Network Working Group
Request for Comments: 2107
Category: Informational

K. Hamzeh
Ascend Communications

February 1997

Ascend Tunnel Management Protocol - ATMP

Status of this Memo

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

IESG Note:

This note documents a private protocol for tunnel management. This protocol is NOT the product of an IETF working group nor is it a standards track document. There is ongoing effort in an IETF working group which could result in a standards track document which specifies a protocol which provides similar functionality.

Abstract

This document specifies a generic tunnel management protocol that allows remote dial-in users to access their home network as if they were directly attached to the home network. The user's client software uses an address contained in the home network address space for the remote access. Packets to and from the home network are tunneled by the Network Access Server (NAS) to which the user connects and a Home Agent (HA) on the user's home network. This allows for the support of access to Virtual Private Networks and also allows for the use of protocols other than IP to be carried over the tunnel. An example of how the RADIUS (Remote Authentication Dial In User Service) can be used to provide the necessary configuration information to support this service is also provided.

1. Introduction

The Ascend Tunnel Management Protocol (ATMP) is a protocol currently being used in Ascend Communication products to allow dial-in client software to obtain virtual presence on a user's home network from remote locations. A user calls into a remote NAS but, instead of using an address belonging to a network directly supported by the NAS, the client software uses an address belonging to the user's "Home Network". This address can be either provided by the client software or assigned from a pool of addresses from the Home Network address space. In either case, this address belongs to the Home Network and therefore special routing considerations are required in

order to route packets to and from these clients. A tunnel between the NAS and a special "Home Agent" (HA) located on the Home Network is used to carry data to and from the client.

ATMP currently allows for both IP and IPX protocols to be tunneled between the NAS and the HA. The protocol to be used, the HA to use, and other user specific information is provided by some configuration mechanism that is beyond the scope of this document. Appendix A illustrates how RADIUS [5] is used to convey this information to the NAS.

The determination of the Home Network address to be used can be accomplished in different ways. It could, for example, be configured in the client and negotiated by IPCP (or IPXCP). Alternatively, it could be defined to be an address specific to the given user ID, or it could be assigned from a pool of addresses provided by the Home Network for the purpose of remote dial-in access. Again, how this address is assigned and how the NAS decides to invoke ATMP for a specific call is beyond the scope of this document.

1.1 Protocol Goals and Assumptions

The ATMP protocol is implemented only by the NAS and HA. No other systems need to be aware of ATMP. All other systems communicate in the normal manner and are unaware that they may be communicating with remote clients. The clients themselves are unaware of ATMP. It is assumed that standard PPP [8] (or SLIP) clients are being used.

Unlike the mobile-IP protocol [3], ATMP assumes that a single NAS will provide the physical connection to a remote client for the duration of the session. The client will not switch between NASes expecting to keep the same IP address and all associated sessions active during these transitions. A particular client can be registered with a given HA only once at any given time. Deregistration with a HA implies loss of all higher layer sessions for that client.

IP multicasting is currently not provided by ATMP.

1.2 Terminology

The terminology used in this document is similar to that used in mobile-IP. As pointed out in the previous section, however, ATMP provides a subset of the functionality provided by mobile-IP and the meanings of the various terms used herein have been modified accordingly.

Connection Profile

A table used to route packets other than by destination address. The Connection Profile is a named entity that contains information indicating how packets addressed to it are to be routed. It may be used to route packets to unregistered IP addresses and for routing protocols other than IP (e.g., IPX).

Foreign Agent (FA)

A routing entity that resides in a NAS on a remote network that allows a mobile node to utilize a home network address. It tunnels datagrams to, and detunnels datagrams from, the home agent for the given home network.

Home Address

An address that is assigned for an extended period of time to a mobile node. It may remain unchanged regardless of where the MN is attached to the Internet. Alternatively, it could be assigned from a pool of addresses. The management of this pool is beyond the scope of this document.

Home Agent (HA)

A router on a mobile node's home network which tunnels datagrams for delivery to, and detunnels datagrams from, a mobile node when it is away from home.

Home Network

The address space of the network to which a user logically belongs. When a workstation is physically connected to a LAN, the LAN address space is the user's home network. ATMP provides for a remote virtual connection to a LAN.

