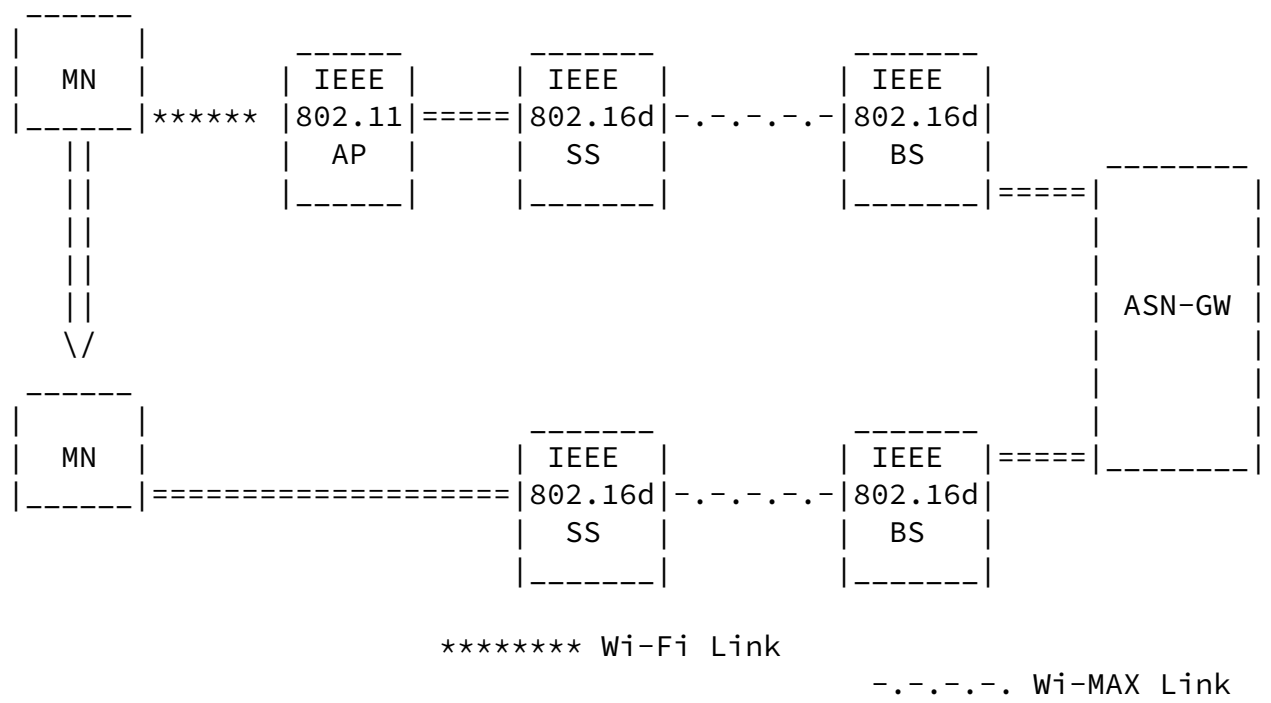


Figure 7: Example of Mobility Scenario with heterogeneous networks

This type of scenario includes a double mobility. The host is initially connected via Wi-Fi and afterwards uses the wired ETH connection (mobility between heterogeneous networks). At the same time the handovers involves two Subscriber Stations of the same WiMAX technology (IEEE 802.16d), following the intra-ASN WiMAX mobility model.

The considered MN hosts some active applications that require specific levels of guaranteed QoS. Therefore the related sessions are initially associated to a particular set of Service Flows (SFs) allocated on the WiMAX channel between the serving SS and its BS. Each SF is characterized by a specific scheduling class and some parameters, like bandwidth and jitter that specify the QoS level for the data traffic.

Following a network-initiated approach, the SF configuration and activation is handled at the ASN-GW level by specific procedures that

intercept different kinds of high level signalling (i.e. QoS NSLP, SIP) in order to extract the QoS parameters required by the application, map them in a set of SFs and finally configure the BSs to allocate the resources on the wireless link.

The MN handover requires the WiMAX channel re-configuration, with the creation and the activation of suitable SFs between the target SS and the related BS. On the other hand, the existing SFs between the serving SS and the related BS MUST be removed. This procedure SHOULD be transparent to the high level signalling and, at the same time, requires the direct action of the ASN-GW for the session management and the explicit resource allocation in the WiMAX link.

This objective can be easily reached with the exchange of MIH messages between the MN and the ASN-GW using the MIH NSLP. When specific MIH Events are received by the gateway, the ASN-GW module that handles the sessions and the WiMAX resource allocation (i.e. the MIH User - MIHU) is informed of probable imminent handovers, configures the resources on the new path and updates its internal status with the up-to-date information about the involved sessions.

