

Network Working Group
Internet-Draft
Obsoletes: RFC [2618](#) (if approved)
Expires: July 24, 2006

D. Nelson
Enterasys Networks
January 20, 2006

RADIUS Auth Client MIB (IPv6)
draft-ietf-radext-rfc2618bis-02.txt

Status of this Memo

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 becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

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 July 24, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This memo defines a set of extensions which instrument RADIUS authentication client 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 clients.

This memo obsoletes [RFC 2618](#) 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 2618](#) are carried forward into this document. The memo also adds UNITS and REFERENCE clauses to selected objects.

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	4
6.	Deprecated Objects	5
7.	Definitions	5
8.	IANA Considerations	19
9.	Security Considerations	19
10.	Normative References	20
Appendix A.	Acknowledgments	21
	Author's Address	22
	Intellectual Property and Copyright Statements	23

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](#)].

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".

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

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 2618](#) [[RFC2618](#)], RADIUS Authentication

Client MIB, by deprecating the radiusAuthServerTable table and adding a new table, radiusAuthServerExtTable, containing radiusAuthServerInetAddressType, radiusAuthServerInetAddress, and radiusAuthClientServerInetPortNumber. The purpose of these added MIB objects is to support version neutral IP addressing formats. The existing table containing radiusAuthServerAddress and radiusAuthClientServerPortNumber is deprecated. The remaining MIB objects are carried forward from [RFC 2618](#) into this document. This memo also adds UNITS and REFERENCE clauses to selected objects.

[RFC 4001](#) [[RFC4001](#)], which defines the SMI Textual Conventions for IPv6 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 [[RFC 4001](#)] 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 Network Access Server (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.

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

Nelson

Expires July 24, 2006

[Page 4]

6. Deprecated Objects

The deprecated table in this MIB is carried forward from [RFC 2618](#) [[RFC2618](#)]. 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 server 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 server, 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-CLIENT-MIB DEFINITIONS ::= BEGIN
```

```
IMPORTS
```

```
    MODULE-IDENTITY, OBJECT-TYPE, OBJECT-IDENTITY,
    Counter32, Integer32, Gauge32,
    IPAddress, TimeTicks, mib-2          FROM SNMPv2-SMI
    SnmpAdminString                     FROM SNMP-FRAMEWORK-MIB
    InetAddressType, InetAddress,
    InetPortNumber                     FROM INET-ADDRESS-MIB
    MODULE-COMPLIANCE, OBJECT-GROUP    FROM SNMPv2-CONF;
```

```
radiusAuthClientMIB MODULE-IDENTITY
```

```
    LAST-UPDATED "200601200000Z" -- 20 Jan 2006
    ORGANIZATION "IETF RADIUS Extensions Working Group."
    CONTACT-INFO
        " Bernard Aboba
        Microsoft
        One Microsoft Way
        Redmond, WA 98052
```


US

Phone: +1 425 936 6605

EEmail: bernarda@microsoft.com"

DESCRIPTION

"The MIB module for entities implementing the client side of the Remote Authentication Dial-In User Service (RADIUS) authentication protocol."

REVISION "200601200000Z" -- 20 Jan 2006

DESCRIPTION "Revised version as published in RFC xxxx. This version obsoletes that of [RFC 2618](#) 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 2618](#) are carried forward into this version."

REVISION "9906110000Z" -- 11 Jun 1999

DESCRIPTION "Initial version as published in [RFC 2618](#)."

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

::= { radiusAuthentication 2 }

radiusMIB OBJECT-IDENTITY

STATUS current

DESCRIPTION

"The OID assigned to RADIUS MIB work by the IANA."

::= { mib-2 67 }

radiusAuthentication OBJECT IDENTIFIER ::= {radiusMIB 1}

radiusAuthClientMIBObjects OBJECT IDENTIFIER

::= { radiusAuthClientMIB 1 }

radiusAuthClient OBJECT IDENTIFIER

::= { radiusAuthClientMIBObjects 1 }

radiusAuthClientInvalidServerAddresses OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of RADIUS Access-Response packets received from unknown addresses."

::= { radiusAuthClient 1 }

radiusAuthClientIdentifier OBJECT-TYPE

SYNTAX SnmpAdminString

Nelson

Expires July 24, 2006

[Page 6]

MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The NAS-Identifier of the RADIUS authentication client.
 This is not necessarily the same as sysName in MIB II."
REFERENCE "[RFC 2865 section 5.32](#)"
::= { radiusAuthClient 2 }

radiusAuthServerTable OBJECT-TYPE
 SYNTAX SEQUENCE OF RadiusAuthServerEntry
 MAX-ACCESS not-accessible
 STATUS deprecated
 DESCRIPTION
 "The (conceptual) table listing the RADIUS authentication
 servers with which the client shares a secret."
 ::= { radiusAuthClient 3 }

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

RadiusAuthServerEntry ::= SEQUENCE {
 radiusAuthServerIndex Integer32,
 radiusAuthServerAddress IpAddress,
 radiusAuthClientServerPortNumber Integer32,
 radiusAuthClientRoundTripTime TimeTicks,
 radiusAuthClientAccessRequests Counter32,
 radiusAuthClientAccessRetransmissions Counter32,
 radiusAuthClientAccessAccepts Counter32,
 radiusAuthClientAccessRejects Counter32,
 radiusAuthClientAccessChallenges Counter32,
 radiusAuthClientMalformedAccessResponses Counter32,
 radiusAuthClientBadAuthenticators Counter32,
 radiusAuthClientPendingRequests Gauge32,
 radiusAuthClientTimeouts Counter32,
 radiusAuthClientUnknownTypes Counter32,
 radiusAuthClientPacketsDropped Counter32
}

radiusAuthServerIndex OBJECT-TYPE
 SYNTAX Integer32 (1..2147483647)

Nelson

Expires July 24, 2006

[Page 7]

