

Network Working Group
Request for Comments: 4672
Category: Informational

S. De Cnodder
Alcatel
N. Jonnala
M. Chiba
Cisco Systems, Inc.
September 2006

RADIUS Dynamic Authorization Client 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) (RFC2865) Dynamic Authorization Client (DAC) 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	3
3. Overview	3
4. RADIUS Dynamic Authorization Client MIB Definitions	3
5. Security Considerations	19
6. IANA Considerations	20
7. Acknowledgements	20
8. References	21
8.1. Normative References	21
8.2. Informative References	21

1. Introduction

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) [RFC2865] Dynamic Authorization Client (DAC) functions that support the dynamic authorization extensions as defined in RFC 3576.

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 Client MIB complements the managed objects used for managing RADIUS authentication and accounting servers, as described in [RFC4669] and [RFC4671], 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 this component 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].

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. [RFC4673] defines the Dynamic Authorization Server MIB and the relationship with other MIB modules. This MIB module for the Dynamic Authorization Client contains the following:

1. Two scalar objects
2. One Dynamic Authorization Server table. This table contains one row for each DAS with which the DAC shares a secret.

4. 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          -- [RFC2578]
    SnmpAdminString       FROM SNMP-FRAMEWORK-MIB -- [RFC3411]
    InetAddressType, InetAddress,
    InetPortNumber        FROM INET-ADDRESS-MIB   -- [RFC4001]
    MODULE-COMPLIANCE,
    OBJECT-GROUP           FROM SNMPv2-CONF;      -- [RFC2580]
```

```
radiusDynAuthClientMIB 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 client side of the Dynamic Authorization Extensions to the Remote Authentication Dial-In User Service (RADIUS) protocol. Copyright (C) The Internet Society (2006). Initial version as published in RFC 4672; for full legal notices see the RFC itself."

REVISION "200609290000Z" -- 29 August 2006

DESCRIPTION "Initial version as published in RFC 4672"

::= { mib-2 145 }

radiusDynAuthClientMIBObjects OBJECT IDENTIFIER ::=

{ radiusDynAuthClientMIB 1 }

radiusDynAuthClientScalars OBJECT IDENTIFIER ::=

{ radiusDynAuthClientMIBObjects 1 }

radiusDynAuthClientDisconInvalidServerAddresses OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of Disconnect-Ack and Disconnect-NAK packets

received from unknown addresses. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

```
::= { radiusDynAuthClientScalars 1 }
```

radiusDynAuthClientCoAInvalidServerAddresses OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of CoA-Ack and CoA-NAK packets received from unknown addresses. Disconnect-NAK packets received from unknown addresses. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

```
::= { radiusDynAuthClientScalars 2 }
```

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."

```
::= { radiusDynAuthClientMIBObjects 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

radiusDynAuthServerAddressType

radiusDynAuthServerAddress

radiusDynAuthServerClientPortNumber

radiusDynAuthServerID

radiusDynAuthClientRoundTripTime

radiusDynAuthClientDisconRequests

Integer32,

InetAddressType,

InetAddress,

InetPortNumber,

SnmpAdminString,

TimeTicks,

Counter32,

