Network Working Group
INTERNET DRAFT
Category: Informational
Expires: April 13, 2004

Farid Adrangi (Ed.)
Intel Corporation
October 14, 2003

RADIUS Extension for Public Wireless LAN
draft-adrangi-radius-extension-for-pwlan-00.txt

Status of this Memo

Abstract

This document describes additional Remote Authentication Dial In User Service (RADIUS) [1] attributes for use of RADIUS AAA (Authentication, Authorization, Accounting) in Public Wireless Local Area Network (PWLAN) deployments. Some of these attributes are already implemented as Vendor Specific Attributes (VSA) in networks today, but are core to PWLAN interoperability and roaming.

Internet Draft RADIUS Attribute Extension for PWLAN 14 October 2003

Table of Contents

1. Introduction.....2
1.2 Applicability.....2
1.3 Requirements language.....3
1.4 Terminology.....3
2. Operation.....3
2.1 RADIUS Support for PWLAN Location Information.....3
2.2 RADIUS Support for Advertising Application-based capabilities..5
2.3 RADIUS Support for Specifying a Mobile IP Home Agent.....7
2.4 RADIUS Support for Specifying DNS Server.....9
2.5 RADIUS Support for Specifying Remote IP Addresses.....10
2.6 RADIUS Support for Specifying IP Address Type Options.....11
2.7 RADIUS Support for Specifying Network Capabilities.....13
4. IANA Considerations.....16
5. Security Considerations.....16
6. Contributors.....17
7. Acknowledgements.....17
8. References.....17
AuthorsÆ Addresses.....18

1. Introduction

Wireless LAN (WLAN) Access Networks (AN) are being deployed in public places such as airports, hotels, shopping malls, and coffee shops by a diverse set of incumbent operators like cellular carriers (GSM and CDMA), Wireless Internet Service Providers (WISP), and fixed broadband operators.

Remote Access Dial In User Service (RADIUS) [1],[2],[3] is the dominant Authentication, Authorization, and Accounting (AAA) protocol in use across broadband networks globally and consequently will be heavily reused in Public WLAN (PWLAN) deployments.

This document describes a number of additional attributes that are needed to enable use of RADIUS AAA in PWLANs in an interoperable manner. Attributes described in this document includes some of Vendor Specific Attributes (VSA) that are recommended by various

standard bodies (such as 3GPP, 3GPP2, GSMA) for PWLAN interworking. Common understanding and Standardization of these attributes is essential to enable improved interoperability and hence successful deployments of PWLANs.

1.2 Applicability

Although proposed attributes in this draft are intended for PWLAN deployments, they can also be used in other networks (e.g., wired networks).

1.3 Requirements language

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

1.4 Terminology

Access Network (AN)
: The PWLAN hotspot network that provides wireless connectivity to the Internet for WLAN clients (or stations) present in the local access area. This MAY be in a separate security and routing domain with respect to the Home Service Network or a Mediating Network.

Home Service Network (HSN)
: The network providing the service and therefore maintaining the direct relationship to the user/subscriber of the WLAN service. All AAA functions are ultimately performed by the HSN.

Access Point (AP)
: ôA station that provides access to the distribution services via the wireless medium for associated Stations.ö

RADIUS server
: ôThis is a server which provides for

authentication/authorization via the protocol described in [1], and for accounting as described in [6].ö It is deployed in the PWLAN AN, MN, and HSN.

2. Operation

Operation is identical to that defined in [1] and [2].

2.1 RADIUS Support for PWLAN Location Information

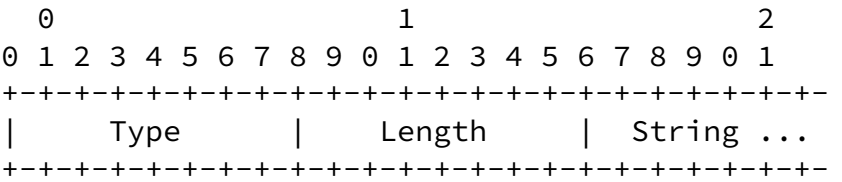
Rationale

When a PWLAN client connects to a PWLAN AN, the information pertaining to the PWLAN AN location and operational ownership needs to be conveyed to the HSN for accounting and services management purposes. This information contains the AN operator name and the AN location information such as Location Name, Location Type, City, State, and Country. This information enables use case scenarios for location aware billing, location aware subscriber authentication / authorization in roaming, and location aware services.

