Next Steps in Signaling (nsis)   T. Sanda (Ed.)
Internet-Draft   Panasonic
Intended status: Informational   X. Fu
Expires: January 27, 2011   University of Goettingen
                                                             S. Jeong
                                                                 HUFS
                                                            J. Manner
                                                                  TKK
                                                        H. Tschofenig
                                               Nokia Siemens Networks
                                                        July 26, 2010

NSIS Protocols operation in Mobile Environments
draft-ietf-nsis-applicability-mobility-signaling-20.txt

Abstract

   Mobility of an IP-based node affects routing paths, and as a result,
   can have a significant effect on the protocol operation and state
   management. This document discusses the effects mobility can cause
   to the Next Steps in Signaling (NSIS) protocol suite, and shows how
   the NSIS protocols operation can work in different scenarios, with
   mobility management protocols.

Status of this Memo

Copyright Notice

Table of Contents

[1](#). **Introduction**

   Mobility of IP-based nodes incurs route changes, usually at the edge
   of the network. Since IP addresses are usually part of flow
   identifiers, the change of IP addresses implies the change of flow
   identifiers (i.e., the General Internet Signalling Transport (GIST)
   message routing information or Message Routing Information (MRI)
   [draft-ietf-nsis-ntlp]). Local mobility usually does not cause the
   change of the global IP addresses, but affects the routing paths
   within the local access network

   The NSIS protocol suite consists of two layers: NSIS Transport Layer
   Protocol (NTLP) and the NSIS Signaling Layer Protocol (NSLP). The
   General Internet Signaling Transport (GIST) [draft-ietf-nsis-ntlp]
   implements the NTLP, which is a signaling application independent
   protocol and transports service-related information between
   neighboring GIST nodes. Each specific service has its own NSLP
   protocol; currently there are two specified NSLP protocols, the QoS
   NSLP [draft-ietf-nsis-qos-nslp], and the NAT/Firewall NSLP
   [draft-ietf-nsis-nslp-natfw]

   The goals of this document are to present the effects of mobility on
   the NTLP/NSLPs and to provide guides on how such NSIS protocols work
   in basic mobility scenarios, including support for Mobile IPv4 and
   Mobile IPv6 scenarios. We also show how these protocols fulfil the
   requirements regarding mobility set forth in [RFC3726]. In general,
   the NSIS protocols work well in mobile environments. The Session ID
   (SID) used in NSIS signaling enables the separation of the signaling
   state and the IP addresses of the communicating hosts. This makes it
   possible to directly update a signaling state in the network due to
   mobility without being forced to first remove the old state and then
   re-establish a new one. This is the fundamental reason why NSIS
   signaling works well in mobile environments. As the additional
   information, mobility specific enhanced operations, e.g. operations
   with crossover node (CRN) are also introduced.

   This document focuses on basic mobility scenarios. Key management
   related to handovers, multihoming and interactions between NSIS and
   other mobility management protocols than Mobile IP are out of scope
   of this document. Also, practical implementations typically need
   various APIs across components within a node. API issues, e.g., APIs
   from GIST to the various mobility and routing schemes, are also out
   of scope of this work. The generic GIST API towards NSLP is flexible
   enough to fulfill most mobility-related needs of the NSLP layer.

2. Requirements Notation and Terminology

   The terminology in this documnet is based on [draft-ietf-nsis-ntlp]
   and [RFC3753]. In addition, the following terms are used. Note that
   in this document, a generic route change caused by regular IP routing
   is referred to as a 'route change', and the route change caused by
   mobility is referred to as 'mobility'.

   (1) Downstream

   The direction from a data sender towards the data receiver.

   (2) Upstream

   The direction from a data receiver towards the data sender.

   (3) Crossover Node (CRN)

   A Crossover Node is a node that for a given function is a merging
   point of two or more paths belonging to flows of the same session
   along which states are installed.

   In the mobility scenarios, there are two different types of merging
   points in the network according to the direction of signaling flows
   followed by data flows, where we assume that the Mobile Node (MN) is
   the data sender.

      Upstream CRN (UCRN): the node closest to the data sender from
      which the state information in the direction from data receiver to
      data sender begins to diverge after a handover.

      Downstream CRN (DCRN): the node closest to the data sender from
      which the state information in the direction from the data sender
      to the data receiver begins to converge after a handover.

   In general, the DCRN and the UCRN may be different due to the
   asymmetric characteristics of routing although the data receiver is
   the same.

   (4) State Update

   State Update is the procedure for the re-establishment of NSIS state
   on the new path, the teardown of NSIS state on the old path, and the
   update of NSIS state on the common path due to the mobility. The
   State Update procedure is used to address mobility for the affected
   flows.

Upstream State Update: State Update for the upstream signaling
flow.

Downstream State Update: State Update for the downstream signaling
flow.

[3](). Challenges with Mobility

   This section identifies problems caused by mobility, which affect the
   operations of NSIS protocol suite.

   1. Change of route and possibly change of the MN's IP address

   Topology changes or network reconfiguration might lead to path
   changes for data packets sent to or from the MN and can cause an IP
   address change of the MN. Traditional route changes usually do not
   cause address changes of the flow endpoints. When an IP address
   changes due to mobility, information within the path-coupled MRI is
   affected (the source or destination address). Consequently, this
   concerns GIST as well as NSLPs, e.g., the packet classifier in QoS
   NSLP or some rules carried in NAT/FW NSLP. So already installed
   firewall rules, NAT bindings, and QoS reservations may become
   invalid, because the installed states refer to a non-existent flow.
   If the affected nodes are also on the new path, this information must
   be updated accordingly.

   2. Double state problem

   After a handover, packets may end up getting delivered through a new
   path. Since the state on the old path still remains as it was after
   re-establishing the state along the new path, we have two separate
   states for the same signaling session. Although the state on the old
   path will be deleted automatically based on the soft state timeout,
   the state timer value may be quite long (e.g., 90s as a default
   value). With the QoS NSLP, this problem might result in the waste of
   resources and lead to failure of admitting new reservations (due to
   lack of resources). With the NAT/FW NSLP, it is still possible to
   re-use this installed state although an MN roams to a new location;
   this means that another host can send data through a firewall without
   any prior NAT/FW NSLP signaling because the previous state did not
   yet expire.

   3. End-to-end signaling and frequency of route changes

   The change of route and IP addresses in mobile environments is
   typically much faster and more frequent than traditional route
   changes caused by node or link failure. This may result in a need to
   speed up the update procedure of NSLP states.

   4. Identification of the crossover node

   When a handover at the edge of a network has happened, in the typical
   case, only some parts of the end-to-end path used by the data packets
   changes. In this situation, the cross-over node (CRN) plays a

central role in managing the establishment of the new signaling
application state, and removing any useless state, while localizing
the signaling only to the affect part of the network.

5. Upstream State Update vs. Downstream State Update

Due to the asymmetric nature of Internet routing, the upstream and
downstream paths are likely not to be exactly the same. Therefore,
state update needs to be handled independently for upstream and
downstream paths.

6. Upstream signaling

If the MN is receiver and moves to a new point of attachment, it is
difficult to signal upstream towards the Correspondent Node (CN).
New signaling states have to be established along the new path, but
for a path-coupled Message Routing Method (MRM) this has to be
initiated in downstream direction. So NTLP signaling state in
upstream direction cannot be initiated by the MN, i.e., GIST cannot
easily send a Query in upstream direction (there is an upstream
Q-mode, but this is only applicable in a limited scope). The use of
additional other protocols such as application level signaling (e.g,
SIP) or mobility management signaling (e.g., Mobile IP) may help to
trigger NSLP and NTLP signaling from the CN side in downstream
direction though.

7. Authorization Issues

The procedure of State Update may be initiated by the MN, the CN, or
even nodes within the network (e.g., crossover node, Mobility Anchor
Point (MAP) in Hierarchical Mobile IP (HMIP)). This State Update on
behalf of the MN raises authorization issues about the entity that is
allowed to make these state modifications.

8. Dead peer and invalid NR problem

When the MN is on the path of a signaling exchange, after handover
the old Access Router (AR) can not forward NSLP messages any further
to the MN. In this case, the old AR's mobility or routing protocol,
or even the NSLP may trigger an error message to indicate that the
last node fails or is truncated. This error message is forwarded and
may mistakenly cause the removal of the state on the existing common
path, if the state is not updated before the error message is
propagated through the signaling peers. This is called the 'invalid
NSIS Receiver (NR) problem'.

9. IP-in-IP Encapsulation

Mobility protocols may use IP-in-IP encapsulation on the segment of
the end-to-end path for routing traffic from the CN to the MN, and
vice versa. Encapsulation harms any attempt to identify and filter
data traffic belonging to, for example, a QoS reservation. Moreover,
encapsulation of data traffic may lead to changes in the routing
paths since the source and the destination IP addresses of the inner
header differ from those of the outer header. Mobile IP uses
tunneling mechanisms to forward data packets among end hosts.
Traversing over the tunnel, NSIS signaling messages are transparent
on the tunneling path due to the change of flow's addresses. In case
of interworking with Mobile IP-tunneling, CRNs can be discovered on
the tunneling path. It enables NSIS protocols to perform State
Update procedure over the IP-tunnel. In this case, GIST needs to
cope with the change of Message Routing Information (MRI) for the CRN
discovery on the tunnel. Also, NSLP signaling needs to determine
when to remove the tunneling segment on the signaling path and/or how
to tear down the old state via interworking with the IP-tunneling
operation. Furthermore, tunneling adds additional IP header as
overhead that must be taken into account by QoS NSLP for example,
when resources must be reserved accordingly. So an NSLP must usually
be aware whether tunneling or route optimization is actually used for
a flow [draft-ietf-nsis-tunnel].

4. Basic Operations for Mobility Support

   This section presents the basic operations of the NSIS protocol suite
   after mobility related route changes. Detailed discussion of the
   operation of Mobile IP with respect to NSIS protocols are discussed
   in the subsequent section.

4.1. General functionality

   The NSIS protocol suite decouples state and flow identification. A
   state is stored and referred by the Session ID (SID). Flows
   associated with a given NSLP state are defined by the Message Routing
   Information (MRI). GIST notices when a routing path associated with
   a SID changes, and provides a notification to the NSLP. It is then
   up to the NSLP to update the state information in the network. Thus,
   the effect is an update to the states, not a full new request. This
   decoupling effectively solves also a typical problem with certain
   signaling protocols, where protocol state is identified by flow
   endpoints, and when flow endpoint addresses change, the whole session
   state becomes invalid.

   A further benefit of the decoupling is that if the MRI, i.e., the IP
   addresses associated with the data flow, remain the same after
   movement, the NSIS signaling will repair only the affected path of
   the end-to-end session. Thus, updating the session information in
   the network will be localized, and no end-to-end signaling will be
   needed. If the MRI changes, end-to-end signaling usually can not be
   avoided since new information for proper data flow identification
   must be provided all the way between the data sender and receiver,
   e.g., in order to update filters, QoS profiles, or other flow related
   session data.

   GIST provides NSLPs with an identifier of the next signaling peer,
   the SII Handle. When this SII Handle changes, the NSLP knows a
   routing change has happened. Yet, the NSLP can also figure out
   whether it is also the crossover node for the session. Thus, CRN
   discovery is always done at the NSLP layer because only NSLPs have a
   notion of end-to-end signaling.

   When a path changes, the session information on the old path needs to
   be removed. Normally, the information is released when the session
   timer is expired after a routing change. But the NSLP running on the
   end-host or the CRN, depending on the direction of the session, may
   use the SII Handle (provided by GIST) to explicitly remove states on
   the old path; new session information is simultaneously set up on the
   new path. Both current NSLPs use sequence numbers to identify the
   order of messages, and this information can be used by the protocols
   to recover from a routing change.