Mobile Node (MN)

A host that wishes to use a Home Network address while physically connected by a point-to-point link (phone line, ISDN, etc.) to a NAS that does not reside on the Home Network. Also referred to as the client.

Mobility Binding

The association of a Home Address with a Foreign Agent IP address and a Tunnel ID.

Network Access Server (NAS)

A device providing temporary, on-demand, network access to users. This access is point-to-point using phone or ISDN lines.

Tunnel

The path followed by a datagram when it is encapsulated. The model is that, while it is encapsulated, a datagram is routed to a knowledgeable decapsulation agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination. Each mobile node connecting to a home agent does so over a unique tunnel, identified by a tunnel identifier which is unique to a given FA-HA pair. A tunnel can carry both IP and IPX datagrams simultaneously.

1.3 Protocol Overview

A mobile node that wishes to use a home address while connected to a remote NAS must register with the appropriate home agent. The foreign agent entity of the remote NAS performs this registration on behalf of the MN. Once registered, a tunnel is established between the FA and HA to carry datagrams to and from the MN. While a MN is registered with an HA, the HA must intercept any packets destined for the MN's home address and forward them via the tunnel to the FA. When the FA detects that the MN has disconnected from the NAS, it issues a deregister request to the HA.

Because ATMP allows protocols other than IP to be carried on its tunnels and also allows unregistered IP address to be used to provide for access to enterprise networks, the HA doesn't necessarily route datagrams received from the MN in the conventional manner. The registration request allows for a named "Connection Profile" to be specified in the registration request. This Connection Profile contains configuration information that tells the HA where to send packets that it receives from the MN.

1.4 Specification Language

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

MUST This word, or the adjective "required", means that the definition is an absolute requirement of the specification.

MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective "recommended", means that, in some circumstances, valid reasons may exist to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course. Unexpected results may result otherwise.
MAY	This word, or the adjective "optional", means that this item is one of an allowed set of alternatives. An implementation which does not include this option MUST be prepared to interoperate with another implementation which does include the option.
silently discard	The implementation discards the datagram without further processing, and without indicating an error to the sender. The implementation SHOULD provide the capability of logging the error, including the contents of the discarded datagram, and SHOULD record the event in a statistics counter.

2.0 Protocol Specification

ATMP defines a set of request and reply messages sent with UDP [4]. The HA listens on UDP port 5150 [6]) for requests from FA's. The UDP checksum field MUST be computed and verified. There are 7 different ATMP message types represented by the following Type values:

Message Type	Type code
Registration Request	1
Challenge Request	2
Challenge Reply	3
Registration Reply	4

Deregister Request	5
Deregister Reply	6
Error Notification	7

2.1 Registration Request

The FA issues a Registration Request to request the HA to establish a mobility binding for the specified MN home address. The request is issued to the HA by the FA upon detecting a MN that wishes to use a home address supported by the HA receiving the request.

