RADIUS Accounting Client MIB (IPv6)
draft-nelson-rfc2620bis-00.txt

Status of this Memo

This document is an Internet-Draft and is subject to all provisions of Section 3 of RFC 3667. By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she become aware will be disclosed, in accordance with RFC 3668.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 12, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This memo updates RFC 2620 by extending the MIB defined in RFC 2620 to add support for IPv6 address formats.
Table of Contents

1. Terminology .................................................. 3
2. Introduction .................................................. 3
3. The Internet-Standard Management Framework .................. 3
4. Scope of Changes ............................................... 3
5. Structure of the MIB Module ................................... 3
6. Deprecated Objects ............................................ 4
7. Definitions ................................................... 4
8. IANA Considerations ........................................... 7
9. Security Considerations ....................................... 7
10. References .................................................... 8
    10.1 Normative References ...................................... 8
    10.2 Informative References .................................... 8
    Author’s Address .............................................. 9
A. Acknowledgments .............................................. 9
    Intellectual Property and Copyright Statements .............. 10
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 2620 [RFC2620] and RFC 2866 [RFC2866].

2. Introduction

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. The objects defined within this memo relate to the RADIUS Accounting Client as defined in RFC 2866 [RFC2866].

3. The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to section 7 of RFC 3410 [RFC3410].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIv2, which is described in STD 58, RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] and STD 58, RFC 2580 [RFC2580].

4. Scope of Changes

This document updates RFC 2620 [RFC2620], RADIUS Accounting Client MIB, by augmenting the conceptual table rows for radiusAccServerEntry, adding new columns called radiusAccServerInetAddressType, radiusAccServerInetAddress, and radiusAccClientServerInetPortNumber. The purpose of these added MIB objects is to support IPv6 addressing formats. The existing table columns radiusAccServerAddress and radiusAccClientServerPortNumber are deprecated but may continue to be used in IPv4-only deployments.

5. Structure of the MIB Module

The structure of the MIB Module defined in this memo extends the structure of the MIB Module defined in RADIUS Accounting Client MIB, RFC 2620 [RFC2620] using the SMI AUGMENTS syntax, but does not alter that structure, except to deprecate the corresponding IPv4-only
address format objects.

6. Deprecated Objects

The following objects, defined in RADIUS Accounting Client MIB, RFC 2620 [RFC2620] are deprecated:

radiusAccServerAddress
radiusAccClientServerPortNumber

7. Definitions

RADIUS-ACC-CLIENT-MIB-IPV6 DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, OBJECT-IDENTITY,
    mib-2 FROM SNMPv2-SMI
    InetAddressType, InetAddress, InetPortNumber
    FROM INET-ADDRESS-MIB
    MODULE-COMPLIANCE, OBJECT-GROUP  FROM SNMPv2-CONF
    radiusAccServerEntry FROM RADIUS-ACC-CLIENT-MIB;

radiusAccClientExtMIB MODULE-IDENTITY
    LAST-UPDATED "200502072051Z"  -- Mon Feb 7 20:51 GMT 2005
    ORGANIZATION "IETF RADIUS Extensions Working Group."
    CONTACT-INFO
        " David B. Nelson
            Enterasys Networks
            50 Minutemann Road
            Andover, MA 01810
            US
            Phone: +1 978 684 1000
            EMail: dnelson@eterasys.com"
    DESCRIPTION
        "An extension to the MIB module for entities
          implementing the client side of the Remote Access
          Dialin User Service (RADIUS) accounting protocol,
          using IPv6 addressing formats. Updates RFC 2620."
    REVISION "200502072051Z"  -- Mon Feb 7 20:51 GMT 2005
    DESCRIPTION "Initial version, published as RFC xxxx."

-- RFC Editor: replace xxx with actual RFC number at the time of
-- publication, and remove this note.

