Network Working Group
INTERNET-DRAFT
<draft-aboba-dynradius-01.txt>
19 November 1997

Bernard Aboba
Microsoft

Lightweight Directory Access Protocol (v3):
Dynamic Attributes for the Remote Access Dialin User Service (RADIUS)

1. Status of this Memo

This document is an Internet-Draft. 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.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the Internet-Drafts Shadow Directories on ds.internic.net (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

The distribution of this memo is unlimited. It is filed as <draft-aboba-dynradius-01.txt>, and expires June 1, 1998. Please send comments to the authors.

2. Abstract

This document defines dynamic attributes used by the Remote Access Dialin User Service (RADIUS). These attributes are written to a dynamic directory service by the RADIUS server in order to provide information about sessions in progress. This information can then be used in order to provide for control of simultaneous logins, or for detection or tracking of security incidents in progress.

3. Introduction

The RADIUS protocol, described in [6]-[9], supports authentication, authorization and accounting for dialup users. To date, RADIUS servers have retrieved their configuration from user databases and/or flat configuration files. In order to consolidate stores of user information, it is desirable to integrate a RADIUS with an LDAP-based directory service.

This document is one of three related specifications which describe how a RADIUS server may be integrated with an LDAP-based directory service. Reference [14] specifies how user data utilized by a RADIUS

server may be stored in an LDAP-based directory service. Reference [15] describes how user credentials submitted during PPP authentication and sent by the NAS in the RADIUS Access-Request may be validated by the RADIUS server.

This document describes how a dynamic directory service may be used to store these and other attributes relating to sessions in progress. Such information can be useful for a variety of purposes including security incident response; simultaneous usage control; or monitoring of connection quality, login time, packet size or bandwidth usage. Due to the frequency of changes to this data, dynamic attributes must be employed, as described in [5] and [10].

Attributes useful for this purpose include attributes from both the Access-Request and Access-Reply. For example, attributes such as Nas-IP-Address, Nas-Port, Nas-Identifier, Called-Station-Id, Calling-Station-Id, and Connect-Info are available from the RADIUS Access-Request packet. Other attributes such as Framed-IP-Address may be computed dynamically, and sent in the RADIUS Access-Accept packet. Attributes relating to a user's resource consumption during a session in progress are made available via the Interim Accounting Record Extension described in [9]. These include Acct-Input-Octets, Acct-Output-Octets, Acct-Session-Id, Acct-Authentic, Acct-Session-Time, Acct-Input-Packets, Acct-Output-Packets, Acct-Terminate-Cause, Acct-Multi-Session-Id, Acct-Link-Count, Acct-Tunnel-Client-Endpoint, and Act-Tunnel-Connection-Id.

Typically it is expected that the RADIUS server will create an entry in the dynamic directory service after a successful authentication, and will delete the entry when the user logs off. However, some implementations may find it desirable to allow persistence of entries relating to failed authentications or logged off users. In this case, a refresh interval is typically set (for example, 24 hours) so that the entries will timeout after an appropriate interval.

3.1. Example

Let us assume that BIGCO wishes to offer dialin access to their domestic sales force, as well as VPN access to contractors and finance employees travelling overseas. In order to consistently manage and account for the use of their NAS devices and Layer 2 tunnel servers (PPTP/L2F/L2TP), BIGCO has chosen to adopt the RADIUS protocol.

As part of this service offering, BIGCO may wish to restrict contractors and finance employees to a single login at a time. In order to implement this policy, it is necessary for the BIGCO RADIUS server to be able to retrieve the number of sessions in progress for a particular user.

BIGCO may also wish to implement auditing and alarming policies. For

example, BIGCO may wish to set an alarm when contractors remain continously logged on for more than a certain amount of time, attempt to access the network from more than one location simultaneously, or

transfer more than a threshold number of octets during a given time period. It may also be desirable to set a threshold on failed authentications during a given time period, in order to detect break-ins in progress.