Similarly, if the mobility management system is based on a centralized approach where handovers are controlled entirely at the ASN-GW level, this MIHU can be able to send specific MIH Commands in order to coordinate all the procedures at the lower layers. In such situation, the handover management and the related decisions can be more efficient if the ASN-GW is able to receive and process the information provided by the Media Independent Information Service. In this case the exchange of MIHF messages with other network entities allows the MIHU to receive both lower layers and upper layers information that can have an impact on the selection of the target network during the handovers.

In the considered scenario, the MIH NSLP message exchange can be used in order to achieve handovers based on the Make Before Break model where the needed resources are configured before the actual disconnection from the serving Point of Attachment (PoA) and afterwards the resources on the old link are released. This approach allows the applications to receive coherent QoS guarantees in case of handovers between different networks.

As shown in Figure 8, the imminent disconnection of the MN from the current Wi-Fi Access Point is notified to the ASN-GW through a Remote MIH Link Going Down message, leading to the automatic resource re-configuration on the WiMAX link. The deletion of the existing SFs between the serving SS and BS is triggered by the following Remote MIH Link Down message that signals the occurred disconnection from

the Wi-Fi network.





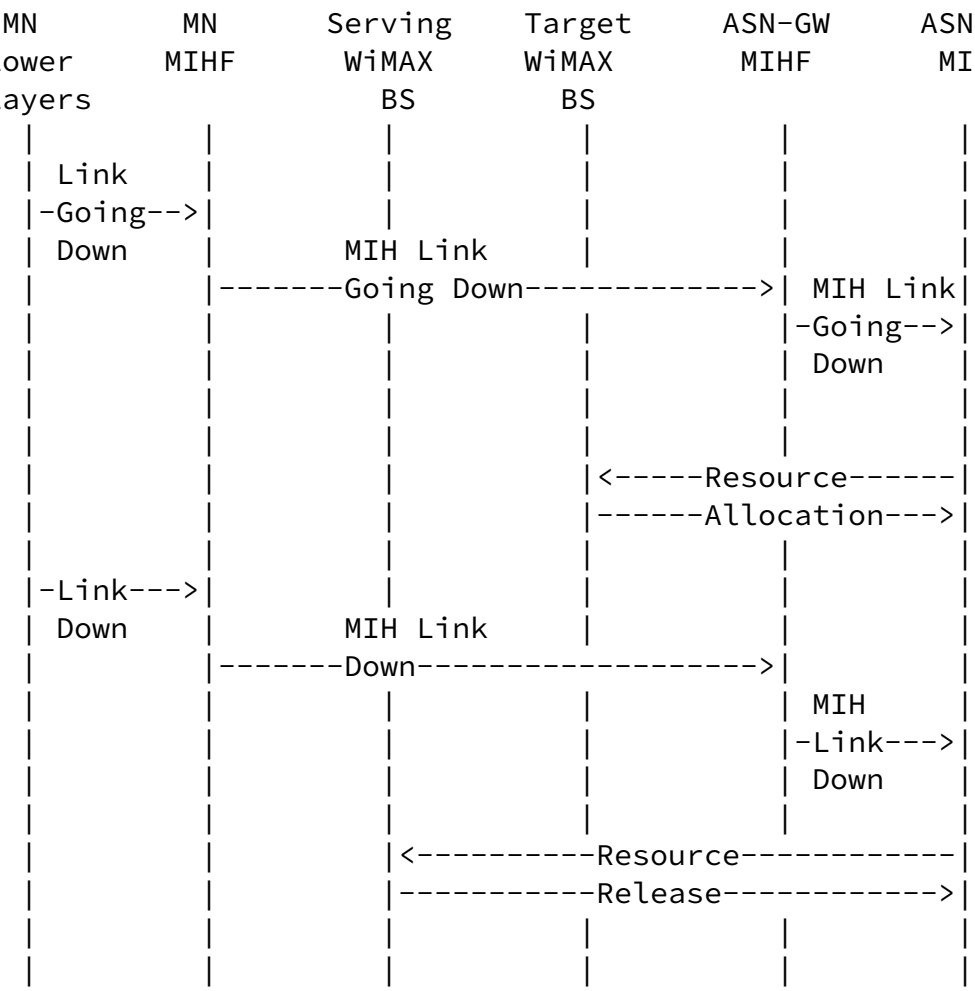


Figure 8: MIHF Signalling and resource control

As a further example (Figure 9), we can consider a mobility scenario in a single WiMAX network, where a Mobile Station IEEE 802.16e (MS) moves from the serving BS to the target BS. Following the intra-ASN scenario, both the BSs are located in the same access service network and are controlled by the same ASN-GW. We can assume that the management of the high level sessions and the associated QoS is handled at the ASN-GW level, as in the previous scenario.