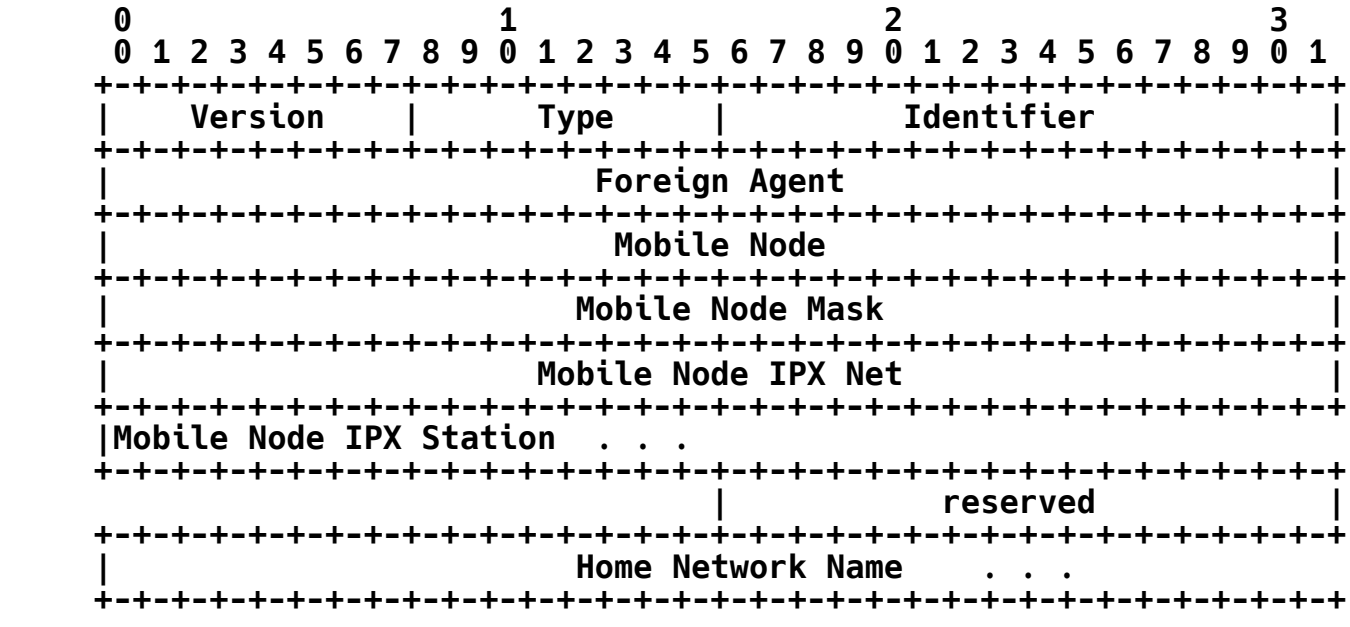
IP fields

Source Address	The IP address of the foreign agent interface from which the request is issued.
Destination Address	The IP address of the home agent.

UDP fields:

Source Port	variable
Destination Port	5150 (or port number configured in FA for given HA)

The UDP header is followed by the ATMP fields shown below:



Version	The ATMP protocol version. MUST be 1.
Type	1 for Registration Request.
Identifier	A 16 bit number used to match replies with requests. A new value should be provided in each new request. Retransmissions of the same request should use the same identifier.
Foreign Agent	The IP address of the foreign agent issuing the request (typically the same as the UDP source address).
Mobile Node	The IP address to be used by the mobile node. This is the mobile node's home address. This field can be all 0's if IPX is to be tunneled to the mobile node.
Mobile Node Mask	The network bit mask for the mobile node. Currently this value should be set to all 1's.
Mobile Node IPX Net	The Network portion of the mobile node's IPX address. This value should be set to all 0's if only IP is to be tunneled.

Mobile Node IPX Station	The 6 octet value used to represent the station portion of the mobile node's IPX address. This value should be set to all 0's if only IP is to be tunneled instead of IPX.
Reserved	This field is for future extensibility and MUST be set to all 0's.
HN Name	This is the name of the "Connection Profile" to be used by the home agent to forward all packets received from the mobile node. This character string is terminated by a NUL character and can be up to 32 characters long, including the NUL terminator.

2.2 Challenge Request

The Home Agent issues a Challenge Request in response to the receipt of a Registration Request from a Foreign Agent. It is used by the Home Agent, in conjunction with the Challenge Reply, to authenticate the Foreign Agent.

