Network Working Group
Internet-Draft
Expires: April 26, 2006

J. Heinanen
TutPro Inc.
G. Weber, Ed.
W. Townsley
S. Booth
W. Luo
Cisco Systems
October 23, 2005

Using RADIUS for PE-Based VPN Discovery
draft-ietf-l2vpn-radius-pe-discovery-02.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a strategy by which Provider Equipment (PE) can be dynamically provisioned for inclusion in PE-based Layer 2 Virtual Private Networks (L2VPNs). This layered strategy utilizes the Remote Authentication Dial In User Service (RADIUS) protocol as a

centralized control mechanism and can be used in conjunction with other proposed mechanisms. The mechanisms described in this document enhance those established by RFC 2868 and conform to those described by the L2VPN Framework.

Table of Contents

1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

This document uses terminology from [I-D.ietf-l2vpn-l2-framework] and [I-D.ietf-l2vpn-signaling].

2. Acronyms

AII: Attachment Individual Identifier
AC: Attachment Circuit
AGI: Attachment Group Identifier
AS: Autonomous System
CE: Customer Equipment
L2VPN: Layer 2 Provider Provisioned Virtual Private Network
NAI: Network Access Identifier
NAS: Network Access Server
PE: Provider Equipment
SAI: Source Attachment Identifier
SAII: Source Attachment Individual Identifier
RADIUS: Remote Authentication Dial In User Service
TAI: Target Attachment Identifier
TAII: Target Attachment Individual Identifier
VPLS: Virtual Private LAN Service
VPN: Virtual Private Network
VPWS: Virtual Private Wire Service

3. Introduction

This document describes how in PE-based VPNs a PE of a VPN can use RADIUS [RFC2865] to authenticate its CEs and discover the other PEs of the VPN. In RADIUS terms, the CEs are users and the PEs are Network Access Servers (NAS) implementing RADIUS client functionality.

A VPN can span multiple Autonomous Systems (AS) and multiple providers. Each PE, however, only needs to be a RADIUS client to a RADIUS server of the "local" provider. In the case in which a CE belongs to a "foreign" VPN, the RADIUS server of the local provider acts as a proxy client to RADIUS of the foreign provider.