Attribute

This attribute describes information pertaining to a PWLAN AN location and operational ownership. It MUST be sent in Access-Request, and Accounting-Request records where the Acc-Status-Type is set to Start or Stop if available.

A summary of the AN Location and Operational-Ownership Information Attribute is shown below.



Name

Access Network Location Information

Type

To be assigned by IANA

Length

>= 3

String

The string field is one or more octets, and it is structured as a set of comma-separated field names and values according to the following ABNF [5].

```
Attribute Value = string [ %d0 location-info ]
string = *CHAR

location-info = item ["," item ]
item = field-name "=" value

field-name = 1*( ALPHA / "-" / "_" / ô:ö / DIGIT)

value = 0*( 0x01-2B / 0x2D-FF ) ; any non-null UTF-8 char
except ","
```

Defined Fields and their Descriptions

Here is a list of field name and description of their values defined in this document. The field names are not case sensitive.

Operator-Name : It contains a PWLAN AN operator name which MUST be a globally known and registered name. One proposal is to structure the content of the field into two parts separated by a colon. The first (also referred to as a prefix) identifies the operator type; example: GSM, WISP. And, the second part identifies a globally known operator defined within the domain of the operator type û for example, GSM:xxxx where xxxx is a unique globally known GSM operator ID. Prefixes describing various operator types MUST be registered with IANA [6]. The

other proposal is to have a prefixed field name where the prefix identifies the operator type (e.g., GSM:Operator-Name, WISP:Operator-Name).

Location-ID : It contains a PWLAN AN location ID defined within the scope of the AN operator name.

Location-name : It contains a PWLAN AN location name defined within the scope of the AN operator name (e.g., starbucks_2)

Location-type : It contains a PWLAN AN location type defined within the scope of the AN operator (e.g., coffee-shop, airport)

City : It contains a city name where an PWLAN AN is located (e.g., Portland)

State : It contains a state name where an PWLAN AN is located (e.g., Oregon)

Country : It contains an ISO (International Organization for Standardization) defined country name where an PWLAN AN is located (e.g., USA).

Example:

Operator-name=GSM:T-Mobile, location-ID=44,location-name=starbucks-4,location-type=coffee shop, city= seattle, state=Washington,country=us

2.2 RADIUS Support for Advertising Application-based capabilities

Rationale

There is a need for a HSN RADIUS server to discover capabilities of a RADIUS client that has initiated a connection to it. The capabilities indicate standard-based applications (e.g., existing dynamic authorization Extension to Remote [5], future prepaid accounting model, etc.) that a PWLAN AN RADIUS

Client supports. This enables the HSN RADIUS server to decide which application services it can use for the connection, or whether or not it should accept the connection. For example, if the subscriber is a prepaid subscriber, and the RADIUS

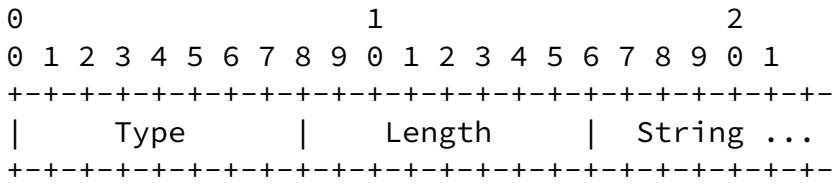
client does not support the prepaid capability, the RADIUS server may want to reject the connection.

Having a standard method for advertising application-based capabilities is essential for interoperability and proper operation of RADIUS for PWLAN in roaming situations.

Attribute

This attribute describes standard-based Applications (also referred to as capabilities) that a PWLAN AN AP supports. These capabilities MUST be identified by their identity numbers assigned by the appropriate standard bodies (e.g., RFC number for IETF). This attribute MUST be sent in Access-Request if available.

A summary of the capability Attribute is shown below.



Name

Generic Capability

Type

To be assigned by IANA

Length

>= 3

String

The string field is one or more octets. This string consists of a comma-delimited list of URIs. These URIs may but do not necessarily correspond to the actual locations of files. However, they must include a FQDN corresponding to the organization responsible for the document or standard to which compliance is claimed. For example:

www.ietf.org/rfc/3580;2548;2607, www.3GPP.org/Release6.

