Applicability Statement of NSIS Protocols in Mobile Environments
draft-ietf-nsis-applicability-mobility-signaling-03.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on April 27, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

The 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 draft discusses the effects mobility can cause to the NSIS protocols, and how the protocols operate in different scenarios, and together with mobility management protocols.

Table of Contents

1. Introduction ........................................... 4
2. Requirements Notation and Terminology .................. 4
3. Problem Statement ..................................... 7
   3.1. General problems .................................. 7
   3.2. Mobility-Related Issues with NSIS Protocols ..... 9
      3.2.1. NTLP-Specific Problems .................. 10
      3.2.2. QoS-NSLP-Specific Problems ............ 10
      3.2.3. NAT/FW NSLP-Specific Problems .......... 11
      3.2.4. Common problems related to both NTLP and NSLP 12
4. Basic Operations for Mobility Support .................. 13
   4.1. Route changes caused by mobility ................. 13
   4.2. CRN discovery .................................. 15
      4.2.1. Possible approaches for CRN discovery .... 15
      4.2.2. The identifiers for CRN discovery ........ 16
      4.2.3. The procedures of CRN discovery ...... 18
   4.3. State Update .................................... 19
      4.3.1. State setup and update .................. 20
      4.3.2. State teardown .......................... 22
5. Applicability Statement ................................ 23
   5.1. Support for macro mobility-based scenarios ...... 23
      5.1.1. Interfaces between Mobile IP and NSIS .... 24
      5.1.2. Mobile IPv4-specific issues ............ 25
      5.1.3. Mobile IPv6-specific issues .......... 28
      5.1.4. Interaction with Mobile IP tunneling .... 30
         5.1.4.1. Interaction scenarios with Mobile IPv4 tunneling .... 30
         5.1.4.2. Interaction scenarios with Mobile IPv6 tunneling .... 37
      5.2. NSIS operations in multihomed mobile environments .... 42
         5.2.1. Multihomed mobile environments .......... 42
         5.2.2. Receiver-initiated reservation in the multihomed environment .......... 44
         5.2.3. Sender-initiated reservation in the multihomed environment .......... 44
         5.2.4. Link/node failure recovery ............ 46
         5.2.5. Load balancing .......................... 46
      5.3. QoS performance considerations in mobility scenarios .... 47
      5.4. Support for Ping-Pong type handover ........... 49
      5.5. Peer failure scenarios ........................ 50
6. Security Considerations ................................ 51
   6.1. MN as data sender ............................... 52
      6.1.1. MN is authorizing entity ................ 52
      6.1.2. CN is authorizing entity ............... 54
1. Introduction

The mobility of IP-based nodes incurs route changes, usually at the edge of the network. Route changes may also be caused by reasons other than mobility, such as routing protocol adaptation in response to varying network conditions (load sharing, load balancing, etc), or...
host multi-homing. Macro mobility also involves the change of the mobile node's IP addresses. Since IP addresses are usually part of flow identifiers, the change of IP addresses implies the change of flow identifiers. Local mobility usually does not cause the change of the global IP addresses, but affects the routing paths within the local access network [3].

In multi-homed mobile networks, mobile nodes (MNs) can have an access to multiple interfaces and obtains multiple addresses (e.g., CoAs and HoAs). It enables the MN to choose most appropriate interface or address according to application (or flow) types or network conditions in homogeneous/heterogeneous environments. The Multihoming helps alleviate various problems caused by wireless bottleneck and mobility events, scarce resources and frequent handovers for examples.

NSIS protocol suit consists of two layers: NSIS Transport Layer Protocol (NTLP) and the NSIS Signaling Layer Protocol (NSLP). The NTLP is an application independent protocol which transports service-related information between nodes in a network, and each specific service has its own NSLP protocol (e.g., QoS-NSLP, NAT/FW-NSLP, etc.).

The goals of this draft are to present the effects of mobility on the NTLP/NSLPs and to provide guides on how such NSIS protocols should work in various mobility scenarios including multihoming. Most of all, this draft mainly discusses the operations of the NSIS protocols in very basic mobility scenarios (e.g., macro mobility management protocols such as Mobile IPv4 and Mobile IPv6), including support for multi-homing. More complex scenarios and issues on interworking with various mobility-related protocols, such as Seamoby and local mobility management protocols, are left for future work.

2. Requirements Notation and Terminology

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 [1].

The terminology in this draft is based on [2] and [3]. In addition,
(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 along which states are installed. The CRN may not necessarily be a physical route splitting point. There exist different types of logical (but not necessarily physical) CRNs depending on the signaling states, flow directions, mobility management types, and the routing infrastructure:

From the perspective of NSIS state (i.e., NSLP and NTLP state), the types of CRN can be classified as follows.

NSLP CRN: a signaling application-aware node in the network where the corresponding signaling flows begin to merge or split after a route change or mobility. If multiple signalling application sessions refer to the same data flow, the NSLP CRN after a route change may be different for each NSLP involved.

NTLP CRN: an NTLP-aware network node where multiple NTLP state begin to merge or split after a route change or mobility.

NSIS CRN: A node is called an NSIS CRN if it an NSLP or an NTLP CRN.

The types of CRN can be further classified according to their location in the network, with respect to the path from data sender to data receiver, as follows.

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 as shown in Figure 1 of Section 4.1, where we assume that the 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.

In case of the route changes, the path change of signaling flows results in forming a chain of two CRNs regardless of the direction of signaling flows followed by data flows as shown in Figure 14 of Appendix A. The CRN chain is referred to as a divergence-convergence pair:

Divergent-convergent UCRN pair: a chain of the nodes at which the state information towards the data sender begins to diverge and to converge after a route changes.

Divergent-convergent DCRN pair: a chain of the nodes at which the state information towards the data receiver begins to diverge and to converge after a route changes.

Routing CRN is the node where the old and new paths (rather physically) merge using regular IP routing. For example, the merging points caused by mobility management protocols are a kind of Routing CRN. Depending on the location of nodes, the routing CRN may not be equal to the NSLP CRN or NTLP CRN.

(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 which is initiated by an upstream signaling initiator. If the MN is a data sender, the State Update is initiated by an NI on the common path (e.g., a CN, an HA, or an MAP).

Downstream State Update: State Update for the downstream signaling flow which is triggered by a downstream signaling initiator. If the MN is a data sender, the State Update is triggered by an NI on the new path (e.g., an MN, a mobility agent, or an AR).

In case of route changes except for mobility, the update of NSIS state on the common path is not required because the flow identifiers do not change, which limits the scope of the required NSIS signaling. Especially, in mobility scenarios, if the NSIS signaling interacts with local mobility management (LMM) protocols (e.g., HMIPv6), the State Update can be localized within the access network.

(5) Dead Peer Discovery (DPD)
The procedure for finding a dead NSIS peer due to a link/node failure or due to an MN moving away.

3. Problem Statement

IP mobility in its simplest form only includes route changes. This section identifies problems caused by mobility, which may have a significant impact on the operations of NSIS protocols.

3.1. General problems

The general problems caused by mobility are as follows.

(1) Change of route and possibly change of the MN IP address

Topology changes might lead to path changes for data packets sent to or from the MN and may lead to an IP address change of the MN.

(2) Latency 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.

(3) Explicit routes

Path-coupled signaling protocols usually expect the data traffic to follow the same path as the signaling, but the data traffic sometimes traverses a path different from the path of signaling traffic due to the adaptation of routing tables to varying network conditions and to techniques such as load balancing, load sharing and mobility. For example, Mobile IP may use the routing headers to define explicit routes, which diverts the traffic from an expected path.

(4) 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 makes 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. If the signaling packets are encapsulated it might be necessary to perform a separate signaling exchange for the tunneled region.

(5) Ping-pong type handover
Signaling protocols should remove state quickly along the old path to limit the waste of resources. However, in a ping-pong type handover, the MN returns to the previous AR after staying with the new AR only for a short while, so the prompt removal of state along the old path would cause the state to be re-established soon again, and therefore it adds overhead.

(6) Upstream State Update vs. Downstream State Update

Since the upstream and downstream paths are likely not to be the same, the upstream and downstream CRNs may not coincide, either. Therefore, the State Update needs to be handled independently for the upstream and the downstream, including the discovery of upstream and downstream CRNs.

(7) State identification problem

A mobility event typically causes the addresses of corresponding flow endpoints to change, and thus it is desirable that the signaling application state is independent of the underlying flows to avoid the state being re-installed completely. Therefore, the identifiers for the session and the flow must not be dependent on each other. This makes it possible to associate the session identifier with the signaling application and with different data flows.

(8) Double reservation problem

Since the state on the old path (and the common path) still remains as it is after re-establishing the state along the new path due to mobility (or route changes), the double reservation problem occurs. Although the state on the old path will be deleted automatically based on the soft state timeout, the refresh timer value may be quite long (e.g., 30s as a default value in RSVP). This problem might result in the waste of resources and lead to failure of other reservations (due to lack of resources). Note, however, that the degree of impact depends on the frequency of path changes and also on the chosen refresh interval.

(9) End-to-end signaling problem

The mobility may change the flow identifier, and the change of flow identifier requires state update along the entire path to reflect the physical location of the MN, resulting in the end-to-end signaling. This also incurs a long state setup delay and increased signaling overhead, which affects overall performance of signaling protocols. The long state setup delay may ultimately give rise to the service blackout or degradation of multimedia services in mobile environments.
Identification of the crossover node

When a handover at the edge of network has happened, in the typical case, only a part of the end-to-end path used by the data packets changes. In this situation, the CRN plays a central role in managing the establishment of the new signaling application state, and removing any useless state.

Key exchange

When a handover happens, nodes on the new path must be able to verify the signaling messages of the MN, and vice versa. For example, if signaling messages are encrypted on a hop-by-hop basis, the new access router should be able to continue the message encryption and decryption with the incoming MN.

Authorization Issues

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

3.2. Mobility-Related Issues with NSIS Protocols

Considering the issues identified in Section 3.1, this section discusses the concerns that arise for the NSIS protocols.

3.2.1. NTLP-Specific Problems

(1) Interfaces between Mobile IP and NSIS protocols

To continue to support the existing NSIS state for a session, the NTLP protocol should be immediately involved in the CRN discovery and State Update after a mobility event (e.g., handover) happens. Therefore, is might be necessary to develop a Mobile IP-specific API or reuse/extend existing APIs from Mobile IP (if applicable) in NSIS to learn quickly about mobility events at the NTLP and at the NSLP layer. Should a common triggering mechanism between routing and NSIS processes be defined to monitor the operations of other mobility protocols and trigger a relevant event accordingly?

(2) Localized State Update

The State Update needs to be localized to improve the performance metrics, such as signaling setup delay, resource utilization. A few issues on the interaction between the micro mobility management protocols and the NSIS protocol suite arise. For example, when interacting with HMIP, how is the Path Update performed with scoped signaling messages within the access network under the control of MAP?
3.2.2. QoS-NSLP-Specific Problems

(1) Invalid NR problem

If MN is receiver, it might be determined as the last QNE (QNR) on the signaling path [5]. If MN, however, moves into a new network attachment point, the old AR can not forward QoS-NSLP messages any further to the MN (QNR). In this case, the old AR's QoS-NSLP may trigger an error message to indicate that the last node fails or is truncated. This error message forwarded to QNI may mistakenly cause the removal of the state on the existing paths. It is called the 'invalid NR problem' [12]. This situation would not be desirable.

(2) Optimal refresh timer value for mobile environments

In the situation where handover occurs frequently, the maintenance of signaling state on the old path for a long time is not necessary. The QoS-NSLP needs to choose appropriate refresh intervals depending on the network environments (e.g., access network, or core network) or access technologies (e.g., 3G, IEEE 802.16, WLAN, etc.).

