Network Working Group
Internet-Draft
Expires: September 7, 2006

X. Fu
Univ. Goettingen
J. Loughney
Nokia
H. Peters
Univ. Goettingen
March 6, 2006

Context Transfer Using GIST
draft-fu-cxtp-gist-01.txt

Status of this Memo

Copyright Notice

Abstract

The CXTP specification uses basic SCTP as transport for CXTP message exchanges between a mobile node's previous and new access routers. It also relies on a pre-established IPsec ESP transport mode tunnel. This document discusses two alternative approaches based on "persistent" associations using either SCTP streams feature or GIST

protocol. While both approaches reduce context transfer latency during handovers, GIST also offers more flexible transport and richer security properties.

Table of Contents

1. Introduction

The Context Transfer Protocol (CXTP) [1] provides a way to improve performance for mobile nodes moving between networks by transferring state context from the previous access router (pAR) to the new access router (nAR) across an IP based network. For each of these context transfers, a new SCTP association is maintained. This document describes alternative potentials based on "persistent" associations between neighboring ARs to reduce the context transfer handover latency due to individual association setup. Similar to the multi-streaming features in the Stream Control Transmission Protocol (SCTP), the General Internet Signaling Transport (GIST) [2] provides the functionality of multiplexing traffic between two peers into a single association, known as messaging association (MA). This technique allows reuse of an existing (secure) communication channel for context transfer between a pAR and any nAR. In addition, the proposed approach could seamlessly interwork with PANA and NSIS protocols, and minimize the involvement of mobile hosts. Such a communication channel is soft state based, which allows an efficient and secure acquisition of state information for roaming devices as well as flexible selection of underlying transport mechanisms and automatic release of unused resources.

2. Terminology

Most of the terms used are defined in the CXTP [1], SCTP [3] and GIST [2] specifications. Below is a list of acronyms used in this document.

- AR Access Router
- pAR previous Access Router
- nAR new Access Router
- CTAR CXTP Activate Request message
- CTAA CXTP Activate Acknowledge message

- o CTD CXTP Data message
- o CTReq CXTP Request message
- o CTDR CXTP Data Reply message
- o CTC CXTP Cancel message
- o MA GIST messaging association
- o MRS GIST message routing state
- o MRI GIST message routing information

3. Design Overview

CXTP message exchange can be divided into two groups: MN-AR and AR-AR

communication. This document mainly addresses the issue of communications between entities within the network. These entities can be either nodes supporting access control or a PEP (Policy Enforcement Point) function, access routers or any other types of nodes. The context transferred can be anything related to mobile nodes' end-to-end communications, such as AAA, header compression, QoS, Policy, and possibly sub-IP protocols and services such as PPP, as supported by RFC 4067 [1].

An access router will likely be able to know its neighboring access routers' address information (either by static configuration or can learn that information by other means), associations between them can be either established on demand or pre-established depending on the policies. An association is a unidirectional context transfer channel.

If a mobile node (MN) requests for context transfer, or an AR predicts an MN is likely to move to another AR, context transfer message exchanges can be made upon the corresponding association. This can be done by either of the following approaches, alternative to the one specified in [1].

3.1. Use of SCTP multiple streams

SCTP allows to send several messages over a single association using multiple streams. Each stream is associated with a unique stream identifier at both endpoints. Multiple streams prevent Head of Line Blocking (HLB); if retransmission occurs at one stream, messages of the other streams of the same association are not delayed.

During establishment of the SCTP association, the pAR and the nAR will negotiate in the INIT and INIT-ACK phase about the number of streams to use, according to section 5.1.1 of [3]. After the association is initialized, the valid outbound stream identifier range for either endpoint shall be between 0 and min (local number of outbound streams, remote maximum inbound streams) - 1. Once a SCTP association is established, there is no need to perform additional negotiation to use multiple streams.

A context identified by a feature profile type (FPT) is assigned an incrementing outbound stream identifier, the context is encoded using CXTP message format and finally sent over a pre-established SCTP association. The same stream identifier MUST NOT be used for concurrent context transfers. The stream identifier is reset when it reaches the range limit.

3.2. Use of GIST as alternative transport

The GIST protocol being developed by the NSIS working group for general signaling transport is independent on the underlying transport protocol, such as UDP, TCP, TCP over TLS or SCTP. In this section we describe the overall approach on how to reuse GIST for general context transfer between two entities within the network that support forwarding of a mobile node's IP traffic.

The CXTP messages exchanged between the entities within the network are encapsulated as a NSIS signaling application running above GIST. This way, features like soft state refreshes and messaging state reuse, transport protocol flexibility and ensured reliable and secure transport will allow CXTP to be applicable in many operational environments.

Typically, GIST operates with a path-coupled discovery procedure to determine the signaling nodes. As the target node addressing information here is already known in advance and the peers communicate in an end-to-end fashion, there is no need to perform GIST path-coupled discovery and maintaining GIST message routing state (MRS).

In GIST, a 32-bit session identifier is assigned to each context transfer randomly. The same session identifier MUST NOT be used for concurrent context transfers.

Note, when SCTP is used for GIST [4], multiple different sessions can be further aggregated over a common GIST session, by using different SCTP streams for each session. This will be useful, for instance, when the sessions are used by different corresponding hosts.

3.3. Applicability scenario

Figure 1 illustrates an example scenario for CXTP using GIST. The scenario also applies for persistent SCTP associations. Non-established associations are denoted with brackets. Theoretically, an AR can maintain (messaging) associations between itself and any number of its neighboring ARs. Assume there is an MN moving from AR2 to AR3, then to AR5 and finally AR6. As there is already an existing association (A3) between AR2 and AR3, AR2 can transfer context of this MN to AR3 through A3 by exchanging CXTP data messages over a specified transport protocol. As there exists no association between AR3 and AR5, a new association will establish A5 on demand when either AR3 or AR5 learns MN's movement or intention to move from AR3 to AR5. Note, GIST can negotiate transport protocol and security properties between these ARs, allowing maximal flexibility and applicability. After A4 is established, AR3 can perform CXTP over it

as usual. If for some (long) period of time AR2 does not anticipate any need for transferring context to any neighboring AR, nor it receives any CXTP message from that neighbor, associations SHOULD be released, avoiding waste of network resources.

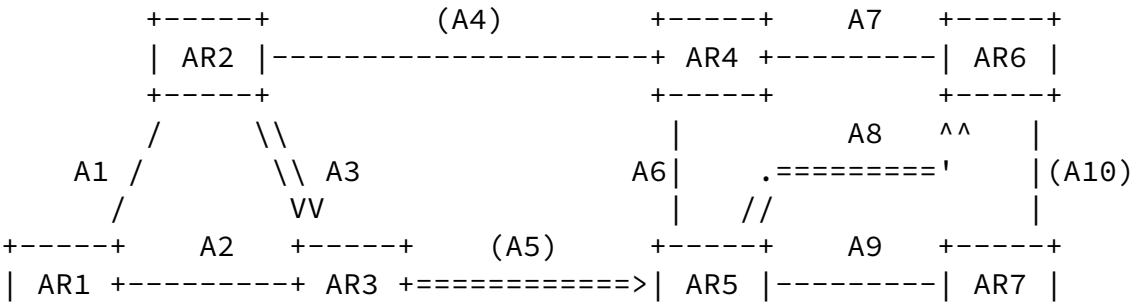
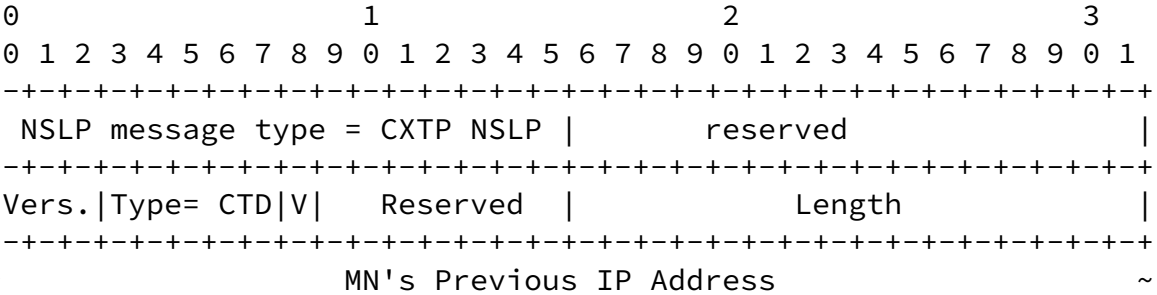


Figure 1: An example scenario for CXTP using GIST

4. Context Transfer NSLP

A new NSIS signaling application type (NSLP ID TBD), "CXTP NSLP", is defined for exchanging encapsulated CXTP messages (CTD, CTReq, CTDR and CTC) between pAR and nAR and possibly creating GIST MAs. Each CXTP NSLP message contains a common NSLP header (as defined in [2]), followed by one of these 4 types of CXTP messages defined in [1]). For example, the CXTP NSLP CTD message is described in Figure 2:



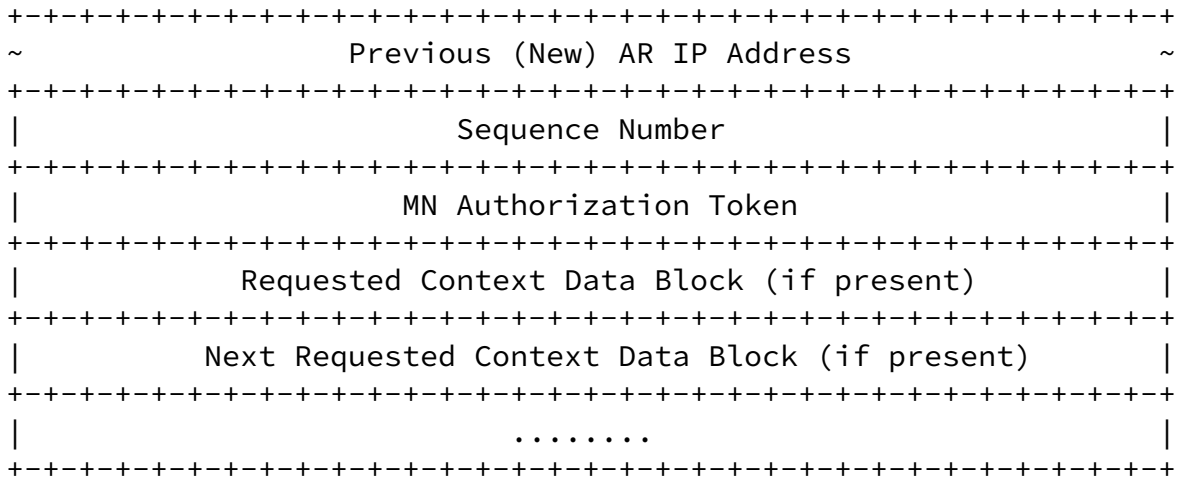


Figure 2: Encapsulated CXTP CTD message

GIST discovery as defined in [2] is modified as follows:

- GIST query messages are used to create MAs between known ARs, thus there is no need to include a router alert option;
- there is no need to create or maintain MRSs upon receipt of a GIST response or confirm message;
- MA-Hello messages are used to keep existing MAs alive, its timer value may be smaller than standard GIST MA lifetime;
- GIST error messages are used to report an unknown CXTP NSLP message type (i.e., a new error code needs to be introduced).

CXTP messages between MN and pAR and between MN and nAR are specified in CXTP [1] as ICMP messages and not modified here.

5. Further Discussions

5.1. Advantages & disadvantages of GIST transport

Advantages:

- "Persistent" associations using a soft state approach reduces session setup latency and requires lower state maintenance cost at access routers. When the association is not used for a long period of time, it will be automatically removed;

- GIST offers more flexible and dynamic selection of underlying

transport protocol, including richer security properties. For instance, this allows to deploy CXTP using TCP/TLS with SCTP "multiple stream"-like feature;

- NSIS-aware networks can easily deploy CXTP NSLP. This naturally offers interworking benefits with other NSLPs, such as QoS NSLP or NAT/Firewall NSLP.

Disadvantages:

- Several features of GIST are not used, such as peer discovery and message routing over a chain of GIST nodes. Thus, it seems a simplified/light-weight version of GIST may be used instead of a full-fledged GIST.

5.2. Triggers for Context Transfer

There are many possibilities to trigger Context Transfer using GIST, some of which are listed below:

- Using the triggers defined in CXTP [1], such as MN-controlled or network-controlled;
- Using some kind of (light-weight) NSIS signaling between the MN and the correspondent node as trigger;
- If the mobile node is using NSIS signaling for other purposes (middlebox configuration, QoS signaling), ARs could notice MN attachment by MN's discovery messages;
- Upon the completion of authentication, e.g., PANA discovery and handshake in PANA mobility optimization [5];
- Upon a successful transfer of PANA context [6].

These triggers can be categorized to either 1) triggers perceived at the nAR or 2) triggers perceived at the pAR. Upon a trigger of category 1), the nAR needs to send a CT-Req over the GIST MA to the pAR, and the latter in turn responds back with a CTD; then an optional CTDR can be sent from the pAR to the nAR. Upon a trigger of category 2), the pAR simply needs to send a CTD over the GIST MA to the nAR.

In either case, if a desired CTD message is not received within a certain period of time (or due to other reasons, e.g., the nAR senses that the MN moves out of its coverage before receiving a CTD), the nAR may issue a CTC to cancel the context transfer using the GIST MA.

5.3. Interworking with NSIS QoS and NAT/FW NSLP protocols

CXTP, especially its use over GIST, can reduce the overhead for the last hop communication between an MN and its AR. Using CXTP/GIST, the AR states related to MN-CN end-to-end communications are transferred seamlessly, without the need to reestablish from the MN.

Figure 3 illustrates an example where QoS NSLP signaling is desired from the MN to the CN. The case of NAT/FW NSLP is similar. Before the handover, QoS NSLP is applied, involving steps 1)-4) and finally reaches CN. Then the MN moves to the nAR, which maintains a (secure) GIST MA with the pAR. Some trigger as described in previous subsection (e.g., either (1) or (1a) or another event) then starts the CXTP/GIST, which results in QoS NSLP state successfully to be transferred from the pAR to the nAR. Once the CXTP/GIST is accomplished, the nAR can then act on behalf on the MN and (re)establish the QoS NSLP state along the path towards the CN using QoS NSLP signaling.

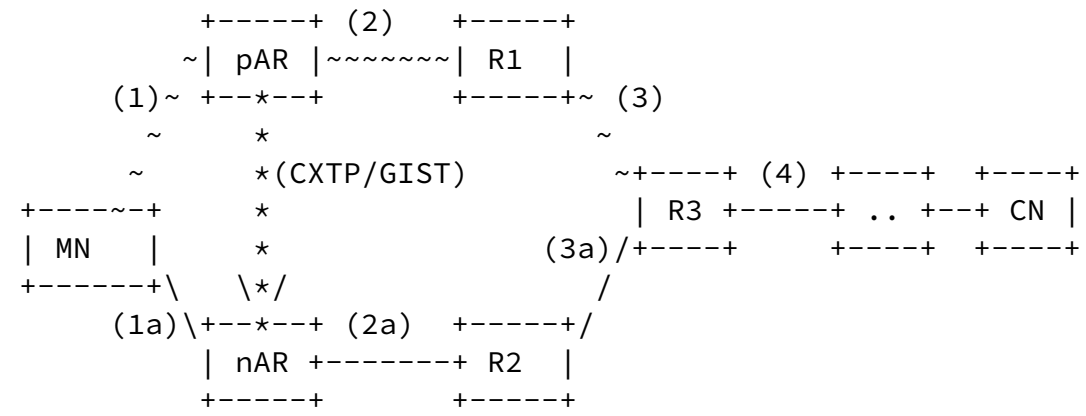


Figure 3: Interworking with NSIS QoS NSLP

5.4. GIST MA bootstrapping, maintenance and inter-domain context transfer issues

CXTP/GIST requires maintaining a GIST MA between neighboring ARs. In cases where ARs belonging to different administrative domains do not have a pre-established GIST MA, or an AR is newly added or rebooted, GIST MAs need to be established on demand in a secure fashion. Further versions of this document will discuss this aspect in more detail.

6. Security Considerations

The security considerations of both [2] and [1] apply. "Persistent" SCTP associations are more vulnerable against blind masquerade attacks against the SCTP Verification Tag. Further security analysis is needed to consider additional security vulnerabilities.

7. Acknowledgements

Kwok-Ho Chan, Hui Deng, James Kempf, Rajeev Koodli, and Hannes Tschofenig provided valuable comments.

8. References

8.1. Normative References

[1] Loughney, J., Nakhjiri, M., Perkins, C., and R. Koodli, "Context Transfer Protocol (CXTP)", RFC 4067, July 2005.

[2] Schulzrinne, H. and R. Hancock, "GIST: General Internet Signaling Transport", draft-ietf-nsis-ntlp-09 (work in progress), February 2006.

[3] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L., and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, October 2000.

8.2. Informative References

[4] Fu, X., "General Internet Signaling Transport (GIST) over SCTP", draft-fu-nsis-ntlp-sctp-01 (work in progress), February 2006.

[5] Forsberg, D., "PANA Mobility Optimizations", draft-ietf-pana-mobopts-01 (work in progress), October 2005.

[6] Bournelle, J., "Use of Context Transfer Protocol (CXTP) for PANA", draft-ietf-pana-cxtp-00 (work in progress), October 2005.

Authors' Addresses

Xiaoming Fu
University of Goettingen
Institute for Informatics
Lotzestr. 16-18
Goettingen 37083
Germany

Email: fu@cs.uni-goettingen.de

John Loughney
Nokia Research Center
Itamerenkatu 11-13
Helsinki 00180
Finland

Email: john.loughney@nokia.com

Henning Peters
University of Goettingen
Institute for Informatics
Lotzestr. 16-18
Goettingen 37083
Germany

Email: hpeters@math.uni-goettingen.de

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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