::= { mib-2 TBA }

-- RFC Editor: replace TBA with IANA assigned OID value, and
-- remove this note.

radiusAccClientExtMIBNotifications OBJECT IDENTIFIER ::= { radiusAccClientExtMIB 0 }
radiusAccClientExtMIBObjects OBJECT IDENTIFIER ::= { radiusAccClientExtMIB 1 }
radiusAccClientExtMIBConformance OBJECT IDENTIFIER ::= { radiusAccClientExtMIB 2 }

-- MIB objects

radiusAccServerExtTable OBJECT-TYPE
SYNTAX SEQUENCE OF RadiusAccServerExtEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "The (conceptual) table listing the RADIUS accounting servers with which the client shares a secret."
 ::= { radiusAccClientExtMIBObjects 1 }

radiusAccServerExtEntry OBJECT-TYPE
SYNTAX RadiusAccServerExtEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "An entry (conceptual row) representing a RADIUS accounting server with which the client shares a secret."
AUGMENTS { radiusAccServerEntry }
 ::= { radiusAccServerExtTable 1 }

RadiusAccServerExtEntry ::= SEQUENCE {
 radiusAccServerInetAddressType InetAddressType,
 radiusAccServerInetAddress InetAddress,
 radiusAccClientServerInetPortNumber InetPortNumber
 }

radiusAccServerInetAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The type of address format used for the radiusAccServerInetAddress object."
 ::= { radiusAccServerExtEntry 1 }

Nelson Expires August 12, 2005 [Page 5]
radiusAccServerInetAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The IP address of the RADIUS accounting
server referred to in this table entry, using
the IPv6 address format."
 ::= { radiusAccServerExtEntry 2 }

radiusAccClientServerInetPortNumber OBJECT-TYPE
SYNTAX InetPortNumber
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The UDP port the client is using to send requests
to this accounting server."
 ::= { radiusAccServerExtEntry 3 }

-- conformance information

radiusAccClientExtMIBCompliances OBJECT IDENTIFIER
 ::= { radiusAccClientExtMIBConformance 1 }

radiusAccClientExtMIBGroups OBJECT IDENTIFIER
 ::= { radiusAccClientExtMIBConformance 2 }

-- compliance statements

radiusAccClientExtMIBCompliance MODULE-COMPLIANCE
STATUS current
DESCRIPTION
"The compliance statement for accounting
clients implementing the RADIUS Accounting
Client IPv6 Extensions MIB."
MODULE -- this module
MANDATORY-GROUPS { radiusAccClientExtMIBGroup }
 ::= { radiusAccClientExtMIBCompliances 1 }

-- units of conformance

radiusAccClientExtMIBGroup OBJECT-GROUP
OBJECTS { radiusAccServerInetAddressType,
radiusAccServerInetAddress,
radiusAccClientServerInetPortNumber }
STATUS current
DESCRIPTION
"The collection of extended objects providing management of RADIUS Accounting Clients using IPv6 address format."
::= { radiusAccClientExtMIBGroups 1 }

END

8. IANA Considerations

This document requires IANA assignment of a number in the MIB-2 OID number space.

9. Security Considerations

There are no management objects defined in this MIB that have a MAX-ACCESS clause of read-write and/or read-create. So, if this MIB is implemented correctly, then there is no risk that an intruder can alter or create any management objects of this MIB via direct SNMP SET operations.

There are a number of managed objects in this MIB that may contain sensitive information. These are:

radiusAccServerInetAddress This can be used to determine the address of the RADIUS accounting server with which the client is communicating. This information could be useful in mounting an attack on the accounting server.

radiusAccClientServerInetPortNumber This can be used to determine the port number on which the RADIUS accounting client is sending. This information could be useful in impersonating the client in order to send data to the accounting server.

It is thus important to control even GET access to these objects and possibly to even encrypt the values of these object when sending them over the network via SNMP. Not all versions of SNMP provide features for such a secure environment.

SNMP versions prior to SNMPv3 do not provide a secure environment. Even if the network itself is secure (for example by using IPSec), there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB.

It is recommended that the implementers consider the security features as provided by the SNMPv3 framework. Specifically, the use
of the User-based Security Model [RFC2574] and the View-based Access Control Model [RFC2575] is recommended. Using these security features, customer/users can give access to the objects only to those principals (users) that have legitimate rights to GET or SET (change/create/delete) them.

10. References

10.1 Normative References


10.2 Informative References


Appendix A. Acknowledgments

The Authors of the original MIB [RFC2620] are Bernard Aboba and Glen Zorn.

Many thanks to all reviewers, especially to David Harrington and Bruno Pape.
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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