(3) Authorization-related issues with teardown

When tearing down the obsolete state after CRN discovery, can the teardown message be sent toward the opposite direction to the state initiating node? This leads to an authorization problem because a node which does not initiate signaling for establishing the NSLP state may delete the state. Please note that this authorization problem heavily depends on the design of the NSLP.

(4) Peering agreement issue

In the inter-domain handover scenarios, how is the peering agreement established for aggregate reservation and authorization to support individual sessions?

(5) Dead peer discovery

A dead peer can occur either because a link or a network node failed, or because the MN moved away without informing QoS-NSLP (it is recommended to link mobility and NSIS signaling such that this does not happen). How can dead peers be detected in a fast and efficient manner?

3.2.3. NAT/FW NSLP-Specific Problems

The NAT/FW-NSLP establishes and maintains firewall pinholes and NAT bindings at NAT/FW-NSLP nodes along the data path [10]. With regard to mobility, a few issues need to be considered:
(1) Update of firewall rules and NAT bindings

When an IP address changes by mobility, firewall rules and/or NAT bindings become invalid because the established flow identifier refers to a non-existent flow, which effectively blocks the end host's traffic. For example, without updating the firewall pinhole by an NSIS-aware data sender (located behind a firewall), data packets with a new source IP address are most likely dropped at the firewall. If a data receiver (located behind a NAT) changes its IP address, incoming packets are rewritten at the NAT and forwarded to the wrong IP address.

The impact of an outdated flow identifier is more severe in the NAT/FW case than in QoS case. In the latter case, the impact is only that the flow experiences best-effort treatment for a limited period of time (until the flow identifier is updated again). Here, do we need to add why the impact in the NAT/FW is more severe although some detailed description exists above?

(2) Re-use of NAT/FW-NSLP's old state

Although NSIS state can be released by applying the soft state principle after a mobility event, states (such as firewall pinholes) can be left in place for some time. Since the NAT/FW-NSLP aims to install pinholes (and NAT bindings), it is still possible to re-use this installed state although a mobile node roams to a new location. This means that another host can send data through a firewall without any prior NSIS NAT/FW signaling because of the previous state which is not yet expired. This might be a problem since an unauthorized end host might be able to inject packets through the firewall for a limited period of time. Deleting state along the old path might help to limit this problem. However, this problem exists anyway due to the capability of IP spoofing as identified in [7], and the main problem is the missing data origin authentication (i.e., missing cryptographic protection of data traffic).

3.2.4. Common problems related to both NTLP and NSLP

(1) CRN discovery-related issues

Which layer should be responsible for the CRN discovery, NTLP (GIST) or NSLP (QoS-NSLP or NAT/FW-NSLP)? Although the QoS-NSLP, for example, can detect the change of signaling path and discover the CRN by keeping track of SII, the CRN discovery at the NTLP layer may also be preferred to at the QoS-NSLP. Concerning CRN discovery, the pros and cons of two mechanisms on CRN discovery dependent on NSIS layers (i.e., either NTLP or NSLP) need to be identified.

(2) CRN discovery and State Update on the IP-tunneling path
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 IP-tunneling of Mobile IP, 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 state via interworking with the IP-tunneling operation.

(3) Issues on API between NTLP and NSLP

In mobile environments, mobility-related information for Path Update can be exchanged through the API specified in [2]. Based on the information, the involved NSLP can initiate State Update by sending necessary signaling messages through the API. However, what information should be sent from GIST to an NSLP to inform of the route changes needs to be discussed further. The details on the API can be an implementation issue.

(4) Multihoming-related issues

An NSIS-aware node (e.g., Mobile Node (MN)) may be multihomed. NSIS signaling can be used in such multihomed environments. In this case, which NXLP functionality is needed in various multihoming scenarios (e.g., bandwidth increase, load balancing, bi-casting, resilience, etc.) is an open question. An overall coordination for interworking between the NSIS protocol suite and multihoming capability needs to be discussed further.

4. Basic Operations for Mobility Support

In this section, the basic protocol interaction of the NSIS protocol suite needed after mobility related route changes is discussed. The basic operations include how to discover an appropriate CRN and how to perform the State Update according to the direction of data flows. The procedures for CRN discovery (explained in Section 4.2.3) can be applied in the same way for both the generic route changes and mobility. However, the State Update for mobility is different from that for the generic route changes as explained in Section 2.

4.1. Route changes caused by mobility

The route change caused by mobility occurs due to the change of the network attachment point of an MN. It causes divergence (or convergence) between the old path where the NSIS state has already been installed and the new path where data forwarding will actually
Although mobility may be considered similar to generic route changes, the main difference is that the Message Routing Information (MRI: e.g., flow identifier) may not change after generic route changes while mobility may cause the change of MRI by having a new network attachment point. Since the session should remain the same after any mobility event, the MRI should not be used to determine the session of any signaling application [4].

The route change brings on the change of signaling topology different from the mobility. That is, the route change results in forming a loop of signaling path that the old path and the new path meet both starting point and end point of the route change (i.e., divergence-convergence pair) (see Appendix). However, as shown in Figure 1, the mobility generally causes signaling path to either converge or diverge depending on the direction of each signaling flow.

(a) The topology for downstream NSIS signaling flow due to mobility
(b) The topology for upstream NSIS signaling flow due to mobility

Figure 1: The topology for NSIS signaling caused by mobility.

These topological changes caused by mobility make the NSIS state
established on the old path useless and thus it should be removed (in the end). In addition, NSIS state should be established newly along the new path and be updated along the common path.

Re-establishment of NSIS signaling should be localized when route changes (including mobility) occur to minimize the impact on the service and to scalability. This localized signaling procedure is referred to as PathUpdate (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 section of the signaling path because the path in the wireless access network usually changes only partially.

One of the most appropriate nodes to perform the State Update is the CRN where the old and new session paths meet. The CRN should be logical merging point, physical merging point. In the end, CRN discovery can be a crucial element to alleviate the double reservation and end-to-end signaling problems identified in Section 3.1.

The NTLP (of a node experiencing a topological change) should detect the route change through the various mechanisms described in [4] at the transport level and notify the relevant NSLP(s). For example, the NSLP should initiate NSIS state re-establishment (i.e., QoS re-establishment) along the new path and the update or removal of the existing state at the signaling application level.

4.2. CRN discovery

4.2.1. Possible approaches for CRN discovery

The approaches for CRN discovery can be divided into two classes depending on which layer is responsible for the CRN discovery (addressed in Section 3.2.2), and whether or not the discovery is coupled with the transport of signaling application messages.

From the NSIS protocol stack point of view, the CRN can be discovered at either NTLP or NSLP layer. For the CRN discovery at the NSLP layer, the information contained in NSLP signaling messages sent from
the NSIS initiator (NI) can be used. For example, the QoS-NSLP of an
NSIS node can determine whether or not the node is a CRN by comparing
the Source Identification Information (SII) contained in the incoming
signaling message to the one stored previously in the node. That is,
when a RESERVE message with an existing SESSION ID and different SII
is received, the QNE knows its upstream peer has changed and realized
it is implicitly the CRN [5].

It is also possible to discover the CRN at the NTLP layer since NTLP

is responsible for detecting the path change of data (or signaling)
flow (and the route changes may easily be detected at the NTLP level
rather than at the NSLP). The CRN discovery at the NTLP level can be
considered as a partial process of the peer discovery (e.g. using
GIST query-response message [2]). In general, the GIST messages have
message routing state information such as flow/session/signaling
application identifiers, so the signaling application can be
identified at the NTLP level. In the connection mode of NTLP, when
NTLP establishes a messaging association between two adjacent peers,
two NTLP peers exchange message routing state information through
GIST query and response messages. In procedure of the messaging
association, CRN is implicitly discovered by comparing MRI contained
in the coming signaling to the one stored previously in the node.
Therefore, although the CRN can be discovered at the NTLP level, the
discovered CRN could be actually an NSLP-aware node which has an
involved signaling application.

The CRN discovery at the NTLP layer is only one part of peer
discovery procedure, and it does not require any explicit process for
CRN discovery itself except for GIST notification on the information
('CRN-is-discovered to NSLP') to NSLP over API. The NTLP level
approach results in decreasing complexity of overall NSIS protocol
processing. If a route change is directly detected by NSLP, the CRN
discovery at the NSLP layer is considered as a way to report the
rerouting. However, this NSLP-level approach requires additional
messages at corresponding NSLPs and thus results in adding complexity
of overall NSIS protocol processing.

There can also be two different approaches for the CRN discovery
depending on whether or not the discovery is coupled with a signaling
message: coupled approach and uncoupled approach. In the coupled
approach, the signaling to install the NSIS state along the new path
or update the state along the common path is performed simultaneously
with the CRN discovery. In the uncoupled approach, the signaling for
the State Update is performed after the CRN discovery is completed.
These two approaches may differ in terms of security. Generally, the
coupled approach would be preferred to the uncoupled approach to
reduce the delay for state update. Note that the CRN discovery and
State Update described in this draft are based on the coupled
approach.

4.2.2. The identifiers for CRN discovery
There are some basic identifiers which can be used for the CRN discovery at the NTLP level: session identifier (SID), flow identifier (MRI), and signaling application identifier (NSLP_ID) related to message routing state [2], and NSLP branch identifier (NSLP_Br_ID) which identifies an NSIS signaling branch.

The SID in GIST messages is used to identify the involved session because it remains the same while the MRI may change. The MRI is used to specify the relationship between the address information and the state (e.g., QoS-NSLP state) re-establishment. In other words, the change of MRI indicates a topological change to the CRN and therefore it represents that the state along the common path should be updated and the refresh reduction mechanism needs to be used on the common path if any.

The NSLP_ID is used to refer to the corresponding NSLP at the NTLP level, and it helps to discover an appropriate NSLP CRN using the GIST peer discovery message.

As a virtual branch identifier, the NSLP_Br_ID is a pointer which identifies peer nodes in GIST messaging association, and it can be used to establish or delete messaging associations between NSIS peers. It can also be used as an identifier to determine the CRN at the NTLP layer. The NSLP_Br_ID may include the location information of NSIS peer nodes with the corresponding NSLP ID obtained by the procedure of GIST message association. For instance, as shown in Figures 1 (b) and 2 (a), for the upstream flow case, node A has messaging association with node C for NSLP 1 on the old path. In this case, the NSLP_Br_ID for node C at the node A is set to 1-D-#1: 1, D, and #1 indicate an NSLP_ID-flow, a direction of node (Downstream or Upstream), and a value of the branch counter, respectively. After a handover, NSLP 1 of node A requires a messaging association for sending its messages towards node D. In this case, NSIS entity A creates another NSLP_Br_ID for NSLP 1 toward node D and increases the counter of NSLP_Br_ID to locally distinguish each virtual interface identifier between adjacent NSLP peers: the [NSLP_Br_ID for the node D at the node A is 1-D-#2:]. Note that the NSLP_Br_ID can be included in the NSIS message, but it can also be considered as an implementation issue. This identifier would be more useful when the physical merging point of the old path and the new path is not an NSLP CRN as shown in Figure 1. Note that GIST message routing state table [2] including the NSLP_Br_ID can also be created as Figure 2.

Optionally, the Mobility identifier as an object form can also be used to inform of the handover of an MN or a route change [12] and therefore to expedite the CRN discovery. The Mobility object is defined in the NTLP (e.g., in GIST payload) [8] or NSLP messages to notify of any mobility event explicitly, and it contains various mobility-related fields such as mobility_event_counter (MEC) and handover_init (HI) fields. For example, the mobility_event_counter
The Mobility identifier is useful to discover the most appropriate CRN.

