Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 2, 2009

D. Nelson
Elbrys Networks, Inc.
G. Weber
Individual Contributor

May 31, 2009

Remote Authentication Dial-In User Service (RADIUS) Authorization for Network Access Server (NAS) Management
draft-ietf-radext-management-authorization-07.txt

Status of this Memo

Copyright Notice

Abstract

This document specifies Remote Authentication Dial-In User Service (RADIUS) attributes for authorizing management access to a Network Access Server (NAS). Both local and remote management are supported, with granular access rights and management privileges. Specific provisions are made for remote management via framed management protocols, and for management access over a secure transport protocol.

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 RFC 2119 [RFC2119].

This document uses terminology from RFC 2865 [RFC2865], RFC 2866 [RFC2866] and RFC 5176 [RFC5176].

The term "integrity protection", as used in this document, is *not* the same as "authentication", as used in SNMP. Integrity protection requires the sharing of cryptographic keys, but it does not require authenticated principals. Integrity protection could be used, for example, with anonymous Diffie-Hellman key agreement. In SNMP, the proof of identity of the principals (authentication) is conflated with tamper-resistance of the protected messages (integrity). In this document, we assume that integrity protection and authentication are separate concerns. Authentication is part of the base RADIUS protocol.

SNMP uses the terms "auth" and "noAuth", as well as "priv" and "noPriv". There is no analog to auth or noAuth in this document. In this document, we are assuming that authentication always occurs when it is required, i.e. as a prerequisite to provisioning of access via an Access-Accept packet.

2. Introduction

RFC 2865 [RFC2865] defines the NAS-Prompt (7) and Administrative (6) values of the Service-Type (6) Attribute. Both of these values provide access to the interactive, text-based Command Line Interface (CLI) of the NAS, and were originally developed to control access to the physical console port of the NAS, most often a serial port.

Remote access to the CLI of the NAS has been available in NAS implementations for many years, using protocols such as Telnet, Rlogin and the remote terminal service of the Secure SHell (SSH). In order to distinguish local, physical, console access from remote access, the NAS-Port-Type (61) Attribute is generally included in Access-Request and Access-Accept messages, along with the Service-Type (6) Attribute, to indicate the form of access. A NAS-Port-Type (61) Attribute with a value of of Async (0) is used to signify a local serial port connection, while a value of Virtual (5) is used to signify a remote connection, via a remote terminal protocol. This usage provides no selectivity among the various available remote terminal protocols (e.g. Telnet, Rlogin, SSH, etc.).

Today, it is common for network devices to support more than the two privilege levels for management access provided by the Service-Type (6) Attribute with values of NAS-Prompt (7) (non-privileged) and Administrative (6) (privileged). Also, other management mechanisms may be used, such as Web-based management, Simple Network Management Protocol (SNMP) and NETCONF. To provide support for these additional features, this specification defines attributes for Framed Management protocols, management protocol security, and management access privilege levels.

Remote management via the command line is carried over protocols such as Telnet, Rlogin and the remote terminal service of SSH. Since these protocols are primarily for the delivery of terminal or pseudo-TTY services, the term "Framed Management" is used to describe management protocols supporting techniques other than the command-line. Typically these mechanisms format management information in a binary or textual encoding such as HTML, XML or ASN.1/BER. Examples include Web-based management (HTML over HTTP or HTTPS), NETCONF (XML over SSH or BEEP or SOAP) and SNMP (SMI over ASN.1/BER). Command line interface, menu interface or other text-based (e.g. ASCII or UTF-8) terminal emulation services are not considered to be Framed Management protocols.

3. Overview

To support the authorization and provisioning of Framed Management access to managed entities, this document introduces a new value for the Service-Type (6) Attribute [RFC2865], and one new attribute. The new value for the Service-Type (6) Attribute is Framed-Management (TBA-1), used for remote device management via a Framed Management protocol. The new attribute is Framed-Management-Protocol (TBA-2), the value of which specifies a particular protocol for use in the remote management session.

Two new attributes are introduced in this document in support of granular management access rights or command privilege levels. The Management-Policy-Id (TBA-4) Attribute provides a text string specifying a policy name of local scope, that is assumed to have been pre-provisioned on the NAS. This use of an attribute to specify use of a pre-provisioned policy is similar to the Filter-Id (11) Attribute defined in [RFC2865] Section 5.11.

The local application of the Management-Policy-Id (TBA-4) Attribute within the managed entity may take the form of (a) one of an enumeration of command privilege levels, (b) a mapping into an SNMP Access Control Model, such as the View Based Access Control Model (VACM) [RFC3415], or (c) some other set of management access policy

rules that is mutually understood by the managed entity and the remote management application. Examples are given in Section 8.

