Network Working Group
Request for Comments: 5608
Category: Standards Track

K. Narayan
Cisco Systems, Inc.
D. Nelson
Elbrys Networks, Inc.

August 2009

Remote Authentication Dial-In User Service (RADIUS) Usage for Simple Network Management Protocol (SNMP) Transport Models

Abstract

This memo describes the use of a Remote Authentication Dial-In User Service (RADIUS) authentication and authorization service with Simple Network Management Protocol (SNMP) secure Transport Models to authenticate users and authorize creation of secure transport sessions. While the recommendations of this memo are generally applicable to a broad class of SNMP Transport Models, the examples focus on the Secure Shell (SSH) Transport Model.

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction

1.1. General

This memo describes the use of a Remote Authentication Dial-In User Service (RADIUS) authentication and authorization service by Simple Network Management Protocol (SNMP) secure Transport Models to authenticate users and authorize creation of secure transport sessions. While the recommendations of this memo are generally applicable to a broad class of SNMP Transport Models, the examples focus on the Secure Shell Transport Model.

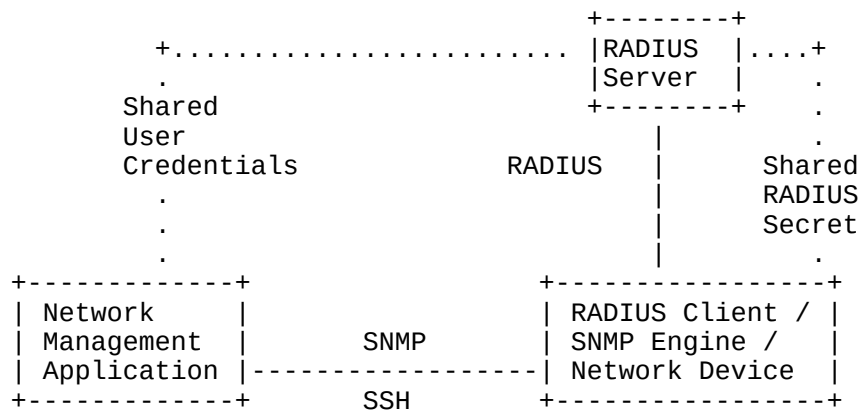
In the context of this document, a Network Access Server (NAS) is a network device or host that contains an SNMP engine implementation, utilizing SNMP Transport Models. It is customary in SNMP documents to indicate which subsystem performs specific processing tasks. In this document, we leave such decisions to the implementer, as is customary for RADIUS documents, and simply specify NAS behavior. Such processing would quite likely be implemented in the secure transport module.

1.2. Requirements Language

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

1.3. System Block Diagram

A block diagram of the major system components referenced in this document may be useful to understanding the text that follows.



Block Diagram

This diagram illustrates that a network management application communicates with a network device, the managed entity, using SNMP over SSH. The network devices uses RADIUS to communicate with a RADIUS server to authenticate the network management application (or the user whose credentials that application provides) and to obtain authorization information related to access via SNMP for purpose of device management. Other secure transport protocols might be used instead of SSH.

1.4. RADIUS Operational Model

The RADIUS protocol [RFC2865] provides authentication and authorization services for network access devices, usually referred to as a Network Access Server (NAS). The RADIUS protocol operates, at the most simple level, as a request-response mechanism. RADIUS clients, within the NAS, initiate a transaction by sending a RADIUS Access-Request message to a RADIUS server, with which the client shares credentials. The RADIUS server will respond with either an Access-Accept message or an Access-Reject message.

RADIUS supports authentication methods compatible with plaintext username and password mechanisms, MD5 Challenge/Response mechanisms, Extensible Authentication Protocol (EAP) mechanisms, and HTTP Digest mechanisms. Upon presentation of identity and credentials, the user is either accepted or rejected. RADIUS servers indicate a successful authentication by returning an Access-Accept message. An Access-Reject message indicates unsuccessful authentication.

