RADIUS Attributes for Tunnel Protocol Support

1. Status of this Memo

This document is an Internet-Draft. 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."

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ds.internic.net (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

The distribution of this memo is unlimited. It is filed as <draft-ietf-radius-tunnel-auth-00.txt>, and expires May 1, 1997. Please send comments to the author.

2. Abstract

This document specifies a set of RADIUS attributes designed to support the provision of mandatory tunneling in dial-up networks. RADIUS attributes for both authorization and accounting are specified.

3. Introduction

Many of the most interesting applications of tunneling protocols such as PPTP [PPTP] and L2TP [L2TP] involve dial-up network access. Some, such as the provision 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, potentially more compelling, applications involve compulsory tunneling: the tunnel is created automatically, without any action from the user and more importantly, without allowing the user any choice in the matter. 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 virtually 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 being subject to manual configuration. 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 server; this document defines those attributes.

4. Attributes

4.1. Tunnel-Type

Description

This Attribute indicates the tunneling protocol to be used. It MAY be used in both Access-Request and Access-Accept packets. A NAS is not required to implement all of these tunnel types, and MUST treat unknown or unsupported Tunnel-Types as though an Access-Reject had been received instead.

A summary of the Tunnel-Type Attribute format is shown below. The fields are transmitted from left to right.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |             Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
Value (cont)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

64 for Tunnel-Type

Length

6

Value

The Value field is four octets.

1 PPTP
4.2. Tunnel-Medium-Type

Description

The Tunnel-Medium-Type Attribute indicates which transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports.

A summary of the Tunnel-Medium-Type Attribute format is given below. The fields are transmitted left to right.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>65</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

Type

65 for Tunnel-Medium-Type

Length

6

Value

The Value field is four octets.

1  IP
2  X.25
3  ATM
4  Frame Relay

4.3. Tunnel-Client-Endpoint

Description

This Attribute indicates the address of the NAS end of the tunnel.

A summary of the Tunnel-Client-Endpoint Attribute format is shown below. The fields are transmitted from left to right.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
+++---------------------------------+---------------------------------+---------------------------------+
|     Type      |    Length     |  String ... |
+++---------------------------------+---------------------------------+---------------------------------+

Type

66 for Tunnel-Client-Endpoint.

Length

>= 3

String
The format of the address represented by the String field depends upon the value of the Tunnel-Medium-Type attribute. This attribute, along with the Tunnel-Server-Endpoint and Tunnel-ID attributes, may be used to provide a globally unique means to identify a tunnel for accounting purposes.

4.4. Tunnel-Server-Endpoint

Description

This Attribute indicates the address of the server end of the tunnel.

A summary of the Tunnel-Server-Endpoint Attribute format is shown below. The fields are transmitted from left to right.

<table>
<thead>
<tr>
<th>1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td>
</tr>
<tr>
<td>--------------------------------------------</td>
</tr>
</tbody>
</table>

+++---------------------------------+---------------------------------+---------------------------------+
|     Type      |    Length     |  String ... |
+++---------------------------------+---------------------------------+---------------------------------+

Type

67 for Tunnel-Server-Endpoint.

Length

>= 3

String
The format of the address represented by the String field depends upon the value of the Tunnel-Medium-Type attribute. This attribute, along with the Tunnel-Client-Endpoint and Tunnel-ID attributes, may be used to provide a globally unique means to identify a tunnel for accounting purposes.
4.5.  Connection-Identifier

Description

This Attribute indicates the identifier assigned to the call.

A summary of the Connection-Identifier Attribute format is shown below. The fields are transmitted from left to right.

| Type | Length | String ...
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>68</td>
<td>&gt;= 3</td>
<td></td>
</tr>
</tbody>
</table>

Type

68 for Connection-Identifier

Length

>= 3

String

The format of the identifier represented by the String field depends upon the value of the Tunnel-Type attribute. This attribute, along with the Tunnel-Client-Endpoint and Tunnel-Server-Endpoint attributes, may be used to provide a globally unique means to identify a call for accounting purposes.

5.  Acknowledgements

Thanks to Gurdeep Singh Pall and Bernard Aboba of Microsoft Corporation, Andy Valencia of cisco Systems, and Kory Hamzeh of Ascend Communications for salient input and review.

6.  Author’s Address

Glen Zorn
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: 206-703-1559
EMail: glennz@microsoft.com