The Management-Privilege-Level (TBA-5) Attribute contains an integer-valued management privilege level indication. This attribute serves to modify or augment the management permissions provided by the NAS-Prompt (7) value of the Service-Type (6) Attribute, and thus applies to CLI management.

To enable management security requirements to be specified, the Management-Transport-Protection (TBA-3) Attribute is introduced. The value of this attribute indicates the minimum level of secure transport protocol protection required for the provisioning of NAS-Prompt (7), Administrative (6) or Framed-Management (TBA-1) service.

4. Domain of Applicability

Most of the RADIUS Attributes defined in this document have broad applicability for provisioning local and remote management access to NAS devices. However, those attributes that provision remote access over framed management protocols and over secure transports have special considerations. This document does not specify details of the integration of these protocols with a RADIUS client in the NAS implementation. However, there are functional requirements for correct application of framed management protocols and/or secure transport protocols that will limit the selection of such protocols that can be considered for use with RADIUS. Since the RADIUS user credentials are typically obtained by the RADIUS client from the secure transport protocol server or the framed management protocol server, the protocol, and its implementation in the NAS, MUST support forms of credentials that are compatible with the authentication methods supported by RADIUS.

RADIUS currently supports the following user authentication methods, although others may be added in the future:

- Password (RFC 2865)
- CHAP (RFC 2865)
- ARAP (RFC 2869)
- EAP (RFC 2869, RFC 3579)
- HTTP Digest (RFC 5090)

The remote management protocols selected for use the RADIUS remote NAS management sessions, for example those described in Section 6.1, and the secure transport protocols selected to meet the protection requirements, as described in Section 6.2, obviously need to support user authentication methods that are compatible with those that exist

in RADIUS. The RADIUS authentication methods most likely usable with these protocols are Password, CHAP and possibly HTTP Digest, with Password being the distinct common denominator. There are many secure transports that support other, more robust, authentication mechanisms, such as public key. RADIUS has no support for public key authentication, except within the context of an EAP Method. The applicability statement for EAP indicates that it is not intended for use as an application-layer authentication mechanism, so its use with the mechanisms described in this document is NOT RECOMMENDED. In some cases, Password may be the only compatible RADIUS authentication method available.

5. New Values for Existing RADIUS Attributes

5.1. Service-Type

The Service-Type (6) Attribute is defined in Section 5.6 of RFC 2865 [RFC2865]. This document defines a new value of the Service-Type Attribute, as follows:

(TBA-1) Framed-Management

The semantics of the Framed-Management service are as follows:

Framed-Management	A framed management protocol session should be started on the NAS.

6. New RADIUS Attributes

This document defines four new RADIUS attributes related to management authorization.

6.1. Framed-Management-Protocol

The Framed-Management-Protocol (TBA-2) Attribute indicates the application-layer management protocol to be used for Framed Management access. It MAY be used in both Access-Request and Access-Accept packets. This attribute is used in conjunction with a Service-Type (6) Attribute with the value of Framed-Management (TBA-1).

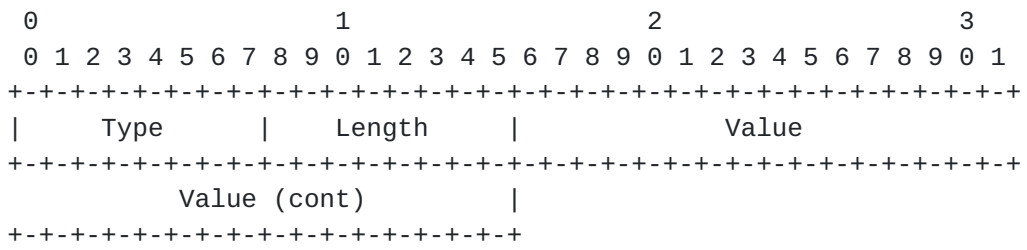
It is RECOMMENDED that the NAS include an appropriately valued Framed-Management-Protocol (TBA-2) Attribute in an Access-Request packet, indicating the type of management access being requested. It is further RECOMMENDED that the NAS include a Service-Type (6) Attribute with the value Framed-Management (TBA-1) in the same

Access-Request packet. The RADIUS server MAY use these attributes as a hint in making its authorization decision.

The RADIUS server MAY include a Framed-Management-Protocol (TBA-2) Attribute in an Access-Accept packet that also includes a Service-Type (6) Attribute with a value of Framed-Management (TBA-1), when the RADIUS Server chooses to enforce a management access policy for the authenticated user that dictates one form of management access in preference to others.

