Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 8, 2008

D. Nelson
Elbrys Networks, Inc.
G. Weber
Cisco Systems, Inc.

July 7, 2007

Remote Authentication Dial-In User Service (RADIUS) Authorization for Network Access Server (NAS) Management
draft-nelson-radius-management-authorization-05.txt

Abstract

This document describes Remote Authentication Dial-In User Service (RADIUS) attributes for the authorization and service provisioning of local and remote management of embedded systems and other managed entities, generally referred to as Network Access Servers (NASes). Specific provisions are made for remote management via framed management protocols, and for more granular levels of access rights

and management privileges.

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] and RFC 2866 [RFC2866].

2. Introduction and Rationale

The remote management Service-Types defined in RFC 2865 [RFC2865] include NAS-Prompt and Administrative. Both of these services provide access to the interactive, ASCII-text, Command Line Interface (CLI) of the managed entity. Current deployments of network equipment include in the managed entity non-CLI, framed-protocol forms of management, such as HTTP, HTTPS, and SNMP. In addition, network devices often support more privilege levels for management access than the two levels supported by NAS-Prompt (non-privileged) and Administrative (privileged). To address these issues, attributes for framed management protocols, management protocol security levels, and management access privilege levels are described.

3. Provisions for Framed Management

Framed Management means management of an entity by means of a non-interactive, non-CLI-style method. The management information is typically formatted in a binary or textual protocol, such as HTTP or SNMP. While remote management by interactive CLI sessions are carried over protocols, such as Telnet, Rlogin, and SSH, these protocols are primarily for the delivery of terminal, or pseudo-TTY services. Command Line Interface, Menu Interface, or other ASCII (UTF-8) terminal emulation interfaces are not considered to be Framed Management protocols, as used in this document. Examples of Framed Management protocols include HTTP, HTTPS, and SNMP.

To support the authorization and provisioning of Framed Management access to managed entities, this document introduces a new value for the Service-Type attribute [RFC2865], and one new attribute. The new value for the Service-Type attribute is Framed-Management. The definition of this service is the provisioning of remote device management via a Framed Management protocol, as described in this section. The new attribute is Framed-Management-Protocol, the value of which specifies a particular protocol for use in the remote management session.

4. Provisions for Granular Management Access Rights

One new attribute is introduced in this document in support of granular management access rights or command privilege levels. The Management-Policy-Id attribute is used to contain the name of a management access rights policy of local scope. This attribute functions similarly to Filter-ID. It is a string variable containing policy name of local scope. The provisioning of the rules invoked by application of this management policy is by means outside the scope of this document, such as by MIB objects.

The local application of the Management-Policy-Id within the managed entity may take the form of (a) one of an enumeration of command privilege levels, (b) a mapping into an SNMP View Based Access Control Method (VACM) table [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.

5. Provisions for Secure CLI Management Access

To provide for the authorization and provisioning of secure Command Line Access management methods, via a secure transport protocol, one new attribute is introduced in this document, Transport-Protocol. The value of this attributes is an enumeration of secure transport protocols that may be required for the provisioning of NAS-Prompt, Administrative or Framed-Management service.

6. New Values for Existing RADIUS Attributes

6.1. Service-Type

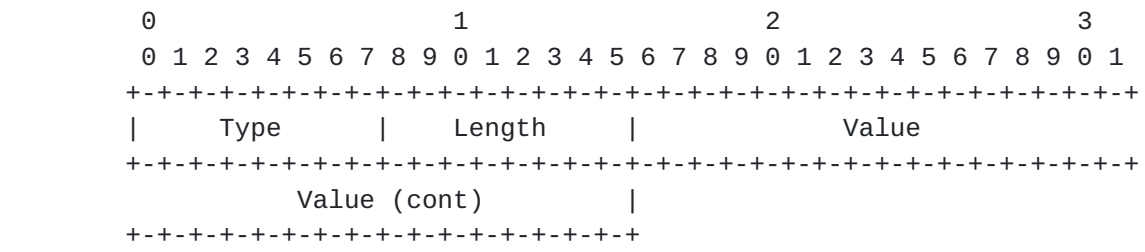
This document defines one new value for an existing RADIUS attribute. The Service-Type attribute is defined in Section 5.6 of RFC 2865 [RFC2865], as follows:

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

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

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

The fields are transmitted from left to right.