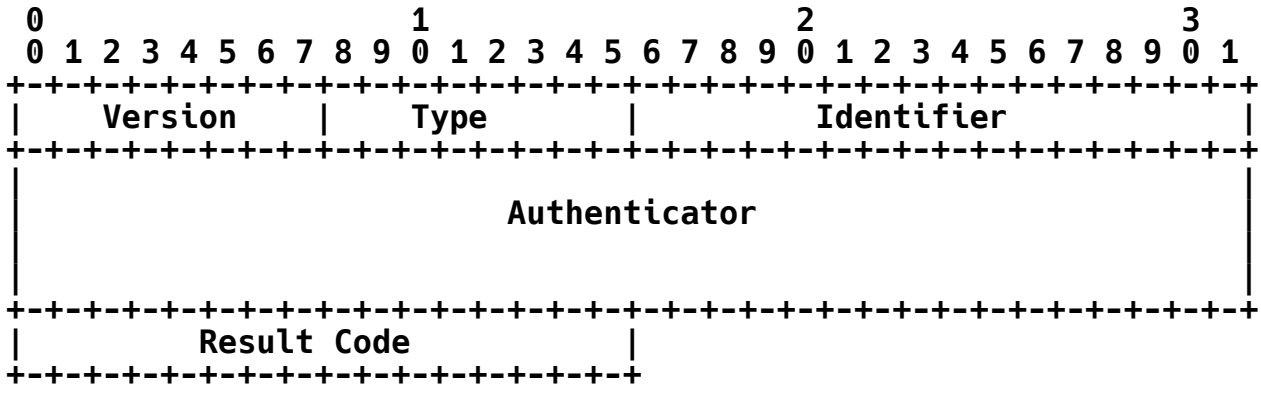
IP fields

Source Address	The IP address of the Home Agent interface from which the request is issued.
Destination Address	Copied form the Source Address of the Registration Request.

UDP fields:

Source Port	variable
Destination Port	Copied from the Source Port of the Registration Request.

The UDP header is followed by the ATMP fields shown below:



Version	The ATMP protocol version. MUST be 1.
Type	2 for Challenge Request
Identifier	A 16 bit number used to match replies with requests. A new value should be provided in each new request. Retransmissions of the same request should use the same identifier.
Authenticator	A series of 16 octet values randomly generated by the Home Agent. The receiving Foreign Agent is to perform an MD5 [7] hash of these values along with a shared secret. The resultant digest is returned in the Challenge Reply. See Sec. 2.3 Retransmissions of the Challenge Request should use the same Authenticator value. A value of all 0's in this field indicates an error occurred with the Registration Request. The error code will be in the following field.

Result Code	If non-zero, this value indicates the error condition that occurred. See Sec. 2.8 for a list of Result Code values and their meanings. A non-zero value in this field implies that the Authenticator field will be zero.

2.3 Challenge Reply

The Foreign Agent issues a Challenge Reply upon receipt of a valid Challenge Request (one with a Result Code of 0) from the Home Agent. The Foreign Agent uses the randomly generated Authenticator value from the Challenge Request along with a shared secret to produce an MD5 digest value which is returned to the Home Agent in the Challenge Reply.

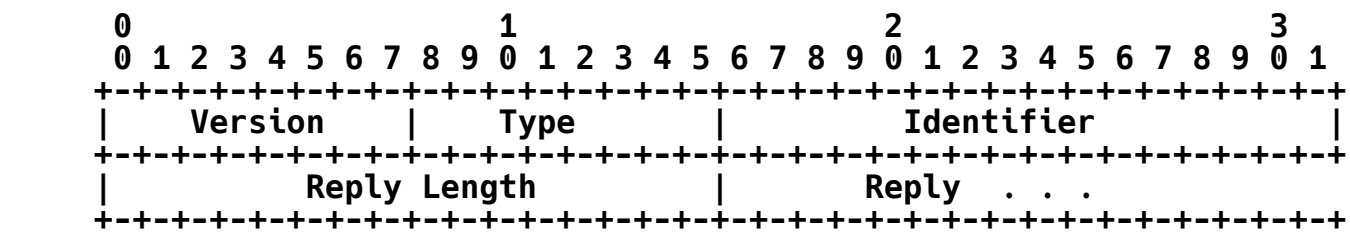
IP fields

Source Address	The IP address of the Foreign Agent interface from which the reply is issued.
Destination Address	Copied from the Source Address of the Challenge Request.

UDP fields:

Source Port	variable
Destination Port	Copied from the Source Port of the Challenge Request.

The UDP header is followed by the ATMP fields shown below:



Version	The ATMP protocol version. MUST be 1.
Type	3 for Challenge Reply
Identifier	Copied from the corresponding Deregistration Request.
Reply Length	This field specifies the length of the challenge reply computation based on the received Authenticator and the shared secret. For MD5 this length will always be 16. This field is provided for future extensibility.
Reply	This is the computed challenge reply. It is computed by performing an MD5 message digest computation over the Authenticator value received in the Challenge Request appended with the secret shared between the Foreign Agent and the Home Agent. The digests produced by MD5 are always 16 octets long.

