Network Working Group
Request for Comments: 4669
Obsoletes: 2619
Category: Standards Track

D. Nelson
Enterasys Networks

August 2006

RADIUS Authentication Server MIB for IPv6

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

Copyright (C) The Internet Society (2006).

Abstract

This memo defines a set of extensions that instrument RADIUS authentication server functions. These extensions represent a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. Using these extensions, IP-based management stations can manage RADIUS authentication servers.

This memo obsoletes RFC 2619 by deprecating the MIB table containing IPv4-only address formats and defining a new table to add support for version-neutral IP address formats. The remaining MIB objects from RFC 2619 are carried forward into this document. This memo also adds UNITS and REFERENCE clauses to selected objects.

Table of Contents

1. 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 Remote Authentication Dial-In User Service (RADIUS) Authentication Server as defined in RFC 2865 [RFC2865].

2. 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].

This document uses the word "malformed" with respect to RADIUS packets, particularly in the context of counters of "malformed packets". While RFC 2865 does not provide an explicit definition of "malformed", malformed generally means that the implementation has determined the packet does not match the format defined in RFC 2865. Some implementations may determine that packets are malformed when the Vendor Specific Attribute (VSA) format does not follow the RFC 2865 recommendations for VSAs. Those implementations are used in deployments today, and thus set the de facto definition of "malformed".

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 obsoletes RFC 2619 [RFC2619], RADIUS Authentication Server MIB, by deprecating the radiusAuthClientTable table and adding a new table, radiusAuthClientExtTable, containing radiusAuthClientInetAddressType and radiusAuthClientInetAddress. The

purpose of these added MIB objects is to support version-neutral IP addressing formats. The existing table containing radiusAuthClientAddress is deprecated. The remaining MIB objects from RFC 2619 are carried forward into this document. This memo also adds UNITS and REFERENCE clauses to selected objects.

RFC 4001 [RFC4001], which defines the SMI Textual Conventions for version-neutral IP addresses, contains the following recommendation.

'In particular, when revising a MIB module that contains IPv4 specific tables, it is suggested to define new tables using the textual conventions defined in this memo [RFC4001] that support all versions of IP. The status of the new tables SHOULD be "current", whereas the status of the old IP version specific tables SHOULD be changed to "deprecated". The other approach, of having multiple similar tables for different IP versions, is strongly discouraged.'

5. Structure of the MIB Module

The RADIUS authentication protocol, described in RFC 2865 [RFC2865], distinguishes between the client function and the server function. In RADIUS authentication, clients send Access-Requests, and servers reply with Access-Accepts, Access-Rejects, and Access-Challenges. Typically, NAS devices implement the client function, and thus would be expected to implement the RADIUS authentication client MIB, while RADIUS authentication servers implement the server function, and thus would be expected to implement the RADIUS authentication server MIB.

However, it is possible for a RADIUS authentication entity to perform both client and server functions. For example, a RADIUS proxy may act as a server to one or more RADIUS authentication clients, while simultaneously acting as an authentication client to one or more authentication servers. In such situations, it is expected that RADIUS entities combining client and server functionality will support both the client and server MIBs. The server MIB is defined in this document, and the client MIB is defined in [RFC4668].

This MIB module contains fourteen scalars as well as a single table, the RADIUS Authentication Client Table, which contains one row for each RADIUS authentication client with which the server shares a secret. Each entry in the RADIUS Authentication Client Table includes thirteen columns presenting a view of the activity of the RADIUS authentication server.

This MIB imports from [RFC2578], [RFC2580], [RFC3411], and [RFC4001].

6. Deprecated Objects

The deprecated table in this MIB is carried forward from RFC 2619 [RFC2619]. There are two conditions under which it MAY be desirable for managed entities to continue to support the deprecated table:

1. The managed entity only supports IPv4 address formats.

2. The managed entity supports both IPv4 and IPv6 address formats, and the deprecated table is supported for backwards compatibility with older management stations. This option SHOULD only be used when the IP addresses in the new table are in IPv4 format and can accurately be represented in both the new table and the deprecated table.

Managed entities SHOULD NOT instantiate row entries in the deprecated table, containing IPv4-only address objects, when the RADIUS client address represented in such a table row is not an IPv4 address. Managed entities SHOULD NOT return inaccurate values of IP address or SNMP object access errors for IPv4-only address objects in otherwise populated tables. When row entries exist in both the deprecated IPv4-only table and the new IP-version-neutral table that describe the same RADIUS client, the row indexes SHOULD be the same for the corresponding rows in each table, to facilitate correlation of these related rows by management applications.