```

radiusDynAuthClientDisconAuthOnlyRequests      Counter32,
radiusDynAuthClientDisconRetransmissions        Counter32,
radiusDynAuthClientDisconAcks                   Counter32,
radiusDynAuthClientDisconNaks                   Counter32,
radiusDynAuthClientDisconNakAuthOnlyRequest    Counter32,
radiusDynAuthClientDisconNakSessNoContext       Counter32,
radiusDynAuthClientMalformedDisconResponses    Counter32,
radiusDynAuthClientDisconBadAuthenticators     Counter32,
radiusDynAuthClientDisconPendingRequests       Gauge32,
radiusDynAuthClientDisconTimeouts              Counter32,
radiusDynAuthClientDisconPacketsDropped        Counter32,
radiusDynAuthClientCoARequests                 Counter32,
radiusDynAuthClientCoAAuthOnlyRequest          Counter32,
radiusDynAuthClientCoARetranmissions           Counter32,
radiusDynAuthClientCoAAcks                     Counter32,
radiusDynAuthClientCoANaks                     Counter32,
radiusDynAuthClientCoANakAuthOnlyRequest       Counter32,
radiusDynAuthClientCoANakSessNoContext         Counter32,
radiusDynAuthClientMalformedCoAResponses       Counter32,
radiusDynAuthClientCoABadAuthenticators        Counter32,
radiusDynAuthClientCoAPendingRequests          Gauge32,
radiusDynAuthClientCoATimeouts                 Counter32,
radiusDynAuthClientCoAPacketsDropped           Counter32,
radiusDynAuthClientUnknownTypes                Counter32,
radiusDynAuthClientCounterDiscontinuity        TimeTicks
}

```

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."

::= { 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 using the version neutral IP address format. The type of this address is determined by the value of the radiusDynAuthServerAddressType object."

::= { radiusDynAuthServerEntry 3 }

radiusDynAuthServerClientPortNumber OBJECT-TYPE

SYNTAX InetPortNumber (1..65535)

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The UDP destination port that the RADIUS Dynamic Authorization Client is using to send requests to this server. The value zero is invalid."

::= { 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. This is not necessarily the same as sysName in MIB II."

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 receipt of the corresponding Disconnect or CoA reply. A value of zero is returned if 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. This also includes the RADIUS Disconnect-Requests that have a Service-Type attribute with value 'Authorize Only'. Disconnect-NAK packets received from unknown addresses. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.1, Disconnect Messages (DM)."

::= { radiusDynAuthServerEntry 7 }

radiusDynAuthClientDisconAuthOnlyRequests 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' sent to this Dynamic Authorization Server. Disconnect-NAK packets received from unknown addresses. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.1, Disconnect Messages (DM)."

::= { radiusDynAuthServerEntry 8 }

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. Disconnect-NAK packets received from unknown addresses. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.1, Disconnect Messages (DM)."
 ::= { radiusDynAuthServerEntry 9 }

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. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.1, Disconnect Messages (DM)."

::= { radiusDynAuthServerEntry 10 }

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. This includes the RADIUS Disconnect-NAK packets received with a Service-Type attribute with value 'Authorize Only' and the RADIUS Disconnect-NAK packets received if no session context was found. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.1, Disconnect Messages (DM)."

::= { radiusDynAuthServerEntry 11 }

radiusDynAuthClientDisconNakAuthOnlyRequest 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' received from this Dynamic Authorization Server. This counter may experience a discontinuity when the DAC module (re)starts, as

indicated by the value of
radiusDynAuthClientCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.1, Disconnect Messages (DM)."

::= { radiusDynAuthServerEntry 12 }

radiusDynAuthClientDisconNakSessNoContext 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 because no session context was found; i.e., it includes an Error-Cause attribute with value 503 ('Session Context Not Found'). This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.1, Disconnect Messages (DM)."

::= { radiusDynAuthServerEntry 13 }

radiusDynAuthClientMalformedDisconResponses OBJECT-TYPE

SYNTAX Counter32

UNITS "replies"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of malformed RADIUS Disconnect-Ack and Disconnect-NAK packets received from this Dynamic Authorization Server. Bad authenticators and unknown types are not included as malformed Disconnect-Ack and Disconnect-NAK packets. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.1, Disconnect Messages (DM), and Section 2.3, Packet Format."

::= { radiusDynAuthServerEntry 14 }

radiusDynAuthClientDisconBadAuthenticators OBJECT-TYPE

SYNTAX Counter32

UNITS "replies"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of RADIUS Disconnect-Ack and Disconnect-NAK packets that contained invalid Authenticator field received from this Dynamic Authorization Server. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.1, Disconnect Messages (DM), and Section 2.3, Packet Format."

::= { radiusDynAuthServerEntry 15 }

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 a Disconnect-Ack, a Disconnect-NAK, a timeout, or a retransmission."

REFERENCE

"RFC 3576, Section 2.1, Disconnect Messages (DM)."

::= { radiusDynAuthServerEntry 16 }

