RADIUS Working Group
INTERNET-DRAFT
Category: Standards Track
<draft-ietf-radius-tunnel-imp-07.txt>
18 May 1998

Bernard Aboba
Microsoft
Glen Zorn
Microsoft

Implementation of PPTP/L2TP Compulsory Tunneling via RADIUS

1. Status of this Memo

2. Abstract

This document discusses implementation issues arising in the provisioning of compulsory tunneling in dial-up networks using the PPTP and L2TP protocols. This provisioning can be accomplished via the integration of RADIUS and tunneling protocols. Implementation issues encountered with other tunneling protocols are left to separate documents.

3. Terminology

Voluntary Tunneling
: In voluntary tunneling, a tunnel is created by the user, typically via use of a tunneling client.

Compulsory Tunneling
: In compulsory tunneling, a tunnel is created without any action from the user and without allowing the user any

choice.

Roaming "Roaming capability" can be loosely defined as the ability to use any one of multiple Internet service providers (ISPs), while maintaining a formal, customer-vendor relationship with only one. Examples of cases where roaming capaility might be required include ISP "confederations" and ISP-provided corporate network access support.

Shared Use Network
This is an IP dialup network whose use is shared by two or more organizations. Shared use networks typically implement distributed authentication and accounting in order to facilitate the relationship among the sharing parties. Since these facilities are also required for implementation of roaming, implementation of shared use is frequently a first step toward development of roaming capabilities. In fact, one of the ways by which a provider can offer roaming service is to conclude shared use agreements with multiple networks. However, to date the ability to accomplish this has been hampered by lack of interoperability among shared use implementations.

Tunnel Network Server
This is a server which terminates a tunnel. In PPTP terminology, this is known as the PPTP Network Server (PNS). In L2TP terminology, this is known as the L2TP Network Server (LNS).

Network Access Server
The Network Access Server (NAS) is the device that clients contact in order to get access to the network. In PPTP terminology this is referred to as the PPTP Access Concentrator (PAC). In L2TP terminology, the NAS is referred to as the L2TP Access Concentrator (LAC).

RADIUS server
This is a server which provides for authentication/authorization via the protocol described in [3], and for accounting as described in [4].

RADIUS proxy
In order to provide for the routing of RADIUS authentication and accounting requests, a RADIUS proxy can be employed. To the NAS, the RADIUS proxy appears to act as a RADIUS server, and to the RADIUS server, the proxy appears to act as a RADIUS client.

Network Access Identifier
In order to provide for the routing of RADIUS authentication

and accounting requests, the userID field used in PPP and in the subsequent RADIUS authentication and accounting requests, known as the Network Access Identifier (NAI) MAY contain structure. This structure provides a means by which the RADIUS proxy will locate the RADIUS server that is to receive the request. This same structure MAY also be used to

locate the tunnel endpoint when domain-based tunneling is used.

4. Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [9].

5. Introduction

Many applications of tunneling protocols involve dial-up network access. Some, such as the provisioning of secure access to corporate intranets via the Internet, are characterized by voluntary tunneling: the tunnel is created at the request of the user for a specific purpose. Other applications involve compulsory tunneling: the tunnel is created without any action from the user and without allowing the user any choice.

Examples of applications that might be implemented using compulsory tunnels are Internet software upgrade servers, software registration servers and banking services. These are all services which, without compulsory tunneling, would probably be provided using dedicated networks or at least dedicated network access servers (NAS), since they are characterized by the need to limit user access to specific hosts.

Given the existence of widespread support for compulsory tunneling, however, these types of services could be accessed via any Internet service provider (ISP). The most popular means of authorizing dial-up network users today is through the RADIUS protocol. The use of RADIUS allows the dial-up users' authorization and authentication data to be maintained in a central location, rather than on each NAS. It makes sense to use RADIUS to centrally administer compulsory tunneling, since RADIUS is widely deployed and was designed to carry this type of information. New RADIUS attributes are needed to carry the tunneling information from the RADIUS server to the NAS and to transfer accounting data from the NAS to the RADIUS accounting server; those attributes are defined in [7] and [13].

5.1. Advantanges of RADIUS-based compulsory tunneling

The use of RADIUS in provisioning of compulsory tunnels has several advantages. These include:

User-based tunneling
Auditing capabilities

5.1.1. User-based Tunneling

Current proposals for routing of tunnel requests include static tunneling, where all users are automatically tunneled to a given endpoint, and realm-based tunneling, where the tunnel endpoint is determined from the realm portion of the userID. User-based tunneling as provided by integration of RADIUS and tunnel protocols offers significant advantages over both of these approaches.

Static tunneling requires dedication of a NAS device to the purpose. In the case of an ISP, this is undesirable because it requires them to dedicate a NAS to tunneling service for a given corporate customer, rather than allowing them to use existing NASes deployed in the field. As a result static tunneling is likely to be costly for deployment of a global service.

Realm-based tunneling assumes that all users within a given realm wish to be treated the same way. This limits flexibility in account management. For example, BIGCO may desire to provide Janet with an account that allows access to both the Internet and the intranet, with Janet's intranet access provided by a tunnel server located in the engineering department. However BIGCO may desire to provide Fred with an account that provides only access to the intranet, with Fred's intranet access provided by a tunnel network server located in the sales department. Such a situation cannot be accommodated with realm-based tunneling, but can be accomodated via user-based tunneling as enabled by the attributes defined in [7]. When deployed in concert with roaming, user-based tunneling offers corporations the ability to provide their users with access to the corporate Intranet on a global basis.

5.2. Auditing Capabilities

The integration of RADIUS and tunnel protocols allows the ISP and the corporation to synchronize their accounting activities so that each side receives a record of the user's resource consumption. This provides the corporation with the means to audit ISP bills.

In auditing, the User-Name, Acct-Tunnel-Connection, Tunnel-Client-Endpoint and Tunnel-Server-Endpoint attributes are typically used to uniquely identify the call, allowing the Accounting-Request sent by the NAS to be reconciled with the corresponding Accounting-Request sent by the tunnel server.

When implementing L2TP/PPTP tunneling based on RADIUS, the Call-Serial-Number SHOULD be used in the Acct-Tunnel-Connection attribute. In L2TP, the Call-Serial-Number is a 32-bit field and in PPTP it is a 16-bit field. As described in [6], in PPTP the combination of IP Address and Call-Serial-Number SHOULD be unique, but this is not

required. In addition, no method for determining the Call-Serial-Number is specified, which leaves open the possibility of wrapping after a reboot.