```
MAX-ACCESS not-accessible
STATUS deprecated
DESCRIPTION
    "A number uniquely identifying each RADIUS
    Authentication server with which this client
    communicates."
::= { radiusAuthServerEntry 1 }

radiusAuthServerAddress OBJECT-TYPE
    SYNTAX      IPAddress
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "The IP address of the RADIUS authentication server
        referred to in this table entry."
    ::= { radiusAuthServerEntry 2 }

radiusAuthClientServerPortNumber OBJECT-TYPE
    SYNTAX Integer32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "The UDP port the client is using to send requests to
        this server."
    REFERENCE "RFC 2865 section 3"
    ::= { radiusAuthServerEntry 3 }

radiusAuthClientRoundTripTime OBJECT-TYPE
    SYNTAX TimeTicks
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "The time interval (in hundredths of a second) between
        the most recent Access-Reply/Access-Challenge and the
        Access-Request that matched it from this RADIUS
        authentication server."
    ::= { radiusAuthServerEntry 4 }

-- Request/Response statistics
--
-- TotalIncomingPackets = Accepts + Rejects + Challenges +
-- UnknownTypes
--
-- TotalIncomingPackets - MalformedResponses -
-- BadAuthenticators - UnknownTypes - PacketsDropped =
-- Successfully received
--
-- AccessRequests + PendingRequests + ClientTimeouts =
```

Nelson

Expires July 24, 2006

[Page 8]

```
-- Successfully received
--
--
```

radiusAuthClientAccessRequests OBJECT-TYPE

```
SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS deprecated
DESCRIPTION
    "The number of RADIUS Access-Request packets sent
    to this server. This does not include retransmissions."
REFERENCE "RFC 2865 section 4.1"
::= { radiusAuthServerEntry 5 }
```

radiusAuthClientAccessRetransmissions OBJECT-TYPE

```
SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS deprecated
DESCRIPTION
    "The number of RADIUS Access-Request packets
    retransmitted to this RADIUS authentication server."
REFERENCE "RFC 2865 sections 2.5, 4.1"
::= { radiusAuthServerEntry 6 }
```

radiusAuthClientAccessAccepts OBJECT-TYPE

```
SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS deprecated
DESCRIPTION
    "The number of RADIUS Access-Accept packets
    (valid or invalid) received from this server."
REFERENCE "RFC 2865 section 4.2"
::= { radiusAuthServerEntry 7 }
```

radiusAuthClientAccessRejects OBJECT-TYPE