<table>
<thead>
<tr>
<th>Message Routing Information</th>
<th>Session ID</th>
<th>NSLP ID</th>
<th>Upstream Peer</th>
<th>Downstream Peer</th>
<th>NSLP Br. ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method = Path Coupled; Flow ID = {IP-#X, IP-#V, protocol, ports}</td>
<td>0xABCD</td>
<td>NSLP1</td>
<td>Pointer to A-C</td>
<td>Pointer to A-D</td>
<td>1-D-#1</td>
</tr>
<tr>
<td>Method = Path Coupled; Flow ID = {IP-#X, IP-#V, protocol, ports}</td>
<td>0x1234</td>
<td>NSLP2</td>
<td>Z</td>
<td>B</td>
<td>1-U-#1</td>
</tr>
</tbody>
</table>

(a) Routing state table at node A (NSLP CRN)

<table>
<thead>
<tr>
<th>Message Routing Information</th>
<th>Session ID</th>
<th>NSLP ID</th>
<th>Upstream Peer</th>
<th>Downstream Peer</th>
<th>NSLP Br. ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method = Path Coupled; Flow ID = {IP-#X, IP-#V, protocol, ports}</td>
<td>0xABCD</td>
<td>NSLP1</td>
<td>Pointer to K-N</td>
<td>Pointer to L-N</td>
<td>1-U-#1</td>
</tr>
<tr>
<td>Method = Path Coupled; Flow ID = {IP-#X, IP-#V, protocol, ports}</td>
<td>0x1234</td>
<td>NSLP2</td>
<td>M</td>
<td>Pointer to N-R</td>
<td>2-U-#1</td>
</tr>
</tbody>
</table>

(b) Routing state table at node N (NSLP CRN)

Figure 2 Routing state table and NSLP branch ID

4.2.3. The procedures of CRN discovery

When a mobility event occurs, the CRN can be recognized by comparing the previously stored identifiers with the identifiers included in the incoming NSIS peer discovery message initiated by an NI (e.g., an MN or a CN). For example, if an NTLP message is routed to an NSIS peer node, the following information (shown in Figure 2 (a) and (b))
should be checked to determine if the current node is CRN:

- Whether or not the same NSLP_ID exists
- Whether or not the corresponding CRN has already been discovered
- Whether or not the same SID and MRI exist
- Whether or not the NSLP_Br_ID has been changed: for example, as shown in Figure 2 (a), for NSLP 1 it has been changed to 1-D-#2 from 1-D-#1 at the node A.
- Optionally, the Mobility identifier can be examined, if any. For example, the MEC field of the Mobility object can be used to find out which message has been sent due to the latest handover.

The CRN discovery can be further divided into the UCRN discovery and DCRN discovery depending on which node is a signaling initiator (by upstream or downstream), or whether the MN is the data sender or receiver:

- If the MN is a data sender and undergoes a handover, the MN begins to transmit signaling messages toward a CN in the downstream direction. If an NSLP-aware node recognizes that the session paths logically converge at that node, then the node determines that it is the DCRN; the procedure for CRN discovery corresponds to the creation of the routing table of node N as shown in Figure 2 (b).

- When an MN (as a sender) undergoes handover, the UCRN can be discovered for the upstream flow. The UCRN should be the node (closest to the MN) where the signaling flow begins to logically diverge: it corresponds to the creation of the routing table of node A as shown in Figure 2 (a). Since the UCRN is determined according as depending on whether the outgoing logical interfaces diverge or not, the UCRN discovery is more complex than the DCRN discovery and needs to be discussed further.

4.3. State Update

The CRN discovery procedures are different depending on the direction of signaling flows in mobility scenarios, and therefore the procedures for State Update also are different according to the direction of the signaling flow. The State Update can be divided into upstream State Update and downstream State Update. For both types of State Update, the NSIS protocol suite may need to interact with various mobility signaling protocols, if any (during or after handover) to obtain performance gains (e.g., through fast
establishment of the NSIS state on the new path). For this purpose, NSIS may also need to monitor the movement of the MN through several methods [4]. In this section, we assume that an MN is the data sender.

4.3.1. State setup and update

Before initiating the State Update, the MN or the CN need to have its session ownership by the procedures for authentication and authorization. The MN or the CN may also check the availability of resources on the new path. In case of QoS-NSLP, the Query message can be used to find the availability of resources in the new access network. If the resources along the new path are not sufficient, it may be needed to keep the state established previously using multihomed interfaces while blocking incoming new requests (see Section 5.2). In this situation, providing NSIS signaling for the State Update over local requests for the resources will be helpful for seamless service. The admission control for the State Update should prefer to admit an existing NSIS state.

In the downstream State Update, if resources are available, the MN initiates the NSIS signaling for state setup toward a CN along the new path and the implicit DCRN discovery is performed by this type of signaling as described in Section 4.2.3. When the DCRN is discovered, it sends a response message towards the MN to notify of the NSLP state installed (e.g., QoS-NSLP state) or installs the NSLP state as a response to the initiated NSLP signaling (e.g., as in RSVP). In case of QoS-NSLP, the sender-initiated approach leads to faster setup than the receiver-initiated approach as in RSVP as shown in Figure 3. And afterward, the DCRN sends a refresh message towards the signaling destination to update the MRI on the common path and also sends a teardown message towards the old AR to delete the NSIS state (if possible).

In the case of upstream State Update, the CN (or a HA/ a GFA/MAP) sends a refresh message toward the MN to perform State Update. UCRN is discovered implicitly by the CN-initiated signaling along the common path as described in Section 4.2.3. In this case, the CN should be informed of the mobility event using an NSIS signaling message sent by the MN or monitoring the mobility signaling procedure (e.g., detecting a change in its binding entry (see Section 5.1)). After the UCRN is determined, it may send a refresh message to the MN along the new path while establishing the messaging association between the newly found peers. Afterwards, the UCRN may send a teardown message towards the old AR to delete the NSIS state (if possible).
The state update on the common path to reflect the changed MRI brings issues on the end-to-end signaling addressed in Section 3.1. Although the state update 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 (in QoS signaling) on the common path as described in Section 3.1. 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/flow identifier. In this case, the NSLP state should be shared for flows with different flow identifiers.
After establishment of the NSIS state along the new path, the state on the obsolete path needs to be quickly removed by the Path Update mechanism to prevent the waste of resources due to double reservation (and resource allocation problem by call blocking) and to reduce the cost of using resources in the access network as identified in Section 3.1. Although the release of the existing state on the old path can be accomplished by the timeout of soft state, the refresh timer value may be quite long to reduce the overhead of signaling messages. Especially, in mobility scenarios, the maintenance of the NSIS state on the old path for a long time is not necessary. Therefore, the transmission of a teardown message is useful to quickly delete the old state. 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 [2].

The CRN is an appropriate point to initiate the teardown toward the old AR after establishment of the state along the new path. The release of the state on the obsolete path can be accomplished by comparing the NSLP_Br_IDS and through reverse routing using SII. This can prevent the teardown message from being forwarded toward along the common path.

It may not be desirable to allow the teardown message to be sent toward the opposite direction to the state initiating node. This is because it leads to an authorization problem because a node which does not initiate signaling for establishing the NSIS state can delete the already established state. One simple way to avoid the authorization problem is to disallow the transmission of the teardown message in the reverse direction [7].

The immediate removal of state along the old path may not be always appropriate for some mobility situations addressed in Section 3. For instance, in the ping-pong type of fast handover, it increases signaling overhead, and thus when to delete the state along the obsolete path needs to be discussed further (see Section 5.4). Another example is the 'invalid NR' problem. If the old AR is the last node on the signaling path due to handover, its NSLP may trigger an error message to indicate that NSLP messages cannot be forwarded any further. This error message can immediately remove the state on the old path, which should not be deleted before re-establishing the state along the new path (make-before-break handover). More details are given in Section 5.5.

5. Applicability Statement
IPv6 [11]. Basically, the following scenarios need to be considered.

(1) A flow associated with an MN, either sent or received by the MN, desires to continually get signaling services even after a Mobile IP handover. In this case, NSIS needs to be able to signal for such flows upon the MN's movement to provide seamless service (e.g. seamless QoS). The signaling procedures will create a new NSIS state branch in the changed direction of flow by using the CRN discovery and State Update.

(2) Either the sender or the receiver (e.g., MN or CN) of a flow can initialize NSIS signaling, and a node within the network (e.g., FA, HA, or CRN) may also initiate NSIS signaling for the given session to handle route changes caused by Mobile IP-based routing, interact with Mobile IP tunneling, or to support seamless handover if necessary. In this case, NSIS signaling needs to be triggered immediately. initiated via a mobility routing interface (e.g., mobility API) between the NSIS protocol and the Mobile IP or by the query routing tables.

(3) Signaling flows, in either direction between an MN and a CN, can be routed directly using a routing header, or indirectly by IP-in-IP encapsulation (or a combination of both approaches) on different segments of the data path depending on the operation of the mobility protocol (e.g., Mobile IPv4, Mobile IPv6, LMM, reverse tunneling, etc.). In this case, the IP-tunneling mechanism makes it difficult for nodes on the tunneling path to intercept or deal with NSIS signaling messages (which require special treatments at NSIS-aware nodes) because of change of message routing information. Therefore, to perform end-to-end signaling, NSIS needs to interact with such IP-tunneling mechanisms.

(4) An MN undergoes either intra-domain (within an access network domain) handover or inter-domain (from an access network domain to another) handover. In case of the inter-domain handover, topology information exchange, authorization and accounting issues may be more complicated. In such various handover scenarios, the interaction between NSIS signaling and some local mobility management protocols (e.g., HMIP, FMIP, etc.) may give rise to significant performance gains (see Section 5.3).

(5) With Mobile IPv6, an MN can support multiple CoAs simultaneously, if it is connected to multiple access networks simultaneously (even if it is connected to one access network). Although only one primary CoA will be used for routing traffic from the CN to the MN, this multi-homing feature potentially can be used to enhance the NSIS signaling performance (see Section 5.2).

5.1.1. Interfaces between Mobile IP and NSIS
As the NSIS WG concentrates on path-coupled signaling, one imposed requirement here is that the NSIS protocols are to be associated with route changes to support route optimization between the CN & the MN, and the IP-in-IP encapsulation from the HA to the MN. This interaction needs to be notified to all NSLPS (by the API between GIST and NSLP) for the CRN discovery and the State Update. Therefore, either NTLP or NSLP needs to have an interface with the Mobile IP to immediately react to the mobility event. In other words, an NSIS implementation needs to be developed to react on mobility events based on the endpoint notification depending on which behaviour of a mobility protocol has taken place (e.g., the timer of Mobile IP expires).

An ideal interface between the NSIS signaling and the Mobile IP should make it possible for NSIS signaling to immediately react to the mobility event whenever Mobile IP changes its related characteristics in any place for the flows. In general, it is appropriate that NTLP is involved in the interaction with Mobile IP rather than NSLP because NTLP is responsible for routing NSIS messages. Therefore, it is reasonable to assume NTLP should be able to notify NSLP for the necessity of state update over API between NTLP and NSLP when the mobility events are detected.

The following issues also arise concerning the API between the NSIS protocol and the Mobile IP.

- Which information should be used to detect the movement? After an MN moves to a new network attachment point, the new reachability information is transferred from the MN to its HA as the last procedure of handover. This procedure indicates that the NTLP may need to interact with a binding process (e.g., a registration request in Mobile IPv4 and Binding Update in Mobile IPv6) to detect the IP address change and refer to the tunneling-related information. Provided that the NTLP detects the mobility using the information regarding binding process, faster state establishment and removal can be performed. However, in the fast or ping-pong type handover, it may result in significant signaling overhead and some possible errors (see Section 5.4).

