RADIUS _____ CHAPTER 6

Introduction

RADIUS (Remote Access Dialup User Service) is a protocol by which users (and in some cases systems) are provided access to secure networks through a centrally managed server. Authentication is provided for a variety of services (login, dialback, SLIP, PPP, etc.). When passwords are exchanged between the PortMaster and the RADIUS server they are encrypted using a shared secret as the encryption key.

Installation

To install RADIUS on a UNIX host, follow the guidelines below:

1) Run **pminstall**.

2) Select option 5, "RADIUS Installation".

3) Log on to your PortMaster(s) and define the Primary and Secondary Servers and set the encryption key (Secret). This procedure is described in Chapter 3 for X-Windows, Chapter 4 for an ASCII terminal, and in Chapter 5 for the Command Prompt Interface.

4) Set values in the clients and users file as described below.

Administration

The users file (located in /etc/raddb by default) uses "attribute/value pairs" provided in the dictionary file. The dictionary file can be modified, but it is not recommended unless you *thoroughly* understand the uses of RADIUS.

User Service Types

Under RADIUS, there are essentially five types of service users can be defined to make use of. They are:

- Login-User
- Framed-User
- Dialback-Login-User
- Dialback-Framed-User
- Outbound-User

Login-User

When defined, this field specifies the users will be allowed direct access to the host or network as defined, upon proper entry of their User Name and Password.

Framed-User

When defined, this field specifies whether the user is authorized to make either a SL/IP or PPP network connection. Optionally, the **Framed-Protocol, Framed-Address,** and **Framed-Netmask** fields must also be specified. Optionally, the **Framed-Routing** and **Framed-Compression** fields may also be defined These fields are described later in this section.

Dialback-Login-User

When defined, this field specifies the user is to be dialed back at a pre-defined telephone number following proper entry of their User Name and Password.

Dialback-Framed-User

When defined, this field specifies the user is allowed either a SL/IP or PPP connection and is to be dialed back at a pre-defined telephone number following proper entry of their User Name and Password. The Dialback telephone number and associated information is maintained in the Location Table.

Outbound-User

When defined, this user will be authenticated through RADIUS when

using the outbound modem pools. See Appendix E, Outbound Security for more information on its use.

Attribute/Value Pairs

This section contains dictionary translations for parsing RADIUS requests and generating responses. All transactions are composed of Attribute/Value Pairs. Values should be stored in the user file with dictionary value translations for ease of administration. The format for all entries except the userid is: attribute=<value>.

Login/Password Attributes

User-Name
This string attribute denotes the User (Login Name) to be authenticated.

Password
This string attribute has a value pair which can either be a quoted clear-text password maintained in the users file or a quoted value of UNIX which forces RADIUS to use /etc/passwd on the RADIUS host or (if NIS is being used) query the NIS server for password authentication.

Client-Id
This field, which must be entered in the standard dotted (".") internet notation, contains the IP address of the PortMaster which is used in the authentication of a user.

Client-Port-Id
This field identifies a PortMaster port which is used in the authentication of a user.

Framed Attributes

Framed-Protocol
This field is used to identify the user as either a SL/IP or PPP user. The default for a User Type of Network User is PPP.

Framed-Address
This field is used to specify the destination IP address or host name of the authenticated Network User. If the PortMaster is configured to use Assigned addresses the default action will be to assign an address to the Network User, otherwise the default action is to negotiate the address.

Framed-Netmask
This field is used to specify the destination netmask of the authenticated network user. The default netmask is 255.255.255.255

Framed-ipxnet
This field is used to specify the IPX network number of the authenticated Network User. This number should be specified in HEX format.

Framed-Routing
This field defines the RIP routing options, there are four possible values which can be specified here, the default is "None". The descriptions of these values follows:

None
If None is specified (or if the field is omitted), RIP (Routing Information Protocol) packets are disabled on the Dial In User's Interface.

Broadcast
If Broadcast is specified, RIP packets are allowed to be sent across the interface.

Listen
If Listen is specified, RIP packets are allowed to be received across the interface.

Broadcast-Listen
If Broadcast-Listen is specified, RIP packets are allowed in both directions across the interface.

Framed-Filter-Id
This field identifies the Packet Filter which has been set up on the PortMaster from which the user is accessing the network. If a user can

access multiple PortMasters on a network, each PortMaster must have identical filters installed. Note that when entering a name into this field that name is mapped in the format of ID.in or ID.out depending on whether an Input Filter or and Output Filter is being defined. If the Framed-Filter-Id is named, for example, FredFilter, internally the PortMaster uses a filter named FredFilter.out.

Framed-MTU
This field specifies the Maximum Transmission Unit allowed across the serial network connection. The maximum for SL/IP must be specified as 1006 while PPP can use an MTU of 1500. The default is 1500 bytes.

