Network Working Group
Internet Draft

S Willens
Livingston
A Rubens
Merit
W A Simpson
Daydreamer
C Rigney
Livingston

expires in six months

May 1994

Remote Authentication Dial In User Service (RADIUS)
draft-ietf-nasreq-radius-01.txt (c)

Status of this Memo

Abstract

This document describes a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server.

Table of Contents

1. Introduction

Managing dispersed serial line and modem pools for large numbers of users can create the need for significant administrative support. Since modem pools are by definition a link to the outside world, they require careful attention to security, authorization and accounting. This can be best achieved by managing a single "database" of users, which allows for authentication (verifying user name and password) as well as configuration information detailing the type of service to deliver to the user (that is, SLIP, PPP, telnet, rlogin).

Key features of RADIUS are:

Client/Server Model

A Network Access Server (NAS) operates as a client of RADIUS. The NAS is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned.

RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the NAS to deliver service to the user.

The RADIUS servers can act as proxy clients to other authentication servers, such as Kerberos.

Network Security

Transactions between the NAS and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the NAS and RADIUS server, to eliminate the possibility that someone snooping on an unsecure network could determine a user's password.

Flexible Authentication Mechanisms

The RADIUS server supports a variety of methods to authenticate a user. When it is provided with the user name and original password given by the user, it can support PPP PAP or CHAP, UNIX login, and other authentication mechanisms available through published API's such as Kerberos and SafeWord.

Extensible Protocol

All transactions are comprised of variable length attribute-value tuples. Adding new attribute values can be achieved without

disturbing existing implementations of the protocol.

Source Code Availability

Livingston Enterprises is making the C source code for RADIUS available without use restrictions.

1.1. Specification of Requirements

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

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

MUST NOT This phrase means that the definition is an absolute prohibition of the specification.

SHOULD This word, or the adjective "recommended", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course.

MAY This word, or the adjective "optional", means that this item is one of an allowed set of alternatives. An implementation which does not include this option MUST be prepared to interoperate with another implementation which

does include the option.

1.2. Terminology

This document frequently uses the following terms:

silently discard
: This means the implementation discards the packet without further processing. The implementation SHOULD provide the capability of logging the error, including the contents of the silently discarded packet, and SHOULD record the event in a statistics counter.

2. Operation

When a NAS is configured to use RADIUS, any user of the NAS presents authentication information to the NAS. This might be with a customizable login prompt, where the user is expected to enter their username and password. Alternatively, the user might use a link framing protocol such as the Point-to-Point Protocol (PPP), which has authentication packets which carry this information.

Once the NAS has obtained such information, it first looks in its local database of users for the username. If found, the user is locally authenticated. If not found, the NAS will create an "Access-Request" containing such attributes as the user's name, the user's password, the ID of the NAS and the Port ID which the user is accessing. When a password is present, it is hidden using a method based on the RSA Message Digest Algorithm MD5 [3].

The Access-Request is submitted to the RADIUS server via the network. If no response is returned within a configurable length of time, the request is re-sent a configurable number of times. After several failed attempts, the NAS can also forward requests to an alternate server in the event that the primary server is down or unreachable.

Once the RADIUS server receives the request, it validates the sending client. The RADIUS server consults a local database of users to find the user whose name matches the request. The user entry in the database contains a list of requirements which must be met to allow access for the user. This always includes verification of the password, but can also specify the NAS or Port to which the user is allowed access.

The RADIUS server MAY make requests of other servers in order to satisfy the request.

If any condition is not met, the RADIUS server sends an "Access-Reject" response indicating that this user request is invalid. If desired, the server MAY also send a text message which MAY be displayed by the NAS to the user. No other attributes are permitted in an "Access-Reject".

If all conditions are met and the RADIUS server wishes to issue a challenge to which the user must respond, the RADIUS server sends an "Access-Challenge" response.

If the NAS receives an Access-Challenge and supports challenge/response it MAY display the text message, if any, to the user, and then prompt the user for a response. It then re-submits its original Access-Request with a new request ID, with the Password

attribute replaced by the response (encrypted), and including the State attribute from the "Access-Challenge", if any. Only 0 or 1 State attributes should be present in a request.

If all conditions are met, the list of configuration values for the user are placed into an "Access Ack" response. These values include the type of usage (SLIP, PPP, Login User), and all necessary values to deliver the desired service. For SLIP and PPP, this includes such values as IP addresses, subnet masks, MTU, desired compression, and desired packet filters. For character mode users, this includes things such as desired protocol, host, and access control filter.

2.1. Challenge/Response

In challenge/response authentication, individual users are given an unpredictable number and challenged to encrypt it and give back the result. Authorized users are equipped with special devices such as smart cards that facilitate calculation of the correct response with ease. Unauthorized users, lacking the appropriate device and lacking knowledge of the secret key necessary to emulate such a device, can only guess at the response.

The Access-Challenge packet typically contains a Reply-Message including a challenge to be displayed to the user, such as a numeric value unlikely ever to be repeated. Typically this is obtained from an external server that knows what type of authenticator should be in the possession of the authorized user and can therefore choose a random or non-repeating pseudorandom number of an appropriate radix and length.

The user then enters the challenge into his device and it calculates a response, which the user enters into the NAS which forwards it to the RADIUS server via a second Access-Request. If the response matches the expected response the RADIUS server replies with an Access-Ack, otherwise an Access-Reject.

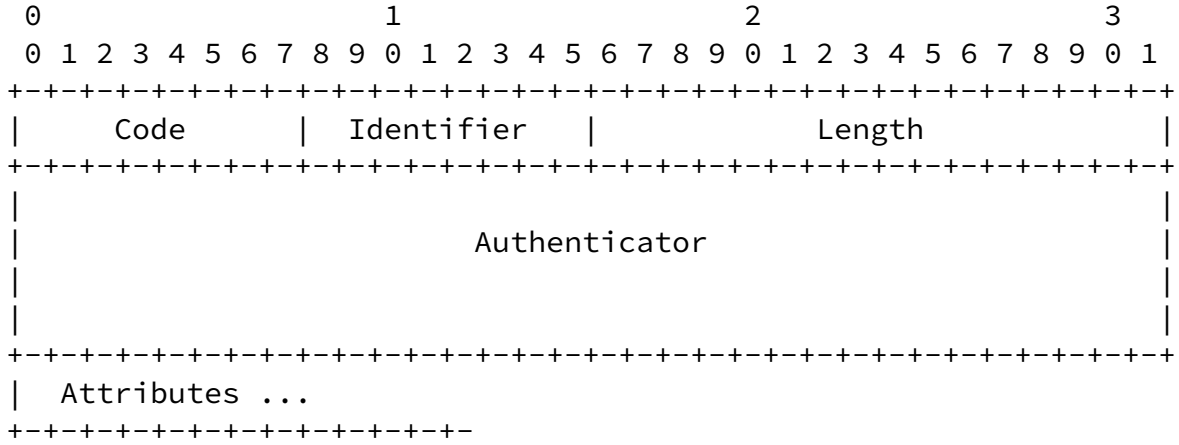
3. Packet Format

Exactly one RADIUS packet is encapsulated in the UDP Data field [1], where the UDP Destination Port field indicates 1645, and the UDP Source Port field is used to indicate the specific request which was made. Each new request MUST use a new UDP Source Port. A retransmitted request does not need to be considered a new request. An Access-Request sent in reply to an Access-Challenge does not need

to be considered a new request and can use the same UDP Source Port as the Access-Request that resulted in the Access-Challenge.

