IETF Next Steps in Signaling
Working Group
Internet-Draft
Expires: April 26, 2004

S. Jeong
HUFS
S. Lee
J. Bang
BJ Lee
SAMSUNG AIT

October 27, 2003

Mobility Functions in the NTLP
draft-jeong-nsis-mobility-ntlp-01.txt

Status of this Memo

Copyright Notice

Abstract

The lower general layer in the NSIS protocol suite, called the NSIS Transport Layer Protocol (NTLP), is intended to provide a general transport service for signaling messages. One of the items on the list of desired features for the NTLP is mobility support. This document identifies possible mobility functions in the NTLP according to the mobility requirements for future signaling protocols.

Table of Contents

1. Introduction

The lower general layer in the NSIS signaling protocol suite, called the NSIS Transport Layer Protocol (NTLP), is intended to provide a general transport service for signaling messages. The actual signaling messages are generated within upper layer signaling applications, each having its own NSIS Signaling Layer Protocol (NSLP) [2]. The main functionality of the NTLP is to discover appropriate NSIS nodes and to deliver the signaling messages to them.

Mobility support is considered as one of the desired features of the NTLP [3, 13, 15, 21, 22]. This document attempts to identify mobility functions that may need to be supported in the NTLP. In this document, the mobility functions in the NTLP refer to the functions which are used to support mobility in NSIS signaling. The possible mobility (-related) functions in the NTLP include interactions with the NSLP, detection of route change caused by mobility, crossover node discovery, dead peer discovery (e.g., dead crossover node discovery), interworking with mobility protocols, and so on. This document mainly discusses possible issues related to each of the mobility functions in the NTLP.

1.1 Terminology

AR: Access Router

CARD: Candidate Access Router Discovery

CN: Correspondent Node

CoA: Care of Address

CRN: Crossover Node

CT: Context Transfer

DPD: Dead Peer Discovery

MN: Mobile Node

NE: NSIS Entity

NF: NSIS Forwarder

NI: NSIS Initiator

NSLP: NSIS Signaling Layer Protocol

NTLP: NSIS Transport Layer Protocol

PD: Peer Discovery

PD Requestor: an NE which sends a PD request message

PD Responder: an NE which receives the PD request message and sends the PD response message

QoS-NSLP: NSLP for QoS Signaling

2. Interactions with the NSLP

In this section, we identify possbile interactions between the NTLP and the NSLP, which can also be applied in mobile scenarios. An incoming NSIS signaling message will first be captured and processed by the NTLP. Any NSIS message related to the associated NSLP (e.g., QoS-NSLP) will be passed to the NSLP via an API from the NTLP. Upon reception of any notification or trigger from the NTLP, the NSLP needs to decide its next behavior on its own. For example, the QoS-NSLP may need to update QoS-NSLP state information or initiate necessary actions such as removal of old QoS reservation states. The change of NTLP states may also trigger the associated NSLP to create, update, or release related NSLP states.

To trigger the NSLP, the NTLP first needs to detect any triggering events. For example, the NTLP may be able to generate a trigger after detecting that a route change due to mobility has occurred. In this case, the triggering message may need to include information about sessions that are impacted by the route change. The NSLP is then responsible for deciding necessary actions for the impacted sessions. The NSLP will also trigger the NTLP via an API to deliver necessary

signaling messages to the next NSIS peer node.

When a mobility event such as a handover (e.g., fast handover in Mobile IPv6) is initiated, the NTLP/NSLP should operate to re-establish the states along the new path as quickly as possible. For this purpose, the interactions with seamoby protocols may be necessary (see Section 5 for further details). It may not be possible to re-establish states (e.g., since the necessary resources are not available on the new path). In this case, it may be desired that the NTLP/NSLP needs to get service availability (e.g., QoS resource availability) in advance or before the handover is completed.