Since NSIS operates on a hop-by-hop basis, any peer can perform state
updates. This is possible because a chain-of-trust is expected
between NSIS nodes. If this weren't the case, e.g., true resource
reservations would not be possible; one misbehaving or compromised
node would effectively break everything. Thus, currently the NSIS
protocols do not limit the roles of each NSIS signaling peer on a
path, and any node can make updates. Yet, some updates are reflected
back to the signaling end points, and they can decide whether the
signaling actually succeeded, or not.

If the signaling packets are encapsulated in a tunnel, it is
necessary to perform a separate signaling exchange for the tunneled
region. Furthermore, a binding is needed to tie the end-to-end and
tunneled session together.

Furthermore, in some cases the NSLP must be aware whether tunneling
is used, since additional tunneling overhead must be taken into
account, e.g., for resource reservations etc.

4.2. QoS NSLP

Figure 1 illustrates an example of QoS NSLP signaling in a Mobile
IPv6 route optimization case, for a data flow from the MN to the CN,
where sender-initiated reservation is used. Once a handover event is
detected in the MN, the MN needs to acquire the new care-of-address
and update the path coupled MRI accordingly. Then the MN issues a
QoS NSLP RESERVE message towards the CN, that carries the unique
session ID and other identification information for the session, as
well as the reservation requirements (step(1)~(4) in Figure 1). Upon
receipt of the RESERVE message, the QoS NSLP nodes (which will be
discovered by the underlying NTLP) establish the corresponding QoS
NSLP state, and forward the message towards the CN. When there is
already an existing NSLP state with the same session ID, the state
will be updated. If all the QoS NSLP nodes along the path support
the required QoS, the CN in turn responds with a RESPONSE message, to
confirm the reservation (step(5)~(6) in Figure 1).

In a bi-directional tunneling case, the only difference is that the
RESERVE message should be sent to the HA instead of the CN, and the
node which responds with a RESPONSE should be the HA instead of the
CN too. More details are discussed in Section 5

Therefore, for the basic operation there is no fundamental difference
among different operation modes of Mobile IP, and the main issue of
mobility support in NSIS is to trigger NSLP signaling appropriately
when a handover event is detected, and the destination of the NSLP
signaling shall follow the Mobile IP data path as being path-coupled
signaling.

In this process, the obsoleted state in the old path is not
explicitly released because the state can be released by timer
expiration. To speed up the process, it may be possible to localize
the signaling. When the RESERVE message reaches a node, depicted as
CRN in this document (step(2) in Figure 1), where a state is
determined for the first time to reflect the same session, the node
may issue a NOTIFY message towards the MN's old care-of-address (CoA)
(step(9) in Figure 1). The QNE adjacent to MN's old position stops
the NOTIFY message (step(10) in Figure 1), and sends RESERVE message
(with Teardown bit set) towards the CN, to release the obsoleted
state (step(11) in Figure 1). This RESERVE with tear message is
stopped by the CRN (step(12) in Figure 1). The Reservation Sequence
Number (RSN) used in the messages is used to distinguish the order of
the signaling. More details are described in Section 4.4

```
    MN    QNE1 MN       QNE2       QNE3      QNE4      CN
  (CoA1)  | (CoA2)       |        (CRN)       |        |
    |     |    |         |          |         |        |
    |     |    |RESERVE  |          |         |        |
    |     |    |-------->|          |         |        |
    |     |    | (1)     |RESERVE   |         |        |
    |     |    |         |--------->|         |        |
    |     |    |         | (2)      |RESERVE  |        |
    |     |    |         |          |-------->|        |
    |     |    |         |          | (3)     |RESERVE |
    |     |    |         |          |         |------->|
    |     |    |         |    NOTIFY|         | (4)    |
    |     |    |         |<---------|         |        |
    |     |    | NOTIFY|     (9)    |         |        |
    |     |<------------|          |         |        |
    |     |    | (10)    |          |         |        |
    |     |RESERVE(T)    |          |         |        |
    |     |------------>|          |         |        |
    |     |    | (11)    |RESERVE(T)|         |        |
    |     |    |         |--------->|         |        |
    |     |    |         | (12)     |         |RESPONSE|
    |     |    |         |          |         |<-------|
    |     |    |         |          |RESPONSE|  (5)    |
    |     |    |         |  RESPONSE|<-------|         |
    |     |    |RESPONSE|<---------|  (6)    |         |
    |     |    |<------ |    (7)    |         |        |
    |     |    | (8)     |          |         |        |
    |     |    |         |          |         |        |
```
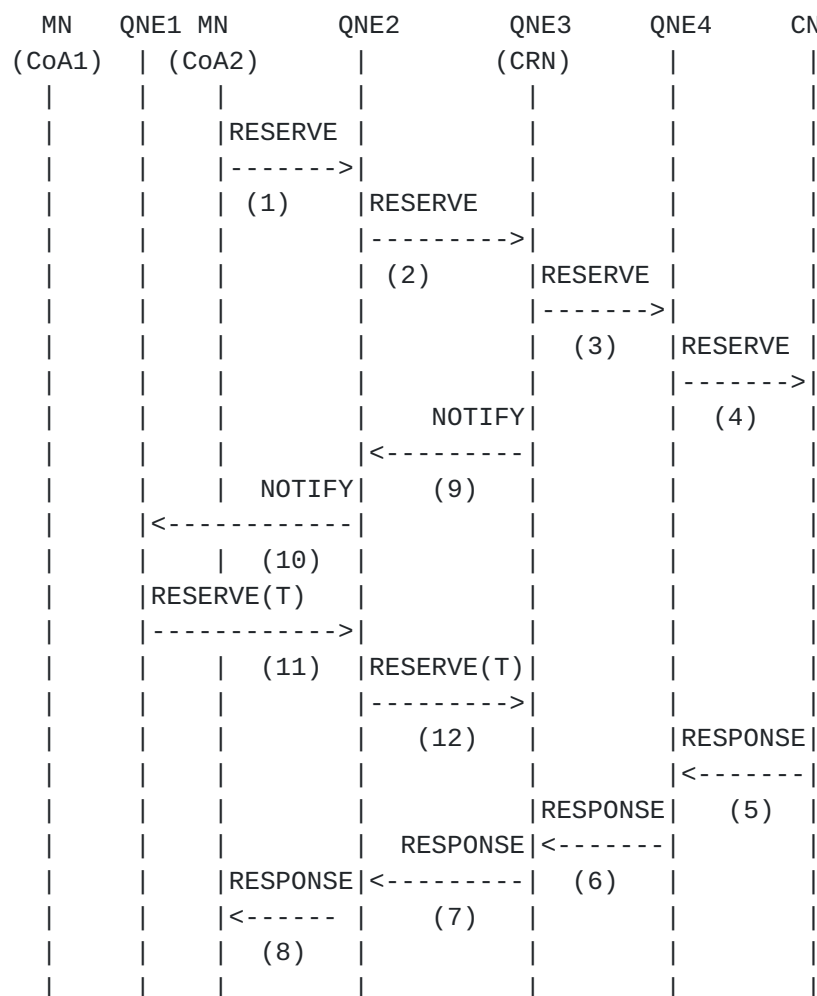
                   Figure 1: Basic operation example

Further cases to consider are:

   * receiver-initiated reservation if MN is sender

   * sender-initiated reservation if MN is receiver

   * receiver-initiated reservation if MN is receiver

In the first case, the MN can easily initiate a new QUERY along the
new path after movement, thereby installing signaling state and
eventually eliciting a new RESERVE from the CN in upstream direction.
Similarly, the second and third cases require the CN to initiate a
RESERVE or QUERY message respectively. The difficulty in both cases
is, however, to let the CN know that the MN has moved. Because the
MN is the receiver it cannot simply use an NSLP message to do so,
because upstream signaling is not possible in this case (cf. Sec. 3,
Upstream Signaling).

4.3. NATFW NSLP

Figure 2 illustrates an example of NATFW NSLP signaling in a Mobile
IPv6 route optimization case, for a data flow from the MN to the CN.
The difference to the QoS NSLP is that for the NATFW NSLP only the
NSIS initiator (NI) can update the signalling session, in any case.
Once a handover event is detected in the MN, the MN must get to know
the new care-of-address and update the path coupled MRI accordingly.
Then the MN issues a NATFW NSLP CREATE message towards the CN, that
carries the unique session ID and other identification information
for the session (step(1)~(4) in Figure 2). Upon receipt of the
CREATE message, the NATFW NSLP nodes (which will be discovered by the
underlying NTLP) establish the corresponding NATFW NSLP state, and
forward the message towards the CN. When there is already an
existing NSLP state with the same session ID, the state will be
updated. If all the NATFW NSLP nodes along the path accept the
required NAT/firewall configuration, the CN in turn responds with a
RESPONSE message, to confirm the configuration (step(5)~(8) in
Figure 2).

In a bi-directional tunneling case, the only difference is that the
CREATE message should be sent to the HA instead of the CN, and the
node which responds with a RESPONSE should be the HA instead of the
CN too.

Therefore, for the basic operation there is no fundamental difference
among different operation modes of Mobile IP, and the main issue of
mobility support in NSIS is to trigger NSLP signaling appropriately
when a handover event is detected, and the destination of the NSLP
signaling shall follow the Mobile IP data path as being path-coupled

signaling.

In this process, the obsoleted state in the old path is not
explicitly released because the state can be released by timer
expiration. To speed up the process, when the CREATE message reaches
a node, depicted as CRN in this document (step(2) in Figure 2), where
a state is determined for the first time to reflect the same session,
the node may issue a NOTIFY message towards the MN's old CoA
(step(9)~(10) in Figure 2) and when the NI notices this, it sends a
CREATE message towards the CN to release the obsoleted state
(step(11)~(12)) in Figure 2).

```
      MN     NI MN            NF1         NF2         NF3      CN
    (CoA1)  | (CoA2)          |          (CRN)       |         |
       |     |    |           |            |          |         |
       |     |    |           |            |          |         |
       |     |    |CREATE     |            |          |         |
       |     |    |------->|            |          |         |
       |     |    | (1)    |CREATE      |          |         |
       |     |    |        |--------->|            |          |
       |     |    |        | (2)      |CREATE    |         |
       |     |    |        |          |------->|            |
       |     |    |        |          | (3)    |CREATE   |
       |     |    |        |          |        |------->|
       |     |    |        |   NOTIFY|        |  (4)   |
       |     |    |        |<--------|        |         |
       |     |    | NOTIFY|   (9)   |        |         |
       |     |<------------|        |        |         |
       |     |    | (10)  |        |        |         |
       |     |CREATE(CoA2) |        |        |         |
       |     |------------>|        |        |         |
       |     |    | (11)  |CREATE(CoA2)      |         |
       |     |    |        |--------->|        |         |
       |     |    |        |  (12)   |        |RESPONSE|
       |     |    |        |          |        |<-------|
       |     |    |        |          |RESPONSE|  (5)   |
       |     |    |        | RESPONSE|<-------|         |
       |     |    |RESPONSE|<---------|  (6)   |         |
       |     |    |<------ |   (7)   |        |         |
       |     |    | (8)    |         |        |         |
       |     |    |        |         |        |         |
       |     |    |        |         |        |         |
```