7. Definitions

```
RADIUS-AUTH-SERVER-MIB DEFINITIONS ::= BEGIN

IMPORTS
       MODULE-IDENTITY, OBJECT-TYPE, OBJECT-IDENTITY,
       Counter32, Integer32,
       IpAddress, TimeTicks, mib-2      FROM SNMPv2-SMI
       SnmpAdminString                  FROM SNMP-FRAMEWORK-MIB
       InetAddressType, InetAddress     FROM INET-ADDRESS-MIB
       MODULE-COMPLIANCE, OBJECT-GROUP  FROM SNMPv2-CONF;

radiusAuthServMIB MODULE-IDENTITY
       LAST-UPDATED "200608210000Z"  -- 21 August 2006
       ORGANIZATION "IETF RADIUS Extensions Working Group."
       CONTACT-INFO
              " Bernard Aboba
                Microsoft
                One Microsoft Way
                Redmond, WA  98052
                US
                Phone: +1 425 936 6605
```

```
                EMail: bernarda@microsoft.com"
        DESCRIPTION
              "The MIB module for entities implementing the server
               side of the Remote Authentication Dial-In User
               Service (RADIUS) authentication protocol.  Copyright
               (C) The Internet Society (2006).  This version of this
               MIB module is part of RFC 4669; see the RFC itself for
               full legal notices."
        REVISION "200608210000Z"  -- 21 August 2006
        DESCRIPTION
              "Revised version as published in RFC 4669.  This
               version obsoletes that of RFC 2619 by deprecating the
               MIB table containing IPv4-only address formats and
               defining a new table to add support for version-neutral
               IP address formats.  The remaining MIB objects from RFC
               2619 are carried forward into this version."
        REVISION "199906110000Z"  -- 11 Jun 1999
        DESCRIPTION "Initial version as published in RFC 2619."
        ::= { radiusAuthentication 1 }

radiusMIB  OBJECT-IDENTITY
       STATUS  current
       DESCRIPTION
             "The OID assigned to RADIUS MIB work by the IANA."
        ::= { mib-2 67 }

radiusAuthentication  OBJECT IDENTIFIER ::= {radiusMIB 1}

radiusAuthServMIBObjects OBJECT IDENTIFIER
        ::= { radiusAuthServMIB 1 }

radiusAuthServ  OBJECT IDENTIFIER
        ::= { radiusAuthServMIBObjects 1 }

radiusAuthServIdent OBJECT-TYPE
       SYNTAX      SnmpAdminString
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
             "The implementation identification string for the
              RADIUS authentication server software in use on the
              system, for example, 'FNS-2.1'."
       ::= {radiusAuthServ 1}

radiusAuthServUpTime OBJECT-TYPE
       SYNTAX      TimeTicks
       MAX-ACCESS  read-only
       STATUS      current
```

```
          DESCRIPTION
                "If the server has a persistent state (e.g., a
                 process), this value will be the time elapsed (in
                 hundredths of a second) since the server process
                 was started.  For software without persistent state,
                 this value will be zero."
          ::= {radiusAuthServ 2}

   radiusAuthServResetTime OBJECT-TYPE
          SYNTAX      TimeTicks
          MAX-ACCESS  read-only
          STATUS      current
          DESCRIPTION
                "If the server has a persistent state (e.g., a process)
                 and supports a 'reset' operation (e.g., can be told to
                 re-read configuration files), this value will be the
                 time elapsed (in hundredths of a second) since the
                 server was 'reset.'  For software that does not
                 have persistence or does not support a 'reset'
                 operation, this value will be zero."
          ::= {radiusAuthServ 3}

   radiusAuthServConfigReset OBJECT-TYPE
          SYNTAX INTEGER { other(1),
                           reset(2),
                           initializing(3),
                           running(4)}
          MAX-ACCESS  read-write
          STATUS      current
          DESCRIPTION
                 "Status/action object to reinitialize any persistent
                  server state.  When set to reset(2), any persistent
                  server state (such as a process) is reinitialized as
                  if the server had just been started.  This value will
                  never be returned by a read operation.  When read,
                  one of the following values will be returned:
                      other(1) - server in some unknown state;
                      initializing(3) - server (re)initializing;
                      running(4) - server currently running."
          ::= {radiusAuthServ 4}

   radiusAuthServTotalAccessRequests OBJECT-TYPE
           SYNTAX Counter32
           UNITS "packets"
           MAX-ACCESS read-only
           STATUS current
           DESCRIPTION
                  "The number of packets received on the
```

```
                authentication port."
        REFERENCE "RFC 2865 section 4.1"
        ::= { radiusAuthServ 5}

   radiusAuthServTotalInvalidRequests OBJECT-TYPE
        SYNTAX Counter32
        UNITS "packets"
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
