Applicability Statement of NSIS Protocols in Mobile Environments

(draft-manyfolks-signaling-protocol-mobility-01.txt)

S. Lee, S. Jeong, H. Tschofenig, X. Fu, J. Manner,
R. Bless, R. Hancock, P. Mendes

Aug. 2, 2004

60th IETF San Diego Meeting

Problem Statement

- In mobility scenarios, operation of NSIS signaling protocols are affected by the following issues:
  - The change of route and possibly change of the MN IP address
  - Latency of route change caused by mobility
  - IP-in-IP encapsulation
  - Ping-Pong type handover
  - Upstream- vs. Downstream Path Update
  - Double reservation problem following a handover
  - Localization signaling problem
  - Session ownership identification
  - Other authorization issues

Mobility-related issues with NSIS protocols (1)

- Specific issues with NTLP
  - GIMPS needs to detect route changes and mobility according to uplink and downlink signaling cases each.
  - Interlayer interaction with signaling applications.
  - Which layer should the (NSLP) CRN discovery be performed at, GIMPS or QoS-NSLP?
  - IP-in-IP encapsulation.

Mobility-related issues with NSIS protocols (2)

- Specific issues with QoS-NSLP
  - When/how is QoS-NSLP signaling initiated after mobility?
  - How/when does an MN know/find out what resources are available before a reservation is made after handover?
  - How/by who can RESPONSE message be sent to the corresponding QNI if QNR (e.g., an MN) of the RESPONSE message performs handover before the receipt of the message?
  - How is refresh time set up in the situation of frequent handover?
  - How does CRN safely remove the state along the old path after the establishment of state along a new path?

Mobility-related issues with NSIS protocols (3)

- Specific issues with NAT/FW NSLP
  - The IP address change caused by mobility makes firewall rules & NAT bindings become invalid.
    - For the QoS-NSLP, it only leads to temporarily weaker QoS
  - Pinholes and NAT bindings can be reused by adversaries due to the non-cryptographic nature of the installed state
  - There may be some differences between the security functionalities required by the QoS NSLP and the NAT/Firewall NSLP.
    - the security solution for NAT/FW-NSLP needs to be reflected in mobility specific security scenarios.

Future work

- Consolidate the list of open issues
- Define design choices for the NSIS protocols
- Evaluate the design choices
- Find answers and make a decision before protocols are frozen

Backup slides

Basic Terminologies

- Crossover Node (CRN)
  - A node that for a given function is a merging point of two or more separate sets of state information, not a physical route splitting point.
  - There can be different types of logical CRNs:
    - NTLP/NSLP CRN, Down/Upstream CRN, Mobility CRN, and Routing CRN
  - Note that the CRN required for QoS-NSLP operation is
    - the NSLP CRN which has the corresponding signaling application information to perform the path update.

- Path Update & Local Repair
  - Path Update
    - 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.
  - In case of route changes
    - the update of NSIS state on the common path is not required and it is called Local Repair which localizes the NSIS signaling.

CRN Discovery & Path Update

- CRN discovery
  - It is more appropriate at GIMPS level than at NSLP level
    - The corresponding NSLP can be identified at the GIMPS level.
    - the route changes may easily be detected at the GIMPS level rather than at the NSLP
  - The following identifiers can be used:
    - Message routing state-related session ID, flow ID, and NSLP ID.
    - The direction of NSIS signaling branch-related NSLP branch ID.

- Path Update-related issues
  - Although the state update on the common path does not give rise to re-process AAA and admission control, it may lead to the signaling overhead and latency.
    - In this case, NSIS needs to interact with local mobility management protocols
  - whether the teardown message can be sent toward the opposite direction to the state initiating node is still an open question.
    - This leads to authorization problem because a node which does not initiate signaling for establishing the NSIS state can delete the state.
  - Ping-Pong type handover
  - The last node detection problem: Invalid NR problem

Interaction with Macro-Mobility Protocols (I)

- Implication to Mobile IP-related scenarios
  - NSIS needs to have an interface with Mobile IP to immediately react to a mobility event. In this case, some issues arise:
    - Which information does the NTLP detect the movement based on?
    - How and what information can the NSLP expect from NTLP, or directly from the routing interface after mobility?
    - How to coordinate the mobility binding update interval and NSIS signaling interval?

Interaction with Macro-Mobility Protocols (II)

- Interaction with Mobile IPv4/v6
  - NSIS signaling may need to interact with IP tunneling to also update the state along the tunneling segment between HA to FA (or MN).
  - In this case, the CRN may eventually be discovered somewhere on the tunneling path, and the new flow identifier for the tunneling state update may also be created.

- Interaction with Mobile IPv6
  - The obsolete path of the existing tunneling segments needs to appropriately be removed after re-establishment of NSIS state along the optimized path.
  - When to remove the tunneling segment and/or how to tear it down through the interworking with the IP-tunneling is still an open issue.

Multihoming Scenarios

- Both new address and old address can be valid during a certain period of time, so the new data path may co-exist with the old one. It leads NEs to maintain double flow identifiers to the same session.

- The inter-domain handover, the latency penalty of NSIS signaling including authentication and authorization can be mitigated if the MN is multi-homed.

- In NSIS WG, does fast state installation by using anticipated handovers, where the MN signals the new path while still connected to the old one, need to be discussed?

Security Considerations

- Analysis on authorization and security implications with the following scenarios:
  - MN as data sender
    - MN is authorizing entity
    - CN is authorizing entity
    - MN and CN are authorized
  - CN as data sender
    - MN is authorizing entity
    - CN is authorizing entity
  - Multi-homing Scenarios
    - MN is data sender
    - CN is data sender
- Many questions raised which need some discussions
- Goal: Answer questions and agree on security mechanism

Other Issues

- QoS Performance Considerations in mobility scenarios
  - In mobile networks, the QoS-NSLP needs to set the refresh timer value depending on the handover type or the reservation style to optimize the resources utilization.
  - Use of refresh reduction
    - State update along the common path, NSIS signaling over wireless channel and in the access networks
  - The signaling latency caused by end-to-end signaling can be reduced by interworking with localized mobility management (LMM).
- Use Cases of Identifiers
  - Session ID, SII, MRI (or flow ID), RSN, and Mobility Object.
- Peer Failure Scenarios in Mobile Environments
  - Possible dead peers: MN, AR, CRN
  - Dead peers may have some impact on services. For example,
    - Invalid NR
    - Incomplete state setup or teardown

Issues beyond the current draft

- Interaction with other mobility-related protocols
  - Micro mobility protocols, Seamoby protocols, & NEMO
- Additional issues on CRN discovery & Path Update
- The Ping-Pong type of movement
- When both end-hosts are mobile
- Bi-directional state establishment
- Priority reservation
- Aggregation of end-to-end flows in mobile environments
- Anticipated handover???

Change History

- Title was changed:
  - From *“Mobility and Internet Signaling Protocols”* to *“Applicability Statement of NSIS Protocols in Mobile Environments”*
- ToC was restructured:

Abstract
1. Introduction
2. Terminology
3. Problem Statement & General Considerations
4. Basic Operations for mobility support
5. Mobility-Related Issues with NSIS Protocols
5.1 Specific Issues with NTLP
5.2 Specific Issues with QoS-NSLP
5.3 Specific Issues with NAT/FW NSLP
5.4 Common issues related to NTLP and NSLP
6. Applicability Statement
6.1 Support for Macro Mobility-based scenarios
6.2 Multihoming/make-before-break scenarios
6.3 QoS Performance Consideration in Mobility Scenarios
6.4 Use cases of Identifiers
6.5 Peer Failure Scenarios
7. Security Considerations
8. Open Issues
Appendix. Anticipated Handoff

CRN discovery and Path Update

- Interwoking with Local mobility management, NEMO, and Seamoby protocols
- Support for the Ping-Pong type handover
- When both end-hosts are mobile
- Bi-directional state establishment
- Priority reservation
- Aggregation reservation