When a NAS receives a Framed-Management-Protocol (TBA-2) Attribute in an Access-Accept packet, it MUST deliver that specified form of management access or disconnect the session. If the NAS does not support the provisioned management application-layer protocol, or the management access protocol requested by the user does not match that of the Framed-Management-Protocol (TBA-2) Attribute in the Access-Accept packet, the NAS MUST treat the Access-Accept packet as if it had been an Access-Reject.

A summary of the Framed-Management-Protocol (TBA-2) Attribute format is shown below. The fields are transmitted from left to right.



Type

(TBA-2) for Framed-Management-Protocol.

Length

6

Value

The Value field is a four octet enumerated value.

1	SNMP
2	Web-based
3	NETCONF
4	FTP
5	TFTP
6	SFTP
7	RCP
8	SCP

All other values are reserved for IANA allocation subject to the provisions of Section 11.

The acronyms used in the above table expand as follows:

- SNMP: Simple Network Management Protocol. [RFC3411], [RFC3412], [RFC3413], [RFC3414], [RFC3415], [RFC3416], [RFC3417], [RFC3418]

- Web-based: Use of an embedded web server in the NAS for management via a generic web browser client. The interface presented to the administrator may be graphical, tabular or textual. The protocol is HTML over HTTP. The protocol may optionally be HTML over HTTPS, i.e. using HTTP over TLS. [HTML] [RFC2616]

- NETCONF: Management via the NETCONF protocol using XML over supported transports (e.g. SSH, BEEP, SOAP). As secure transport profiles are defined for NETCONF, the list of transport options may expand. [RFC4741], [RFC4742], [RFC4743], [RFC4744]

- FTP: File Transfer Protocol, used to transfer configuration files to and from the NAS. [RFC0959]

- TFTP: Trivial File Transfer Protocol, used to transfer configuration files to and from the NAS. [RFC1350]

- SFTP: SSH File Transfer Protocol, used to securely transfer configuration files to and from the NAS. SFTP uses the services of SSH. [SFTP] See also Section 3.7, "SSH and File Transfers" of [SSH]. Additional information on the "sftp" program may typically be found in the online documentation ("man" pages) of Unix systems.

- RCP: Remote CoPy file copy utility (Unix-based), used to transfer configuration files to and from the NAS. See Section 3.7, "SSH and File Transfers" of [SSH]. Additional information on the "rcp" program may typically be found in the online documentation ("man" pages) of Unix systems.

- SCP: Secure CoPy file copy utility (Unix-based), used to transfer configuration files to and from the NAS. The "scp" program is a simple wrapper around SSH. It's basically a patched BSD Unix "rcp" which uses ssh to do the data transfer (instead of using "rcmd"). See Section 3.7, "SSH and File Transfers" of [SSH]. Additional information on the "scp" program may typically be found in the online documentation ("man" pages) of Unix systems.

6.2. Management-Transport-Protection

The Management-Transport-Protection (TBA-3) Attribute specifies the minimum level of protection that is required for a protected transport used with the framed or non-framed management access session. The protected transport used by the NAS MAY provide a greater level of protection, but MUST NOT provide a lower level of protection.

When a secure form of non-framed management access is specified, it means that the remote terminal session is encapsulated in some form of protected transport, or tunnel. It may also mean that an explicit secure mode of operation is required, when the framed management protocol contains an intrinsic secure mode of operation. The Management-Transport-Protection (TBA-3) Attribute does not apply to CLI access via a local serial port, or other non-remote connection.

When a secure form of Framed Management access is specified, it means that the application-layer management protocol is encapsulated in some form of protected transport, or tunnel. It may also mean that

an explicit secure mode of operation is required, when the Framed Management protocol contains an intrinsic secure mode of operation.

A value of "No Protection (1)" indicates that a secure transport protocol is not required, and that the NAS SHOULD accept a connection over any transport associated with the application-layer management protocol. The definitions of management application to transport bindings are defined in the relevant documents that specify those management application protocols. The same "No Protection" semantics are conveyed by omitting this attribute from an Access-Accept packet.

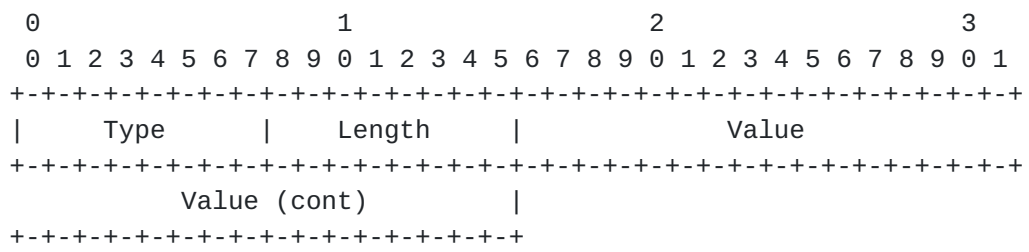
Specific protected transport protocols, cipher suites, key agreement methods, or authentication methods are not specified by this attribute. Such provisioning is beyond the scope of this document.

