Internet Engineering Task Force
Internet-Draft
Expires: April, 2004

R. Hancock
J. Manner (ed.)
C. Shen

October, 2003

Interactions of Routing and Mobility on NTLP and NSLP

<draft-hancock-nsis-routing-mobility-00.txt>

Status of this Memo

This document is a submission to Next Steps in Signaling Working Group. Comments should be submitted to the nsis@ietf.org mailing list.

Distribution of this memo is unlimited.

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026. 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 in April, 2004.

Abstract

IP packet routing and changes in routes can have major influence on protocols and services that set state in network nodes. Routing may change, for example, due to node failure within the network, need for load balancing, multihoming or due to end-host or even network mobility. This draft is a first step in helping us to decide on how these problems should be handled and how interactions with other protocols should be handled and a stimulus to further security work.

Table of Contents

1 Introduction 2
2 Short Problem Statement 3
3 Session Path Change 4
3.1 Problem Statement 4
3.2 Possible Scenarios for Session Path Change 5
3.2.1 Cases corresponding to a NNE as UCOR 6
3.2.2 Cases corresponding to a PNE as UCOR 8
3.2.3 Cases corresponding to a FNE as UCOR 10
3.3 Detection of Session Path Change 12
3.4 Response to Route Change caused Session Path Change 13
3.4.1 Network Monitoring based UCOR detection 13
3.4.2 Data Packet Monitoring based UCOR detection 14
3.4.3 Signaling packet Monitoring based DCOR detection 14
3.5 Other cases 15
3.6 QoS routing Considerations 15
3.7 Response to Mobility Caused Session Path Change 15
4 IP Mobility and Multihoming 15
4.1 Comparison with Route Changes 15
4.2 Analysis Overview 17
4.3 MN-Terminating Session 19
4.3.1 CN (Sender) Initiated Setup and Teardown 19
4.3.2 MN (Receiver) Initiated Setup and Teardown 21
4.4 MN-Originating Session 25
4.4.1 MN (Sender) Initiated Setup and Teardown 25
4.4.2 CN (Receiver) Initiated Setup and Teardown 27
4.5 Summary of the Analysis 29
4.6 Further Interactions with Fast Handover Protocols 31
5 Security Considerations 33
6 Contributors 34
7 Acknowledgments 34
8 Informative References 34
9 Author's Addresses 34

1. Introduction

This draft addresses Mobility related considerations for NSIS. Given the scope of mobility, it is helpful to discuss it together with two other closely related topics, namely, route change and IP address changes. Generally speaking, the relationship among the three is:

1. All mobility necessarily incurs route change, usually at edge of the network. But route change may also be caused by reasons other than mobility, such as routing protocol adaptation in response to varying network conditions. The latter type of route changes usually occurs in the middle of the network.

2. Normal IP mobility (i.e., Macro-mobility) involves change of MN IP addresses. Micro mobility usually does not cause change of IP addresses. Hierarchical mobility contains both macro-mobility and micro-mobility scenarios and thus limits the effect of IP address change into a smaller scale than that of macro-mobility. Since IP

address is usually part of the flow identifier, change of IP addresses implies change of flow identifier.

A route change triggered by host mobility may or may not involve changes in IP addresses. Some Local Mobility Management (LMM) mechanisms may change the IP address assigned to the mobile node within the access network, for example, mechanisms based on a hierarchy of mobility handling routers. Some protocols either use tunneling to forward packets towards the new location of the mobile node, or set and update per-host routing entries in the network, as for instance, ad-hoc routing protocols.

Issues that also affect the state management in NSIS are host multihoming, the actual routing path created by mobility management protocols, whether the routing is optimal or triangular, the use of a context transfer framework, and who and when notices the need for updating states. This latter involves noticing the need to update states, for example, whether it is the sender or the receiver of the data stream, or some intermediary router. Moreover, whole mobile networks will need to be studied in more depth in the context of NSIS.

2. Short Problem Statement

The various services that may make use of the forthcoming NSIS protocols set state within network nodes and routers. There are various issues that must be handled carefully when the NSIS protocols are used in non-static environments, as for instance, mobile nodes in wireless access networks. The following list is a short summary of the main issues that must be considered when the NTLP and NSLP protocols are used in dynamic environments:

- Interactions with session state information and routing information (=IP address)

- If session states are set for single unicast communications, state on the obsolete path must be removed quickly after the routing changes.

- Changes in states and routing should only be signaled within the affect part of the network, and, thus, should not require end-to-end signaling. This may not always be possible, if, for example, the IP address of the sender or receiver changes.

- Possibility to keep signaling local, or within an identified scope. This would be useful, especially in mobile networks, to be able to reserve only local resources. This feature would require that the node terminating the NSIS signaling must be a different node than the one receiving the user data.

- Various LMM mechanisms use tunneling or affect routing table entries. These changes, and tunnels in general, affect the way NSIS protocols are able to set state on the same path as the user data,

and are able to identify the original IP packets carrying user data.

- Route changes noticed by NTLP, or some other entity within an NSIS router, should be propagated to NSLP, and or NTLP, respectively. This is similar to the operation of RSVP, where routing changes noticed by the router are propagated to the RSVP process running on the router.

- Interactions of NTLP/NSLP and Mobile IP need to be taken into account.

- Interactions with NTLP/NSLP and CARD and CT need to be studied.

- Slow wireless links may require additional considerations within NSIS, for example, state refreshes, and any other NSIS-related signaling, should be sent less frequent over the wireless link than within the wired network.

- Issues in discovering the cross-over router to find the limit of the affected path.

- A critical issue is also the security of the signaling, AAA and encryption. When a node moves or routing changes happen within the network, how can the new peer, for example, a new access router, authenticate and decrypt protected NTLP/NSLP messages?

3. Session Path Change

3.1. Problem Statement

In this document session path change is used to refer to the common aspect of route change and mobility. Path change is further divided into downstream path change and upstream path change: In NSIS context, a downstream path change occurs when the outgoing interface for a session has changed; an upstream path change occurs when the incoming interface for a session has changed. Path change results in divergence of packets in data plane and/or in control plane. We refer to the node where this divergence starts as the Upstream Cross-Over Router (UCOR) and the node where this divergence ends as a Downstream Cross-Over Router (DCOR).

It should be noted that:

1. It is possible to adopt a more NSIS-aware UCOR/DCOR definition rather than this strict "route splitting point" definition. For example, in cases where the route splitting point is not NSIS capable, the UCOR/DCOR could be defined as the NTLP/NSLP node downstream or upstream of it.

2. Although this definition is meant to refer to routers (as the name

suggests). It is also possible and interesting to extend it to include end nodes especially in Mobility and Multi-homing scenarios. For example, in sender mobility case, the MN *could* view the result of its mobility functions (change of IP address) as similar to a

downstream routing change event (it needs intelligence to do that) and be defined as a UCOR. In multi-homing case, the MN *could* view the result of its multi-homing functions (change of outgoing interface) as similar to a downstream routing change event and be defined as a UCOR.

We consider a mixed signaling configuration scenario outlined in Figure 1 (copied from [1]), i.e., not all routers in the path are NSIS Entities (NEs); All NEs support NTLP; but not all NEs support all NSLPs. We use NSLP1 as an example in the description below. We refer to the three types of nodes seen by a particular session as: Full-NSIS Entity or FNE (supports NTLP and the specific NSLP1), Partial NSIS Entity or PNE (supports NTLP but not the specific NSLP1); Non-NSIS Entity (NNE) (supports neither NTLP nor NSLP1).

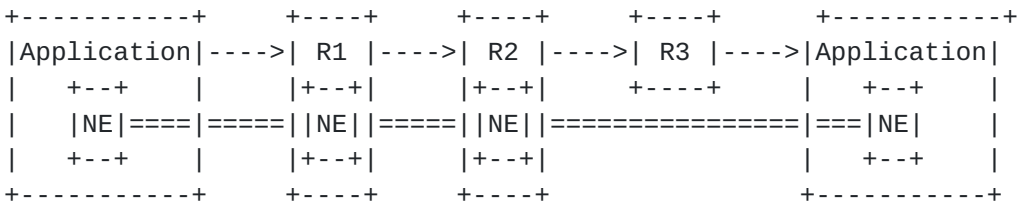


Figure 1(a): Simple Signaling and Data Flows

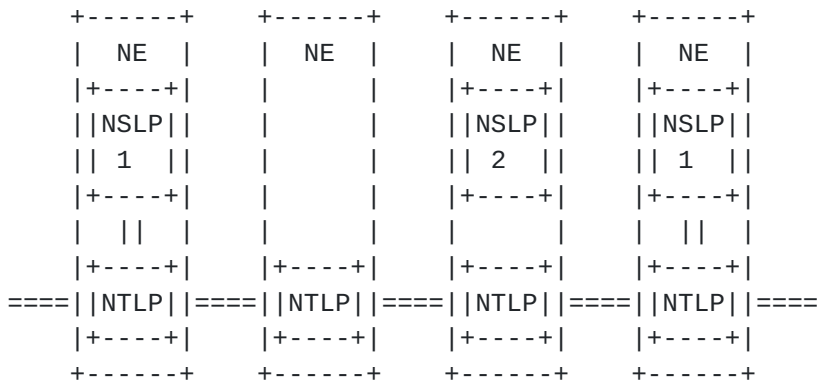


Figure 1(b): Signaling with Heterogeneous NSLPs

3.2. Possible Scenarios for Session Path Change

Session path change can be caused by either route change or mobility. The main difference of these two cases, in terms of UCOR and DCOR can be summarized as follows:

In case of route change, usually both UCOR and DCOR exist and they form a loop; In case of mobility, Sender mobility will create a DCOR, Receiver mobility will create a UCOR. If the MN is both sending and

receiving, there will be both UCOR and DCOR, they may or may not be in the same physical node depending on the routing symmetry. Session path changes caused by mobility are analyzed in more detail in Section 4.1.

Since either UCOR or DCOR can be any of the FNE, PNE or NNE, we have 9 possible UCOR/DCOR combinations for route change and 6 possible cases for sender/receiver mobility. From topology point of view, the 6 mobility cases are actually simplified versions of corresponding route change cases. However, mobility also involves other aspects not present in route change, such as mobility signaling and change of Flow Identifiers.

In the following, we illustrate the 9 route change scenarios.