Note that conformance to one specification may imply conformance to others as well. Thus, it is not necessary or even possible to list all standards that the PWLAN AN supports. In many cases, the referenced URIs will correspond to best practices documents that reference standards and also indicate which optional elements of those standards must be implemented.

2.3 RADIUS Support for Specifying a Mobile IP Home Agent

Rationale

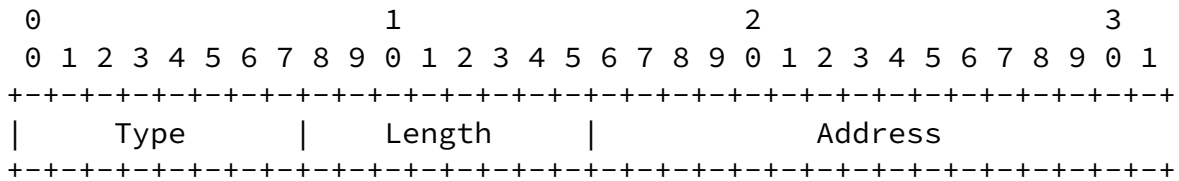
In Mobile IP [7], a Mobile-IP enabled client registers with its home agent when it attaches to the network for the first time, or when it changes its network point of attachment. In typical service provider deployments, networks are geographically dispersed within a single large administrative domain. In such networks, it is possible to deploy the home agents in each geographical area. When a PWLAN client authenticates to its HSN RADIUS server through a PWLAN AN, the HSN RADIUS server may want to specify the optimal home agent for that PWLAN client based on the PWLAN AN location information.

There is a need for an interoperable method by which the home RADIUS server can indicate the Mobile IP home agent that should used by the PWLAN client to the RADIUS client. Note that the home agent can later be indicated to the PWLAN client through a specific means û for example, it can be relayed in the ôhome agent addressö field of a DHCP reply if the client acquires its IP address through DHCP [8].

Attribute (IPv4 version)

This attribute indicates the home agent IPv4 Address that can be used by a Mobile-IP enabled PWLAN client. This attribute SHOULD be sent in Access-Accept if available.