The NTLP/NSLP states established on the old path should be removed immediately after re-establishing the states along the new path because the old states should not be maintained any longer. To do this, the NSLP of an appropriate NSIS entity (NE) (e.g., crossover node) may ask the associated NTLP to deliver a teardown message to the NEs on the old path. In this case, the NTLP should know where to send the teardown message on the obsolete path.

3. Detection of Route Change Caused by Mobility

In mobile scenarios, a route change (rerouting) may occur due to a mobility event that can be characterized by the change of the IP address (e.g., care-of-address (CoA)) of one of the end points (e.g., an MN) due to a handover. Link or node failure (or management-related operations) may also cause a route change. However, this document considers only route changes due to mobility-related events such as an MN's handover.

A route change caused by mobility should be detected by the NTLP for necessary state creation, update, or removal. A route change can be detected when the NTLP of an NE finds out that the route taken by a flow has changed (e.g., by checking the incoming interface). To

provide fast adaptation to route changes for particular destinations, the NTLP may be in interaction with routing protocols.

The route change event detected by the NTLP will then be used to trigger the NSLP associated with the sessions which are impacted by the route change. When the NSLP receives a trigger from the NTLP, it sends necessary NSLP messages along the new route with the help of the NTLP.

Although the route change caused by a mobility event may be considered similar to the normal route change, the main difference from the normal route change is the fact that the flow identifier should be updated at the NEs involved with the session along the end-to-end signaling path. To do this, the crossover node (CRN), the merging point of the old and new signaling paths, should be discovered first, and the NTLP of the CRN needs to forward a state update message further towards the other end point (e.g., CN). The NTLP of the CRN should also send a state installation message on the new path and a state teardown message on the obsolete path. The detailed discussion about the crossover node discovery can be found in the following section.

4. Crossover Node (CRN) Discovery

In this section, we discuss how to find the CRN in general and the role of the CRN (especially in QoS re-establishment). We also discuss possible use of seamoby protocols such as CT or CARD for the CRN discovery during handover.

When a route change due to a handover occurs, the NTLP signaling for the NSIS peer discovery and service (e.g., QoS) re-establishment should be localized to improve scalability and reduce signaling overhead. To achieve this, the CRN should be discovered quickly by the NTLP, and the NSLP (e.g., QoS-NSLP) should be triggered by the NTLP for necessary actions (such as QoS re-establishment on the new path and teardown of old reservation states on the obsolete path). For the CRN discovery, some information including the MOBILITY object, the session identifier, the flow identifier, and the incoming interface can be used.

The MOBILITY object may be defined in the NTLP message (e.g., GIMPS payload) to notify any mobility event explicitly. The MOBILITY object may contain various mobility-related fields such as the handover_init field and the mobility_event_counter field. The handover_init field can be used to explicitly notify that a handover is initiated for fast state re-establishment. The mobility_event_counter field can be used to detect the latest hanover event to avoid confusion about where to send a confirmation message which indicates that the CRN has been found. This type of confirmation may be needed when the MN moves toward the second new AR immediately after it experiences a handover to the first new AR from the old AR, because the CRN discovery message from the second new AR may arrive earlier that that of the first new AR. The MOBILITY object may also be defined in the NSLP in a similar way. In this case, there should be some relationship between the MOBILITY objects of the NTLP and the NSLP.

The session identifier can be very useful for the crossover node discovery. It should be globally unique and independent from the IP address of an end node (e.g., MN) to identify the involved session easily even after a change of the CoA due to a handover to a new AR. It is important that for the duration of a data flow, the session identifier has to remain the same while the flow identifier (see below) information associated with the same data flow may change.

The flow identifier is normally used to identify a particular data flow for which the specific service (e.g., QoS) is requested from the network. For example, a flow identifier may consist of a combination of source IP address, destination IP address, and flow label in IPv6-based networks. This flow identifier may also be used to specify the relationship between the address information and the state

re-establishment (e.g., QoS-NSLP state re-establishment).