Note that a 16-bit Call-Serial-Number is not sufficient to distinguish a given call from all other calls over an extended time period. For example, if the Call-Serial-Number is assigned monotonically, the NAS in question has 96 ports which are continually busy and the average call is of 20 minutes duration, then a 16-bit Call-Serial-Number will wrap within 65536/(96 * 3 calls/hour * 24 hours/day) = 9.48 days.

6. Authentication alternatives

RADIUS-based compulsory tunneling can support both single authentication, where the user is authenticated at the NAS or tunnel server, or dual authentication, where the user is authenticated at both the NAS and the tunnel server. When single authentication is supported, a variety of modes are possible, including telephone-number based authentication. When dual-authentication is used, a number of modes are available, including dual CHAP authentications; CHAP/EAP authentication; CHAP/PAP(token) authentication; and EAP/EAP authentication, using the same EAP type for both authentications.

The alternatives are described in more detail below.

6.1. Single authentication

Single authentication alternatives include:

NAS authentication
NAS authentication with RADIUS reply forwarding
Tunnel server authentication

6.1.1. NAS authentication

With this approach, authentication and authorization (including tunneling information) occurs once, at the NAS. The advantages of this approach are that it disallows network access for unauthorized NAS users, and allows RADIUS accounting to be used at the NAS. Disadvantages are that it requires that the tunnel server trust the NAS, since no user authentication occurs at the tunnel server. Due to the lack of user authentication, accounting cannot take place at the tunnel server with strong assurance that the correct party is being billed.

NAS-only authentication is most typically employed along with LCP forwarding and tunnel authentication, both of which are supported in L2TP, described in [5]. Thus, the tunnel server can be set up to accept all calls occurring within authenticated tunnels, without requiring PPP authentication. This approach is not compatible with roaming, since the tunnel server will typically only be set up to

accept tunnels from a restricted set of NASes. A typical initiation sequence looks like this:

Client and NAS: Call Connected
Client and NAS: PPP LCP negotiation

```
Client and NAS: PPP authentication
NAS to RADIUS Server: RADIUS Access-request
RADIUS server to NAS: RADIUS Access-Accept/Access-Reject
NAS to Tunnel Server: L2TP Incoming-Call-Request w/LCP forwarding
Tunnel Server to NAS: L2TP Incoming-Call-Reply
NAS to Tunnel Server: L2TP  Incoming-Call-Connected
Client and Tunnel Server: NCP negotiation
NAS to RADIUS Server: RADIUS Accounting-Request with
  Acct-Status-Type=Tunnel-Link-Start
RADIUS Server to NAS: RADIUS Accounting-Response
```

The process begins with an incoming call to the NAS, and the PPP LCP negotiation between the client and the NAS. In order to authenticate the client, the NAS will send a RADIUS Access-Request to the RADIUS server and will receive a RADIUS Access-Accept including tunnel attributes, or an Access-Reject.

In the case where an L2TP tunnel is indicated, the NAS will now bring up a control connection if none existed before, and the NAS and tunnel server will bring up the call. At this point, data will begin to flow through the tunnel. The NAS will typically employ LCP forwarding, although it is also possible for the tunnel server to renegotiate LCP. If LCP renegotiation is to be permitted, the NAS SHOULD NOT send an LCP CONFACK completing LCP negotiation. Rather than sending an LCP CONFACK, the NAS will instead send an LCP DOWN message. The Client MAY then renegotiate LCP, and from that point forward, all PPP packets originated from the client will be encapsulated and sent to the tunnel server.

Since address assignment will occur at the tunnel server, the client and NAS MUST NOT begin NCP negotiation. Instead, NCP negotiation will occur between the client and the tunnel server.

6.1.2. NAS authentication with RADIUS reply forwarding

With this approach, authentication and authorization occurs once at the NAS and the RADIUS reply is forwarded to the tunnel server. This approach disallows network access for unauthorized NAS users; does not require trust between the NAS and tunnel server; and allows for RADIUS accounting to be used at both ends of the tunnel. However, it also requires that both ends share the same secret with the RADIUS server, since that is the only way that the tunnel server can check the RADIUS reply.

In this approach, the tunnel server will share secrets with all the NASes and associated RADIUS servers, and there is no provision for LCP renegotiation by the tunnel server. Also, the tunnel server will need

to know how to handle and verify RADIUS Access-Accept messages.

While this scheme can be workable if the reply comes directly from a RADIUS server, it would become unmanageable if a RADIUS proxy is involved, since the reply would be authenticated using the secret shared by the client and proxy, rather than the RADIUS server. As a

result, this scheme is impractical.

6.1.3. Tunnel server authentication

In this scheme, authentication and authorization occurs once at the tunnel server. This requires that the NAS determine that the user needs to be tunneled (through RADIUS or NAS configuration). Where RADIUS is used, the determination can be made using one of the following methods:

Telephone-number based authentication
User-Name

6.1.3.1. Telephone-number based authentication

Using the Calling-Station-Id and Called-Station-Id RADIUS attributes, authorization and subsequent tunnel attributes can be based on the phone number originating the call, or the number being called. This allows the RADIUS server to authorize users based on the calling phone number or to provide tunnel attributes based on the Calling-Station-Id or Called-Station-Id. Similarly, in PPTP/L2TP the tunnel server MAY choose to reject or accept the call based on the Dialed Number and Dialing Number included in the PPTP/L2TP Incoming-Call-Request packet sent by the NAS.

The use of RADIUS accounting by the NAS and/or the tunnel server allows for accounting to take place based on the Calling-Station-Id and Called-Station-Id. RADIUS as defined in [3] requires that an Access-Request packet contain a User-Name attribute as well as either a CHAP-Password or User-Password attribute, which must be non-empty. To satisfy this requirement the Called-Station-Id or Calling-Station-Id may be furnished in the User-Name attribute and a dummy value may be used in the User-Password or CHAP-Password attribute.