It is RECOMMENDED that the NAS include an appropriately valued Management-Transport-Protection (TBA-3) Attribute in an Access-Request packet, indicating the level of transport protection for the management access being requested, when that information is available to the RADIUS client. The RADIUS server MAY use this attribute as a hint in making its authorization decision.

The RADIUS server MAY include a Management-Transport-Protection (TBA-3) Attribute in an Access-Accept packet that also includes a Service-Type (6) Attribute with a value of Framed-Management (TBA-1), when the RADIUS Server chooses to enforce an management access security policy for the authenticated user that dictates a minimum level of transport security.

When a NAS receives a Management-Transport-Protection (TBA-3) Attribute in an Access-Accept packet, it MUST deliver the management access over a transport with equal or better protection characteristics or disconnect the session. If the NAS does not support protected management transport protocols, or the level of protection available does not match that of the Management-Transport-Protection (TBA-3) Attribute in the Access-Accept packet, the NAS MUST treat the response packet as if it had been an Access-Reject.

A summary of the Management-Transport-Protection (TBA-3) Attribute format is shown below. The fields are transmitted from left to right.



Type

(TBA-3) for Management-Transport-Protection.

Length

6

Value

The Value field is a four octet enumerated value.

1	No-Protection
2	Integrity-Protection
3	Integrity-Confidentiality-Protection

All other values are reserved for IANA allocation subject to the provisions of Section 11.

The names used in the above table are elaborated as follows:

- No-Protection: No transport protection is required. Accept connections via any supported transport.

- Integrity-Protection: The management transport MUST provide Integrity Protection, i.e. protection from unauthorized modification, using a cryptographic checksum.

- Integrity-Confidentiality-Protection: The management transport MUST provide both Integrity Protection and Confidentiality Protection, i.e. protection from unauthorized modification, using a cryptographic checksum, and protection from unauthorized disclosure, using encryption.

The configuration or negotiation of acceptable algorithms, modes and credentials for the cryptographic protection mechanisms used in implementing protected management transports is outside the scope of this document. Many such mechanisms have standardized methods of configuration and key management.

6.3. Management-Policy-Id

The Management-Policy-Id (TBA-4) Attribute indicates the name of the management access policy for this user. Zero or one Management-Policy-Id (TBA-4) Attributes MAY be sent in an Access-Accept packet. Identifying a policy by name allows the policy to be used on different NASes without regard to implementation details.

Multiple forms of management access rules may be expressed by the underlying named policy, the definition of which is beyond the scope of this document. The management access policy MAY be applied contextually, based on the nature of the management access method. For example, some named policies may only be valid for application to NAS-Prompt (7) services and some other policies may only be valid for SNMP.

The management access policy named in this attribute, received in an Access-Accept packet, MUST be applied to the session authorized by the Access-Accept. If the NAS supports this attribute, but the policy name is unknown, or if the RADIUS client is able to determine that the policy rules are incorrectly formatted, the NAS MUST treat the Access-Accept packet as if it had been an Access-Reject.

No precedence relationship is defined for multiple occurrences of the Management-Policy-Id (TBA-4) Attribute. NAS behavior in such cases is undefined. Therefore, two or more occurrences of this attribute SHOULD NOT be included in an Access-Accept or CoA-Request. In the absence of further specification defining some sort of precedence relationship, it is not possible to guarantee multi-vendor interoperability when using multiple instances of this attribute in a single Access-Accept or CoA-Request packet.

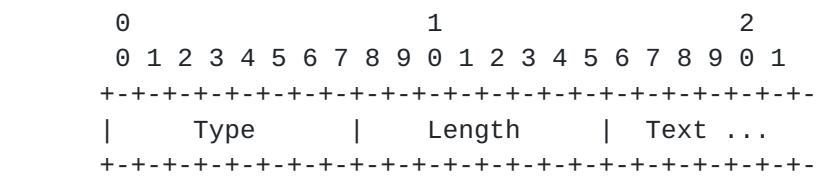
The content of the Management-Policy-Id (TBA-4) Attribute is expected to be the name of a management access policy of local significance to the NAS, within a namespace of significance to the NAS. In this regard, the behavior is similar to that for the Filter-Id (11) Attribute. The policy names and rules are committed to the local configuration data-store of the NAS, and are provisioned by means beyond the scope of this document, such as via SNMP, NETCONF or CLI.

The namespace used in the Management-Policy-Id (TBA-4) Attribute is simple and monolithic. There is no explicit or implicit structure or hierarchy . For example, in the text string "example.com", the "." (period or dot) is just another character. It is expected that text string matching will be performed without parsing the text string into any sub-fields.