                  Figure 2: NATFW NSLP operation example
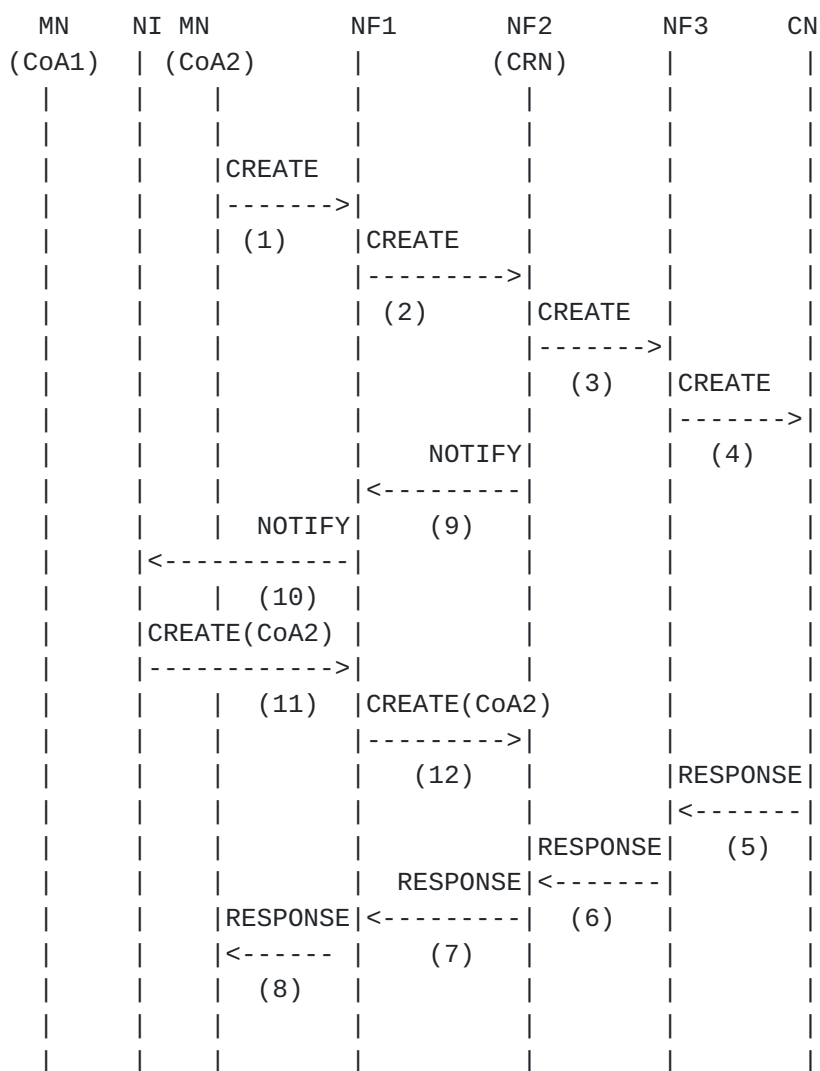
4.4. Localized signaling in mobile scenarios

This section describes detailed CRN operations. As described in previous sections, CRN operations are informational.

As shown in Figure 3, mobility generally causes signaling path to either converge or diverge depending on the direction of each signaling flow.
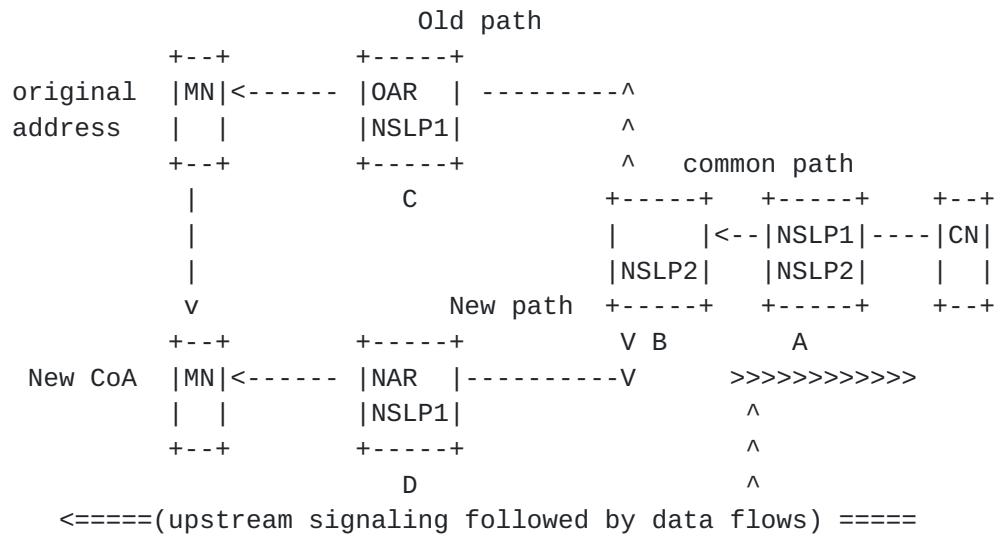
```
                              Old path
            +--+           +-----+
   original |MN|<------ |OAR  | ---------^
   address  |  |        |NSLP1|          ^
            +--+        +-----+          ^   common path
             |              C          +-----+   +-----+     +--+
             |                         |     |<--|NSLP1|----|CN|
             |                         |NSLP2|   |NSLP2|    |  |
             v              New path   +-----+   +-----+    +--+
            +--+        +-----+          V B         A
   New CoA  |MN|<------ |NAR  |----------V      >>>>>>>>>>>>
            |  |        |NSLP1|                      ^
            +--+        +-----+                      ^
                           D                         ^
       <=====(upstream signaling followed by data flows) =====

   (a) The topology for upstream NSIS signaling flow due to
       mobility (in case the MN is a data sender)


                              Old path
            +--+           +-----+
   original |MN|------> |OAR  | ----------V
            |  |        |NSLP1|
   address  +--+        +-----+          V   common path
             |              K          +-----+   +-----+     +--+
             |                         |     |---|NSLP1|--->|CN|
             |                         |NSLP2|   |NSLP2|    |  |
             v              New path   +-----+   +-----+    +--+
            +--+        +-----+          ^ M         N
   New CoA  |MN|------> |NAR  |-----------^      >>>>>>>>>>>>
            |  |        |NSLP1|                      ^
            +--+        +-----+                      ^
                           L                         ^
       ====(downstream signaling followed by data flows) ======>

   (b) The topology for downstream NSIS signaling flow due to
       mobility (in case the MN is a data sender)



       Figure 3: The topology for NSIS signaling caused by mobility
```
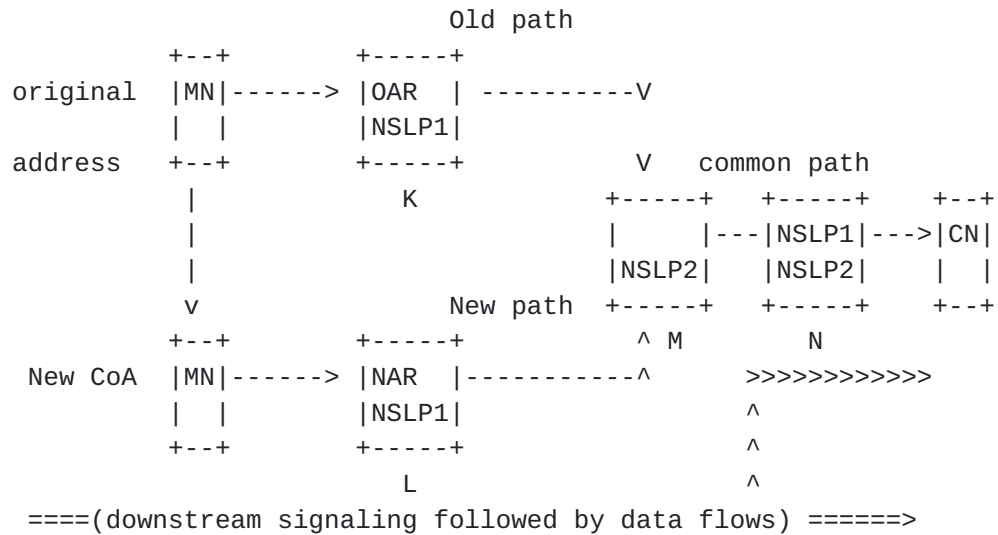
   These topological changes due to mobility cause the NSIS state
   established in the old path to be useless. Such state may be removed
   as soon as possible. In addition, NSIS state needs to be established
   along the new path and be updated along the common path. The re-
   establishment of NSIS signaling may be localized when route changes
   (including mobility) occur to minimize the impact on the service and
   to avoid unnecessary signaling overhead. This localized signaling

procedure is referred to as State Update (refer to the terminology
section). In mobile environments, for example, the NSLP/ NTLP needs
to limit the scope of signaling information only to the affected
portion of the signaling path because the signaling path in the
wireless access network usually changes only partially.

4.4.1. CRN Discovery

The CRN is discovered at the NSLP layer. In case of QoS NSLP, when a
RESERVE message with an existing SESSION_ID is received and its
Source Identification Information (SII) and MRI are changed, the QNE
knows its upstream or downstream peer has changed by the handover,
for sender-oriented and receiver-oriented reservations, respectively.
And realizes it is implicitly the CRN.

4.4.2. Localized State Update

In the downstream State Update, the MN initiates the RESERVE with a
new RSN for state setup toward a CN and also the implicit DCRN
discovery is performed by the procedure of signaling as described in
Section 4.4.1. The MRI from the DCRN to the CN (i.e., common path)
is updated by the RESERVE message. DCRN may also send NOTIFY with
"Route change (0x02)" to previous upstream peer. The NOTIFY is
forwarded hop-by-hop and reaches the edge QNE (i.e., QNE1 in
Figure 1). After the QNE is aware that the MN as QNI has disappeard
(how this is can be noticed is out of scope of NSIS, yet, e.g., GIST
will eventually know this through undelivered messages), the QNE
sends a tearing RESERVE towards downstream. When the tearing RESERVE
reaches the DCRN, it stops forwarding and drops it. Note that,
however, it is not necessary for GIST state to be explicitly removed
because of the inexpensiveness of the state maintenance at the GIST
layer [draft-ietf-nsis-ntlp]. Note that, the sender-initiated
approach leads to faster setup than the receiver-initiated approach
as in RSVP [RFC2205].

In the scenario of an upstream State Update, there are two possible
methods for state update. One is the CN (or a HA/ a Gateway Foreign
Agent (GFA)/ a MAP) sends the refreshing RESERVE message toward the
MN to perform State Update upon receiving trigger (e.g., Mobile IP
(MIP) binding update). UCRN is discovered implicitly by the CN-
initiated signaling along the common path as described in
Section 4.4.1. When the refreshing RESERVE reaches to the adjacent
QNE of UCRN, the QNE sends back a RESPONSE saying "full QoS
Specification (QSPEC) required". Then the UCRN sends the RESERVE
with full QSPEC towards the MN to set up a new reservation. The UCRN
may also send tearing RESERVE to previous downstream peer. The
tearing RESERVE is forwarded hop-by-hop and reaches to the edge QNE.
After the QNE is aware that the MN as QNI has disappeard, the QNE

drops the tearing peer. Another method is, if GIST hop is already
established on the new path (e.g. by QUERY from the CN, or the HA/
GFA/ MAP) when MN gets a hint from GIST that routing has changed, the
MN sends a NOTIFY towards upstream saying "Route Change" 0x02. When
the NOTIFY hits UCRN, the UCRN is aware that the NOTIFY is for a
known session comes from a new SII-Handle. Then the UCRN sends a
RESERVE with a new RSN and an RII towards the MN. By receiving the
RESERVE, the MN replies RESPONSE. The UCRN may also send tearing
RESERVE to previous downstream peer. The tearing RESERVE is
forwarded hop-by-hop and reaches to the edge QNE. After the QNE is
aware that the MN as QNI is disappeared, the QNE drops the tearing
peer.