In the case of telephone-number based authentication, a typical initiation sequence looks like this:

Client and NS: Call Connected
NAS to RADIUS Server: RADIUS Access-request
RADIUS server to NAS: RADIUS Access-Accept/Access-Reject
NAS to Tunnel Server: PPTP/L2TP Incoming-Call-Request
Tunnel Server to NAS: PPTP/L2TP Incoming-Call-Reply
NAS to Tunnel Server: PPTP/L2TP Incoming-Call-Connected
Client and Tunnel Server: PPP LCP negotiation
Client and Tunnel Server: PPP authentication
Tunnel Server to RADIUS Server: RADIUS Access-request (optional)
RADIUS server to Tunnel Server: RADIUS Access-Accept/Access-Reject

```
Client and Tunnel Server: NCP negotiation
NAS to RADIUS Server: RADIUS Accounting-Request
  with Acct-Status-Type=Tunnel-Link-Start
RADIUS Server to NAS: RADIUS Accounting-Response
Tunnel Server to RADIUS Server: RADIUS Accounting-Request
```

with Acct-Status-Type=Tunnel-Link-Start (Optional)
RADIUS Server to Tunnel Server: RADIUS Accounting-Response

The process begins with an incoming call to the NAS. If configured for telephone-number based authentication, the NAS sends a RADIUS Access-Request containing the Calling-Station-Id and the Called-Station-Id attributes. The RADIUS server will then respond with a RADIUS Access-Accept or Access-Reject.

The NAS MUST NOT begin PPP authentication before bringing up the tunnel. If timing permits, the NAS MAY bring up the tunnel prior to beginning LCP negotiation with the peer. If this is done, then LCP will not need to be renegotiated between the peer and tunnel server, nor will LCP forwarding need to be employed.

If the initial telephone-number based authentication is unsuccessful, the RADIUS server sends a RADIUS Access-Reject. In this case, the NAS MUST send an LCP-Terminate and disconnect the user.

In the case where tunnel attributes are included in the RADIUS Access-Accept, and a PPTP/L2TP tunnel is indicated, the NAS will now bring up a control connection if none existed before. This is accomplished by sending a PPTP/L2TP Start-Control-Connection-Request message to the tunnel server. The tunnel server will then reply with a PPTP/L2TP Start-Control-Connection-Reply. If this message indicates an error, or if the control connection is terminated at any future time, then the NAS MUST send an LCP-Terminate and disconnect the user.

The NAS will then send an PPTP/L2TP Incoming-Call-Request message to the tunnel server. Among other things, this message will contain the Call Serial Number, which along with the NAS-IP-Address and Tunnel-Server-Endpoint is used to uniquely identify the call. The tunnel server will reply with a PPTP/L2TP Incoming-Call-Reply message. If this message indicates an error, then the NAS MUST send an LCP-Terminate and disconnect the user. If no error is indicated, the NAS then replies with a PPTP/L2TP Incoming-Call-Connected message.

At this point, data MAY begin to flow through the tunnel. If LCP negotiation had been begun between the NAS and the client, then LCP forwarding may be employed, or the client and tunnel server will now renegotiate LCP and begin PPP authentication. Otherwise, the client and tunnel server will negotiate LCP for the first time, and then move on to PPP authentication.

If a renegotiation is required, at the time that the renegotiation begins, the NAS SHOULD NOT have sent an LCP CONFACK completing LCP negotiation, and the client and NAS MUST NOT have begun NCP negotiation. Rather than sending an LCP CONFACK, the NAS will instead send an

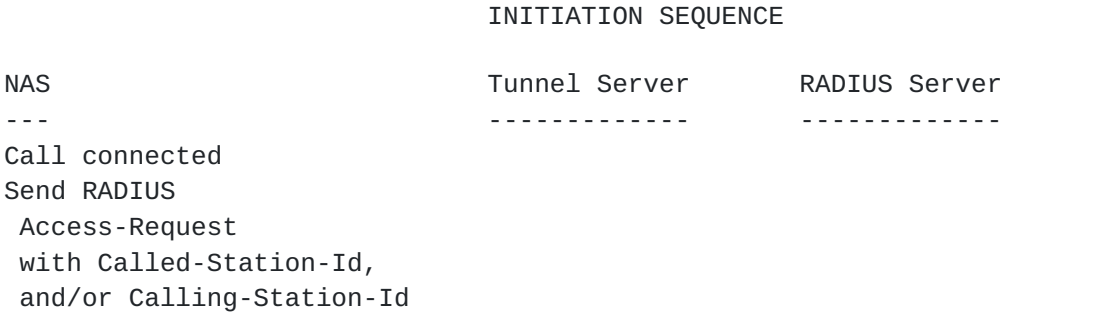
LCP DOWN message. The Client MAY then renegotiate LCP, and from that point forward, all PPP packets originated from the client will be encapsulated and sent to the tunnel server. When LCP re-negotiation has been concluded, the NCP phase will begin, and the tunnel server will assign an address to the client.

If L2TP is being used as the tunnel protocol, and LCP renegotiation is required, the NAS MAY in its initial setup notification include a copy of the LCP CONFACKs sent in each direction which completed LCP negotiation. The tunnel server MAY then use this information to avoid an additional LCP negotiation. With L2TP, the initial setup notification can also include the authentication information required to allow the tunnel server to authenticate the user and decide to accept or decline the connection. However, in telephone-number based authentication, PPP authentication MUST NOT occur prior to the NAS bringing up the tunnel. As a result, L2TP authentication forwarding MUST NOT be employed.