3.2.1. Cases corresponding to a NNE as UCOR

The following Figure 2 shows an example network before path change:

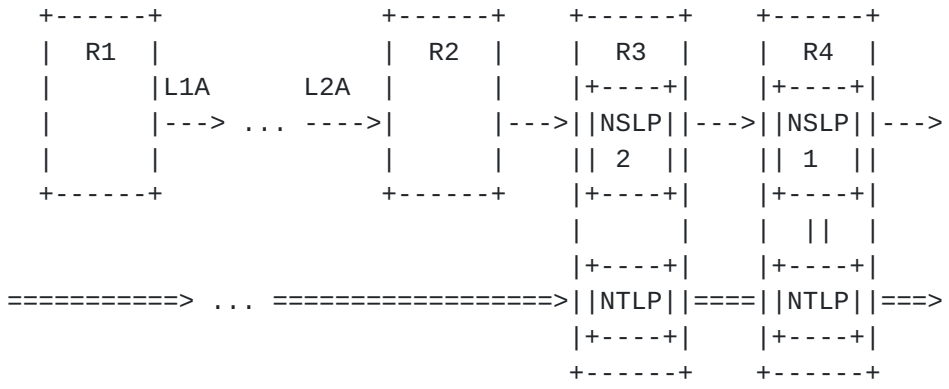


Figure 2: Case A: UCOR is an NNE,

The following three figures show the three possibilities after path change for the example network:

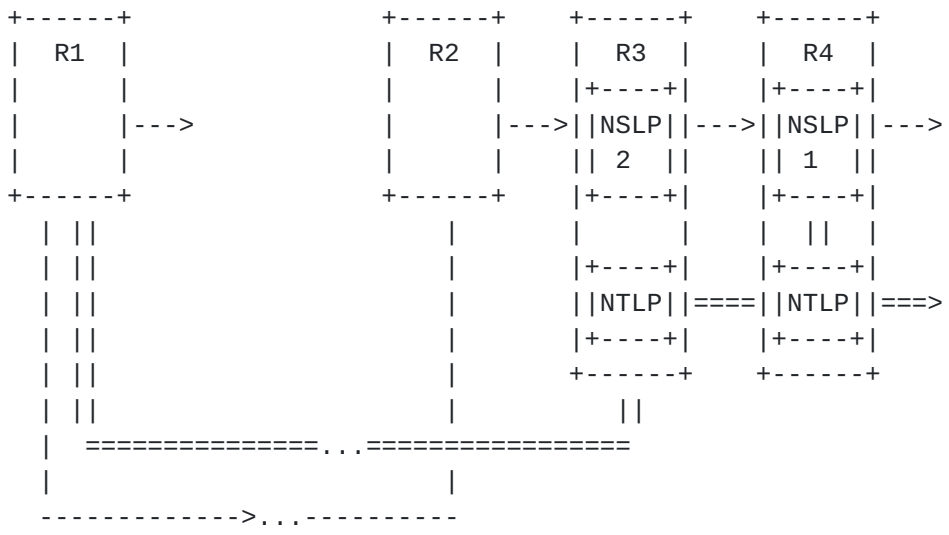


Figure 3a: Case A.I DCOR is an NNE

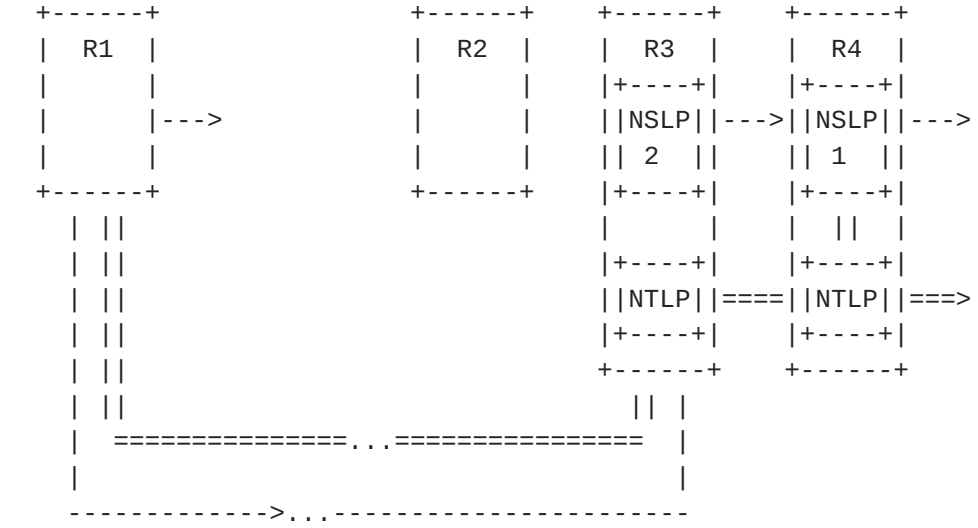
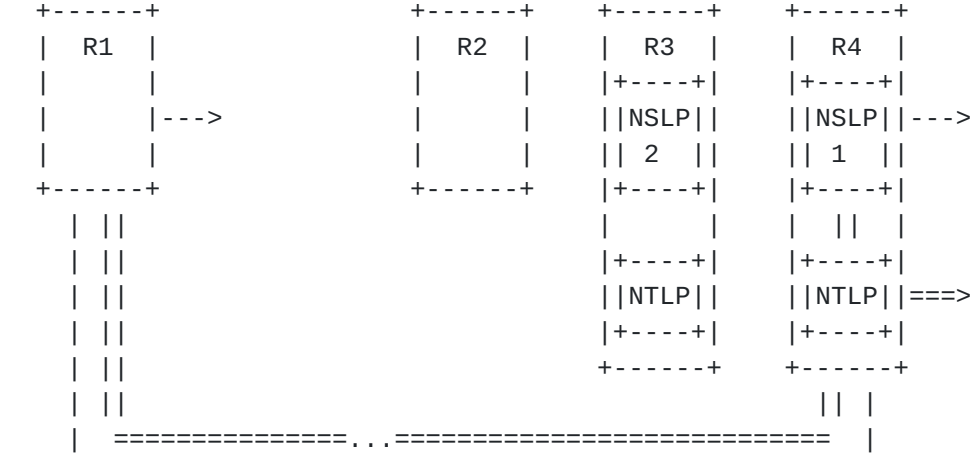


Figure 3b: Case A.II DCOR is an PNE



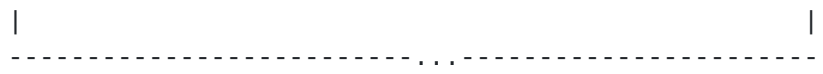


Figure 3c: Case A.III: DCOR is an FNE

3.2.2. Cases corresponding to a PNE as UCOR

The following Figure 4 shows an example network before path change:

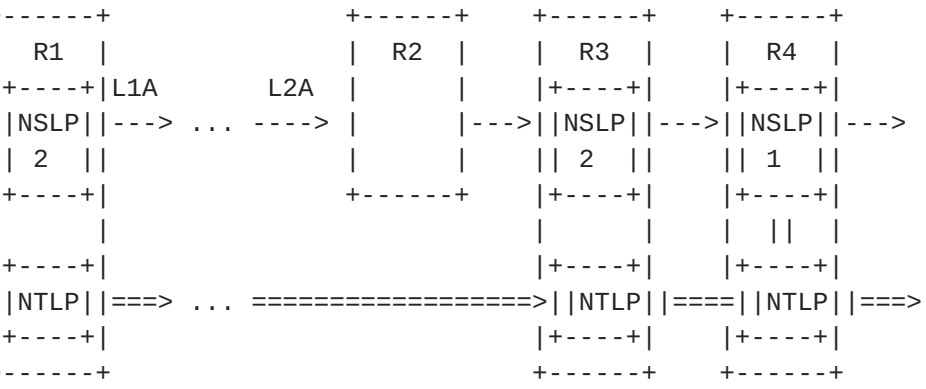


Figure 4: Case B: UCOR is a PNE

The following three figures show the three possibilities after path change for the example network:

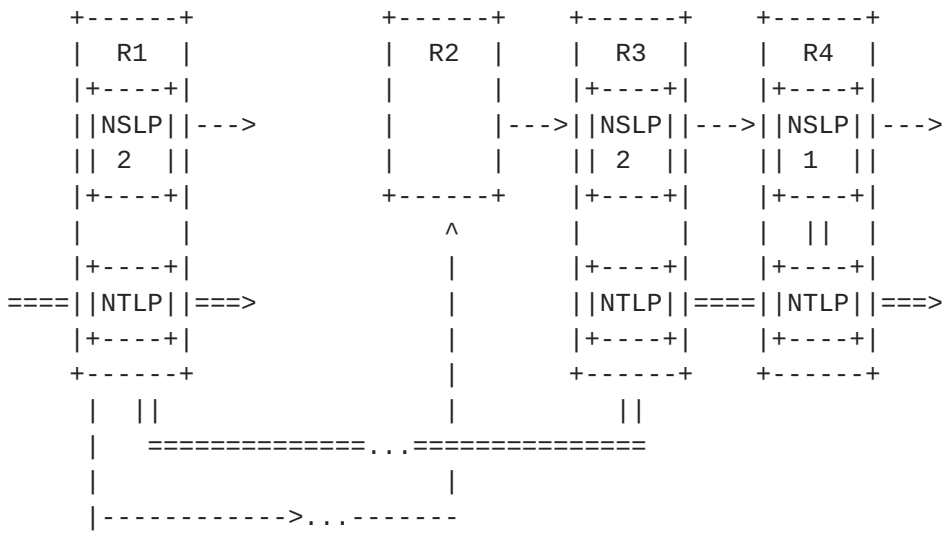


Figure 5a: Case B.I: DCOR is an NNE

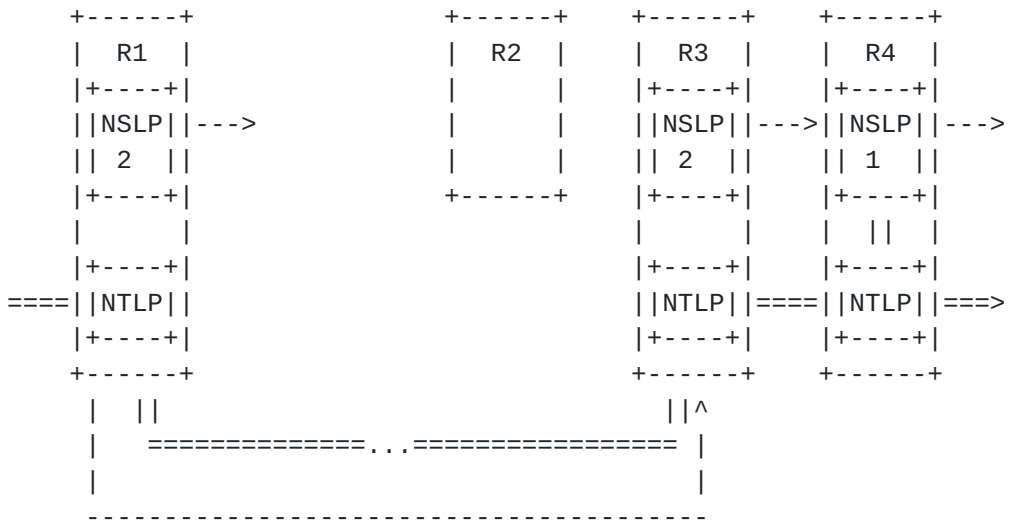
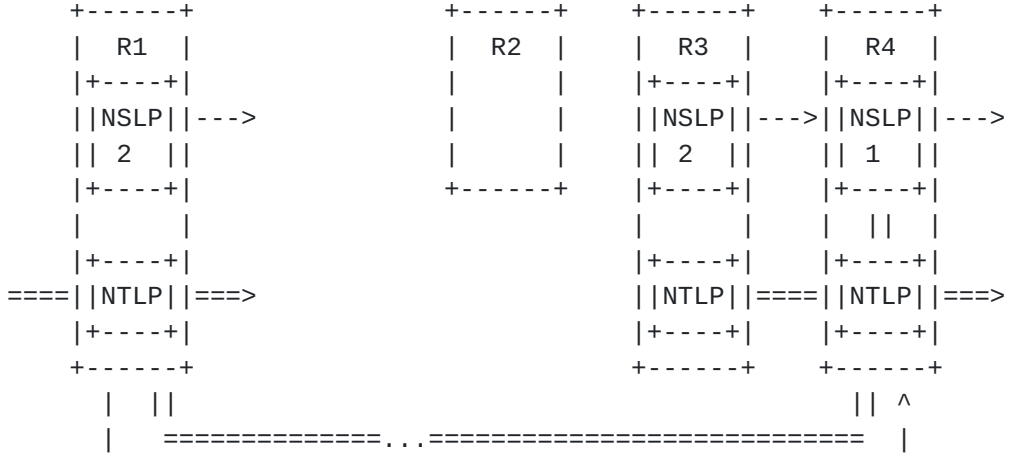


Figure 5b: Case B.II: DCOR is a PNE



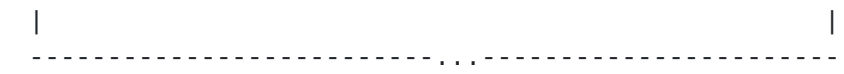


Figure 5c: Case B.III: DCOR is a FNE

3.2.3. Cases corresponding to a FNE as UCOR

The following Figure 6 shows an example network before path change:

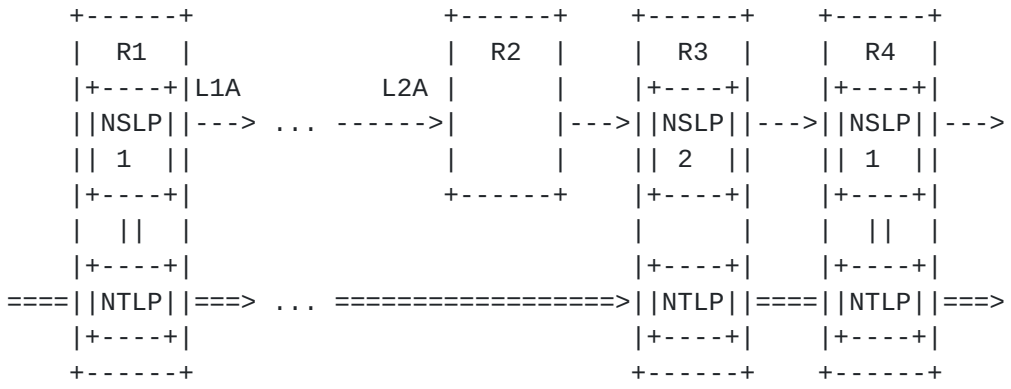


Figure 6: Case C: UCOR is a FNE

The following three figures show the three possibilities after path change for the example network:

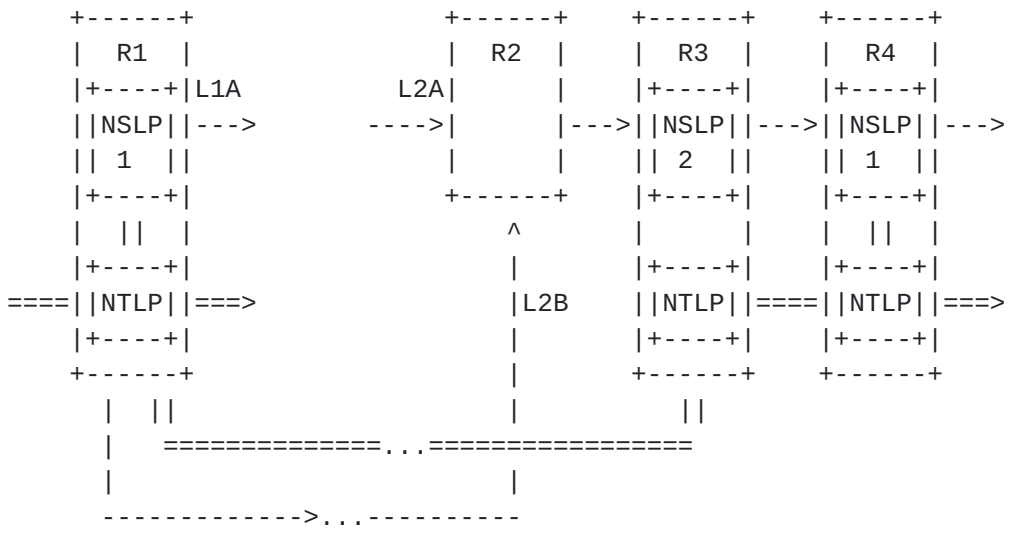


Figure 7a: Case C.I: DCOR is a NNE

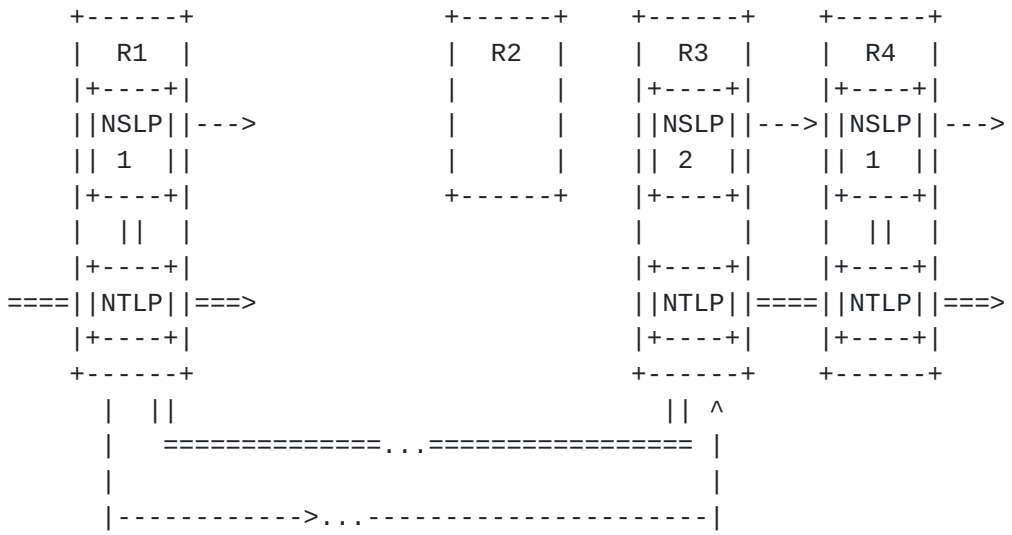
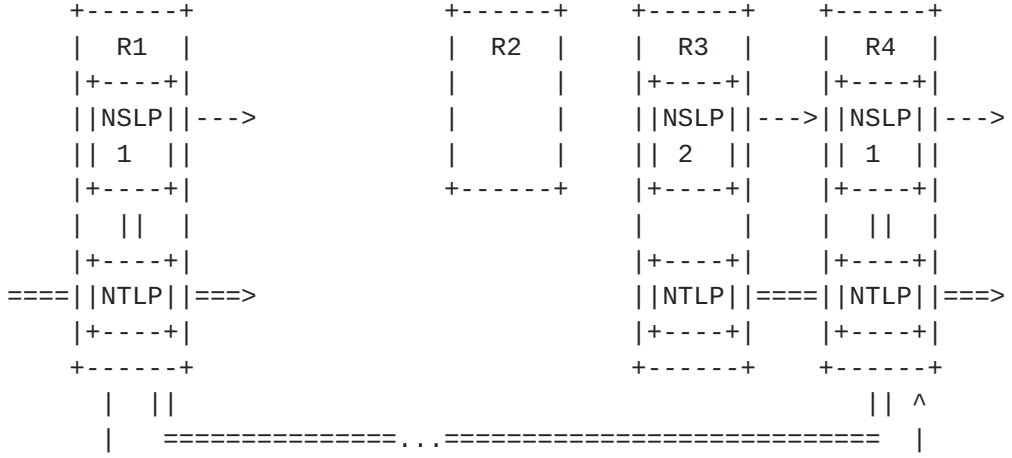


Figure 7b: Case C.II: DCOR is a PNE



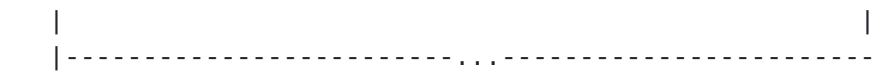


Figure 7c: Case C.III: DCOR is a FNE

Following is a summary of the above 9 cases with their indexes (UCOR-DCOR).

- o A.I NNF - NNF
- o A.II NNF - PNF
- o A.III NNF - FNF
- o B.I PNF - NNF
- o B.II PNF - PNF
- o B.III PNF - FNF
- o C.I FNF - NNF
- o C.II FNF - PNF
- o C.III FNF - FNF

In all above 9 cases, route change will affect the NTLP/NSLP peer relationship of the UCOR and DCOR depending on the number of NEs in the old path and new path between the UCOR and DCOR. The 6 mobility cases as simplified versions of the route change cases may be derived from above figures by taking away either UCOR or DCOR appropriately. So similar changes in NTLP/NSLP peer relationship of UCOR/DCOR can be expected.