2.4 Registration Reply

A Registration Reply is issued by a Home Agent in reply to a Challenge Reply received from a Foreign Agent. The Registration Reply indicates to the Foreign Agent whether the registration was accepted by the Home Agent or not. It also provides a "tunnel ID" to uniquely identify the tunnel to be associated with this session.

The Home Agent calculates the same MD5 hash on the Challenge Request Authenticator field and the shared secret. The resulting digest is compared with the Reply value in the Challenge Reply and if it is equal, authentication is successful. Otherwise the registration is not accepted and the Foreign Agent is informed by the Result Code of the Registration Reply that registration failed due to an authentication failure.

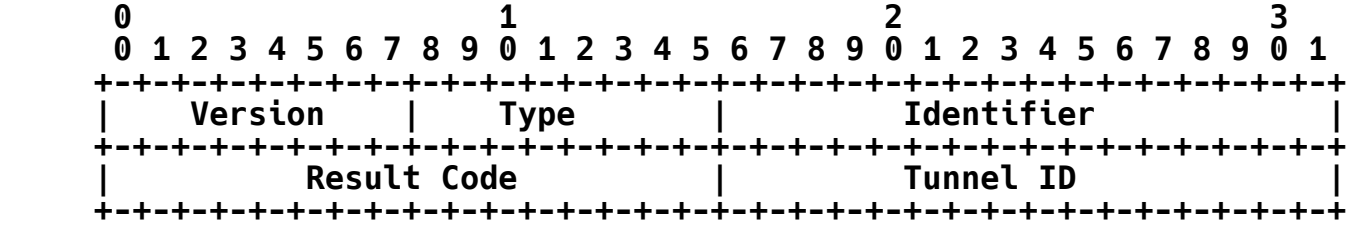
IP fields

Source Address	The IP address of the Home Agent interface from which the reply is issued.
Destination Address	Copied from the Source Address of the Challenge Reply.

UDP fields:

Source Port	variable
Destination Port	Copied from the Source Port of the Challenge Reply.

The UDP header is followed by the ATMP fields shown below:



Version	The ATMP protocol version. MUST be 1.
Type	4 for Registration Reply
Identifier	Copied from the corresponding Registration Request.
Result Code	Specifies the result of the registration and authentication attempt by the Foreign Agent. Sec. 2.8 for a list of Result Code values and their meanings.
Tunnel ID	This is the identifier used to indicate a given mobility binding between a given Mobile Node and Home Agent. This identifier is used to distinguish multiple tunnels between a given Foreign Agent-Home Agent pair. It is carried in the "key" field of the GRE [1] tunnel packets that ATMP uses as the tunnel protocol. It is also used in Deregistration Requests and Error Notification messages to indicate the particular mobility binding to which they relate.

2.5 Deregistration Request

The Deregistration Request is issued by the Foreign Agent to the Home Agent to indicate that the specified mobility binding is to be ended. This request may result from the Foreign Agent detecting that its connection to the Mobile Node has terminated. It can also be issued in response to a detected error condition by the Foreign Agent or receipt of an Error Notification message from the Home Agent.

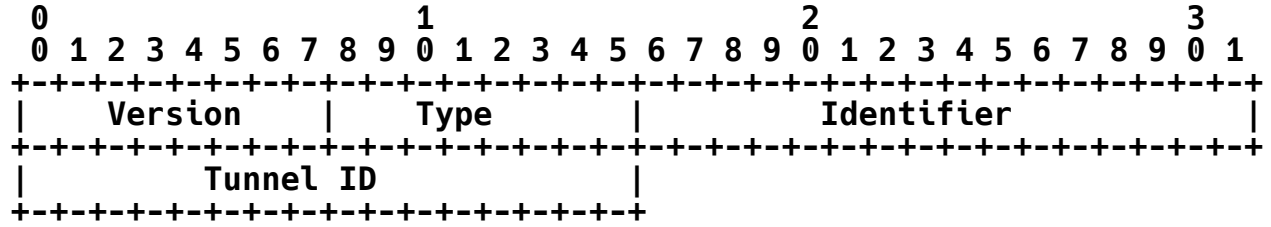
IP fields

Source Address	The IP address of the Foreign Agent interface from which the request is issued.
Destination Address	5150 (or port number configured in FA for given HA)

UDP fields:

Source Port	variable
Destination Port	Copied from the Source Port of the Challenge Reply.