              "The number of RADIUS Access-Request packets
               received from unknown addresses."
        REFERENCE "RFC 2865 section 4.1"
        ::= { radiusAuthServ 6 }

   radiusAuthServTotalDupAccessRequests OBJECT-TYPE
       SYNTAX Counter32
       UNITS "packets"
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
             "The number of duplicate RADIUS Access-Request
              packets received."
       REFERENCE "RFC 2865 section 4.1"
       ::= { radiusAuthServ 7 }

   radiusAuthServTotalAccessAccepts OBJECT-TYPE
       SYNTAX Counter32
       UNITS "packets"
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
             "The number of RADIUS Access-Accept packets sent."
       REFERENCE "RFC 2865 section 4.2"
       ::= { radiusAuthServ 8 }

   radiusAuthServTotalAccessRejects OBJECT-TYPE
      SYNTAX Counter32
      UNITS "packets"
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
            "The number of RADIUS Access-Reject packets sent."
      REFERENCE "RFC 2865 section 4.3"
      ::= { radiusAuthServ 9 }

   radiusAuthServTotalAccessChallenges OBJECT-TYPE
      SYNTAX Counter32
```

```
          UNITS "packets"
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
                "The number of RADIUS Access-Challenge packets sent."
          REFERENCE "RFC 2865 section 4.4"
          ::= { radiusAuthServ 10 }

   radiusAuthServTotalMalformedAccessRequests OBJECT-TYPE
          SYNTAX Counter32
          UNITS "packets"
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
                "The number of malformed RADIUS Access-Request
                 packets received.  Bad authenticators
                 and unknown types are not included as
                 malformed Access-Requests."
          REFERENCE "RFC 2865 section 4.1"
          ::= { radiusAuthServ 11 }

   radiusAuthServTotalBadAuthenticators OBJECT-TYPE
          SYNTAX Counter32
          UNITS "packets"
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
                "The number of RADIUS Authentication-Request packets
                 that contained invalid Message Authenticator
                 attributes received."
          REFERENCE "RFC 2865 section 3"
          ::= { radiusAuthServ 12 }

   radiusAuthServTotalPacketsDropped OBJECT-TYPE
          SYNTAX Counter32
          UNITS "packets"
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
                "The number of incoming packets
                 silently discarded for some reason other
                 than malformed, bad authenticators or
                 unknown types."
          REFERENCE "RFC 2865 section 3"
          ::= { radiusAuthServ 13 }

   radiusAuthServTotalUnknownTypes OBJECT-TYPE
          SYNTAX Counter32
```

```
          UNITS "packets"
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
                "The number of RADIUS packets of unknown type that
                 were received."
          REFERENCE "RFC 2865 section 4"
          ::= { radiusAuthServ 14 }


   radiusAuthClientTable OBJECT-TYPE
          SYNTAX     SEQUENCE OF RadiusAuthClientEntry
          MAX-ACCESS not-accessible
          STATUS     deprecated
          DESCRIPTION
                "The (conceptual) table listing the RADIUS
                 authentication clients with which the server shares
                 a secret."
          ::= { radiusAuthServ 15 }


   radiusAuthClientEntry OBJECT-TYPE
          SYNTAX     RadiusAuthClientEntry
          MAX-ACCESS not-accessible
          STATUS     deprecated
          DESCRIPTION
                "An entry (conceptual row) representing a RADIUS
                 authentication client with which the server shares a
                 secret."
          INDEX      { radiusAuthClientIndex }
          ::= { radiusAuthClientTable 1 }

   RadiusAuthClientEntry ::= SEQUENCE {
          radiusAuthClientIndex                          Integer32,
          radiusAuthClientAddress                        IpAddress,
          radiusAuthClientID                       SnmpAdminString,
          radiusAuthServAccessRequests                   Counter32,
          radiusAuthServDupAccessRequests                Counter32,
          radiusAuthServAccessAccepts                    Counter32,
          radiusAuthServAccessRejects                    Counter32,
          radiusAuthServAccessChallenges                 Counter32,
          radiusAuthServMalformedAccessRequests          Counter32,
          radiusAuthServBadAuthenticators                Counter32,
          radiusAuthServPacketsDropped                   Counter32,
          radiusAuthServUnknownTypes                     Counter32
   }

   radiusAuthClientIndex OBJECT-TYPE
```

```
            SYNTAX     Integer32 (1..2147483647)
            MAX-ACCESS not-accessible
            STATUS     deprecated
            DESCRIPTION
                  "A number uniquely identifying each RADIUS
                   authentication client with which this server
                   communicates."
            ::= { radiusAuthClientEntry 1 }

      radiusAuthClientAddress OBJECT-TYPE