A summary of the Mobile IPv4 home agent Attribute is shown below.



```
          Address (cont)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```


Name

Mobile IPv4 Home Agent

Type

To be assigned by IANA

Length

6

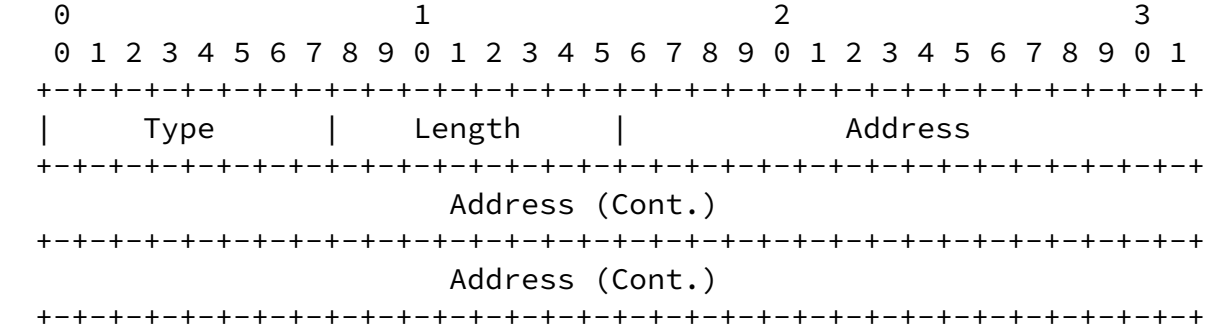
Address

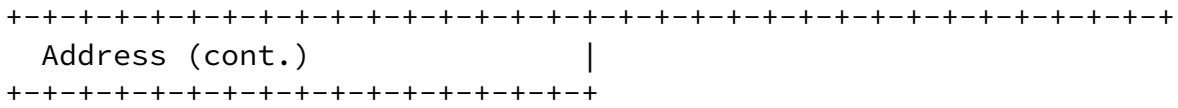
The Address filed is four octets. It contains a Mobile IP home agent address.

Attribute (IPv6 version)

This attribute indicates the home agent IPv6 Address that can be used by a Mobile-IP enabled PWLAN client. This attribute SHOULD be sent in Access-Accept if available.

A summary of the Mobile IPv6 home-agent Attribute is shown below.





Name

Mobile IPv6 Home Agent

Type

To be assigned by IANA

Length

18

Address

The Address filed is four octets. It contains a Mobile IP home agent address.

2.4 RADIUS Support for Specifying DNS Server

Rationale

Once a PWLAN client authenticated, it will most likely acquire an IP address by sending a Request to a DHCP [8] server in the PWLAN AN. The DHCP server allocates an IP address and sends it to the PWLAN client in a DHCP reply. The DHCP server also has an option of sending a DNS update to the DNS server specified by the HSN.

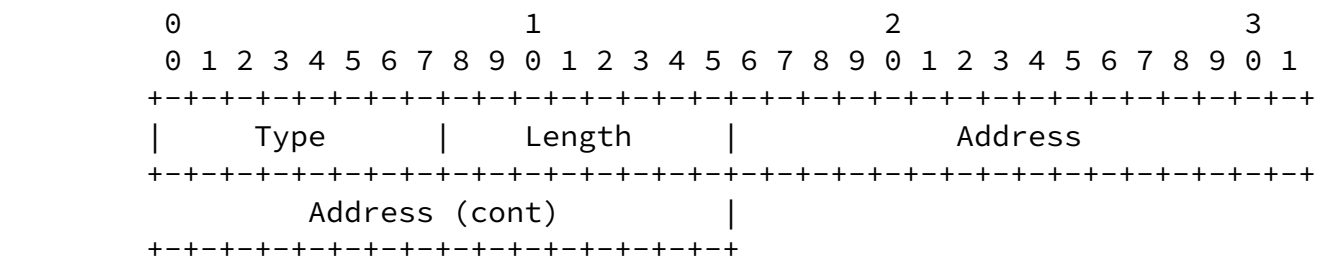
There is a need for an interoperable method by which a HSN RADIUS server can indicate the DNS server to the RADIUS client for a given PWLAN client.

Attribute (IPv4 Version)

This attribute indicates IPv4 address of a DNS server that should be used for a PWLAN client, most likely by a DHCP

server. This attribute SHOULD be sent in Access-Accept if available.

A summary of the DNS Server IPv4 Address Attribute is shown below.



Name

DNS Server IPv4 Address

Type

To be assigned by IANA

Length

6

Address

The Address field is four octets

Attribute (IPv6 Version)

To Be Defined

2.5 RADIUS Support for Specifying Remote IP Addresses

Rationale

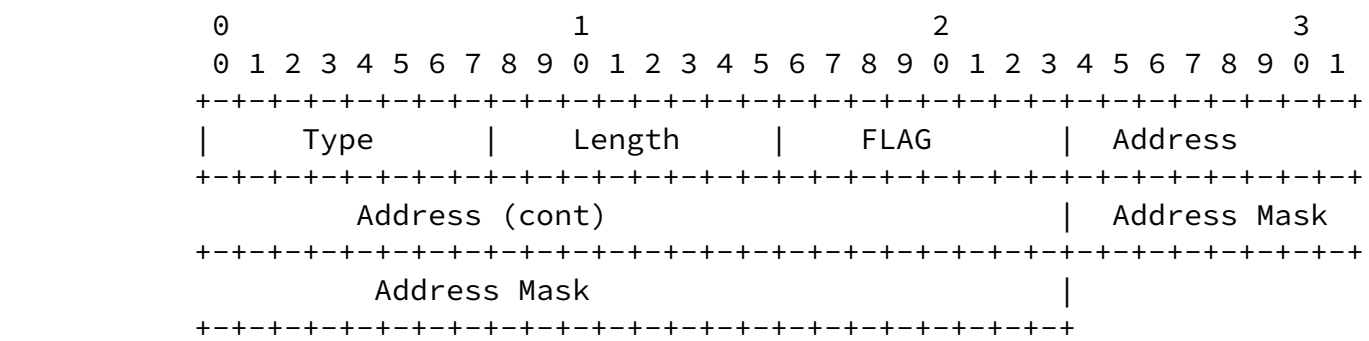
A HSN RADIUS server may want to restrict its subscribers accessing to certain remote IP addresses for different types of servers (such as, web servers, multimedia servers, mail

servers, etc.) based on their subscription profiles. Or, a HSN RADIUS server may want to monitor a range of remote IP address that its subscribers may connect to for accounting purposes. There is a need for an interoperable method by which one or more remote IP address associated with various services can be indicated to the RADIUS client for a given PWLAN Client for access authorization and/or accounting purposes.

Attribute (IPv4 Version)

This attribute indicates an IPv4 address and address mask which together identify one or more IPv4 address. It SHOULD be sent in Access-Accept, and Accounting-Request records where the Acc-Status-Type is set to Start or Stop.