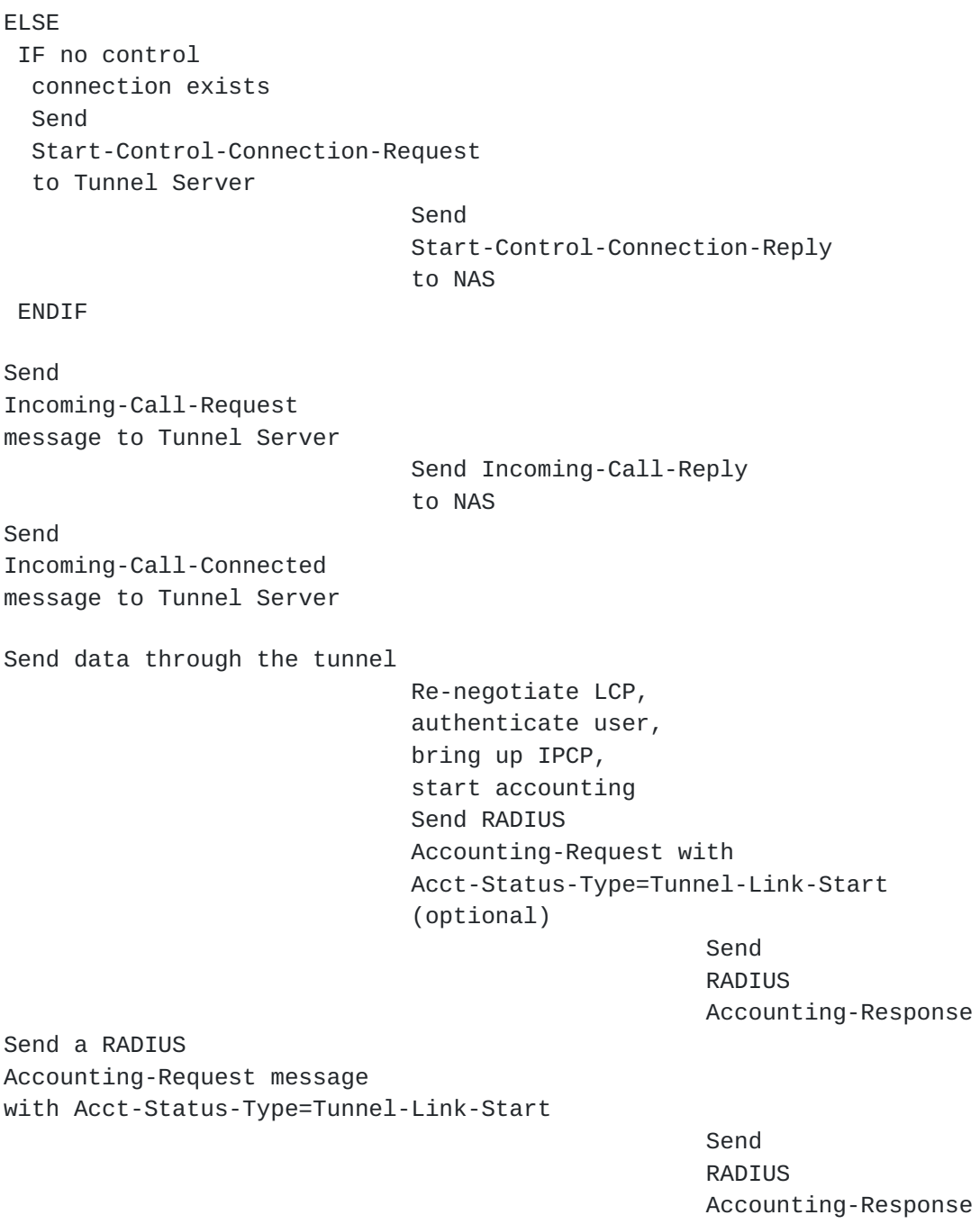
In performing the PPP authentication, the tunnel server can access its own user database, or alternatively can send a RADIUS Access-Request. The latter approach is useful in cases where authentication forwarding is enabled, such as with roaming or shared use networks. In this case, the RADIUS and tunnel servers are under the same administration and are typically located close together, possibly on the same LAN. Therefore having the tunnel server act as a RADIUS client provides for unified user administration. Note that the tunnel server's RADIUS Access-Request is typically sent directly to the local RADIUS server rather than being forwarded via a proxy.

After the tunnel has been brought up, the NAS and tunnel server will typically start accounting. In the case of the NAS, this is done by sending a RADIUS Accounting-Request packet with Acct-Status-Type=Tunnel-Start to a RADIUS server. When an individual call is brought up, a RADIUS Accounting-Request packet is sent with Acct-Status-Type=Tunnel-Link-Start. The tunnel server can produce its own accounting records, or it MAY send a RADIUS Accounting-Request packet to a local RADIUS server.

The interactions involved in initiation of a compulsory tunnel with telephone-number based authentication are summarized below. In order to simplify the diagram that follows, we have left out the client. However, it is understood that the client participates via PPP negotiation, authentication and subsequent data interchange with the Tunnel Server.




LCP starts
IF authentication
succeeds
Send ACK
ELSE Send NAK
IF NAK DISCONNECT



6.1.3.2. User-Name

Since authentication will occur only at the tunnel-server, tunnel initiation must occur prior to user authentication at the NAS. As a result, this scheme typically uses either the domain portion of the userID or attribute-specific processing on the RADIUS server. Since the user identity is never verified by the NAS, either the tunnel

server owner must be willing to be billed for all incoming calls, or other information such as the Calling-Station-Id must be used to verify the user's identity for accounting purposes.

In attribute-specific processing RADIUS may be employed and an attribute is used to signal tunnel initiation. For example, tunnel

attributes can be sent back if the User-Password attribute contains a dummy value (such as "tunnel" or "L2TP"). Alternatively, a userID beginning with a special character ('*') could be used to indicate the need to initiate a tunnel. When attribute-specific processing is used, the tunnel server may need to renegotiate LCP.

Another solution involves using the domain portion of the userID; all users in domain X would be tunneled to address Y. This proposal supports compulsory tunneling, but does not provide for user-based tunneling.

In order for the NAS to start accounting on the connection, it would need to use the identity claimed by the user in authenticating to the tunnel server, since it did not verify the identity via RADIUS. However, in order for that to be of any use in accounting, the tunnel endpoint needs to have an account relationship with the NAS owner. Thus even if a user has an account with the NAS owner, they cannot use this account for tunneling unless the tunnel endpoint also has a business relationship with the NAS owner. Thus this approach is incompatible with roaming.

A typical initiation sequence involving use of the domain portion of the userID looks like this:

```
Client and NAS: Call Connected
Client and NAS: PPP LCP negotiation
Client and NAS: Authentication
NAS to Tunnel Server: PPTP/L2TP Incoming-Call-Request
Tunnel Server to NAS: PPTP/L2TP Incoming-Call-Reply
NAS to Tunnel Server: PPTP/L2TP  Incoming-Call-Connected
Client and Tunnel Server: PPP LCP re-negotiation
Client and Tunnel Server: PPP authentication
Tunnel Server to RADIUS Server: RADIUS Access-request (optional)
RADIUS server to Tunnel Server: RADIUS Access-Accept/Access-Reject
Client and Tunnel Server: NCP negotiation
NAS to RADIUS Server: RADIUS Accounting-Request
  with Acct-Status-Type=Tunnel-Link-Start
RADIUS Server to NAS: RADIUS Accounting-Response
Tunnel Server to RADIUS Server: RADIUS Accounting-Request
   with Acct-Status-Type=Tunnel-Link-Start (Optional)
RADIUS Server to Tunnel Server: RADIUS Accounting-Response
```

The process begins with an incoming call to the NAS, and the PPP LCP negotiation between the Client and NAS. The authentication process will then begin and based on the domain portion of the userID, the NAS will now bring up a control connection if none existed before, and the NAS and tunnel server will bring up the call. At this point, data MAY begin to flow through the tunnel. The client and tunnel server MAY