            SYNTAX     IpAddress
            MAX-ACCESS read-only
            STATUS     deprecated
            DESCRIPTION
                  "The NAS-IP-Address of the RADIUS authentication client
                   referred to in this table entry."
            REFERENCE "RFC 2865 section 2"
            ::= { radiusAuthClientEntry 2 }

      radiusAuthClientID OBJECT-TYPE
            SYNTAX     SnmpAdminString
            MAX-ACCESS read-only
            STATUS     deprecated
            DESCRIPTION
                  "The NAS-Identifier of the RADIUS authentication client
                   referred to in this table entry.  This is not
                   necessarily the same as sysName in MIB II."
            REFERENCE "RFC 2865 section 5.32"
            ::= { radiusAuthClientEntry 3 }

      -- Server Counters

      --
      -- Responses = AccessAccepts + AccessRejects + AccessChallenges
      --
      -- Requests - DupRequests - BadAuthenticators - MalformedRequests -
      -- UnknownTypes -  PacketsDropped - Responses = Pending
      --
      -- Requests - DupRequests - BadAuthenticators - MalformedRequests -
      -- UnknownTypes - PacketsDropped = entries logged

      radiusAuthServAccessRequests OBJECT-TYPE
            SYNTAX Counter32
            UNITS "packets"
            MAX-ACCESS read-only
            STATUS deprecated
            DESCRIPTION
                  "The number of packets received on the authentication
```

```
                port from this client."
        REFERENCE "RFC 2865 section 4.1"
        ::= { radiusAuthClientEntry  4 }

   radiusAuthServDupAccessRequests OBJECT-TYPE
        SYNTAX Counter32
        UNITS "packets"
        MAX-ACCESS read-only
        STATUS deprecated
        DESCRIPTION
              "The number of duplicate RADIUS Access-Request
               packets received from this client."
        REFERENCE "RFC 2865 section 4.1"
        ::= { radiusAuthClientEntry  5 }

   radiusAuthServAccessAccepts OBJECT-TYPE
        SYNTAX Counter32
        UNITS "packets"
        MAX-ACCESS read-only
        STATUS deprecated
        DESCRIPTION
              "The number of RADIUS Access-Accept packets
               sent to this client."
        REFERENCE "RFC 2865 section 4.2"
        ::= { radiusAuthClientEntry  6 }

   radiusAuthServAccessRejects OBJECT-TYPE
      SYNTAX Counter32
      UNITS "packets"
      MAX-ACCESS read-only
      STATUS deprecated
      DESCRIPTION
              "The number of RADIUS Access-Reject packets
               sent to this client."
       REFERENCE "RFC 2865 section 4.3"
       ::= { radiusAuthClientEntry  7 }

   radiusAuthServAccessChallenges OBJECT-TYPE
        SYNTAX Counter32
        UNITS "packets"
        MAX-ACCESS read-only
        STATUS deprecated
        DESCRIPTION
              "The number of RADIUS Access-Challenge packets
               sent to this client."
        REFERENCE "RFC 2865 section 4.4"
        ::= { radiusAuthClientEntry  8 }
```

```
   radiusAuthServMalformedAccessRequests OBJECT-TYPE
          SYNTAX Counter32
          UNITS "packets"
          MAX-ACCESS read-only
          STATUS deprecated
          DESCRIPTION
                "The number of malformed RADIUS Access-Request
                 packets received from this client.
                 Bad authenticators and unknown types are not included
                 as malformed Access-Requests."
          REFERENCE "RFC 2865 section 3"
          ::= { radiusAuthClientEntry  9 }

   radiusAuthServBadAuthenticators OBJECT-TYPE
          SYNTAX Counter32
          UNITS "packets"
          MAX-ACCESS read-only
          STATUS deprecated
          DESCRIPTION
                "The number of RADIUS Authentication-Request packets
                 that contained invalid Message Authenticator
                 attributes received from this client."
          REFERENCE "RFC 2865 section 3"
          ::= { radiusAuthClientEntry  10 }

   radiusAuthServPacketsDropped OBJECT-TYPE
         SYNTAX Counter32
         UNITS "packets"
         MAX-ACCESS read-only
         STATUS deprecated
         DESCRIPTION
                 "The number of incoming packets from this
                  client silently discarded for some reason other
                  than malformed, bad authenticators or
                  unknown types."
          REFERENCE "RFC 2865 section 3"
          ::= { radiusAuthClientEntry  11 }

   radiusAuthServUnknownTypes OBJECT-TYPE
          SYNTAX Counter32
          UNITS "packets"
          MAX-ACCESS read-only
          STATUS deprecated
          DESCRIPTION
                "The number of RADIUS packets of unknown type that
                 were received from this client."
          REFERENCE "RFC 2865 section 4"
          ::= { radiusAuthClientEntry  12 }
```

```
   -- New MIB objects added in this revision

   radiusAuthClientExtTable OBJECT-TYPE
          SYNTAX     SEQUENCE OF RadiusAuthClientExtEntry
          MAX-ACCESS not-accessible
          STATUS     current
          DESCRIPTION
                "The (conceptual) table listing the RADIUS