A summary of the Remote IP Address(s) Attribute is shown below.



Name

Remote IPv4 Address(s)

Type

To be assigned by IANA

Length

10

Flag

1 : The address is used in conjunction with the Address Mask, to identify the range of address that a PWLAN client

MAY establish an IP connection with.

2 : The address is used in conjunction with the Address Mask, to identify the range of address to be monitored for accounting purposes.

3: Both (1) and (2)

Address

The Address field is four octets

The address field is four octets. It contains an IPv4 address.

Address Mask

The Address Mask is four octets. It contains an IPv4 address mask that in conjunction with the Address define the range of address.

Attribute (IPv6 Version)

To Be Defined

2.6 RADIUS Support for Specifying IP Address Type Options

Rationale

A PWLAN AN may have an option of assigning a layer 3 public (i.e., routable) or private (i.e., non-routable) address to a PWLAN client. If the option is available, a HSN may also want to influence which address type (i.e., public or private) should be assigned to the PWLAN client depending on the clientÆs subscription profile.

There is a need for an interoperable method by which 1) a PWLAN AN can indicate the IP address type options to a HSN. 2) A HSN can specify the desired IP address type.

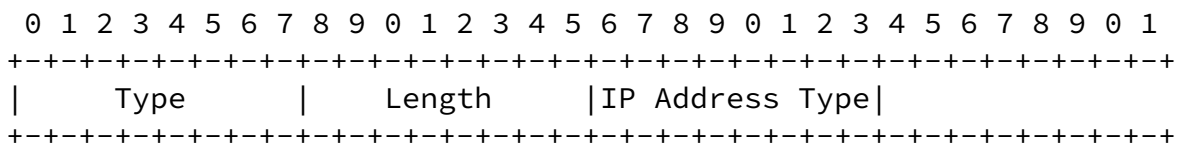
Attribute

This attribute indicates IPv4 address type options. It can be present in Access-Request, Access-Accept, and Accounting-Request records where the Acc-Status-Type is set to Start or Stop if available. When it is used in an Access-Accept and Accounting-Request packets, the Address Type value MUST be 1 or 2.

A PWLAN AN includes this attribute to advertise its IP address type options for a given PWLAN client. A RADIUS server includes this attribute in the Access-Accept to specify an IP address type option for the PWLAN client.

A RADIUS server MUST NOT include this attribute in the Access-Accept if the IP Address Type options were not advertised in the Access-Request. If an invalid IP Address Type option is received in the Access-Accept, then the PWLAN AN MUST use its default IP Address Type option for the PWLAN client. Otherwise, the PWLAN AN MUST assign an IP address according to the specified type option, and it MUST include this attribute in Accounting-Request packets to indicate the used IP address type option. If an IP address type option is not specified in the Access-Accept, the PWLAN AN MUST NOT include this attribute in Accounting-Request packets.

A summary of the home-agent Attribute is shown below.



Name

IP Address Type Options

Type

To be assigned by IANA

Length

1

Address Type

1 : Public Address Type
2 : Private Address Type
3 : Public and Private Type

2.7 RADIUS Support for Specifying Network Capabilities

Rationale

