RADIUS Dynamic Authorization Server MIB

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

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 Remote Authentication Dial-In User Service (RADIUS) (RFC 2865) Dynamic Authorization Server (DAS) functions that support the dynamic authorization extensions as defined in RFC 3576.

Table of Contents

1. Introduction ....................................................2  
   1.1. Requirements Notation ......................................2  
   1.2. Terminology ................................................2  
2. The Internet-Standard Management Framework ......................2  
3. Overview ........................................................3  
4. RADIUS Dynamic Authorization Server MIB Definitions .............5  
5. Security Considerations ........................................20  
6. IANA Considerations ............................................21  
7. Acknowledgements ...............................................21  
8. References .....................................................21  
   8.1. Normative References ......................................21  
   8.2. Informative References ....................................22
1. 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. This RADIUS Dynamic Authorization Server (DAS) MIB complements the managed objects used for managing RADIUS authentication and accounting clients as described in [RFC4668] and [RFC4670], respectively.

1.1. 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].

1.2. Terminology

Dynamic Authorization Server (DAS)

The component that resides on the NAS that processes the Disconnect and Change-of-Authorization (CoA) Request packets [RFC3576] sent by the Dynamic Authorization Client.

Dynamic Authorization Client (DAC)

The component that sends Disconnect and CoA-Request packets to the Dynamic Authorization Server. Although this component often resides on the RADIUS server, it is also possible for it to be located on a separate host, such as a Rating Engine.

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.

2. 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].

De Cnodder, et al.                    Informational                      [Page 2]
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].

3. Overview

"Dynamic Authorization Extensions to RADIUS" [RFC3576] defines the operation of Disconnect-Request, Disconnect-ACK, Disconnect-NAK, CoA-Request, CoA-ACK, and CoA-NAK packets. Typically, NAS devices implement the DAS function, and thus would be expected to implement the RADIUS Dynamic Authorization Server MIB, whereas DACs implement the client function and thus would be expected to implement the RADIUS Dynamic Authorization Client MIB.

However, it is possible for a RADIUS Dynamic Authorization entity to perform both client and server functions. For example, a RADIUS proxy may act as a DAS to one or more DACs while simultaneously acting as a DAC to one or more DASs. In such situations, it is expected that RADIUS entities combining client and server functionality will support both the client and server MIBs.

This memo describes the MIB for Dynamic Authorization Servers and relates to the following documents as follows:

[RFC4668] describes the MIB for a RADIUS Auth Client MIB.
[RFC4669] describes the MIB for a RADIUS Auth Server MIB.
[RFC4670] describes the MIB for a RADIUS Acct Client MIB.
[RFC4671] describes the MIB for a RADIUS Acct Server MIB.
[RFC4672] describes the MIB for a RADIUS Dynamic Auth Client.

A NAS typically implements the MIBs for a RADIUS Authentication Client, a RADIUS accounting client, and a RADIUS Dynamic Authorization Server. However, any one MIB can be implemented without implementing any of the other MIBs; i.e., the MIBs have no dependencies on each other. A typical case would be for a device to implement the MIBs RADIUS authentication server, RADIUS accounting server, and RADIUS Dynamic Authorization Client. A RADIUS proxy might implement any, all, or a subset of the MIBs listed above and the MIB as defined in this document.
This MIB module for the Dynamic Authorization Server contains the following:

1. Three scalar objects.

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

RADIUS DYNAUTH SERVER MIB DEFINITIONS ::= BEGIN

IMPORTS
MODULE-IDENTITY, OBJECT-TYPE,
Counter32, Integer32, mib-2,
TimeTicks FROM SNMPv2-SMI -- [RFC2578]
SnmpAdminString FROM SNMP-FRAMEWORK-MIB -- [RFC3411]
InetAddressType,
InetAddress FROM INET-ADDRESS-MIB -- [RFC4001]
MODULE-COMPLIANCE,
OBJECT-GROUP FROM SNMPv2-CONF; -- [RFC2580]

radiusDynAuthServerMIB MODULE-IDENTITY
LAST-UPDATED "200608290000Z" -- 29 August 2006
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 Jonnala
  Cisco Systems, Inc.
  Divyasree Chambers, B Wing,
  O’Shaugnessy Road,
  Bangalore-560027, India.

