Dynamic Authorization Client MIB
draft-decnodder-radext-dynauth-client-mib-03.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 21, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes the RADIUS dynamic authorization client
(DAC) functions that support the dynamic authorization extensions as defined in RFC3576.

Table of Contents

1. Requirements notation .............................. 3
2. Introduction ..................................... 4
3. The Internet-Standard Management Framework .......... 5
4. Terminology ...................................... 6
5. Overview ......................................... 7
6. RADIUS Dynamic Authorization Client MIB Definitions ... 8
7. Security Considerations ............................. 19
8. IANA considerations ................................ 21
9. Acknowledgements .................................. 22
10. References ........................................ 23
   10.1 Normative References ............................ 23
   10.2 Informative References .......................... 23
   Authors’ Addresses .................................. 24
   Intellectual Property and Copyright Statements ........ 25
1. Requirements notation

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

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. It is becoming increasingly important to support Dynamic Authorization extensions on the network access server (NAS) devices to handle the Disconnect and Change-of-Authorization (CoA) messages as described in [RFC3576]. As a result, the effective management of RADIUS Dynamic Authorization entities is of considerable importance. It complements the managed objects used for managing RADIUS authentication and accounting servers as described in [RFC2619] and [RFC2621], respectively.
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 [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, RFC2578 [RFC2578], STD 58, RFC2579 [RFC2579] and STD 58, RFC2580 [RFC2580].
4. Terminology

Dynamic Authorization Server (DAS)

The component that resides on the NAS which processes the Disconnect and CoA requests sent by the Dynamic Authorization Client as described in [RFC3576].

Dynamic Authorization Client (DAC)

The component which sends the Disconnect and CoA requests to the Dynamic Authorization Server as described in [RFC3576].

Dynamic Authorization Server Port

The UDP port on which the Dynamic Authorization server listens for the Disconnect and CoA requests sent by the Dynamic Authorization Client.
5. Overview

The RADIUS dynamic authorization extensions defined in [RFC3576], distinguish between the client function and the server function. [DYNSEVR] defines the terms Dynamic Authorization Server (DAS) and Dynamic Authorization Client (DAC), the MIB for the DAS, and the relationship with other MIB modules. This MIB module for the dynamic authorization client contains the following:

1. one scalar object

2. One Dynamic Authorization Server Table. This table contains one row for each DAS that the DAC shares a secret with.
6. RADIUS Dynamic Authorization Client MIB Definitions

RADIUS-DYNAUTH-CLIENT-MIB DEFINITIONS ::= BEGIN

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

radiusDynAuthClientMIB MODULE-IDENTITY
LAST-UPDATED "200502070000Z" -- 7 February 2005
ORGANIZATION "IETF RADEXT Working Group"
CONTACT-INFO
" Stefaan De Cnodder
   Alcatel
   Francis Wellesplein 1
   B-2018 Antwerp
   Belgium

   Phone: +32 3 240 85 15
   EMail: stefaan.de_cnodder@alcatel.be

Nagi Reddy Jonnalala
Future Soft
480 - 481, Anna Salai
Nandanam, Chennai
India

EMail: nagi_reddy.jonnala@alcatel.be

Murtaza Chiba
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose CA, 95134

Phone: +1 408 525 7198
EMail: mchiba@cisco.com "

DESCRIPTION
"The MIB module for entities implementing the client
side of the Dynamic Authorization extensions Remote
Access Dialin User Service (RADIUS) protocol.