When a reply is generated, the Ports are reversed.

A summary of the RADIUS data format is shown below. The fields are transmitted from left to right.



Code

The Code field is one octet, and identifies the type of RADIUS packet. When a packet is received with an invalid Code field, it is silently discarded.

RADIUS Codes (decimal) are assigned as follows:

1	Access-Request
2	Access-Ack
3	Access-Reject
11	Access-Challenge

Identifier

The Identifier field is one octet, and aids in matching requests and replies.

Length

The Length field is two octets. It indicates the length of the packet including the Code, Identifier, Length, Authenticator and Attribute fields. Octets outside the range of the Length field should be treated as padding and should be ignored on reception.

Authenticator

The Authenticator field is sixteen octets. The most significant octet is transmitted first. This value is used to authenticate the reply from the RADIUS server, and is used in the password hiding algorithm.

The Request Authenticator value depends upon the method used to generate the octets, and is independent of the hash algorithm used to generate any response. The value SHOULD be unique and unpredictable.

The Ack, Reject, or Challenge Authenticator field contains a one-way MD5 hash calculated over a stream of octets consisting of the RADIUS packet, beginning with the Code field, including the Identifier, the Length, the Request Authenticator, and the response Attributes, followed by (concatenated with) a "shared secret".

The one-way hash algorithm is chosen such that it is computationally infeasible to determine the secret from the known request and response values.

The secret SHOULD be at least as large and unguessable as a well-chosen password. It is preferred that the secret be at least the length of the hash value for the hashing algorithm chosen (16 octets for MD5). This is to ensure a sufficiently large range for the secret to provide protection against exhaustive search attacks.

Each Request Authenticator value SHOULD be unique over the lifetime of a secret, since repetition of a request value in conjunction with the same secret would permit an attacker to reply with a previously intercepted response. Since it is expected that the same secret MAY be used to authenticate with servers in disparate geographic regions, the request SHOULD exhibit global and temporal uniqueness.

Each Request Authenticator value SHOULD also be unpredictable, lest an attacker trick a server into responding to a predicted future request, and then use the response to masquerade as that server to another authenticator.

Although protocols such as RADIUS are incapable of protecting against theft of an authenticated session via realtime active wiretapping

attacks, generation of unique unpredictable requests can protect against a wide range of active attacks against authentication.

3.1. Access-Request

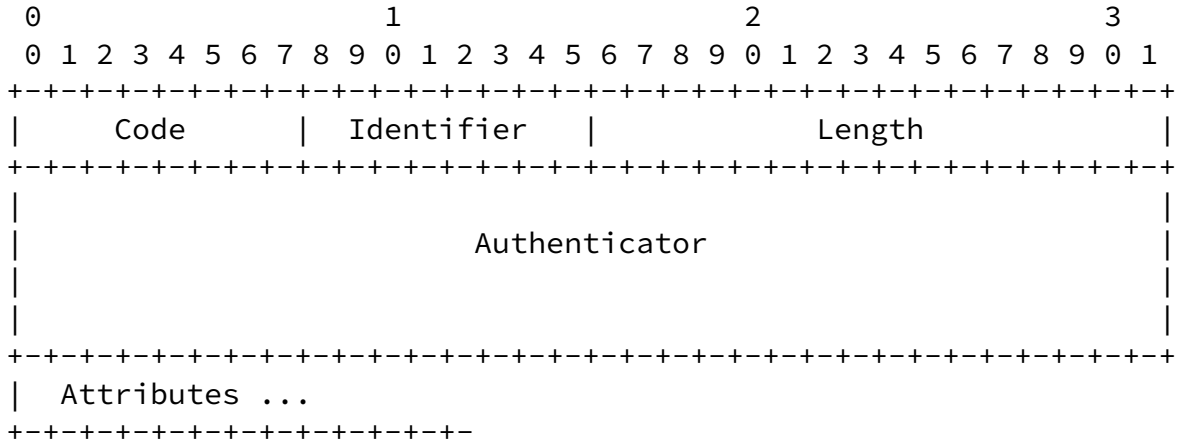
Description

Access-Request packets are sent to a RADIUS server, and convey information used to determine whether a user is allowed access to a specific NAS, and any special services requested for that user. An implementation wishing to Authenticate a user MUST transmit a RADIUS packet with the Code field set to 1 (Access-Request).

Upon receipt of an Access-Request, an appropriate reply MUST be transmitted.

This request MUST contain attributes containing the ID of the NAS and the user's name, and SHOULD contain attributes with the user's password and the Port ID which the user is accessing. It MAY contain additional attributes as a hint to the server. When a password is present, it is hidden using a method based on the RSA Message Digest Algorithm MD5 [3].

A summary of the Access-Request packet format is shown below. The fields are transmitted from left to right.



Code

1 for Access-Request.

Identifier

The Identifier field MUST be changed whenever the content of the Attributes field changes, and whenever a valid reply has been received for a previous request. For retransmissions, the Identifier MAY remain unchanged.

Authenticator

The Authenticator value MUST be changed each time a new Identifier is used.

Attributes

The Attribute field is variable in length, and contains the list of attributes that are required for the type of service, as well as any desired optional attributes.