- How and what information can the NSLP expect from NTLP, or directly from the routing interface after a mobility event happens?

- How is the mobility binding update interval coordinated with the NSIS signaling interval? Since the binding update or the registration request occurs periodically even for the MN with the same point of attachment, the movement detection based on the binding process may cause the NTLP/NSLP to initiate the CRN discovery and the State Update inappropriately. To avoid the problem, the change of CoA should be checked carefully. Although this issue is closely related to implementation, it should be
An overall coordination/synchronization for the interworking between the NSIS and the Mobile IP needs to be discussed further.

5.1.2. Mobile IPv4-specific issues

With Mobile IPv4, the data flows are forwarded based on the triangular routing, and an MN retains a new CoA from the FA (or an external method such as DHCP) in the visited access network [5]. When the MN acts as a sender, the downstream data flows sent from the MN are directly transferred to the CN not necessarily through the HA or indirectly through the HA using the reverse routing. On the other hand, upstream data 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 needs to interact with the IP tunneling procedure of Mobile IP for signaling.

Note that in QoS-NSLP scenarios, if MN is a sender and its Mobile IPv4 protocol stack uses triangular routing mechanism, the receiver-initiated approach is not suited to establish the QoS states over the Mobile IPv4. For reason of this, the path of QUERY messages directly sent from an MN to a CN (as shown in Figure 4 (a)) is not identical with that of RESPONSE messages, as response of QUERY, forwarded via HA from the CN to the MN (as shown in Figure 4 (d) or (e)). Therefore, in this case, the Mobile IP should use the reverse tunneling mechanism and the QUERY messages need to be forwarded over reverse tunneling from FA to HA (as shown in Figure 4 (b) or (c)). On the other hand, since in the sender-initiated approach, RESERVE messeges travel in the same direction as data flow without any QUERY message to establish the desired QoS states, this approach can be used for both triangular routing and reverse tunneling mechanisms.

The Figures 5 (a) to (e) show the NSIS signaling flows depending on the direction of data flows and the routing methods.

---

<table>
<thead>
<tr>
<th>MN</th>
<th>FA (or FL)</th>
<th>CN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IPv4-based Standard IP routing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>(a) MIPv4: MN--&gt;CN, no reverse tunnel</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>MN</th>
<th>FA</th>
<th>HA</th>
<th>CN</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 (normal)</td>
<td>IPv4(tunnel)</td>
<td>IPv4 (normal)</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td>-----------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Internet-Draft NSIS Signaling in Mobility October 2005
Concerning CRN discovery and State Update, the following signaling procedures occur dependent on the direction of signaling flows, either downstream or upstream signaling flow.

When an MN (as a sender) arrives at a new FA and the corresponding binding process for the FA CoA is completed,

- For the downstream signaling flow, the MN needs to perform the CRN discovery (DCRN) and the (downstream) 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 as shown in Figure 4 (a). If the reverse tunnel is used and the state along the tunneling path does not exist, the NSIS state should be established along the tunneling path from the FA to the HA as shown in Figure 4 (b). In this case, a DCRN may be discovered on the tunneling path and the new flow identifier for the state update on the tunnel may need to be created. That is, signaling flows over the tunnel are considered as separated flows and thus the tunnel endpoints can initiate a new signaling session for the flow over the tunnel (see Section 5.1.3).
- For the upstream signaling flow, the CN may initiate the NSIS signaling to update the existing state between the CN and the HA, and afterwards HA forwards the NSIS signaling to FA. In this case, NSIS signaling should interact with the IP tunneling operation to update the state along the tunneling segment from the HA to the FA as shown in Figure 4 (d). During this operation, a UCRN may be discovered on the tunneling path, and the new flow identifier for the state update on the tunnel may need to be created.

When the MN (as a sender) arrives at a new foreign link (FL) and the corresponding binding process for the co-located CoA is completed,

- For the downstream signaling flow, the NSIS signaling for the DCRN discovery and the State Update is the same as the case for FA CoA above except for the use of the reverse tunnel path from the MN to the HA as shown in Figure 4 (C). That is, in this case, one of tunnel end points is to be the MN, not the FA.

- For the upstream signaling flow, the NSIS signaling for the UCRN discovery and the State Update is also the same as the case for FA CoA above except for the end point of tunneling path from the HA to the MN as shown in Figure 4 (e).

Note that the DCRN and UCRN may be identified at the same node on the tunneling path of Mobile IP. For example, NSIS CRN may be usually the HA if the HA and the FA are NSIS-aware but the NSIS signaling over the tunneling path is not coped with. Therefore, the CRN discovery will be affected depending on the type of interaction between NSIS signaling and IP tunneling. The FA and the HA should be NSIS-aware to do the State Update along the appropriate path. The effect that the IP tunneling has on the CRN discovery and the State Update should be discussed in Section 5.1.3.

5.1.3. Mobile IPv6-specific issues

Unlike Mobile IPv4, with Mobile IPv6, the FA is not required in the data path and the route optimization process between the MN and CN can be used to avoid the triangular routing in the Mobile IPv4 scenarios as shown in Figure 5 [9]. If the use of route optimization is not mandatory, 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 described in Section 5.1.2.

In Mobile IPv6-based scenarios, the non-existence of FA depicts the endpoint of IP-tunneling is extended to the MN. If the MN is a sender and route optimization is optional, it should initiate both tunnel signaling session and end-to-end signaling session by using reverse tunneling. In this case, HA as another tunnel endpoint needs
to react on the tunnel signaling messages and to forward the end-to-end NSIS signaling messages to the CN. However, if the route optimization in Mobile IPv6 is used as mandatory, NSIS signaling is not necessary to interact with IP-tunneling any more. It also means that NSIS signaling should not be initiated simultaneously with Binding Update messages.

Concerning CRN discovery and State Update, the following signaling procedures occur dependent on the direction of signaling flows, either downstream or upstream signaling flow.

When an MN (as a sender) arrives at a new AR and the binding process is successfully completed, 

- For the downstream signaling flow, the MN initiates NSIS signaling for the DCRN discovery and the (downstream) State Update to establish the state along the new optimized path between the MN and the CN as shown in Figure 5 (a). On the other hand, the MN initiates tunnel NSIS signaling for DCRN discovery and the State Update over the tunneling path from the MN to the HA if the reverse tunnel is used, as shown in Figures 5 (b). In this case, CRN discovery over tunnel can be performed as the same approach described in Section 4.2 and more detailed considerations are described in Section 5.1.3.

- For the upstream signaling flow, the CN may also update the state along the common path toward the HA through the State Update, and afterward the NSIS state along the tunneling segment from the HA to the MN may be updated via the interaction with IP tunneling operation as shown in Figure 5 (d). In this case, the HA needs to create a new NSIS tunnel signaling toward the MN as the tunnel endpoint for UCRN discovery and the State Update. The obsolete path of the existing tunneling segments needs to be removed after re-establishment of NSIS state along the new tunneling path. When to remove the tunneling segment and/or how to tear it down through the interworking with the IP-tunneling operation is still an open issue. However, if the route optimization is used between the CN and the MN, for the upstream flow, CN needs to newly initiate end-to-end NSIS signaling to discover an appropriate UCRN and do the State Update along a new path between the CN and the MN as shown in Figure 5 (c): the bidirectional state establishment may be required between the CN and the MN.

```
MN                                            CN
|                               |                                      |
IPv6+HomeAddressOpt             |                                      |
--------------------------------->|
|IPv6+HomeAddressOptOpt         |
(a) MIPv6: MN-->CN, no reverse tunnel
```
As described in Section 5.1.2, interaction scenarios with Mobile IP tunneling can vary dependent on

(i) Whether version of IP mobility management protocol is Mobile IPv4 or Mobile IPv6,

(ii) Whether mode of QoS-NSLP signaling is sender-initiated or receiver-initiated,

(iii) Whether signaling mode over tunnel is sequential or parallel.

(iv) Whether tunnel signaling supports per-flow or per-aggregate approach.

In Mobile IPv4 scenarios, Mobile IP stack of an MN can use direct routing or reverse tunneling to send data flows from the MN itself to its CN. If sender-initiated approach for the mode of QoS-NSLP signaling is used and also MN is a sender, both the direct routing and reverse tunneling can be used to perform QoS-NSLP signaling. However, if receiver-initiated approach is used, delivery of QoS-NSLP signaling messages can only be available in using reverse tunneling.

However, in Mobile IPv6 scenarios, route optimization or bi-...
directional tunneling is utilized to transport data flows between MN and CN. In interaction scenarios with Mobile IPv6 tunneling, consideration on bi-directional tunneling needs to be taken into, that is, both sender-initiated and receiver-initiated modes only use the reverse tunneling to forward signaling flows from the MN to the CN to interwork with tunneling and solve the ingress filtering-related problem.

In this section, we assume that MN acts as a sender and CN runs as a receiver in interworking scenarios between Mobile IP and NSIS signaling.

5.1.4.1. Interaction scenarios with Mobile IPv4 tunneling

The procedure of NSIS-tunnel signaling in Mobile IPv4-based scenarios is as follows.

In case of that QoS-NSLP operates under the sender-initiated approach, after MN moves into a new network attachment point, QoS-NSLP over MN initiates RESERVE (end-to-end) message to start the State Update procedure. GIST below the QoS-NSLP adds GIST header and then sends the encapsulated RESERVE message to peer GIST node with corresponding QoS-NSLP for DCRN discovery. In this case, the peer

GIST node is a FA if the FA is an NSIS-aware node. The FA is one of endpoints of Mobile IP tunneling: Tentry. Concerning interaction scenarios with tunnel signaling originated from the FA, two scenarios can be considered dependent on whether NSIS signaling interacts with the Mobile IP tunneling: One is that the NSIS signaling is discerned on the tunneling path between the FA and corresponding HA, and then the tunneling path becomes an NSIS-aware cloud. Another is otherwise, and here the tunneling path is transparent as a logical link to NSIS signaling [19].

In the NSIS-aware tunneling scenarios, receiving the RESERVE State Update message from the MN, the QoS-NSLP of FA explicitly creates a new RESERVE-t (tunnel) message, which keeps the existing (end-to-end) Session ID and includes a new (tunneling) Flow ID different from the (end-to-end) flow ID, to distinguish the NSIS signaling messages over the Mobile IPv4 tunneling path. The RESERVE-tunnel message is forwarded toward HA as another end point of Mobile IPv4 tunneling and just valuable on the tunneling path between the FA and the HA. Also, receiving the RESERVE-tunnel message from the FA, the HA should decide whether it initiates a RESPONSE-tunnel message toward FA reacting to the RESERVE-tunnel message, or make the RESPONSE-tunnel message wait until a RRESPONSE message, which is created to react the RESERVE message, from the CN arrives.

In this procedure of NSIS-tunnel signaling, again, consideration on two categories of tunnel signaling mode is taken into, either sequential or parallel mode. On the one hand, provided that the tunnel signaling mode is sequential, the RESERVE signaling toward the
HA is resumeed after confirming completeness of NSIS tunnel signaling through the RESERVE- and the RESPONSE-tunneling signaling messages as shown in Figure 6. Arriving at HA, the RESERVE message is forwarded to CN to update or refresh the existing NSIS states (QoS-NSLP and GIST) on common path. The CN initiates RESPONSE message, responding to the RESERVE message, toward the HA as its destination, and afterwards the HA forwards the RESPONSE message to FA after encapsulating the message. Finally, FA sends the RESPONSE message to MN after decapsulating it. Note that both end-to-end signaling messages, the RESPONSE and the RESERVE messages are not discernable on the tunneling path, as like a logical link, and those messages play a role of NSIS signaling for the establishment of end-to-end state.