```
SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS deprecated
DESCRIPTION
    "The number of RADIUS Access-Reject packets
    (valid or invalid) received from this server."
REFERENCE "RFC 2865 section 4.3"
::= { radiusAuthServerEntry 8 }
```


Nelson

Expires July 24, 2006

[Page 9]

radiusAuthClientAccessChallenges OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS deprecated

DESCRIPTION

"The number of RADIUS Access-Challenge packets
(valid or invalid) received from this server."

REFERENCE "[RFC 2865 section 4.4](#)"

::= { radiusAuthServerEntry 9 }

-- "Access-Response" includes an Access-Accept, Access-Challenge
-- or Access-Reject

radiusAuthClientMalformedAccessResponses OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS deprecated

DESCRIPTION

"The number of malformed RADIUS Access-Response
packets received from this server.
Malformed packets include packets with
an invalid length. Bad authenticators or
Message Authenticator attributes or unknown types
are not included as malformed access responses."

::= { radiusAuthServerEntry 10 }

radiusAuthClientBadAuthenticators OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS deprecated

DESCRIPTION

"The number of RADIUS Access-Response packets
containing invalid authenticators or Message
Authenticator attributes received from this server."

REFERENCE "[RFC 2865 section 3](#), [RFC 2869 section 5.14](#)"

::= { radiusAuthServerEntry 11 }

radiusAuthClientPendingRequests OBJECT-TYPE

SYNTAX Gauge32

MAX-ACCESS read-only

STATUS deprecated

DESCRIPTION

"The number of RADIUS Access-Request packets
destined for this server that have not yet timed out
or received a response. This variable is incremented

Nelson

Expires July 24, 2006

[Page 10]

when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout or retransmission."

REFERENCE "[RFC 2865 section 2](#)"

::= { radiusAuthServerEntry 12 }

radiusAuthClientTimeouts OBJECT-TYPE

SYNTAX Counter32

UNITS "timeouts"

MAX-ACCESS read-only

STATUS deprecated

DESCRIPTION

"The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout."

REFERENCE "[RFC 2865 section 2](#), [RFC 2869 section 2.3.2](#)"

::= { radiusAuthServerEntry 13 }

radiusAuthClientUnknownTypes OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS deprecated

DESCRIPTION

"The number of RADIUS packets of unknown type which were received from this server on the authentication port."

::= { radiusAuthServerEntry 14 }

radiusAuthClientPacketsDropped OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS deprecated

DESCRIPTION

"The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason."

::= { radiusAuthServerEntry 15 }

-- New MIB Objects in this revision

radiusAuthServerExtTable OBJECT-TYPE

SYNTAX SEQUENCE OF RadiusAuthServerExtEntry

Nelson

Expires July 24, 2006

[Page 11]

```
MAX-ACCESS not-accessible
STATUS      current
DESCRIPTION
    "The (conceptual) table listing the RADIUS authentication
        servers with which the client shares a secret."
::= { radiusAuthClient 4 }
```

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

```
RadiusAuthServerExtEntry ::= SEQUENCE {
    radiusAuthServerExtIndex          Integer32,
    radiusAuthServerInetAddressType  InetAddressType,
    radiusAuthServerInetAddress      InetAddress,
    radiusAuthClientServerInetPortNumber  InetPortNumber,
    radiusAuthClientExtRoundTripTime  TimeTicks,
    radiusAuthClientExtAccessRequests  Counter32,
    radiusAuthClientExtAccessRetransmissions  Counter32,
    radiusAuthClientExtAccessAccepts   Counter32,
    radiusAuthClientExtAccessRejects   Counter32,
    radiusAuthClientExtAccessChallenges Counter32,
    radiusAuthClientExtMalformedAccessResponses Counter32,
    radiusAuthClientExtBadAuthenticators Counter32,
    radiusAuthClientExtPendingRequests Gauge32,
    radiusAuthClientExtTimeouts        Counter32,
    radiusAuthClientExtUnknownTypes    Counter32,
    radiusAuthClientExtPacketsDropped   Counter32
}
```