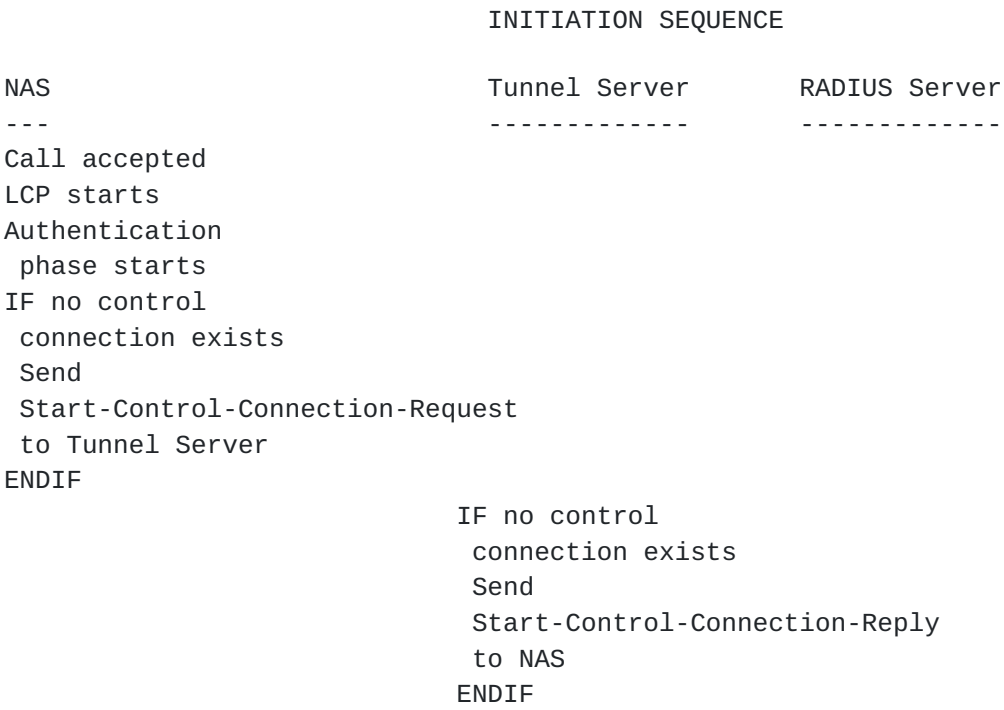
now renegotiate LCP and will complete PPP authentication.

At the time that the renegotiation begins, the NAS SHOULD NOT have sent an LCP CONFACK completing LCP negotiation, and the client and NAS MUST NOT have begun NCP negotiation. Rather than sending an LCP CONFACK, the NAS will instead send an LCP DOWN message. The Client MAY

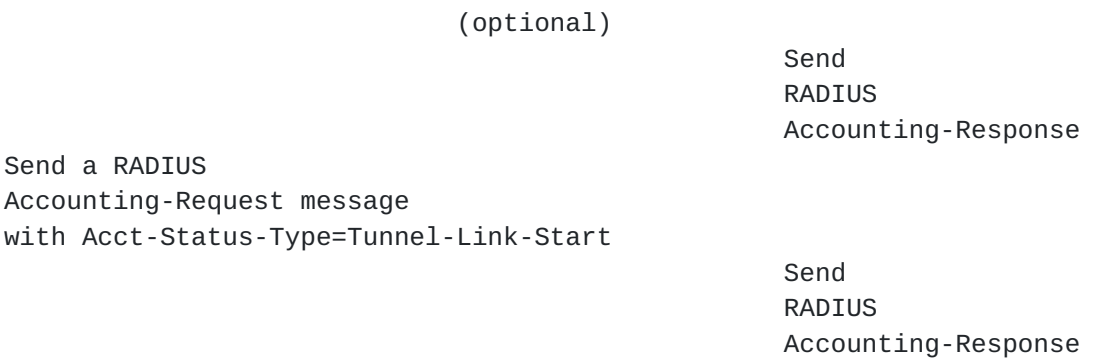
then renegotiate LCP, and from that point forward, all PPP packets originated from the client will be encapsulated and sent to the tunnel server. In single authentication compulsory tunneling, L2TP authentication forwarding MUST NOT be employed. When LCP re-negotiation has been concluded, the NCP phase will begin, and the tunnel server will assign an address to the client.

In performing the PPP authentication, the tunnel server can access its own user database, or it MAY send a RADIUS Access-Request. After the tunnel has been brought up, the NAS and tunnel server MAY start accounting.

The interactions are summarized below.



```
                    bring up IPCP,
                    start accounting
                    Send RADIUS
                    Accounting-Request with
                    Acct-Status-Type=Tunnel-Link-Start
```



6.2. Dual authentication

In this scheme, authentication occurs both at the NAS and the tunnel server. This requires the dial-up client to handle dual authentication, with attendant LCP re-negotiations. In order to allow the NAS and tunnel network server to authenticate against the same database, this requires RADIUS client capability on the tunnel network server, and possibly a RADIUS proxy on the NAS end.

Advantages of dual authentication include support for authentication and accounting at both ends of the tunnel; use of a single userID/password pair via implementation of RADIUS on the tunnel network server; no requirement for telephone-number based authentication, or attribute-specific processing on the RADIUS server.

Dual authentication allows for accounting records to be generated on both the NAS and tunnel server ends, making auditing possible. Also the tunnel endpoint does not need to have an account relationship with the NAS owner, making this approach compatible with roaming.

A disadvantage of dual authentication is that unless LCP forwarding is used, LCP will need to be renegotiated; some clients do not support it at all, and others only support only a subset of the dual authentication combinations. Feasible combinations include PAP/PAP(token), PAP/CHAP, PAP/EAP, CHAP/PAP(token), CHAP/CHAP, CHAP/EAP, EAP/CHAP, and EAP/EAP.