Additionally, the incoming interface may also be used for the CRN discovery together with the unique session identifier if the CRN is the NSIS-aware merging point of the old and new paths. If the merging point is not NSIS-aware and can't act as a CRN, the nearest (from the merging point) NSIS-aware node along the joined/common/unchanged path can act as a CRN for the involved session. In this case, the incoming interface may not be useful for the CRN discovery because the NSIS-aware node is no longer a merging point of the old and new paths. Therefore, in this case, other identifiers (e.g., flow identifier, MOBILITY Object, and so on) may also be needed to discover the crossover node on the joined/common/unchanged path.

When a route change caused by mobility occurs, the CRN can be recognized by comparing the existing session identifier with the session identifier of the flow received from an incoming interface. If the session identifier is still the same and the flow identifier or interface number has been changed, the current NSIS-aware node is recognized as a CRN. As mentioned above, the MOBILITY object can also be used to indicate that the MN has experienced a handover and a route has occurred.

The CRN discovery may also be initiated during handover (i.e., before the handover is completed), for instance, for fast QoS-NSLP re-establishment or pre-establishment. However, in this case, an efficient mechanism is needed to find a candidate CRN. For example, after a mobility event is detected by the NTLP, the current AR may use a candidate access router discovery (e.g., CARD [10]) protocol to transfer the context for QoS-NSLP re-establishment immediately. After candidate ARs are found, a context transfer mechanism (e.g., CT [9]) can be used to transfer the context including the QoS-NSLP session information to re-establish QoS-NSLP states quickly. If an appropriate AR is found and the context transfer is completed, a candidate CRN can be discovered easily since the candidate CRN discovery is basically the same as above.

In some cases, however, it may not be possible to use mobility-related protocols such as CT and CARD. In this case, the MN can initiate the CRN discovery only after it changes the point of attachment. To expedite the discovery process, it may be useful to transmit the peer discovery message (by the NTLP) and the first binding update message at the same time.

5. Dead Peer Discovery (DPD)

It may be possible that the CRN may be found dead before re-establishing states on the new path or removing the old states on the obsolete path. It is also possible that the old AR cannot communicate with the MN (the peer node of the OAR) any longer after a handover is initiated. Therefore, an efficient mechanism (which should be used by the NTLP) is needed to find dead peers immediately to minimize service interruption. This section first discusses a possible way of finding live NSIS peers and then how to discover dead NSIS peers.

Before the delivery of any NTLP messages, the NE (e.g., NI, NF, or NR) first needs to launch the peer discovery (PD) mechanism which sends a PD request message (e.g., Scout message in CASP [4]) to its neighboring nodes along the signaling path to detect its NSIS peer. The transmission of PD messages by the NTLP may be separated from the transmission of regular signaling messages since PD messages may be difficult to protect. It is also possible to combine both types of messages for efficiency in message delivery. For example, the detection of an NSIS peer and establishment of a QoS-NSLP state can be performed by sending an NSIS message.

An NE which sends a PD request message is called a PD requestor, and an NE which receives the PD request message and sends an acknowledgement (ACK) message is called a PD responder. Upon receiving a PD request message, the PD responder sends an ACK. The ACK message includes a cookie for security protection. The PD requestor needs to check the cookie to make sure security protection. In this way, NSIS peers can be found securely and easily.

Note that NEs may not always transmit signaling messages successfully to its NSIS peer along the signaling path. For example, signaling messages may not be delivered to its peer when an NF (or NR) is temporarily or permanently disconnected from the network due to the failure of communication links (or processors), system rebooting, node congestion, or a mobile node's handover, causing the change of signaling path in the network. Therefore, dead peers which are no longer reachable should be detected. To do this, the PD requestor periodically transmits a ferret message (i.e., a PD request message) to its neighboring peers. The PD requestor must receive an ACK message from its peer (i.e., the PD responder) within a certain amount of time to determine if its peer is still alive.