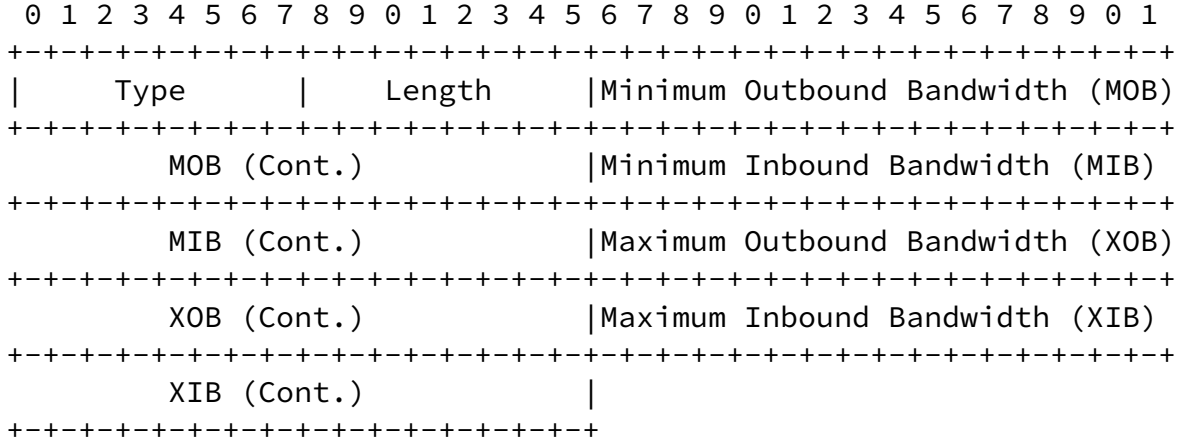
When a PWLAN client connects to a PWLAN AN, it may use certain services (e.g., real-time or multimedia services) that require a minimum network resources for the desired Quality of Service (QoS) and user experience. A PWLAN AN may be able to allocate network resources (e.g., radio and wired network bandwidth, radio network delays) for a PWLAN client within the AN, or influence the routing of its packets to outside (i.e., determining the next external hop).

The intent is to provide a generic and simple framework within which a PWLAN AN can advertise its network capabilities for a given PWLAN client to the HSN RADIUS server. And, the HSN RADIUS server then can specify the Network capability settings that it wants for that PWLAN client. The specified network capability settings also need to be indicated in the accounting packets.

Attribute (Network Capability Advertisement)

This attribute indicates network capabilities that a PWLAN AN can provide for a given PWLAN client. It SHOULD be sent in Access-Request if available.

A summary of the Network Capability Advertisement Attribute is shown below.



Name

Network Capability Advertisement

Type

To be assigned by IANA

Length

16

Minimum Outbound Bandwidth

The minimum bandwidth (bits per second) that can be guaranteed by the PWLAN AN for outbound packets.

Minimum Inbound Bandwidth

The minimum bandwidth (bits per second) that can be guaranteed by PWLAN AN for inbound packets.

Maximum Outbound Bandwidth

The maximum bandwidth (bits per second) that can be guaranteed by the PWLAN AN for outbound packets.

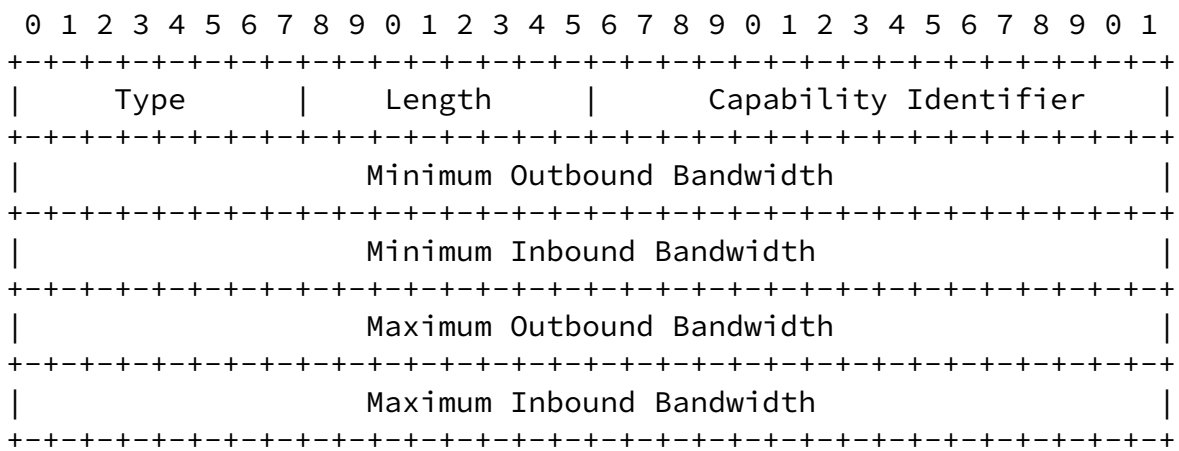
Maximum Inbound Bandwidth

The maximum bandwidth (bits per second) that can be guaranteed by the PWLAN AN for inbound packets.

Attribute (Specifying Network capabilities)

This attribute indicates network capability settings that MUST be used for a PWLAN client. It is allowed only in Access-Accept packets. However, it MUST NOT be present in Access-Accept if network capabilities were not advertised in the Access-Request.

A summary of the Specifying Network Capabilities Attribute is shown below.



Name

Specifying Network Capability Settings

Type

To be assigned by IANA

Length

18

Capability Identifier

A unique identifier used by the HSN RADIUS AAA to identify a specific network capability settings.

Minimum Outbound Bandwidth

The minimum bandwidth (bits per second) specified by the HSN RADIUS AAA. It MUST be equal or greater than the advertised Minimum Outbound Bandwidth.

Minimum Inbound Bandwidth

The minimum bandwidth (bits per second) specified by the HSN RADIUS AAA. It MUST be equal or greater than the advertised Minimum Inbound Bandwidth.

Maximum Outbound Bandwidth