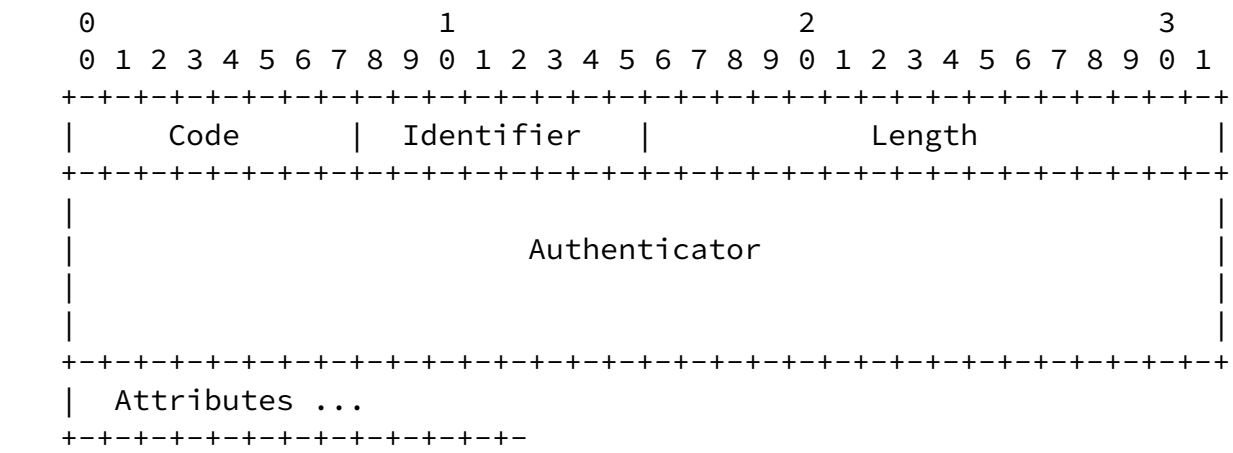
3.2. Access-Ack

Description

Access-Ack packets are sent by the RADIUS server, and provide specific configuration information necessary to begin delivery of services to the user. If every Attribute received in an Access-Request is recognizable and all values are acceptable, then the RADIUS implementation MUST transmit a packet with the Code field set to 2 (Access-Ack).

On reception of an Access-Ack, the Identifier field is matched with a pending Access-Request. Additionally, the Authenticator field MUST contain the correct response for the pending Access-Request. Invalid packets are silently discarded.

A summary of the Access-Ack packet format is shown below. The fields are transmitted from left to right.



Code

2 for Access-Ack.

Identifier

The Identifier field is a copy of the Identifier field of the Access-Request which caused this Access-Ack.

Authenticator

The Authenticator value is calculated from the Access-Request value, as described earlier.

Attributes

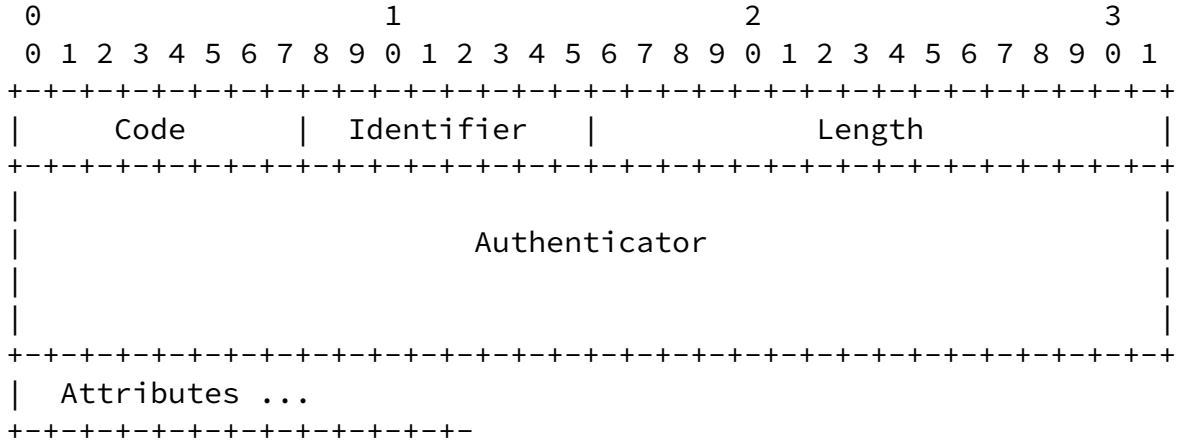
The Attribute field is variable in length, and contains a list of zero or more Attributes.

3.3. Access-Reject

Description

If any value of the received Attributes is not acceptable, then the RADIUS server MUST transmit a packet with the Code field set to 3 (Access-Reject). It MAY include a Reply-Message Attribute with a text message which the NAS MAY display to the user.

A summary of the Access-Reject packet format is shown below. The fields are transmitted from left to right.



Code

3 for Access-Reject.

Identifier

The Identifier field is a copy of the Identifier field of the Access-Request which caused this Access-Reject.

Authenticator

The Authenticator value is calculated from the Access-Request value, as described earlier.

Attributes

The Attribute field is variable in length, and contains a list of zero or more Attributes.

3.4. Access-Challenge

Description

If the RADIUS server desires to send the user a challenge requiring a response, then the RADIUS server MUST respond to the Access-Request by transmitting a packet with the Code field set to 4 (Access-Challenge).

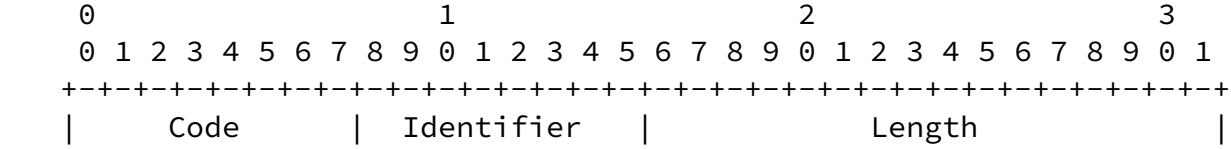
The Attributes field MAY have a Reply-Message Attribute. and MAY have a State Attribute. No other attributes are permitted in an Access-Challenge.

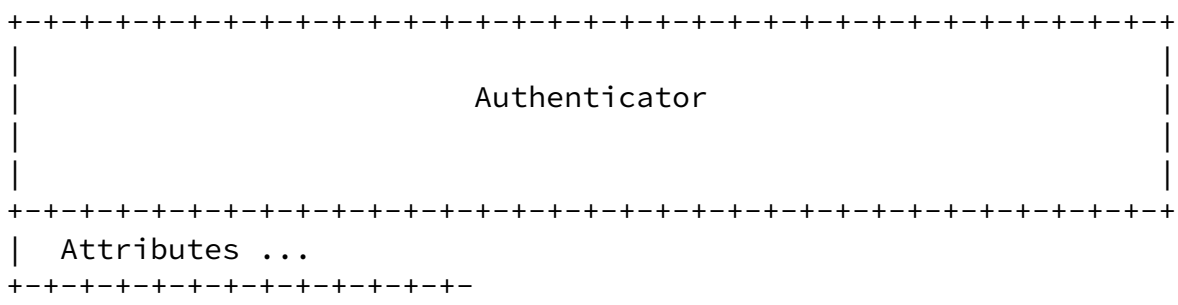
On receipt of an Access-Challenge, the Identifier field is matched with a pending Access-Request. Additionally, the Authenticator field MUST contain the correct response for the pending Access-Request. Invalid packets are silently discarded.