The State Update on the common path to reflect the changed MRI brings
issues on the end-to-end signaling addressed in Section 3. Although
the State Update over the common path does not give rise to re-
processing of AAA and admission control, it may lead to the increased
signaling overhead and latency.

One of the goals of the State Update is to avoid the double
reservation on the common path as described in Section 3. The double
reservation problem on the common path can be solved by establishing
a signaling association using a unique SID and by updating packet
classifier/MRI. In this case, even though the flows on the common
path have different MRIs, it refers to the same NSLP state.

5. Interaction with Mobile IPv4/v6

   Mobility management solutions like Mobile IP try to hide mobility
   effects from applications by providing stable addresses and avoiding
   address changes. On the other hand, the MRI [draft-ietf-nsis-ntlp]
   contains flow addresses and will change if the CoA changes. This
   makes impact on some NSLPs such as QoS NSLP and NAT/FW NSLP.

   QoS NSLP must be mobility-aware because it needs to care about the
   resources on the actual current path, and sending a new RESERVE or
   QUERY for the new path. Applications on top of Mobile IP communicate
   along logical flows that use home addresses, whereas QoS NSLP has to
   be aware of the actual flow path, e.g., whether the flow is currently
   tunneled or route-optimized etc. QoS NSLP may have to obtain current
   link properties, especially additional overhead due to mobility
   header extensions that must be taken into account in QSPEC (e.g., the
   m parameter in the traffic model (TMOD)). Therefore, NSLPs must
   interact with mobility management implementations in order to request
   information about the current flow address (CoAs), source addresses,
   tunneling, or, overhead. Furthermore, an implementation must select
   proper interface addresses in the natural language interface (NLI) in
   order to ensure that a corresponding Messaging Association is
   established along the same path as the flow in the MRI. Moreover,
   the home agent needs to perform additional actions (e.g.,
   reservations) for the tunnel. If the home agent lacks support of a
   mobility-aware QoS NSLP a missing tunnel reservation is usually the
   result. Practical problems may occur in situations where a home
   agent needs to send a GIST query (with S-flag=1) towards the MN's
   Home Address and the query is not tunneled due to route optimization
   between HA and MN: the query will be wrongly intercepted by QNEs
   within the tunnel.

   NAT/FW box needs to be configured before MIP signaling, hence NAT/FW
   signaling will have to be performed, to allow Return Routability Test
   (RRT) and Binding Update (BU)/Binding Acknowledgement (BA) messages
   to traverse the NAT/FWs in the path. After RRT and BU/BA are
   completed, another NAT/FW signaling needs to be performed for passing
   the data. Optimized version can include a combined NAT/FW message to
   cover both RRT and BU/BA messages pattern. However this may require
   NAT/FW NSLP to do a slight update to support carrying multiple NAT/FW
   rules in one signaling round trip.

   This section analyzes NSIS operation with tunneled route case
   especially for QoS NSLP.

5.1. Interaction with Mobile IPv4

   In Mobile IPv4 [RFC3344], the data flows are forwarded based on
   triangular routing, and an MN retains a new CoA from the Foreign
   Agent (FA) (or an external method such as DHCP) in the visited access
   network. When the MN acts as a data sender, the data and signaling
   flows sent from the MN are directly transferred to the CN not
   necessarily through the HA or indirectly through the HA using the
   reverse tunneling. On the other hand, when the MN act as a data
   receiver, the data and signaling flows sent from the CN are routed
   through the IP tunneling between the HA and the FA (or the HA and the
   MN in case of the Co-located CoA). With this approach, routing is
   dependent on the HA, and therefore the NSIS protocols interact with
   the IP tunneling procedure of Mobile IP for signaling.

   The Figure 4 (a) to (e) show the NSIS signaling flows depending on
   the direction of the data flows and the routing methods.
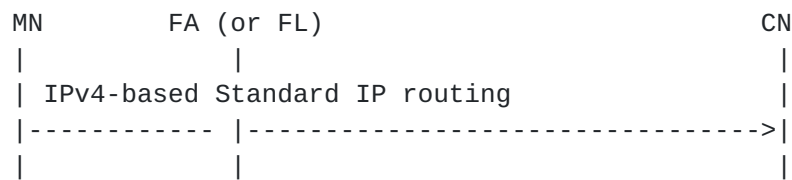
```
         MN        FA (or FL)                            CN
         |          |                                     |
         | IPv4-based Standard IP routing                 |
         |----------- |----------------------------------->|
         |           |                                     |

         (a) MIPv4: MN-->CN, no reverse tunnel

         MN                 FA                HA            CN
         | IPv4 (normal)   |                 |             |
         |--------------->| IPv4(tunnel)     |             |
         |                 |--------------->| IPv4 (normal)|
         |                 |                 |------------->|

         (b) MIPv4: MN-->CN, the reverse tunnel with FA CoA

         MN                 (FL)              HA            CN
         |                  |                 |             |
         |         IPv4(tunnel)               |             |
         |------------------------------->|IPv4 (normal)   |
         |                  |                 |------------->|

         (c) MIPv4: MN-->CN, the reverse tunnel with Co-located CoA

         CN                 HA                FA            MN
         |IPv4 (normal)    |                 |             |
         |-------------->|                 |             |
         |                 | MIPv4 (tunnel)  |             |
         |                 |--------------->| IPv4 (normal)|
         |                 |                 |------------->|

         (d) MIPv4: CN-->MN, Foreign agent Care-of-address

         CN                 HA                (FL)          MN
         |IPv4(normal )    |                 |             |
         |-------------->|                 |             |
         |                 | MIPv4 (tunnel)  |             |
         |                 |------------------------------->|
         |                 |                 |             |

         (e) MIPv4: CN-->MN with Co-located Care-of-address
```
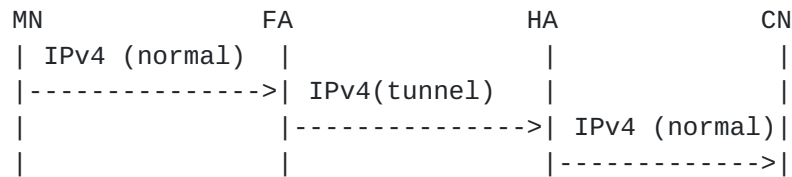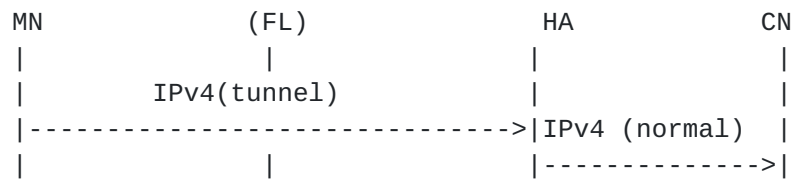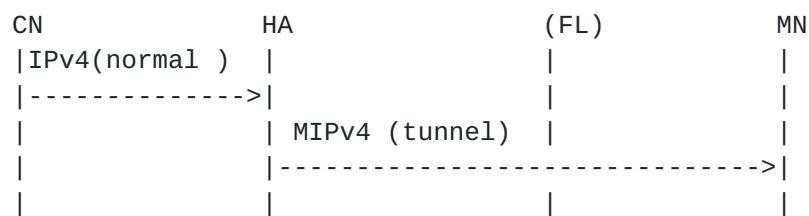
   Figure 4: NSIS signaling flows under different Mobile IPv4 scenarios

   When an MN (as a signaling sender) arrives at a new FA and the
   corresponding binding process is completed (Figure 4 (a), (b) and

(c)), the MN performs the CRN discovery (DCRN) and the State Update
toward the CN (as described in Section 4) to establish the NSIS state
along the new path between the MN and the CN. In case reverse tunnel
is not used (Figure 4 (a)), a new NSIS state is established on direct
path from the MN to the CN. If the reverse tunnel and FA CoA are
used (Figure 4 (b)), a new NSIS state is established along a
tunneling path from the FA to the HA separately from end-to-end path.
CRN discovery and State Update in tunneling path is also separately
performed if necessary. If the reverse tunnel and co-located CoA are
used (Figure 4 (c)) the NSIS signaling for the DCRN discovery and the
State Update is the same as the case of using FA CoA above except for
the use of the reverse tunneling path from the MN to the HA. That
is, in this case, one of tunnel end points is the MN, not the FA.

When an MN (as a signaling receiver) arrives at a new FA and the
corresponding binding process is completed (Figure 4 (d) and (e)),
the MN sends NOFITY message to the signaling sender, i.e., the CN.
In case FA CoA is used (Figure 4 (d)), the CN initiates a NSIS
signaling to update an existing state between the CN and the HA, and
afterwards the NSIS signaling messages are forwarded to the FA and
reaches to the MN. A new NSIS state is established along the
tunneling path from the HA to the FA separately from end-to-end path.
During this operation, a UCRN is discovered on the tunneling path,
and a new MRI for the State Update on the tunnel may need to be
created. CRN discovery and State Update in tunneling path is also
separately performed if necessary. In case collocated CoA is used
(Figure 4 (d)) the NSIS signaling for the UCRN discovery and the
State Update is also the same as the case of using FA CoA above
except for the end point of tunneling path from the HA to the MN.

Note that Mobile IPv4 optionally supports route optimization. In the
case route optimization is supported, the signaling operation will be
the same as Mobile IPv6 route optimization.

5.2. Interaction with Mobile IPv6

Unlike Mobile IPv4, with Mobile IPv6 [RFC3775], the FA is not
required on the data path. If an MN moves to visited network, a CoA
at the network is allocated like co-located CoA in Mobile IPv4. In
addition, the route optimization process between the MN and CN can be
used to avoid the triangular routing in the Mobile IPv4 scenarios.

If the route optimization is not used, data flow routing and NSIS
signaling procedures (including the CRN discovery and the State
Update) will be similar to the case of using the Mobile IPv4 with co-
located CoA. However, if Route Optimization is used, signaling
messages are sent directly from the MN to the CN, or from the CN to
the MN. Therefore, route change procedures described in Section 4

are applicable to this case.

5.3. Interaction with Mobile IP tunneling

In this section, we assume that MN acts as an NI and CN acts as an NR
in interworking between Mobile IP and NSIS signaling.

Scenarios for interaction with Mobile IP tunneling vary depending on:

   - Whether a tunneling entry point (Tentry) is an MN or other node.
   In case Mobile IPv4 co-located CoA or Mobile IPv6, Tentry is an
   MN. In case Mobile IPv4 FA CoA case, Tentry is a FA. In both
   case, a HA is tunneling exit point (Texit).

   - Whether the mode of QoS-NSLP signaling is sender-initiated or
   receiver initiated.

   - Whether the operation mode over tunnel is with pre-configured
   QoS sessions or with dynamically created QoS sessions as described
   in [draft-ietf-nsis-tunnel].

The following subsection describes sender-initiated and receiver-
initiated reservation with Mobile IP tunneling and CRN discovery and
State Update with Mobile IP tunneling.

5.3.1. Sender-Initiated Reservation with Mobile IP tunnel

The following scenario assumes that a FA is a Tentry. However the
procedure is the same for the case an MN is a Tentry if it is
considered that the MN and the FA are the same node.

