Network Working Group
Request for Comments: 3374
Category: Informational

J. Kempf, Ed.

September 2002

Problem Description: Reasons For Performing Context Transfers Between Nodes in an IP Access Network

Status of this Memo

Copyright Notice

Abstract

In IP access networks that support host mobility, the routing paths between the host and the network may change frequently and rapidly. In some cases, the host may establish certain context transfer candidate services on subnets that are left behind when the host moves. Examples of such services are Authentication, Authorization, and Accounting (AAA), header compression, and Quality of Service (QoS). In order for the host to obtain those services on the new subnet, the host must explicitly re-establish the service by performing the necessary signaling flows from scratch. In some cases, this process would considerably slow the process of establishing the mobile host on the new subnet. An alternative is to transfer information on the existing state associated with these services, or context, to the new subnet, a process called "context transfer". This document discusses the desirability of context transfer for facilitating seamless IP mobility.

Table of Contents

1.0 Introduction....2
2.0 Reference Definitions....3
3.0 Scope of the Context Transfer Problem....3
4.0 The Need for Context Transfer....4
4.1 Fast Context Transfer-candidate Service Re-establishment....4
4.1.1 Authentication, Authorization, and Accounting (AAA)....4
4.1.2 Header Compression....5
4.1.3 Quality of Service (QoS)....6
4.2 Interoperability....6
5.0 Limitations on Context Transfer....7
5.1 Router Compatibility....7
5.2 Requirement to Re-initialize Service from Scratch....7
5.3 Suitability for the Particular Service....7
5.4 Layer 2 Solutions Better....7
6.0 Performance Considerations....8
7.0 Security Considerations....8
8.0 Recommendations....9
9.0 Acknowledgements....9
10.0 References....10
11.0 Complete List of Authors' Addresses....12
12.0 Full Copyright Statement....14

1.0 Introduction

In networks where the hosts are mobile, the routing path through the network must often be changed in order to deliver the host's IP traffic to the new point of access. Changing the basic routing path is the job of a IP mobility protocol, such as Mobile IPv4 [1] and Mobile IPv6 [2]. But the success of real time services such as VoIP telephony, video, etc., in a mobile environment depends heavily upon the minimization of the impact of this traffic redirection. In the process of establishing the new routing path, the nodes along the new path must be prepared to provide similar routing treatment to the IP packets as was provided along the old routing path.

In many cases, the routing treatment of IP packets within a network may be regulated by a collection of context transfer-candidate services that influence how packets for the host are treated. For example, whether a particular host has the right to obtain any routing at all out of the local subnet may depend on whether the host negotiated a successful AAA exchange with a network access server at some point in the past. Establishing these services initially results in a certain amount of related state within the network and requires a perhaps considerable amount of time for the protocol

exchanges. If the host is required to re-establish those services by the same process as it uses to initially establish them, delay-sensitive real time traffic may be seriously impacted.

An alternative is to transfer enough information on the context transfer-candidate service state, or context, to the new subnet so that the services can be re-established quickly, rather than require the mobile host to establish them from scratch. The transfer of service context 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. Context transfer at a minimum can be used to replicate the configuration information needed to establish the respective protocols and services. In addition, it may also provide the capability to replicate state information, allowing stateful protocols and services at the new node to be activated along the new path with less delay and less signaling overhead.

In this document, a case is made for why the Seamoby Working Group should investigate context transfer.

2.0 Reference Definitions

Context

The information on the current state of a service required to re-establish the service on a new subnet without having to perform the entire protocol exchange with the mobile host from scratch.

Context Transfer

The movement of context from one router or other network entity to another as a means of re-establishing specific services on a new subnet or collection of subnets.

Context Transfer Candidate Service

A service that is a candidate for context transfer. In this document, only services that are concerned with the forwarding treatment of packets, such as QoS and security, or involve granting or denying the mobile host access to the network, such as AAA, are considered to be context transfer-candidate services.

3.0 Scope of the Context Transfer Problem

The context transfer problem examined in this document is restricted to re-establishing services for a mobile host that are, in some sense, related to the forwarding treatment of the mobile host’s

packets or network access for the mobile host. It is not concerned with actually re-establishing routing information. Routing changes due to mobility are the domain of the IP mobility protocol. In addition, transfer of context related to application-level services, such as those associated with the mobile host's HTTP proxy, is also not considered in this document, although a generic context transfer protocol for transferring the context of services related to forwarding treatment or network access may also function for application-level services as well.