                 authentication clients with which the server shares
                 a secret."
          ::= { radiusAuthServ 16 }

   radiusAuthClientExtEntry OBJECT-TYPE
          SYNTAX     RadiusAuthClientExtEntry
          MAX-ACCESS not-accessible
          STATUS     current
          DESCRIPTION
                "An entry (conceptual row) representing a RADIUS
                 authentication client with which the server shares a
                 secret."
          INDEX      { radiusAuthClientExtIndex }
          ::= { radiusAuthClientExtTable 1 }

   RadiusAuthClientExtEntry ::= SEQUENCE {
          radiusAuthClientExtIndex                 Integer32,
          radiusAuthClientInetAddressType          InetAddressType,
          radiusAuthClientInetAddress              InetAddress,
          radiusAuthClientExtID                    SnmpAdminString,
          radiusAuthServExtAccessRequests          Counter32,
          radiusAuthServExtDupAccessRequests       Counter32,
          radiusAuthServExtAccessAccepts           Counter32,
          radiusAuthServExtAccessRejects           Counter32,
          radiusAuthServExtAccessChallenges        Counter32,
          radiusAuthServExtMalformedAccessRequests Counter32,
          radiusAuthServExtBadAuthenticators       Counter32,
          radiusAuthServExtPacketsDropped          Counter32,
          radiusAuthServExtUnknownTypes            Counter32,
          radiusAuthServCounterDiscontinuity       TimeTicks
   }

   radiusAuthClientExtIndex OBJECT-TYPE
          SYNTAX     Integer32 (1..2147483647)
          MAX-ACCESS not-accessible
          STATUS     current
          DESCRIPTION
                "A number uniquely identifying each RADIUS
                 authentication client with which this server
                 communicates."
```

```
          ::= { radiusAuthClientExtEntry 1 }

   radiusAuthClientInetAddressType OBJECT-TYPE
            SYNTAX     InetAddressType
            MAX-ACCESS read-only
            STATUS     current
            DESCRIPTION
                  "The type of address format used for the
                   radiusAuthClientInetAddress object."
            ::= { radiusAuthClientExtEntry 2 }

      radiusAuthClientInetAddress OBJECT-TYPE
            SYNTAX     InetAddress
            MAX-ACCESS read-only
            STATUS     current
            DESCRIPTION
                  "The IP address of the RADIUS authentication
                   client referred to in this table entry, using
                   the version-neutral IP address format."
            ::= { radiusAuthClientExtEntry 3 }


   radiusAuthClientExtID OBJECT-TYPE
          SYNTAX     SnmpAdminString
          MAX-ACCESS read-only
          STATUS     current
          DESCRIPTION
                "The NAS-Identifier of the RADIUS authentication client
                 referred to in this table entry.  This is not
                 necessarily the same as sysName in MIB II."
          REFERENCE "RFC 2865 section 5.32"
          ::= { radiusAuthClientExtEntry 4 }

   -- Server Counters

   --
   -- Responses = AccessAccepts + AccessRejects + AccessChallenges
   --
   -- Requests - DupRequests - BadAuthenticators - MalformedRequests -
   -- UnknownTypes -  PacketsDropped - Responses = Pending
   --
   -- Requests - DupRequests - BadAuthenticators - MalformedRequests -
   -- UnknownTypes - PacketsDropped = entries logged

   radiusAuthServExtAccessRequests OBJECT-TYPE
          SYNTAX Counter32
          UNITS "packets"
          MAX-ACCESS read-only
```

```
          STATUS current
          DESCRIPTION
                "The number of packets received on the authentication
                 port from this client.  This counter may experience a
                 discontinuity when the RADIUS Server module within the
                 managed entity is reinitialized, as indicated by the
                 current value of radiusAuthServCounterDiscontinuity."
          REFERENCE "RFC 2865 section 4.1"
          ::= { radiusAuthClientExtEntry  5 }

   radiusAuthServExtDupAccessRequests OBJECT-TYPE
          SYNTAX Counter32
          UNITS "packets"
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
                "The number of duplicate RADIUS Access-Request
                 packets received from this client.  This counter may
                 experience a discontinuity when the RADIUS Server
                 module within the managed entity is reinitialized, as
                 indicated by the current value of
                 radiusAuthServCounterDiscontinuity."
          REFERENCE "RFC 2865 section 4.1"
          ::= { radiusAuthClientExtEntry  6 }

   radiusAuthServExtAccessAccepts OBJECT-TYPE
          SYNTAX Counter32
          UNITS "packets"
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
                "The number of RADIUS Access-Accept packets
                 sent to this client.  This counter may experience a
                 discontinuity when the RADIUS Server module within the
                 managed entity is reinitialized, as indicated by the