If the NAS supports challenge/response, receipt of a valid Access-Challenge indicates that a new Access-Request SHOULD be submitted. The NAS MAY display the text message, if any, to the user, and then prompt the user for a response. It then re-submits its original Access-Request with a new request ID, with the Password attribute replaced by the user's response (encrypted), and including the State attribute from the "Access-Challenge", if any. Only 0 or 1 State attributes should be present in a request.

A NAS which supports PAP MAY forward the Reply-Message to the dialin client and accept a PAP response which it can use as though the user had entered the response.

A summary of the Access-Challenge packet format is shown below. The fields are transmitted from left to right.





Code

11 for Access-Challenge.

Identifier

The Identifier field is a copy of the Identifier field of the Access-Request which caused this Access-Challenge.

Authenticator

The Authenticator value is calculated from the Access-Request value, as described earlier.

Attributes

The Attributes field is variable in length, and contains a list of zero or more Attributes.

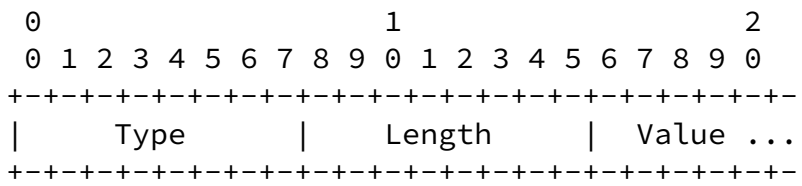
4. Attributes

RADIUS Attributes carry the specific authentication, authorization, information and configuration details for the request and reply.

Some Attributes MAY be listed more than once. The effect of this is Attribute specific, and is specified by each such Attribute description.

The end of the list of Attributes is indicated by the length of the RADIUS packet.

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



Type

The Type field is one octet. Up-to-date values of the RADIUS Type field are specified in the most recent "Assigned Numbers" RFC [2]. Values 192-223 are reserved for experimental use, values 224-240 are reserved for implementation-specific use, and values 241-255 are reserved and should not be used. This specification concerns the following values:

1	User-Name
2	User-Password
3	Challenge-Response
4	NAS-Identifier
5	NAS-Port
6	User-Service
7	Framed-Protocol
8	Framed-Address
9	Framed-Netmask
10	Framed-Routing
11	Framed-Filter
12	Framed-MTU
13	Framed-Compression
14	Login-Host
15	Login-Service
16	Login-TCP-Port
17	(deprecated)

```
      18      Reply-Message
      19      Callback-Number
      20      Callback-Name
      21      (unassigned)
      22      Framed-Route
      23      Framed-IPX-Network
      24      State
```

Length

The Length field is one octet, and indicates the length of this Attribute including the Type, Length and Value fields. If an Attribute is received in a Access-Request but with an invalid Length, an Access-Reject SHOULD be transmitted.

Value

The Value field is zero or more octets and contains information specific to the Attribute. The format and length of the Value field is determined by the Type and Length fields.

The format of the value field is one of four data types.

string 0-253 octets

address 32 bit value, most significant octet first.

integer 32 bit value, most significant octet first.

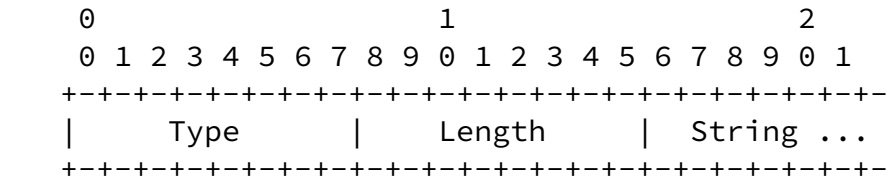
time 32 bit value, most significant octet first -- seconds since 00:00:00 GMT, January 1, 1970.

4.1. User-Name

Description

This attribute indicates the name of the user to be authenticated. It is only used in Access-Request packets.

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



Type

1

Length

>= 3

String

The String field is one or more octets.

The format of the username may be one of several forms:

monolithic Consisting only of alphanumeric characters. This simple form might be used to locally manage a NAS.

provider/name
Two monolithic portions separated by a slash. The provider part indicates the realm in which the name part applies.

name@fqdn SMTP address. The Fully Qualified Domain Name (with or without trailing dot) indicates the realm in which the name part applies.

distinguished name
A name in ASN.1 form used in Public Key authentication systems.

4.2. User-Password

Description

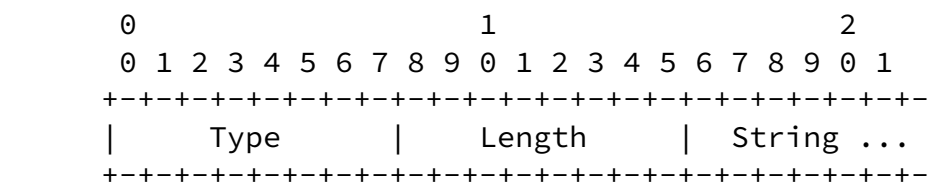
This attribute indicates the password of the user to be authenticated. It is only used in Access-Request packets.

On transmission, the password is hidden. A one-way MD5 hash is

calculated over a stream of octets consisting of the "shared secret", followed by (concatenated with) the Request Authenticator. This value is xor'd with each successive 16 octet segment of the password.

On receipt, the same mask is created. Repeating the xor function yields the original password.

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



Type

2

Length

>= 3

String

The String field is one or more octets.

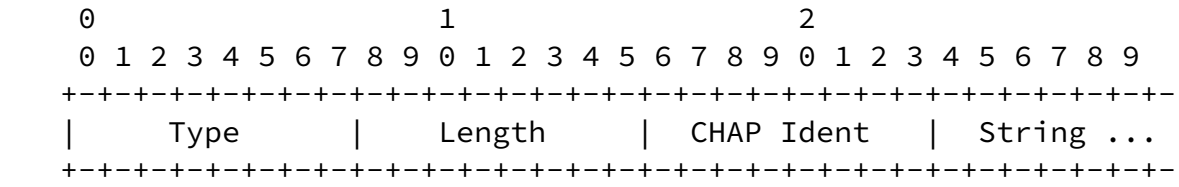
4.3. Challenge-Response

Description

This attribute indicates the response value provided by a PPP Challenge-Handshake Authentication Protocol (CHAP) user in response to the challenge. It is only used in Access-Request packets.

The CHAP challenge value is found in the RADIUS Authenticator field.

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



Type

3

Length

>= 18

CHAP Ident

This field is one octet, and contains the CHAP Identifier from the CHAP Response packet.