Copyright (C) The Internet Society (2005). This initial
version of this MIB module was published in RFC yyy;
for full legal notices see the RFC itself. Supplementary
radiusDynamicAuthorization OBJECT IDENTIFIER ::= { mib-2 xxx }

radiusDynAuthClientMIBObjects OBJECT IDENTIFIER ::= { radiusDynAuthClientMIB 1 }

radiusDynAuthClient OBJECT IDENTIFIER ::= { radiusDynAuthClientMIBObjects 1 }

radiusDynAuthClientInvalidServerAddresses OBJECT-TYPE
  SYNTAX Counter32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION
    "The number of RADIUS Dynamic Authorization messages (both Disconnect and CoA) received from unknown addresses."
  ::= { radiusDynAuthClient 1 }

radiusDynAuthServerTable OBJECT-TYPE
  SYNTAX SEQUENCE OF RadiusDynAuthServerEntry
  MAX-ACCESS not-accessible
  STATUS current
  DESCRIPTION
    "The (conceptual) table listing the RADIUS Dynamic Authorization servers with which the client shares a secret."
  ::= { radiusDynAuthClient 2 }

radiusDynAuthServerEntry OBJECT-TYPE
  SYNTAX RadiusDynAuthServerEntry
  MAX-ACCESS not-accessible
  STATUS current
  DESCRIPTION
    "An entry (conceptual row) representing one Dynamic Authorization Server with which the client shares a secret."
  INDEX { radiusDynAuthServerIndex }
  ::= { radiusDynAuthServerTable 1 }
RadiusDynAuthServerEntry ::= SEQUENCE {
  radiusDynAuthServerIndex             Integer32, 
  radiusDynAuthServerAddressType       InetAddressType, 
  radiusDynAuthServerAddress           InetAddress, 
  radiusDynAuthServerClientPortNumber  Integer32, 
  radiusDynAuthServerID                SnmpAdminString, 
  radiusDynAuthClientRoundTripTime     TimeTicks, 
  radiusDynAuthClientDisconRequests    Counter32, 
  radiusDynAuthClientDisconRetransmissions Counter32, 
  radiusDynAuthClientDisconAcks        Counter32, 
  radiusDynAuthClientDisconNaks        Counter32, 
  radiusDynAuthClientMalformedDisconResponses Counter32, 
  radiusDynAuthClientDisconBadAuthenticators Counter32, 
  radiusDynAuthClientDisconPendingRequests Gauge32, 
  radiusDynAuthClientDisconTimeouts     Counter32, 
  radiusDynAuthClientDisconPacketsDropped Counter32, 
  radiusDynAuthClientCoARequests       Counter32, 
  radiusDynAuthClientCoAAcks           Counter32, 
  radiusDynAuthClientCoANaks           Counter32, 
  radiusDynAuthClientMalformedCoAResponses Counter32, 
  radiusDynAuthClientCoABadAuthenticators Counter32, 
  radiusDynAuthClientCoAPendingRequests Gauge32, 
  radiusDynAuthClientCoATimeouts       Counter32, 
  radiusDynAuthClientCoAPacketsDropped Counter32,
  radiusDynAuthClientUnknownTypes      Counter32
}

radiusDynAuthServerIndex OBJECT-TYPE
SYNTAX      Integer32 (1..2147483647)
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION  
"A number uniquely identifying each RADIUS Dynamic Authorization server with which this Dynamic Authorization client communicates. This number is allocated by the agent implementing this MIB module, and is unique in this context."
::= { radiusDynAuthServerEntry 1 }

radiusDynAuthServerAddressType OBJECT-TYPE
SYNTAX      InetAddressType
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION  
"The type of IP-Address of the RADIUS Dynamic Authorization server referred to in this table entry."
radiusDynAuthServerAddress OBJECT-TYPE
SYNTAX     InetAddress
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
    "The IP-Address value of the RADIUS Dynamic
    Authorization server referred to in this table entry."
::= { radiusDynAuthServerEntry 3 }

radiusDynAuthServerClientPortNumber OBJECT-TYPE
SYNTAX     Integer32 (0..65535)
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
    "The UDP port the RADIUS Dynamic Authorization client is
    using to send requests to this server."
::= { radiusDynAuthServerEntry 4 }

radiusDynAuthServerID OBJECT-TYPE
SYNTAX     SnmpAdminString
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
    "The NAS-Identifier of the RADIUS Dynamic
    Authorization server referred to in this table
    entry."
REFERENCE
    "RFC 2865, Section 5.32, NAS-Identifier."
::= { radiusDynAuthServerEntry 5 }