The maximum bandwidth (bits per second) specified by the HSN RADIUS AAA. It MUST be equal or less than the advertised Maximum Outbound Bandwidth.

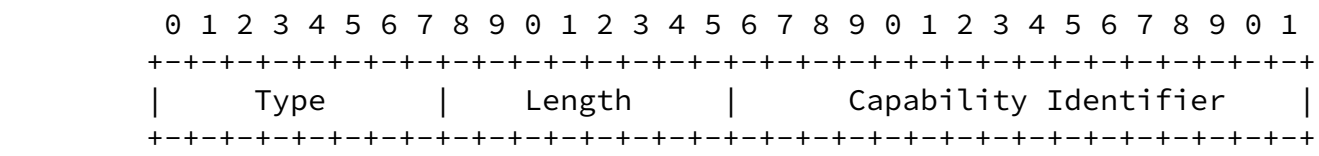
Maximum Inbound Bandwidth

The maximum bandwidth (bits per second) specified by the HSN RADIUS AAA. It MUST be equal or less than the advertised Maximum Inbound Bandwidth.

Attribute (Network Capability Settings for Accounting)

This attribute indicates Network capability settings in use for a PWLAN client for accounting purposes. It SHOULD be sent in Accounting-Request records where the Acc-Status-Type is set to Start or Stop.

A summary of the Network Capability for Accounting is shown below.



Name

Network Capability Settings for Accounting

Type

To be assigned by IANA

Length

2

Capability Identifier

A unique ID known by the HSN RADIUS AAA that indicates specific capability settings.

4. IANA Considerations

To be completed

This draft introduces new RADIUS Attributes. Therefore, there is a need for obtaining new attribute TYPE numbers from IANA.

5. Security Considerations

The attributes in this document have no additional security considerations beyond those already identified in [?].

6. Contributors

This document is a joint work of the contributing authors (in alphabetical order):

- Farid Adrangi (Intel)
- Farooq Bari (AT&T Wireless)

- Blair Bullock (iPass)
- Kountal Chowdury (Nortel)
- Pasi Eronen (Nokia)
- Mark Grayson (Cisco)
- Ed Van Horne (Cisco)
- Jouni Korhonen (teliasonera)
- Victor Lortz (Intel)
- Avi Lior (Bridgewater)
- Serge Manning (Sprint)
- Jose Puthenkulam (Intel)

7. Acknowledgements

The authors would like to thank Bernrad Aboba (of Microsoft), Parviz Yeganeh (of Cisco), Gopal Dommety (of Cisco) for their feedback and guidance.

8. References

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

[2] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[3] Rigney, C., Willats, W., Calhoun, P., "RADIUS Extensions", RFC 2869, June 2000.

[4] Chiba, M., Dommety, G., Eklund, M., Mitton, D., Aboba, B., "Dynamic Authorization Extensions to Remote Authentication Dial-In User Service (RADIUS)", Internet Draft (work in progress), RFC 3576, July 2003.

[5] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[6] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[7] C. Perkins, "IP Mobility Support for IPv4", RFC 3344, August 2002.

[8] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

AuthorsÆ Addresses

Farid Adrangi
Email: farid.adrangi@intel.com Phone:+1 503-712-1791
Farooq Bari
Email : Farooq.bari@attws.com Phone:
Blair Bullock
Email: bbullock@ipass.com Phone:
Pasi Eronen
Email: pasi.eronen@nokia.com
Mark Grayson
Email: mgrayson@cisco.com Phone:
Victor Lortz
Email: victor.lortz@intel.com Phone:+1 503-264-3253
Jose Puthenkulam

Full Copyright Statement

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