Radius Addendum

to the *Remote Annex Administrator's Guide for UNIX*

Part No. 166-024-832 Rev. A
August 1996

Bay Networks

Security Addendum to the Remote Annex Administrator's Guide for UNIX

RADIUS Addendum to the Remote Annex Administrator's Guide for UNIX

This addendum describes how to configure **erpcd** to use a Remote Authentication Dial-in User Services (RADIUS) server with the Remote Annex family of products. See the *Remote Annex Administrator's Guide for UNIX* and the *Annex Manager User Guide* for detailed information on Remote Annex products.

This addendum covers the following topics:

- Overview
- RADIUS Authentication
- RADIUS Accounting
- RADIUS Authorization
- RADIUS Configuration Management
- RADIUS Dictionary File

Overview

RADIUS is an IETF- developed protocol that defines a communication standard between a Network Access Server (NAS) and a host-based communication server. RADIUS modes are as follows:

- RADIUS Authentication includes authentication of the dial-up user to the RADIUS server, as well as authentication of the RADIUS server to the NAS. RADIUS supports authentication modes PAP and CHAP (Challenge Handshake Authentication Protocol), user name, and password validation.
- RADIUS Accounting, another IETF-developed protocol, defines a communication standard between an NAS and a host-based accounting server. It records duration of service, packet throughput, and raw throughput.

- RADIUS Authorization is supported in this release for those users that select and configure RADIUS in the acp_regime file. Once a user is configured for RADIUS authorization, the authorization information is supplied by a RADIUS server.

RADIUS and ACP Protocol Operation

RADIUS and ACP servers work together to provide the user with a standard means of communication between a Network Access Server and a host-based server.

When or If...	The...
the security profile matches "radius" as a regime,	expedited remote procedure call daemon (ERPCD) / ACP prompts the Remote Annex for the user name and password.
the user name and password are entered correctly,	ERPCD / ACP sends a RADIUS Access-Request packet to the RADIUS server (this packet contains the normal RADIUS header and the Access-Request attributes).
the Access-Accept, Access-Reject, or Access-Challenge packet fails to arrive in the specified amount of time,	ERPCD / ACP re-sends the packet.
no response is received,	ERPCD / ACP sends the Access-Request packet to the backup RADIUS server, if configured in the **erpcd.conf** file.

(continued on next page)

When or If...	The...
ERPCD / ACP receives an Access-Accept packet,	ERPCD / ACP considers the user validated.
ERPCD / ACP receives an Access-Reject or an unsupported Access-Challenge or the backup RADIUS server also fails to respond,	ERPCD / ACP considers the user invalidated

RADIUS Authentication

RADIUS authentication supports the authentication modes PAP and CHAP, as well as user name and password validation. This section covers the following topics:

- PPP and CHAP Support
- Access-Request Attributes
- Access-Accept and Access-Reject Attributes

PPP and CHAP Support

RADIUS requires PPP / CHAP enforcement to be in the RADIUS server. The RADIUS client in the ACP server needs access to three pieces of information needed for validation:

- CHAP challenge from the Remote Annex to the PPP client
- CHAP ID from the PPP client to the Remote Annex
- CHAP response from the PPP client to the Remote Annex

When the above three pieces of information are accessed:

The...	Then...
Remote Annex sends all three pieces of information to the ACP server in an ACP Authorization-Request message,	determines if the regime is "radius" and sends a request to the RADIUS server containing the CHAP information needed for validation.
RADIUS server validates the information and returns either an Access-Accept or Access-Reject message,	the ACP server responds to the Remote Annex with REQ_GRANTED or REQ_DENIED for authorization.

If the regime is not "radius," the ACP server ignores the regime and validates against the **chap_secret** entry in the **acp_userinfo** file.

Access-Request Attributes

ERPCD / ACP sends each Access-Request packet indicating how the user has connected to the Annex. This information can be used by the server as a hint or a restriction. The following section defines the available access-request attributes:

User-Name Indicates the name of the user that the RADIUS server will authenticate. An unterminated ASCII string identical to the user name that ERPCD / ACP retrieves via the user name prompt. You can specify up to 31 alphanumeric characters.

User-Password Specifies the password of the user that the RADIUS server will authenticate.

CHAP-Password Specifies the response value provided by a CHAP user in response to the password challenge.