  Phone: +91 94487 60828
  EMail: njonnala@cisco.com

  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 server
side of the Dynamic Authorization Extensions to the
Remote Authentication Dial-In User Service (RADIUS)
radiusDynAuthServerMIBObjects OBJECT IDENTIFIER ::= 
    { mib-2 146 }

radiusDynAuthServerScalars    OBJECT IDENTIFIER ::= 
    { radiusDynAuthServerMIBObjects 1 }

radiusDynAuthServerDisconInvalidClientAddresses OBJECT-TYPE
SYNTAX  Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "The number of Disconnect-Request packets received from
unknown addresses. This counter may experience a
discontinuity when the DAS module (re)starts, as
indicated by the value of
radiusDynAuthServerCounterDiscontinuity."
 ::= { radiusDynAuthServerScalars 1 }

radiusDynAuthServerCoAInvalidClientAddresses OBJECT-TYPE
SYNTAX  Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "The number of CoA-Request packets received from unknown
addresses. This counter may experience a discontinuity
when the DAS module (re)starts, as indicated by the
value of radiusDynAuthServerCounterDiscontinuity."
 ::= { radiusDynAuthServerScalars 2 }

radiusDynAuthServerIdentifier OBJECT-TYPE
SYNTAX  SnmpAdminString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "The NAS-Identifier of the RADIUS Dynamic Authorization
Server. This is not necessarily the same as sysName in
MIB II."
REFERENCE
    "RFC 2865, Section 5.32, NAS-Identifier."
 ::= { radiusDynAuthServerScalars 3 }
radiusDynAuthClientTable OBJECT-TYPE
SYNTAX SEQUENCE OF RadiusDynAuthClientEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"The (conceptual) table listing the RADIUS Dynamic
Authorization Clients with which the server shares a
secret."
 ::= { radiusDynAuthServerMIBObjects 2 }

radiusDynAuthClientEntry OBJECT-TYPE
SYNTAX RadiusDynAuthClientEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"An entry (conceptual row) representing one Dynamic
Authorization Client with which the server shares a
secret."
INDEX { radiusDynAuthClientIndex }
 ::= { radiusDynAuthClientTable 1 }

RadiusDynAuthClientEntry ::= SEQUENCE {
   radiusDynAuthClientIndex                     Integer32,
   radiusDynAuthClientAddressType               InetAddressType,
   radiusDynAuthClientAddress                   InetAddress,
   radiusDynAuthServDisconRequests              Counter32,
   radiusDynAuthServDisconAuthOnlyRequests      Counter32,
   radiusDynAuthServDupDisconRequests           Counter32,
   radiusDynAuthServDisconAcks                  Counter32,
   radiusDynAuthServDisconNaks                  Counter32,
   radiusDynAuthServDisconNakAuthOnlyRequests   Counter32,
   radiusDynAuthServDisconNakSessNoContext      Counter32,
   radiusDynAuthServDisconUserSessRemoved       Counter32,
   radiusDynAuthServMalformedDisconRequests     Counter32,
   radiusDynAuthServDisconBadAuthenticators     Counter32,
   radiusDynAuthServDisconPacketsDropped        Counter32,
   radiusDynAuthServCoARequests                 Counter32,
   radiusDynAuthServCoAAuthOnlyRequests         Counter32,
   radiusDynAuthServDupCoARequests              Counter32,
   radiusDynAuthServCoAAcks                     Counter32,
   radiusDynAuthServCoANaks                     Counter32,
   radiusDynAuthServCoANakAuthOnlyRequests      Counter32,
   radiusDynAuthServCoANakSessNoContext         Counter32,
   radiusDynAuthServCoAUserSessChanged          Counter32,
   radiusDynAuthServMalformedCoARequests        Counter32,
   radiusDynAuthServCoABadAuthenticators        Counter32,
   radiusDynAuthServCoAPacketsDropped           Counter32,
   radiusDynAuthServUnknownTypes                Counter32,
}
radiusDynAuthServerCounterDiscontinuity OBJECT-TYPE
SYNTAX TimeTicks
DESCRIPTION "Time between the last two RADIUS Dynamic Authorization Server MIB updates."
::= { radiusDynAuthServerEntry 1 }

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

radiusDynAuthClientAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The type of IP address of the RADIUS Dynamic Authorization Client referred to in this table entry."
::= { radiusDynAuthClientEntry 2 }

radiusDynAuthClientAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The IP address value of the RADIUS Dynamic Authorization Client referred to in this table entry, using the version neutral IP address format. The type of this address is determined by the value of the radiusDynAuthClientAddressType object."
::= { radiusDynAuthClientEntry 3 }

radiusDynAuthServDisconRequests OBJECT-TYPE
SYNTAX Counter32
UNITS "requests"
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The number of RADIUS Disconnect-Requests received from this Dynamic Authorization Client. This also includes the RADIUS Disconnect-Requests that have a Service-Type attribute with value 'Authorize Only'. This counter may experience a discontinuity when the
DAS module (re)starts as indicated by the value of
radiusDynAuthServerCounterDiscontinuity.