An important consideration in whether a service is a candidate for context transfer is whether it is possible to obtain a "correct" context transfer for the service in a given implementation and deployment, that is, one which will result in the same context at the new access router as would have resulted had the mobile host undergone a protocol exchange with the access router from scratch. For some services, the circumstances under which context transfer may result in correctness may be very limited [11].

4.0 The Need for Context Transfer

There are two basic motivations for context transfer:

1) The primary motivation, as mentioned in the introduction, is the need to quickly re-establish context transfer-candidate services without requiring the mobile host to explicitly perform all protocol flows for those services from scratch.

2) An additional motivation is to provide an interoperable solution that works for any Layer 2 radio access technology.

These points are discussed in more detail in the following subsections.

4.1 Fast Context Transfer-candidate Service Re-establishment

As mentioned in the introduction, there are a variety of context transfer-candidate services that could utilize a context transfer solution. In this section, three representative services are examined. The consequences of not having a context transfer solution are examined as a means of motivating the need for such a solution.

4.1.1 Authentication, Authorization, and Accounting (AAA)

One of the more compelling applications of context transfer is facilitating the re-authentication of the mobile host and re-establishment of the mobile host's authorization for network access in a new subnet by transferring the AAA context from the

mobile host's previous AAA server to another. This would allow the mobile host to continue access in the new subnet without having to redo an AAA exchange with the new subnet's AAA server. Naturally, a security association between the AAA servers is necessary so that the mobile host's sensitive authentication information can be securely transferred.

In the absence of context transfer, there are two ways that can currently be used for AAA:

1) Layer 2 mechanisms, such as EAP [3] in PPP [4] or 802.1x [5] can be used to redo the initial protocol exchange, or possibly to update it. Currently, there is no general Layer 3 mechanism for conducting an AAA exchange between a host and an AAA server in the network.

2) If the mobile host is using Mobile IPv4 (but not Mobile IPv6 currently), the host can use the AAA registration keys [6] extension for Mobile IPv4 to establish a security association with the new Foreign Agent.

Since 2) is piggybacked on the Mobile IPv4 signaling, the performance is less likely to be an issue, but 2) is not a general solution. The performance of 1) is likely to be considerably less than is necessary for maintaining good real time stream performance.

4.1.2 Header Compression

In [7], protocols are described for efficient compression of IP headers to avoid sending large headers over low bandwidth radio network links. Establishing header compression generally requires from 1 to 4 exchanges between the last hop router and the mobile host with full or partially compressed headers before full compression is available. During this period, the mobile host will experience an effective reduction in the application-available bandwidth equivalent to the uncompressed header information sent over the air. Limiting the uncompressed traffic required to establish full header compression on a new last hop router facilitates maintaining adequate application-available bandwidth for real time streams, especially for IPv6 where the headers are larger.

Context transfer can help in this case by allowing the network entity performing header compression, usually the last hop router, to transfer the header compression context to the new router. The timing of context transfer must be arranged so that the header context is transferred from the old router as soon as the mobile host

is no longer receiving packets through the old router, and installed on the new router before any packets are delivered to or forwarded from the mobile host.

4.1.3 Quality of Service (QoS)

Significant QoS protocol exchanges between the mobile host and routers in the network may be required in order to establish the initial QoS treatment for a mobile host's packets. The exact mechanism whereby QoS for a mobile host should be established is currently an active topic of investigation in the IETF. For existing QoS approaches (Diffsrv and Intsrv) preliminary studies have indicated that the protocol flows necessary to re-establish QoS in a new subnet from scratch can be very time consuming for Mobile IP, and other mobility protocols may suffer as well.

A method of transferring the mobile host's QoS context from the old network to the new could facilitate faster re-establishment of the mobile host's QoS treatment on the new subnet. However, for QoS mechanisms that are end-to-end, transferring context at the last hop router may be insufficient to completely re-initialize the mobile host's QoS treatment, since some number of additional routers in the path between the mobile host and corresponding node may also need to be involved.

4.2 Interoperability

A particular concern for seamless handover is that different Layer 2 radio protocols may define their own solutions for context transfer. There are ongoing efforts within 3GPP [8] and IEEE [9] to define such solutions. These solutions are primarily designed to facilitate the transfer of Layer 2-related context over a wired IP network between two radio access networks or two radio access points. However, the designs can include extensibility features that would allow Layer 3 context to be transferred. Such is the case with [10], for example.