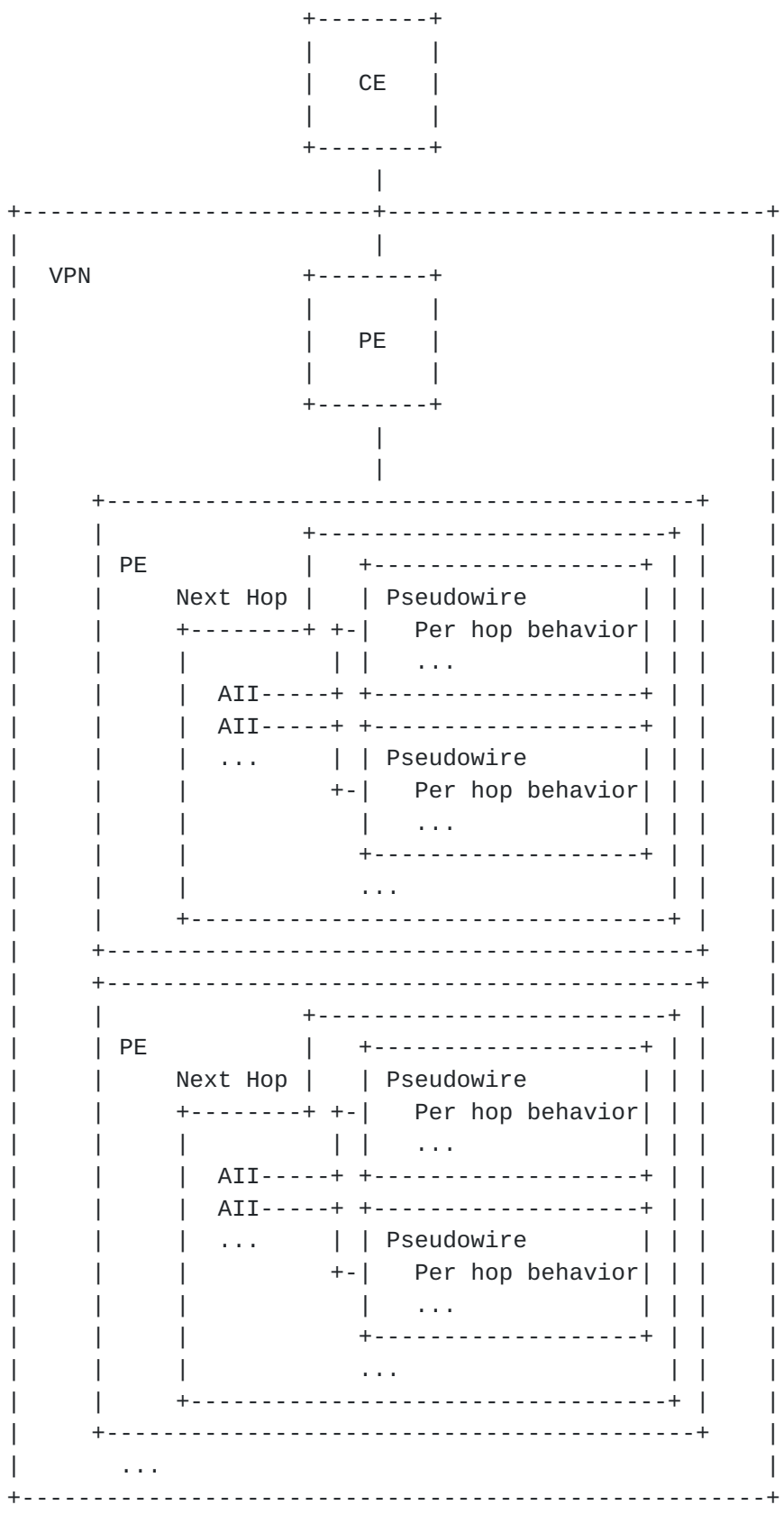
4. Information Model

This document presents a model wherein authorization for participation in a PE-based VPN can be divided into three different layers of access.

- CE or AC Authorization
- VPN Authorization
- Pseudowire Authorization

The first layer is AC authorization, in which a first sign of life on a particular AC triggers an authorization resulting in provisioning information particular to the circuit in question. Once the AC is authorized, its VPN membership is authorized separately. This authorization step may result in a number of pseudowire specific connections; each of which may be authorized separately. The relationships between these three data representations are shown in the diagram below.

Using a layered approach allows the different stages of authorization to be satisfied by separate means based on deployment scenario. It also allows one model to apply to various deployment architectures including VPLS and VPWS. If all three authorization stages are accommodated by a RADIUS server, the stages may be combined into a single transaction instead of having three separate transactions.


CE
VPN
PE
PE
Next Hop
Pseudowire
Per hop behavior
...
AII-----+
AII-----+
...
Pseudowire
Per hop behavior
...
PE
Next Hop
Pseudowire
Per hop behavior
...
AII-----+
AII-----+
...
Pseudowire
Per hop behavior
...

- Each pseudowire may have its own per-hop behavior and arbitrary configuration information
- Each pseudowire is associated with an AII
- Each PE includes an arbitrary number of AIIs
- Each PE has one associated next hop address
- The VPN includes an arbitrary number of PEs

The following two sections define how the components of this data model may be represented as RADIUS attributes so the components of this information model may be communicated from a centralized location out into the network elements.

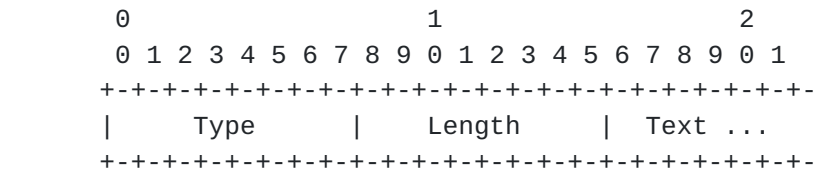
5. New RADIUS Attributes

This document defines several new RADIUS Attributes which are described in detail in this section.

5.1. Router-Distinguisher

This attribute represents a Router Distinguisher as described in [I-D.ietf-l3vpn-rfc2547bis]. It MAY be included in an Access-Request message. This attribute MUST NOT be included in Access-Request messages that also include a "VPN-ID" attribute.

A summary of the Router-Distinguisher attribute format is shown below. The fields are transmitted from left to right.



Type

(TBA) for Router-Distinguisher.

Length

>= 7

Text

The Text field is composed of three colon separated parts: a type, an administrator, and an assigned number.

Where the type is "0", the administrator contains a 16-bit Autonomous

System Number (ASN), and the assigned number is a 32-bit value assigned by enterprise responsible for the ASN, e.g. "0:114:23".

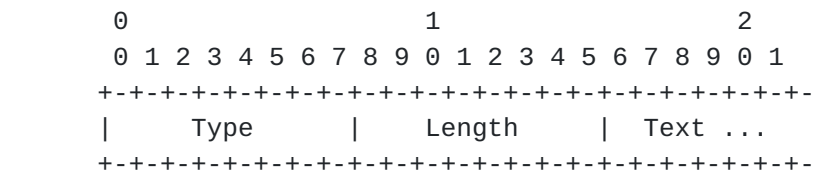
Where the type is "1", the administrator contains an IP address, and the assigned number is a 16-bit value assigned by the enterprise controlling the IP address space, e.g. "1:1.2.3.4:10001".