The UDP header is followed by the ATMP fields shown below:



Version	The ATMP protocol version. MUST be 1.
Type	5 for Deregistration Request
Identifier	A 16 bit number used to match replies with requests. A new value should be provided in each new request. Retransmissions of the same request should use the same identifier.

Tunnel ID	Tunnel identifier of the mobility binding to be terminated.

2.6 Deregistration Reply

The Deregistration Reply is issued by the Home Agent in response to a Deregistration Request received from a Foreign Agent. If the Deregistration Request was valid, the Home Agent removes the specified mobility binding from its tables and issues an affirmative reply. Otherwise the Home Agent issues a Deregistration Reply with a Result Code indicating the reason for failure of the Deregistration Request.

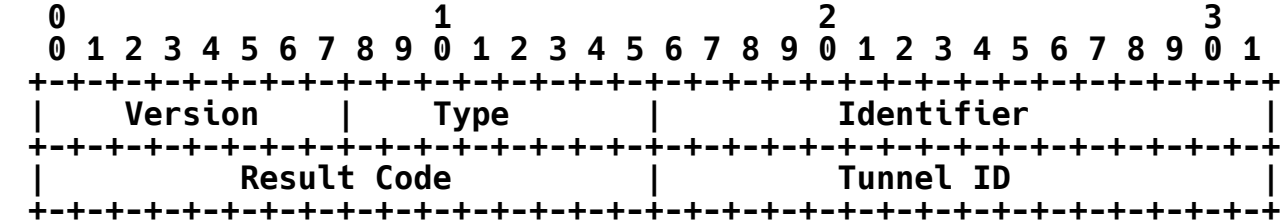
IP fields

Source Address	The IP address of the Home Agent interface from which the reply is issued.
Destination Address	Copied from the Source Address of the received Deregistration Request.

UDP fields:

Source Port	variable
Destination Port	Copied from the Source Port of the received Deregistration Request.

The UDP header is followed by the ATMP fields shown below:



Version	The ATMP protocol version. MUST be 1.
Type	6 for Deregistration Reply
Identifier	Copied from the corresponding Deregistration Request.

Result Code	Specifies the result of the registration and authentication attempt by the Foreign Agent. Sec. 2.8 for a list of Result Code values and their meanings.
Tunnel ID	Tunnel identifier of the mobility binding specified in the Deregistration Request.

2.7 Error Notification

This message is sent by either agent to inform the other agent that an error condition has occurred. It provides a last-ditch error recovery mechanism that is used for conditions that cannot be reported back to the sender by the normal request-reply mechanism, such as the receipt of a spontaneously generated reply.

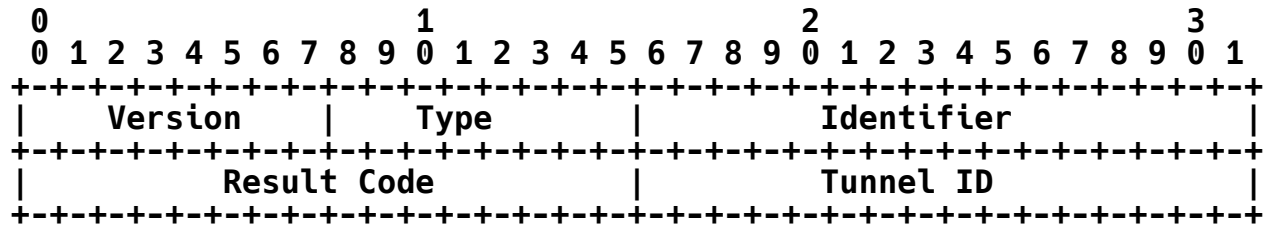
IP fields

Source Address	The IP address of the issuing agent interface from which this message is issued.
Destination Address	The IP address of the Home Agent or Foreign Agent to which this message is to be issued.