Access-Accept messages are populated with one or more service provisioning attributes, which control the type and extent of service provided to the user at the NAS. The authorization portion may be thought of as service provisioning. Based on the configuration of the user's account on the RADIUS server, upon authentication, the NAS is provided with instructions as to what type of service to provide to the user. When that service provisioning does not match the capabilities of the NAS, or of the particular interface to the NAS over which the user is requesting access, RFC 2865 [RFC2865] requires that the NAS MUST reject the access request. RFC 2865 describes service provisioning attributes for management access to a NAS, as well as various terminal emulation and packet forwarding services on the NAS. This memo describes specific RADIUS service provisioning attributes that are useful with secure transports and SNMP Transport Models.

RADIUS servers are often deployed on an enterprise-wide or organization-wide basis, covering a variety of disparate use cases. In such deployments, all NASes and all users are serviced by a common pool of RADIUS servers. In many deployments, the RADIUS server will handle requests from many different types of NASes with different capabilities, and different types of interfaces, services, and protocol support.

In order for a RADIUS server to make the correct authorization decision in all cases, the server will often need to know something about the type of NAS at which the user is requesting access, the type of service that the user is requesting, and the role of the user in the organization. For example, many users may be authorized to receive network access via a Remote Access Server (RAS), Virtual Private Network (VPN) server, or LAN access switch. Typically only a small sub-set of all users are authorized to access the administrative interfaces of network infrastructure devices, e.g., the Command Line Interface (CLI) or SNMP engine of switches and routers.

In order for the RADIUS server to have information regarding the type of access being requested, it is common for the NAS (i.e., the RADIUS client) to include "hint" attributes in the RADIUS Access-Request message, describing the NAS and the type of service being requested.

This document recommends appropriate "hint" attributes for the SNMP service type.

1.5. RADIUS Usage with Secure Transports

Some secure transport protocols that can be used with SNMP Transport Models have defined authentication protocols supporting several authentication methods. For example, the Secure Shell (SSH) Authentication protocol [RFC4252] supports multiple methods (including public key, password, and host-based) to authenticate SSH clients.

SSH Server integration with RADIUS traditionally uses the username and password mechanism.

Secure transport protocols do not, however, specify how the transport interfaces to authentication clients, leaving such as implementation specific. For example, the "password" method of SSH authentication primarily describes how passwords are acquired from the SSH client and transported to the SSH server, the interpretation of the password and validation against password databases is left to SSH server implementations. SSH server implementations often use the Pluggable Authentication Modules [PAM] interface provided by operating systems such as Linux and Solaris to integrate with password-based network authentication mechanisms such as RADIUS, TACACS+ (Terminal Access Controller Access-Control System Plus), Kerberos, etc.

Secure transports do not typically specify how to utilize authorization information obtained from a AAA service, such as RADIUS. More often, user authentication is sufficient to cause the secure transport server to begin delivering service to the user. Access control in these situations is supplied by the application to which the secure transport server session is attached. For example, if the application is a Linux shell, the user’s access rights are controlled by that user account’s group membership and the file system access protections. This behavior does not closely follow the traditional service provisioning model of AAA systems, such as RADIUS.

1.6. Domain of Applicability

Most of the RADIUS Attributes referenced in this document have broad applicability for provisioning remote management access to NAS devices using SNMP. However, the selection of secure transport protocols has special considerations. This document does not specify details of the integration of secure transport protocols with a RADIUS client in the NAS implementation. However, there are functional requirements for correct application of framed management

protocols and 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 obtained by the RADIUS client from the secure transport protocol server, or in some cases directly from the SNMP engine, the secure transport 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 (Challenge Handshake Authentication Protocol) - RFC 2865
- ARAP (Apple Remote Access Protocol) - RFC 2869
- EAP (Extensible Authentication Protocol) - RFC 2869, RFC 3579
- HTTP Digest - RFC 5090

The secure transport protocols selected for use with RADIUS and SNMP 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.

1.7. SNMP Transport Models

The Transport Subsystem for SNMP [RFC5590] defines a mechanism for providing transport layer security (TLS) for SNMP, allowing protocols such as SSH and TLS to be used to secure SNMP communication. The Transport Subsystem allows the modular definition of Transport Models for multiple secure transport protocols. Transport Models rely upon the underlying secure transport for user authentication services. The Transport Model (TM) then maps the authenticated identity to a model-independent principal, which it stores in the tmStateReference. When the selected security model is the Transport Security Model (TSM), the expected behavior is for the securityName to be set by the

TSM from the authenticated principal information stored in the tmStateReference by the TM.