radiusDynAuthClientRoundTripTime OBJECT-TYPE
SYNTAX     TimeTicks
UNITS      "hundredths of a second"
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
    "The time interval (in hundredths of a second) between
    the most recent Disconnect or CoA request and the
    reception of the corresponding Disconnect or CoA reply.
    A value of zero is returned in case no reply has been
    received yet from this server."
::= { radiusDynAuthServerEntry 6 }

radiusDynAuthClientDisconRequests OBJECT-TYPE
SYNTAX     Counter32
UNITS "requests"
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of RADIUS Disconnect-Requests sent to this Dynamic Authorization server."
REFERENCE "RFC 3576, Section 2.1, Disconnect Messages (DM)."
::= { radiusDynAuthServerEntry 7 }

radiusDynAuthClientDisconRetransmissions OBJECT-TYPE
SYNTAX Counter32
UNITS "retransmissions"
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of RADIUS Disconnect-request packets retransmitted to this RADIUS Dynamic authorization server."
REFERENCE "RFC 3576, Section 2.1, Disconnect Messages (DM)."
::= { radiusDynAuthServerEntry 8 }

radiusDynAuthClientDisconAcks OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of RADIUS Disconnect-ACK packets received from this Dynamic Authorization server."
REFERENCE "RFC 3576, Section 2.1, Disconnect Messages (DM)."
::= { radiusDynAuthServerEntry 9 }

radiusDynAuthClientDisconNaks OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of RADIUS Disconnect-NAK packets received from this Dynamic Authorization server."
REFERENCE "RFC 3576, Section 2.1, Disconnect Messages (DM)."
::= { radiusDynAuthServerEntry 10 }

radiusDynAuthClientMalformedDisconResponses OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of malformed RADIUS Disconnect-Response packets received from this Dynamic Authorization server. Bad authenticators and unknown types are not included as malformed Disconnect-Responses."
REFERENCE
"RFC 3576, Section 2.1, Disconnect Messages (DM), and Section 2.3, Packet Format."
::= { radiusDynAuthServerEntry 11 }

radiusDynAuthClientDisconBadAuthenticators OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS Disconnect-Response packets which contained invalid Signature attributes received from this Dynamic Authorization server."
REFERENCE
"RFC 3576, Section 2.1, Disconnect Messages (DM), and Section 2.3, Packet Format."
::= { radiusDynAuthServerEntry 12 }

radiusDynAuthClientDisconPendingRequests OBJECT-TYPE
SYNTAX Gauge32
UNITS "requests"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS Disconnect-request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Disconnect-Request is sent and decremented due to receipt of an Disconnect-Ack, Disconnect-NAK or a timeout or a retransmission."
REFERENCE
"RFC 3576, Section 2.1, Disconnect Messages (DM)."
::= { radiusDynAuthServerEntry 13 }

radiusDynAuthClientDisconTimeouts OBJECT-TYPE
SYNTAX Counter32
UNITS "timeouts"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of Disconnect request timeouts to this server. After a timeout the client may retry to the same 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 Disconnect-Request as well as a timeout."
REFERENCE
"RFC 3576, Section 2.1, Disconnect Messages (DM)."
::= { radiusDynAuthServerEntry 14 }

radiusDynAuthClientDisconPacketsDropped OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of incoming Disconnect-Responses from this Dynamic Authorization server silently discarded by the client application for some reason other than malformed, bad authenticators or unknown types."
REFERENCE
"RFC 3576, Section 2.1, Disconnect Messages (DM), and Section 2.3, Packet Format."
::= { radiusDynAuthServerEntry 15 }

radiusDynAuthClientCoARequests OBJECT-TYPE
SYNTAX Counter32
UNITS "requests"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS CoA-Requests sent to this Dynamic Authorization server."
REFERENCE
"RFC 3576, Section 2.2, Change-of-Authorization Messages (CoA)."
::= { radiusDynAuthServerEntry 16 }