   - When an MN moves into a new network attachment point, QoS- NSLP
   in the MN initiates RESERVE (end-to-end) message to start the
   State Update procedure. The GIST below the QoS-NSLP adds GIST
   header and then sends the encapsulated RESERVE message to peer
   GIST node with corresponding QoS-NSLP. In this case, the peer
   GIST node is a FA if the FA is an NSIS-aware node. The FA is one
   of the endpoints of Mobile IP tunneling: Tentry. For proper NSIS
   tunneling operation, a Mobile IP endpoint is required to be NSIS
   tunneling aware. In case of interaction with tunnel signaling
   originated from the FA, there can be two scenarios depending on
   whether the tunnel already has pre-configured QoS sessions or not.
   In former case the FA map end-to-end QoS signaling requests
   directly to existing tunnel sessions. In latter case the FA
   dynamically initiate and maintain tunnel QoS sessions that are
   then associated with the corresponding end-to-end QoS sessions.
   [draft-ietf-nsis-tunnel].

- Figure 5 shows the typical NSIS operation over tunnels with pre-
configured QoS sessions. Both the FA and the HA are configured
with information about the Flow ID of the tunnel QoS session.
Upon receiving a RESERVE message from the MN, the FA checks tunnel
QoS configuration, determines whether and how this end-to-end
session can be mapped to a pre-configured tunnel session. The FA
then tunnels the RESERVE message to the HA. The CN replies with a
RESPONSE message which arrives at the HA, the FA and the MN.

- Figure 6 shows the typical NSIS operation over tunnels with
dynamically created QoS sessions. When the FA receives an end-to-
end RESERVE message from the MN, the FA chooses the tunnel Flow
ID, creates the tunnel session and associates the end-to-end
session with the tunnel session. The FA then sends a tunnel
RESERVE' message matching the request of the end-to-end session
towards the HA to reserve tunnel resources. The tunnel RESERVE'
message is processed hop-by-hop inside the tunnel for the flow
identified by the chosen tunnel Flow ID, while the end-to-end
RESERVE message passes through the tunnel intermediate nodes
(Tmid). When these two messages arrive at the HA, the HA creates
the reservation state for the tunnel session, and sends a tunnel
RESPONSE' message to the FA. At the same time, the HA updates the
end-to-end RESERVE message based on the result of the tunnel
session reservation, and forwards the end-to-end RESERVE message
along the path towards the CN. When the CN receives the end-to-
end RESERVE message, it sends an end-to-end RESPONSE message back
to the MN.

More detailed operations are specifid in [draft-ietf-nsis-tunnel].

```
   MN (Sender)   FA (Tentry)        Tmid        HA (Texit)  CN (Receiver)
        |             |              |            |             |
        |   RESERVE   |              |            |             |
        +------------>|              |            |             |
        |             |   RESERVE    |            |             |
        |             +--------------------------->|            |
        |             |              |            |   RESERVE   |
        |             |              |            +------------>|
        |             |              |            |   RESPONSE  |
        |             |              |            |<------------+
        |             |    RESPONSE  |            |             |
        |             |<---------------------------+            |
        |   RESPONSE  |              |            |             |
        |<------------+              |            |             |
        |             |              |            |             |
```
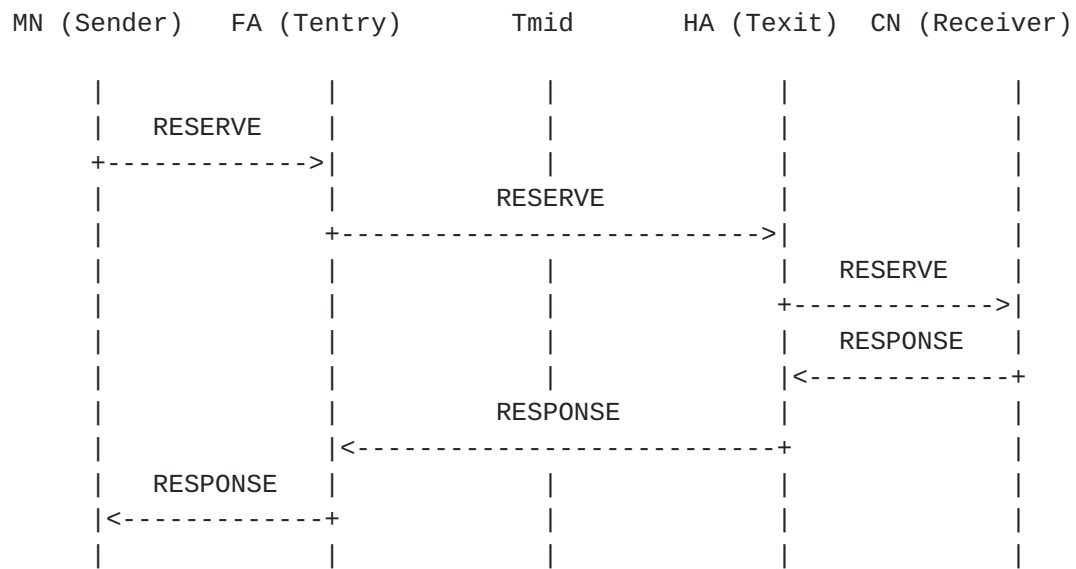
Figure 5: Sender-Initiated QoS-NSLP over Tunnel with Pre-configured
                          QoS Sessions

```
   MN (Sender)   FA (Tentry)        Tmid        HA (Texit)  CN (Receiver)
        |             |              |             |             |
        | RESERVE     |              |             |             |
        +------------>|              |             |             |
        |             | RESERVE'     |             |             |
        |             +============>|             |             |
        |             |              | RESERVE'    |             |
        |             |              +============>|             |
        |             |           RESERVE          |             |
        |             +--------------------------->|             |
        |             |              | RESPONSE'   |             |
        |             |              |<============+             |
        |             | RESPONSE'    |             |             |
        |             |<============+              |             |
        |             |              |             | RESERVE     |
        |             |              |             +------------>|
        |             |              |             | RESPONSE    |
        |             |              |             |<------------+
        |             |           RESPONSE         |             |
        |             |<---------------------------+             |
        | RESPONSE    |              |             |             |
        |<------------+              |             |             |
        |             |              |             |             |
```
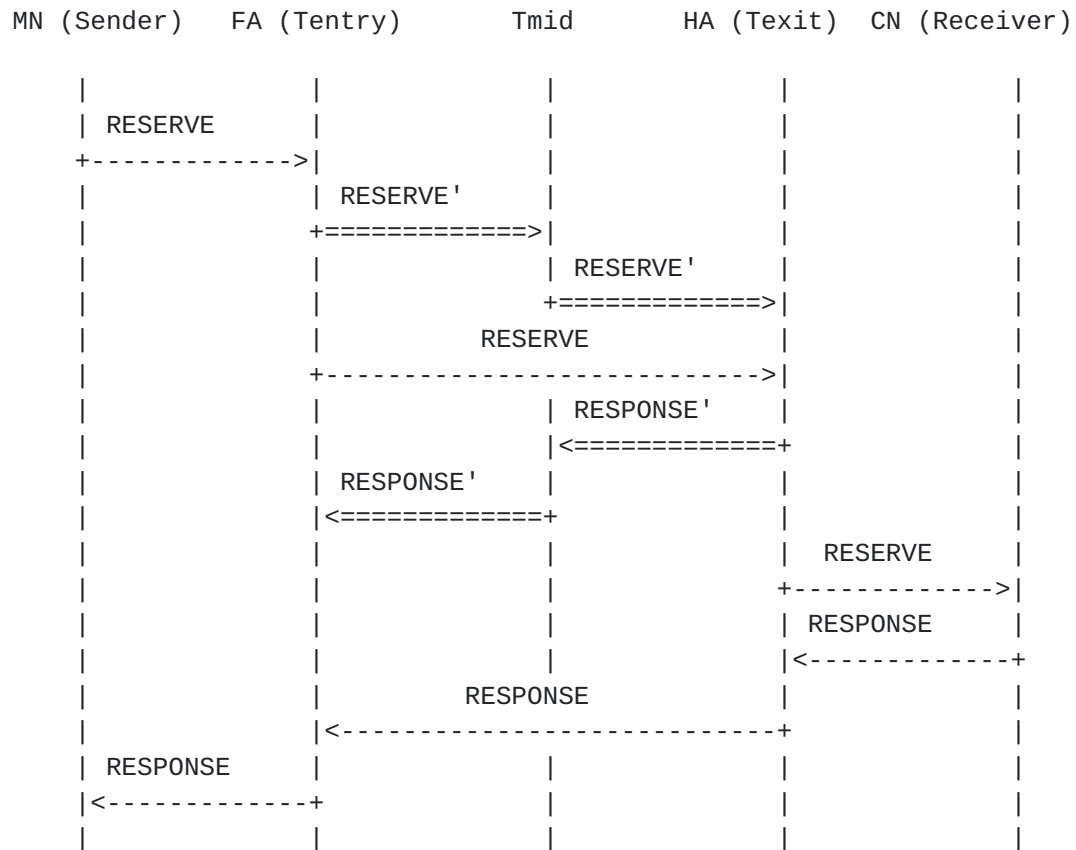
Figure 6: Sender-Initiated QoS NSLP over Tunnel with Dynamically
Created QoS Sessions

5.3.2. Receiver-Initiated Reservation with Mobile IP tunnel

Figure 7 and Figure 8 show examples of receiver-initiated operation
over Mobile IP tunnel with pre-configured and dynamically created QoS
session, respectively. Basic Operation is the same as sender-
initiated case.
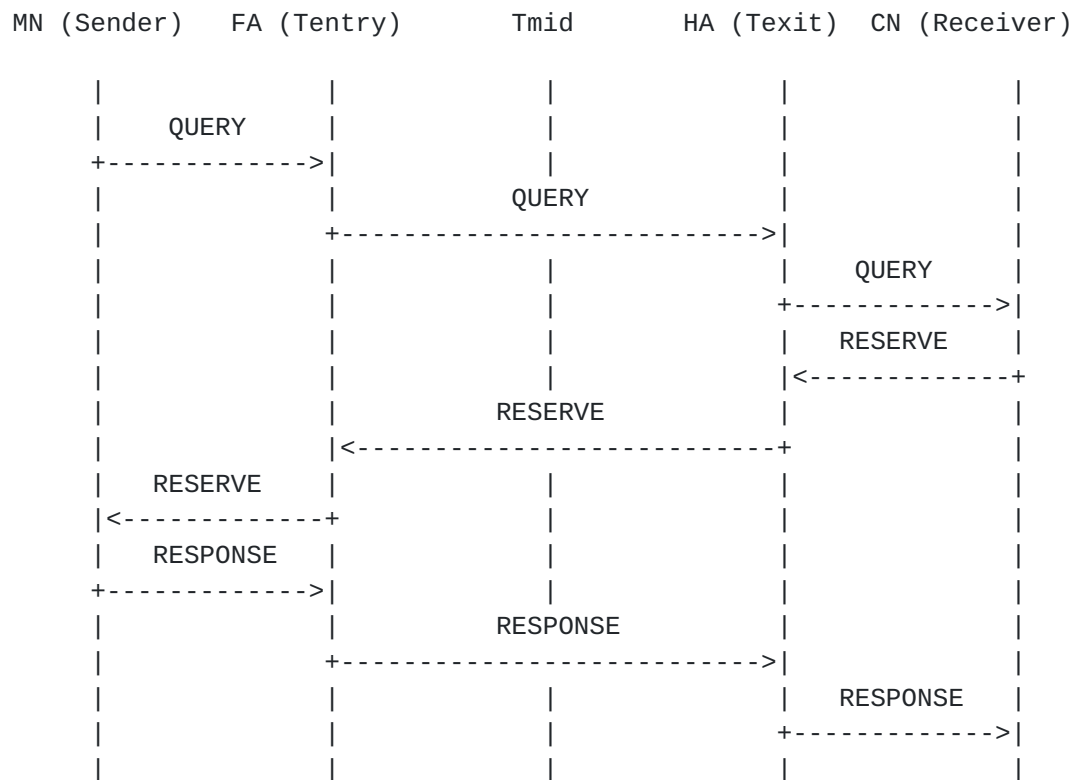
```
   MN (Sender)   FA (Tentry)        Tmid        HA (Texit)  CN (Receiver)

       |               |               |               |               |
       |    QUERY      |               |               |               |
       +------------->|               |               |               |
       |               |     QUERY     |               |               |
       |               +--------------------------->|               |
       |               |               |               |    QUERY      |
       |               |               |               +------------->|
       |               |               |               |    RESERVE    |
       |               |               |               |<------------+
       |               |     RESERVE   |               |               |
       |               |<---------------------------+               |
       |    RESERVE    |               |               |               |
       |<------------+               |               |               |
       |    RESPONSE   |               |               |               |
       +------------->|               |               |               |
       |               |    RESPONSE   |               |               |
       |               +--------------------------->|               |
       |               |               |               |    RESPONSE   |
       |               |               |               +------------->|
       |               |               |               |               |
```

