

Network Working Group  
Internet-Draft  
Expires: November 19, 2005

S. De Cnodder  
Alcatel  
N. Jonnala  
Consult  
M. Chiba  
Cisco Systems, Inc.  
May 18, 2005

Dynamic Authorization Client MIB  
draft-ietf-radext-dynauth-client-mib-00.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/lid-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 November 19, 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](#).

Internet-Draft

Dynamic Authorization Client MIB

May 2005

## Table of Contents

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

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. [\[DYNSERV\]](#) 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.



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,  
InetPortNumber FROM INET-ADDRESS-MIB  
MODULE-COMPLIANCE, OBJECT-GROUP FROM SNMPv2-CONF;

radiusDynAuthClientMIB MODULE-IDENTITY

LAST-UPDATED "200505160000Z" -- 16 May 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

E-Mail: stefaan.de\_cnodder@alcatel.be

Nagi Reddy Jonnala  
Consult  
4-486, Nutakki  
AP, India, PIN: 522303

Phone: +91 8645 275314

E-Mail: nagireddyj@yahoo.com

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

Phone: +1 408 525 7198

E-Mail: 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 yyyy;

---

```
        for full legal notices see the RFC itself.  Supplementary
        information may be available on
        http://www.ietf.org/copyrights/ianamib.html."
-- RFC Ed.: replace yyyy with actual RFC number & remove this note

        REVISION "200505160000Z" -- 16 May 2005
        DESCRIPTION "Initial version as published in RFC yyyy"
-- RFC Ed.: replace yyyy with actual RFC number & remove this note
        ::= { radiusDynamicAuthorization 2 }

radiusDynamicAuthorization    OBJECT IDENTIFIER ::= { mib-2 xxx }
-- The value xxx to be assigned by IANA.

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 InetPortNumber,
    radiusDynAuthServerID             SnmpAdminString,
    radiusDynAuthClientRoundTripTime  TimeTicks,
    radiusDynAuthClientDisconRequests Counter32,
    radiusDynAuthClientDisconRetransmissions Counter32,
    radiusDynAuthClientDisconAcks     Counter32,
    radiusDynAuthClientDisconNaks     Counter32,
    radiusDynAuthClientMalformedDisconResponses Counter32,
    radiusDynAuthClientDisconBadAuthenticators Counter32,
    radiusDynAuthClientDisconPendingRequests Gauge32,
    radiusDynAuthClientDisconTimeouts Counter32,
    radiusDynAuthClientDisconPacketsDropped Counter32,
    radiusDynAuthClientCoARequests    Counter32,
    radiusDynAuthClientCoARetransmissions 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

De Cnodder, et al.

Expires November 19, 2005

[Page 10]

---

Internet-Draft

Dynamic Authorization Client MIB

May 2005

"The type of IP-Address of the RADIUS Dynamic  
Authorization server referred to in this table entry."  
 ::= { radiusDynAuthServerEntry 2 }

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 InetPortNumber  
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 Counter32

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 }

```
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
```

De Cnodder, et al.

Expires November 19, 2005

[Page 17]

---

Internet-Draft

Dynamic Authorization Client MIB

May 2005

```
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 }
```

END

De Cnodder, et al.

Expires November 19, 2005

[Page 18]

---

Internet-Draft

Dynamic Authorization Client MIB

May 2005

## [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,  
radiusDynAuthClientCoARequests,  
radiusDynAuthClientCoARetransmissions,  
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

- [DYNSERV] De Cnodder, S., Jonnala, N., and M. Chiba, "RADIUS Dynamic Auhtorization Server MIB", [draft-decnodder-radext-dynauth-server-mib-01.txt](#), work in progress, June 2004.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), March 1997.
- [RFC2578] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Structure of Management Information Version 2 (SMIV2)", STD 58, [RFC 2578](#), April 1999.
- [RFC2579] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Textual Conventions for SMIV2", STD 58, [RFC 2579](#), April 1999.
- [RFC2580] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Conformance Statements for SMIV2", STD 58, [RFC 2580](#), April 1999.
- [RFC3576] Chiba, M., Dommetry, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", [RFC 3576](#), July 2003.

### 10.2 Informative References

- [RFC2618] Aboba, B. and G. Zorn, "RADIUS Authentication Client MIB", [RFC 2618](#), June 1999.
- [RFC2619] Zorn, G. and B. Aboba, "RADIUS Authentication Server MIB", [RFC 2619](#), June 1999.
- [RFC2620] Aboba, B. and G. Zorn, "RADIUS Accounting Client MIB", [RFC 2620](#), June 1999.
- [RFC2621] Zorn, G. and B. Aboba, "RADIUS Accounting Server MIB", [RFC 2621](#), 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.

Internet-Draft

Dynamic Authorization Client MIB

May 2005

#### 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  
Consult  
4-486, Nutakki  
AP, India, PIN: 522303

Phone: +91 8645 275314  
Email: nagireddyj@yahoo.com

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

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

Internet-Draft

Dynamic Authorization Client MIB

May 2005

### 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](mailto: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.