                 current value of radiusAuthServCounterDiscontinuity."
          REFERENCE "RFC 2865 section 4.2"
          ::= { radiusAuthClientExtEntry  7 }

   radiusAuthServExtAccessRejects OBJECT-TYPE
         SYNTAX Counter32
         UNITS "packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
                "The number of RADIUS Access-Reject packets
                 sent to this client.  This counter may experience a
                 discontinuity when the RADIUS Server module within the
```

```
                managed entity is reinitialized, as indicated by the
                current value of radiusAuthServCounterDiscontinuity."
        REFERENCE "RFC 2865 section 4.3"
        ::= { radiusAuthClientExtEntry  8 }

   radiusAuthServExtAccessChallenges OBJECT-TYPE
        SYNTAX Counter32
        UNITS "packets"
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
              "The number of RADIUS Access-Challenge packets
               sent to this client.  This counter may experience a
               discontinuity when the RADIUS Server module within the
               managed entity is reinitialized, as indicated by the
               current value of radiusAuthServCounterDiscontinuity."
        REFERENCE "RFC 2865 section 4.4"
        ::= { radiusAuthClientExtEntry  9 }

   radiusAuthServExtMalformedAccessRequests OBJECT-TYPE
        SYNTAX Counter32
        UNITS "packets"
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
              "The number of malformed RADIUS Access-Request
               packets received from this client.  Bad authenticators
               and unknown types are not included as malformed
               Access-Requests.  This counter may experience a
               discontinuity when the RADIUS Server module within the
               managed entity is reinitialized, as indicated by the
               current value of radiusAuthServCounterDiscontinuity."
        REFERENCE "RFC 2865 sections 3, 4.1"
        ::= { radiusAuthClientExtEntry  10 }

   radiusAuthServExtBadAuthenticators OBJECT-TYPE
        SYNTAX Counter32
        UNITS "packets"
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
              "The number of RADIUS Authentication-Request packets
               that contained invalid Message Authenticator
               attributes received from this client.  This counter
               may experience a discontinuity when the RADIUS Server
               module within the managed entity is reinitialized, as
               indicated by the current value of
               radiusAuthServCounterDiscontinuity."
```

```
          REFERENCE "RFC 2865 section 3"
          ::= { radiusAuthClientExtEntry  11 }

   radiusAuthServExtPacketsDropped OBJECT-TYPE
         SYNTAX Counter32
         UNITS "packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
                "The number of incoming packets from this client
                 silently discarded for some reason other than
                 malformed, bad authenticators or unknown types.
                 This counter may experience a discontinuity when the
                 RADIUS Server module within the managed entity is
                 reinitialized, as indicated by the current value of
                 radiusAuthServCounterDiscontinuity."
          REFERENCE "RFC 2865 section 3"
          ::= { radiusAuthClientExtEntry  12 }

   radiusAuthServExtUnknownTypes OBJECT-TYPE
          SYNTAX Counter32
          UNITS "packets"
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
                "The number of RADIUS packets of unknown type that
                 were received from this client.  This counter may
                 experience a discontinuity when the RADIUS Server
                 module within the managed entity is reinitialized, as
                 indicated by the current value of
                 radiusAuthServCounterDiscontinuity."
          REFERENCE "RFC 2865 section 4"
          ::= { radiusAuthClientExtEntry  13 }

   radiusAuthServCounterDiscontinuity OBJECT-TYPE
            SYNTAX TimeTicks
            UNITS "centiseconds"
            MAX-ACCESS read-only
            STATUS current
            DESCRIPTION
                  "The number of centiseconds since the last
                   discontinuity in the RADIUS Server counters.
                   A discontinuity may be the result of a
                   reinitialization of the RADIUS Server module
                   within the managed entity."
            ::= { radiusAuthClientExtEntry 14 }
```

```
   -- conformance information

   radiusAuthServMIBConformance  OBJECT IDENTIFIER
          ::= { radiusAuthServMIB 2 }

   radiusAuthServMIBCompliances  OBJECT IDENTIFIER
          ::= { radiusAuthServMIBConformance 1 }

   radiusAuthServMIBGroups  OBJECT IDENTIFIER
          ::= { radiusAuthServMIBConformance 2 }

   -- compliance statements

   radiusAuthServMIBCompliance MODULE-COMPLIANCE
               STATUS  deprecated
               DESCRIPTION
                     "The compliance statement for authentication