REFERENCE
"RFC 3576, Section 2.1, Disconnect Messages (DM)."
 ::= { radiusDynAuthClientEntry 4 }

radiusDynAuthServDisconAuthOnlyRequests OBJECT-TYPE
SYNTAX Counter32
UNITS "requests"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS Disconnect-Requests that include
a Service-Type attribute with value ‘Authorize Only’
received from this Dynamic Authorization Client. This
counter may experience a discontinuity when the DAS
module (re)starts, as indicated by the value of
radiusDynAuthServerCounterDiscontinuity."

REFERENCE
"RFC 3576, Section 2.1, Disconnect Messages (DM)."
 ::= { radiusDynAuthClientEntry 5 }

radiusDynAuthServDupDisconRequests OBJECT-TYPE
SYNTAX Counter32
UNITS "requests"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of duplicate RADIUS Disconnect-Request
packets received from this Dynamic Authorization
Client. This counter may experience a discontinuity
when the DAS module (re)starts, as indicated by the
value of radiusDynAuthServerCounterDiscontinuity."

REFERENCE
"RFC 3576, Section 2.1, Disconnect Messages (DM)."
 ::= { radiusDynAuthClientEntry 6 }

radiusDynAuthServDisconAcks OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS Disconnect-ACK packets sent to
this Dynamic Authorization Client. This counter may
experience a discontinuity when the DAS module
(re)starts, as indicated by the value of
radiusDynAuthServerCounterDiscontinuity."
REFERENCE
  "RFC 3576, Section 2.1, Disconnect Messages (DM)."
 ::= { radiusDynAuthClientEntry 7 }

radiusDynAuthServDisconNaks OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
  "The number of RADIUS Disconnect-NAK packets
  sent to this Dynamic Authorization Client. This
  includes the RADIUS Disconnect-NAK packets sent
  with a Service-Type attribute with value ‘Authorize
  Only’ and the RADIUS Disconnect-NAK packets sent
  because no session context was found. This counter
  may experience a discontinuity when the DAS module
  (re)starts, as indicated by the value of
  radiusDynAuthServerCounterDiscontinuity."
REFERENCE
  "RFC 3576, Section 2.1, Disconnect Messages (DM)."
 ::= { radiusDynAuthClientEntry 8 }

radiusDynAuthServDisconNakAuthOnlyRequests OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
  "The number of RADIUS Disconnect-NAK packets that
  include a Service-Type attribute with value
  ‘Authorize Only’ sent to this Dynamic Authorization
  Client. This counter may experience a discontinuity
  when the DAS module (re)starts, as indicated by the
  value of radiusDynAuthServerCounterDiscontinuity."
REFERENCE
  "RFC 3576, Section 2.1, Disconnect Messages (DM)."
 ::= { radiusDynAuthClientEntry 9 }

radiusDynAuthServDisconNakSessNoContext OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
  "The number of RADIUS Disconnect-NAK packets
  sent to this Dynamic Authorization Client
  because no session context was found. This counter may
experience a discontinuity when the DAS module
(re)starts, as indicated by the value of
radiusDynAuthServerCounterDiscontinuity.

REFERENCE
  "RFC 3576, Section 2.1, Disconnect Messages (DM)."
::= { radiusDynAuthClientEntry 10 }

radiusDynAuthServDisconUserSessRemoved OBJECT-TYPE
SYNTAX  Counter32
UNITS    "sessions"
MAX-ACCESS read-only
STATUS   current
DESCRIPTION
  "The number of user sessions removed for the
  Disconnect-Requests received from this
  Dynamic Authorization Client. Depending on site-
  specific policies, a single Disconnect request
  can remove multiple user sessions. In cases where
  this Dynamic Authorization Server has no
  knowledge of the number of user sessions that
  are affected by a single request, each such
  Disconnect-Request will count as a single
  affected user session only. This counter may experience
  a discontinuity when the DAS module (re)starts, as
  indicated by the value of
  radiusDynAuthServerCounterDiscontinuity."
REFERENCE
  "RFC 3576, Section 2.1, Disconnect Messages (DM)."
::= { radiusDynAuthClientEntry 11 }