If Layer 2 protocols were to be widely adopted as an optimization measure for Layer 3 context transfer, seamless mobility of a mobile host having Layer 2 network interfaces that support multiple radio protocols would be difficult to achieve. Essentially, a gateway or translator between Layer 2 protocols would be required, or the mobile host would be required to perform a full re-initialization of its context transfer-candidate services on the new radio network, if no translator were available, in order to hand over a mobile host between two access technologies.

A general Layer 3 context transfer solution may also be useful for Layer 2 protocols that do not define their own context transfer protocol. Consideration of this issue is outside the scope of the Seamoby Working Group, however, since it depends on the details of the particular Layer 2 protocol.

5.0 Limitations on Context Transfer

Context transfer may not always be the best solution for re-establishing context transfer-candidate services on a new subnet. There are certain limitations on when context transfer may be useful. These limitations are discussed in the following subsections.

5.1 Router Compatibility

Context transfer between two routers is possible only if the receiving router supports the same context transfer-candidate services as the sending router. This does not mean that the two nodes are identical in their implementation, nor does it even imply that they must have identical capabilities. A router that cannot make use of received context should refuse the transfer. This results in a situation no different than a mobile host handover without context transfer, and should not be considered an error or failure situation.

5.2 Requirement to Re-initialize Service from Scratch

The primary motivation for context transfer assumes that quickly re-establishing the same level of context transfer-candidate service on the new subnet is desirable. And yet, there may be situations where either the device or the access network would prefer to re-establish or re-negotiate the level of service. For example, if the mobile host crosses administrative domains where the operational policies change, negotiation of a different level of service may be required.

5.3 Suitability for the Particular Service

Context transfer assumes that it is faster to establish the service by context transfer rather than from scratch. This may not be true for certain types of service, for example, multicast, "push" information services.

5.4 Layer 2 Solutions Better

Context transfer is an enhancement to improve upon the performance of a handover for Layer 3 context transfer-candidate services. Many networks provide support for handover at Layer 2, within and between

subnets. Layer 3 context transfer may not provide a significant improvement over Layer 2 solutions, even for Layer 3 context, if the handover is occurring between two subnets supporting the same Layer 2 radio access technology.

6.0 Performance Considerations

The purpose of context transfer is to sustain the context transfer-candidate services being provided to a mobile host's traffic during handover. It is essentially an enhancement to IP mobility that ultimately must result in an improvement in handover performance. A context transfer solution must provide performance that is equal to or better than re-initializing the context transfer-candidate service between the mobile host and the network from scratch. Otherwise, context transfer is of no benefit.

7.0 Security Considerations

Any context transfer standard must provide mechanism for adequately securely the context transfer process, and a recommendation to deploy security, as is typically the case for Internet standards. Some general considerations for context transfer security include:

- Information privacy: the context may contain information which the end user or network operator would prefer to keep hidden from unauthorized viewers.

- Transfer legitimacy: a false or purposely corrupted context transfer could have a severe impact upon the operation of the receiving router, and therefore could potentially affect the operation of the access network itself. The potential threats include denial of service and theft of service attacks.

- Security preservation: part of the context transfer may include information pertinent to a security association established between the mobile host and another entity on the network. For this security association to be preserved during handover, the transfer of the security context must include the appropriate security measures.

It is expected that the measures used to secure the transport of information between peers (e.g., IPSEC [10]) in an IP network should be sufficient for context transfer. However, given the above considerations, there may be reason to provide for additional security measures beyond the available IETF solutions.

Since context transfer requires a trust relationship between network entities, the compromise of only one of the network entities that transfer context may be sufficient to reduce the security of the whole system, if for example the context transferred includes encryption keying material. When the host moves from the compromised network entity to an uncompromised network entity in the presence of context transfer, the compromised context may be used to decrypt the communication channel. When context transfer is not used, a compromise of only one network entity only gives access to what that network entity can see. When the mobile host moves to an uncompromised network entity in the absence of context transfer, security can be re-established at the new entity. However, to the extent that context transfer happens primarily between routers, the security of context transfer will depend on the security of the routers. Any compromise of security on a router that affects context transfer may also lead to other, equally serious disruptions in network traffic.

The context transfer investigation must identify any novel security measures required for context transfer that exceed the capabilities of the existing or emerging IETF solutions.