                      servers implementing the RADIUS Authentication
                      Server MIB.  Implementation of this module is for
                      IPv4-only entities, or for backwards compatibility
                      use with entities that support both IPv4 and
                      IPv6."
               MODULE  -- this module
               MANDATORY-GROUPS { radiusAuthServMIBGroup }

               OBJECT        radiusAuthServConfigReset
               WRITE-SYNTAX  INTEGER { reset(2) }
               DESCRIPTION  "The only SETable value is 'reset' (2)."

               ::= { radiusAuthServMIBCompliances 1 }


   radiusAuthServMIBExtCompliance MODULE-COMPLIANCE
               STATUS  current
               DESCRIPTION
                     "The compliance statement for authentication
                      servers implementing the RADIUS Authentication
                      Server IPv6 Extensions MIB.  Implementation of
                      this module is for entities that support IPv6,
                      or support IPv4 and IPv6."
               MODULE  -- this module
               MANDATORY-GROUPS { radiusAuthServExtMIBGroup }

               OBJECT        radiusAuthServConfigReset
               WRITE-SYNTAX  INTEGER { reset(2) }
               DESCRIPTION  "The only SETable value is 'reset' (2)."

               OBJECT radiusAuthClientInetAddressType
```

```
                SYNTAX InetAddressType { ipv4(1), ipv6(2) }
                DESCRIPTION
                  "An implementation is only required to support
                   IPv4 and globally unique IPv6 addresses."

                OBJECT radiusAuthClientInetAddress
                SYNTAX InetAddress ( SIZE (4|16) )
                DESCRIPTION
                  "An implementation is only required to support
                   IPv4 and globally unique IPv6 addresses."

                ::= { radiusAuthServMIBCompliances 2 }


   -- units of conformance

   radiusAuthServMIBGroup OBJECT-GROUP
         OBJECTS {radiusAuthServIdent,
                  radiusAuthServUpTime,
                  radiusAuthServResetTime,
                  radiusAuthServConfigReset,
                  radiusAuthServTotalAccessRequests,
                  radiusAuthServTotalInvalidRequests,
                  radiusAuthServTotalDupAccessRequests,
                  radiusAuthServTotalAccessAccepts,
                  radiusAuthServTotalAccessRejects,
                  radiusAuthServTotalAccessChallenges,
                  radiusAuthServTotalMalformedAccessRequests,
                  radiusAuthServTotalBadAuthenticators,
                  radiusAuthServTotalPacketsDropped,
                  radiusAuthServTotalUnknownTypes,
                  radiusAuthClientAddress,
                  radiusAuthClientID,
                  radiusAuthServAccessRequests,
                  radiusAuthServDupAccessRequests,
                  radiusAuthServAccessAccepts,
                  radiusAuthServAccessRejects,
                  radiusAuthServAccessChallenges,
                  radiusAuthServMalformedAccessRequests,
                  radiusAuthServBadAuthenticators,
                  radiusAuthServPacketsDropped,
                  radiusAuthServUnknownTypes
                 }
         STATUS  deprecated
         DESCRIPTION
               "The collection of objects providing management of
                a RADIUS Authentication Server."
         ::= { radiusAuthServMIBGroups 1 }
```

```
   radiusAuthServExtMIBGroup OBJECT-GROUP
         OBJECTS {radiusAuthServIdent,
                  radiusAuthServUpTime,
                  radiusAuthServResetTime,
                  radiusAuthServConfigReset,
                  radiusAuthServTotalAccessRequests,
                  radiusAuthServTotalInvalidRequests,
                  radiusAuthServTotalDupAccessRequests,
                  radiusAuthServTotalAccessAccepts,
                  radiusAuthServTotalAccessRejects,
                  radiusAuthServTotalAccessChallenges,
                  radiusAuthServTotalMalformedAccessRequests,
                  radiusAuthServTotalBadAuthenticators,
                  radiusAuthServTotalPacketsDropped,
                  radiusAuthServTotalUnknownTypes,
                  radiusAuthClientInetAddressType,
                  radiusAuthClientInetAddress,
                  radiusAuthClientExtID,
                  radiusAuthServExtAccessRequests,
                  radiusAuthServExtDupAccessRequests,
                  radiusAuthServExtAccessAccepts,
                  radiusAuthServExtAccessRejects,
                  radiusAuthServExtAccessChallenges,
                  radiusAuthServExtMalformedAccessRequests,
                  radiusAuthServExtBadAuthenticators,
                  radiusAuthServExtPacketsDropped,
                  radiusAuthServExtUnknownTypes,
                  radiusAuthServCounterDiscontinuity
                 }
         STATUS  current
         DESCRIPTION
               "The collection of objects providing management of
                a RADIUS Authentication Server."
         ::= { radiusAuthServMIBGroups 2 }

   END
```