If an alarm is triggered, it may be desirable to have access to the Nas-IP-Address, Nas-Port, Called-Station-Id and Calling-Station-Id for the failed login attempt or session in progress so that the call may be traced.

4. Object definitions

The RADIUS dynamic attribute schema includes definition of the following objects:

Dynamic RADIUS Person Class

4.1. Dynamic RADIUS Person Class

```
( DynamicRadiusPersonClass 1
    NAME 'dynamicRadiusPersonClass'
    SUP top
    STRUCTURAL
    MUST (
           userName $ acctSessionId $ connectionStatus
    )
    MAY ( nasIPAddress $ nasPort $ framedIPAddress $
          class $ calledStationId $ callingStationId $
          nasIdentifier $ acctInputOctets $
          acctOutputOctets $ acctAuthentic $
          acctSessionTime $ acctInputPackets $ acctOutputPackets $
          acctTerminateCause $ acctMultiSessionId $ acctLinkCount $
          acctInputGigawords $ acctOutputGigawords $
          nasPortType $ tunnelType $ tunnelMediumType $
          acctTunnelClientEndpoint $ acctTunnelConnection $
          tunnelPrivateGroupId $ connectInfo $ authenticationType $
          eapType $ encryptionType $ sessionLocalStartTime $
          sessionLocalEndTime $ ispId $ connectionStatus $
          serviceClass
        )
)
```