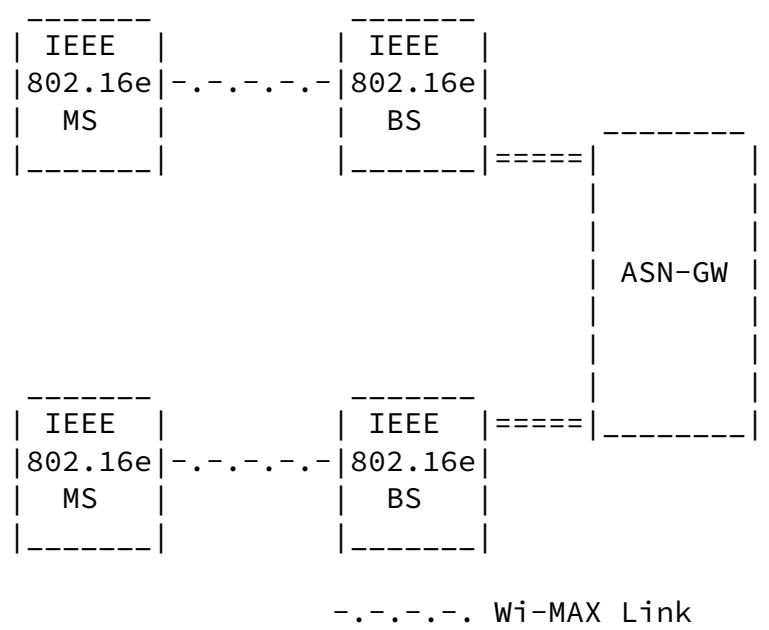


Figure 9: Example of Mobility Scenario in a WiMAX network - ASN-anchored

In this case, the handover management can be coordinated directly among the MS and the involved BSs, through the creation and the activation of suitable SFs on the target path and the deletion of the previous ones. Nevertheless the ASN-GW can obtain some notifications about the handovers and the occurred changes in lower layers through the MIH Event Service messages received through the MIH NSLP. These notifications allow the ASN-GW to correctly update the mobility "context" (SS and BS MAC address, SFs and classifiers, WiMAX security information, HA IP address, CoA, DHCP server, AAA server) for each existing session, so that it is able to manage possible resource re-configuration if required by the associated high level signalling.

In IEEE 802.16e networks, the MS can move between BSs under control of different ASNs and managed by different ASN-GWs (CSN-anchored mobility). In this case, the functionalities for the handover management SHOULD be split among different entities located not only in the ASN but also in the Connectivity Service Network and in the core network. The MIH NSLP protocol can be used in order to propagate the MIH Event and Command messages along the full path between the serving and the target BS, towards all the MIH peers located in ASNs and CSNs of different domains (Figure 10).