3.3. Detection of Session Path Change

By default the time until some action may be taken to tackle the path divergence depends on when the next signaling action (e.g. NTLP refresh or NSLP refresh, if applicable) is scheduled. Path change detection may be used to shorten this period. The detection mechanism is also related to its causes: route change or mobility.

In this section we only discuss route change detection. Note that mobility caused path change would usually be triggered by node movement. Movement detection is part of the mobility scheme and out of scope of this document.

A summary of route change detection methods are provided in [1].

(a) monitoring changes in local interface state

(b) monitoring topology changes in a link-state routing protocol

(c) inference from changes in data packet TTL

(d) inference from loss of packet stream in a flow-aware router

(e) inference from changes in signaling packet TTL

(f) changed route of an end-to-end addressed signaling packet

(g) changed route of a specific end-to-end addressed probe packet

These methods can be categorized as being based on network monitoring (method a-b), based on data packet monitoring (method c-d) and based on monitoring signaling protocol messages (method e-g).

Whatever method is used, the detection function needs to be mapped to NTLP, NSLP and the corresponding routing related module.

Network monitoring based approach is applicable in all NNE, PNE and FNEs. It is usually used to detect downstream route change. Data packet monitoring is in theory possible in all NE types. In reality it would only ever be done on FNEs. This is because in order to monitor the data flow right, the NE needs to be told about its characteristics, and only an FNE would have this information. Signaling protocol message based monitoring is usually applicable only in PNE and FNEs, but not in NNEs. It is usually used to detect upstream route change.

From Signaling application point of view, if the detection is not done by itself, there are normally two methods it can learn about path change from the actual detection function: polling or asynchronous notification.

3.4. Response to Route Change caused Session Path Change

In this section we look at responses of nodes that detect path changes (refer to as detection nodes below) upon a session path change event. The main focus here is to identify the UCOR/DCOR and take appropriate local repair actions. Local repair essentially tries to achieve the following as fast (and secure) as possible: Installation of state on the new path; and removal of state on the old path. Under the layer split concept, we will probably have local repair problem in both layers. It is important to note that, generally speaking, to do any of these route change procedures, an involved node has to have per-flow state ('be a stateful node' in Westberg-speak).

3.4.1. Network Monitoring based UCOR detection

Network Monitoring may be used to identify UCOR. It is important to note that in case of route change, a chain of routers between the actual UCOR and DCOR, inclusive, may detect the route to a destination has changed. But only the first router where the session traffic actually starts to diverge should be identified as UCOR. It is still an open question how these routers may decide locally whether they are indeed the UCOR or not.

If this kind of decision can be made, those Detection Routers other than the UCOR or DCOR may do the following depending on its NSIS capability: do nothing (NNE); delete the existing session state (FNE) and delete related NTLP state only if the connection is also no longer used by any other session (PNE and FNE). Alternatively, the Detection Routers other than UCOR or DCOR may do nothing but waiting

for explicit state teardown or timeout.

The action taken by UCOR also depends on its type.

If UCOR is a NNE (case A.I-A.III), there is nothing much we can do.

If UCOR is a PNE (case B.I-B.III), an NTLP level local repair is invoked. This may involve: if a "rediscovery timer" (such as in [2] similar to the route pinning effect) is used, stop it immediately (un-pin the route) and construct a discovery message for an immediate peer discovery. The discovery result will tell the NTLP whether its peer has changed or not. If a new peer is discovered, NTLP may create an association with the new peer and teardown its original association with the old peer (if that connection is no longer used by any application sessions). In either case (NTLP peer changed or not), subsequent NSLP refresh for this session will be able to use updated peer information without delay.

If UCOR is a FNE (case C.I-C.III) A NSLP local repair may follow the NTLP local repair. In these cases, the NTLP may deliver a signal to NSLP that causes NSLP to start a local repair for downstream route change. An example procedure could involve: NSLP sends "RESERVE" refresh (as in terminology of [3])immediately, without waiting for the refresh timer timeout. This message will be forwarded by NTLP towards its updated peer and thus setup necessary states in any newly added NSLP nodes up to the DCOR. Explicit teardown of orphaned states in the obsolete path might be initiated by messages from UCOR, DCOR or even those routers themselves.

If NSLP level local repair is desired in the case when UCOR is a PNE, the NSLP needs to maintain a reverse routing state vs. flow id. The PNE noticed a routing change for a given flow id, and knows any NSLP-aware nodes that can handle the route change must be upstream of it. So it looks up the reverse routing state table and notifies its upstream neighbor, and then the upstream neighbor (which may be another PNE) has to repeat the process until an FNE is reached. (What is hard is for the upstream node to know whether or not to forward this notification any further.)

3.4.2. Data Packet Monitoring based UCOR detection

These two methods could give some idea of upstream route change, but do not tell exactly where the change is. Also there could be many detection nodes but hard to tell which one is the Action Node. It might be costly to ask each of them to do local repair. But if they indeed do, the process might be similar to that in the next section.

3.4.3. Signaling packet Monitoring based DCOR detection

Signaling Packet Monitoring may be used to detect upstream route changes. As mentioned above, this approach requires that the DCOR be signaling aware so these cases correspond to cases A.III, B.III,

C.III. In a way similar to that of RSVP, NSLP can identify DCOR by comparing the SII contained in the signaling message. For example, if the "RESERVE" message for the same session is found to have arrived from a node with a different SII, upstream route change is assumed.

The main action DCOR needs to take is the removal of orphaned state in the obsolete path. (Only applicable when those routers between UCOR and DCOR cannot delete the state themselves earlier). This also requires the NTLP to support explicit routing based on SII. The DCOR issues a teardown message towards the old peer's SII, this message will be routed peer to peer in the reversed direction along the obsolete segment and tear down any related state inside the segment. This teardown message might also contain some flag indicating it is a local repair teardown to facilitate them being identified by the UCOR. UCOR should terminate the local repair teardown messages when they arrive.

3.5. Other cases

There are several cases that the above discussion does not cover, including case A.I,A.II, B.I,B.II, C.I,C.II, when the DCOR is not FNE. In fact, it seems that if the Detection Routers between UCOR and DCOR do not require an explicit state teardown message, these cases will be fine as far as DCOR is concerned. Otherwise, more analysis is needed.

3.6. QoS routing Considerations

The above discussion applies to normal routing mechanisms which do not differentiate route selection for signaling packets or data packets. In the presence of QoS routing, it is important to make sure signaling packets and data packets of the same session will select the same route for path-coupled operation. If route pinning is used, the route should be unpinned immediately whenever a route change is detected or notified. Other than that, the process should be similar to that of the above.

3.7. Response to Mobility Caused Session Path Change

Mobility caused session path change can be divided into path change with or without change of Flow ID. The case without change of Flow ID usually falls into the Micro-mobility category. The analysis of this case will be provided in a later version of this document.

4. IP Mobility and Multihoming

4.1. Comparison with Route Changes

The basic case of route change processing for a single flow can be extended to the more complex situations of IP layer mobility and multihoming. These have several aspects in common with the route

change case, specifically:

a) the significance of upstream and downstream crossover routers (including how to find them, especially in heterogeneous signaling

application environments)

b) the possibility that the characteristics of the two path segments may be very different (for example, with different resource availabilities, or even supporting totally different resource negotiation capabilities)

c) the possibility that the different paths may traverse different administrative domains, so that authorization status for one path may be inapplicable to the other.

However, there are several features of the IP mobility and multihoming situations which lead to additional requirements on the signaling, or suggest that alternative signaling designs may be appropriate. The most important of these are as follows:

1. IP mobility and multihoming introduce a new address for the mobile or multihomed node, and this address will lead to a new flow identification. This new flow identification will (generally) have to be communicated to the correspondent (so it can update transport or application layer state to recognize the new flow), and also to intermediate nodes on the path (so they can update packet classifiers to recognize the new flow). In contrast, in the route change case, it may be possible to hide the signaling entirely between the UCOR and DCOR, especially if path characteristics and authorization properties do not change.

2. The 'new' flow may persist for some time in parallel with the old. This is certainly true in the multihoming case, and can also be case with IP mobility. Indeed, the most important initial usage of IP mobility may be mainly in inter-technology, inter-system scenarios, where the actual 'handover' process takes a long time to complete, and so make-before-break is actually necessary to achieve any form of session continuity. The signaling solution therefore has to manage these two flows 'side-by-side', as compared to the route change case where a very rapid flow path modification is the goal.

3. Conversely, in the IP mobility case, it is also likely that at some stage the 'old' flow involving the old IP address has resources which are to be released, but that the old flow path is not physically available to send signaling messages on (and even that the old IP address is not even valid). This can make explicit teardown of such resources much harder; however, since this includes scarce resources on access links, it may be that long refresh times are in use (to minimize signaling overhead) and so explicit teardown is of additional importance. In the route change case, the UCOR and DCOR are typically reachable even after the route change, at least by some path.

4. Mobility events and multihoming configurations are generally known (and in fact initially only known) to the flow endpoints and cannot be independently detected in the network infrastructure (except in the micro mobility scenarios mentioned in section TBD 3.7). Therefore, crossover router discovery has to be done as a side effect

of NSIS signaling exchanges, often end to end ones. Discovery is therefore a more time consuming process, but less vulnerable to the complex case where multiple nodes believe they are the crossover router, which can occur in the route change case with local signaling repair being triggered by direct interactions with the routing process.

5. Finally, the most significant difference is that in the mobility and multihoming case, the network infrastructure is asked to perform joint operations on two different flows which are only associated by their session identifier. However, only the flow endpoints have any reason to accept assertions about the relationship between such flows: the signaling initiator is actually responsible for choosing the session identifier for each flow, and its correspondent will have been updated (somehow, presumably securely) at the transport or application layer.

In contrast, nodes within the network have no reason to accept that a new flow is related in any way to the old; we have to prevent the situation that any node in the Internet can send a signaling message into the network with a session identifier which effectively 'steals' resources at any node it crosses which has a flow with a matching session identifier. These and other security issues with the session identifier have been analyzed in more detail in [4]. In the route change case, the flow identifier is constant and flow identifier spoofing is difficult in practice because of the constraints imposed by the routing system. Decoupling the session identification from these constraints is the signaling equivalent of breaking the connection between locators and identifiers, which is well known to lead to a large of number of interesting security issues; an excellent overview of these issues in the context of Mobile IP is provided in [5].