In the case of a dual authentication, a typical initiation sequence looks like this:

Client and NAS: PPP LCP negotiation
Client and NAS: PPP authentication
NAS to RADIUS Server: RADIUS Access-request
RADIUS server to NAS: RADIUS Access-Accept/Access-Reject
NAS to Tunnel Server: PPTP/L2TP Incoming-Call-Request
Tunnel Server to NAS: PPTP/L2TP Incoming-Call-Reply

NAS to Tunnel Server: PPTP/L2TP Incoming-Call-Connected
Client and Tunnel Server: PPP LCP re-negotiation (optional)
Client and Tunnel Server: PPP authentication
Tunnel Server to RADIUS Server: RADIUS Access-request (optional)
RADIUS server to Tunel Server: RADIUS Access-Accept/Access-Reject

```
Client and Tunnel Server: NCP negotiation
NAS to RADIUS Server: RADIUS Accounting-Request
  with Acct-Status-Type=Tunnel-Link-Start
RADIUS Server to NAS: RADIUS Accounting-Response
Tunnel Server to RADIUS Server: RADIUS Accounting-Request
   with Acct-Status-Type=Tunnel-Link-Start (Optional)
RADIUS Server to Tunnel Server: RADIUS Accounting-Response
```

The process begins with an incoming call to the NAS. The client and NAS then begin LCP negotiation. Subsequently the PPP authentication phase starts, and the NAS sends a RADIUS Access-Request message to the RADIUS server. If the authentication is successful, the RADIUS server responds with a RADIUS Access-Accept containing tunnel attributes.

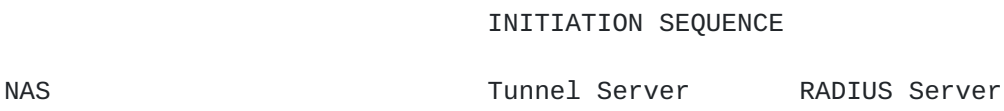
In the case where a PPTP/L2TP tunnel is indicated, the NAS will now bring up a control connection if none existed before, and the NAS and tunnel server will bring up the call. At this point, data MAY begin to flow through the tunnel. The client and tunnel server MAY now renegotiate LCP and go through another round of PPP authentication. At the time that this renegotiation begins, the NAS SHOULD NOT have sent an LCP CONFACK completing LCP negotiation, and the client and NAS MUST NOT have begun NCP negotiation. Rather than sending an LCP CONFACK, the NAS will instead send an LCP DOWN message. The Client MAY then renegotiate LCP, and from that point forward, all PPP packets originated from the client will be encapsulated and sent to the tunnel server. When LCP re-negotiation has been concluded, the NCP phase will begin, and the tunnel server will assign an address to the client.

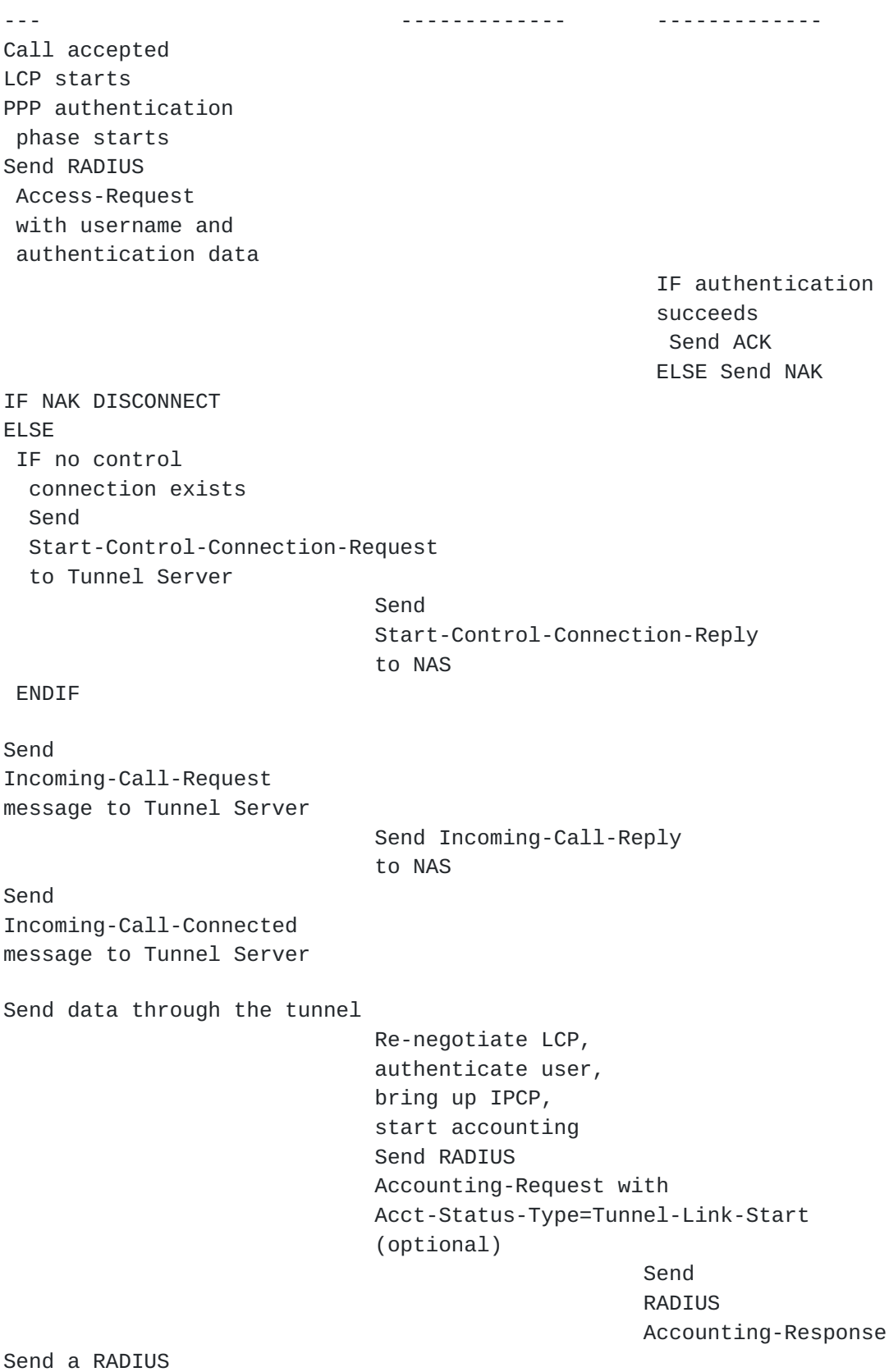
If L2TP is being used as the tunnel protocol, the NAS MAY in its initial setup notification include a copy of the LCP CONFACKs sent in each direction which completed LCP negotiation. The tunnel server MAY then use this information to avoid an additional LCP negotiation. With L2TP, the initial setup notification can also include the authentication information required to allow the tunnel server to authenticate the user and decide to accept or decline the connection. However, this facility creates a vulnerability to replay attacks, and can create problems in the case where the NAS and tunnel server authenticate against different RADIUS servers. As a result, where user-based tunneling via RADIUS is implemented, L2TP authentication forwarding SHOULD NOT be employed.