In this case, concerning CRN discovery in the sequential mode of tunnel signaling, CRN discovery on the tunneling path is reconciled with that over end-to-end path. That is, the CRN caused by mobility is discovered just one time between the FA and the HA. This can be possible by using the 'CRN_DISCOVERY (CD) flag bit' mentioned in Section 4.2.3. Since tunnel signaling in the first place is performed, the FA can set the 'CD flag bit' in the RESERVE message, to address that already CRN is discovered for forward direction, if the CRN is already discovered over the tunnel path through NSIS-tunnel signaling messages. Therefore, CRN discovery by end-to-end NSIS signaling is not performed any more.

After the CRN is discovered successfully on the tunneling path, the CRN can perform the State Update procedure. If the CRN on the tunneling path teardowns the state on the old path, the CRN may initiate RESERVE-tunnel message toward the FA.

![Diagram of NSIS signaling in Mobility]
On the other hand, provided that tunnel signaling mode is parallel, receiving the RESERVE message from the MN, the FA forwards it to the HA at the drop of a hat. Also, arriving at the HA from the CN, the RESPONSE message is again forwarded from the HA to the FA regardless of the delivery of RESPONSE-tunnel message as shown in Figure 7. Since in this parallel mode the end-to-end signaling messages do not reconcile with both NSIS-tunnel signaling messages, the RESERVE- and RESPONSE-tunneling messages, the tunneling path operates as like a logical link and thus NON-QoS-HOP flag is set within the RESERVE message although NSIS-tunnel signaling messages are available on the tunnel path.

Concerning CRN discovery in the parallel mode of tunnel signaling, CRN discovery on the tunneling path is not reconciled with that over end-to-end path. That is, the CRN caused by mobility is discovered through tunnel signaling and end-to-end signaling messages, respectively. For CRN discovery through the tunnel signaling messages, the CRN is discovered over the tunneling path from the FA to the HA, which the discovered CRN between the FA and the HA sets the 'CD flag bit'. However, for the CRN discovery through the end-to-end signaling messages, the CRN is ferreted at HA provided that the HA is an NSIS-aware node, which the HA sets the 'CD flag bit' in RESERVE message. Note that the first crossover node on the end-to-end signaling path is the HA because the tunneling path is considered as a logical link for the end-to-end signaling messages.

Provided that the CRN is discovered successfully on the tunneling path, the CRN can perform the State Update procedure. In order to teardown the state on the old path, the CRN discovered on the tunneling path may be able to initiate RESERVE-tunnel message toward the FA. Also, the CRN discovered by the end-to-end signaling messages (e.g., HA) can perform the State Update procedure to remove the old state from itself to FA.
Concerning QoS-NSLP signaling mode, provided that QoS-NSLP operates under the receiver-initiated approach, QoS-NSLP over MN initiates QUERY message to start the State Update procedure after MN moves into a new network attachment point. GIST below the QoS-NSLP adds GIST header and sends the encapsulated QUERY message to peer GIST node with corresponding QoS-NSLP. In this case, the peer GIST node is a FA as one of endpoints of Mobile IPv4 tunneling (Tentry). Two scenarios can be considered dependent on whether NSIS signaling interacts with the Mobile IPv4 tunneling: One is that the NSIS signaling is discerned on the tunneling path between the FA and the HA, and then the tunneling path becomes an NSIS-aware cloud. Another is otherwise, and here the tunneling path is shown as a logical link to NSIS signaling.

In the NSIS-aware tunneling scenarios, receiving the QUERY message from the MN, the FA just transfers it toward the HA unlike receipt of the RESERVE message, and then the HA sends the QUERY message to its CN. As reacting to QUERY message, CN initiates the RESERVE message toward the HA to update or refresh the existing NSIS states (QoS-NSLP and GIST) on common path, and afterwards the HA forwards it toward the FA. After the receipt of the RESERVE message, the FA as Tentry begins to perform the NSIS-tunnel signaling as shown in Figures 8 and 9. Moreover, receiving the RESERVE message from the HA, the FA should decide whether it forwards the RESERVE message toward MN irregardless of procedure of NSIS-tunnel signaling, or make delivery of the RESERVE message be postponed until all the procedures of NSIS-tunnel signaling are completed.

In this procedure of NSIS-tunnel signaling, again, consideration on two categories of tunnel signaling mode is taken into, either sequential or parallel mode. On the one hand, provided that the
tunnel signaling mode is sequential, the RESERVE signaling forward
the MN is transferred after confirming completeness of NSIS tunnel
signaling through the Query-, the RESERVE-, and the RESPONSE-tunnel
signaling messages as shown in Figure 8. Concerning the procedure of
NSIS-tunnel signaling, receiving the RESERVE message from the HA, the
QoS-NSLP of FA creates a new QUERY-tunnel message, which keeps the
existing (end-to-end) Session ID and includes a new (tunneling) Flow
ID different from the (end-to-end) Flow ID, to interact with Mobile
IPv4 tunneling. The QUERY-tunnel message is forwarded toward HA as
Texit. Also, receiving the QUERY-tunnel message, the HA initiates
RESERVE-tunnel message, responding the QUERY-tunnel message, toward

Concerning CRN discovery in the sequential mode of tunnel signaling,
CRN discovery on the tunneling path is not reconciled with that over
end-to-end path unlike sender-initiated mode of QoS-NSLP. That is,
firstly, the CRN caused by mobility is discovered at the HA through
the end-to-end signaling (e.g., RESERVE message), which the HA sets
the 'CD flag bit' in the RESERVE message. Next, the tunnel CRN is
discovered at a certain tunnel node between the HA and FA, which the
CRN discovered at any node over the tunnel path sets the 'CD flag
bit' in the RESERVE-tunnel message.

In this case, the procedure for the removal of the state on the old
path is identical with the case of the parallel tunnel signaling mode
in sender-initiated QoS NSLP signaling.

<table>
<thead>
<tr>
<th>MN (Sender)</th>
<th>FA (Tentry)</th>
<th>Tnode</th>
<th>HA (Texit)</th>
<th>CN (Receiver)</th>
</tr>
</thead>
<tbody>
<tr>
<td>QUERY</td>
<td>QUERY</td>
<td>RESERVE</td>
<td>QUERY</td>
<td>RESERVE</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td>--------</td>
<td>-----------</td>
<td>---------------</td>
</tr>
<tr>
<td>+------------+-----------</td>
<td>--------+-----------+---------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QUERY-t</td>
<td>QUERY-t</td>
<td>RESERVE-t</td>
<td>RESPONSE-t</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>--------</td>
<td>-----------</td>
<td>---------------</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>-------</td>
<td>-----------</td>
<td>---------------</td>
</tr>
</tbody>
</table>
Sequential Mode

On the other hand, provided that tunnel signaling mode is parallel, receiving the RESERVE message from the HA, the FA forwards it to the MN at the drop of a hat. After receiving the RESERVE message from the FA, the MN forwards the RESPONSE message to the HA via FA regardless of the delivery of RESPONSE-tunnel message as shown in Figure 9. Since in this parallel mode the end-to-end signaling messages do not reconcile with both NSIS-tunnel signaling messages, the RESERVE- and RESPONSE-tunneling messages, the tunneling path operates as like a logical link and thus NON-QoS-HOP flag is set within the RESERVE message although NSIS-tunnel signaling messages are available on the tunnel path.

Concerning CRN discovery in the parallel mode of tunnel signaling, CRN discovery on the tunneling path is not also reconciled with that over end-to-end path as like the sequential mode of tunnel signaling. That is, all the procedure of CRN discovery is identical with the sequential mode of tunnel signaling. In this case, the procedure for the removal of the state on the old path is also identical with the case of the sequential tunnel signaling mode in receiver-initiated QoS NSLP signaling.
5.1.4.2. Interaction scenarios with Mobile IPv6 tunneling

In Mobile IPv6-based scenarios, tunneling path is further extended to MN from HA unlike the Mobile IPv4-based. That is, the MN as one of the end points of tunneling path is in charge of most functionalities of FA. All the procedures of State Update in interaction with Mobile IPv6 is similar to those in interaction with Mobile IPv4 except there is no the FA, and MN instead of FA is responsible for tunnel-related functionalities. The procedure of NSIS-tunnel signaling in Mobile IPv6-based scenarios is as follows.

Provided that QoS-NSLP operates under the sender-initiated approach, after MN moves into a new network attachment point, QoS-NSLP over MN initiates RESERVE message to start the State Update procedure. GIST below the QoS-NSLP adds GIST header and sends the encapsulated RESERVE message to peer GIST node with corresponding QoS-NSLP for DCRN discovery. In this case, the peer GIST node would be a HA if the HA is NSIS-aware, and the MN is one of endpoints of Mobile IPv6 tunneling (Tentry). Two scenarios can be considered dependent on whether NSIS signaling interacts with the Mobile IPv6 tunneling: One is that the NSIS signaling is discerned on the tunneling path between the MN and corresponding HA, and then the tunneling path becomes an NSIS-aware cloud. Another is otherwise, and here the tunneling path is shown as a logical link to NSIS signaling.

In this procedure of NSIS-tunnel signaling, again, consideration on two categories of tunnel signaling mode is taken into, either sequential or parallel mode. On the one hand, provided that the tunnel signaling mode is sequential, before initiating the RESERVE message, the QoS-NSLP of MN creates a new RESERVE-tunnel message, which keeps the existing (end-to-end) Session ID and includes a new (tunneling) Flow ID different from the (end-to-end) flow ID, to interact with Mobile IPv6 tunneling. The RESERVE-tunnel message is forwarded toward HA as another end point of Mobile IPv6 tunneling to discover the DCRN and perform the State Update. Also, receiving the RESPONSE-tunnel message from the FA, the HA should initiates a RESPONSE-tunnel message toward MN reacting to the RESERVE-tunnel message. The RESERVE signaling toward the HA is performed after confirming completeness of NSIS tunnel signaling through the RESERVE- and the RESPONSE-tunneling signaling messages as shown in Figure 10. Arriving at HA from the MN, the RESERVE message is forwarded to CN to
update or refresh the existing NSIS states (QoS-NSLP and GIST) on common path. The CN initiates RESPONSE message, responding to the RESERVE message, toward the HA as its destination, and then the HA forwards the RESPONSE message to MN via corresponding AR.

Concerning CRN discovery in the sequential mode of tunnel signaling, CRN discovery on the tunneling path is reconciled with that over end-to-end path. That is, the CRN caused by mobility is discovered just one time between the MN and the HA. This can be possible by using the 'CRN_DISCOVERY (CD) flag bit'. Since tunnel signaling in the first place is performed for CRN discovery, the MN set the 'CD flag bit' in the RESERVE message, to address that already CRN is discovered for forward direction, if the CRN over the tunnel path is already discovered through NSIS-tunnel signaling messages. Therefore, CRN discovery by end-to-end NSIS signaling is not performed any more.

After the tunnel-CRN is discovered, the CRN can perform the State Update procedure. If the tunnel-CRN teardowns the state on the old tunnel path, the CRN may initiate RESERVE-tunnel message toward the AR.

On the other hand, provided that tunnel signaling mode is parallel, MN initiates the RESERVE and the RESERVE-tunnel messages toward the HA at the same time. Also, arriving at the HA from the CN, the

Figure 10: Sender-Initiated QoS NSLP over Tunnel - Sequential Mode
RESPONSE message is again forwarded from the HA to the MN regardless of the delivery of RESPONSE-tunnel message as shown in Figure 11. Since in this parallel mode the end-to-end signaling messages do not reconcile with both NSIS-tunnel signaling messages, the RESERVE- and RESPONSE-tunneling messages, the tunneling path operates as like a logical link and thus NON-QoS-HOP flag is set within the RESERVE message although NSIS-tunnel signaling messages are available on the tunnel path.