If the PD requestor does not receive any ACK message from the PD responder within a certain amount of time (i.e., the PD timer expires), the PD requestor retransmits the same PD message to the PD responder one more time. If the PD requestor does not still receive

any ACK message from the PD responder, the PD requestor will consider the PD responder as a dead peer. In this case, the PD requestor will send a new PD message to find its new peer. This rediscovery process is actually the same as the PD mechanism described above. If the peer node failure (due to a link or node processor failure) causes any route change, the NTLP may need to interact with a routing protocol to determine where to send the new PD message.

If an MN acts as an NI or NR, a route change in the network may occur (e.g., due to handover). In this case, the old AR will find that its peer (i.e., MN) is not alive any longer since it will not receive any ACK from the MN in response to the periodic transmission of PD request messages. However, in this case, the NTLP of the old AR should not generate any error message to avoid teardown of existing states before the CRN initiates a teardown message on the obsolete path. The old AR can be considered as the actual last node on the old path after the MN changes the point of attachment.

It is important to verify the correctness of PD messages for security purposes. For example, an efficient mechanism may need to be used in order to determine if the PD message has been received from the authorized peer. If the PD request message is found to be valid, the PD responder sends an ACK message immediately. Upon receiving the ACK message from the PD responder, the PD requestor may need to inspect the cookie of the received ACK message from the PD responder for security protection.

6. Interworking with Mobility Protocols

The NSIS protocol needs to efficiently handle the path change due to mobility in order to support existing fast and seamless mobility mechanisms although the NSIS protocol is not to be coupled tightly with mobility protocols (e.g., FMIPv6, HMIPv6, or MIPv6). To do this, the movement of an MN should be detected first by the NTLP of an MN or AR. For example, the NTLP of an MN can detect movement with the help of monitoring layer 2 connections, and the NTLP of an AR can also detect movement by receiving a handover initiation message (e.g., 'RtSolPr' message in Fast Handover for MIPv6). The NSLP is then triggered by the NTLP to act appropriately. For example, the QoS-NSLP may appropriately set the MOBILITY object of an outgoing QoS-NSLP message for fast QoS state re-establishment [24].

After receiving the information on the mobility event, the NTLP of the AR may interact with a candidate access router discovery protocol (e.g., CARD) to find an appropriate AR (an NSIS-aware node) before the handover is completed. After the appropriate AR is discovered, the NTLP may trigger the NSLP, and the NSLP may need to interact with the context transfer (CT) protocol to transfer the NSLP state information to the newly discovered AR.

After handover, the NTLP of a new AR may detect handover completion, which can be used to minimize the service re-establishment delay and the data packet loss. For instance, when an MN begins to transmit first Binding Update (BU) message to its CN (or MAP in case of HMIPv6), the NTLP may initiate peer discovery and send NSLP messages at the same time to create a new state on the new signaling path for

the same signaling application.

7. Security Considerations

The NTLP may rely on the security mechanisms described in [4]. Securing the NTLP can be provided by CMS which allows resource objects and related objects defined in this document to be encapsulated and protected by CMS. Therefore, no separate specification within the NTLP may be necessary to describe the format of these objects. This allows some flexibility in including protected objects to link the authorization step of different protocols and to transport local information within domains. The functionality described in [19] and [20] can be provided without substantial protocol modification/extensions.

8. Summary

This document identified what kind of mobility functions should be supported in the NTLP according to the mobility requirements for future signaling protocols. Possible mobility functions for the NTLP include interactions with the NSLP, detection of route change caused by mobility, crossover node discovery, dead peer discovery, interworking with mobility protocols, and so on. There are still some issues to be addressed in further detail, including the last NSIS node detection, crossover node discovery in receiver- and sender-initiated modes, IP-in-IP encapsulation, interworking with seamoby protocols, security and AAA, and etc.

References

[1] Brunner, M., "Requirements for Signaling Protocols", draft-ietf-nsis-req-09 (work in progress), August 2003.

[2] Hancock, R., "Next Steps in Signaling: Framework", draft-ietf-nsis-fw-04 (work in progress), September 2003.

[3] Chaskar, H., "Requirements of a Quality of Service (QoS) Solution for Mobile IP", RFC 3583, September 2003.