In performing the PPP authentication, the tunnel server can access its own user database, or it MAY send a RADIUS Access-Request. After the tunnel has been brought up, the NAS and tunnel server MAY start accounting.

The interactions involved in initiation of a compulsory tunnel with

dual authentication are summarized below.





Call accepted
LCP starts
PPP authentication
phase starts
Send RADIUS
Access-Request
with username and
authentication data
IF authentication
succeeds
Send ACK
ELSE Send NAK
IF NAK DISCONNECT
ELSE
IF no control
connection exists
Send
Start-Control-Connection-Request
to Tunnel Server
Send
Start-Control-Connection-Reply
to NAS
ENDIF
Send
Incoming-Call-Request
message to Tunnel Server
Send Incoming-Call-Reply
to NAS
Send
Incoming-Call-Connected
message to Tunnel Server
Send data through the tunnel
Re-negotiate LCP,
authenticate user,
bring up IPCP,
start accounting
Send RADIUS
Accounting-Request with
Acct-Status-Type=Tunnel-Link-Start
(optional)
Send
RADIUS
Accounting-Response
Send a RADIUS
Accounting-Request message

```
with Acct-Status-Type=Tunnel-Link-Start
                                                    Send
                                                    RADIUS
                                                    Accounting-Response

ENDIF
```

7. Termination sequence

The tear down of a compulsory tunnel involves an interaction between the client, NAS, Tunnel Server, and RADIUS Accounting server. This interaction is virtually identical regardless of whether telephone-number based authentication, single authentication, or dual authentication is being used. In any of the cases, the following events occur:

```
Tunnel Server to NAS: PPTP/L2TP Call-Clear-Request (optional)
NAS to Tunnel Server: PPTP/L2TP Call-Disconnect-Notify
NAS to RADIUS Server: RADIUS Accounting-Request
 with Acct-Status-Type=Tunnel-Link-Stop
RADIUS Server to NAS: RADIUS Accounting-Response
Tunnel Server to RADIUS Server: RADIUS Accounting-Request
   with Acct-Status-Type=Tunnel-Link-Stop (Optional)
RADIUS Server to Tunnel Server: RADIUS Accounting-Response
```

Tunnel termination can occur due to a client request (PPP termination), a tunnel server request (Call-Clear-Request), or a line problem (call disconnect).

In the case of a client-requested termination, the tunnel server MUST terminate the PPP session. The tunnel server MUST subsequently send a Call-Clear-Request to the NAS. The NAS MUST then send a Call-Disconnect-Notify message to the tunnel server, and will disconnect the call.

The NAS MUST also respond with a Call-Disconnect-Notify message and disconnection if it receives a Call-Clear-Request from the tunnel server without a client-requested termination.

In the case of a line problem or user hangup, the NAS MUST send a Call-Disconnect-Notify to the tunnel server. Both sides will then tear down the call.

After call tear down is complete, if RADIUS accounting is being used then the NAS MUST send a RADIUS Accounting-Request with Acct-Status-Type=Tunnel-Link-Stop packet to a RADIUS accounting server.

The tunnel server MAY produce its own accounting records, or it MAY use RADIUS accounting. If RADIUS accounting is being used then the tunnel server MUST send a RADIUS Accounting-Request with Acct-Status-Type=Tunnel-Link-Stop to a RADIUS accounting server.

The interactions involved in termination of a compulsory tunnel are summarized below. In order to simplify the diagram that follows, we have left out the client. However, it is understood that the client MAY participate via PPP termination and disconnection.

TERMINATION SEQUENCE

NAS Tunnel Server RADIUS Server

```
---                          -------------        -------------
IF user disconnected
 send
 Call-Disconnect-Notify
 message to tunnel server
                             Tear down the call
                             stop accounting
                             Send RADIUS
                             Accounting-Request with
                             Acct-Status-Type=Tunnel-Link-Stop
                             (optional)
                                                  Send RADIUS
                                                  Accounting-Response
ELSE IF client requests
 termination
                             send
                             Call-Clear-Request
                             to the NAS
 Send
 Call-Disconnect-Notify
 message to tunnel server
 Disconnect the user
                             Tear down the call
                             stop accounting
                             Send RADIUS
                             Accounting-Request with
                             Acct-Status-Type=Tunnel-Link-Stop
                             (optional)
                                                  Send RADIUS
                                                  Accounting-Response

 Send a RADIUS
 Accounting-Request message
 with Acct-Status-Type=Tunnel-Link-Stop
                                                  Send RADIUS
                                                  Accounting-Response

ENDIF
```

8. Use of distinct RADIUS servers

In the case that the NAS and the tunnel server are using distinct RADIUS servers, some interesting cases can arise in the provisioning of compulsory tunnels.

8.1. Distinct userIDs

If distinct RADIUS servers are being used, it is likely that distinct userID/password pairs will be required to complete the RADIUS and tunnel authentications. One pair will be used in the initial PPP authentication with the NAS, and the second pair will be used for authentication at the tunnel server.

However, in order to provide maximum ease of use in the case where the userID/password pairs are identical, tunnel clients typically attempt authentication with the same userID/password pair as was used in the initial PPP negotiation. Only after this fails do they prompt the user for the second pair.

In this case, tunnel client implementations SHOULD take care not to put up error messages indicating a bad password. Instead a dialog SHOULD be presented requesting the tunnel userID/password combination.

In the case where token cards are being used for both authentications, the tunnel client MUST NOT attempt to present the token used in the first authentication during the second authentication, since these will never be identical. Instead the user SHOULD be prompted to enter the second token.

The same issue arises in L2TP if the NAS attempts to forward authentication information to the tunnel server in the initial setup notification. Since the userID/password pair used for tunnel authentication is different from that used to authenticate against the NAS, forwarding authentication information in this manner will cause the tunnel authentication to fail. As a result, where user-based tunneling via RADIUS is implemented, L2TP authentication forwarding SHOULD NOT be employed.

8.2. Multilink PPP issues

It is possible for the two RADIUS servers to return different Port-Limit attributes. For example, it is conceivable that the NAS RADIUS server will only grant use of a single channel, while the tunnel RADIUS server will grant more than one channel. In this case, the correct behavior is for the tunnel client to open a connection to another NAS in order to bring up a multilink bundle on the tunnel server. The client MUST NOT indicate to the NAS that this additional link is being brought up as part of a multilink bundle; this will only be indicated in the subsequent negotiation with the tunnel server.