Overloading or subdividing this simple name with multi-part

specifiers (e.g. Access=remote, Level=7) is likely to lead to poor multi-vendor interoperability and SHOULD NOT be utilized. If a simple, unstructured policy name is not sufficient, it is RECOMMENDED that a Vendor Specific (26) Attribute be used instead, rather than overloading the semantics of Management-Policy-Id.

A summary of the Management-Policy-Id (TBA-4) Attribute format is shown below. The fields are transmitted from left to right.



Type

(TBA-4) for Management-Policy-Id.

Length

>= 3

Text

The Text field is one or more octets, and its contents are implementation dependent. It is intended to be human readable and the contents MUST NOT be parsed by the receiver; the contents can only be used to look up locally defined policies. It is RECOMMENDED that the message contain UTF-8 encoded 10646 [RFC3629] characters.

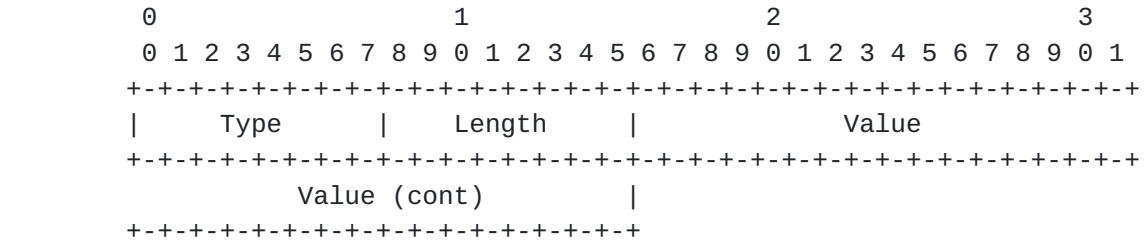
6.4. Management-Privilege-Level

The Management-Privilege-Level (TBA-5) Attribute indicates the integer-valued privilege level to be assigned for management access for the authenticated user. Many NASes provide the notion of differentiated management privilege levels denoted by an integer value. The specific access rights conferred by each value are implementation dependent. It MAY be used in both Access-Request and Access-Accept packets.

The mapping of integer values for this attribute to specific collections of management access rights or permissions on the NAS is vendor and implementation specific. Such mapping is often a user configurable feature. It's RECOMMENDED that greater numeric values imply greater privilege. However, it would be a mistake to assume that this recommendation always holds.

The management access level indicated in this attribute, received in an Access-Accept packet, MUST be applied to the session authorized by the Access-Accept. If the NAS supports this attribute, but the privilege level is unknown, the NAS MUST treat the Access-Accept packet as if it had been an Access-Reject.

A summary of the Management-Privilege-Level (TBA-5) Attribute format is show below. The fields are transmitted from left to right.



Type

(TBA-5) for Management-Privilege-Level.

Length

6

Value

The Value field is a four octet Integer, denoting a management privilege level.

It is RECOMMENDED to limit use of the Management-Privilege-Level (TBA-5) Attribute to sessions where the Service-Type (6) Attribute has a value of NAS-Prompt (7) (not Administrative). Typically, NASes treat NAS-Prompt as the minimal privilege CLI service and Administrative as full privilege. Using the Management-Privilege-Level (TBA-5) Attribute with a Service-Type (6) Attribute having a value of NAS-Prompt (7) will have the effect of increasing the minimum privilege level. Conversely, it is NOT RECOMMENDED to use this attribute with a Service-Type (6) Attribute with a value of of Administrative (6), which may require decreasing the maximum privilege level.

It is NOT RECOMMENDED to use the Management-Privilege-Level (TBA-5) Attribute in combination with a Management-Policy-Id (TBA-4) Attribute or for management access methods other than interactive CLI. The behavior resulting from such an overlay of management

access control provisioning is not defined by this document, and in the absence of further specification is likely to lead to unexpected behaviors, especially in multi-vendor environments.

7. Use with Dynamic Authorization

It is entirely OPTIONAL for the NAS management authorization attributes specified in this document to be used in conjunction with Dynamic Authorization extensions to RADIUS [RFC5176]. When such usage occurs, those attributes MAY be used as listed in the Table of Attributes in Section 10.

Some guidance on how to identify existing management sessions on a NAS for the purposes of Dynamic Authorization is useful. The primary session identifiers SHOULD be User-Name (1) and Service-Type (6). To accommodate instances when that information alone does not uniquely identify a session, a NAS supporting Dynamic Authorization SHOULD maintain one or more internal session identifiers that can be represented as RADIUS Attributes. Examples of such attributes include Acct-Session-Id (44), Acct-Multi-Session-Id (50), NAS-Port (5) or NAS-Port-Id (87). In the case of a remote management session, common identifier values might include things such as the remote IP address and remote TCP port number, or the file descriptor value for use with the open socket. Any such identifier is obviously transient in nature, and implementations SHOULD take care to avoid and/or properly handle duplicate or stale values.