Type

6 for Service-Type.

Length

6 Value

The Value field is four octets.

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

(TBA) Framed-Management

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

Framed-Management	A framed protocol session should be started for a remote management user or application, such as HTTP or SNMP.

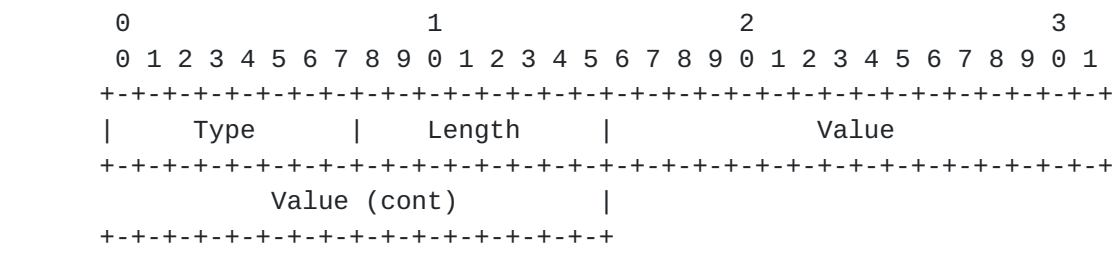
7. New RADIUS Attributes

This document defines three new RADIUS attributes related to remote management authorization.

7.1. Framed-Management-Protocol

The Framed-Management-Protocol attribute indicates the protocol to be used for framed management access. It MAY be used in both Access-Request and Access-Accept packets.

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



Type

(TBA) for Framed-Management-Protocol.

Length

6

Value

The Value field is four octets.

1	SNMP-Transport-Model
2	HTTP
3	HTTPS/TLS
4	SFTP (via SSH)
5	SCP (via SSH)

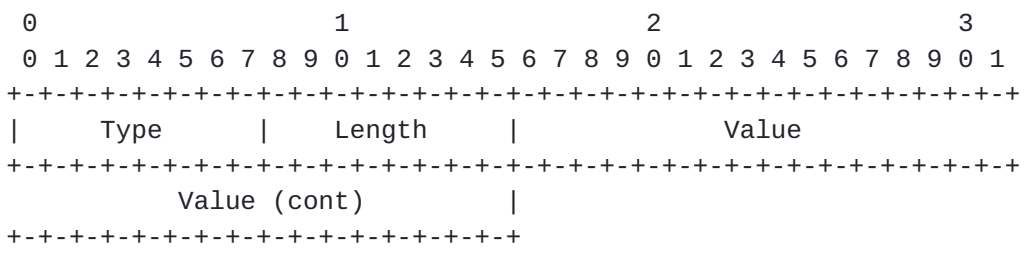
7.2. Transport-Protocol

The Transport-Protocol attribute indicates the mandated secure transport protocol for use with framed- or non-framed management access sessions. It MAY be used in both Access-Request and Access-Accept packets. This attribute MAY be used in conjunction with other managemetn access provisioning attributes.

When a secure form of Non-Framed management access is specified, for example Telnet carried within Secure Shell (SSH), for access to the interactive CLI prompt of the NAS, it generally means that the terminal emulation session is encapsulated in some form of protected application transport, or tunnel. It may also mean that an explicit secure mode of operation is required, when the terminal emulation access protocol contains an intrinsic secure mode of operation.

This attribute may be used with Framed access for SNMP secure Tranport Models to specify a specific transport protocol.

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



Type

(TBA) for Transport-Protocol.

Length

6

Value

The Value field is four octets.

1	None
2	Secure Shell (SSH)
3	Transport Layer Security (TLS)

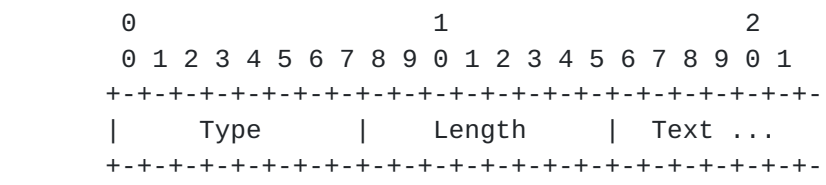
7.3. Management-Policy-Id

The Management-Policy-Id attribute indicates the name of the management access policy for this user. Zero or more Management-Policy-Id 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 services and some other policies may only be valid for application to SMNPv3 services.