4.2. Analysis Overview

In what follows, we consider the impact of these mobility and multihoming specific considerations on a set of four basic scenarios, similar to the route change analysis of the previous section. The requirements on session identifier behavior are outlined, as well as the implications for overall signaling behavior and consequences for signaling update latency. These 'call flows' can be used as a starting point for deriving requirements on detailed NSIS functionality to support mobile or multihoming operation; some of these are mentioned during the analysis.

We consider here only a simplified set of possible scenarios. Specifically, we initially only have four. In what follows we use the term MN for the mobile or multihomed node, and CN for its

correspondent.

*) There is a choice of whether the session (i.e. the paired flows) is inbound or outbound from the MN;

*) There is an independent choice of whether the MN or CN has initiated the signaling.

In addition, for each scenario, we consider the cases of setup of the new flow and the teardown of the old (of course, these two could be carried out simultaneously).

This is still a highly simplified set of possibilities. Our main restriction is that there is a hop-by-hop authorization procedure, where each node requests resources or other state manipulations from its direct NSIS neighbor, and this request propagates from one end of the flow (the initiator) to the other (the responder). Clearly, more complex authorization scenarios are possible, and this would have a major impact on the analysis. It turns out that the hop-by-hop authorization assumption, while a very natural approach (and possibly the only one which is operationally feasible), has a strong influence on what exchanges are necessary and restricts how much these can be optimized. Further discussion of the NSIS authorization problem, specifically in the case of QoS, is contained in [6].

In addition to this simplification, we only consider homogeneous signaling environments, where the single signaling application is supported on all the nodes we care about (i.e. every node considered below is an FNE, including MN and CN). Also, for this mobility analysis, we have not attempted to distinguish precisely between NSLP and NTLP functionality, except in separating the concept of setting up reverse path state and installing signaling application state (the former being basic NTLP functionality and the latter being the role of the NSLP, along with authorization aspects).

In the teardown case, it is still somewhat open whether a tear can propagate in the opposite direction to the original state setup. This would correspond to a node removing state which it did not install, and therefore might not be consistent with a strict viewpoint on authorization. However, in a soft-state protocol, the same effect can in any case be simulated by having nodes unilaterally reduce their state refresh period to some small time and notify their initiating peer of this fact in case the state still needs to be retained for some reason. We call this process 'accelerated expiration'. (If this whole discussion seems absurdly finicky, simply replace the phrase 'accelerated expiration' by 'teardown by the responder'.)

One of the main goals of this signaling is to avoid double reservations on the shared path segment. Influenced by the QoS use case, we refer to this as 'state sharing' (e.g. a resource reservation can be used by packets for either flow). In reality, the correct processing depends on the specifics of the signaling application, for which the concept of sharing might not even apply, but some form of merging or joint processing still would.

4.3. MN-Terminating Session

In the case where the session is terminating at the MN, we have the situation shown diagrammatically in Figure 8.

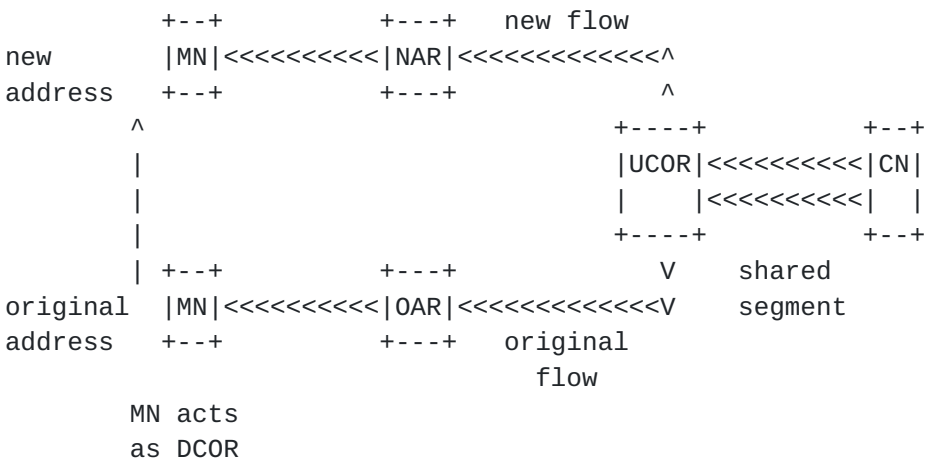


Figure 8: Session from CN to MN

The following facts are common to both sender and receiver initiated variants:

*) In general, only a NSIS message sent all the way downstream from the CN can discover the UCOR.

*) The CN must know the MN's new address to be able to send this message.

*) The CN must be informed of this new address by a (end-to-end) upper layer message from the MN. We refer to this message as 'add-IP'; it can be sent as soon as the MN is <= 1RTT in advance of being able to receive messages addressed to it. It is this message which must initiate the whole re-routing process.

The MN- and CN-initiated cases are now considered separately.

4.3.1. CN (Sender) Initiated Setup and Teardown

The sender initiated case is the simplest of all the four cases, for both setup and teardown.

For the setup case, the NSIS function in the CN is triggered by the add-IP message. Because the CN is managing the signaling for the session anyway, it has all the information necessary to be able to send a single downstream NSIS message for the new flow which travels

all the way to the MN; in particular, the CN can make the correlation between the old and new flows based on local upper layer information and set the session identifier in the signaling for the new flow appropriately. On the shared segment, it can update the state to

refer to both flows for the same session identifier; on the new segment, it installs state in the normal way for a new flow (this includes any admission control operations). Flow traffic can be sent immediately after this NSIS message has been sent, and it will receive correct treatment provided it does not 'overtake' the signaling (which could travel more slowly on the new path segment, since the NSIS processing there is more complex).

For the teardown case, the simplest solution is that the MN sends a corresponding 'delete-IP' message end-to-end to the CN, which then tears the old flow state down in the same way.

Another possibility is that the MN could send this delete-IP in an upstream NSIS message hop-by-hop, which would remove the state by accelerated expiration and carry the upper layer delete-IP message as a payload. Ideally this can be sent via the OAR, either directly from the MN or via the NAR if FMIP edge tunneling or context transfer is being used. Otherwise, it has to be sent using the reverse path state of the new flow, but ignored until it reaches the UCOR at which point it continues upstream as normal and is also reflected back along the old path towards the OAR as far as possible. Traffic sent by the CN during this time (while the delete-IP message is still propagating upstream) will receive degraded treatment as the state is gradually removed.

In both teardown cases, there is a potential race condition if the teardown or its equivalent is processed on the shared segment before the installation of the new flow state (because then the session as a whole would be lost there and the new flow state request would have to go through admission control). This means that the MN must monitor inbound NSIS signaling and only generate messages which could start the teardown process when the new flow setup has apparently completed.

All of these message sequences are shown diagrammatically in Figure 9.

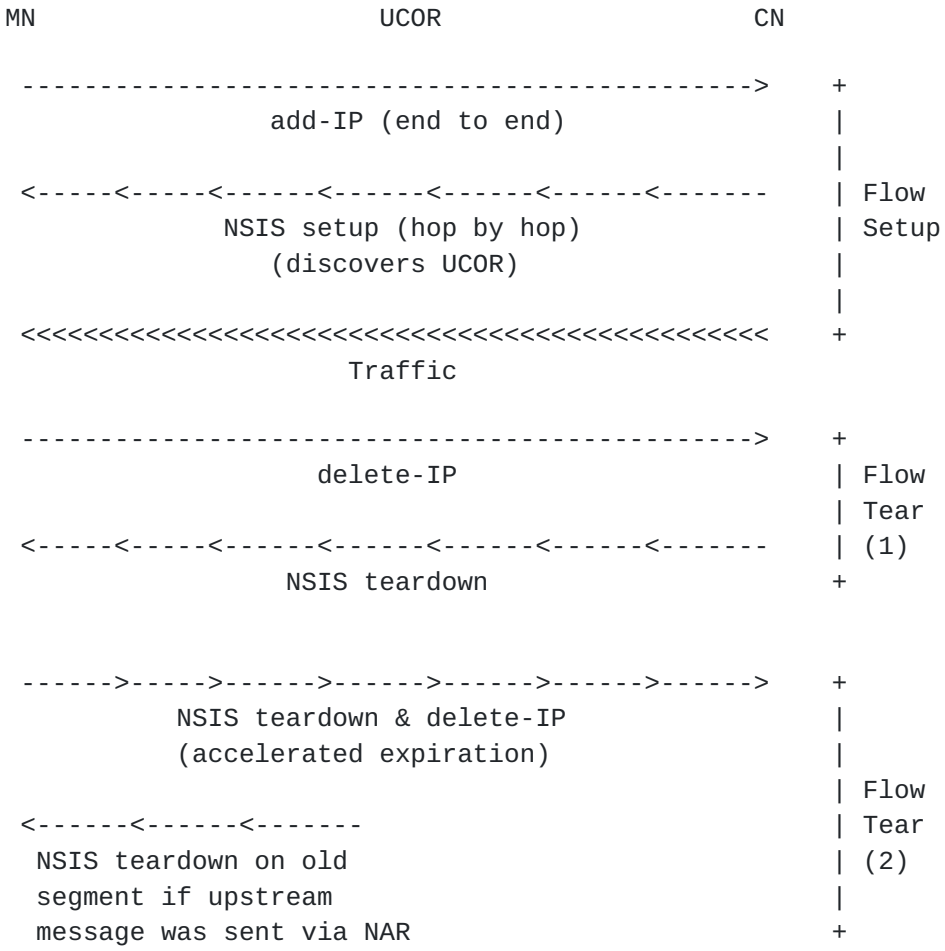


Figure 9: CN(Sender)-Initiated MN-Terminating Flows

Session Identifier Security Considerations: In this particular case, there are no interesting requirements on the session identifier. This is because all signaling state modification requests are either 'fresh' (and so no optimizations were possible with it anyway), or because the requests come from the same peers as the state was originally installed by, and the initial request comes from the initiator itself. (It will be seen that all the other cases are rather more complex.)

4.3.2. MN (Receiver) Initiated Setup and Teardown

The receiver initiated case is more complex than the sender initiated case, for both setup and teardown.