In order for the session identification attributes to be available to the Dynamic Authorization Client, a NAS supporting Dynamic Authorization for management sessions SHOULD include those session identification attributes in the Access-Request message for each such session. Additional discussion of session identification attribute usage may be found in Section 3 of [RFC5176].

8. Examples of attribute groupings

1. Unprotected CLI access, via the local console, to the "super-user" access level:

   * Service-Type (6) = Administrative (6)
   * NAS-Port-Type (61) = Async (0)
   * Management-Transport-Protection (TBA-3) = No-Protection (1)

2. Unprotected CLI access, via a remote console, to the "super-user" access level:

* Service-Type (6) = Administrative (6)
* NAS-Port-Type (61) = Virtual (5)
* Management-Transport-Protection (TBA-3) = No-Protection (1)

3. CLI access, via a fully-protected secure remote terminal service to the non-privileged user access level:

   * Service-Type (6) = NAS-Prompt (7)
   * NAS-Port-Type (61) = Virtual (5)
   * Management-Transport-Protection (TBA-3) = Integrity-Confidentiality-Protection (3)

4. CLI access, via a fully-protected secure remote terminal service, to a custom management access level, defined by a policy:

   * Service-Type (6) = NAS-Prompt (7)
   * NAS-Port-Type (61) = Virtual (5)
   * Management-Transport-Protection (TBA-3) = Integrity-Confidentiality-Protection (3)
   * Management-Policy-Id (TBA-4) = "Network Administrator"

5. CLI access, via a fully-protected secure remote terminal service, with a management privilege level of 15:

   * Service-Type (6) = NAS-Prompt (7)
   * NAS-Port-Type (61) = Virtual (5)
   * Management-Transport-Protection (TBA-3) = Integrity-Confidentiality-Protection (3)
   * Management-Privilege-Level (TBA-5) = 15

6. SNMP access, using an Access Control Model specifier, such as a custom VACM View, defined by a policy:

   * Service-Type (6) = Framed-Management (TBA-1)
   * NAS-Port-Type (61) = Virtual (5)
   * Framed-Management-Protocol (TBA-2) = SNMP (1)
   * Management-Policy-Id (TBA-4) = "SNMP Network Administrator View"

   There is currently no standardized way of implementing this management policy mapping within SNMP. Such mechanisms are the topic of current research.

7. SNMP fully-protected access:

   * Service-Type (6) = Framed-Management (TBA-1)

   * NAS-Port-Type (61) = Virtual (5)
   * Framed-Management-Protocol (TBA-2) = SNMP (1)
   * Management-Transport-Protection (TBA-3) = Integrity-
      Confidentiality-Protection (3)

8. Web (HTTP/HTML) access:

   * Service-Type (6) = Framed-Management (TBA-1)
   * NAS-Port-Type (61) = Virtual (5)
   * Framed-Management-Protocol (TBA-2) = Web-based (2)

9. Secure web access, using a custom management access level,
    defined by a policy:

   * Service-Type (6) = Framed-Management (TBA-1)
   * NAS-Port-Type (61) = Virtual (5)
   * Framed-Management-Protocol (TBA-2) = Web-based (2)
   * Management-Transport-Protection (TBA-3) = Integrity-
      Confidentiality-Protection (3)
   * Management-Policy-Id (TBA-4) = "Read-only web access"

9. Diameter Translation Considerations

When used in Diameter, the attributes defined in this specification can be used as Diameter AVPs from the Code space 1-255 (RADIUS attribute compatibility space). No additional Diameter Code values are therefore allocated. The data types and flag rules for the attributes are as follows:

		AVP Flag rules				
				SHOULD	MUST	
Attribute Name	Value Type	MUST	MAY	NOT	NOT	Encr
Service-Type (new value)	Enumerated	M	P		V	Y
Framed-Management-Protocol	Enumerated	M	P		V	Y
Management-Transport-Protection	Enumerated	M	P		V	Y
Management-Policy-Id	UTF8String	M	P		V	Y
Management-Privilege-Level	Integer	M	P		V	Y

The attributes in this specification have no special translation requirements for Diameter to RADIUS or RADIUS to Diameter gateways; they are copied as is, except for changes relating to headers, alignment, and padding. See also [RFC3588] Section 4.1 and [RFC4005] Section 9.

What this specification says about the applicability of the attributes for RADIUS Access-Request packets applies in Diameter to AA-Request [RFC4005].