The Secure Shell protocol provides a secure transport channel with support for channel authentication via local accounts and integration with various external authentication and authorization services such as RADIUS, Kerberos, etc. The Secure Shell Transport Model [RFC5592] defines the use of the Secure Shell protocol as the basis for a Transport Model.

2. RADIUS Usage for SNMP Transport Models

There are two use cases for RADIUS support of management access via SNMP. These are (a) service authorization and (b) access control authorization. RADIUS almost always involves user authentication as prerequisite to authorization, and there is a user authentication phase for each of these two use cases. The first use case is discussed in detail in this memo, while the second use case is a topic of current research, and beyond the scope of this document. This document describes the way in which RADIUS attributes and messages are applied to the specific application area of SNMP Transport Models. User authentication and service authorization via RADIUS are undertaken by the secure transport module, that underlies the SNMP Transport Model.

User authentication for SNMP Transport Models has the same syntax and semantics as user authentication for any other network service. In the context of SNMP, the "user" is thought of as a "principal" and may represent a host, an application, or a human.

Service authorization allows a RADIUS server to authorize an authenticated principal to use SNMP, optionally over a secure transport, typically using an SNMP Transport Model. This memo describes mechanisms by which such information can be requested from a RADIUS server and enforced within the NAS. An SNMP architecture, [RFC3411], does not make a distinction between user authentication and service authorization. In the case of existing, deployed security models, such as the User-based Security Model (USM), this distinction is not significant. For SNMP Transport Models, this distinction is relevant and important.

It is relevant because of the way in which SSH implementations have traditionally integrated with RADIUS clients. Those SSH implementations traditionally seek to obtain user authentication (e.g., validation of a username and password) from an outside authentication service, often via a PAM-style interface. The service authorization in traditional SSH server implementations comes via the restrictions that the operating system (OS) shell (and file system,

etc.) place on the user by means of access controls tied to the username or the username's membership in various user groups. These OS-style access controls are distinct from the service provisioning features of RADIUS. If we wish to use existing SSH server implementations, or slightly adapt them, for use with SNMP Transport Models, and we wish to support RADIUS-provisioned service authorization, we need to be aware that the RADIUS service authorization information will need to be obtained by the relevant SNMP models from the SSH module.

One reason that RADIUS-provisioned service authorization is important is that in many deployments, the RADIUS server's back-end authentication database contains credentials for many classes of users, only a small portion of which may be authorized to access the management interfaces of managed entities (NASes) via SNMP. This is in contrast to the way USM for SNMP works, in which all principals entered to the local configuration data-store are authorized for access to the managed entity. In the absence of RADIUS-provisioned service authorization, network management access may be granted to unauthorized, but properly authenticated, users. With SNMPv3, an appropriately configured Access Control Model would serve to alleviate the risk of unauthorized access.

2.1. RADIUS Authentication for Transport Protocols

This document will rely on implementation specific integration of the transport protocols with RADIUS clients for user authentication.

It is REQUIRED that the integration of RADIUS clients with transport protocols utilize appropriate "hint" attributes in RADIUS Access-Request messages, to signal to the RADIUS server the type of service being requested over the transport session. Specific attributes for use with SNMP Transport Models are recommended in this document.

RADIUS servers, compliant to this specification, MAY use RADIUS "hint" attributes, as described herein, to inform the decision whether to accept or reject the authentication request.

2.2. RADIUS Authorization for Transport Protocols

In compliance with RFC 2865, NASes MUST enforce implicitly mandatory attributes, such as Service-Type, within an Access-Accept message. NASes MUST treat Access-Accept messages that attempt to provision unsupported services as if they were an Access-Reject. NASes SHOULD treat unknown attributes as if they were provisioning unsupported services. See [RFC5080] for additional details.

A NAS that is compliant to this specification MUST treat any RADIUS Access-Accept message that provisions a level of transport protection (e.g., SSH) that cannot be provided, and/or application service (e.g., SNMP) that cannot be provided over that transport, as if an Access-Reject message had been received instead. The RADIUS Service-Type Attribute is the primary indicator of the service being provisioned, although other attributes may also convey service provisioning information.