5. Attribute definitions

5.1. New Attribute Types Used in the Dynamic RADIUS Person Class

```
   ( radius dynamicRadiusPersonClass 1
       NAME 'userName'
```

```
       DESC 'the name of the user'
       EQUALITY caseIgnoreIA5Match
       SYNTAX 'IA5String{128}'
       SINGLE-VALUE
)

   ( radius dynamicRadiusPersonClass 4
       NAME 'nasIPAddress'
       DESC 'IP address of the NAS'
       EQUALITY caseIgnoreIA5Match
       SYNTAX 'IA5String{128}'
       SINGLE-VALUE
)

   ( radius dynamicRadiusPersonClass 5
       NAME 'nasPort'
       DESC 'Physical port number of the NAS
            Authenticating the user'
       EQUALITY integerMatch
       SYNTAX 'INTEGER'
       SINGLE-VALUE
)

   ( radius dynamicRadiusPersonClass 8
       NAME 'framedIPAddress'
       DESC 'IP address to be assigned to the user
            in dotted decimal notation'
       EQUALITY caseIgnoreIA5Match
       SYNTAX 'IA5String{128}'
       SINGLE-VALUE
    )

   ( radius dynamicRadiusPersonClass 25
       NAME 'class'
       DESC 'The service class for the user'
       EQUALITY caseIgnoreIA5Match
       SYNTAX 'IA5String{128}'
    )

   ( radius dynamicRadiusPersonClass 30
       NAME 'calledStationId'
       DESC 'Phone number to which the user placed the call'
       EQUALITY caseIgnoreIA5Match
       SYNTAX 'IA5String{128}'
    )

   ( radius dynamicRadiusPersonClass 31
       NAME 'callingStationId'
       DESC 'Phone number from which the user placed the call'
       EQUALITY caseIgnoreIA5Match
       SYNTAX 'IA5String{128}'
```

```
    )
   ( radius dynamicRadiusPersonClass 32
```

```
            NAME 'nasIdentifier'
            DESC 'String identifying the NAS'
            EQUALITY caseIgnoreIA5Match
            SYNTAX 'IA5String{128}'
            SINGLE-VALUE
         )

        ( radius dynamicRadiusPersonClass 42
            NAME 'acctInputOctets'
            DESC 'How many octets have been received from the port during the
session'
            EQUALITY integerMatch
            SYNTAX 'INTEGER'
            SINGLE-VALUE
         )

        ( radius dynamicRadiusPersonClass 43
            NAME 'acctOutputOctets'
            DESC 'How many octets have been sent to the port during the session'
            EQUALITY integerMatch
            SYNTAX 'INTEGER'
            SINGLE-VALUE
         )

        ( radius dynamicRadiusPersonClass 44
            NAME 'acctSessionId'
            DESC 'Unique Accounting ID string for the session'
            EQUALITY caseIgnoreIA5Match
            SYNTAX 'IA5String{128}'
            SINGLE-VALUE
         )

        ( radius dynamicRadiusPersonClass 45
            NAME 'acctAuthentic'
            DESC 'Indicates how the user was authenticated. Values include
RADIUS
                  (1), Local (2), Remote (3)'
            EQUALITY integerMatch
            SYNTAX 'INTEGER'
            SINGLE-VALUE
         )

        ( radius dynamicRadiusPersonClass 46
            NAME 'acctSessionTime'
            DESC 'How many seconds the user has received service for'
            EQUALITY integerMatch
            SYNTAX 'INTEGER'
            SINGLE-VALUE
         )

        ( radius dynamicRadiusPersonClass 47
```

```
            NAME 'acctInputPackets'
            DESC 'How many packets have been received from the port during the
session'
            EQUALITY integerMatch
            SYNTAX 'INTEGER'
            SINGLE-VALUE
```

```
         )

        ( radius dynamicRadiusPersonClass 48
            NAME 'acctOutputPackets'
            DESC 'How many packets have been sent to the port during the
session'
            EQUALITY integerMatch
            SYNTAX 'INTEGER'
            SINGLE-VALUE
         )

        ( radius dynamicRadiusPersonClass 49
            NAME 'acctTerminateCause'
            DESC 'Integer identifying how the session was terminated.'
            EQUALITY integerMatch
            SYNTAX 'INTEGER'
            SINGLE-VALUE
         )

        ( radius dynamicRadiusPersonClass 50
            NAME 'acctMultiSessionId'
            DESC 'Unique string linking together multiple related sessions.'
            EQUALITY caseIgnoreIA5Match
            SYNTAX 'IA5String{128}'
         )

        ( radius dynamicRadiusPersonClass 51
            NAME 'acctLinkCount'
            DESC 'Count of links in a multilink session at time of last
measurement.'
            EQUALITY integerMatch
            SYNTAX 'INTEGER'
         )

        ( radius dynamicRadiusPersonClass 52
            NAME 'acctInputGigawords'
            DESC 'This is an extended accounting attribute, included
                  to allow for keeping track of long or fast sessions. If
                  used, it represents bits 32-63 of the number of inbound
                  octets during the session.'
            EQUALITY integerMatch
            SYNTAX 'INTEGER'
            SINGLE-VALUE
         )

        ( radius dynamicRadiusPersonClass 53
            NAME 'acctOutputGigawords'