UDP fields:

Source Port	variable
Destination Port	If issued to a Home Agent, 5150 (or the port number configured for the given HA). If issued to a Foreign Agent, the source port number saved from the original Registration Request.

The UDP header is followed by the ATMP fields shown below:



Version	The ATMP protocol version. MUST be 1.
Type	7 for Error Notification
Identifier	If issued in response to a received reply type message, this value should be copied from the identifier field of the reply. Otherwise the identifier should be the value that would be used for the next generated request.
Result Code	This indicates the type of error detected. The possible result codes are defined in Sec. 2.8.
Tunnel ID	Tunnel identifier of the mobility binding to which this message pertains. If the Error Notification is being sent in response to an unsolicited reply, the Tunnel ID is copied from the reply.

2.8 Result Codes

Error Code	Description
0 NO_ERROR	Successful operation
1 AUTH_FAILED	Authentication of the Foreign Agent failed. Registration denied.
2 NOT_ENABLED	The Home Agent is not configured to run ATMP.
3 TOO_MANY	Too many Mobile Node sessions. Home Agent is out of resources.
4 PARAMETER_ERROR	An invalid value was detected in an ATMP message.
5 INVALID_TUNNEL_ID	The Tunnel ID contained in a GRE packet is invalid or the corresponding mobility binding does not exist. This usually occurs when either the MN or HA has reset.
6 TIMEOUT	A response to an ATMP request was not received in time.

7	NET_UNREACHABLE	The Home Network for this mobility binding is not operational (the "Connection Profile" is "down" or is not defined).
8	GENERAL_ERROR	General Error indication.

2.9 Protocol Operation

Upon detection of a Mobile Node requiring ATMP service, the NAS invokes its ATMP Foreign Agent entity.The FA retrieves configuration information for the user involved.This information is obtained in a method particular to the NAS and is not specified by this document. The information obtained MUST include the Home Agent address and the shared secret for this HA.It also MAY include the Home Network Name, if a Connection Profile is to be used for this session.

The FA then sends a Registration Request to the HA informing it that an MN wishes to register with it. The FA then waits for the HA to respond with a Challenge Request. The FA retransmits the Registration Request every 2 seconds until it receives the Challenge Request. If, after 10 retransmissions, no Challenge Request is received, the FA will terminate the Registration Request, logs the registration failure, and disconnects the MN.

Upon receipt of the Challenge Request, the FA examines the Result code. If it indicates an error condition, the condition is logged and the MN is disconnected. If the result is zero, the FA generates a Challenge Reply. The Challenge Reply is generated by appending the Authenticator obtained from the Challenge Request with the shared secret (obtained from the configuration data) and then computing the MD5 hash of this concatenated string (authenticator + secret). The 16 octet hash is then returned in the Challenge Reply for validation by the HA.

Upon receipt of the Challenge Reply from the FA, the HA does the same computation of the MD5 hash based on the Challenge Request Authenticator and the shared-secret (which it too must be configured with). If this digest matches that provided in the Challenge Reply by the FA then the authentication is successful and the registration is accepted. If the authentication fails, or resource limitations prohibit the registration attempt, the HA returns a Registration Reply with a non-zero result code to the FA.

If the HA accepts the Challenge Reply from the FA, it assigns a Tunnel ID to this session and returns this Tunnel ID in a Registration Reply with a zero result code. This Tunnel ID needs to be unique for the FA-HA pair. The Tunnel ID is used to multiplex and demultiplex the packets sent between a given FA-HA pair.

At the time the HA decides to accept a registration, it creates a control block that associates the Tunnel ID with the appropriate routing information. If the Registration Request included a Home Network Name, this name is saved in the table and used as the name of the Connection Profile for this session.

Upon receipt of the Registration Reply, the FA examines the result code. If it is non-zero, the FA logs the registration failure and disconnects the MN. If it is zero, the FA saves the Tunnel ID in a control block associated with the MN session. The FA and HA are now ready to exchange data packets for this MN session.

On the FA side, all data received from the MN will be encapsulated using GRE and sent to the HA with the assigned Tunnel ID included in the GRE Key field. When the HA receives a GRE packet it decapsulates it and routes it using the routing information contained in the HA's control block associated with this Tunnel ID.