radiusDynAuthServMalformedDisconRequests OBJECT-TYPE
SYNTAX  Counter32
UNITS    "requests"
MAX-ACCESS read-only
STATUS   current
DESCRIPTION
  "The number of malformed RADIUS Disconnect-Request
  packets received from this Dynamic Authorization
  Client. Bad authenticators and unknown types are not
  included as malformed Disconnect-Requests. This counter
  may experience a discontinuity when the DAS module
  (re)starts, as indicated by the value of
  radiusDynAuthServerCounterDiscontinuity."
REFERENCE
  "RFC 3576, Section 2.1, Disconnect Messages (DM), and
  Section 2.3, Packet Format."
::= { radiusDynAuthClientEntry 12 }
radiusDynAuthServDisconBadAuthenticators OBJECT-TYPE
SYNTAX     Counter32
UNITS      "requests"
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
  "The number of RADIUS Disconnect-Request packets that contained an invalid Authenticator field received from this Dynamic Authorization Client. This counter may experience a discontinuity when the DAS module (re)starts, as indicated by the value of radiusDynAuthServerCounterDiscontinuity."
REFERENCE  
  "RFC 3576, Section 2.1, Disconnect Messages (DM), and Section 2.3, Packet Format."
::= { radiusDynAuthClientEntry 13 }

radiusDynAuthServDisconPacketsDropped OBJECT-TYPE
SYNTAX     Counter32
UNITS      "requests"
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
  "The number of incoming Disconnect-Requests from this Dynamic Authorization Client silently discarded by the server application for some reason other than malformed, bad authenticators, or unknown types. This counter may experience a discontinuity when the DAS module (re)starts, as indicated by the value of radiusDynAuthServerCounterDiscontinuity."
REFERENCE  
  "RFC 3576, Section 2.1, Disconnect Messages (DM), and Section 2.3, Packet Format."
::= { radiusDynAuthClientEntry 14 }

radiusDynAuthServCoARequests OBJECT-TYPE
SYNTAX     Counter32
UNITS      "requests"
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
  "The number of RADIUS CoA-requests received from this Dynamic Authorization Client. This also includes the CoA requests that have a Service-Type attribute with value 'Authorize Only'. This counter may experience a discontinuity when the DAS module (re)starts, as indicated by the value of radiusDynAuthServerCounterDiscontinuity."

De Cnodder, et al.           Informational                     [Page 12]
radiusDynAuthServCoAAuthOnlyRequests OBJECT-TYPE
SYNTAX Counter32
UNITS "requests"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS CoA-requests that include a Service-Type attribute with value ‘Authorize Only’ received from this Dynamic Authorization Client. This counter may experience a discontinuity when the DAS module (re)starts, as indicated by the value of radiusDynAuthServerCounterDiscontinuity."
REFERENCE
"RFC 3576, Section 2.2, Change-of-Authorization Messages (CoA)."
 ::= { radiusDynAuthClientEntry 15 }

radiusDynAuthServDupCoARequests OBJECT-TYPE
SYNTAX Counter32
UNITS "requests"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of duplicate RADIUS CoA-Request packets received from this Dynamic Authorization Client. This counter may experience a discontinuity when the DAS module (re)starts, as indicated by the value of radiusDynAuthServerCounterDiscontinuity."
REFERENCE
"RFC 3576, Section 2.2, Change-of-Authorization Messages (CoA)."
 ::= { radiusDynAuthClientEntry 16 }

radiusDynAuthServCoAAcks OBJECT-TYPE
SYNTAX Counter32
UNITS "replies"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS CoA-ACK packets sent to this Dynamic Authorization Client. This counter may experience a discontinuity when the DAS module
(re)starts, as indicated by the value of radiusDynAuthServerCounterDiscontinuity.

REFERENCE
"RFC 3576, Section 2.2, Change-of-Authorization Messages (CoA)."
::= { radiusDynAuthClientEntry 18 }

radiusDynAuthServCoANaks OBJECT-TYPE
SYNTAX     Counter32
UNITS      "replies"
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
"The number of RADIUS CoA-NAK packets sent to this Dynamic Authorization Client. This includes the RADIUS CoA-NAK packets sent with a Service-Type attribute with value ‘Authorize Only’ and the RADIUS CoA-NAK packets sent because no session context was found. This counter may experience a discontinuity when the DAS module (re)starts, as indicated by the value of radiusDynAuthServerCounterDiscontinuity."