            DESC 'This is an extended accounting attribute, included
                  to allow for keeping track of long or fast sessions. If
                  used, it represents bits 32-63 of the number of outbound
                  octets during the session.'
```

```
        EQUALITY integerMatch
        SYNTAX 'INTEGER'
        SINGLE-VALUE
    )
```

```
        ( radius dynamicRadiusPersonClass 61
            NAME 'nasPortType'
            DESC 'Port on which the user has logged in. Values include
                  Async(1), Sync(2), ISDN Sync(3), V.120(4), V.110(5) and
Virtual(6).'
            EQUALITY integerMatch
            SYNTAX 'INTEGER'
         )

        ( radius dynamicRadiusPersonClass 64
            NAME 'tunnelType'
            DESC 'Type of tunnel set up. Values include
                  PPTP(1), L2F(2), L2TP(3), ATMP(4), VTP(5),
                  AH(6), IP-IP(7)'
            EQUALITY integerMatch
            SYNTAX 'INTEGER'
            SINGLE-VALUE
         )

        ( radius dynamicRadiusPersonClass 65
            NAME 'tunnelMediumType'
            DESC 'Medium tunnel runs over. Values include IP(1),
                  X.25(2), ATM(3), Frame Relay(4).'
            EQUALITY integerMatch
            SYNTAX 'INTEGER'
            SINGLE-VALUE
         )

        ( radius dynamicRadiusPersonClass 66
            NAME 'acctTunnelClientEndpoint'
            DESC 'This is the address of the Tunnel Client Endpoint.'
            EQUALITY caseIgnoreIA5Match
            SYNTAX 'IA5String{128}'
            SINGLE-VALUE
         )

        ( radius dynamicRadiusPersonClass 67
            NAME 'tunnelServerEndpoint'
            DESC 'The address of the tunnel server. The format
                  of the string depends on the tunnelMediumType
                  attribute.'
            EQUALITY integerMatch
            SYNTAX 'INTEGER'
            SINGLE-VALUE
         )

        ( radius dynamicRadiusPersonClass 68
            NAME 'acctTunnelConnection'
            DESC 'This is the connection Id assigned to the call; it is
included in
                  Accounting-Request packets and written to ILS. A tag field
```

```
lives
                in the first four octets.'
            EQUALITY caseIgnoreIA5Match
            SYNTAX 'IA5String{128}'
            SINGLE-VALUE
         )
```

```
   ( radius dynamicRadiusPersonClass 69
       NAME 'tunnelPrivateGroupId'
       DESC 'This is the private group Id assigned to the call.
             A tag field lives in the first four octets.'
       EQUALITY caseIgnoreIA5Match
       SYNTAX 'IA5String{128}'
       SINGLE-VALUE
   )

 ( radius dynamicRadiusPersonClass 77
       NAME 'connectInfo'
       DESC 'This is the connect string returned by the modem in the
             initial connection, or by post-termination diagnostics.'
       EQUALITY caseIgnoreIA5Match
       SYNTAX 'IA5String{128}'
   )

   ( radius dynamicRadiusPersonClass 257
       NAME 'authenticationType'
       DESC 'This attribute indicates the authentication
            type for the user. Values include PAP (1),
            CHAP(2), EAP(3), MS-CHAP(4), and SPAP(5).'
       EQUALITY integerMatch
       SYNTAX 'INTEGER'
       SINGLE-VALUE
    )

   ( radius dynamicRadiusPersonClass 258
       NAME 'eapType'
       DESC 'This attribute indicates the EAP type for this
            user. It should only have a value when EAP is
            enabled for the user.'
       EQUALITY integerMatch
       SYNTAX 'INTEGER'
       SINGLE-VALUE
    )

   ( radius dynamicRadiusPersonClass 259
       NAME 'encryptionType'
       DESC 'Encryption type used (40-bit RC4 (1), 128-bit RC4 (2)).'
       EQUALITY integerMatch
       SYNTAX 'INTEGER'
       SINGLE-VALUE
    )

   ( radius dynamicRadiusPersonClass 260
       NAME 'sessionLocalStartTime'
       DESC 'This is a timestamp giving session start in local time.'
       EQUALITY caseIgnoreIA5Match
       SYNTAX 'IA5String{128}'
       SINGLE-VALUE
```

```
    )
   ( radius dynamicRadiusPersonClass 261
```

```
      NAME 'sessionLocalEndTime'
      DESC 'This is a timestamp giving session end in local time.'
      EQUALITY caseIgnoreIA5Match
      SYNTAX 'IA5String{128}'
      SINGLE-VALUE
   )

  ( radius dynamicRadiusPersonClass 262
      NAME 'ispId'
      DESC 'String identifying the local ISP to which the user
            is connected'
      EQUALITY caseIgnoreIA5Match
      SYNTAX 'IA5String{128}'
      SINGLE-VALUE
   )

  ( radius dynamicRadiusPersonClass 263
      NAME 'connectionStatus'
      DESC 'Indicates status of the connection. Values include
            Failed Authentication (1), Logged On (2), or
            Logged Off (3).'
      EQUALITY integerMatch
      SYNTAX 'INTEGER'
      SINGLE-VALUE
   )

  ( radius dynamicRadiusPersonClass 264
      NAME 'serviceClass'
      DESC ' String identifying class of service given to user.'
      EQUALITY caseIgnoreIA5Match
      SYNTAX 'IA5String{128}'
      SINGLE-VALUE
   )
```