```
radiusAuthServerExtIndex OBJECT-TYPE
    SYNTAX      Integer32 (1..2147483647)
    MAX-ACCESS not-accessible
    STATUS      current
    DESCRIPTION
        "A number uniquely identifying each RADIUS
            Authentication server with which this client
            communicates."
    ::= { radiusAuthServerExtEntry 1 }
```

Nelson

Expires July 24, 2006

[Page 12]

radiusAuthServerInetAddressType OBJECT-TYPE

SYNTAX InetAddressType

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The type of address format used for the
radiusAuthServerInetAddress object."

::= { radiusAuthServerExtEntry 2 }

radiusAuthServerInetAddress OBJECT-TYPE

SYNTAX InetAddress

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The IP address of the RADIUS authentication
server referred to in this table entry, using
the version neutral IP address format."

::= { radiusAuthServerExtEntry 3 }

radiusAuthClientServerInetPortNumber OBJECT-TYPE

SYNTAX InetPortNumber

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The UDP port the client is using to send requests
to this server."

REFERENCE "[RFC 2865 section 3](#)"

::= { radiusAuthServerExtEntry 4 }

radiusAuthClientExtRoundTripTime OBJECT-TYPE

SYNTAX TimeTicks

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The time interval (in hundredths of a second) between
the most recent Access-Reply/Access-Challenge and the
Access-Request that matched it from this RADIUS
authentication server."

REFERENCE "[RFC 2865 section 2](#)"

::= { radiusAuthServerExtEntry 5 }

-- Request/Response statistics

--

-- TotalIncomingPackets = Accepts + Rejects + Challenges +

-- UnknownTypes

--

-- TotalIncomingPackets - MalformedResponses -

-- BadAuthenticators - UnknownTypes - PacketsDropped =

Nelson

Expires July 24, 2006

[Page 13]

```
-- Successfully received
--
-- AccessRequests + PendingRequests + ClientTimeouts =
-- Successfully received
--
--
```

radiusAuthClientExtAccessRequests OBJECT-TYPE

```
SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "The number of RADIUS Access-Request packets sent
    to this server. This does not include retransmissions."
REFERENCE "RFC 2865 section 4.1"
::= { radiusAuthServerExtEntry 6 }
```

radiusAuthClientExtAccessRetransmissions OBJECT-TYPE

```
SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "The number of RADIUS Access-Request packets
    retransmitted to this RADIUS authentication server."
REFERENCE "RFC 2865 sections 2.5, 4.1"
::= { radiusAuthServerExtEntry 7 }
```

radiusAuthClientExtAccessAccepts OBJECT-TYPE

```
SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "The number of RADIUS Access-Accept packets
    (valid or invalid) received from this server."
REFERENCE "RFC 2865 section 4.2"
::= { radiusAuthServerExtEntry 8 }
```

radiusAuthClientExtAccessRejects OBJECT-TYPE

```
SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "The number of RADIUS Access-Reject packets
    (valid or invalid) received from this server."
```

Nelson

Expires July 24, 2006

[Page 14]

REFERENCE "[RFC 2865 section 4.3](#)"

::= { radiusAuthServerExtEntry 9 }

radiusAuthClientExtAccessChallenges OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of RADIUS Access-Challenge packets
(valid or invalid) received from this server."

REFERENCE "[RFC 2865 section 4.4](#)"

::= { radiusAuthServerExtEntry 10 }

-- "Access-Response" includes an Access-Accept, Access-Challenge

-- or Access-Reject

radiusAuthClientExtMalformedAccessResponses OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of malformed RADIUS Access-Response
packets received from this server.
Malformed packets include packets with
an invalid length. Bad authenticators or
Message Authenticator attributes or unknown types
are not included as malformed access responses."

REFERENCE "[RFC 2865](#) sections [3](#), [4](#)"

::= { radiusAuthServerExtEntry 11 }

radiusAuthClientExtBadAuthenticators OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of RADIUS Access-Response packets
containing invalid authenticators or Message
Authenticator attributes received from this server."

REFERENCE "[RFC 2865 section 3](#)"

::= { radiusAuthServerExtEntry 12 }

radiusAuthClientExtPendingRequests OBJECT-TYPE

SYNTAX Gauge32

UNITS "packets"

MAX-ACCESS read-only

Nelson

Expires July 24, 2006

[Page 15]

STATUS current

DESCRIPTION

"The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout or retransmission."

REFERENCE "[RFC 2865 section 2](#)"

::= { radiusAuthServerExtEntry 13 }

radiusAuthClientExtTimeouts OBJECT-TYPE

SYNTAX Counter32

UNITS "timeouts"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout."

REFERENCE "[RFC 2865](#) sections [2.5](#), [4.1](#)"

::= { radiusAuthServerExtEntry 14 }

radiusAuthClientExtUnknownTypes OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of RADIUS packets of unknown type which were received from this server on the authentication port."

REFERENCE "[RFC 2865 section 4](#)"

::= { radiusAuthServerExtEntry 15 }

radiusAuthClientExtPacketsDropped OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason."

::= { radiusAuthServerExtEntry 16 }

Nelson

Expires July 24, 2006

[Page 16]