Figure 7: Receiver-Initiated QoS NSLP over Tunnel with Pre-Configured
                              QoS Session

```
   MN (Sender)  FA (Tentry)       Tmid       HA (Texit)  CN (Receiver)

       |    QUERY    |            |            |            |
       +------------>|            |            |            |
       |            |   QUERY'    |            |            |
       |            +============>|            |            |
       |            |            |   QUERY'    |            |
       |            |            +============>|            |
       |            |            | RESPONSE'   |            |
       |            |            |<============+            |
       |            | RESPONSE'   |            |            |
       |            |<===========+            |            |
       |            |           QUERY          |            |
       |            +-------------------------->|            |
       |            |            |            |   QUERY    |
       |            |            |            +------------>|
       |            |            |            |  RESERVE    |
       |            |            |            |<------------+
       |            |            | RESERVE'    |            |
       |            |            |<============+            |
       |            | RESERVE'    |            |            |
       |            |<===========+            |            |
       |            |          RESERVE         |            |
       |            |<-------------------------+            |
       |            | RESPONSE'   |            |            |
       |            +============>|            |            |
       |            |            | RESPONSE'   |            |
       |            |            +============>|            |
       | RESERVE    |            |            |            |
       |<-----------+            |            |            |
       | RESPONSE    |            |            |            |
       +------------>|            |            |            |
       |            |          RESPONSE         |            |
       |            +-------------------------->|            |
       |            |            |            |  RESPONSE   |
       |            |            |            +------------>|
       |            |            |            |            |
```
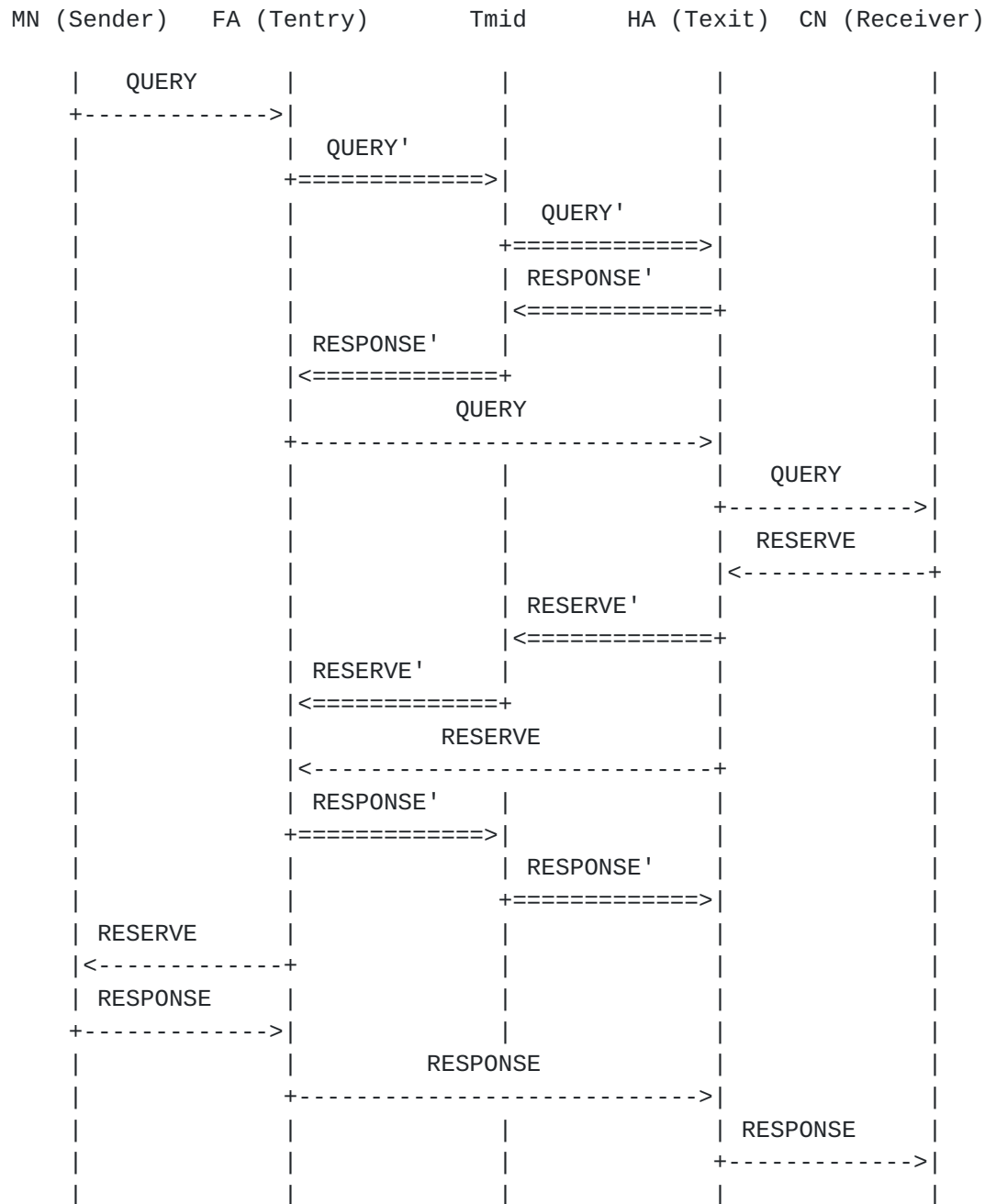
         Figure 8: Receiver-Initiated QoS NSLP over Tunnel with Dynamically
                           Created QoS Session

5.3.3. CRN discovery and State Update with Mobile IP tunneling

   In case the tunnel is dynamically created mode, interaction with
   Mobile IP tunneling scenario can define two types of CRNs, i.e., a
   CRN on end-to-end path and a CRN on tunneling path while pre-
   configured mode only have the one on end-to-end. CRN discovery and

State Update for these two paths are operated independently.

CRN discovery for end-to-end path is initiated by the MN by sending
RESERVE (sender-initiated case) or QUERY (receiver-initiated case)
message. As MN uses HoA as source address even after handover, a CRN
is found by normal route change process (i.e., the same SID and FID,
but different SII handle). If a HA is QoS-NSLP aware, the HA is
found as the CRN. The CRN initiate tearing process on the old path
as described in [draft-ietf-nsis-qos-nslp]

CRN discovery for tunneling path is initiated by Tentry by sending
RESERVE' (sender-initiated case) or QUERY' (receiver-initiated case)
message. The route change procedures described in Section 4 are
applicable to this case.

End-to-end state inside the tunnel should not be torn until all
states inside the tunnel have been torn from imprementation
perspective. But detailed discussions are out-of-scope of this
document.

6. Further Studies

   All sections above dealt with basic issues on NSIS mobility support.
   This section introduces potential issues and possible approaches for
   complicated scenarios in the mobile environment, i.e., peer failure
   scenarios, multihomed scenarios, and interworking with other mobility
   protocols, which may need to be resolved in the future. Topics in
   this section are out-of-scope of this document. Detailed operations
   in this section are just for future references.

6.1. NSIS Operation in the multihomed mobile environment

   In multihomed mobile environments, multiple interfaces and addresses
   (i.e., CoAs and HoAs) are available. This case, two major issues can
   be considered. One is how to select or acquire the most appropriate
   interface(s) and/or address(es) from end-to-end QoS point of view.
   The other is, when multiple paths are simultaneously used for load-
   balancing purpose, how to differentiate and manage two types of CRNs,
   i.e., CRN between two on-going Paths (LB-CRN: Load Balancing CRN) and
   CRN between the old and new paths caused by MN's handover (HO-CRN:
   Handover CRN). This section introduces possible approaches for these
   issues.

6.1.1. Selecting the best interface(s)/CoA(s)

   In MIPv6 route optimization case, if multiple CoAs registration is
   provided [RFC5648], the contents of QUERYs sent by candidate CoAs can
   be used to select the best interface(s)/CoA(s).

   Assume that an MN is a data sender and has multiple interfaces. Now
   the MN moves to a new location and acquires CoA(s) for multiple
   interfaces. After the MN performs the BU/BA procedure, it sends
   QUERY messages toward the CN through the interface(s) associated with
   the CoA(s). On receiving the QUERY messages, the CN or Gateway,
   determines the best (primary) CoA(s) by checking 'QoS available'
   field in the QUERY messages. Then a RESERVE message is sent toward
   the MN to reserve resources along the path the primary CoA takes. If
   the reservation is not successful, the CN transmits another RESERVE
   message using the CoA with the next highest priority. The CRN may
   initiate a teardown (RESERVE with the TEAR flag set) message toward
   old access router (OAR) to release the reserved resources on the old
   path.