For the setup case, the process begins the same as with sender initiation, with an end-to-end add-IP message. Even though the CN is not controlling the overall signaling process, its NSIS function must still be triggered by this to send a downstream NSIS message whose

sole purpose is to discover the UCOR and set up reverse routing state on the new path. In principal this should be no different from what was needed to set up reverse routing state for the original flow; however, the NSIS message needs to include the same signaling

application identifier and session identifier as used for the signaling for the original flow. This may have some implications for how the session identifier values are managed.

There are then two cases for how the actual state installation should take place. This has to be done by signaling messages flowing in the MN-CN direction.

1. The downstream message goes all the way to the MN on the new path; this is followed by a setup message in the upstream direction. This is processed normally on the new path segment, and once it reaches the UCOR state merging can take place on the shared segment.

2. The downstream message reaches the UCOR, and this is immediately able to begin state merging on the shared segment. In the meantime, the downstream message continues to the MN and causes state setup on the new path segment (but this only needs to carry on up to the UCOR).

These two options are illustrated in Figure 10. There are different options for when traffic can be sent from the CN, depending on whether the CN waits to see that state has been installed before using the new path. In particular, if the CN wants a guarantee that state has been installed end to end, the timing optimization of option (2) is not actually exploited in reality. The two options differ in what requirements are placed on the session identifier so far as implied authorization is concerned, and these are discussed at the end of this subsection.

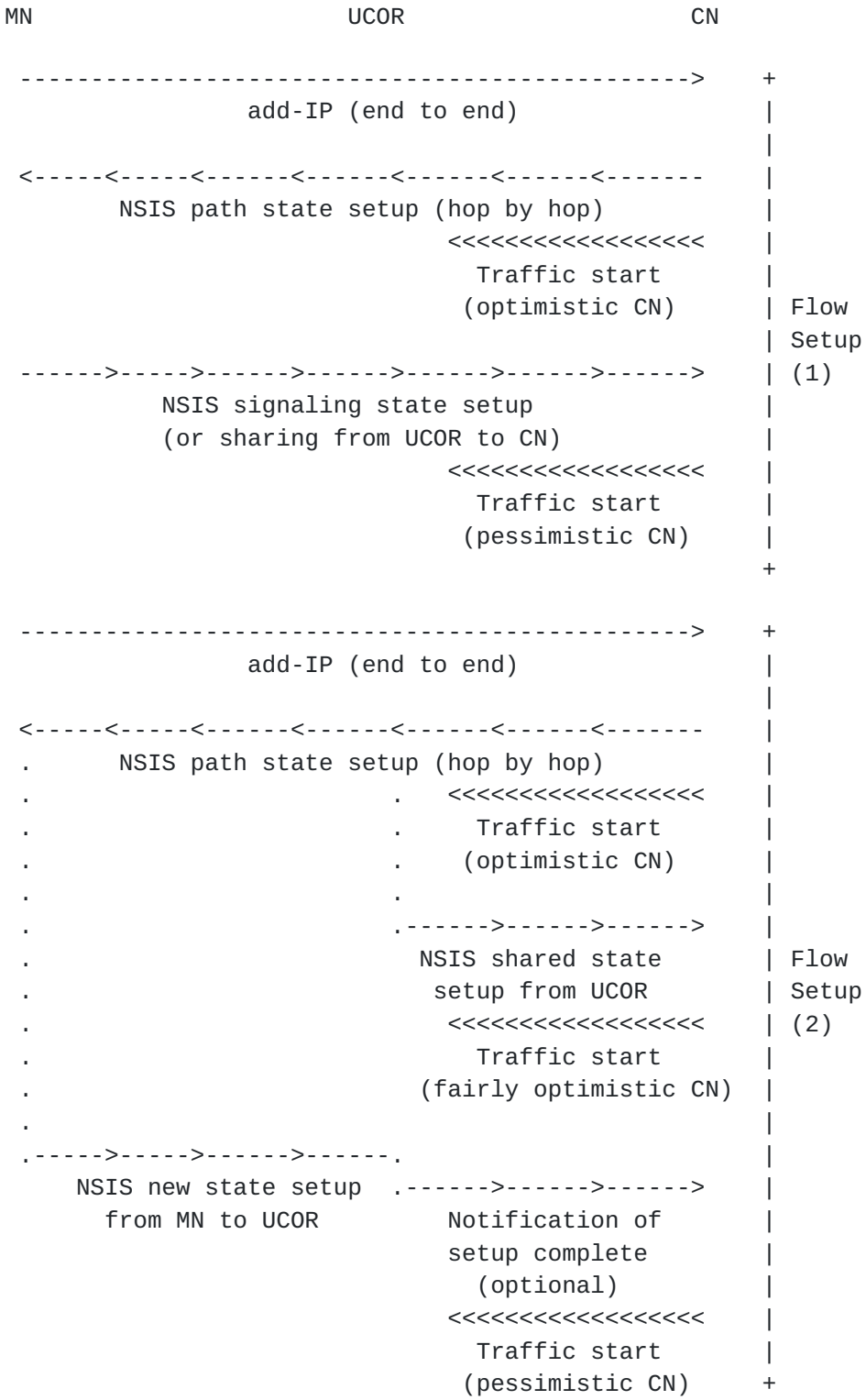


Figure 10: MN(Receiver)-Initiated MN Terminating Flows
(Setup cases)

The teardown case can be handled in two ways also. If the route via

the OAR is still available (directly or via the NAR), the MN can send an upstream hop-by-hop NSIS message which removes state on the old path and can carry delete-IP as a payload. If the route is unavailable, this message has to be sent upstream using the reverse path state of the new flow; from the UCOR to the CN it is handled as

normal, and at the UCOR it is turned round and used to remove the old path state via accelerated expiration. The same possibilities for a race condition exist as in the CN(sender) initiated case. These sequences are shown in Figure 11.

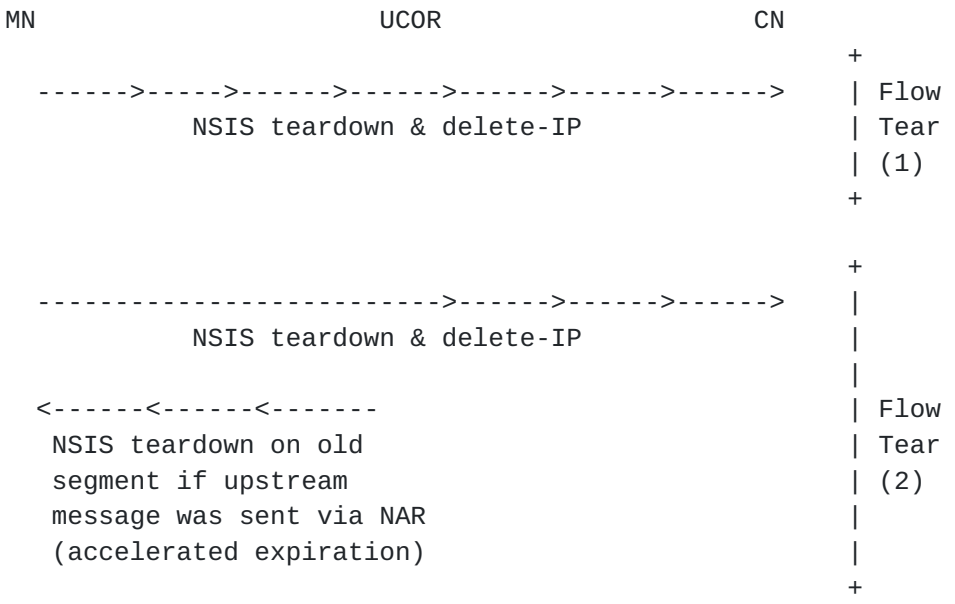


Figure 11: MN(Receiver)-Initiated MN Terminating Flows (Teardown cases)

Session Identifier Security Considerations: For this receiver initiated case, we have two security issues for the session identifier, and which ones are relevant depends on which setup message sequence is used.

*) The 'Different Peer' Issue: When the UCOR sets up the sharing of signaling state for the two flows on the path back to the CN, it is essentially saying: "the state which I previously installed on behalf of my downstream peer on the old path [e.g. maybe the OAR] can now also be used on behalf of my downstream peer on the new path [e.g. maybe the NAR]". In other words, the UCOR has to reason that the two downstream peers (who could be in different administrative domains and may have no knowledge of each other) are happy to have their independent requests for upstream state use shared resources solely on the basis that the session identifiers match, and hence (presumably) that they originated with the same MN. A legalistic downstream peer on the old path might claim that the resources it had reserved and paid for on the shared segment had just been been stolen. This assumption is needed for both setup cases.

*) The 'Indirect Initiator' Issue: In addition, when the 'speeded up'

setup approach (case 1) is used, where the UCOR begins to install state sharing on the upstream path as soon as it has seen the downstream path state message with an existing session identifier for a new flow, the UCOR is doing this without having received any signaling message originating (directly or indirectly) from the MN

which actually initiated the signaling. In other words, the UCOR is saying "I believe that the new flow I am being told about for this session identifier is one which is for the same MN as the existing flow, and I therefore believe that MN will be happy for state to be shared between the two flows". If the UCOR is only willing to proceed after verifying this information by a signaling exchange which involves the MN itself, this reduces to the simpler case 1 setup approach, i.e. with no latency saving.

Note that no additional considerations apply from the teardown case, because either signaling comes from the MN like a normal teardown or accelerated expiration is used.

4.4. MN-Originating Session

In the case where the session is originating at the MN, we have the situation shown diagrammatically in Figure 12.

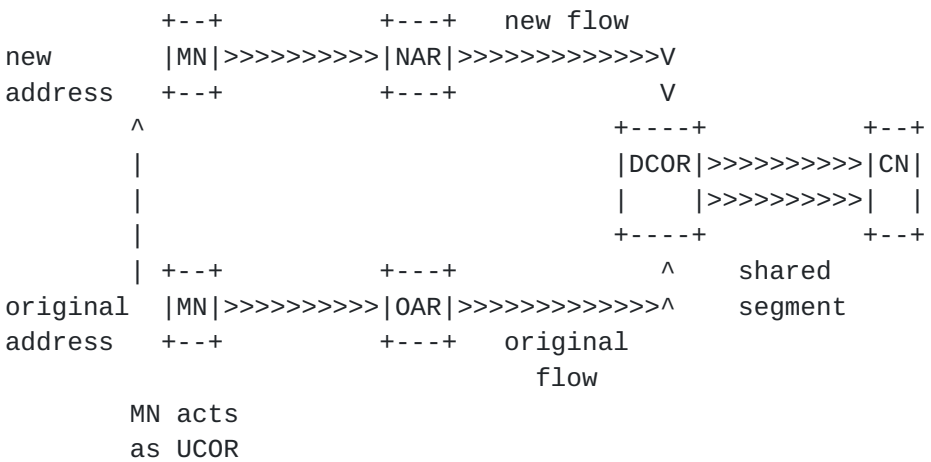


Figure 12: Session from MN to CN

The general treatment of the MN originating session is simpler than the MN terminating case, because the node which has moved can also directly generate the signaling which discovers the COR - there is no need to involve the CN in this process. However, we still expect there to be an end to end add-IP message, if only to inform the CN of the new address (without which traffic sent from this new address will probably be ignored or filtered). This message can be sent as soon as the new IP address is active, and traffic can be sent as soon as the add-IP procedure is complete. The remaining discussion differs between the MN- and CN-initiated cases.