NAS-IP-Address Indicates the IP address of the Annex authenticating the user or sending an Accounting packet.

NAS-Port-Type

Specifies the physical port type handling the user session. This value corresponds to the physical port type. Supported port types are:

- Async (0)
- ISDN Sync (2)
- ISDN Async V.120 (3)
- Virtual (5)

NAS-Port

Specifies the port number to which the user has connected.

NAS–Port number example:

`nxxx (decimal)`

n=	Description
0	Serial interface port
2	Virtual (VCLI, FTP)
3	Dial-out
4	Ethernet (outbound)

Framed-Protocol

Specifies the link level protocol type allowed to the user. Supported values are:

- PPP
- SLIP

Service-Type

Specifies the type of service the user is to receive. Supported types of service are:

- Login
- Framed
- NAS–Prompt
- Outbound
- Administrative

Access-Accept and Access-Reject Attributes

Attributes included in the RADIUS Access-Accept and Access-Reject packets are ignored by ERPCD / ACP in this version. However, ERPCD / ACP does instruct the Remote Annex to display any text sent in a Reply-Message attribute as long as the user is a CLI or port server user.

RADIUS Accounting

RADIUS Accounting defines a communication standard between a NAS and a host-based accounting server. It records duration of service, packet throughput and raw throughput. This section covers the following topics:

- RADIUS Accounting Process
- Accounting-Request Attributes

RADIUS Accounting Process

The following table describes the RADIUS accounting process:

When or If...	The...
the Remote Annex sends an ACP Audit-log to the server,	security profile for the ACP Authorization-Request must match the "radius" regime in the **acp_regime** file (the time qualifier is ignored due to time-based matching).
ERPCD / ACP receives a login or logout log request,	ERPCD / ACP sends an Accounting-Request packet to the RADIUS Accounting server.
The ERPCD / ACP server receives the RADIUS Accounting-Response,	ERPCD / ACP returns the ACP audit log verification PDU to the Remote Annex.

Accounting-Request Attributes

ERPCD / ACP sends each Accounting-Request packet with the following attributes:

Acct-Status-Type Marks whether the Accounting packet sent to the RADIUS server is the beginning or end of a session.

- Start (1) – ERPCD / ACP login events
- Stop (2) – ERPCD / ACP logout events
- Accounting–On (7) – ACP logging connection becomes active
- Accounting–Off (8) – ACP audit logging connection becomes inactive

Acct-Delay-Time Specifies how many seconds the RADIUS client has been trying to send this Accounting packet.

Acct-Input-Octets Specifies how many octets have been received during the session.

Acct-Output-Octets Specifies how many octets have been sent during the session.

Acct-Session-Id A unique numeric string identified with the session reported in the packet.

Acct-Authentic Specifies how the user is authenticated. Always set to RADIUS.

Acct-Input-Packets Specifies how many packets have been received during the session.

Acct-Output-Packets Specifies how many packets have been sent during the session.

Acct-Session-Time Specifies the elapsed session time as calculated in RADIUS.

Other Attributes All attributes that are included in the Access-Request packet are also included in the Accounting-Request packet.

RADIUS Authorization

The following section details the RADIUS authorization attributes supported for this release.

Service-Type (6)

Specifies the type of service the user will initially receive.

Usage: If specified, this attribute limits the user to the following types of service. If not specified, the user is not limited, and can proceed with the type of service already present.

- Login - The user will be connected to a host with a terminal service protocol.
- Framed - A framed protocol (SLIP, PPP, IPX/SLIP) will be started for the user.
- Outbound - The user will be granted access to an outgoing device. (e.g. Port service)
- NAS-Prompt - The user will be given CLI access to the Remote Annex.

Dependencies:

- Login and NAS-Prompt users must be using a non-protocol async connection.
- The Login user must also have a Login-Service and target protocol dependent host specified, or the user will be connected to a CLI prompt.
- The Framed user can connect to the Annex with the protocol authorized or, once authorized, can use an async ASCII connection with the use of CLI commands.

Framed-Protocol (7)

Specifies the protocol type allowed to the user.

Usage: Values supported:

- PPP - The user accessing the NAS can use PPP or MP framing. If any other type of framing is in use, the call is rejected. Outgoing calls would use PPP framing.
- SLIP

Dependencies: This attribute is only used in conjunction with a Service-Type of Framed.