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 and as a timeout. A send to a different server is counted as a Disconnect-Request and as a timeout. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.1, Disconnect Messages (DM)."

::= { radiusDynAuthServerEntry 17 }

radiusDynAuthClientDisconPacketsDropped OBJECT-TYPE

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

"The number of incoming Disconnect-Ack and Disconnect-NAK packets from this Dynamic Authorization Server silently discarded by the client application for some reason other than malformed, bad authenticators, or unknown types. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.1, Disconnect Messages (DM), and Section 2.3, Packet Format."

::= { radiusDynAuthServerEntry 18 }

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. This also includes CoA requests that have a Service-Type attribute with value 'Authorize Only'. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

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

::= { radiusDynAuthServerEntry 19 }

radiusDynAuthClientCoAAuthOnlyRequest 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' sent to this Dynamic Authorization Client. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

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

::= { radiusDynAuthServerEntry 20 }

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. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

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

::= { radiusDynAuthServerEntry 21 }

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. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

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

::= { radiusDynAuthServerEntry 22 }

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. This includes the RADIUS CoA-NAK packets received with a Service-Type attribute with value 'Authorize Only' and the RADIUS CoA-NAK packets received because no session context

was found. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

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

::= { radiusDynAuthServerEntry 23 }

radiusDynAuthClientCoANakAuthOnlyRequest 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' received from this Dynamic Authorization Server. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

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

::= { radiusDynAuthServerEntry 24 }

radiusDynAuthClientCoANakSessNoContext 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 because no session context was found; i.e., it includes an Error-Cause attribute with value 503 ('Session Context Not Found'). This counter may experience a discontinuity when the DAC module (re)starts as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

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

::= { radiusDynAuthServerEntry 25 }

radiusDynAuthClientMalformedCoAResponses OBJECT-TYPE

SYNTAX Counter32

UNITS "replies"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

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

REFERENCE

"RFC 3576, Section 2.2, Change-of-Authorization Messages (CoA), and Section 2.3, Packet Format."

::= { radiusDynAuthServerEntry 26 }

radiusDynAuthClientCoABadAuthenticators OBJECT-TYPE

SYNTAX Counter32

UNITS "replies"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of RADIUS CoA-Ack and CoA-NAK packets that contained invalid Authenticator field received from this Dynamic Authorization Server. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.2, Change-of-Authorization Messages (CoA), and Section 2.3, Packet Format."

::= { radiusDynAuthServerEntry 27 }

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, a CoA-NAK, or a timeout, or a retransmission."

REFERENCE

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

::= { radiusDynAuthServerEntry 28 }

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 and as a timeout. A send to a different server is counted as a CoA-Request and as a timeout. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

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

::= { radiusDynAuthServerEntry 29 }

radiusDynAuthClientCoAPacketsDropped OBJECT-TYPE

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

"The number of incoming CoA-Ack and CoA-NAK from this Dynamic Authorization Server silently discarded by the client application for some reason other than malformed, bad authenticators, or unknown types. This counter may experience a discontinuity when the DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.2, Change-of-Authorization Messages (CoA), and Section 2.3, Packet Format."

::= { radiusDynAuthServerEntry 30 }

radiusDynAuthClientUnknownTypes OBJECT-TYPE

SYNTAX Counter32
UNITS "replies"
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 DAC module (re)starts, as indicated by the value of radiusDynAuthClientCounterDiscontinuity."

REFERENCE

"RFC 3576, Section 2.3, Packet Format."

::= { radiusDynAuthServerEntry 31 }

radiusDynAuthClientCounterDiscontinuity 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 DAC module within the managed entity."

::= { radiusDynAuthServerEntry 32 }

-- 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. Implementation of this module is for entities that support IPv4 and/or IPv6."

MODULE -- this module

MANDATORY-GROUPS { radiusDynAuthClientMIBGroup }

OBJECT radiusDynAuthServerAddressType

SYNTAX InetAddressType { ipv4(1), ipv6(2) }

DESCRIPTION

"An implementation is only required to support IPv4 and globally unique IPv6 addresses."

OBJECT radiusDynAuthServerAddress

SYNTAX InetAddress (SIZE(4|16))

DESCRIPTION

"An implementation is only required to support IPv4 and globally unique IPv6 addresses."