   In case of sender-initiated reservation, a similar approach is
   possible. That is, the QUERY and RESERVE messages are initiated by
   an MN, and the MN selects the Primary CoA based on the information
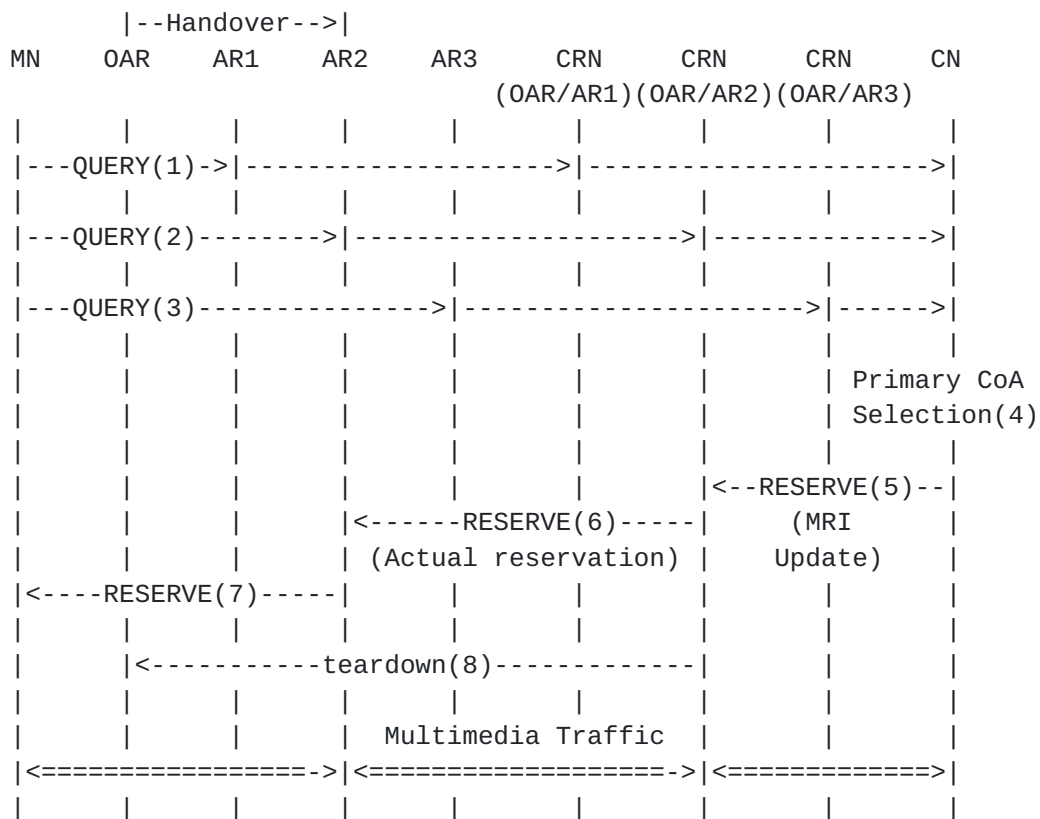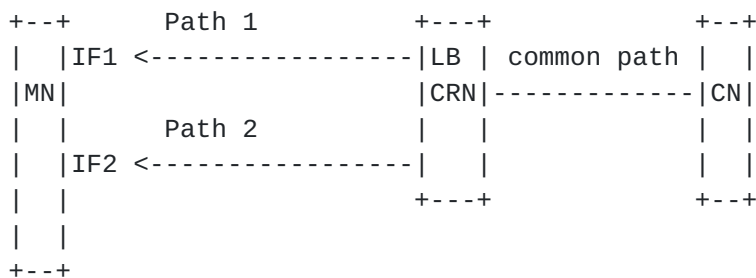   delivered by the QUERY message.

```
              |--Handover-->|
    MN      OAR     AR1     AR2     AR3     CRN      CRN      CRN      CN
                                         (OAR/AR1)(OAR/AR2)(OAR/AR3)
    |       |       |       |       |       |        |        |       |
    |---QUERY(1)->|--------------------->|---------------------->|
    |       |       |       |       |       |        |        |       |
    |---QUERY(2)-------->|--------------------->|-------------->|
    |       |       |       |       |       |        |        |       |
    |---QUERY(3)--------------->|---------------------->|------>|
    |       |       |       |       |       |        |        |       |
    |       |       |       |       |       |        |        | Primary CoA
    |       |       |       |       |       |        |        | Selection(4)
    |       |       |       |       |       |        |        |       |
    |       |       |       |       |       |        |<--RESERVE(5)--|
    |       |       |       |<------RESERVE(6)-----|    (MRI        |
    |       |       |       | (Actual reservation) |    Update)     |
    |<----RESERVE(7)-----|       |       |        |        |       |
    |       |       |       |       |       |        |        |       |
    |       |<-----------teardown(8)--------------|        |       |
    |       |       |       |       |       |        |        |       |
    |       |       |       | Multimedia Traffic   |        |       |
    |<===============->|<==================->|<============>|
    |       |       |       |       |       |        |        |       |
```

           Figure 9: Receiver-initiated reservation in the multihomed
                                environment

6.1.2. Differentiation of two types of CRNs
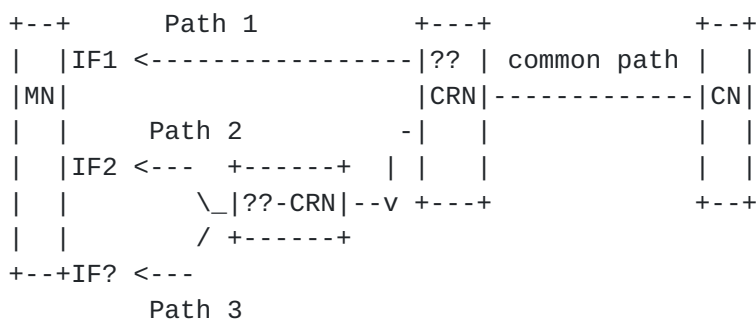
   When multiple interfaces of the MN are simultaneously used for load-
   balancing purpose, a possible approach for distinguishing LB-CRN and
   HO-CRN will introduce an identifier to determine the relationship
   between interfaces and paths.

   An MN uses interface 1 and interface 2 for the same session, where
   the paths (say path 1 and path 2) have the same SID but different
   FIDs as shown in (a) of Figure 10. Now one of the interfaces of MN
   performs a handover and obtains a new CoA, the MN will try to
   establish a new path (say Path 3) with the new FID, as shown in (b)
   of Figure 10. In this case the CRN between path 2 and path 3 cannot
   determine if it is LB-CRN or HO-CRN since for both cases, SID is the
   same but FIDs are different. Hence the CRN will not know if State
   Update is required. One possible solution to solve this issue will
   introduce path classification identifier which shows the relationship
   between interfaces and paths. For example, signaling messages and
   QNEs belong to paths from interface 1 and interface 2 carry the

identifier '00' and '02', respectively. By having this identifier,
the CRN between path 2 and path 3 will be able to determine whether
it is LB-CRN or HO-CRN. For example, if path 3 carries '00', the CRN
is LB-CRN, and if '01', the CRN is HO-CRN.

```
   +--+        Path 1              +---+              +--+
   |  |IF1 <-----------------|LB | common path |  |
   |MN|                      |CRN|-------------|CN|
   |  |        Path 2        |   |             |  |
   |  |IF2 <----------------|   |             |  |
   |  |                      +---+             +--+
   |  |
   +--+
   (a) NSIS Path classification in multihomed environments

   +--+        Path 1           +---+              +--+
   |  |IF1 <-----------------|?? | common path |  |
   |MN|                      |CRN|-------------|CN|
   |  |        Path 2      -|   |             |  |
   |  |IF2 <---   +------+  | |   |             |  |
   |  |        \_|??-CRN|--v +---+              +--+
   |  |        / +------+
   +--+IF? <---
           Path 3
```

   (b) NSIS Path classification after handover

      Figure 10: The topology for NSIS signaling in multihomed mobile
                              environments

[6.2](). **Interworking with other mobility protocols**

   Unlike the generic route changes, in mobility scenarios, the end-to-
   end signaling problem by the State Update gives rise to the
   degradation of network performance, e.g., increased signaling
   overhead, service blackout, and so on. To reduce signaling latency
   in the Mobile IP-based scenarios, the NSIS protocol suite may need to
   interwork with localized mobility management (LMM). If the GIST/NSLP
   (QoS-NSLP or NAT/FW-NSLP) protocols interact with Hierarchical Mobile
   IPv6 and the CRN is discovered between an MN and an MAP, the State
   Update can be localized by address mapping. However, how the State
   Update is performed with scoped signaling messages within the access
   network under the MAP is for future study.

In the inter-domain handover, a possible way to mitigate the latency
penalty is to use the multi-homed MN. It is also possible to allow
the NSIS protocols to interact with mobility protocols such as
Seamoby protocols (e.g., Candidate Access Router Discovery (CARD)
[RFC4066] and Context Transfer Protocol (CXTP) [RFC4067]) and Fast
Mobile IP (FMIP). Another scenario is to use peering agreement which
allows aggregation authorization to be performed for aggregate
reservation on an inter- domain link without authorizing each
individual session. How these approaches can be used in NSIS
signaling is for further study.

6.3. Intermediate node becomes a dead peer

The failure of a (potential) NSIS CRN may result in incomplete state
re-establishment on the new path and incomplete teardown on the old
path after handover. In this case, a new CRN should be re-discovered
immediately by the CRN discovery procedure.

The failure of an AR may make the interactions with Seamoby protocols
(such as CARD and CXTP) impossible. In this case, the neighboring
peer closest to the dead AR may need to interact with such protocols.
A more detailed analysis of interactions with Seamoby protocols is
left for future work.

In Mobile IP-based scenarios, the failures of NSIS functions at an FA
and an HA may result in incomplete interaction with IP-tunneling. In
this case, recovery for NSIS functions needs to be performed
immediately. In addtion, a more detailed analysis of interactions
with IP-tunneling is left for future work.

7. Security Considerations

This document does not introduce new security concerns. The security
considerations pertaining to the standard NSIS protocol
specifications [gist, qos-nslp, natfw-nslp] remain relevant. When
deployed in service provider networks, it is mandatory to ensure that
only authorized entities are permitted to initiate re-establishment
and removal of NSIS states in mobile environments, including the use
of NSIS proxies and CRN.

8. IANA Considerations

   This memo includes no request to IANA.

9. Change History

   [Note to the RFC editor: Please remove this section before
   publication]

9.1. Changes from -00 version

   The major change made to the initial (-00) version of the draft is to
   re-arrange the issues addressed in the draft in order to clearly
   identify general issues caused by mobility itself and NSIS protocols-
   specific issues. The generic route changes-related text in Section 4
   was moved into Appendix to make this draft more mobility-specific.

   Specifically, the following changes have been made:

   1.   Removed the terminologies, 'uplink' and 'downlink' in Section 2.

   2.   Removed the terminology, 'local repair' in Sections 2 and 4.

   3.   Re-arranged all problems in Section 3 by merging the 'mobility-
         related issues with NSIS protocols' section and the 'problem
         statement and general considerations' section.

   4.   Removed the general considerations section in Section 3.

   5.   Modified the problem statement section and moved it into the
         general problem section in Section 3.1.

   6.   Added more problems including 'Identification of the crossover
         node', 'Key exchanges', and 'AA-related Issues' to Section 3.1

   7.   Added the 'Multihoming-related issues' to Section 3.2.4

   8.   Removed the issues on 'how to immediately delete the state on
         the old path' in Section 3.2.

   9.   Moved the generic route changes-related text in Section 4.1 into
         Appendix.

   10.   Removed the figure describing "NSIS signaling topology for
         downstream signaling flow after the route changes in the middle
         of the network" in Figure 2.

   11.   Added 'NSLP_IDs' to each node in Figure 1.

   12.   Removed the 'use cases of identifiers' section, and instead,
         added the 'support for ping-pong type handover' section to
         Section5.

13.   Added this change history.

9.2. Changes from -01 version

Version -02 includes mainly a number of clarifications on the issues
raised in this draft and more details in some specific areas.
Specifically, the following changes have been made:

1.   Defined the terminologies, 'route change' and 'mobility' in
      Section 2.

2.   Clarified the terminology, 'Crossover node (CRN)' in Section 2.

3.   Removed the terminology, 'mobility CRN' in Section 2.

4.   The issue, 'Priority of signaling messages' in Section 3.2.2 was
      closed, and thus removed it.

5.   Clarified the issue, 'CRN discovery and State Update on the IP-
      tunneling path in Section 3.2.4.

6.   Added the pros and cons of two mechanisms on CRN discovery
      dependent on NSIS layers to Section 4.2.1.

7.   Clarified the identifier, NSLP_Br_ID for CRN discovery in
      Section 4.2.2.

8.   Added the scenario on interaction between NSIS and Mobile IP to
      Section 5.1.

9.   Clarified interaction issues with IP-tunneling according to
      reservation initiation type (receiver-initiated or sender-
      initiated) in Mobile IPv4-based scenarios and added those to
      Section 5.1.1.1.

10.   1Clarified interaction issues between NSIS protocols and IP-
      tunneling in Mobile IPv6 and added those to Section 5.1.1.2.

11.   Clarified the multihoming-related issues in Section 5.2.

12.   Added the issues on usage of 'hint' information to trigger NSIS
      signaling in mobility to Section 5.5.

13.   Identified the dead peer-related issues in Mobile IP-based
      scenario in Section 5.5.

9.3. Changes from -02 version

   In version -03, tunneling-related and multihoming-related scenarios
   were newly added in Sections 5.1.3 and 5.2, respectively. Also, the
   terminology, 'Path Update' is changed into 'State Update' in Section
   3.2.4.