Framed-Compression
This field specifies whether or not to use Van-Jacobson header compression. The possible values are Van-Jacobson TCP-IP, or None. Since the default protocol is PPP, the default for compression is "**On**".

Login-Host
This field identifies the host to which a login user is connected.

Login-Service
This field has four possible settings. They are:

Telnet
Uses the "telnet" (port 23 by default) protocol to establish a connection with the host.
Rlogin
Uses the "rlogin" (port 513 by default) protocol to establish a connection with the host.

TCP-Clear
Uses the PortMaster "Netdata" (port 6000 by default) protocol to establish a connection with the host.

PortMaster

Uses the PortMaster "pmd" (port 1642) protocol to establish a connection with the host.

Login-TCP-Port
When defined, this field is used to force a user's connection to a specific TCP port number (such as 23, the default telnet port).

Dialback-No
This field must be defined in order to utilize the dialback facility of the PortMaster. It is a string which contains the telephone number to be dialed by the PortMaster after successful authentication.

Expiration
This numerical field specifies the amount of time before a password will expire. This is expressed as "December 12, 1999", for example.

Framed-Route
This field allows for the specification of a static route. There can be as many "Framed-Routes" as required for the remote connection. The format of this attribute is Framed-Route="destination gateway metric" where destination is the destination host or network, gateway is the node which provides the route to the host or network, and metric is the cost, or "hop-count" to the gateway. If the connection has been configured to use Assigned Addresses or if the address is negotiated, the notation of 0.0.0.0 will cause the gateway to be learned.

Users file examples

Following are some example of how a users file might be set up using a few of the facilities of the RADIUS server.

Login-User:

```
fred    Password = "UNIX"
        User-Service-Type = Login-User,
        Login-Host = powerhost,
        Login-Service = PortMaster
```

In the above example, the Login ID of "fred" has his password maintained either in /etc/passwd or through NIS. This user would literally login (at the login: prompt) as "fred". The default host is a host which can be looked up successfully through /etc/hosts or a name service such as NIS or DNS. RADIUS also supports C2 security.
Finally, fred's login service is defined as PortMaster. Notice that the username/password line does *not* have a comma following the entry, while the each line of options does. Further, note that the last line of the entry does *not* have a comma which indicates the end of the entry for the user. This is because the first line contains the "Authentication Items" and the remaining lines are known as the "Response Items".

Dialback-Login-User

```
bfred   Password = "somethingclever"
        User-Service-Type = Dialback-User,
        Dialback-No = "18005551212",
        Login-Host = powerhost,
        Login-Service = PortMaster
```

In the above example, notice the Password entry "somethingclever". This is literally the string the user fred enters at the password: prompt. Except for the "Dialback-User" and the "Dialback-No" entries, the user is treated no differently than the earlier example for fred.

Framed-User

```
sfred   Password = "UNIX", Client-Id=portmaster1, Client-Port-Id=1
        User-Service-Type = Framed-User,
        Framed-Protocol = SLIP,
        Framed-Address = 199.199.1.50,
        Framed-Netmask = 255.255.255.0,
        Framed-Routing = None,
        Framed-Compression = Van-Jacobsen-TCP-IP,
        Framed-MTU = 1006
```

In the above example, a SL/IP user with the login ID of sfred has his password maintained either in /etc/passwd or in NIS and has a defined protocol of SL/IP. The Client-ID and Client-Port-Id settings force fred to only be allowed to login on Port S0 of portmaster1. Further, the destination address has been set to 199.199.1.50 and the netmask has been defined as 255.255.255.0. The netmask must match that of the destination network. By setting the Framed-Routing to "None", no RIP packets will be sent or received across the interface; note that if the Framed-Routing entry were simply not included, no RIP packets would be sent or received across the interface. Also, having defined Framed-Compression, the Van Jacobsen header compression has been enabled. Finally, the Maximum Transmission Unit has been set to 1006 which is the highest allowed by the SL/IP protocol.

Dialback-Framed-User

```
sbfred  Password = "UNIX"
        User-Service-Type = Dialback-Framed-User,
        Dialback-Name = "f_location",
```

In this example, the user sfred is defined as a Dialback Framed User using SL/IP. The field "Dialback-Name" is used to specify the name of the Location Table entry to be used for dialing to the user's location.

Managing the clients file

The clients file is a file in the format of:

PortMaster_Name *Encryption_Key*

Where PortMaster_Name is the name of the PortMaster using RADIUS and Encryption_Key is the RADIUS "secret" being used by that PortMaster. This style of management allows the flexibility of each Port-Master having a separate "secret" or Encryption Key.
This is used in conjunction with the RADIUS client functions described in the sections appropriate to your environment - refer to Chapter 3 for management under X-Windows, Chapter 4 for management with an ASCII Terminal, and Chapter 5 for management from the Command Prompt Interface.