Internet Engineering Task Force
INTERNET DRAFT
Expires September 2001

Juha Heinanen
Telia Finland
March, 2001

Inverse ARP over Unidirectional Virtual Circuits
<draft-heinanen-inarp-uni-01.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC 2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This memo describes operation of an Inverse Address Resolution Protocol (InARP) over unidirectional virtual circuits such as MPLS LSPs.

1. Introduction

Inverse Address Resolution Protocol (InARP) [1] is commonly used by stations (usually routers) connected via Frame Relay or ATM virtual circuits to automatically learn the protocol addresses of their peers. InARP is needed when a station only knows that a virtual circuit to another station exists, but doesn't have any knowledge of protocol layer identity of the other station. This can happen either if the virtual circuit is network provisioned or if some other address than the protocol address of the other station is used in the virtual circuit setup.

When a Frame Relay or ATM local station has discovered the hardware address (Frame Relay DLCI or ATM VPI/VCI) of a remote station, it sends an InARP Request to query the protocol address of the remote station. The remote station learns the protocol address of the local station from the source protocol address field of the InARP request and the corresponding hardware address from the frame header of the InARP request. The remote station then sends an InARP response containing its own protocol address to the learned hardware address.

The above procedure does not work if the stations are connected via unidirectional virtual circuits, such as network provisioned MPLS LSPs. In order to be able migrate from network provisioned Frame Relay or ATM virtual circuits to network provisioned MPLS LSPs, a new version of InARP is needed. This memo describes the operation of InARP in situations where one or more unidirectional virtual circuits are used to implement bidirectional connectivity between two stations.

2. Protocol Operation

Once the local station (A) learns the hardware address (label) of an outgoing unidirectional virtual circuit, it constructs an InARP request to find out the protocol address of the remote station (B) to which this virtual circuit leads to. The InARP request contains the protocol address (pA) and hardware address (hA) of the local station in the source protocol and hardware address fields, respectively:

```
ar$op   8       (InARP request)
ar$sha  hA
ar$spa  pA
ar$tha  unknown
ar$tpa  unknown
```

When the remote station (B) receives the request, it constructs a response by including its own protocol address (pB) in the source protocol address field and by copying the source protocol and hardware addresses from the request to the target protocol and hardware address fields, respectively:

```
ar$op   9       (InARP response)
ar$sha  unknown
ar$spa  pB
ar$tha  hA
ar$tpa  pA
```

Because of unidirectionality of the virtual circuits, the remote station can't use the either the source hardware address in the request or the hardware address in the frame header to send the

response back to the local station. Instead, the remote station first checks if it itself has already learned about a virtual circuit, which has the same target protocol address as the source protocol address in the request. If so, the remote station sends the response to such a virtual circuit. If not, the remote station sends the response to every virtual circuit whose target protocol address is still unknown to it.

When the local station receives an InARP response, it first checks if the target address pair of the response matches an existing outgoing virtual circuit. If so, it creates a new protocol address/hardware address mapping for the virtual circuit based on the protocol address and hardware address fields of the response. I not, it silently discards the response.

Once the local station unlearns the hardware address (label) of an outgoing virtual circuit, it deletes the protocol address/hardware address mapping that was associated with it. Even if the local station doesn't unlearn a hardware address, it may be desirable to age the address/hardware address mapping after a time period. The implementation of aging (if any) is outside the scope of this memo.

3. Scalability Considerations

The above operation could potentially result in generation of a large number of simultaneous InARP responses. The worst case occurs when a full mesh of virtual circuits connecting N stations is created simultaneously and each local station sends simultaneously N-1 InARP requests to each of which every remote station (having not yet learned any addresses) replies with N-1 InARP responses.

Although it is not likely in practice that all virtual circuits are created simultaneously, InARP implementations can also help to alleviate the problem. The local stations could wait a random time interval after virtual circuit discovery before sending out their InARP requests. That would creating an effect similar to as if the stations and their virtual circuits had been added one at a time.

4. Security Considerations

This document specifies a functional enhancement to the ARP family of protocols, and is subject to the same security constraints that affect ARP and similar address resolution protocols. Because authentication is not a part of ARP, there are known security issues relating to its use (e.g., host impersonation). No additional security mechanisms have been added to the ARP family of protocols by this document.

Acknowledgements

I would like to thank Joel Halpern of Longitude Systems for his constructive comments on earlier versions of this memo.

References

[1] Bradley, T., Brown, C., and Malis, A., Inverse Address Resolution Protocol. RFC 2390, September 1998.

Author's Address

Juha Heinanen
Telia Finland, Inc.
Hallituskatu 16
33200 Tampere, Finland
Email: jh@telia.fi

Full Copyright

Copyright (C) The Internet Society (2000). 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.