4.4.1. MN (Sender) Initiated Setup and Teardown

The setup case is relatively simple here. The MN originates an NSIS signaling state setup message for the new flow with the same session identifier as for the existing flow (which it chose anyway). This has to be sent on the new path (via the NAR) and state is set up from

the MN to DCOR in the normal way. The DCOR can be identified when it processes this message, and the remainder of the state is set up shared with the existing flow from the DCOR to the CN.

For the teardown case, no delete-IP message is strictly needed (the MN just stops using the old address when it feels like it). If the NSIS teardown message can be sent using the old path (via the OAR), state teardown is done in the usual way (once the state for the new flow has been set up, i.e. to avoid losing the state completely on the shared segment). If only the new path is available, the message has to be sent via the DCOR and use accelerated expiration on the upstream segment from the DCOR towards the OAR. This is basically the same set of possibilities as for receiver-initiated MN-terminating flows (which is reasonable, since in each case it is the MN which is managing the signaling process).

All these message sequences are shown in Figure 13.

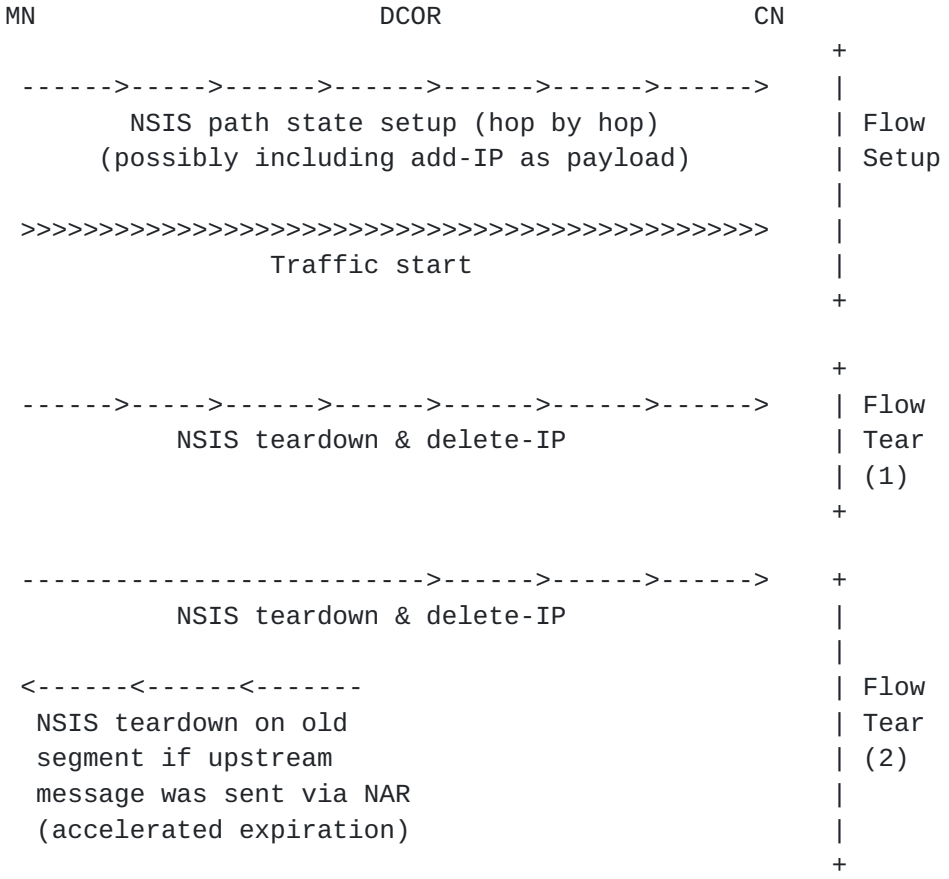


Figure 13: MN(Receiver)-Initiated MN Terminating Flows

Session Identifier Security Considerations: The 'Different Peer' security issue applies to state sharing on the shared path segment

identically as in the other MN initiated case. However, since all state manipulation messages originate at the MN, the 'Indirect Initiator' issue does not arise.

4.4.2. CN (Receiver) Initiated Setup and Teardown

The setup case here has to install reverse path state to allow the signaling state manipulation messages to propagate upstream from the CN. Note that the reverse path state is being installed for the new flow, and at the DCOR this will be different from the reverse path state for the existing flow for that session. Therefore, the reverse path state must be indexed by the flow identification, rather than the session identification.

Once reverse path state has been installed, signaling state installation can be done by two methods, similar to the other receiver initiated case. The difference is that the 'early' setup can take place on the new path segment rather than on the shared path segment.

Teardown is quite simple in this case. A delete-IP message is needed to inform the CN that the old flow is no longer active; however, once this has been received, the teardown can be initiated from the CN with normal signaling (the necessary reverse path state already exists to route this signaling).

All these signaling exchanges are shown in Figure 14 below.

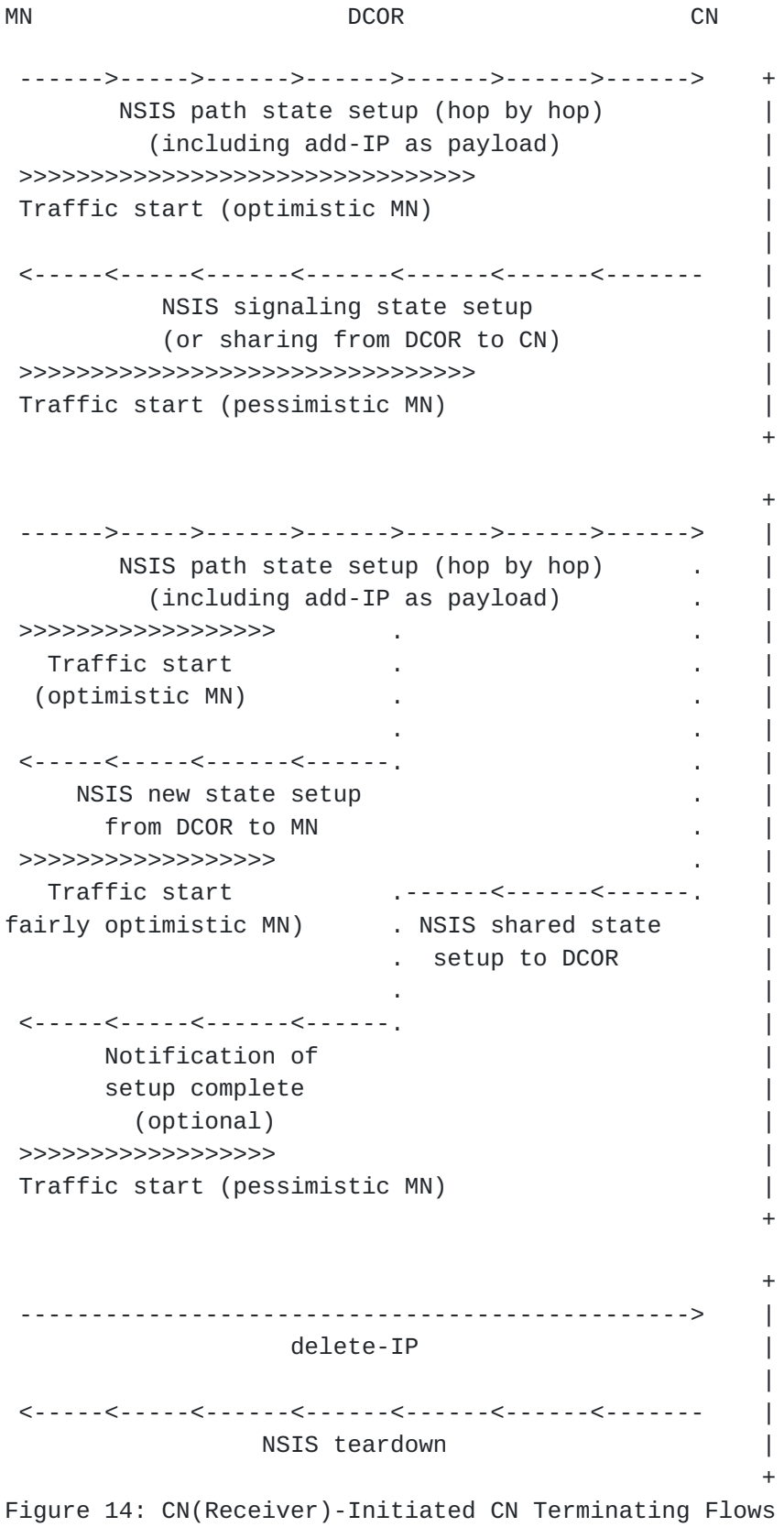


Figure 14: CN(Receiver)-Initiated CN Terminating Flows

Session Identifier Security Considerations: In this case, the shared path segment has both flows initiated by the same endpoint. Therefore, the 'Different Peer' issue does not arise. However, the 'Indirect Initiator' issue arises in the second flow setup case, where the DCOR attempts to install state on the new path segment

before any signaling messages have arrived from the CN. As before, any confirmation exchange between the CN and DCOR reduces this case to the simpler setup exchange.

4.5. Summary of the Analysis

The most significant conclusion of the analysis is that the interaction with the authorisation model has extremely important impacts on the message flows. In many cases, the information needed to complete the mobility processing (updates on the shared path or installation/teardown on the new and old segments) is available at the crossover router quite early in the message exchange, but the crossover router may be unable to use it because it comes from an unknown neighbour or from the 'wrong direction'. This is therefore an authorisation issue. Authorisation interactions are sometimes considered as an 'add-on' during design, especially if some sophisticated special purpose authorisation protocol is being used. However, even the filtering that is done on messages to ensure they come from an appropriate source can be considered as an authorisation issue; ignoring these issues when designing the basic message flows is liable to mean that the protocol design ends up being fundemantally incapable of being secured against theft-of-service attacks and other abuses.