```
-- conformance information

radiusAuthClientMIBConformance OBJECT IDENTIFIER
    ::= { radiusAuthClientMIB 2 }

radiusAuthClientMIBCompliances OBJECT IDENTIFIER
    ::= { radiusAuthClientMIBConformance 1 }

radiusAuthClientMIBGroups OBJECT IDENTIFIER
    ::= { radiusAuthClientMIBConformance 2 }

-- compliance statements

radiusAuthClientMIBCompliance MODULE-COMPLIANCE
    STATUS deprecated
    DESCRIPTION
        "The compliance statement for authentication clients
        implementing the RADIUS Authentication Client 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 { radiusAuthClientMIBGroup }

    ::= { radiusAuthClientMIBCompliances 1 }

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

    ::= { radiusAuthClientMIBCompliances 2 }

-- units of conformance

radiusAuthClientMIBGroup OBJECT-GROUP
    OBJECTS { radiusAuthClientIdentifier,
        radiusAuthClientInvalidServerAddresses,
        radiusAuthServerAddress,
        radiusAuthClientServerPortNumber,
```



```
        radiusAuthClientRoundTripTime,
        radiusAuthClientAccessRequests,
        radiusAuthClientAccessRetransmissions,
        radiusAuthClientAccessAccepts,
        radiusAuthClientAccessRejects,
        radiusAuthClientAccessChallenges,
        radiusAuthClientMalformedAccessResponses,
        radiusAuthClientBadAuthenticators,
        radiusAuthClientPendingRequests,
        radiusAuthClientTimeouts,
        radiusAuthClientUnknownTypes,
        radiusAuthClientPacketsDropped
    }
    STATUS deprecated
    DESCRIPTION
        "The basic collection of objects providing management of
        RADIUS Authentication Clients."
    ::= { radiusAuthClientMIBGroups 1 }

radiusAuthClientExtMIBGroup OBJECT-GROUP
    OBJECTS { radiusAuthClientIdentifier,
        radiusAuthClientInvalidServerAddresses,
        radiusAuthServerInetAddressType,
        radiusAuthServerInetAddress,
        radiusAuthClientServerInetPortNumber,
        radiusAuthClientExtRoundTripTime,
        radiusAuthClientExtAccessRequests,
        radiusAuthClientExtAccessRetransmissions,
        radiusAuthClientExtAccessAccepts,
        radiusAuthClientExtAccessRejects,
        radiusAuthClientExtAccessChallenges,
        radiusAuthClientExtMalformedAccessResponses,
        radiusAuthClientExtBadAuthenticators,
        radiusAuthClientExtPendingRequests,
        radiusAuthClientExtTimeouts,
        radiusAuthClientExtUnknownTypes,
        radiusAuthClientExtPacketsDropped
    }
    STATUS current
    DESCRIPTION
        "The collection of extended objects providing
        management of RADIUS Authentication Clients
        using version neutral IP address format."
    ::= { radiusAuthClientMIBGroups 2 }

END
```

Nelson

Expires July 24, 2006

[Page 18]

8. IANA Considerations

This document requires no new IANA assignments.

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.

Some of the readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP. These are the tables and objects and their sensitivity/vulnerability:

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

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

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

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPsec), even then, 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 module.

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

10. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2574] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", [RFC 2574](#), April 1999.
- [RFC2575] Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", [RFC 2575](#), April 1999.
- [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.
- [RFC2618] Aboba, B. and G. Zorn, "RADIUS Authentication Client MIB", [RFC 2618](#), June 1999.
- [RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", [RFC 2865](#), June 2000.
- [RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", [RFC 3410](#), December 2002.
- [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.

- [RFC3418] Presuhn, R., "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", STD 62, [RFC 3418](#), December 2002.
- [RFC4001] Daniele, M., Haberman, B., Routhier, S., and J. Schoenwaelder, "Textual Conventions for Internet Network Addresses", [RFC 4001](#), February 2005.

[Appendix A](#). Acknowledgments

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

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

Author's Address

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

Email: dnelson@enterasys.com

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 (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.

Acknowledgment

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