Concerning CRN discovery in the parallel mode of tunnel signaling, CRN discovery on the tunneling path is not reconciled with that over end-to-end path. That is, in this case the CRN discovery procedure is identical with the parallel mode of Mobile IPv4 tunnel signaling except for extension of the tunnel path from the FA to the MN.

Provided that the CRN is discovered successfully on the tunneling path, the CRN can perform the State Update procedure. In order to teardown the state on the old tunnel path, the CRN discovered on the tunneling path may be able to initiate RESERVE-tunnel message toward the MN. Also, the CRN discovered by the end-to-end signaling messages (e.g., HA) can perform the State Update procedure to remove the old state from itself to MN. In this case, the RESERVE message for removal of obsolete state is transparent over the nodes within the tunnel path.

![Figure 11: Sender-Initiated QoS NSLP over Tunnel - Parallel Mode](image-url)
Concerning QoS-NSLP signaling mode, provided that QoS-NSLP operates under the receiver-initiated approach, after MN moves into a new network attachment point, QoS-NSLP over MN initiates QUERY message to start the State Update procedure. GIST below the QoS-NSLP adds GIST header and sends the encapsulated QUERY message to peer GIST node with corresponding QoS-NSLP. In this case, the peer GIST node is a HA if the HA is an NSIS-aware node. Also, the MN is one of endpoints of Mobile IPv6 tunneling (Tentry). Two scenarios can be considered dependent on whether NSIS signaling interacts with the Mobile IPv6 tunneling: One is that the NSIS signaling is discerned on the tunneling path between the MN and the HA, and then the tunneling path becomes an NSIS-aware cloud. Another is otherwise, and here the tunneling path is shown as a logical link to NSIS signaling.

In this procedure of NSIS-tunnel signaling, again, consideration on two categories of tunnel signaling mode is taken into, either sequential or parallel mode. On the one hand, provided that the tunnel signaling mode is sequential, MN initiates QUERY message toward the HA, and then the HA send the QUERY message to its CN. In this case, as reacting to QUERY message, CN initiates the RESERVE message toward the HA to update the existing NSIS states (QoS-NSLP and GIST) on common path, and afterwards the HA forwards it to the MN as destination. After the receipt of the RESERVE message, the MN as Tentry begins to perform the NSIS-tunnel signaling as shown in Figures 12.

Concerning the procedure of NSIS-tunnel signaling, receiving the RESERVE message, the QoS-NSLP of MN creates a new QUERY-tunnel message, which keeps the existing (end-to-end) Session ID and includes a new (tunneling) Flow ID different from the (end-to-end) flow ID, to interact with node within the tunneling path. The QUERY-tunnel message is forwarded toward HA as Texit. Also, receiving the QUERY-tunnel message from the MN, the HA again initiates the RESERVE-tunnel message toward MN to response the QUERY-tunnel message. If the MN sends the RESPONSE-tunnel toward HA as react of the RESERVE-tunnel message, NSIS-tunnel signaling is finalized. Note that MN can initiate the RESPONSE message to HA as soon as receiving the RESERVE-tunnel message from the HA.

Concerning CRN discovery in the sequential mode of tunnel signaling, CRN discovery on the tunneling path is not reconciled with that over end-to-end path unlike sender-initiated mode of QoS-NSLP. That is, firstly, the CRN caused by mobility is discovered at the HA through the end-to-end signaling (e.g., RESERVE message), which the HA sets the 'CD flag bit' in the RESERVE message. Next, the tunnel CRN is discovered at a certain tunnel node between the HA and MN, which the CRN discovered at any node over the tunnel path sets the 'CD flag bit' in the RESERVE-tunnel message. In this case, the procedure for
the removal of the state on the old path is identical with the case of the parallel tunnel signaling mode in sender-initiated QoS NSLP signaling.

On the other hand, provided that tunnel signaling mode is parallel, MN initiates the QUERY and the QUERY-tunnel messages to the HA at the same time. Also, arriving at the HA, the Query message is again forwarded from the HA to the CN regardless of the delivery of QUERY-tunnel message as shown in Figure 13. Since in this parallel mode the end-to-end signaling messages do not reconcile with both NSIS-tunnel signaling messages, the QUERY-, the RESERVE- and RESPONSE-tunneling messages, the tunneling path operates as like a logical link and thus NON-QoS-HOP flag is set within the RESERVE message although NSIS-tunnel signaling messages are available on the tunnel path.

Concerning CRN discovery in the parallel mode of tunnel signaling, CRN discovery on the tunneling path is not also reconciled with that over end-to-end path as like the sequential mode of tunnel signaling. That is, the CRN discovery procedure is identical with the parallel mode of sender-initiated QoS-NSLP signaling. In this case, the procedure for the removal of the state on the old path is also identical with the case of the sequential tunnel signaling mode in receiver-initiated QoS NSLP signaling.
5.2. NSIS operations in multihomed mobile environments

In multihomed mobile environments, multiple interfaces and addresses (i.e., CoAs and HoAs) are available and thus how to select or acquire the most appropriate interface and/or address is of great concern [draft-montavont-mobileip-multihoming-pb-statement-04]. One of the NSIS's goals is to achieve end-to-end signaling for various signaling applications. However, some reasons such as scarce wireless resources, usage of tunneling, and frequent change of end host's address make it difficult for NSIS signaling to achieve end-to-end signaling. In this case, the interaction between the multihoming schemes and NSIS signaling protocols could alleviate problems caused by wireless bottleneck and mobility events. In this section, we discuss some NSIS signaling issues on interworking with multihomed networks and also present on how NSIS signaling (in particular QoS signaling) should perform multihomed signaling in mobility scenarios.

5.2.1. Multihomed mobile environments

In order to achieve the multihomed QoS signaling, the MN would need to register several CoAs with the unique HoA. However, since the present specification of MIPv6 only allows the MN to register a single CoA per HoA, a solution like [draft-wakikawa-mobileip-multiplecoa-04] needs to be used for multiple CoAs registration. On the other hand, when the MN has more...
than one HoA given either by one HA or multiple HAs, multiple CoAs registration may not happen because each CoA could be bound with single HoA. Throughout the scenario in this draft, we assume that an appropriate multiple CoAs registration mechanism is provided.

When a route optimization is used, a direct connection is established between an MN and a CN, in which case another reservation needs to be made while releasing the existing reservation engaged in the HA. In order to avoid this situation, the NSIS signaling for resource reservation needs to be performed only after finishing the route optimization, which is the way assumed in the following scenarios. On the other hand, without route optimization the resource reservation could be performed immediately after establishing the reverse tunnel.

In this section we are detailing the two scenarios for multihomed QoS signaling: receiver-initiated reservation and sender-initiated reservation. Figure 14 depicts the multihomed mobile environment where an MN with multiple interfaces moves to new area in which several ARs could possibly serve the MN. After handover, the MN checks the strength of the beacon signal and the available link bandwidth that neighboring ARs provide, and chooses the most stable ARs. An MN acquires multiple CoAs from the chosen ARs each of which is advertising single prefix, and then each CoA is assigned to one of the interfaces of the MN.

---

Figure 14. Illustration of the Multihomed environment

Internet-Draft NSIS Signaling in Mobility October 2005

We assumed homogeneous wireless interfaces in this draft although multihoming with multiple interfaces would be more efficient on heterogeneous interfaces due to the increased path diversity. The issues on heterogeneous interfaces are for further study.

Seamoby protocols such as CARD [RFC4066] and CTP [RFC4067] are not considered in this draft because an anticipated handover mechanism is not used. As a first step, this draft discusses interaction with...
The interaction with micro-mobility management protocols are for further study for performance optimization.

5.2.2. Receiver-initiated reservation in the multihomed environment

- BU and QUERY message transmission

After handover, an MN acquires multiple CoAs through aforementioned procedures and immediately sends a Binding Update to the CN for each of newly acquired CoAs. The CN acknowledges the binding update (BU) by sending a binding acknowledgment (BA) to the MN.

On receiving each BA, the MN immediately sends a QUERY message toward the CN through the interface associated with the CoA, to probe the network for information about the data path (the procedure (1)-(3) in Figure 15). The available resource on the path is recorded in the 'QoS Available' object of the QSPEC contained in the QUERY message.

- Intermediate node operation

The intermediate node inspects the 'QoS Available' object of the received QUERY message, and if its available resource is less than what 'QoS Available' says currently, the node adapts it accordingly.
Therefore, when the QUERY message reaches the CN, the 'QoS available' reflects the bottleneck of the resources on the path.

**o Primary CoA selection**

On receiving the QUERY messages the CN performs the Primary CoA determination procedure for the MN (4). The QUERY messages received no later than a certain time period after the reception of the first QUERY message are taken into account for the procedure. The time period is used to prevent the QUERY messages that arrive too late or have been dropped on the way from delaying the decision procedure. Though the small waiting time might exclude several messages from the procedure it would be desirable to maintain the time period to be small because the QUERY messages along the path with good condition would have been arrived earlier than others. On the other hand, the procedure could be immediately started even before the time period elapses when all Query messages are received, which is possible because the CN is aware of the total number of QUERY messages to receive beforehand through the number of BU messages.

The CN determines the Primary CoA based first on the available bandwidth and second on the arrival time of Query messages. When the available resource pertained in a QUERY message is conforming to the MN's BW requirement, the CoA delivered in the QUERY message is selected as the Primary CoA. In the case of more than one conforming QUERY messages, the message arrived first is selected.

**o Reservation re-establishment and teardown**

The CN sends a RESERVE message toward the MN to reserve resources along the path the Primary CoA takes. In this case, the RESERVE message activates two different actions: flow ID update and resource reservation. A flow ID consisting of source and destination addresses is used to identify the data communication route. On receiving RESERVE message, the nodes between the CN and the CRN updates the existing flow ID by replacing the old CoA with the new one, and uses the existing reservations for new path (5). On the other hand, resource reservations are performed between the CRN and new AR to establish new path (6). 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 (8).

5.2.3. Sender-initiated reservation in the multihomed environment

Sender-initiated reservation shares the procedure of receiver-initiated approach except that in the sender-initiated reservation, the QUERY and RESERVE messages are initiated by an MN, where the MN
selects the Primary CoA based on the information delivered by the QUERY message. As in the receiver-initiated reservation, the teardown message (RESERVE with the TEAR flag set) is initiated by the CRN to release the reservation in the obsolete path.

5.2.4. Link/node failure recovery

In case of link or node failures in the networks, NSIS state on the affected path will be removed. In this case, NSIS state immediately needs to be recovered on an alternative path to provide the seamless service for applications. If an on-going session is temporarily disrupted due to a wireless link failure in the multihomed environment, an MN needs to find an alternative path via an available interface to re-establish the session state. Suppose that an MN has three interfaces each of which is associated with a wireless link. If the current wireless link which is used for communication fails, the MN selects an alternative link via an alternative interface which is able to support the MN's QoS requirement and re-establishes NSIS state along the new path. The path selection and NSIS signaling procedure are similar to the case above except for the absence of the teardown message (RESERVE with the TEAR flag set).

5.2.5. Load balancing

There may be a situation where an MN may need to distribute its traffic load to multiple paths via multiple interfaces. In this case, the MN can send multiple QUERY messages to multiple interfaces to establish NSIS state on multiple paths.