radiusDynAuthClientCoARetransmissions OBJECT-TYPE
SYNTAX Counter32
UNITS "retransmissions"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS CoA-request packets..."
retransmitted to this RADIUS Dynamic authorization server."
REFERENCE
"RFC 3576, Section 2.2, Change-of-Authorization
Messages (CoA)."
::= { radiusDynAuthServerEntry 17 }

radiusDynAuthClientCoAacks OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of RADIUS CoA-ACK packets
received from this Dynamic Authorization server"
REFERENCE
"RFC 3576, Section 2.2, Change-of-Authorization
Messages (CoA)."
::= { radiusDynAuthServerEntry 18 }

radiusDynAuthClientCoANaks OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of RADIUS CoA-NAK packets
received from this Dynamic Authorization server." 
REFERENCE
"RFC 3576, Section 2.2, Change-of-Authorization
Messages (CoA)."
::= { radiusDynAuthServerEntry 19 }

radiusDynAuthClientMalformedCoAResponses OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of malformed RADIUS CoA-Response
packets received from this Dynamic Authorization
server. Bad authenticators and unknown types are
not included as malformed CoA-Responses."
REFERENCE
"RFC 3576, Section 2.2, Change-of-Authorization
Messages (CoA), and Section 2.3, Packet Format."
::= { radiusDynAuthServerEntry 20 }
radiusDynAuthClientCoABadAuthenticators OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of RADIUS CoA-Response packets
which contained invalid Signature attributes
received from this Dynamic Authorization server."
REFERENCE "RFC 3576, Section 2.2, Change-of-Authorization
Messages (CoA), and Section 2.3, Packet Format."
 ::= {radiusDynAuthServerEntry 21 }

radiusDynAuthClientCoAPendingRequests OBJECT-TYPE
SYNTAX Gauge32
UNITS "requests"
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of RADIUS CoA-request packets destined for
this server that have not yet timed out or received a
response. This variable is incremented when an
CoA-Request is sent and decremented due to receipt of
a CoA-Ack, CoA -NAK or a timeout or a retransmission."
REFERENCE "RFC 3576, Section 2.2, Change-of-Authorization
Messages (CoA)."
 ::= {radiusDynAuthServerEntry 22 }

radiusDynAuthClientCoATimeouts OBJECT-TYPE
SYNTAX Counter32
UNITS "timeouts"
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of CoA request timeouts to this server.
After a timeout the client may retry to the same
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 CoA-Request as well
as a timeout."
REFERENCE "RFC 3576, Section 2.2, Change-of-Authorization
Messages (CoA)."
 ::= {radiusDynAuthServerEntry 23 }

radiusDynAuthClientCoAPacketsDropped OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of incoming CoA-Responses from this Dynamic Authorization server silently discarded by the client application for some reason other than malformed, bad authenticators or unknown types."
REFERENCE "RFC 3576, Section 2.2, Change-of-Authorization Messages (CoA), and Section 2.3, Packet Format."
::= { radiusDynAuthServerEntry 24 }

radiusDynAuthClientUnknownTypes OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of incoming packets of unknown types which were received on the Dynamic Authorization port."
REFERENCE "RFC 3576, Section 2.3, Packet Format."
::= { radiusDynAuthServerEntry 25 }

-- conformance information
radiusDynAuthClientMIBConformance
OBJECT IDENTIFIER ::= { radiusDynAuthClientMIB 2 }
radiusDynAuthClientMIBCompliances
OBJECT IDENTIFIER ::= { radiusDynAuthClientMIBConformance 1 }
radiusDynAuthClientMIBGroups
OBJECT IDENTIFIER ::= { radiusDynAuthClientMIBConformance 2 }

-- compliance statements
radiusDynAuthClientMIBCompliance MODULE-COMPLIANCE
STATUS current
DESCRIPTION "The compliance statement for entities implementing the RADIUS Dynamic Authorization Client."
MODULE -- this module
MANDATORY-GROUPS { radiusDynAuthClientMIBGroup }
::= { radiusDynAuthClientMIBCompliances 1 }