For traditional SSH usage, RADIUS servers typically provision management access service, as SSH is often used to access the command line shell of a host system, e.g., the NAS. RFC 2865 defines two types of management access service attributes, one for privileged access to the Command Line Interface (CLI) of the NAS and one for non-privileged CLI access. These traditional management access services are not used with SNMP. [RFC5607] describes further RADIUS service provisioning attributes for management access to the NAS, including SNMP access.

2.3. SNMP Service Authorization

The Transport Subsystem for SNMP [RFC5590] defines the notion of a session, although the specifics of how sessions are managed is left to Transport Models. The Transport Subsystem defines some basic requirements for transport protocols around creation and deletion of sessions. This memo specifies additional requirements for transport protocols during session creation and for session termination.

RADIUS servers compliant to this specification MUST use RADIUS service provisioning attributes, as described herein, to specify SNMP access over a secure transport. Such RADIUS servers MAY use RADIUS "hint" attributes included in the Access-Request message, as described herein, in determining what, if any, service to provision.

NASes compliant to this specification MUST use RADIUS service provisioning attributes, as described in this section, when they are present in a RADIUS Access-Accept message, to determine whether the session can be created, and they MUST enforce the service provisioning decisions of the RADIUS server.

The following RADIUS attributes MUST be used, as "hint" attributes included in the Access-Request message to signal use of SNMP over a secure transport (i.e., authPriv) to the RADIUS server:

1. Service-Type with a value of Framed-Management.

2. Framed-Management-Protocol with a value of SNMP.

3. Management-Transport-Protection with a value of Integrity-Confidentiality-Protection.

The following RADIUS attributes MUST be used in an Access-Accept message to provision SNMP over a secure transport that provides both integrity and confidentiality (i.e., authPriv):

1. Service-Type with a value of Framed-Management.

2. Framed-Management-Protocol with a value of SNMP.

3. Management-Transport-Protection with a value of Integrity-Confidentiality-Protection.

The following RADIUS attributes MUST be optionally used, to authorize use of SNMP without protection (i.e., authNoPriv):

1. Service-Type with a value of Framed-Management.

2. Framed-Management-Protocol with a value of SNMP.

3. Management-Transport-Protection with a value of No-Protection.

There are no combinations of RADIUS attributes that denote the equivalent of SNMP noAuthNoPriv access, as RADIUS always involves the authentication of a user (i.e., a principal) as a prerequisite for authorization. RADIUS can be used to provide an "Authorize-Only" service, but only when the request contains a "cookie" from a previous successful authentication with the same RADIUS server (i.e., the RADIUS State Attribute).

The following RADIUS attributes are used to limit the extent of a secure transport session carrying SNMP traffic, in conjunction with an SNMP Transport Model:

1. Session-Timeout

2. Inactivity-Timeout.

Refer to [RFC2865] for a detailed description of these attributes. The Session-Timeout Attribute indicates the maximum number of seconds that a session may exist before it is unconditionally disconnected. The Inactivity-Timeout Attribute indicates the maximum number of seconds that a transport session may exist without any protocol activity (messages sent or received) before the session is disconnected. These timeouts are enforced by the NAS.

3. Table of Attributes

Table 1 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	0	0	1	User-Name	[RFC2865]
0-1	0	0	0	2	User-Password	[RFC2865]
0-1 *	0	0	0	4	NAS-IP-Address	[RFC2865]
0-1 *	0	0	0	95	NAS-IPv6-Address	[RFC3162]
0-1 *	0	0	0	32	NAS-Identifier	[RFC2865]
0-1	0-1	0	0	6	Service-Type	[RFC2865]
0-1	0-1	0	0-1	24	State	[RFC2865]
0	0-1	0	0	27	Session-Timeout	[RFC2865]
0	0-1	0	0	28	Idle-Timeout	[RFC2865]
0-1	0-1	0-1	0-1	80	Message-Authenticator	[RFC3579]
0-1	0-1	0	0	133	Framed-Management-Protocol	[RFC5607]
0-1	0-1	0	0	134	Management-Transport-Protection	[RFC5607]

Table 1

Table 2 defines the meaning of the entries in Table 1.

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.
*	Only one of these attribute options SHOULD be included.