Because the authorisation constraints arise from the hop-by-hop authorisation assumption, it might be that a more flexible or powerful authorisation model would make mobility handling much easier. For example, if the signaling initiator had a direct authorisation relationship with the COR, most of these problems would be eliminated. However, the consequence of routing is that in general the COR can be anywhere in the network, and the precise location of the COR depends on what handover has taken place and the flow direction. Therefore, in general, to have a prior authorisation relationship with the COR means in practice that the signaling initiator must have this relationship with every NSIS node along the flow path; this is likely to be operationally infeasible.

Two different session id security issues were identified, the 'Different Peer' and 'Indirect Initiator' issues. The applicability of these issues is shown in the following table (which has some pleasing structural symmetries).

Table 1: Applicability of Session Id Issues to Various Scenarios

Mobile originating or terminating?	Sender or receiver initiated?	Different Peer issue	Indirect Initiator issue
Terminating (inbound)	Sender	N/A	N/A
Terminating (inbound)	Receiver	Applies to resource sharing on shared segment	Applies only if accelerated setup on shared segment is done from UCOR
Originating	Sender	Applies to resource sharing on shared segment	N/A
Originating	Receiver	N/A	Applies only if accelerated setup on new segment is done from DCOR

The indirect initiator issue applies in 50% of the cases, but only if speedup up state installation is needed from the COR. This case needs to be analysed from two perspectives:

*) Whether the speedup is actually valuable. Clearly, in some cases (e.g. multihoming) it is probably not; on the other hand, if one is attempting to achieve a seamless hard IP handover, every speedup is valuable. Techniques such as those in [Thomas] could be used to model whether signalling is on the critical time path in the overall setup process.

*) Whether the threat is real, and what form of session identifier protection mitigates it best.

The different peer issue also applies in 50% of the cases, but is unavoidable in those cases. Whether it is a problem depends again on finer details of the authorisation model. For example, one approach would be for the second flow on the shared segment to be given a lower priority (if this concept is applicable to the signalling

application in use); this prevents it from stealing resources from the first flow, only using resources that the first flow is not using. In slow time, the new peer would take over the session completely (e.g. after the first flow is deleted). This would be perfectly applicable for QoS signalling for example, but might be

very dangerous for middlebox control.

The analysis also exposes some interesting protocol interactions in the end system, especially concerning how and when addresses are allocated and released and used for traffic, and how and when session identifiers are allocated and coordinated. Race conditions could be commonplace and additional end-to-end or end-to-COR acknowledgements might be needed to handle them. This requires further call flow analysis, but can probably only be completed once the allocation of mobility functionality to different layers of the NSIS protocol stack has been defined in more detail.

A topic that has not yet been considered is the use of network internal mobility proxies (e.g. as are used in several local mobility management schemes). These have several properties which are very relevant to the issues analysed here, in particular:

*) they may be able to hide the end system address change (making it look more like a routing change);

*) they may provide a fixed internal node which will always be the COR for a local mobility event, or at least allow the COR to be pre-authorisation between the MN and proxy, which could address both of the session id security issues (especially the indirect initiator one).

Further analysis of such LMM solutions is needed to determine whether there is a common signalling approach to each of them, and whether signalling interactions with them can be constrained inside the network or whether it would require different behaviour in MN or (even worse) CN to exploit them.

4.6. Further Interactions with Fast Handover Protocols

In the context of mobility between different access routers, it is common to consider additional local performance optimizations in two areas: selection of the best access router to handover to, and transfer of state information between the access routers to avoid having to regenerate it in the new access router after handover. The Seamoby working group is developing protocols solutions for these functions (CARD and CT respectively) but the following considerations apply to these functions in general, regardless of which particular protocol is used to implement them.

Detailed solutions are not proposed here, but rather a discussion of the way in which these functions should interact with NSIS signaling. In addition, signaling should be able to operate independently of these protocols (and this is the assumption for the main mobility analysis earlier in this document). However, significant performance

gains could be achieved if they could be made to cooperate. In addition, the resource signaling aspects of these CARD/CT and NSIS protocols could profitably use a common set of resource types and definitions, since they will probably be supporting the same overall

signaling application.

The question arises, what the mode of interaction should be: independent operation, NSIS triggering access router discovery and state transfer, or vice versa. The questions for the two cases seem to be independent.

For access router discovery, a typical model of operation is that the mobile carries out an information gathering exercise about a range of capabilities. In addition, where those capabilities relate purely to the AR and mobile, there is no role for NSIS (its special functionality is not relevant). However, considering resource aspects, one aspect of the AR 'capability' is resource availability on the path between it and the correspondent, and NSIS should be able to fulfill this part. Indeed, this is effectively precisely the application considered in [7], where it is a sort of special case of resource signaling during handover. This means that CARD should be able to trigger some of the NSIS signalling, maybe discovering COR location and checking admission control status on the new path, before the handover has actually taken place.

Therefore, a possible model of access router discovery/NSIS relationship is that some entity in a candidate AR triggers NSIS using resource and reservation information (including session id) from the current AR to find out about what would be available on the new path. Note that this should be a query rather than an actual state setup; this semantic could be included either in the service definition or the signalling itself.

The case of state transfer is more complex. There are two obvious options, corresponding to whether one transfers just signaling application state or NSIS protocol state as well:

1. "State transfer triggering NSIS": A state transfer process passes the to request that resource.

2. "NSIS using state transfer": NSIS transfers its own state information from the old to the new AR. It can then carry out the same update signaling as though it was a single 'virtual AR' which had just had a topology change towards the correspondent. (This is essentially the conceptual model of [8].)

The first model is simpler, and maybe more in line with the basic state transfer expectation; however, it seems hard to avoid double reservations since the two NSIS protocol instances are not coordinated (if we regard the session identifier as part of NSIS protocol state rather than signaling application state). In addition, NSIS protocol state may itself be time consuming to set up (for example, if it requires peer-peer authentication before actual

signaling messages can be transferred.) Therefore, the second model seems more appropriate. An advantage of the 'virtual AR' model is that it ensures that the impact of the interaction is limited to the NSIS instances at ARs themselves, since the rest of the network must be able to handle a topology change anyway: the scenario looks more

like a route change with an IP address change rather than a full mobility event.

Note that there is an open issue of who is responsible between the mobile and AR to decide that the state transfer procedures have not happened for whatever reason - e.g. because they were not even implemented - and take recovery action to have the mobile refresh reservations promptly. It appears this has to be an NSIS responsibility in the AR, and probably requires a custom notification message for this circumstance.

5. Security Considerations

This draft discusses signaling flows to handle route change and mobility events and multihoming scenarios. Many security considerations apply to such signaling flows; in particular, all the issues of message protection, denial of service protection, theft and abuse of service, authorisation and so on that apply to the 'normal' signaling case continue to apply here also.

Some special considerations arise from the route change/mobility issues discussed in this draft. In particular, authorisation for path change (for flows) and more particularly for flow change (for sessions) needs to be considered carefully. The latter is extensively discussed in section 4, and section 4.5 in particular.

A second special issue is the need to do rapid signaling exchanges during or after handovers. This is not a security issue itself, but it does impose new performance constraints on the security mechanisms that are used to protect signaling in general. Specifically, in the case of a MN attaching to a new AR, the need for time consuming node authentication procedures before signaling information can be exchanged should be minimised; this might be a motivation for context transfer of such authentication state.

It appears that there are few or no new basic denial of service attacks that arise in these scenarios (or rather, any attack that could be mounted in these scenarios could also be mounted in the normal case). Instead, the new problem is that signaling flows which might have been seen as denial of service attacks in the normal case (such as signaling messages for a flow arriving from a previously unknown peer) now have to be treated as potentially legitimate and secured by other means.

Once the functionality described in this document has been allocated to specific components in the NSIS protocol suite, a more complete security analysis of the overall protocol behaviours will be required. In the meantime, consideration of the scenarios described

here may be helpful in refining the view of what are the realistic security goals for NSIS signaling as a whole.

6. Contributors

This draft initially written by Robert Hancock, Jukka Manner, and Charles Q. Shen.

7. Acknowledgments

Acknowledgments go to Xiaoming Fu, Eleanor Hepworth, Cornelia Kappler, Georgios Karagiannis, Andrew McDonald, Henning Schulzrinne, Hannes Tschofenig.

8. Informative References

[1] R. Hancock, et al., "Next Steps in Signaling: Framework". Internet Draft (work in progress), draft-ietf-nsis-fw-04

[2] H. Schulzrinne, "CASP - Cross-Application Signaling Protocol". Internet Draft (work in progress), draft-schulzrinne-nsis-casp-01

[3] S. van den Bosch, et al., "NSLP for Quality-of-Service Signaling". Internet Draft (work in progress), draft-ietf-nsis-qos-nslp-00

[4] H. Tschofenig, et al., "Security Implications of the Session Identifier". Internet Draft (work in progress), draft-tschofenig-nsis-sid-00

[5] P. Nikander, et al., "Mobile IP version 6 Route Optimization Security Design Background". Internet Draft (work in progress), draft-nikander-mobileip-v6-ro-sec-01

[6] H. Tschofenig, et al., "QoS NSLP Authorization Issues". Internet Draft (work in progress), draft-tschofenig-nsis-qos-authz-issues-00

[7] X. Fu, et al., "QoS-Conditionalized Binding Update in Mobile IPv6". Internet Draft (work in progress), draft-tkn-nsis-qosbinding-mipv6-00

[8] M. Thomas, "Analysis of Mobile IP and RSVP Interactions". Internet Draft (work in progress), draft-thomas-nsis-rsvp-analysis-00

9. Author's Addresses

Questions about this document may be directed to:

Robert Hancock
Roke Manor Research Ltd

Romsey, Hants, SO51 0ZN
United Kingdom

Voice: +44-1794-833601

Fax: +44-1794-833434
E-Mail: robert.hancock@roke.co.uk

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

Voice: +358-9-191-44210
Fax: +358-9-191-44441
E-Mail: jmanner@cs.helsinki.fi

Charles Q. Shen
Department of Electrical Engineering
Columbia University
500 West 120th Street
New York, NY 10027
USA

Voice: +1-212-854-5599
Fax: +1-212-932-9421
E-Mail: charles@ee.columbia.edu