9.4. Changes from -03 version

   Version -04 includes mainly a number of clarifications on the issues
   raised in this draft and more details in some specific areas.
   Specifically, the following changes have been made:

   1.   The issue, 'Peering agreement issue' in Section 3.2.2 was
        closed, and thus removed it.

   2.   Clarified the issue, 'Interfaces between Mobile IP and NSIS
        protocols' in Section 3.2.1.

   3.   Clarified the issue, 'Authorization-related issues with
        teardown' in Section 3.2.2.

   4.   Clarified the issue, 'Dead peer discovery' in Section 3.2.2.

   5.   Clarified the issue, 'Invalid NR problem' in Section 3.2.2.

   6.   Clarified the issue, 'CRN discovery and State Update on the IP-
        tunneling path' in Section 3.2.4.

   7.   Clarified the issue, 'Multihoming-related issues' in Section
        3.2.4.

   8.   Changed Figure 1 (a) into (b) in Section 4.1.

   9.   Changed Figure 1 (b) into (a) in Section 4.1.

   10. Clarified the identifier, NSLP_Br_ID for CRN discovery in
        Section 4.2.2.

   11. Clarified the identifier, Mobility identifier for CRN discovery
        in Section 4.2.2.

   12. Added the text on 'CRN_DISCOVERY flag bit' in Section 4.2.3, and
        clarified the role of 'CD flag bit' in Section 4.3.1.

   13. Clarified the issues on 'interaction with Mobile IP tunneling'
        and added those to Section 5.1.4.

14. Clarified the issues on 'load balancing in multihomed mobile
     environments' and added those to Section 5.2.5.

15. Changed Problems of the heading name in Section 3.2 into
     Challenges.

9.5. Changes from -04 version

Version -05 includes mainly a number of clarifications on the issues
raised in this draft and more details in some specific areas.
Specifically, the following changes have been made:

1.   'Explicit routes' in Section 3.1 (3) was removed.

2.   Clarified the problem, 'Double reservation problem' in Section
     3.1 (7).

3.   Clarified the issue, 'CRN discovery-related issues' in Section
     3.2.4 (1).

4.   Clarified the issue, 'Issues on API between NTLP and NSLP' in
     Section 3.2.4 (3).

5.   Clarified the issue, 'approaches for CRN discovery' in Section
     4.2.1.

6.   Changed NSLP_Br_ID (of identifiers for CRN discovery) into
     State_Br_ID in Section 4.2.2 for clarification.

7.   Clarified the issue, 'double reservation problem on the common
     path' in Section 4.3.1.

8.   Clarified the issue, 'Interfaces between Mobile IP and NSIS' in
     Section 5.1.1.

9.   Removed the sencond paragraph on the issue, 'Explicit routes' in
     Section 4.1.

10. Clarified the issue, 'refresh timer value in mobility scenarios'
     in Section 5.3.

11. Removed the third paragraph on the issue, 'usage of Reservation
     Sequence Number (RSN) to support ping-pong type hanover' in
     Section 5.4.

12. Clarified the issues on 'peer failure' in Section 5.5.

13. Removed Figure 3 'Sender- vs. Receiver-initiated reservation' in
     Section 4.3.1.

9.6. Changes from -05 version

In Version -06, contents of this draft were re-selected and re-
structured:

1. Section 4 and 5 of -05 were divided into two parts:

    1. 'Main' part, which is focusing on examples and describing how
        mobility is handled by the NSIS protocols. Topics here will
        be route change handling and NSIS interwork with MIP v4/v6
        (Section 4 and Section 5 in -06)

    2. 'Further Study' part, which introduces summary of potential
        issues and possible approaches for other topics. These
        topics are out-of-scope for discussing details (Section 6 in
        -06)

2. Specific parameters and terms were removed from 'Main' part

3. Showing similar detailed operations were avoided in 'Interaction
    with MIP tunneling section (Section 5.3)'

4. In Further Study section Section 6:

    1. Detailed operations were removed

    2. Ping-pong issue was removed

5. Problem Statement (Section 3) was cleaned up

9.7. Changes from -06 version

Changes in Version -07 are:

1. 'Invalid NR problem' are moved from Further Study section

2. Figure 7 (Receiver-Initiated QoS NSLP over Tunnel -Parallel Mode)
    are changed

3. Terminologies 'NSLP CRN', 'NTLP CRN' 'NSIS CRN' 'Divergent-
    convergent UCRN' and 'Divergent-convergent DCRN' are removed from
    Terminology section.

4. 'Open Issues' section is added

9.8. Changes from -07 version

   Changes in Version -08 are:

   1. Figure 1 was updated (NOTIFY message from CRN is added)

   2. Section 4.2.1 (CRN discovery) was updated to be synchronized with
       QoS-NSLP draft

   3. Title of Section 4.2.2 was changed from "State setup and update"
       to "Localized State Update"

   4. Section 4.2.2 (Localized State Update) was updated to be
       synchronized with QoS-NSLP draft

   5. Section 4.2.3 (State teardown) was deleted because the issues was
       already solved

   6. Title of Section 4.2.3 was changed to "State teardown
       consideration"

9.9. Changes from -08 version

   Changes in Version -09 are:

   1. Security Consideration Section (Section 7) was cleaned up.

   2. Security Consideration issue was removed from Open Issue section
       (Section 8).

   3. NAT traversal issues were removed from Open Issue section
       (Section 8).

9.10. Changes from -09 version

   Changes in Version -10 are:

   1. Introduction was updated accordingly.

   2. Definition of RFC2119 terms were removed from Section 2

   3. Definition of Upstream/Downstream State Update were cleaned up

   4. Title of Section 3 was changed from "Problem Statement" to
       "Challenges with Mobility"

   5. NSIS solutions are removed from Section 3

6. [Section 4](#) was cleaned up

7. More detailed description was added to [Section 5](#)

9.11. Changes from -10 version

Change in Version -11 is:

1. Introduction part of [Section 5](#) was updated.

9.12. Changes from -11 version

Change in Version -12 are:

1. [Section 4.3](#) (NATFW section) was added.

2. Open Issue section was closed.

9.13. Changes from -12 version

Changes in Version -13 are:

1. "Upstream signaling" was added to [Section 3](#)

2. Three more cases were discussed in [Section 4.2](#)

3. Definition of Upstream/Downstream State Update were cleaned up

4. Figure 3 was removed because it was't really necessary for the
    discussion.

9.14. Changes from -13 version

Change in Version -14 is:

1. Figure 3 was re-added with appropriate changes.

9.15. Changes from -14 version

Change in Version -15 is:

1. Title was changed because this draft is not talking about AS.

9.16. Changes from -15 version

Changes in Version -16 are:

   1. RFC2205, RFC3726, RFC3753 and draft-ietf-nsis-tunnel were changed
       from Normative references to Informative references.

   2. IANA Consideration was added.

   3. RFC4066 and RFC4067 was added to Informative References.

9.17. Changes from -16 version

   Changes in Version -17 is:

   1. Some editorial changes were made.

9.18. Changes from -17 version

   Changes in Version -18 is:

   1. Some editorial changes were made.

9.19. Changes from -18 version

   Changes in Version -19 are:

   1. Abstract and Introduction were changed to clearly say the NSIS
       protocols operations can work in mobility environments without
       particular operations, and additional operations such as CRN
       discovery are only for enhancement and informational.

   2. Some texts were added to section 4 to say the state in old path
       can be torn by timer.

   3. Consideration in tearing down end-to-end tunneling state was
       mentioned in section 5.

   4. Authorization for CRN was briefly mentioned in security
       consideration.

   5. Some editorial changes were made.

10. Contributors

   Sung-Hyuck Lee was the first editor of the draft. Since version 06
   of the draft, Takako Sanda has taken the editorship.

   Many individuals have contributed to this draft. Since it was not
   possible to list them all in the authors section, this section was
   created to have a sincere respect for other authors, Paulo Mendes,
   Robert Hancock, Roland Bless, Shivanajay Marwaha and Martin
   Stiemerling. Separating authors into two groups was done without
   treating any one of them better (or worse) than others.

11. Acknowledgements

The authors would like to thank Byoung-Joon Lee, Charles Q. Shen, Cornelia Kappler, Henning Schulzrinne, and Jongho Bang for significant contributions in four earlier drafts and the previous draft. The authors would also like to thank Robert Hancock, Andrew Mcdonald, John Loughney, Rudiger Geib, Cheng Hong, Elena Scialpi, Pratic Bose, Martin Stiemerling and Luis Cordeiro for their useful comments and suggestions.

12. References

12.1. Normative Reference

[RFC3344]   Perkins, C., "IP Mobility Support for IPv4", RFC3344 ,
            August 2002.

[RFC3775]   Johnson, D., "Mobility Support in IPv6", RFC3775 ,
            June 2004.

[draft-ietf-nsis-nslp-natfw]
            Stiemerling, M., "NAT/Firewall NSIS Signaling Layer
            Protocol (NSLP)", Internet
            Draft draft-ietf-nsis-nslp-natfw-25, Work in progress ,
            April 2010.

[draft-ietf-nsis-ntlp]
            Schulzrinne, H., "GIST: General Internet Signaling
            Transport", Internet Draft draft-ietf-nsis-ntlp-20, Work
            in progress , June 2009.

[draft-ietf-nsis-qos-nslp]
            Manner, J., "NSLP for Quality-of-Service Signaling",
            Internet Draft draft-ietf-nsis-qos-nslp-18, Work in
            progress , January 2010.

12.2. Informative References

[RFC2205]   Braden, B., "Resource ReSerVation Protocol (RSVP) --
            Version 1 Functional Specification", RFC2205 ,
            September 1997.

[RFC3726]   Brunner, (Ed), M., "Requirements for Signaling Protocols",
            RFC3726 , June 2004.

[RFC3753]   Manner, J., "Mobility Related Terminology", RFC3753 ,
            June 2004.

[RFC4066]   Liebsch, M., "Candidate Access Router Discovery (CARD)",
            RFC4066 , July 2005.

[RFC4067]   Loughney, J., "Context Transfer Protocol (CXTP)",
            RFC4067 , July 2005.

[RFC5648]   Wakikawa, R., "Multiple Care-of-Address Registration",
            RFC5648 , October 2009.

[draft-ietf-nsis-tunnel]

Shen, C., "NSIS Operation Over IP Tunnels", Internet
Draft draft-ietf-nsis-tunnel-10, Work in Progress ,
April 2010.

Authors' Addresses

    Takako Sanda
    Panasonic Corporation
    600 Saedo-cho, Tsuzuki-ku, Yokohama
    Kanagawa 224-8539
    Japan

    Phone: +81 45 938 3056
    Email: sanda.takako@jp.panasonic.com

    Xiaoming Fu
    Computer Networks Group, University of Goettingen
    Lotzestr. 16-18
    Goettingen 37083
    Germany

    Email: fu@cs.uni-goettingen.de

    Seong-Ho Jeong
    Hankuk University of FS
    89 Wangsan Mohyun
    Yongin-si, Gyeonggi-do 449-791
    Korea

    Phone: +82 31 330 4642
    Email: shjeong@hufs.ac.kr

    Jukka Manner
    Helsinki University of Technology
    P.O. Box 3000
    Espoo FIN-02015
    Finland

    Phone: +358 9 451 2481
    Email: jukka.manner@tkk.fi

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo
02600
Finland

Phone: +358 50 4871445
Email: Hannes.Tschofenig@nsn.com