8. Security Considerations

There are a number of management objects defined in this MIB that have a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. These are:

radiusAuthServConfigReset
This object can be used to reinitialize the persistent state of any server. When set to reset(2), any persistent server state (such as a process) is reinitialized as if the server had just been started. Depending on the server implementation details, this action may or may not interrupt the processing of pending request in the server. Abuse of this object may lead to a Denial of Service attack on the server.

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

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

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

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 implementers consider the security features as provided by the SNMPv3 framework (see [RFC3410], section 8), including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

9. References

9.1. Normative References

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

[RFC2578] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

[RFC2579] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

[RFC2580] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "Conformance Statements for SMIv2", STD 58, RFC 2580, April 1999.

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

[RFC4001] Daniele, M., Haberman, B., Routhier, S., and J. Schoenwaelder, "Textual Conventions for Internet Network Addresses", RFC 4001, February 2005.

9.2. Informative References

[RFC2619] Zorn, G. and B. Aboba, "RADIUS Authentication Server MIB", RFC 2619, June 1999.

[RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, December 2002.

[RFC4668] Nelson, D., "RADIUS Authentication Client MIB for IPv6", RFC 4668, August 2006.

Appendix A. Acknowledgements

The authors of the original MIB are Bernard Aboba and Glen Zorn.

Many thanks to all reviewers, especially to David Harrington, Dan Romascanu, C.M. Heard, Bruno Pape, Greg Weber, and Bert Wijnen.

Author's Address

David B. Nelson
Enterasys Networks
50 Minuteman Road
Andover, MA 01810
USA

EMail: dnelson@enterasys.com

Full Copyright Statement

Copyright (C) The Internet Society (2006).

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.

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.

Intellectual Property

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.

Acknowledgement

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