8.0 Recommendations

The following steps are recommended for Seamoby:

- Investigation into candidate router-related services for context and an analysis of the transfer requirements for each candidate;

- The development of a framework and protocol(s) that will support the transfer of context between the routing nodes of an IP network.

The context transfer solution must inter-work with existing and emerging IP protocols, in particular, those protocols supporting mobility in an IP network.

9.0 Acknowledgements

The editor would like to thank the Seamoby CT design team (listed at the end of the document as co-authors), who were largely responsible for the initial content of this document, for their hard work, and especially Gary Kenward, who shepherded the document through its initial versions.

10.0 References

[1] Perkins, C., "IP Mobility Support", RFC 3220, January 2002.

[2] Johnson, D. and C. Perkins, "Mobility Support in IPv6", Work in Progress.

[3] Blunk, L. and Vollbrecht, J., "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[4] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[5] IEEE Std. P802.1X/D11, "Standard for Port based Network Access Control", March 2001.

[6] Perkins, C., and P. Calhoun, "AAA Registration Keys for Mobile IP", Work in Progress.

[7] Borman, C., Burmeister, C., Degermark, M., Fukushima, H., Hannu, H., Jonsson, L., Hakenberg, R., Koren T., Le, K., Martensson, A., Miyazaki, A., Svanbro, K., Wiebke, T., Yoshimura, T. and H. Zheng, "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", RFC 3095, July 2001.

[8] 3GPP TR 25.936 V4.0.0, "Handovers for Real Time Services from PS Domain," 3GPP, March 2001.

[9] IEEE Std. 802.11f/D2.0, "Draft Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," July 2001.

[10] Kent, S. and Atkinson, R., "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[11] Aboba, B. and M. Moore, "A Model for Context Transfer in IEEE 802", Work in Progress.

11.0 Complete List of Authors' Addresses

O. Henrik Levkowetz
A Brand New World
Osterogatan 1
S-164 28 Kista
SWEDEN

Phone: +46 8 477 9942
EMail: henrik@levkowetz.com

Pat R. Calhoun
Black Storm Networks
110 Nortech Parkway
San Jose CA 95134
USA

Phone: +1 408-941-0500
EMail: pcalhoun@bstormnetworks.com

James Kempf
NTT DoCoMo USA Laboratories
181 Metro Drive, Suite 300
San Jose, CA 95110
USA

Phone: 408-451-4711
EMail: kempf@docomolabs-usa.com

Gary Kenward
Nortel Networks
3500 Carling Avenue
Nepean, Ontario K2G 6J8
CANADA

Phone: +1 613-765-1437
EMail: gkenward@nortelnetworks.com

Hamid Syed
Nortel Networks
100 Constellation Crescent
Nepean Ontario K2G 6J8
CANADA

Phone: +1 613 763-6553
EMail: hmsyed@nortelnetworks.com

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

Phone: +358-9-191-44210
EMail: jmanner@cs.helsinki.fi

Madjid Nakhjiri
Motorola
1501 West Shure Drive
Arlington Heights IL 60004
USA

Phone: +1 847-632-5030
EMail: madjid.nakhjiri@motorola.com

Govind Krishnamurthi
Communications Systems Laboratory, Nokia Research Center
5 Wayside Road
Burlington MA 01803
USA

Phone: +1 781 993 3627
EMail: govind.krishnamurthi@nokia.com

Rajeev Koodli
Communications Systems Lab, Nokia Research Center
313 Fairchild Drive
Mountain View CA 94043
USA

Phone: +1 650 625 2359
EMail: rajeev.koodli@nokia.com

Kulwinder S. Atwal
Zucotto Wireless Inc.
Ottawa Ontario K1P 6E2
CANADA

Phone: +1 613 789 0090
EMail: kulwinder.atwal@zucotto.com

Michael Thomas
Cisco Systems
375 E Tasman Rd
San Jose CA 95134
USA

Phone: +1 408 525 5386
EMail: mat@cisco.com

Mat Horan
COM DEV Wireless Group
San Luis Obispo CA 93401
USA

Phone: +1 805 544 1089
EMail: mat.horan@comdev.cc

Phillip Neumiller
3Com Corporation
1800 W. Central Road
Mount Prospect IL 60056
USA

EMail: phil_neumiller@3com.com

12.0 Full Copyright Statement

Acknowledgement

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