What is said about Access-Accept applies in Diameter to AA-Answer messages that indicate success.

10. Table of Attributes

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

Access Messages

Request	Accept	Reject	Challenge	#	Attribute
0-1	0-1	0	0	TBA-2	Framed-Management-Protocol
0-1	0-1	0	0	TBA-3	Management-Transport-Protection
0	0-1	0	0	TBA-4	Management-Policy-Id
0	0-1	0	0	TBA-5	Management-Privilege-Level

Accounting Messages

Request	Response	#	Attribute
0-1	0	TBA-2	Framed-Management-Protocol
0-1	0	TBA-3	Management-Transport-Protection
0-1	0	TBA-4	Management-Policy-Id
0-1	0	TBA-5	Management-Privilege-Level

Change-of-Authorization Messages

Request	ACK	NAK	#	Attribute
0	0	0	TBA-2	Framed-Management-Protocol
0	0	0	TBA-3	Management-Transport-Protection
0-1	0	0	TBA-4	Management-Policy-Id (Note 1)
0-1	0	0	TBA-5	Management-Privilege-Level (Note 1)

Disconnect Messages Request	ACK	NAK	#	Attribute
0	0	0	TBA-2	Framed-Management-Protocol
0	0	0	TBA-3	Management-Transport-Protection
0	0	0	TBA-4	Management-Policy-Id
0	0	0	TBA-5	Management-Privilege-Level

(Note 1) When included within a CoA-Request, these attributes represent an authorization change request. When one of these attributes is omitted from a CoA-Request, the NAS assumes that the attribute value is to remain unchanged. Attributes included in a CoA-Request replace all existing values of the same attribute(s).

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.

11. IANA Considerations

This document contains placeholders ("TBA-n") for assigned numbers within the RADIUS Attributes Types registry (http://www.iana.org/assignments/radius-types), to be assigned by IANA at the time this document should be published as an RFC.

- New enumerated value for the existing Service-Type Attribute:
  - Framed-Management (TBA-1)
- New RADIUS Attribute Types:
  - Framed-Management-Protocol (TBA-2)
  - Management-Transport-Protection (TBA-3)
  - Management-Policy-Id (TBA-4)
  - Management-Privilege-Level (TBA-5)

The enumerated values of the newly assigned RADIUS Attribute Types as defined in this document are to be assigned at the same time as the new Attribute Types.

For the Framed-Management-Protocol Attribute:

1	SNMP
2	Web-based
3	NETCONF
4	FTP
5	TFTP
6	SFTP
7	RCP
8	SCP

For the Management-Transport-Protection Attribute:

1	No-Protection
2	Integrity-Protection
3	Integrity-Confidentiality-Protection

Assignments of additional enumerated values for the RADIUS attributes defined in this document are to be processed as described in [RFC3575], subject to the additional requirement of a published specification.

12. Security Considerations

12.1. General Considerations

This specification describes the use of RADIUS and Diameter for purposes of authentication, authorization and accounting for management access to devices within networks. RADIUS threats and security issues for this application are described in [RFC3579] and [RFC3580]; security issues encountered in roaming are described in [RFC2607]. For Diameter, the security issues relating to this application are described in [RFC4005] and [RFC4072].

This document specifies new attributes that can be included in existing RADIUS packets, which may be protected as described in [RFC3579] and [RFC5176]. In Diameter, the attributes are protected as specified in [RFC3588]. See those documents for a more detailed description.

The security mechanisms supported in RADIUS and Diameter are focused on preventing an attacker from spoofing packets or modifying packets in transit. They do not prevent an authorized RADIUS/Diameter server or proxy from inserting attributes with malicious intent.

A legacy NAS may not recognize the attributes in this document that supplement the provisioning of CLI management access. If the value of the Service-Type Attribute is NAS-Prompt or Administrative, the legacy NAS may silently discard such attributes, while permitting the

user to access the CLI management interface(s) of the NAS. This can lead to users improperly receiving authorized management access to the NAS, or access with greater levels of access rights than were intended. RADIUS servers SHOULD attempt to ascertain whether or not the NAS supports these attributes before sending them in an Access-Accept provisioning CLI access.

It is possible that certain NAS implementations may not be able to determine the protection properties of the underlying transport protocol as specified by the Management-Transport-Protection Attribute. This may be a limitation of the standard application programming interface of the underlying transport implementation or of the integration of the transport into the NAS implementation. In either event, NASes conforming to this specification, which cannot determine the protection state of the remote management connection MUST treat an Access-Accept message containing a Management-Transport-Protection Attribute containing a value other than No-Protection (1) as if it were an Access-Reject message, unless specifically overridden by local policy configuration.