Where the type is "2", the administrator contains a 32-bit ASN, and the assigned number is a 16-bit value assigned by the enterprise responsible for the ASN, e.g. "2:70000:216".

5.2. VPN-ID

This attribute represents a VPN-ID as described in [RFC2685]. It MAY be included in an Access-Request message. This attribute MUST NOT be included in Access-Request messages that also include a Router-Distinguisher attribute.

A summary of the VPN-ID attribute format is shown below. The fields are transmitted from left to right.



Type

(TBA) for VPN-ID.

Length

>= 5

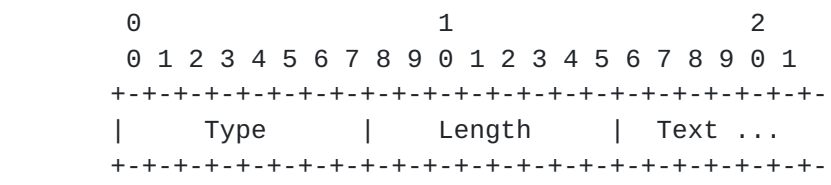
Text

The Text field is composed of two colon separated parts: a VPN authority Organizationally Unique Identifier, and a VPN index, e.g. "101:14".

5.3. Attachment-Individual-ID

This attribute indicates a Attachment-Individual-ID as described in [I-D.ietf-l2vpn-signaling].

A summary of the Attachment-Individual-ID attribute format is shown below. The fields are transmitted from left to right.



Type

(TBA) for Attachment-Individual-ID.

Length

>= 3

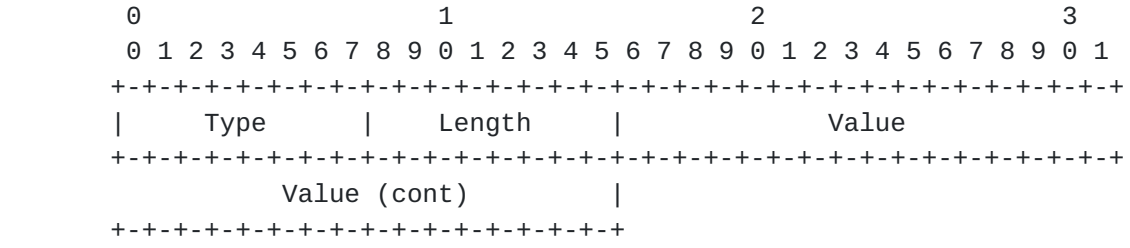
Text

The Text field is an encoding of the Source Attachment Individual Identifier, e.g. "2".

5.4. Per-Hop-Behavior

This attribute indicates a Per-Hop-Behavior as described in [RFC3140].

A summary of the Per-Hop-Behavior attribute format is shown below. The fields are transmitted from left to right.



Type

(TBA) for Per-Hop-Behavior.

Length

6

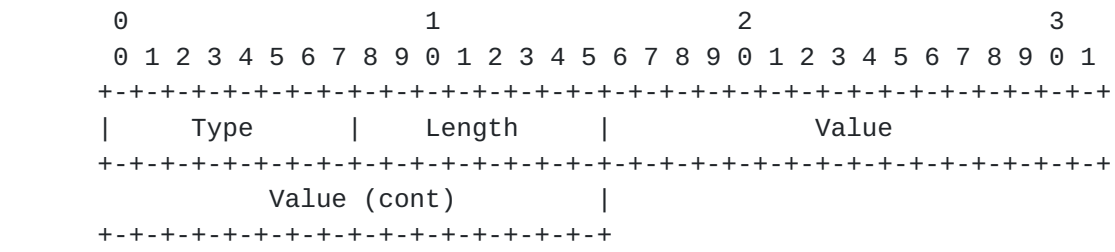
Integer

The lower 16-bits of the value contains the Per-Hop-Behavior value as described in [RFC3140].

5.5. PE-Router-ID

This attribute typically indicates an IPv4 address for a particular PE member of a VPN, though it may be some arbitrary value assigned by the owner of the ID space.

A summary of the PE-Router-ID attribute format is shown below. The fields are transmitted from left to right.



Type

(TBA) for PE-Router-ID.

