

Classical IP and ARP over ATM to NHRP Transition

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1998). All Rights Reserved.

Abstract

This document describes methods and procedures for the graceful transition from an ATMARP LIS[1] to an NHRP LIS[2] network model over ATM.

1. Introduction

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [6].

ATMARP defines an initial application of classical IP and ARP in an ATM network environment configured as a LIS[1]. ATMARP only considers application of ATM as a direct replacement for the "wires" and local LAN segments connecting IP end-stations and routers operating in the "classical" LAN-based paradigm.

The NBMA Next Hop Resolution Protocol (NHRP) allows a source station (a host or router), wishing to communicate over a Non-Broadcast, Multi-Access (NBMA) subnetwork, to determine the internetworking layer addresses and NBMA addresses of suitable "NBMA next hops" toward a destination station. If the destination is connected to the NBMA subnetwork and direct communication is administratively allowed, then the NBMA next hop is the destination station itself. Otherwise, the NBMA next hop is the egress router from the NBMA subnetwork that is "nearest" to the destination station. For the purposes of this document, the NBMA network is of type ATM.

It is reasonable to expect that ATMARP Clients and NHRP Clients will initially coexist within a LIS. Thus, it is necessary to define a graceful transition, including a period of coexistence, from the use of ATMARP to the use of NHRP for address resolution in the LIS [1][2]. In short, NHSs will be required to respond to ATMARP Client queries in a fashion which will permit continued use of the ATMARP Client within the LIS during the ATMARP to NHRP transition period. Note that this document places no protocol requirements upon ATMARP[1] servers.

For the following, it will be assumed that the reader is familiar with the terminology as described in [1][2][3].

2. Service Requirements

If NHRP is to be used in a LIS then only NHSs will be used in the LIS; that is, there will not be a mixture of NHSs and ATMARP servers within the same LIS. Since ATMARP servers will not be able to understand NHCs and since, as described below, NHSs will respond to ATMARP Clients, this is a reasonable simplifying restriction.

This document will only address SVC based environments and will not address PVC environments. This document will refer only to ATM AAL5 as the NBMA and IP as the protocol layer since ATMARP only addresses these protocols.

2.1 NHRP Server Requirements

If NHRP Servers (NHS) are to be deployed in a LIS which contains both ATMARP Clients and NHRP Clients then NHSs MUST respond to ATMARP_Requests sent by ATMARP Clients in the same fashion that an ATMARP Server would respond as described in [1]. To do this, the NHS MUST first recognize the LLC/SNAP ATMARP code point with LLC=0xAA-AA-03, OUI=0x00-00-00, and ethertype=0x08-06. Further, the NHS MUST recognize the packet formats described in Section 8.7 of [1]. However, since this document does not extend to PVC environments,

NHSs MUST only receive/respond to values of ar\$op of 1,2,10 (Decimal). If an NHS receives an ATMARP message with ar\$op values other than those previously noted then the NHS MUST discard the packet and MUST NOT take any further action.

When an NHS receives a valid (as defined in the previous paragraph) ATMARP_Request packet, the NHS MUST follow the rules described in Section 8.4 of [1] with the following additional processing:

- 1) When an ATMARP_Request causes a new table entry in the NHS for an ATMARP Client, that table entry MUST be marked as being of type "ATMARP" so that it can be differentiated from an NHRP sourced entry.
- 2) An ATMARP_Request MUST NOT cause an ATMARP_Reply to be sent if that ATMARP_Request contains an off-LIS protocol address. This should never happen because the IP stack on the requesting machine should automatically send the packet to the default router. If this does occur then the ATMARP_Request MUST cause an ATMARP_NAK to be sent to the originator.

In [1], an ATMARP_Request packet also serves as a registration/registration-update packet which would cause a server to add an entry to a server's cache or to update a previously existing entry. When an NHS receives an ATMARP_Request which causes the creation of a new cache entry in the NHS or updates an existing entry then that cache entry will have a holding time of 20 minutes (this is the default value in [1]).

An NHS receiving an NHRP Resolution Request MUST NOT send a positive NHRP Resolution Reply for a station which registered via ATMARP if the station sending the NHRP Resolution Request is outside the LIS of the station which registered itself via ATMARP. This is because the station which registered via ATMARP is almost certainly not prepared to accept a cut-through. When this occurs, the replying NHS must send NHRP Resolution Reply which contains a CIE code of "4 - Administratively Prohibited" as described in [2]. This type of reply does not preclude the station sending the NHRP Resolution Request from sending its data packets along the routed path but it does preclude that station from setting up a cut-through VC.

2.2 Multi-server environments

Since NHRP servers may work in a multi-server environment on a per LIS basis during the transition, it is necessary to know how cache synchronization occurs. These rules may be found in [5].

3. Security Considerations

Not all of the security issues relating to IP over ATM are clearly understood at this time, due to the fluid state of ATM specifications, newness of the technology, and other factors.

It is believed that ATM and IP facilities for authenticated call management, authenticated end-to-end communications, and data encryption will be needed in globally connected ATM networks. Such future security facilities and their use by IP networks are beyond the scope of this memo.

There are known security issues relating to host impersonation via the address resolution protocols used in the Internet [4]. No special security mechanisms have been added to ATMARP. While NHRP supplies some mechanisms for authentication, ATMARP does not. Since any security mechanism is only as good as its weakest link, it should be assumed that when NHRP and ATMARP exist with a given LIS, the security of a combination is only as good as that supplied by ATMARP.

References

- [1] Laubach, M. and J. Halpern, "Classical IP and ARP over ATM", RFC 2225, April 1998.
- [2] Luciani, J., Katz, D., Piscitello, D., Cole, B. and N. Doraswamy, "NBMA Next Hop Resolution Protocol (NHRP)", RFC 2332, April 1998.
- [3] Luciani, J., Armitage, G., Halpern, J. and N. Doraswamy, "Server Cache Synchronization Protocol (SCSP)", RFC 2334, April 1998.
- [4] Security Problems in the TCP/IP Protocol Suite, Bellovin, ACM Computer Communications Review, Vol. 19, Issue 2, pp. 32-48, 1989.
- [5] Luciani, J., "A Distributed NHRP Service Using SCSP", RFC 2335, April 1998.
- [6] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

Acknowledgments

Thanks to Andy Malis for his input on this draft.

Author's Addresses

James V. Luciani
Bay Networks
3 Federal Street
Mail Stop: BL3-03
Billerica, MA 01821
Phone: +1 978 916 4734
Email: luciani@baynetworks.com

Full Copyright Statement

Copyright (C) The Internet Society (1998). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