String

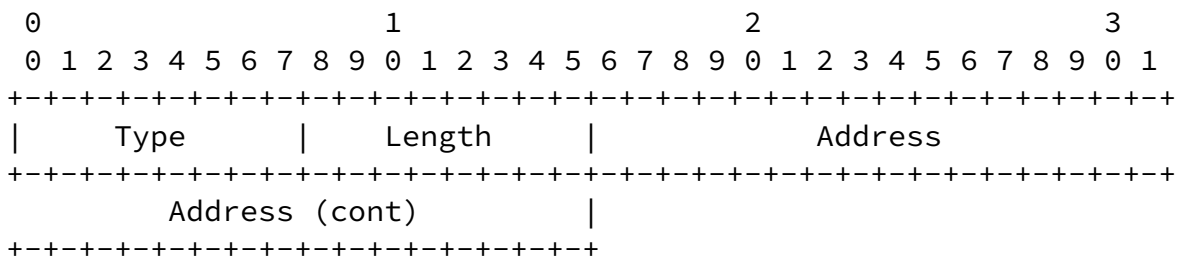
The String field is 16 octets when MD5 is used for CHAP.

4.4. NAS-Identifier

Description

This attribute indicates the Identifying Address of the NAS which is authenticating the user. It is only used in Access-Request packets.

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



Type

4

Length

6

Address

The Address field is four octets.

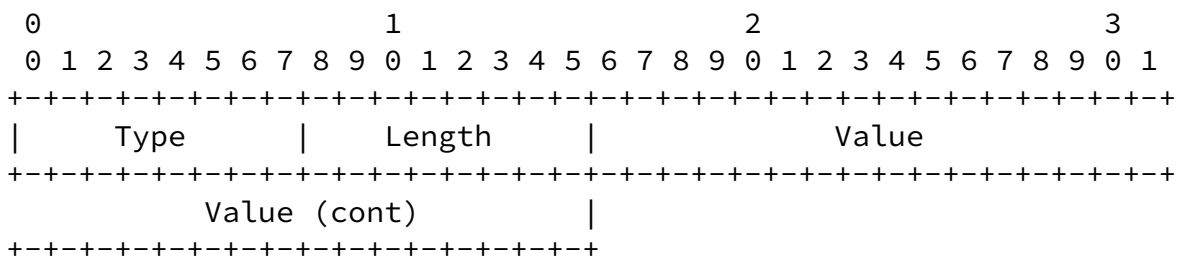
4.5. NAS-Port

Description

This attribute indicates the port number of the NAS which is

authenticating the user. It is only used in Access-Request packets.

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



Type

5

Length

6

Value

The Value field is four octets. Despite the rather large size of the field, values range from 0 to 65535.

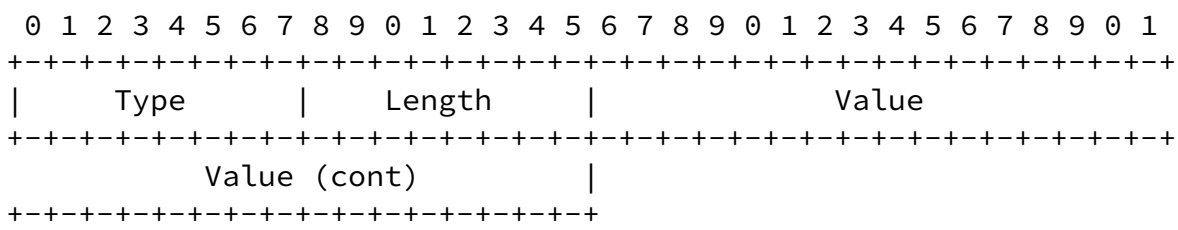
4.6. User-Service

Description

This attribute indicates the type of link the user has requested, or a change in the type of link to be configured. It is used in both Access-Request and Access-Ack packets.

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

0 1 2 3



Type

6

Length

6

Value

The Value field is four octets.

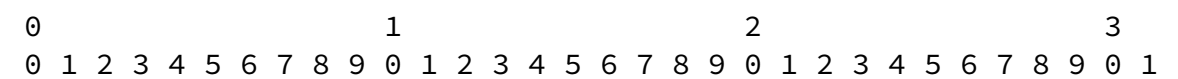
1	Login
2	Framed
3	Callback Login
4	Callback Framed
5	Outbound User
6	Shell User

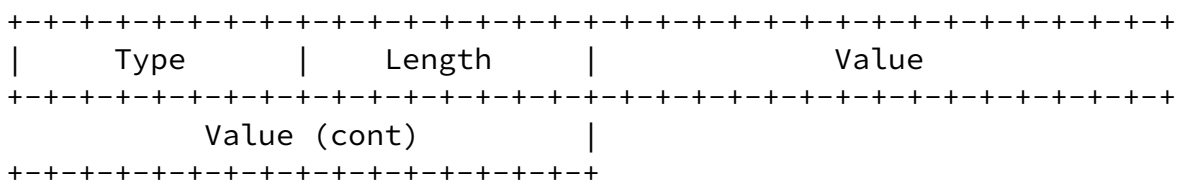
4.7. Framed-Protocol

Description

This attribute indicates the framing to be used for framed access. It is used in both Access-Request and Access-Ack packets.

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





Type

7

Length

6

Value

The Value field is four octets.

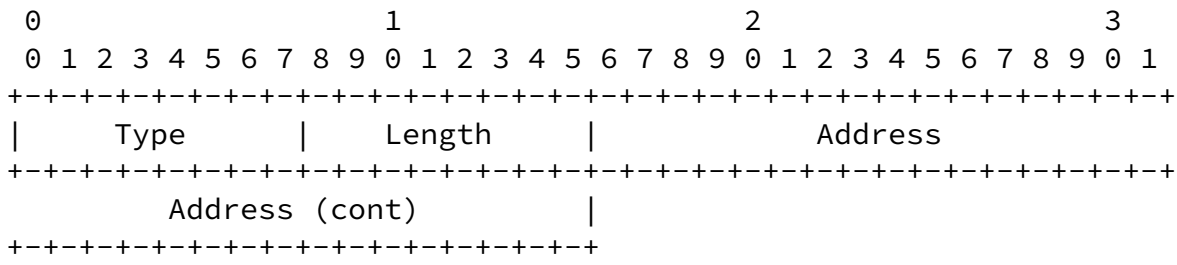
1 PPP
2 SLIP

4.8. Framed-Address

Description

This attribute indicates the address to be configured for the user. It is only used in Access-Ack packets.