Length

6

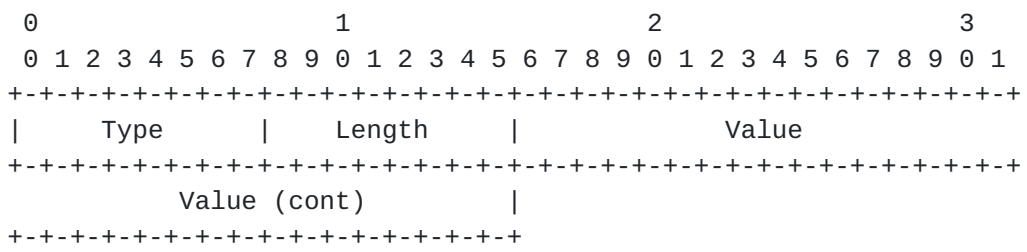
Address

Typically, the value indicates the IPv4 address of a particular PE member of a VPN.

5.6. PE-Address

This attribute indicates an IPv4 address for a particular PE member of a VPN. In relation to the PE for which a CE is joining the VPN, this would be the initial's PE's next hop address.

A summary of the PE-Address attribute format is shown below. The fields are transmitted from left to right.



Type

(TBA) for PE-Address.

Length

6

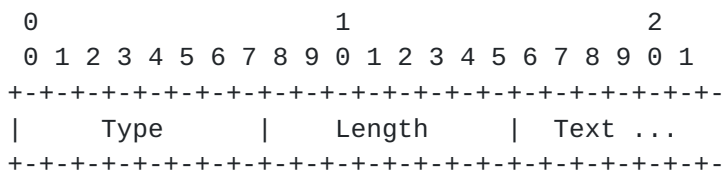
Address

The value indicates the IPv4 address of a particular PE member of a VPN.

5.7. PE-Record

This attribute represents a single element within a particular PE's description. A group of PE-Records combine to form a complete PE description when returned during VPN authorization.

A summary of the PE-Record attribute format is shown below. The fields are transmitted from left to right.



Type

(TBA) for PE-Record.

Length

>= 8

Text

The Text field contains an AII prefixed by a PE-Router-ID and separated by a colon, e.g. "1.1.1.1:14" where the PE-Router-ID is

1.1.1.1 and the AII is 14. This represents a particular pseudowire. The value is optionally suffixed by a colon separated list of attribute value pairs containing pseudowire-specific configuration, e.g. "1.1.1.1:14:PHB=256".

6. New Values for Existing RADIUS Attributes

6.1. Service-Type

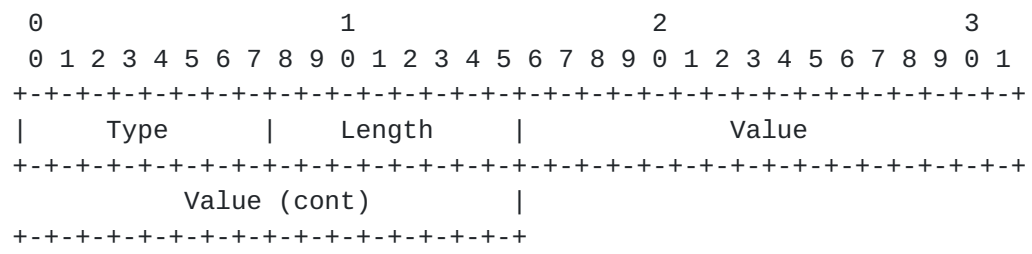
This document defines one new value for an existing RADIUS attribute. The Service-Type attribute is defined in Section 5.6 of RFC 2865 [RFC2865], as follows:

This Attribute indicates the type of service the user has requested, or the type of service to be provided. It MAY be used in both Access-Request and Access-Accept packets.

A NAS is not required to implement all of these service types, and MUST treat unknown or unsupported Service-Types as though an Access-Reject had been received instead.

A summary of the Service-Type Attribute format is shown below.

The fields are transmitted from left to right.



Type

6 for Service-Type.

Length

6

Value

The Value field is four octets.

This document defines one new value for the Service-Type attribute.

(TBA) L2VPN

The semantics of the L2VPN service are as follows:

L2VPN A CE is requesting to join a VPN.

6.2. User-Name

This attribute defined by [RFC2865] takes a value depending on which layer of VPN authorization is occurring.

- For CE/AC authorization, the User-Name value contains either a Network Access Identifier (NAI) associated with the CE [RFC2486], or an implementation dependent AC name.
- For VPN authorization, the User-Name value contains the VPN-ID or a Router-Distinguisher.
- For pseudowire authorization, the User-Name value contains a PE-Router-ID.

7. Table of Attributes

The following tables provide a guide to which attributes may be found in which kinds of packets, and in what quantity.