-- units of conformance
radiusDynAuthClientMIBGroup OBJECT-GROUP
OBJECTS { radiusDynAuthClientInvalidServerAddresses,
radiusDynAuthServerAddressType,
radiusDynAuthServerAddress,
radiusDynAuthServerClientPortNumber,
radiusDynAuthServerID,
radiusDynAuthClientRoundTripTime,
radiusDynAuthClientDisconRequests,
radiusDynAuthClientDisconRetransmissions,
radiusDynAuthClientDisconAcks,
radiusDynAuthClientDisconNaks,
radiusDynAuthClientMalformedDisconResponses,
radiusDynAuthClientDisconBadAuthenticators,
radiusDynAuthClientDisconPendingRequests,
radiusDynAuthClientDisconTimeouts,
radiusDynAuthClientDisconPacketsDropped,
radiusDynAuthClientCoARequests,
radiusDynAuthClientCoARetransmissions,
radiusDynAuthClientCoAAcks,
radiusDynAuthClientCoANaks,
radiusDynAuthClientMalformedCoAResponses,
radiusDynAuthClientCoABadAuthenticators,
radiusDynAuthClientCoAPendingRequests,
radiusDynAuthClientCoATimeouts,
radiusDynAuthClientCoAPacketsDropped,
radiusDynAuthClientUnknownTypes
}
STATUS  current
DESCRIPTION
"The collection of objects providing management of a RADIUS Dynamic Authorization Client."
::= { radiusDynAuthClientMIBGroups 1 }
7. Security Considerations

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

radiusDynAuthServerAddress and radiusDynAuthServerAddressType

These can be used to determine the address of the DAS with which the DAC is communicating. This information could be useful in mounting an attack on the DAS.

radiusDynAuthServerID

This can be used to determine the Identifier of the DAS. This information could be useful in impersonating the DAS.

radiusDynAuthServerClientPortNumber

This can be used to determine the port number on which the DAC is sending. This information could be useful in mounting an attack on the DAS.

The other readable objects are not really considered as being sensitive or vulnerable. These objects are:
radiusDynAuthClientInvalidServerAddresses,
radiusDynAuthClientRoundTripTime,
radiusDynAuthClientDisconRequests,
radiusDynAuthClientDisconRetransmissions,
radiusDynAuthClientDisconAcks,
radiusDynAuthClientDisconNaks,
radiusDynAuthClientMalformedDisconResponses,
radiusDynAuthClientDisconBadAuthenticators,
radiusDynAuthClientDisconPendingRequests,
radiusDynAuthClientDisconTimeouts,
radiusDynAuthClientDisconPacketsDropped,
radiusDynAuthClientCoARetransmissions,
radiusDynAuthClientCoARequests,
radiusDynAuthClientCoAAcks,
radiusDynAuthClientCoANaks,
radiusDynAuthClientMalformedCoAResponses,
radiusDynAuthClientCoABadAuthenticators,
radiusDynAuthClientCoAPendingRequests,
radiusDynAuthClientCoATimeouts,
radiusDynAuthClientCoAPacketsDropped, and
radiusDynAuthClientUnknownTypes.

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.
8. IANA considerations

IANA is requested to assign an OID under mib-2.
9. Acknowledgements

This document reuses some of the work done in earlier RADIUS MIB specifications [RFC2619] and [RFC2621].

The authors would also like to acknowledge the following people for their comments to this document: Anjaneyulu Pata, Dan Romascanu, and Bert Wijnen.
10. References

10.1 Normative References


10.2 Informative References


Authors’ Addresses

Stefaan De Cnodder
Alcatel
Francis Wellesplein 1
B-2018 Antwerp
Belgium

Phone: +32 3 240 85 15
Email: stefaan.de_cnodder@alcatel.be

Nagi Reddy Jonnala
Future Soft
480 - 481, Anna Salai
Nandanam, Chennai
India

Email: nagi_reddy.jonnala@alcatel.be

Murtaza Chiba
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose CA, 95134

Phone: +1 408 525 7198
Email: mchiba@cisco.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 (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.