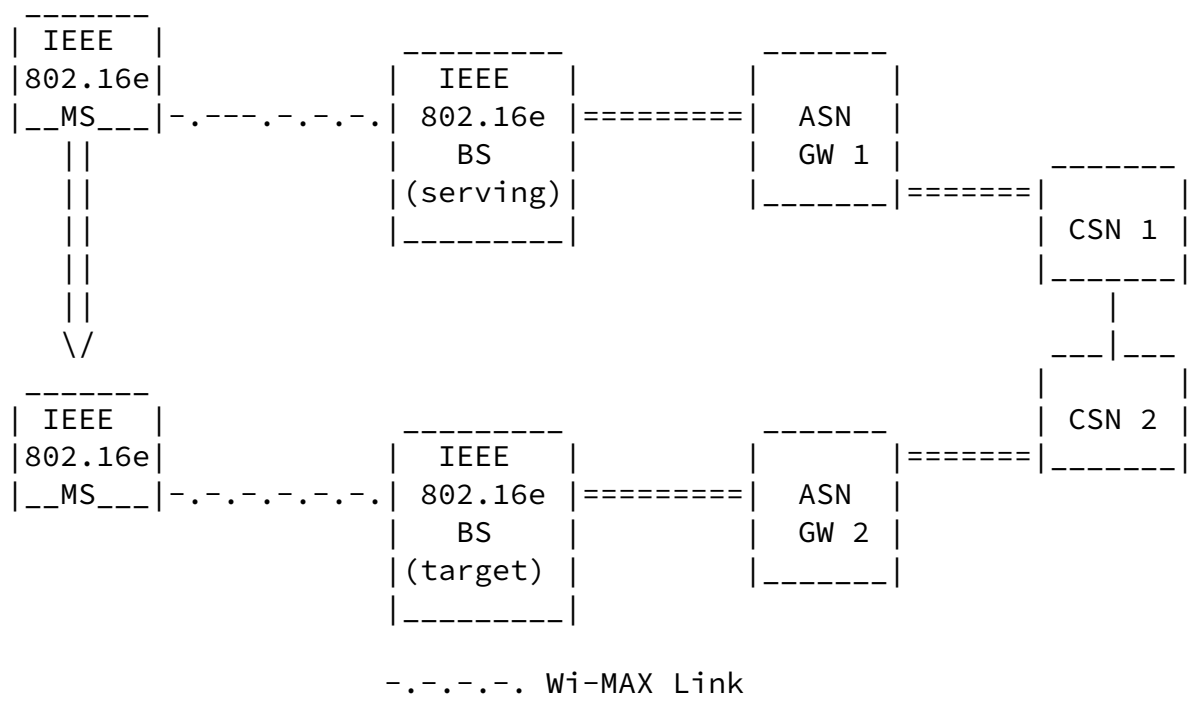


Figure 10: Example of Mobility Scenario in a WiMAX network - CSN-anchored

## 6. Security Considerations

The exchange of MIH NSLP messages MUST be secured against security threats, which have been identified in [7]. GIST is responsible for some of the security aspects of signalling [3]. Additionally, NSLPs MUST be in charge of threats concerning authorization, message protection, rate limitation, and prevention of denial of service attacks, as described in [4]. The use of these mechanisms in MIH NSLP is under study.

## 7. Open issues

This document specifies the MIH NSLP protocol, but leaves some issues unaddressed:

- The usage of MIH NSLP and GIST as the MIHF transport protocol adds additional security threats that are not addressed in the GIST and MIHF specifications. Some of these security issues are:
  - The interception of MIH Messages by middle MIHF entities;





  - The registration and deregistration process;
  - Unauthorized requests or unauthorized MIH Messages.
- The MIH NSLP registration procedure needs to include a refresh feature to maintain the MIH Registry Server updated. The MIH Registry Server should use soft states to store the mapping information;
- A default timer value SHOULD be proposed for the MIH NSLP message retransmit timer.
- The MIH NSLP messages MUST be specified. A MIH NSLP Message SHOULD consist of:
  - A common message header;
  - A group of type-length-value (TLV) objects.

- Several optimizations SHOULD be done to the MIH NSLP protocol. These optimizations SHOULD minimize the number of signalling messages and improve the MIH NSLP performance. An example of an optimization is the usage of a cache feature for the MIHF ID and IP Address mapping in the source and middle MIH NSLP.

These open issues will be addressed in future versions of this document.

## 8. Acknowledgments

The authors would like to thank all the partners of the IST FP6 Integrated Project WEIRD which were involved in the development of the mobility architecture of the project, especially, Eugen Borcoci, Massimiliano Taglieri and Bruno Sousa.

## 9. Normative References

[1] Melia, T., Bajko, G., Das, S., Golmie, N., Xia, Z., and J. Zuniga, "Mobility Services Framework Design", draft-ietf-mipshop-mstp-solution-01 (work in progress), February 2008.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[3] Hancock, R., Karagiannis, G., Loughney, J., and S. Van den





Bosch, "Next Steps in Signaling (NSIS): Framework", RFC 4080, June 2005.

[4] Schulzrinne, H. and R. Hancock, "GIST: General Internet Signalling Transport", draft-ietf-nsis-ntlp-15 (work in progress), February 2008.

[5] Manner, J., Karagiannis, G., and A. McDonald, "NSLP for Quality-of-Service Signaling", draft-ietf-nsis-qos-nslp-16 (work in progress), February 2008.

[6] "IEEE Draft Standard for Local and Metropolitan Area Networks:

Media Independent Handover Services", IEEE 802.21 Working Group, February 2007.

[7] Tschofenig, H. and D. Kroeselberg, "Security Threats for Next Steps in Signaling (NSIS)", RFC 4081, June 2005.

## Authors' Addresses

Luis Cordeiro
University of Coimbra
Polo II - Pinhal de Marrocos
Coimbra 3030-290
Portugal

Email: cordeiro@dei.uc.pt

Marilia Curado
University of Coimbra
Polo II - Pinhal de Marrocos
Coimbra 3030-290
Portugal

Email: marilia@dei.uc.pt

Pedro Neves
Portugal Telecom Inovacao, S.A.
Rua Eng. Jose Ferreira Pinto Basto
Aveiro 3810-106
Portugal

Email: est-p-neves@ptinovacao.pt





Susana Sargento
University of Aveiro
Campus Universitario de Santiago
Aveiro 3810-193
Portugal

Email: ssargento@det.ua.pt

Giada Landi
Consorzio Pisa Ricerche
Via Turati, 43-45
Pisa  56125
Italy

Email: g.landi@cpr.it

Xiaoming Fu
University of Goettingen
Lotzestrasse 16-18
Goettingen  37083
Germany

Email: fu@cs.uni-goettingen.de

## Full Copyright Statement



## Intellectual Property



## Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).