CE/AC Authorization

Request	Accept	Reject	Challenge	#	Attribute
0	0-1	0	0	TBA	Router-Distinguisher
0	0-1	0	0	TBA	VPN-ID

VPN Authorization

Request	Accept	Reject	Challenge	#	Attribute
0-1	0	0	0	TBA	Router-Distinguisher
0-1	0	0	0	TBA	VPN-ID
0	0+	0	0	TBA	Attachment-Individual-ID
0	0-1	0	0	TBA	Per-Hop-Behavior
0	0-1	0	0	TBA	PE-Router-ID
0	0-1	0	0	TBA	PE-Address
0	0+	0	0	TBA	PE-Record

Pseudowire Authorization
VPN Authorization

Request	Accept	Reject	Challenge	#	Attribute
0-1	0	0	0	TBA	Router-Distinguisher
0-1	0	0	0	TBA	VPN-ID
1	0	0	0	TBA	Attachment-Individual-ID
0	0-1	0	0	TBA	Per-Hop-Behavior

The following table defines the meaning of the above table entries.

0	This attribute MUST NOT be present in a packet.
0+	Zero or more instances of this attribute MAY be present in a packet.
0-1	Zero or one instance of this attribute MAY be present in a packet.
1	Exactly one instance of this attribute MUST be present in a packet.

8. Examples

CE/AC Authorization

```
  Request
    User-Name = "providerX/atlanta@vpnY.domainZ.net" (CE NAI)
    NAS-IP-Address = "1.1.1.1"
  Response
    VPN-ID = "100:14"

  Request
    User-Name = "ATM14.0.1" (AC Name)
    NAS-IP-Address = "1.1.1.1"
  Response
    Router-Distinguisher = "1:1.2.3.4:10001"
```

VPN Authorization

```
  Request
    User-Name = "100:14"  (VPN-ID)
    NAS-IP-Address = "1.1.1.1"
  Response
    PE-Record = "2.2.2.2:14"  (PE-Router-ID:AII)
    PE-Record = "2.2.2.2:15"
    PE-Record = "3.3.3.3:24"
    PE-Record = "3.3.3.3:25"

  Request
    User-Name = "100:14"  (VPN-ID)
    NAS-IP-Address = "1.1.1.1"
  Response
    PE-Record = "2.2.2.2:14:PHB=256"
```

Pseudowire Authorization

```
  Request
    User-Name = "2.2.2.2" (PE-Router-ID)
    NAS-IP-Address = "1.1.1.1"
    Attachment-Individual-ID = "14"
    VPN-ID = "100:14"
  Response
    Per-Hop-Behavior = "256"
```

9. Security Considerations

[TBD]

10. IANA Considerations

[TBD]

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC2868] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

[RFC2685] Fox, B. and B. Gleeson, "Virtual Private Networks Identifier", RFC 2685, September 1999.

11.2. Informative References

[I-D.ietf-l2vpn-signaling] Rosen, E., "Provisioning, Autodiscovery, and Signaling in L2VPNs", draft-ietf-l2vpn-signaling-06 (work in progress), September 2005.

[I-D.ietf-pwe3-control-protocol] Martini, L., "Pseudowire Setup and Maintenance using the Label Distribution Protocol", draft-ietf-pwe3-control-protocol-17 (work in progress), June 2005.

[I-D.ietf-l3vpn-rfc2547bis] Rosen, E., "BGP/MPLS IP VPNs", draft-ietf-l3vpn-rfc2547bis-03 (work in progress), October 2004.

[RFC2279] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.

[I-D.ietf-l2vpn-l2-framework] Andersson, L. and E. Rosen, "Framework for Layer 2 Virtual Private Networks (L2VPNs)", draft-ietf-l2vpn-l2-framework-05 (work in progress),

June 2004.

[RFC2486] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC 2486, January 1999.

[RFC3140] Black, D., Brim, S., Carpenter, B., and F. Le Faucheur, "Per Hop Behavior Identification Codes", RFC 3140, June 2001.

Authors' Addresses

Juha Heinanen
TutPro Inc.
Utsjoki
Finland

Email: jh@tutpro.com

Greg Weber (editor)
Cisco Systems
10850 Murdock Road
Knoxville, TN 37932
US

Email: gdweber@cisco.com

W. Mark Townsley
Cisco Systems
7025 Kit Creek Road
Research Triangle Park, NC 27709
US

Email: mark@townsley.net

Skip Booth
Cisco Systems
7025 Kit Creek Road
Research Triangle Park, NC 27709
US

Email: ebooth@cisco.com

Wei Luo
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134
US

Email: luo@cisco.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.