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



Type

8

Length

6

Address

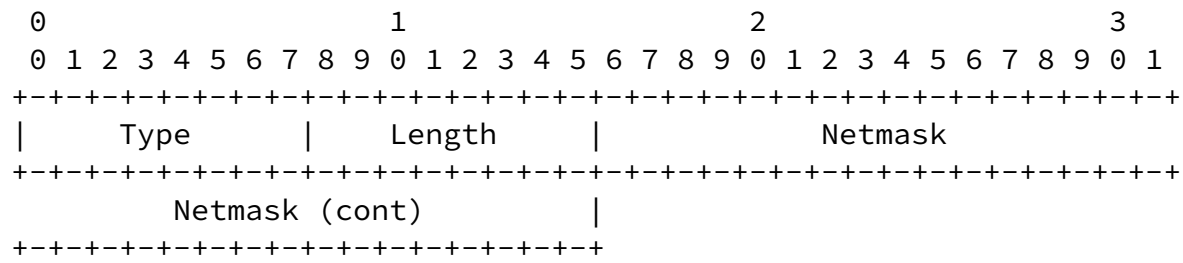
The Address field is four octets. The value 0xFFFFFFFF indicates that the NAS should allow the user to select an address (e.g. Negotiated). The value 0xFFFFFFFE indicates that the NAS should select an address for the user (e.g. Assigned from a pool of addresses kept by the NAS).

4.9. Framed-Netmask

Description

This attribute indicates the IP netmask to be configured for the user when the user is a router to a network. It is unnecessary when routing is used. It is only used in Access-Ack packets.

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



Type

9

Length

6

Netmask

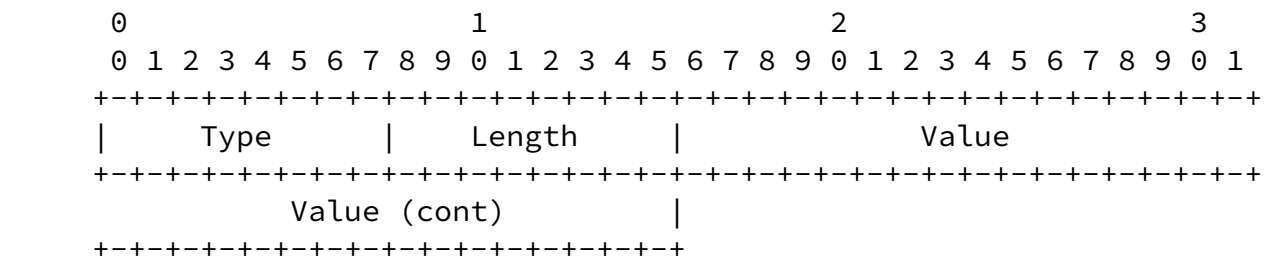
The Netmask field is four octets.

4.10. Framed-Routing

Description

This attribute indicates the routing method for the user, when the user is a router to a network. It is only used in Access-Ack packets.

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



Type

10

Length

6

Value

The Value field is four octets.

0 None
1 Send routing packets
2 Listen for routing packets
3 Send and Listen

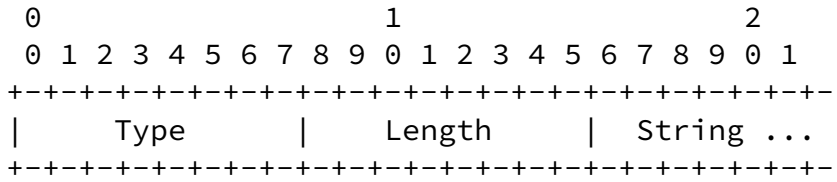
4.11. Framed-Filter

Description

This attribute indicates the name of the filter list for this user.

Using a name for a filter list allows independence from multiple NAS implementations. However, the name used might be dependent on the NAS making the request, rather than the user.

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



Type

11

Length

>= 3

String

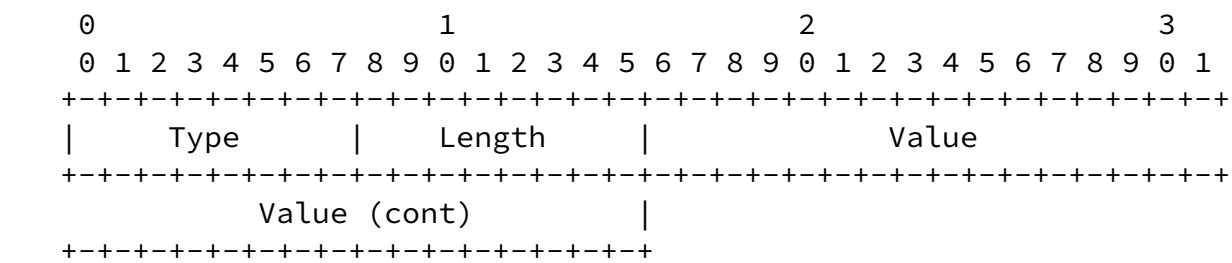
The String field is one or more octets.

4.12. Framed-MTU

Description

This attribute indicates the Maximum Transmission Unit to be configured for the user, when it is not negotiated by some other means (such as PPP). It is only used in Access-Ack packets.

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



Type

12

Length

6

Value

The Value field is four octets. Despite the rather large size of the field, values range from 64 to 65535.

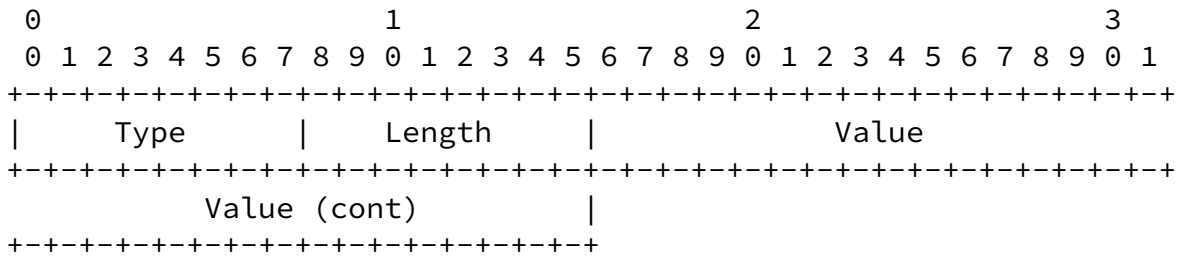
4.13. Framed-Compression

Description

This attribute indicates a compression protocol to be used for the link.

More than one compression protocol attribute MAY be sent. It is the responsibility of the NAS to apply the proper compression protocol to appropriate link traffic.

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



Type

13

Length

6

Value

The Value field is four octets.