Suppose that an MN wants to set up NSIS state on a path which is able to support the specific bandwidth requirement for a certain application in the multihomed environment. It may not be possible to find a feasible path for such a requirement. In this case, multiple paths can be used at the same time so that the bandwidth requirement can be met. Note that the flow identifier on each path may be different although the session identifier is unchanged.

5.3. QoS performance considerations in mobility scenarios

The routing characteristics of Mobile IP described in Section 5.1 cause the session path to frequently be changed and thus the NSIS signaling in such dynamic environments may cause the various problems mentioned in Section 3.1. In QoS-NSLP, critical issues which make QoS performance being degraded should be resolved to guarantee services for that data flow. In this section, particularly, QoS performance in terms of resource utilization and signaling latency is discussed to give some guidelines on how NSIS protocols should interact with mobility management protocols.

As an example of resource utilization, the double reservation problem can be alleviated by usage of a unique session identifier and the
State Update procedure including CRN discovery. However, management of the resource utilization in overall NSIS signaling processing point of view should be taken into account; in this regard, the adjustment of refresh interval is one of crucial elements which decide performance metrics of resource utilization as mentioned in Section 3.2. This issue needs to be discussed further in the case of the soft state approach to release the obsolete state in mobility scenarios is preferred to any explicit tear-down approach.

The NSIS protocol suite normally uses a soft-state approach based on the peer-to-peer refresh to manage state in NEs. The peer-to-peer based refresh allows the NSIS to appropriately select the refresh interval by considering the current network environment. For example, the refresh timer value in networks with scarce resources (e.g., mobile/wireless (access) networks) may set for a long time to decrease the overhead of signaling messages. If any explicit teardown messages for state removal are not used, in the situation where handover happens very frequently, the dynamic adjustment of the refresh interval can reduce the waste of resources. In this case, the refresh timer value needs to be set to a smaller value in the mobile/wireless networks than that in the core (wired) network as in [5]. To create dynamic refresh intervals, a general mechanism to be able to choose an optimal refresh timer value according to various mobile environments needs to be considered. However, this approach requires refresh interval traits dependent on specific network environments. When an MN, for example, roams from WLAN to UMTS or WiMAX (or WiBro) networks, the refresh interval in the UMTS or WiMAX (or WiBro) networks need to be set up differently from the WLAN networks. This advanced approach to automatically decide refresh intervals is further study.

Note that unlike the QoS-NSLP, the refresh timer of NTLP state does not need to be adjusted in the network since signaling application as resource reservation is not involve directly. Furthermore, the NTLP state along the obsolete path does not need to be explicitly removed before the expiration of refresh timer.

In mobile wireless networks, QoS-NSLP (rather than the NTLP) is able to set the refresh timer value depending on the handover type (e.g., make-before-break or break-before-make) or the reservation style (e.g., pre-establishment or re-establishment) to optimize the resources utilization. For example, in the make-before-break handover, an appropriate refresh time interval can be notified using the reserved field of REFRESH object. If the refresh timer value is set to a little higher value than the estimated handover latency, the MN can be provided with seamless QoS service using the pre-reserved resources without the waste of resources [6].

After the state setup on the new path, QNEMs on the signaling path may send a refresh message to the neighboring peer node before the refresh timer expires to update only the state previously installed.
along the path, or update the changed MRI along the common path. In this case, the overhead required to perform refresh can be reduced, in a way similar to the refresh reduction in RSVP [16]. Once a RESPONSE message which indicates the successful installation of a reservation has been received, subsequent RESERVE messages for refresh can simply refer to the existing reservation, rather than including the complete reservation specification. For example, in case of QoS-NSLP, only the SID and the SII with no QSPEC are sent to just refresh the state (e.g., reservation) previously installed. The changed flow ID together with those IDs is only sent to update it along the common path. Especially, transmission of the reduced number of refresh messages over wireless channels, access networks, or core networks results in the efficient utilization of resources.

As mentioned in Section 3.1, unlike the generic route changes, in mobility scenarios, the end-to-end signaling problem by the Path Update gives rise to the degradation of network performance such as increased signaling overhead, service blackout, and so on. To reduce signaling latency in the Mobile IP-based scenarios, the NSIS protocol suite needs to interwork with localized mobility management (LMM). If the GIST/NSLP (QoS-NSLP or NAT/FW-NSLP) protocols interacts with Hierarchical Mobile IPv6 and the CRN is discovered between an MN and 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 further 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

† Internet-Draft NSIS Signaling in Mobility October 2005

the NSIS protocols to interact with mobility protocols such as Seamoby protocols (e.g., CARD [RFC4066] and CXTP [RFC4067]) and 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.

5.4. Support for Ping-Pong type handover

NSIS signaling needs to consider the interaction with ping-pong type handover as addressed in Section 3.1 because it has a significant effect on when to initiate signaling for state setup or for state release. With the sender-initiated approach, if an MN (as a sender) undergoes a handover into a new AR, the NTLP interacts with the binding process of Mobile IP to initiate state setup. However, if the MN moves to other ARs or the previous AR again in a short while, signaling using the interaction with the binding process may result in considerable signaling overhead and some possible errors. Immediate teardown of state on the old path may also bring on the similar result. Some identifiers defined in [5] [6] may be useful for this situation.

An NE (e.g. QNE) can determine if it is a merging point (i.e. an
1-draft-ietf-nsis-applicability-mobility-signaling-03.txt

NSLP CRN) of the old and new paths, and then it can perform an involved state setup on the new path and state teardown on the old path. However, if the QNE receives an NSIS message (e.g., RESERVE) with a special flag (e.g. NO_REPLACE flag) set but with the different SII, state teardown on the old path should not happen. This may apply to a ping-pong type handover where the MN wishes to keep state to its old attachment point in case it moves back there. For interaction with the ping-pong type handover, NSIS should determine when to set the NO_REPLACE flag depending on when and where the MN handovers. It requires NSIS to monitor or react on the mobility events over possible API. It is still an open issue and needs to be discussed further.

The Reservation Sequence Number (RSN) may be useful in detecting duplicate messages in the mobile environment. For example, it is possible for the MN to move to the second NAR soon after being attached to the 1st NAR. The CRN may receive the RESERVE messages (with different RSN) twice when the RESERVE message from the 1st NAR arrives later than the RESERVE message from the 2nd NAR. In this case, the CRN should determine which RESERVE message is the latest one via the RSN.

The Mobility object described in Section 4.2.2 can be defined in the NTLP (e.g., in GIST payload) or NSLP messages to notify of any mobility event explicitly, and it may contain various mobility-related fields, e.g., mobility_event_counter (MEC). The MEC field can inform the CRN of which incoming massage is the latest and so it is useful to detect the latest handover event for avoiding any confusion about where to send a confirmation message and to handle the ping-pong type of movement.

5.5. Peer failure scenarios

A dead peer can occur either because a link or a network node failed, or because the MN moved away without informing NSLP/NTLP (it is recommended to link mobility- and NSIS signaling such that this does not happen).

Dead peers of interest in mobility scenarios include CRN, MN, AR (or FA), and HA. In general, it is possible that only NSIS functions (i.e., NTLP/NSLP) of the node may fail, or the that the node itself fails completely. In this regard, the following issues arise.

- An MN may either fail or move (or just operate normally). When it fails, it becomes a dead peer. If it moves and changes its IP address without notifying NSLP/NTLP, it also becomes a dead peer. The failure or movement of an MN may cause the 'invalid NR' problem [8] where the NR is the MN mentioned in Section 3.2. If the MN moves, care should be taken to prevent the teardown of NSIS state on the old path before the NSIS state is re-established on the new path. In this case, an error message (or refresh
timeout) should not be generated (or happen) to avoid any teardown on the old path and common path. The problem can be solved by using hanover_init (HI) field of the Mobility object described in Section 5.4. The HI field can explicitly inform AR (or CRN) that a handover is now initiated, and thus the AR does not initiate any error messages (or refresh timeout) when it does not receive responses to refresh messages from the MN [6]. In this case, AR's possible approach may be a proxy for the MN (the last node) and it may be able to send RESPONSE messages in response to REFRESH (or RESERVE) messages from a upstream node. AR may also forward the error message including the HI field toward CN to prevent the NI from removing the NSIS state. However, it is still an open issue whether the hint information such as the HI field through NSIS signaling messages needs to be forwarded.

- 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 described in Section 4.2.3.

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

In any case, dead peers should be discovered fast to minimize service interruption. The procedures for dead peer discovery (DPD) should be the same no matter why a peer is dead, because an NE discovering a dead peer cannot judge the specific reason. The procedures for DPD should be handled by the NTLP. In fact, the DPD can be considered as an extension to the GIST peer discovery. A peer discovery message can be periodically transmitted to the neighboring peer (e.g., responding node in [2]), and the responding node can send a response message. To determine if the peer is alive, the use of a timer may be helpful. For example, the response message may need to be received by the sender (e.g., querying node in [2]) before the timer expires. Otherwise, the responding node can be considered dead.

6. Security Considerations

This section describes authorization issues for mobility scenarios in...
NSIS: It tries to raise additional questions beyond those discussed in [7].

For the discussion of various authorization problems we assume that initial authorization is strongly coupled to authorization handling in subsequent message interactions. Making this assumption has some implication to the signaling message behavior. It is certainly possible that the entities who request the initial reservation or a firewall pinhole and those who subsequently cause modifications are not the same entities.

NSIS NSLPs define a flexible authorization scheme. As argued in [8] it is necessary to consider cases where the sender, the receiver or both are authorizing a reservation. For NAT and Firewall signaling it is necessary that, the sender and the receiver, authorize the creation of a NAT binding and the creation of a firewall pinhole and the reason is described in [8].

Subsequently, we will consider the case where the mobile node acts as a data sender followed by a discussion of the CN as a data sender.

6.1. MN as data sender

This section refers to Figure 1 where the MN acts as a data sender which moves from one point of attachment to another.

This description starts with an initial signaling exchange triggered by the MN. The user (or another entity associated the initial setup) provides the credentials for setup as part of the NSLP authorization procedure (e.g., QoS reservation).

6.1.1. MN is authorizing entity

This scenario considers the initial flow setup executed by the MN whereby the MN provides authorization for the initial flow setup. The initial setup might be used to create state for subsequent authorization actions by the MN. It is obvious that the authorization for the NSLP application (e.g., QoS NSLP) has to be provided. Depending on the underlying authorization model it might be either peer-to-peer or end-to-middle. This authorization decision can possibly be treated independently of the authorization issues discussed in this section.

The following questions seem to be interesting:

- Should the MN indicate that it is the authorizing entity for subsequent actions to all entities along the path?
- What information should be used for this purpose?
- Who should add this information? Should the visited network of
the MN add something to the signaling message during the initial flow setup?

- How do other entities along the path learn this information?

```
MN                  CN

--------------------------> +
ACTION (MN is authz)      |
<--------------------------|
ACK                       |
```

Traffic

Figure 16: MN authorized initial reservation

Next, the case for a mobile node authorizing the DCRN is considered. This communication is illustrated in Figure 17.

The movement of the mobile node after the initial flow setup requires authorization. Various session ownership authorization issues are illustrated in [7].

```
MN                  DCRN                  CN

--------------------------> + E.g.
ACTION                    Movement    with state
<--------------------------| creation at
ACK                        + new path
```

Figure 17: MN authorizes DCRN

The following questions are of interest:

- Why should the DCRN execute something on behalf of the MN? (i.e., why should it trust the MN and what information can the DCRN use for verification? [the trust is not the other way round: the MN trusts the DCRN?]) As an example, the DCRN might delete state along the old segment.

- Should the DCRN alone be able to start signaling (the DCRN might be a dedicated node in some mobility protocols (e.g., MAP)) since it is the node which has more information than other nodes based on the mobility signaling protocols?
How should other nodes between the MN and the DCRN and the nodes between the DCRN and the CN know that the DCRN is now acting on behalf of the MN?