6. Acknowledgments

Thanks to David Eitelbach, Ashwin Palenkar and Gurdeep Singh Pall of Microsoft for useful discussions of this problem space.

7. References

[1] W. Yeong, T. Howes, S. Kille, "Lightweight Directory Access Protocol." RFC 1777, March 1995.

[2] "Information Processing Systems - Open Systems Interconnection - The Directory: Overview of Concepts, Models and Service." ISO/IEC JTC 1/SC21, International Standard 9594-1, 1988.

[3] "Information Processing Systems - Open Systems Interconnection -

The Directory: Selected Object Classes." Recommendation X.521 ISO/IEC JTC 1/SC21, International Standard 9594-7, 1993.

[4] M. Wahl, A. Coulbeck, T. Howes, S. Kille, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions. " Internet Draft (work in progress), draft-ietf-asid-ldapv3-attributes-08.txt, Critical Angle, Isode, Netscape, October 1997.

[5] Y. Yaacovi, M. Wahl, T. Genovese, "Lightweight Directory Access Protocol (v3): Extensions for Dynamic Directory Services. " Internet Draft (work in progress), draft-ietf-asid-ldapv3-dynamic-06.txt, Microsoft, Critical Angle, September 1997.

[6] C. Rigney, A. Rubens, W. Simpson, S. Willens. "Remote Authentication Dial In User Service (RADIUS)." RFC 2138, Livingston, Merit, Daydreamer, April 1997.

[7] C. Rigney. "RADIUS Accounting." RFC 2139, Livingston, April 1997.

[8] C. Rigney, W. Willats. "RADIUS Extensions." Work in progress, draft-ietf-radius-ext-01.txt, Livingston, June 1997.

[9] P.R. Calhoun, M.A. Beadles, A. Ratcliffe. "RADIUS Accounting Interim Accounting Record Extension." Work in progress, draft-ietf-radius-acct-interim-00.txt, 3Com, CompuServe, UUNET, July 1997.

[10] Y. Yaacovi, M. Wahl, T. Genovese, "Lightweight Directory Access Protocol: Dynamic Attributes." Internet Draft (work in progress), draft-ietf-asid-dynatt-00.txt, Microsoft, Critical Angle, July 1997.

[11] J. Hodges, R.L. Morgan, M. Wahl, "Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security." Internet Draft (work in progress), draft-ietf-asid-ldapv3-tls-01.txt, Stanford, Critical Angle, June 1997.

[12] M. Wahl, T. Hoews, S. Kille, "Lightweight Directory Access Protocol (v3)." Internet Draft (work in progress), draft-ietf-asid-protocol-08.txt, Critical Angle, Netscape, Isode, October 1997.

[13] M. Wahl, T. Hoews, S. Kille, "Lightweight Directory Access Protocol (v3)." Internet Draft (work in progress), draft-ietf-asid-protocol-08.txt, Critical Angle, Netscape, Isode, October 1997.

[14] B. Aboba, "Lightweight Directory Access Protocol (v3): Schema for the Remote Access Dialin User Service (RADIUS) " Internet Draft (work in progress), draft-aboba-radius-01.txt, Microsoft, November 1997.

[15] B. Aboba, "Lightweight Directory Access Protocol (v3): Extension for PPP Authentication" Internet Draft (work in progress), draft-aboba-ppp-01.txt, Microsoft, November 1997.

[16] T. Howes, L. Howard, "A Simple Caching Scheme for LDAP and X.500 Directories." Internet Draft (work in progress), draft-ietf-asid-

8. Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: 425-936-6605
EMail: bernarda@microsoft.com