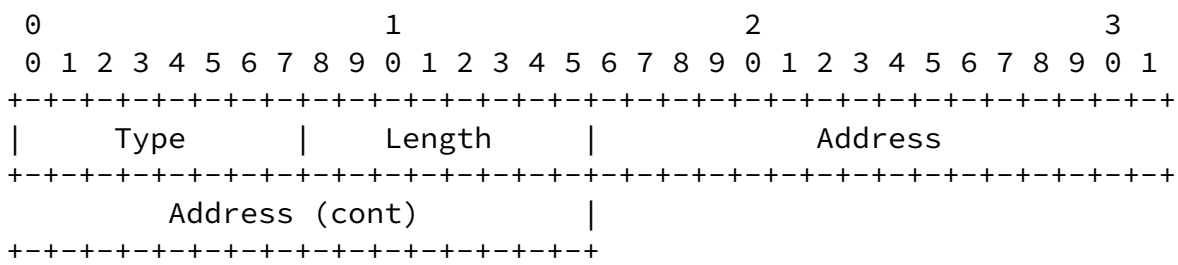
1 VJ TCP/IP header compression
2 IPX header compression

4.14. Login-Host

Description

This attribute indicates the system with which the user is to be automatically connected, when the Login-Service attribute is listed. It is only used in Access-Ack packets.

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



Type

14

Length

6

Address

The Address field is four octets. The value 0xFFFFFFFF indicates that the NAS SHOULD allow the user to select an address. The value 0 indicates that the NAS SHOULD select a host to connect the user to.

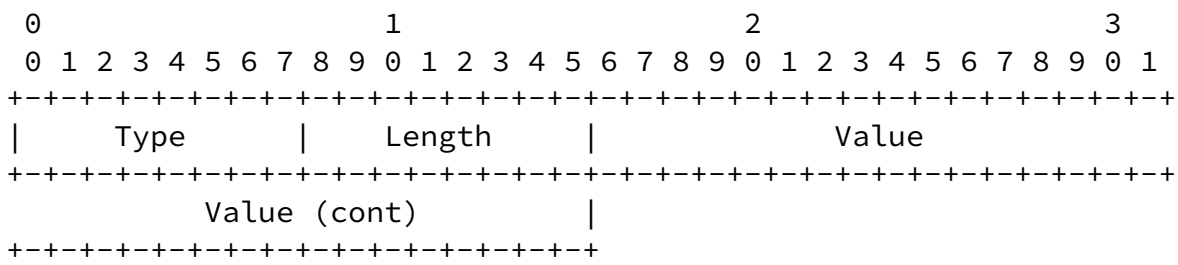
4.15. Login-Service

Description

This attribute indicates the service with which the user is to be

automatically connected. It is only used in Access-Ack packets.

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



Type

15

Length

6

Value

The Value field is four octets.

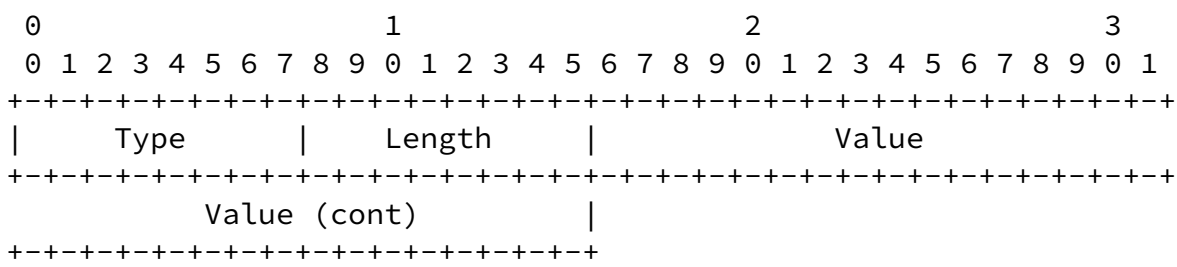
0	Telnet
1	Rlogin
2	TCP
3	Portmaster (proprietary)

4.16. Login-TCP-Port

Description

This attribute indicates the TCP port with which the user is to be automatically connected, when the Login-Service attribute is listed. It is only used in Access-Ack packets.

A summary of the Login-TCP-Port attribute format is shown below. The fields are transmitted from left to right.



Type

16

Length

6

Value

The Value field is four octets. Despite the rather large size of the field, values range from 0 to 65535.

4.17. Change-Password

Description

THIS ATTRIBUTE HAS BEEN DEPRECATED.

4.18. Reply-Message

Description

This attribute indicates text which MAY be displayed to the user.

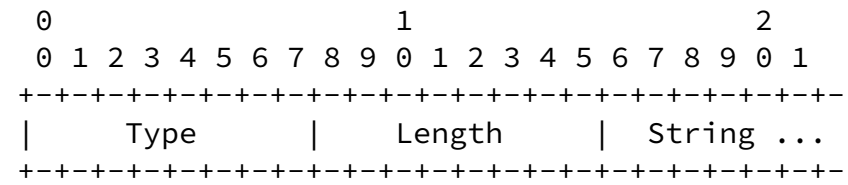
When used in an Access-Ack, it is the success message.

When used in an Access-Reject, it is the failure message. It MAY indicate a dialog message to prompt the user before another Access-Request attempt.

When used in an Access-Challenge, it MAY indicate a dialog message to prompt the user for a response.

Multiple Reply-Message's MAY be included and if any are displayed, they MUST be displayed in the same order as they appear in the packet.

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



Type

18

Length

>= 3

String

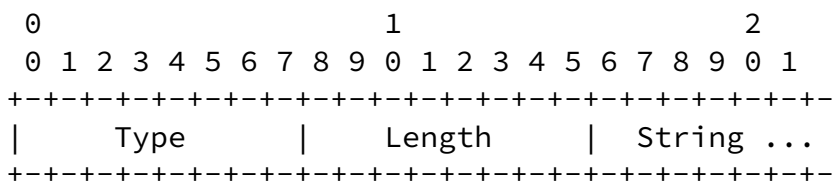
The String field is one or more octets, and its contents are implementation dependent. It is intended to be human readable, and MUST NOT affect operation of the protocol. It is recommended that the message contain displayable ASCII characters 32 through 126 decimal. Mechanisms for extension to other character sets are the topic of future research.

4.19. Callback-Number

Description

This attribute indicates a dialing string to be used for callback. It is used in both Access-Request and Access-Ack packets.

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



Type

19

Length

>= 3

String

The String field is one or more octets. The actual format of the information is site or application specific, and a robust implementation SHOULD support the field as undistinguished octets.

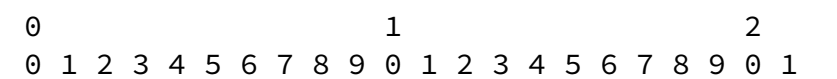
It is intended that only an authorized user will have correct site specific information to make use of the Callback. The codification of the range of allowed usage of this field is outside the scope of this specification.

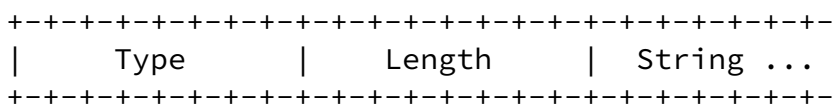
4.20. Callback-Name

Description

This attribute indicates the name of a place to be called. It is used in both Access-Request and Access-Ack packets.