Use of the No-Protection (1) option for the Management-Transport-Protection (TBA-3) Attribute is NOT RECOMMENDED in any deployment where secure management or configuration is required.

12.2. RADIUS Proxy Operation Considerations

The device management access authorization attributes presented in this document present certain considerations when used in RADIUS proxy environments. These considerations are not different from those that exist in RFC 2865 [RFC2865] with respect to the Service-Type Attribute values of Administrative and NAS-Prompt.

Most RADIUS proxy environments are also multi-party environments. In multi-party proxy environments it is important to distinguish which entities have the authority to provision management access to the edge devices, i.e. NASes, and which entities only have authority to provision network access services of various sorts.

It may be important that operators of the NAS are able to ensure that access to the CLI, or other management interfaces of the NAS, is only provisioned to their own employees or contractors. One way for the NAS to enforce this requirement is to use only local, non-proxy RADIUS servers for management access requests. Proxy RADIUS servers could be used for non-management access requests, based on local policy. This "bifurcation" of RADIUS authentication and authorization is a simple case of separate administrative realms. The NAS may be designed so as to maintain separate lists of RADIUS servers for management AAA use and for non-management AAA use.

An alternate method of enforcing this requirement would be for the first-hop RADIUS proxy server, operated by the owner of the NAS, to filter out any RADIUS attributes that provision management access rights that originate from "up-stream" proxy servers not operated by the NAS owner. Access-Accept messages that provision such locally un-authorized management access MAY be treated as if they were an Access-Reject by the first-hop proxy server.

An additional exposure present in proxy deployments is that sensitive user credentials, e.g passwords, are likely to be available in cleartext form at each of the proxy servers. Encrypted or hashed credentials are not subject to this risk, but password authentication is a very commonly used mechanism for management access authentication, and in RADIUS passwords are only protected on a hop-by-hop basis. Malicious proxy servers could misuse this sensitive information.

These issues are not of concern when all the RADIUS servers, local and proxy, used by the NAS are under the sole administrative control of the NAS owner.

13. Acknowledgments

Many thanks to all reviewers, including Bernard Aboba, Alan DeKok, David Harrington, Mauricio Sanchez, Juergen Schoenwaelder, Hannes Tschofenig, Barney Wolff and Glen Zorn.

14. References

14.1. 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.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

14.2. Informative References

[HTML] Raggett, D., Le Hors, A., and I. Jacobs, "The HTML 4.01 Specification, W3C", December 1999.

[RFC0959] Postel, J. and J. Reynolds, "File Transfer Protocol", STD 9, RFC 959, October 1985.

[RFC1350] Sollins, K., "The TFTP Protocol (Revision 2)", STD 33, RFC 1350, July 1992.

[RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

[RFC3412] Case, J., Harrington, D., Presuhn, R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3412, December 2002.

[RFC3413] Levi, D., Meyer, P., and B. Stewart, "Simple Network Management Protocol (SNMP) Applications", STD 62, RFC 3413, December 2002.

[RFC3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, December 2002.

[RFC3415] Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3415, December 2002.

[RFC3416] Presuhn, R., "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3416, December 2002.

[RFC3417] Presuhn, R., "Transport Mappings for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3417, December 2002.

[RFC3418] Presuhn, R., "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", STD 62,

RFC 3418, December 2002.

[RFC3575] Aboba, B., "IANA Considerations for RADIUS (Remote Authentication Dial In User Service)", RFC 3575, July 2003.

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3580] Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, September 2003.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC4005] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[RFC4072] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

[RFC4741] Enns, R., "NETCONF Configuration Protocol", RFC 4741, December 2006.

[RFC4742] Wasserman, M. and T. Goddard, "Using the NETCONF Configuration Protocol over Secure SHell (SSH)", RFC 4742, December 2006.

[RFC4743] Goddard, T., "Using NETCONF over the Simple Object Access Protocol (SOAP)", RFC 4743, December 2006.

[RFC4744] Lear, E. and K. Crozier, "Using the NETCONF Protocol over the Blocks Extensible Exchange Protocol (BEEP)", RFC 4744, December 2006.

[RFC5176] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 5176, January 2008.

[SFTP] Galbraith, J. and O. Saarenmaa, "SSH File Transfer Protocol", July 2006.

[SSH] Barrett, D., Silverman, R., and R. Byrnes, "SSH, the

Secure Shell: The Definitive Guide, Second Edition,
O'Reilly and Associates", May 2005.

Authors' Addresses

David B. Nelson
Elbrys Networks, Inc.
75 Rochester Avenue, Unit 3
Portsmouth, NH 03801
USA

Email: d.b.nelson@comcast.net

Greg Weber
Individual Contributor
Knoxville, TN 37932
USA

Email: gdweber@gmail.com