RADIUS

BayLISA

Mountain View, California

February 15,1996

Carl Rigney

Livingston Enterprises, Inc.

cdr@livingston.com

REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

- *Why* is RADIUS needed?
- *What* is RADIUS?
- *How* does RADIUS work?
- *Who* does RADIUS?
- *Where* can you find out more about RADIUS?

WHY IS RADIUS NEEDED?

- Dial-In desireable but Security a must
- Scalability
- Single Point of Administration
- Way to Link Network Access Servers and Authentication Methods

WHAT IS RADIUS?

- UDP/IP based Protocol for a Network Access Server (NAS) to communicate with a database server of authorized users
- Authentication
- Authorization
- Accounting (optionally)
- Simple, Flexible, Scalable, Reliable

HOW DOES RADIUS WORK?

- NAS prompts dial-in user for Username, Password
- NAS encrypts Password and sends that and Username to RADIUS server in an *access-request* packet
- RADIUS server looks up Username in database, confirms Password, and sends back packet with one of 3 responses:
  - *access-accept* (and includes authorization information)
  - *access-reject* (with optional message)
  - *access-challenge* (with optional message and state)
- If NAS receives *access-challenge* it may prompt the user for additional information and send another *access-request* to the RADIUS server, including the state attribute sent in the *access-challenge*
- Works with PAP, CHAP

WHO DOES RADIUS?

- Originally written by Steve Willens of Livingston Enterprises and distributed freely
- Many other NAS and smart card vendors supporting or adopting RADIUS
- RADIUS Working Group formed at 32nd IETF to document it as a standards-track RFC

WHERE CAN YOU FIND OUT MORE?

- ftp://ftp.livingston.com/pub/radius/
  - current Internet-Drafts
  - archive of ietf-radius mailing list
- ietf-radius-request@livingston.com
  - Mailing list for RADIUS Working Group
  - To join, send email with "`subscribe`" in body
- cdr@livingston.com
  - To contact RADIUS Working Group Chair and Document Editor, Carl Rigney
- ftp://ftp.livingston.com/pub/le/radius/
  - RADIUS 1.16 server source
  - white paper with more information
- info@livingston.com
  - For more information on Livingston Enterprises
- resume@livingston.com
  - Just in case you were curious

RADIUS PACKET

Code	Identifier	Length
Authenticator		
Attributes ...		

Code = **ACCESS-REQUEST**
ACCESS-ACCEPT
ACCESS-REJECT
ACCOUNTING-REQUEST
ACCOUNTING-RESPONSE
ACCESS-CHALLENGE

ATTRIBUTES

Type	Length	Value...

- Type, Length, Value (TLV) 3-tuple
- Types of Attributes
  - 1- 63 likely to be used in RFC
  - 64-191 to be used for future expansion if necessary
  - 192-223 reserved for experimental use
  - 224-240 reserved for implementation specific use within a server
  - 241-255 reserved
- Length = 2-255 including 2 octets for Type and Length fields
- Four kinds of Values
  - string - 0-253 octets
  - ipaddr - 4 octets in network byte order (also used for IPX Net Numbers)
  - integer - 32 bit value in big endian order (high byte first)

ATTRIBUTE TYPES

User-Name
User-Password
CHAP-Password
NAS-IP-Address
NAS-Port
Service-Type
Framed-Protocol
Framed-IP-Address
Framed-IP-Netmask
Framed-Routing
Filter-Id
Framed-MTU
Framed-Compression
Login-IP-Host
Login-Service
Login-Port
Reply-Message
Callback-Number
Callback-Id
Framed-Route
Framed-IPX-Network
State
Class
Vendor-Specific
Session-Timeout
Idle-Timeout
Termination-Action
Called-Station-Id
Calling-Station-Id
NAS-Identifier
Proxy-State
CHAP-Challenge
NAS-Port-Type

ACCOUNTING ATTRIBUTE TYPES

Acct-Status-Type
Acct-Delay-Time
Acct-Input-Octets
Acct-Output-Octets
Acct-Session-Id
Acct-Authentic
Acct-Session-Time
Acct-Input-Packets
Acct-Output-Packets
Acct-Terminate-Cause

INSTALLATION OF RADIUSD 1.16

- Implementation vs. Protocol
  - Data Dictionary is just a method of Implementation
- /etc/radiusd
- /etc/raddb/
- /usr/adm/radacct/

/etc/raddb

- *clients* shared secrets
- *dictionary* defines attributes and values for users file
- *logfile* errors and warning messages
- *users* user authentication/authorization information

/etc/raddb/dictionary

```
ATTRIBUTE     User-Name          1      string
ATTRIBUTE     Password           2      string
ATTRIBUTE     CHAP-Password      3      string
ATTRIBUTE     Client-Id          4      ipaddr
ATTRIBUTE     Client-Port-Id     5      integer
ATTRIBUTE     Login-Service      15     integer

VALUE         Login-Service      Telnet    0
VALUE         Login-Service      Rlogin    1
VALUE         Login-Service      TCP-Clear 2
```


/etc/raddb/users

```
# PPP user with address Assigned by NAS
#
Peg    Password = "ge55gep"
       User-Service-Type = Framed-User,
       Framed-Protocol = PPP,
       Framed-Address = 255.255.255.254,
       Framed-Compression = Van-Jacobsen-TCP-IP,
       Framed-Filter-Id = "student",
       Framed-MTU = 1500
#
# Login User to default host
#
DEFAULT  Password = "UNIX"
         User-Service-Type = Login-User,
         Login-Service = Rlogin
```


/usr/adm/radacct/*pmname*/detail

- Start of Service Record

```
Wed Jan 10 14:24:02 1996
        Acct-Session-Id = "1C000011"
        User-Name = "nancy"
        Client-Id = 149.198.1.18
        Client-Port-Id = 14
        NAS-Port-Type = ISDN
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Called-Station-Id = "5557422"
        User-Service-Type = Framed-User
        Framed-Protocol = PPP
        Framed-Address = 149.198.15.1
        Acct-Delay-Time = 0
```


- End of Service Record

```
Wed Jan 10 15:38:42 1996
        Acct-Session-Id = "1C000011"
        User-Name = "nancy"
        Client-Id = 149.198.1.18
        Client-Port-Id = 14
        NAS-Port-Type = ISDN
        Acct-Status-Type = Stop
        Acct-Session-Time = 4483
        Acct-Authentic = RADIUS
        Acct-Input-Octets = 140158
        Acct-Output-Octets = 28723318
        Called-Station-Id = "5557422"
        User-Service-Type = Framed-User
        Framed-Protocol = PPP
        Framed-Address = 149.198.15.1
        Acct-Delay-Time = 0
```


PAP and CHAP Authentication

- PAP ID and Password sent as RADIUS User-Name and User-Password

- CHAP is more complicated:
  1. NAS generates CHAP Challenge and sends to dial-in user
  2. user sends back CHAP ID and challenge response
  3. NAS sends RADIUS *access-request* packet to server with challenge as authenticator, CHAP ID as User-Name, challenge response as CHAP-Password (3)
  4. RADIUS server uses User-Name to look up password (which must be in cleartext), encrypts authenticator with that using MD5 and compares result to CHAP-Password
  5. If they match, server sends back *access-accept*, otherwise sends back *access-reject*