[4] Schulzrinne, H., "CASP - Cross-Application Signaling Protocol", draft-schulzrinne-nsis-casp-01 (work in progress), March 2003.

[5] Schulzrinne, H., "A Quality-of-Service Resource Allocation Client for CASP", draft-schulzrinne-nsis-casp-qos-01 (work in progress), March 2003.

[6] McDonald, A., "A Quality of Service NSLP for NSIS", draft-mcdonald-nsis-qos-nslp-00 (work in progress), June 2003.

[7] Bosch, S., "NSLP for Quality-of-Service signaling", draft-ietf-nsis-qos-nslp-00 (work in progress), September 2003.

[8] Schulzrinne, H., "GIMPS: General Internet Messaging Protocol for Signaling", draft-schulzrinne-nsis-ntlp-00 (work in progress), June 2003.

[9] Loughney, J., "Context Transfer Protocol", draft-ietf-seamoby-ctp-04 (work in progress), October 2003.

[10] Liebsch, M., "Candidate Access Router Discovery", draft-ietf-seamoby-card-protocol-04 (work in progress), September 2003.

[11] Tschofenig, H. and D. Kroeselberg, "Security Threats for NSIS", draft-ietf-nsis-threats-02 (work in progress), July 2003.

[12] Buchli, M., "A Network Service Layer Protocol for QoS signaling", draft-buchli-nsis-nslp-00 (work in progress), June 2003.

[13] Fu, X., "Mobility Issues in Next Steps in Signaling (NSIS)", draft-fu-nsis-mobility-01 (work in progress), October 2003.

[14] Koodli, R., "Fast Handovers for Mobile IPv6", draft-ietf-mobileip-fast-mipv6-08 (work in progress), October 2003.

[15] Lee, S., "QoS Signaling for IP-based Radio Access Networks",

draft-lee-nsis-signaling-ran-00 (work in progress), June 2003.

[16] Braden, B., Zhang, L., Berson, S., Herzog, S. and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

[17] Berger, L., Gan, D., Swallow, G., Pan, P., Tommasi, F. and S. Molendini, "RSVP Refresh Overhead Reduction Extensions", RFC 2961, April 2001.

[18] Westberg, L., "A Proposal for RSVPv2", draft-westberg-proposal-for-rsvpv2-01 (work in progress), November 2002.

[19] Hamer, L-N., Gage, B. and H. Shieh, "Framework for Session Set-up with Media Authorization", RFC 3521, April 2003.

[20] Hamer, L-N., Gage, B., Kosinski, B. and H. Shieh, "Session Authorization Policy Element", RFC 3520, April 2003.

[21] Shen, C., "Several Framework Issues Regarding NSIS and Mobility", draft-shen-nsis-mobility-fw-00 (work in progress), July 2002.

[22] Chaskar, H. and C. Westphal, "QoS Signaling Framework for Mobile IP", draft-westphal-nsis-qos-mobileip-00 (work in progress), June 2002.

[23] Schulzrinne, H., "GIMPS: General Internet Messaging Protocol for Signaling", draft-ietf-nsis-ntlp-00 (work in progress), October 2003.

[24] Lee, S., "Mobility Functions in the QoS-NTLP", draft-jeong-nsis-mobility-ntlp-00 (work in progress), October 2003.

Authors' Addresses

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

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

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

Jongho Bang
SAMSUNG Advanced Institute of Technology
i-Networking Lab.
San 14-1, Nongseo-ri, Giheung-eup
Yongin-si, Gyeonggi-do 449-712
KOREA

Phone: +82 31 280 9585
EMail: jh0278.bang@samsung.com

Byoung-Joon (BJ) Lee
SAMSUNG Advanced Institute of Technology
i-Networking Lab.
San 14-1, Nongseo-ri, Giheung-eup
Yongin-si, Gyeonggi-do 449-712
KOREA

Phone: +82 31 280 9626
EMail: bj33.lee@samsung.com

Intellectual Property Statement

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.