When the HA receives a packet destined for the MN's Home Address, it MUST encapsulate it in a GRE packet and forward it to the appropriate FA. The Tunnel ID is included in the GRE Key field to allow the FA to demultiplex the packet.

When the FA receives a GRE packet, it will examine the Tunnel ID in the GRE Key field to see if it matches the Tunnel ID assigned to any of the MN's currently connected to the FA. If so, the packet is decapsulated and forwarded to the MN. If the Tunnel ID doesn't match any active MN's, an Error Notification message is issued to the HA and the GRE packet is silently discarded.

When the FA wishes to disconnect the MN from the HA, it issues a Deregistration Request. This request is issued every 2 seconds. If after 10 attempts a Deregistration Reply is not received from the HA, an error condition is logged and the MN is disconnected. Upon receipt of a Deregistration Reply from the HA, the FA deallocates the Tunnel ID and disconnects the MN.

3.0 Security Considerations

The Registration function of ATMP is protected by a Challenge/Response mechanism similar to CHAP [2]. The Home Agent challenges each registration attempt by a Foreign Agent for authentication.This authentication requires the configuration of a shared secret for each HA/client pair.

4.0 Author's Address

Kory Hamzeh
Ascend Communications
1275 Harbor Bay Parkway
Alameda, CA 94502

EMail: kory@ascend.com

5.0 References

[1] Hanks, S. Li, T., Farinacci, D., and Traina, P., "Generic Routing Encapsulation (GRE)", RFC 1701, October 1994.

[2] Lloyd, B., and W. Simpson, "PPP Authentication Protocols", RFC 1334, October 1992.

[3] Perkins, C., "IP Mobility Support", RFC 2002, October 1996.

[4] Postel, J., "User Data Protocol", STD 6, RFC 768, August 1990.

[5] Rigney, C., Rubens, A., Simpson, W., and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2058, January 1997.

[6] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1700, October, 1994.

[7] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

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

Appendix A

Additional RADIUS Attributes for ATMP

This appendix indicates the RADIUS attributes that have been added by Ascend to support ATMP for IP. Currently these are defined as non-vendor-specific attributes but have been included in [5].

```
Attribute: "Ascend-Home-Agent-IP-Addr"
Type:      IP-Address
Value:     The IP address of the Home Agent

Attribute: "Ascend-Home-Agent-Password"
Type:      String
Value:     Secret shared for this user with HA

Attribute: "Ascend-Home-Network-Name"
Type:      String
Value:     Name of Connection Profile for this session

Attribute: "Ascend-Home-Agent-UDP-Port"
Type:      Integer
Value:     The destination UDP port number for the specified HA
```

Appendix B

IPX Operation

ATMP specifies a mechanism which allows IPX clients to receive mobility services from a HA. Section 2 details the protocol used to register, deregister, and authenticate a tunnel used for IPX. Note that ATMP is based on IP datagrams for the management of tunnels and, thus, IPX tunneling with ATMP always requires an underlying IP network.

Each IPX mobile client requires an IPX network number and node address pair. Since IPX does not support a similar facility to IP's "host route," an enterprise-unique network number needs to be chosen for each home agent. This network number MUST be distinct from the IPX network number assigned to any of the home agent's LAN interfaces. Each mobile client tunneled to the home agent MUST use the same IPX network number.

For example, consider a home agent which supports two mobile clients. The home agent is on a LAN network with an IPX address of AA000001. The home agent's client network may be assigned AA000002. The two mobile clients may have addresses AA000002:0040F1000001 and AA000002:0040F1000002 respectively.

IPX node numbers need to be unique on a given network. A mechanism must exist to guarantee that for each home agent's network, a given mobile client's node address is unique. Several techniques may be employed to assure unique node addresses. The current implementation of ATMP described in this document relies on RADIUS to assign a node address at the foreign agent. The following RADIUS attributes are included for IPX operation in addition to the attributes described in Appendix A for IP operation:

Attribute: "Framed-IPX-Network" (See [5] for details).

Attribute: "Ascend-IPX-Node-Addr"
Type: String
String: The node address for the mobile client in 12 octet ASCII representing the hexadecimal string. Both lower and upper case characters are permissible.