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





Type

20

Length

>= 3

String

The String field is one or more octets. The actual format of the information is site or application specific, and a robust implementation SHOULD support the field as undistinguished octets.

It is intended that only an authorized user will have correct site specific information to make use of the Callback. The codification of the range of allowed usage of this field is outside the scope of this specification.

4.21. (unassigned)

Description

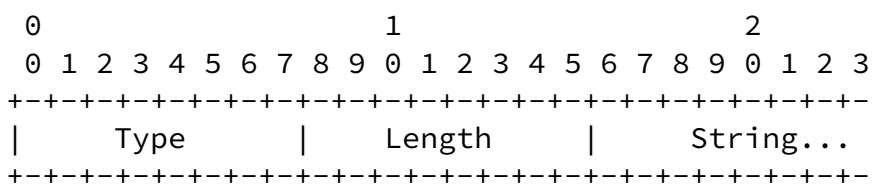
THIS ATTRIBUTE CODE HAS NOT BEEN ASSIGNED.

4.22. Framed-Route

Description

This attribute provides routing information to be configured for the user. It is used in the Access-Ack packet and can appear multiple times.

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



Type

22

Length

>= 3

String

The String field is one or more octets, and its contents are implementation dependent. It is intended to be human readable and MUST NOT affect operation of the protocol. It is recommended that the message contain displayable ASCII characters 32 through 126 decimal.

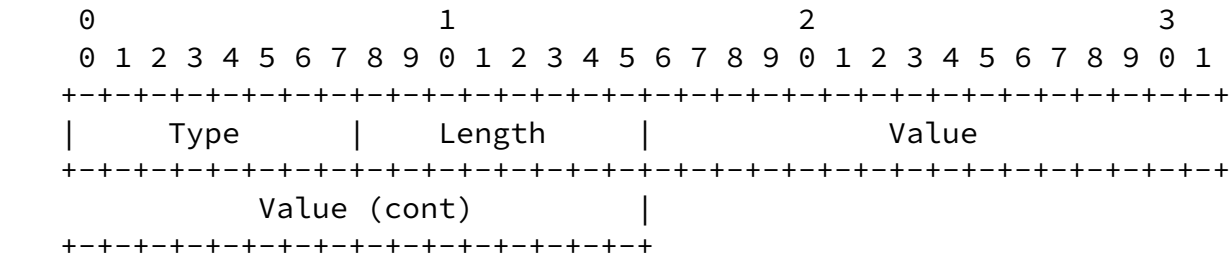
It MAY contain a destination address in dotted quad form, a space, a gateway address in dotted quad form, a space, and a decimal metric.

4.23. Framed-IPX-Network

Description

This attribute indicates the IPX Network number to be configured for the user. It is used in Access-Ack packets.

A summary of the Framed-IPX-Network attribute format is shown below. The fields are transmitted from left to right.



Type

23

Length

6

Value

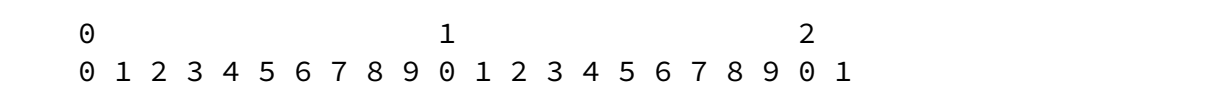
The Value field is four octets.

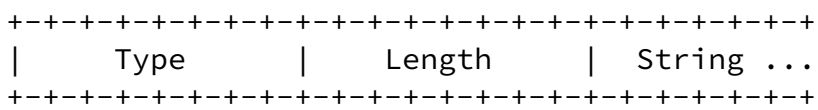
4.24. State

Description

This attribute is available to be sent by the server to the client in an Access-Challenge and should be sent unmodified from the client to the server in an Access-Ack reply to that Challenge. No interpretation by the client should be made. A packet may have only one State attribute. Usage of the State attribute is implementation dependent.

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





Type

20

Length

>= 3

String

The String field is one or more octets. The actual format of the information is site or application specific, and a robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.

Security Considerations

Security issues are the primary topic of this document.

In practice, within or associated with each RADIUS server, there is a database which associates "user" names with authentication information ("secrets"). It is not anticipated that a particular named user would be authenticated by multiple methods. This would make the user vulnerable to attacks which negotiate the least secure method from among a set (such as PAP rather than CHAP). Instead, for each named user there should be an indication of exactly one method used to authenticate that user name. If a user needs to make use of different authentication methods under different circumstances, then distinct user names SHOULD be employed, each of which identifies exactly one authentication method.

Passwords and other secrets should be stored at the respective ends such that access to them is as limited as possible. Ideally, the secrets should only be accessible to the process requiring access in order to perform the authentication.

The secrets should be distributed with a mechanism that limits the number of entities that handle (and thus gain knowledge of) the secret. Ideally, no unauthorized person should ever gain knowledge of the secrets. It is possible to achieve this with SNMP Security Protocols [4], but such a mechanism is outside the scope of this specification.

Other distribution methods are currently undergoing research and experimentation. The SNMP Security document [4] also has an excellent overview of threats to network protocols.

References

[1] Postel, J., "User Datagram Protocol", RFC 768, USC/Information Sciences Institute, August 1980.

[2] Reynolds, J., and J. Postel, "Assigned Numbers", RFC 1340, USC/Information Sciences Institute, July 1992.

[3] Rivest, R., and S. Dusse, "The MD5 Message-Digest Algorithm", MIT Laboratory for Computer Science and RSA Data Security, Inc., RFC 1321, April 1992.

[4] Galvin, J., McCloghrie, K., and J. Davin, "SNMP Security Protocols", Trusted Information Systems, Inc., Hughes LAN Systems, Inc., MIT Laboratory for Computer Science, RFC 1352, July 1992.

Acknowledgments

RADIUS was originally developed by Livingston Enterprises for their PortMaster series of Network Access Servers.

Chair's Address

The working group can be contacted via the current chair:

John Vollbrecht
Merit Network, Inc.
1071 Beal Ave.
Ann Arbor, MI 48109

EMail: jrv@merit.edu

Author's Address

Questions about this memo can also be directed to:

Steve Willens
Livingston Enterprises
6920 Koll Center Parkway, Suite 220
Pleasanton, CA 94566

EMail: steve@livingston.com

Allan C. Rubens
Merit Network, Inc.
1071 Beal Ave.
Ann Arbor, MI 48109

EMail: acr@merit.edu

William Allen Simpson
Daydreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071

EMail: Bill.Simpson@um.cc.umich.edu

Carl Rigney
Livingston Enterprises
6920 Koll Center Parkway, Suite 220
Pleasanton, CA 94566

EMail: cdr@livingston.com