```

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

```

```

GROUP                radiusDynAuthClientNoSessGroup
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)."
```

```
 ::= { radiusDynAuthClientMIBCompliances 1 }
```

```
-- units of conformance
```

```

radiusDynAuthClientMIBGroup OBJECT-GROUP
    OBJECTS { radiusDynAuthClientDisconInvalidServerAddresses,
               radiusDynAuthClientCoAInvalidServerAddresses,
               radiusDynAuthServerAddressType,
               radiusDynAuthServerAddress,
               radiusDynAuthServerClientPortNumber,
               radiusDynAuthServerID,
               radiusDynAuthClientRoundTripTime,
               radiusDynAuthClientDisconRequests,
               radiusDynAuthClientDisconRetransmissions,
               radiusDynAuthClientDisconAcks,
               radiusDynAuthClientDisconNaks,
               radiusDynAuthClientMalformedDisconResponses,
               radiusDynAuthClientDisconBadAuthenticators,
               radiusDynAuthClientDisconPendingRequests,
               radiusDynAuthClientDisconTimeouts,
               radiusDynAuthClientDisconPacketsDropped,
               radiusDynAuthClientCoARequests,
               radiusDynAuthClientCoARetransmissions,
               radiusDynAuthClientCoAAcks,
               radiusDynAuthClientCoANaks,
               radiusDynAuthClientMalformedCoAResponses,
               radiusDynAuthClientCoABadAuthenticators,
               radiusDynAuthClientCoAPendingRequests,
               radiusDynAuthClientCoATimeouts,
               radiusDynAuthClientCoAPacketsDropped,
               radiusDynAuthClientUnknownTypes,
               radiusDynAuthClientCounterDiscontinuity
            }
    STATUS current

```

DESCRIPTION

"The collection of objects providing management of
a RADIUS Dynamic Authorization Client."

::= { radiusDynAuthClientMIBGroups 1 }

radiusDynAuthClientAuthOnlyGroup OBJECT-GROUP

OBJECTS { radiusDynAuthClientDisconAuthOnlyRequests,
radiusDynAuthClientDisconNakAuthOnlyRequest,
radiusDynAuthClientCoAAAuthOnlyRequest,
radiusDynAuthClientCoANakAuthOnlyRequest
}

STATUS current

DESCRIPTION

"The collection of objects supporting the RADIUS
messages including Service-Type attribute with
value 'Authorize Only'."

::= { radiusDynAuthClientMIBGroups 2 }

radiusDynAuthClientNoSessGroup OBJECT-GROUP

OBJECTS { radiusDynAuthClientDisconNakSessNoContext,
radiusDynAuthClientCoANakSessNoContext
}

STATUS current

DESCRIPTION

"The collection of objects supporting the RADIUS
messages that are referring to non-existing sessions."

::= { radiusDynAuthClientMIBGroups 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:

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 destination port number to which the DAC is sending. This information could be useful in mounting an attack on 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 145 under mib-2.

7. Acknowledgements

The authors would also 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

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2578] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.
- [RFC2579] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "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.
- [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.
- [RFC3576] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.
- [RFC4001] Daniele, M., Haberman, B., Routhier, S., and J. Schoenwaelder, "Textual Conventions for Internet Network Addresses", RFC 4001, February 2005.

8.2. Informative References

- [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.
- [RFC4669] Nelson, D., "RADIUS Authentication Server MIB for IPv6", RFC 4669, August 2006.
- [RFC4671] Nelson, D., "RADIUS Accounting Server MIB for IPv6", RFC 4671, August 2006.

[RFC4673] De Cnodder, S., Jonnala, N., and M. Chiba, "RADIUS Dynamic Authorization Server MIB", RFC 4673, September 2006.

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).