It is also conceivable that the NAS RADIUS server will allow the client to bring up multiple channels, but that the tunnel RADIUS server will allow fewer channels than the NAS RADIUS server. In this case, the client should terminate use of the excess channels.

9. UserID Issues

In the provisioning of roaming and shared use networks, one of the requirements is to be able to route the authentication request to the user's home RADIUS server. This authentication routing is accomplished

based on the userID submitted by the user to the NAS in the initial PPP authentication. The userID is subsequently relayed by the NAS to the RADIUS server in the User-Name attribute, as part of the RADIUS Access-Request.

Similarly, references [5] and [6] refer to use of the userID in determining the tunnel endpoint. However, since none of these references provide guidelines for how RADIUS or tunnel routing is to be accomplished, the possibility of conflicting interpretations exists.

9.1. UserID convergence in user-based tunneling

The use of RADIUS in provisioning of compulsory tunneling relieves the userID from having to do double duty. Rather than being used both for routing of the RADIUS authentication/authorization request as well for determination of the tunnel endpoint, the userID is now used solely for routing of RADIUS authentication/authorization requests. Tunnel attributes returned in the RADIUS Access-Response are then used to determine the tunnel endpoint.

Since the framework described in this document allows both ISPs and tunnel users to authenticate users as well as to account for resources consumed by them, and provides for maintenance of two distinct userID/password pairs, this scheme provides a high degree of flexibility. Where RADIUS proxies and tunneling are employed, it is possible to allow the user to authenticate with a single userID/password pair at both the NAS and the tunnel endpoint. This is accomplished by routing the NAS RADIUS Access-Request to the same RADIUS server used by the tunnel server.

As described in [8], the recommended form for the user ID is userID@realm, i.e. fred@bigco.com.

10. Security considerations

In compulsory tunneling, PAP authentication SHOULD NOT be used, since this will typically involve transmission of a cleartext password over the Internet. A possible exception is where PAP is used to support a one time password or token.

Where RADIUS proxies are deployed, the Access-Reply sent by the RADIUS server may be processed by one or more proxies prior to being received by the NAS. In order to ensure that tunnel attributes arrive without modification, intermediate RADIUS proxies forwarding the Access-Reply MUST NOT modify tunnel attributes. If the RADIUS proxy does not support tunnel attributes, then it MUST send an Access-Reject to the NAS. This is necessary to ensure that the user is only granted access if the services requested by the RADIUS server can be provided.

Since RADIUS tunnel attributes are used for compulsory tunneling, address assignment is handled by the tunnel server rather than the NAS. As a result, if tunnel attributes are present, the NAS MUST

ignore any address assignment attributes sent by the RADIUS server. In addition, the NAS and client MUST NOT begin NCP negotiation, since this could create a time window in which the client will be capable of sending packets to the transport network, which is not permitted in compulsory tunneling.

11. Acknowledgements

Thanks to Gurdeep Singh Pall of Microsoft for many useful discussions of this problem space, and to Allan Rubens of Ascend and Bertrand Buclin of AT&T Labs Europe for his comments on this document.

12. References

[1] B. Aboba, J. Lu, J. Alsop, J. Ding, W. Wang. "Review of Roaming Implementations." RFC 2194, Microsoft, Aimnet, i-Pass Alliance, Asiainfo, Merit, September 1997.

[2] B. Aboba, G. Zorn. "Dialup Roaming Requirements." Internet draft (work in progress), draft-ietf-roamops-roamreq-09.txt, Microsoft, March 1998.

[3] C. Rigney, A. Rubens, W. Simpson, S. Willens. "Remote Authentication Dial In User Service (RADIUS)." RFC 2138, Livingston, Merit, Daydreamer, April 1997.

[4] C. Rigney. "RADIUS Accounting." RFC 2139, Livingston, April 1997.

[5] A. Valencia, K. Hamzeh, A. Rubens, T. Kolar, M. Littlewood, W. Townsley, J. Taarud, G. Pall, B. Palter, W. Verthein. "Layer Two Tunneling Protocol L2TP." Internet draft (work in progress), draft-ietf-pppext-l2tp-10.txt, Ascend Communications, Microsoft, Copper Mountain Networks, U.S. Robotics, March 1998.

[6] K. Hamzeh, G. S. Pall, J. Taarud, W. Verthein, W. A. Little. "Point-to-Point Tunneling Protocol -- PPTP." ." Internet draft (work in progress), draft-ietf-pppext-pptp-02.txt, Ascend Communications, Microsoft, Copper Mountain Networks, U.S. Robotics, September 1997.

[7] G. Zorn, D. Leifer, A. Rubens, J. Shriver. "RADIUS Attributes for Tunnel Protocol Support." Internet draft (work in progress), draft-ietf-radius-tunnel-auth-05.txt, Microsoft, Ascend Communications, Shiva Corporation, April 1998.

[8] B. Aboba, M. A. Beadles. "The Network Access Identifier." Internet draft (work in progress), draft-ietf-roamops-nai-10.txt, Microsoft, CompuServe, March 1998.

[9] S. Bradner. "Key words for use in RFCs to Indicate Requirement Levels." RFC 2119, Harvard University, March, 1997.

[10] C. Rigney, W. Willats. "RADIUS Extensions." Work in progress, draft-ietf-radius-ext-01.txt, Livingston, June, 1997.

[11] P. Calhoun, A.C. Rubens, B. Aboba. "Extensible Authentication Protocol Support in RADIUS." Internet draft (work in progress), draft-ietf-radius-eap-05.txt, Sun Microsystems., Merit Network, Microsoft, May, 1998.

[12] L. Blunk, J. Vollbrecht. "PPP Extensible Authentication Protocol (EAP)." RFC 2284, Merit Network, Inc., March 1998.

[13] G. Zorn, D. Mitton. "RADIUS Accounting Modifications for Tunnel Protocol Support." Internet draft (work in progress), draft-ietf-radius-tunnel-acct-00.txt, Microsoft, Bay Networks, November 1997.

13. Chair's Address

The RADIUS Working Group can be contacted via the current chair:

Carl Rigney
Livingston Enterprises
4464 Willow Road
Pleasanton, California 94588

Phone: +1 510 426 0770
E-Mail: cdr@livingston.com

14. Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 425 936 6605
EMail: bernarda@microsoft.com

Glen Zorn
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 425 703 1559
EMail: glennz@microsoft.com