REFERENCE
"RFC 3576, Section 2.2, Change-of-Authorization Messages (CoA)."
::= { radiusDynAuthClientEntry 19 }

radiusDynAuthServCoANakAuthOnlyRequests OBJECT-TYPE
SYNTAX     Counter32
UNITS      "replies"
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
"The number of RADIUS CoA-NAK packets that include a Service-Type attribute with value ‘Authorize Only’ sent to this Dynamic Authorization Client. This counter may experience a discontinuity when the DAS module (re)starts, as indicated by the value of radiusDynAuthServerCounterDiscontinuity."

REFERENCE
"RFC 3576, Section 2.2, Change-of-Authorization Messages (CoA)."
::= { radiusDynAuthClientEntry 20 }

radiusDynAuthServCoANakSessNoContext OBJECT-TYPE
SYNTAX     Counter32
UNITS      "replies"
MAX-ACCESS read-only
STATUS     current
DESCRIPTION

"The number of RADIUS CoA-NAK packets sent to this
Dynamic Authorization Client because no session context
was found. This counter may experience a discontinuity
when the DAS module (re)starts, as indicated by the
value of radiusDynAuthServerCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.2, Change-of-Authorization
Messages (CoA)."

::= { radiusDynAuthClientEntry 21 }

radiusDynAuthServCoAUserSessChanged OBJECT-TYPE
SYNTAX Counter32
UNITS "sessions"
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The number of user sessions authorization
changed for the CoA-Requests received from this
Dynamic Authorization Client. Depending on site-
specific policies, a single CoA request can change
multiple user sessions’ authorization. In cases where
this Dynamic Authorization Server has no knowledge of
the number of user sessions that are affected by a
single request, each such CoA-Request will
count as a single affected user session only. This
counter may experience a discontinuity when the DAS
module (re)starts, as indicated by the value of
radiusDynAuthServerCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.2, Change-of-Authorization
Messages (CoA)."

::= { radiusDynAuthClientEntry 22 }

radiusDynAuthServMalformedCoARequests OBJECT-TYPE
SYNTAX Counter32
UNITS "requests"
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The number of malformed RADIUS CoA-Request packets
received from this Dynamic Authorization Client. Bad
authenticators and unknown types are not included as
malformed CoA-Requests. This counter may experience a
discontinuity when the DAS module (re)starts, as
indicated by the value of
radiusDynAuthServerCounterDiscontinuity."

REFERENCE
"RFC 3576, Section 2.2, Change-of-Authorization Messages (CoA), and Section 2.3, Packet Format."
::= { radiusDynAuthClientEntry 23 }

radiusDynAuthServCoABadAuthenticators OBJECT-TYPE
SYNTAX Counter32
UNITS "requests"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of RADIUS CoA-Request packets that contained an invalid Authenticator field received from this Dynamic Authorization Client. This counter may experience a discontinuity when the DAS module (re)starts, as indicated by the value of radiusDynAuthServerCounterDiscontinuity."
REFERENCE
"RFC 3576, Section 2.2, Change-of-Authorization Messages (CoA), and Section 2.3, Packet Format."
::= { radiusDynAuthClientEntry 24 }

radiusDynAuthServCoAPacketsDropped OBJECT-TYPE
SYNTAX Counter32
UNITS "requests"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of incoming CoA packets from this Dynamic Authorization Client silently discarded by the server application for some reason other than malformed, bad authenticators, or unknown types. This counter may experience a discontinuity when the DAS module (re)starts, as indicated by the value of radiusDynAuthServerCounterDiscontinuity."
REFERENCE
"RFC 3576, Section 2.2, Change-of-Authorization Messages (CoA), and Section 2.3, Packet Format."
::= { radiusDynAuthClientEntry 25 }

radiusDynAuthServUnknownTypes OBJECT-TYPE
SYNTAX Counter32
UNITS "requests"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of incoming packets of unknown types that were received on the Dynamic Authorization port. This counter may experience a discontinuity when the DAS
module (re)starts, as indicated by the value of radiusDynAuthServerCounterDiscontinuity."