The case of a corresponding node triggering an action is discussed in the paragraph below. Figure 18 shows the exchange graphically.

In this scenario the CN wants to, for example, tear-down a reservation.

MN               DCRN               CN

Internet-Draft     NSIS Signaling in Mobility    October 2005

Figure 18: CN triggers action

The following questions arise:

- Why should the MN trust the trigger? Why should the intermediate nodes trust it?
- Is it possible to specify the security properties of the trigger message in more detail? Is this an NSIS signaling message?
- The discussions about an indicator which entity to charge for the reservation might be relevant (see [8]).
- Should the CN restrict the actions of the MN (e.g., delete, update, create action of established state information)? On the shared segment it might, for example, be possible to restrict the allowed action to a flow identifier update.

6.1.2. CN is authorizing entity

This scenario is similar to the CN triggering in Section 6.1.1. Two slightly different protocol variations will be considered. Authorizing some actions in the reverse data flow direction is more difficult as it can easily be seen in Figure 19.

6.1.2.1. CN asks MN to trigger action (on behalf of the CN)

In Figure 19 the CN authorizes the MN to start signaling after, for
example, a movement. After receiving the trigger message (and some
authorization information) the mobile node starts signaling along the
new segment and automatically discovers the DCRN. The message
c Travels along the shared segment to the CN and updates the flow
identifier (if necessary). The MN might additionally allow the DCRN
to delete the reservation along the old segment.

MN  DCRN  CN

Internet-Draft  NSIS Signaling in Mobility  October 2005

TRIGGER

ACTION (CN is authz; MN on behalf of CN)

Action: 'create' along)  Action: 'update' along)
  new segment)  shared segment)

Action: 'delete' along)
  old segment)

ACK

Traffic

Figure 19: CN asks MN to trigger an action (on behalf of the CN)

The following questions need to be considered:

- How should the "delegation" mechanism work such that intermediate
  nodes believe the MN that it is acting on behalf of the CN?

- Is it possible to carry this information with the trigger message
  from the CN and the MN?

6.1.2.2. CN uses installed state to route message backwards

The CN uses NSIS installed state to route a signaling message
backwards along the path. In some rare cases the DCRN node might be
known already. In this case it is possible to stop the update
process along the shared segment and to possibly mark installed state
along the old segment for deletion. When the MN receives the message
it again has to install state along the new segment towards the DCRN.
The mobile node might also trigger the deletion of resources along the old segment together with this state creation (pessimistic delete). An optimistic delete operation is certainly more error prone.

Figure 20: CN uses installed state to route message backwards

Figure 20 raises a few questions:

The security properties of the trigger message need to be evaluated.

It is not always possible to route signaling message backwards from the CN to the MN:

- state at the new path might not be established (hence the signaling message cannot travel backwards)
- the signaling message might not reach the MN via the old segment.

In the multi-homing case where the mobile node can be reached via more than one path it is possible to execute this exchange. The same might be true for some local repair cases.

The messages triggered by the MN (namely create state along the new segment) need to be evaluated.

[Diagram showing the exchange of messages between MN, DCNR, and CN, with actions and acknowledgments.]

Internet-Draft NSIS Signaling in Mobility October 2005
6.1.2.3. MN and CN are authorized

If we argue that the authorization at the NSLP layer is somehow tight to the authorization for certain protocol actions then we also have to consider the case where the MN and the CN have to contribute to the authorization decision. This situation appears, for example, in the NAT/Firewall signaling case but also in the area of QoS reservation where both parties might need to share the cost of a reservation.

If both end hosts are authorized then some signaling message exchanges are less difficult since the trigger message does not need to delegate the authorization decision. Some problems, however, do not disappear such as the session ownership problem and additional problems might be caused by certain solution approaches. Since this section does not discuss solutions the reader is referred to the [7] draft which lists a few proposals for addressing the session ownership problem.

6.1.3. CN as data sender

In this section we consider the scenarios where the CN acts as a data sender. Figure 1 shows the topology and the participating entities.

6.1.3.1. CN is authorizing entity

This scenario is similar to the one described in Section 6.1.1. No additional problems arise with a scenario where the CN is both data sender and also the authorizing entity. In Figure 8 the CN authorizes the UCNR to delete the old segment and to establish a new reservation along the new segment. Furthermore, at the shared segment only an update of the flow identifier might be necessary.
Since the mobile node first detects the route changes. A trigger to the CN allows the CN to quickly react on the route changes. There are three variants:

- The MN sends a trigger to the CN and the CN starts signaling as shown in Figure 21.

- The MN routes the message back along the reverse path using the previously established state along the old route. This mechanism only works if the MN is able to send messages along the old path. As a generic mechanism this is not suggested.

- An intermediate node act on its own. This might be possible that the UCRN is an entity which participates in the mobility signaling (e.g., Mobility Anchor Point (MAP)) exchange. Depending on the message exchange it needs to be studied whether the signaling message provides sufficient authorization to trigger the NSIS exchange.

6.1.3.2. MN is authorizing entity

In this scenario we consider the case where the CN is the data sender but the MN authorizes actions. The considerations are similar to those elaborated in Section 6.1.3 where the MN is the data sender but the CN is the authorizing entity.

6.1.4. Multi-homing Scenarios

Multi-homing scenarios have the property that more than one path belongs to a signaling session. In Figure 12 the MN uses two interfaces to route NSIS message towards the CN. The two individual flows are tight together by using the same session identifier and then associate it with the two flow identifiers. The MN needs to indicate that both reservations need to be kept alive (and the DCRN should not delete a reservation). At the shared segment only a single reservation might be stored (if desired).

From an authorization point of view the session ownership issues is
applicable since the DCRN needs to merge the two reservations into a single one along the shared segment.

6.1.4.1. MN as data sender

This section shows the multi-homing scenario with the MN as a data sender.

If the MN is the authorizing entity then the session ownership problem needs to be solved. Without solving this type of authorization problem it is possible for an adversary to "join" the reservation at the shared segment. Furthermore, it is an open issue whether reservation merging is allowed only for cases where one flow identifier is used at different interfaces or even with different flow identifiers.

If the CN is the authorizing entity then, again, some message needs to be sent from the CN to the MN to trigger the exchange or to route the request backwards along the established path. The MN is reachable via the two paths.

```
segment 2

+---+                  +---+                  +---+
| MN |                  | DCRN |                  | CN |
|UCRN|                  |    |                  |    |
+----+                  +----+                  +----+

V+----------------------------------^        +---+
V| AR|---------------------------------| AR|
    V----------------------------------V

segment 1

+---+
| AR|---------------------------------|
    V----------------------------------V

+---+                  +---+                  +---+

shared segment
```

Figure 22: Multi-homed MN as data sender

6.1.4.2. CN as data sender

This section shows the multi-homing scenario with the CN as a data sender. The scenario is simpler (for the CN authorizing case) than the one described in Section 6.1 since the signaling message along the shared segment travels the previously established path. It shows some similarities with a route change scenario. At the mobile node
itself the two paths merge which again leads to a session ownership problem. How should the MN know whether a signaling message with the same session identifier hitting a different interface belongs to the indicated session authorized by the CN?

![Diagram]

Figure 23: Multi-homed CN as data sender

If the MN is the authorizing entity then again communication between the end hosts is required as a trigger. Routing the signaling messages in the reverse path might, in some cases, also be possible.

6.1.5. Proxy Scenario

The proxy scenarios refer to those cases where one of the end hosts or even both end hosts are not NSIS aware. Two security implications need to be studied:

- First, there is an authorization issue with regard to the NSLP application. For QoS signaling the end host (and the user) has to authorize the QoS reservation since the reservation might require the user is charged for it. Since the end host is not NSIS aware some other mechanism or protocol needs to be available which provides this functionality. For NAT/Firewall signaling delayed authorization assures that both end hosts authorize the packet filter creation at their local networks (particularly in case of missing trust relationship between intermediate networks).

- Second, the authorization issues which relate to the session ownership problem also need to be studied. Since the session ownership issues are related to the signaling participating nodes and not to the users or the true end points we think that it does...
6.1.6. Conclusion

This section tries to point to some authorization aspects for NSIS signaling in a mobility environment. Performance is important in mobility environments but a proper security handling accounts for a high percentage of the total performance. It is important to consider this aspect in the analysis of mobility proposals.

From the scenarios we can observe the following issues:

- Signaling in the direction of the data path is simpler than in the opposite direction.
- There are many similarities between the scenarios where the MN acts as a data sender and the scenarios the CN acts as a data sender, particularly if multi-homing scenarios are included.
- Many authorization problems arise after the initial setup of resources along the path. This problem can be stated as: "Is an entity allowed to perform the indicated action?" Only a few problems are related to the initial signaling message exchange.
- If the data sender triggers the signaling message exchange and also provides authorization then the complexity can be kept fairly low.
- NSLP authorization decisions should be treated separately from authorization decisions which affect the signaling message exchange.

During the work a few open issues have been selected:

- This section does not consider the different message types.
- The implication of price determination caused by mobility is excluded from this description.
- It was tried to keep the description in this section very generic. Implications of certain mobility protocols are therefore not considered.

7. Change History

Internet-Draft NSIS Signaling in Mobility October 2005

7.1. 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 Section 5.
13. Added this change history.

7.2. 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. Clarified 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.

7.3. Changes from -02 version

Version -03 includes mainly tunneling-related and multihoming-related scenarios in Sections 5.1.3 and Section 5.2, respectively. Also, the terminology, 'Path Update' is changed into 'State Update' in Section 3.2.4.

8. References

8.1. Normative References


8.2. Informative References
1-draft-ietf-nsis-applicability-mobility-signaling-03.txt


Internet-Draft NSIS Signaling in Mobility October 2005


Appendix A. Contributors

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 and Roland Bless. Separating authors into two groups was done without treating any one of them better (or worse) than others.

A.1. Acknowledgement

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, Dakako Sanda, Rudiger Geib, Cheng Hong Elena Scialpi, and Pratic Bose for their useful comments and suggestions.

Appendix B. Generic Route Changes

The mobility occurs due to the change of the network attachment point, but the generic route changes is associated with load sharing, load balancing, or a link (or node) failure. These cause divergence (or convergence) between the old path along which state has already been installed and the new path along which data forwarding will actually happen.

The route changes brings on the change of signaling topology and it results in difference according to the types of route changes (e.g., the route changes or mobility). The route changes generally forms two common paths, an old path, and a new path, where the old path and the new path begin to diverge from one common path and afterward to converge to another common path for each direction of signaling flows.
(a) The topology for downstream NSIS signaling flow after route changes

(b) The topology for upstream NSIS signaling flow after route changes
Authors' Addresses

Sung-Hyuck Lee
SAMSUNG Advanced Institute of Technology
San 14-1, Nongseo-ri, Giheung-eup
Yongin-si, Gyeonggi-do  449-712
KOREA

Phone: +82 31 280 9585
Email: starsu.lee@samsung.com

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
Hannes Tschofenig
Siemens AG
Otto-Hahn-Ring 6
Munich, 81739
Germany

Phone:
Email: Hannes.Tschofenig@siemens.com

Xiaoming Fu
University of Goettingen
Telematics Group
Lotzestr. 16-18
Goettingen 37083
Germany

Email: fu@cs.uni-goettingen.de

Jukka Manner
Department of Computer Science University of Helsinki
P.O. Box 26 (Teollisuuskatu 23)
HELSINKI, FIN-00014
Finland

Phone: +358-9-191-44210
Email: jmanner@cs.helsinki.fi
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity