Internet Engineering Task Force
Internet Draft
draft-ietf-seamoby-ct-reqs-05.txt
Expires: April 2003

Gary Kenward, editor

October, 2002

General Requirements for Context Transfer

Status of this Memo

Copyright Notice

Abstract

The success of time sensitive services like VoIP telephony, video, etc., in a mobile environment depends heavily on the ability to minimize the impact of the traffic redirection during a change of packet forwarding path. In the process of establishing the new forwarding path, the nodes along the new path must be prepared to provide similar forwarding treatment to the IP packets. The transfer of context information may be advantageous in minimizing the impact of host mobility on IP services. This document captures the set of requirements for a context transfer solution and the requirements for a generic context transfer protocol to carry the context between the context transfer peers.

Table of Contents

1 Introduction

There are a large number of IP access networks that support mobile hosts. For example, wireless Personal Area Networks (PANs), wireless LANs, satellite WANs and cellular WANs. The nature of this mobility is such that the communication path to the host may change frequently and rapidly.

In networks where the hosts are mobile, the forwarding path through the access network must often be redirected in order to deliver the host's IP traffic to the new point of access. The success of time sensitive services like VoIP telephony, video, etc., in a mobile environment depends heavily upon the ability to minimize the impact of this traffic redirection. In the process of establishing the new forwarding path, the nodes along the new path must be prepared to provide similar forwarding treatment to the IP packets.

The information required to support a specific forwarding treatment provided to an IP flow is part of the context for that flow. To minimize the impact of a path change on an IP flow, the context must be replicated from the forwarding nodes along the existing path to the forwarding nodes along the new path. The transfer of context information may be advantageous in minimizing the impact of host mobility on, for example, AAA, header compression, QoS, Policy, and possibly sub-IP protocols and services such as PPP.

An analysis of the context transfer problem is captured in [2]. This document captures the requirements for a context transfer solution and the requirements for a generic context transfer protocol to carry the context between the context transfer peers.

2 Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [1].

3 Terminology

Most of the terms used in this document are defined in [2].

Access Router (AR)
An IP router residing in an Access Network and connected to one or more points of access. An AR offers connectivity to MNs.

4 General Requirements

This section addresses the facilities and services required in the access network to properly support context transfer. The context transfer solution will have to assume certain characteristics of the access network and the mobility solution, and the availability of certain triggering events,
transport options, and so forth. These support capabilities are not necessarily part of context transfer, per se, but are needed for context transfer to operate as defined and effect the expected enhancements to MN traffic handover. For convenience, this collection of support capabilities are referred to as the "context transfer solution".

4.1 The context transfer solution MUST define the characteristics of the IP level trigger mechanisms that initiate the transfer of context.

4.2 The IP level context transfer triggers MAY be initiated by a link level (layer two) event.

4.3 The IP level trigger mechanisms for context transfer MUST hide the specifics of any layer 2 trigger mechanisms.

Handover at the IP level is a consequence of a change in the physical path used to communicate between the MN and the access network. The mechanisms utilized to change the communications path at layer 2 are specific to the physical characteristics of the medium, and often specific to the layer 2 transmission technology being used (e.g. TIA IS 2000, ETSI UMTS R4, IEEE 802.11).

In order for any action to be taken at the IP level to maintain IP sessions during a layer 2 path change, some indication of the path change must be made available to the IP level. One example of an indicator would be the trigger event that initiates context transfer.

Since it is expected that IP handover, and thus context transfer will work irrespective of the layer 2 technology, the IP level solutions must not utilize specific layer 2 information. The conditions and events that caused the generation of an IP level trigger must be opaque to the IP level. This implies that there are general characteristics of an IP level trigger that need to be defined so that the triggers generated by different layer 2 solutions will have identical semantics at the IP level.

4.4 The IP level context transfer triggers MAY be initiated by IP level (layer three) signalling.

4.5 Any IP level signalling for Context Transfer MUST be separated from the actual transfer of context.

4.6 The context transfer solution MAY support one-to-many context transfer.

An MN may have connectivity to the access network through more than one physical path at any given time, depending upon the characteristics of the physical medium, and the layer 1 and 2 protocols and services.

The different physical paths may connect into the network via different ARs. In this scenario, two or more ARs may be candidates for handover of the MN's traffic and each will require the appropriate IP context when forwarding commences. Exactly which AR will be the target of the handover is often not known until the handover is initiated, and providing the necessary context to all the candidate ARs can only accelerate the handover process.

A one-to-many context transfer may be achieved using either a series of point-to-point transfers, or a point-to-multipoint (multicast) transfer.

4.7 The context transfer solution MUST support context transfer before, during and after handover.

4.8 The context transfer solution MUST support a distributed approach in which the Access Routers act as peers during the context transfer.

One main distinction between the various alternative approaches to context transfer is the choice of the functional entity or entities that orchestrate the transfer. A context transfer solution that relies upon the ARs to effect a context transfer should be the most efficient approach, as it involves the fewest possible entities. At the very least, the number of protocol exchanges should be less when there are fewer entities involved.

4.9 The entities transferring context MUST support a process for mutual authentication prior to initiating the transfer.

It is believed that if a formal authentication exchange (e.g. exchanging credentials) were done during the context transfer, the computation overhead for both the sender and the receiver would cause additional and unnecessary latency to the handoff process. Therefore, the CT peers MUST exchange credentials prior to any context transfer.

4.10 The context transfer solution SHOULD provide mechanisms to selectively enable or disable context transfer for particular IP microflows or groups of IP microflows.

The context associated with an MN's microflows is normally to be transferred whenever it is required to support forwarding. However,

there may be conditions where it is desirable to selectively disable context transfer for specific microflows.

For example, it may be desirable to provide an MN with the capability to disallow the transfer of the context associated with one or more of its microflows when handover occurs between networks administered by different operators.

Local mechanisms for allowing context transfer to be disabled on a per microflow basis have to be provided for in the context transfer solution. These mechanisms will most likely be captured as part of the CT MIB, and possibly, as part of a PIB, if policy based management is considered desirable.

There are other mechanisms and protocols required to manage or control the per microflow disabling of context transfer. These are clearly out of the scope of the context transfer work.

4.11 Context information MAY be transferred in phases.

Providing for phased transfers allows the context acquisition and transfer to be prioritized.

4.12 The context information to be transferred MUST be available at the AR performing the transfer, prior to the initiation of a given phase of the context transfer.

To effect a rapid transfer, the context information has to be readily available when the AR begins a phase of the transfer.

If the context transfer is comprised of a single phase, then all of the context must be available prior to the transfer initiation.

4.13 The context transfer solution MUST include methods for interworking with any IETF IP mobility solutions.

4.14 The context transfer solution MAY include methods for interworking with non-IETF mobility solutions.

4.16 The context transfer solution MUST be scalable.

5. Protocol Requirements

This section captures the general requirements for the context transfer protocol.

5.1 General Protocol Requirements

5.1.1 The context transfer protocol MUST be capable of transferring all of the different types of feature context necessary to support the

MN's traffic at a receiving AR.

5.1.2 **The context transfer protocol design MUST define a standard representation for encapsulating context information in the IP packet** payload that will be interpreted uniformly and perspicuously by different implementations.

5.1.3 **The context transfer protocol MUST operate autonomously from the content of the context information being transferred.**

5.1.4 **The context transfer protocol design MUST define a standard method for labelling each feature context being transferred.**

Various protocols participate in setting up the service support for any given microflow, and many of these protocols require feature specific state to be maintained for the life of the IP session. The context transfer protocol should provide a generic mechanism to carry context information to an AR, irrespective of the context type.

Given that the desired context transfer protocol is a single, generic protocol for transferring all feature context, the collection of information representing the context for a given feature must be encapsulated into a standard representation and labelled. Encapsulation is necessary to keep the context for different features separated. The receiving AR will use the label on an encapsulated context to associate it with the appropriate service feature and process the content appropriately.

The context transfer protocol does not need to know the contents of these nuggets of encapsulated information. Indeed, for the protocol to be independent from the type of context being transferred, it must be oblivious the actual context.

5.1.5 **The context transfer protocol design MUST provide for the future definition of new feature contexts.**

The context transfer solution must not attempt to define all possible feature contexts to be transferred. Instead, it must provide for the definition of new contexts in support of future service features, or feature evolution. Guidance should be provided to future users of context transfer on the best approach to defining feature context.

5.2 Transport Requirements

This section contains requirements on the context transfer transport.

5.2.1 **The context transfer protocol MUST be specified so that it is independent of the underlying transport.**

Recognizing that the transport characteristics for context transfer will depend on the particular application, it should be possible to

transfer context directly on top of reliable transports, such as TCP or SCTP, unreliable transports, such as UDP, or as an option or extension on another protocol, such as handover signalling.

5.3 Security

5.3.1 The protocol MUST provide for "security provisioning".

The security of the context information being exchanged between ARs must be ensured. Security provisioning includes protecting the integrity, confidentiality, and authenticity of the transfer, as well as protecting the ARs against replay attacks.

5.3.2 The security provisioning for context transfer MUST NOT require the creation of application layer security.

5.3.3 The protocol MUST provide for the security provisioning to be disabled.

In some environments, the security provisioning provided for by the context transfer protocol may not be necessary, or it may be preferred to minimize the context transfer protocol overhead.

5.4 Timing Requirements

5.4.1 A context transfer MUST complete with a minimum number of protocol exchanges between the source AR and the rest of the ARs.

The number of protocol exchanges required to perform a peer to peer interaction is directly related to the unreliability, resource consumption, and completion time of that interaction. A context transfer will require signalling and data exchanges, but, as a general rule, by keeping the number of these exchanges to a minimum, the reliability, resource utilization and completion delay of the transfer should improve.

5.4.2 The context transfer protocol design MUST minimize the amount of processing required at the sending and receiving Access Routers.

If the context transfer protocol requires the context information to be transferred in a form that requires significant additional processing at each AR, delays may be incurred that impact the reliability of the context. In other words, the context may become obsolete before it can be reconstructed at the receiving AR.

Also, AR processing delay contributes to the overall context transfer delay, and may make fulfilling requirements 5.4.1 and 5.4.2 difficult.

An example of a protocol design that would increase the processing delay at the receiver is where the context information is segmented,

and the ordering of the segments is not preserved during transfer; segmenting at the sender, and more likely, re-ordering of the segments at the receiver could introduce significant additional AR processing delays.

5.4.3 The Context Transfer protocol MUST meet the timing constraints required by all the feature contexts.

A given feature context may have timing constraints imposed by the nature of the service being support. The delivered context must always comply with the requirements of the service if it is to be useable.

5.4.4 The context transfer solution MUST provide for the aggregation of multiple contexts.

5.4.5 If context aggregation is not support by the transport protocol (via the Nagle algorithm [3]) then the context transfer protocol MUST provide it.

There may be instances where there are multiple context transfers pending. To reduce the overall transfer time, as well as transport overhead that might be incurred by separately transferring each context, the sending AR may choose to aggregate the contexts and execute one transfer operation.

Note that if contexts are aggregated, the labelling method required by 5.1.4 must include an identifier that allows the contexts to be separated at the receiving AR.

5.5 Context Update and Synchronization

5.5.1 The base context transfer protocol SHOULD NOT provide direct support for synchronization with outside events, since synchronization is not a requirement for all or even most feature contexts.

5.5.2 The base context transfer protocol MUST allow individual feature context specifications to define their own synchronization with external events.

5.5.3 The base context transfer protocol SHOULD NOT provide support for updating context after it is transferred, since individual feature contexts will differ in their need for update.

5.5.4 The base context transfer protocol MUST allow individual feature context specifications to define their own update procedures if required.

Most feature contexts will not require synchronization, however there are a few that may. Header compression, for example, may require

that the header compressor on the old access router cease and the compressor on the new router start in synchrony with hand over of routing to the new router; otherwise, the compressor on the new router will not be properly synchronized. Since most contexts don't need synchronization support, the general CT solution need not support it, but it should not provide a hindrance to those feature contexts that do.

Feature contexts will differ in whether or not they require update. A feature context such as QoS parameters for the service level agreement with a user may not involve dynamically changing information, but it may change during or after context transfer. Such feature contexts may benefit from allowing the context to change after the transfer is completed. Other feature contexts, such as header compression, may be tightly synchronized with external events and changes on the old router need to be discarded since the new router's state may already have been modified.

5.6 Interworking with handover mechanisms

5.6.1 The context transfer protocol MAY provide input to the handover process.

5.6.2 The context transfer protocol MUST include methods for exchanging information with the handover process.

Both context transfer and handover require information on the AR candidates for handover. The context transfer entities may, in the process of establishing and supporting context transfer, acquire information that would be useful to the handover process in determining the new forwarding path: for example, the outcome of an admission control decision at a receiving AR.

5.7 Partial Handover

5.7.1 The context transfer protocol MAY provide a mechanism for supporting partial handovers.

In a situation where no single AR is capable of receiving a handover of all of an MN's traffic, a mechanism could be provided that would allow different IP microflows to be handed over to different ARs. The information transferred to each AR must be limited to only the context required to support the microflows that are actually handed over. Thus, the context transfer protocol would need a mechanism for partitioning the context and transferring each portion to the appropriate AR.

6 Standardization of Feature Contexts

The context transfer protocol provides a basic framework in which

feature contexts of varying types can be transferred. Recognizing that the particular feature contexts may have very different needs with regard to update, synchronization, and transport, the base context transfer protocol requirements are designed to not constrain how the context transfer protocol is used for particular feature contexts with respect to these points. In addition, some feature contexts may require additional processing on the target access router before they can be of use. Individual feature contexts will be standardized by the method of IETF standards action. The standardization of a feature context should describe how a feature context utilizes the base context transfer protocol; if update, synchronization, and additional processing are required, and, if so, how they are achieved; and the transport used for the feature context.

7 References

[1] Bradner, S., "Keywords for use in RFCs to Indicate Requirement Levels", RFC2119 (BCP), IETF, March 1997.

[2] Kempf, J., editor, "Problem Description: Reasons For Performing Context Transfers Between Nodes in an IP Access Network", draft-ietf-seamoby-context-transfer-problem-stat-04.txt, May 2002.

[3] Nagle, J., "Congestion Control in IP/TCP", RFC 896, January 1984.

8 Acknowledgements

Thank you to all who participated in the Seamoby working group context transfer design team.

9 Author's Addresses

Hamid Syed
Nortel Networks
100 Constellation Crescent
Ottawa, Ontario. K2G 6J8 Phone: +1 613 763 6553
Canada Email: hmsyed@nortelnetworks.com

Gary Kenward
Nortel Networks
100 Constellation Crescent
Ottawa, Ontario. K2G 6J8 Phone: +1 613 765 1437
Canada Email: gkenward@nortelnetworks.com

Pat R. Calhoun
Black Storm Networks
250 Cambridge Avenue, Suite 200
Palo Alto, CA 94306 Phone: +1 650 617 2932
USA Email: pcalhoun@bstormnetworks.com

Madjid Nakhjiri
Motorola
1501 West Shure Drive
Arlington Heights IL 60004 Phone: +1 847 632 5030
USA Email: madjid.nakhjiri@motorola.com

Rajeev Koodli
Communications Systems Laboratory, Nokia Research Center
313 Fairchild Drive
Mountain View CA 94043 Phone: +1 650 625 2359
USA Email: rajeev.koodli@nokia.com

Kulwinder S. Atwal
Zucotto Wireless Inc.
Ottawa Ontario K1P 6E2 Phone: +1 613 789 0090
CANADA EMail: kulwinder.atwal@zucotto.com

Mark Smith
COM DEV Wireless
3450 Broad Street, Suite 107
San Luis Obispo, CA 93401 Phone: +1 805 544 1089
USA Email: mark.smith@comdev.cc

Govind Krishnamurthi
Communications Systems Laboratory, Nokia Research Center
5 Wayside Road
Burlington MA 01803 Phone: +1 781 993 3627
USA EMail: govind.krishnamurthi@nokia.com

James Kempf
DoCoMo Communication Laboratories USA
180 Metro Drive, Suite 300
San Jose, CA 95110 Phone: +1 408 451 4711
USA EMail: kempf@docomolabs-usa.com

10 Full Copyright Statement

11 Funding Acknowledgement

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