REFERENCE
"RFC 3576, Section 2.3, Packet Format."
 ::= { radiusDynAuthClientEntry 26 }

radiusDynAuthServerCounterDiscontinuity OBJECT-TYPE
SYNTAX TimeTicks
UNITS "hundredths of a second"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The time (in hundredths of a second) since the last counter discontinuity. A discontinuity may be the result of a reinitialization of the DAS module within the managed entity."
 ::= { radiusDynAuthClientEntry 27 }

-- conformance information

radiusDynAuthServerMIBConformance
OBJECT IDENTIFIER ::= { radiusDynAuthServerMIB 2 }

radiusDynAuthServerMIBCompliances
OBJECT IDENTIFIER ::= { radiusDynAuthServerMIBConformance 1 }

radiusDynAuthServerMIBGroups
OBJECT IDENTIFIER ::= { radiusDynAuthServerMIBConformance 2 }

-- compliance statements

radiusAuthServerMIBCompliance MODULE-COMPLIANCE
STATUS current
DESCRIPTION
"The compliance statement for entities implementing the RADIUS Dynamic Authorization Server. Implementation of this module is for entities that support IPv4 and/or IPv6."

MODULE -- this module
MANDATORY-GROUPS { radiusDynAuthServerMIBGroup }

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

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

GROUP             radiusDynAuthServerAuthOnlyGroup
DESCRIPTION
"Only required for Dynamic Authorization Clients that
are supporting Service-Type attributes with value
'Authorize-Only'."

GROUP             radiusDynAuthServerNoSessGroup
DESCRIPTION
"This group is not required if the Dynamic
Authorization Server cannot easily determine whether
a session exists (e.g., in case of a RADIUS
proxy)."

::= { radiusDynAuthServerMIBCompliances 1 }

-- units of conformance

radiusDynAuthServerMIBGroup OBJECT-GROUP
  OBJECTS { radiusDynAuthServerDisconInvalidClientAddresses,
             radiusDynAuthServerCoAInvalidClientAddresses,
             radiusDynAuthServerIdentifier,
             radiusDynAuthClientAddressType,
             radiusDynAuthClientAddress,
             radiusDynAuthServDisconRequests,
             radiusDynAuthServDupDisconRequests,
             radiusDynAuthServDisconAcks,
             radiusDynAuthServDisconNaks,
             radiusDynAuthServDisconUserSessRemoved,
             radiusDynAuthServMalformedDisconRequests,
             radiusDynAuthServDisconBadAuthenticators,
             radiusDynAuthServDisconPacketsDropped,
             radiusDynAuthServCoARequests,
             radiusDynAuthServDupCoARequests,
             radiusDynAuthServCoAacks,
             radiusDynAuthServCoANaks,
             radiusDynAuthServCoAUserSessChanged,
             radiusDynAuthServMalformedCoARequests,
             radiusDynAuthServCoABadAuthenticators,
             radiusDynAuthServCoAPacketsDropped,
             radiusDynAuthServUnknownTypes,
             radiusDynAuthServerCounterDiscontinuity
  }

STATUS  current
DESCRIPTION
"The collection of objects providing management of a RADIUS Dynamic Authorization Server."
 ::= { radiusDynAuthServerMIBGroups 1 }

radiusDynAuthServerAuthOnlyGroup OBJECT-GROUP
 OBJECTS { radiusDynAuthServDisconAuthOnlyRequests,
radiusDynAuthServDisconNakAuthOnlyRequests,
radiusDynAuthServCoAAuthOnlyRequests,
radiusDynAuthServCoANakAuthOnlyRequests }
 STATUS current
 DESCRIPTION
"The collection of objects supporting the RADIUS messages including Service-Type attribute with value 'Authorize Only'."
 ::= { radiusDynAuthServerMIBGroups 2 }

radiusDynAuthServerNoSessGroup OBJECT-GROUP
 OBJECTS { radiusDynAuthServDisconNakSessNoContext,
radiusDynAuthServCoANakSessNoContext }
 STATUS current
 DESCRIPTION
"The collection of objects supporting the RADIUS messages that are referring to non-existing sessions."
 ::= { radiusDynAuthServerMIBGroups 3 }

END
5. 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:

radiusDynAuthClientAddress and radiusDynAuthClientAddressType

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

radiusDynAuthServerIdentifier

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

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.
6. IANA Considerations

The IANA has assigned OID number 146 under mib-2.

7. Acknowledgements

The authors would like to acknowledge the following people for their comments on this document: Bernard Aboba, Alan DeKok, David Nelson, Anjaneyulu Pata, Dan Romascanu, Juergen Schoenwaelder, Greg Weber, Bert Wijnen, and Glen Zorn.

8. References

8.1. Normative References


8.2. 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
Cisco Systems, Inc.
Divyasree Chambers, B Wing, O'Shaugnessy Road
Bangalore-560027, India

Phone: +91 94487 60828
EMail: njonnala@cisco.com

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

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