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 policy name is unknown, or the policy rules are incorrectly formatted, the NAS SHOULD treat the packet as if it had been an Access-Reject.

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



Type

(TBA) 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 MUST NOT affect operation of the protocol. It is recommended that the message contain UTF-8 encoded 10646 [RFC2279] characters.

8. Examples of attribute groupings

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

   * Service-Type (6) = Administrative (6)
   * Transport-Protocol (xx) = None (1)

2. CLI access, via SSH/telnet, to the non-privileged user access level:

   * Service-Type (6) = NAS-Prompt (7)
   * Transport-Protocol (xx) = SSH (2)

3. CLI access, via SSH/telnet, to a custom management access level, defined by a policy:

   * Service-Type (6) = NAS-Prompt (7)
   * Transport-Protocol (xx) = SSH (2)
   * Management-Policy-Id (xx) = "Network Administrator"

4. SNMPv3 access, using a custom VACM View, defined by a policy:

   * Service-Type (6) = Framed-Management (xx)

   * Framed-Management-Protocol (xx) = SNMP-Transport-Model (3)
   * Management-Policy-Id (xx) = "SNMP Network Administrator View"

5. SNMP secure Transport Model access, using the Secure Shell Transport Model:

   * Service-Type (6) = Framed-Management (xx)
   * Framed-Management-Protocol (xx) = SNMP-Transport-Model (3)
   * Transport-Protocol (xx) = SSH (2)

6. Web (HTTP) access:

   * Service-Type (6) = Framed-Management (xx)
   * Framed-Management-Protocol (xx) = HTTP (4)

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

   * Service-Type (6) = Framed-Management (xx)
   * Framed-Management-Protocol (xx) = HTTPS (5)
   * Transport-Protocol (xx) = TLS (3)
   * Management-Policy-Id (xx) = "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				
Attribute Name	Value Type	MUST	MAY	SHLD NOT	MUST NOT	Encr
Service-Type (new value)						
	Enumerated	M	P		V	Y
Framed-Management-Protocol						
	Enumerated	M	P		V	Y
Transport-Protocol						
	Enumerated	M	P		V	Y
Management-Policy-Id						
	UTF8String	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] or Diameter-EAP-Request [RFC4072]. What is said about Access-Challenge applies in Diameter to AA-Answer [RFC4005] or Diameter-EAP-Answer [RFC4072] with Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH.

What is said about Access-Accept applies in Diameter to AA-Answer or Diameter-EAP-Answer messages that indicate success. Similarly, what is said about RADIUS Access-Reject packets applies in Diameter to AA-Answer or Diameter-EAP-Answer messages that indicate failure.

What is said about COA-Request applies in Diameter to Re-Auth-Request [RFC4005].

10. Proxy Operation Considerations

The device management access authorization attributes presented in this document present certain considerations when used in 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 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 are 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 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.

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.

11. 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-Request	Accept	Reject	Challenge	#	Attribute
0-1	0-1	0	0	TBA	Framed-Management-Protocol
0-1	0-1	0	0	TBA	Transport-Protocol
0	0+	0	0	TBA	Management-Policy-Id

Accounting-Request	Response	#	Attribute
0-1	0	TBA	Framed-Management-Protocol
0-1	0	TBA	Transport-Protocol
0+	0	TBA	Management-Policy-Id

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.

12. IANA Considerations

This document contains placeholders ("TBA") for assigned numbers within the RADIUS Attributes registry, to be assigned by IANA at the time this document should be published as an RFC.

13. Security Considerations

This specification describes the use of RADIUS and Diameter for purposes of authentication, authorization and accounting for management access to devices within local area 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 [RFC3576]. 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.

Any of the attributes described in this memo, with the exception of Service-Type, may not be understood by the NAS which receives it. A legacy NAS not compliant with this specification may silently discard these attributes while permitting the user to access the management interface(s) of the NAS. This can lead to users improperly receiving unauthorized 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.

14. Acknowledgments

Many thanks to all reviewers, including Barney Wolff and Mauricio Sanchez.

15. Normative References

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

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

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

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

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

[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.

[RFC3576] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, 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.

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
Cisco Systems, Inc.
10850 Murdock Road
Knoxville, TN 37932
USA

Email: gdweber@cisco.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).