Table 2

SSH integration with RADIUS traditionally uses usernames and passwords (with the User-Password Attribute), but other secure transports could use other authentication mechanisms, and would include RADIUS authentication attributes appropriate for that mechanism instead of User-Password.

This document does not describe the usage of RADIUS Accounting or Dynamic RADIUS Re-Authorization. Such RADIUS usages are not currently envisioned for SNMP, and are beyond the scope of this document.

4. Security Considerations

This specification describes the use of RADIUS for purposes of authentication and authorization. Threats and security issues for this application are described in [RFC3579] and [RFC3580]; security issues encountered in roaming are described in [RFC2607].

Additional security considerations for use of SNMP with secure Transport Models [RFC5590] and the Transport Security Model [RFC5591] are found in the "Security Considerations" sections of the respective documents.

If the SNMPv1 or SNMPv2c Security Model is used, then securityName comes from the community name, as per RFC 3584. If the User-based Security Model is selected, then securityName is determined using USM. This may not be what is expected when using an SNMP secure Transport Model with an external authentication service, such as RADIUS.

Simultaneously using a secure transport with RADIUS authentication and authorization, and the SNMPv1 or SNMPv2c or USM security models is NOT RECOMMENDED. See the "Coexistence, Security Parameters, and Access Control" section of [RFC5590].

There are good reasons to provision USM access to supplement AAA-based access, however. When the network is under duress, or the AAA-service is unreachable, for any reason, it is important to have access credentials stored in the local configuration data-store of the managed entity. USM credentials are a likely way to fulfill this requirement. This is analogous to configuring a local "root" password in the "/etc/passwd" file of a UNIX workstation, to be used as a backup means of login, for times when the Network Information Service (NIS) authentication service is unreachable.

The Message-Authenticator (80) Attribute [RFC3579] SHOULD be used with RADIUS messages that are described in this memo. This is useful because the Message-Authenticator Attribute is the best available mechanism in RADIUS as it stands today to provide tamper-evident integrity protection of the service provisioning attributes in an Access-Accept packet. It is slightly less important for Access-Request packets, although it may be desirable to protect any "hint" attributes contained in those messages. This protection mitigates the fact that RADIUS messages are not encrypted and that attributes could be added, deleted or modified by an adversary in a position to intercept the packet.

5. Acknowledgements

The authors would like to acknowledge the contributions of David Harrington and Juergen Schoenwaelder for numerous helpful discussions in this space, and Wes Hardaker for his thoughtful review comments.

6. References

6.1. 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.

[RFC5080] Nelson, D. and A. DeKok, "Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes", RFC 5080, December 2007.

[RFC5590] Harrington, D. and J. Schoenwaelder, "Transport Subsystem for the Simple Network Management Protocol (SNMP)", RFC 5590, June 2009.

[RFC5591] Harrington, D. and W. Hardaker, "Transport Security Model for Simple Network Management Protocol (SNMP)", RFC 5591, June 2009.

[RFC5607] Nelson, D. and G. Weber, "Remote Authentication Dial-In User Service (RADIUS) Authorization for Network Access Server (NAS) Management", RFC 5607, July 2009.

6.2. Informative References

[PAM] Samar, V. and R. Schemers, "UNIFIED LOGIN WITH PLUGGABLE AUTHENTICATION MODULES (PAM)", Open Group RFC 86.0, October 1995, <http://www.opengroup.org/rfc/mirror-rfc/rfc86.0.txt>.

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

[RFC3162] Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.

[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.

[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.

[RFC4252] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Authentication Protocol", RFC 4252, January 2006.

[RFC5592] Harrington, D., Salowey, J., and W. Hardaker, "Secure Shell Transport Model for Simple Network Management Protocol (SNMP)", RFC 5592, June 2009.

Authors' Addresses

Kaushik Narayan
Cisco Systems, Inc.
10 West Tasman Drive
San Jose, CA 95134
USA

Phone: +1.408.526.8168
EMail: kaushik_narayan@yahoo.com

David Nelson
Elbrys Networks, Inc.
282 Corporate Drive
Portsmouth, NH 03801
USA

Phone: +1.603.570.2636
EMail: dnelson@elbrysnetworks.com