Framed-IP-Address (8)

Specifies the IP address of the remote user.

Usage: If specified, this attribute specifies the IP network address of the remote accessing system.

255.255.255.255 – Specifies that the Annex should allow the user to negotiate the address.

255.255.255.254 – Specifies that the Annex should try to use DHCP (if configured) to choose an address for the user.

Dependencies: This attribute is only meaningful when used in conjunction with framed IP-based connections.

Framed-IP-Netmask (9)

Specifies the IP netmask to be configured for the user when the user is a Router to the network.

Usage: If specified, this attribute indicates the IP netmask of the remote subnet.

Dependencies: This attribute can only be used with a Framed-IP-Address attribute defined.

Login-IP-Host (14)

Specifies the IP address of the terminal service host to which the user is automatically connected.

Usage: This attribute is used with Login-Service (Telnet or Rlogin).

- If set to all ones (FFs), this indicates that the user is prompted to select an address.

Dependencies: This attribute only applies to Login connections.

- If Service-Type=Login, and Login-Service=Telnet or Rlogin, and a Login-IP-Host is specified, a terminal service connection will be started for the user immediately after login. If not specified, the user is given CLI access.

Login-Service (15)

Specifies which terminal service protocol will be used for a Login user.

Usage: This attribute is used with Service-Type=Login. Terminal service to the specified host is started immediately after login.

Values supported:

- Telnet
- Rlogin

Dependencies: This attribute only applies to Login connections.

- For Telnet and Rlogin values, the Login-IP-Host attribute must be specified.

Login-TCP-Port (16)

Specifies the TCP port number to use for the terminal services connection.

Usage: This attribute is optional for Telnet Login connections. The value specifies a TCP port number on the target host. The default is the standard 34.

Dependencies: This attribute only applies to Telnet-based Login connections.

Reply-Message (18)

Contains a text string which is either a prompt or an informational message.

Usage:

- Used in Access-Challenge / Response exchanges as the text for a follow-up user prompt.
- Can be supplied by management input to the user's database record. If received in an Access-Accept message, it should be displayed to a non-protocol user after login.
- Can be used in Access-Reject messages as an error message text.
- Can be used in Accounting-Request messages to log additional information.

Dependencies: On some systems, this text will override normal error or termination messages.

Framed-Route (22)

Specifies a static IP route to be added to the Remote Annex's routing table. For dial-in framed users, this route only exists for the duration of the session.

Usage: The route string should use the following format:

```
dest/mask gateway metric[s]
```

dest	destination IP address in decimal dotted quad format.
mask	a valid decimal netmask.
metric	one or more decimal metrics separated by spaces.

- If the gateway address is specified as 0.0.0.0, the IP address of the user should be used as the gateway address.
- Some systems may provide additional metrics, which will be ignored by the Annex.

Dependencies: This attribute applies only to Framed connections.

Class (25)

Contains information entered in the Authorization database for accounting purposes.

Usage: The contents of this attribute is held in the session and passed on to the RADIUS Accounting Request messages for logging. It can be used to indicate user information as desired.

Session Timeout (27)

Specifies the number of seconds that the service is to be provided to the user before termination of the session.

Usage: This optional attribute is used to restrict user's usage.

Dependencies: This attribute applies only for Remote Annex services that support it.

Port-Limit (62)

Specifies the maximum number of concurrent link sessions that a Multilink PPP user can use.

Usage: If specified, the attribute value is the maximum link count.

Dependencies: This attribute is used only for PPP Framed connections.

Configuration Management

Configuring the RADIUS server and RADIUS Accounting server involves setting parameters to define the server's operating and administrative attributes. This section covers the following topics:

- The **erpcd.conf** file
  - RADIUS Server and Accounting Server Format
  - Response Timeout and Number of Retries Format
  - Secret Format
  - Fail-over Algorithm Process

The erpcd.conf File

The **erpcd.conf** file is expanded to specify the default RADIUS server and RADIUS Accounting servers, as well as:

- The secret shared with the server
- The response timeout
- The number of retries
- A backup server for each RADIUS server and RADIUS Accounting server

Edit erpcd.conf **Locally**

Because the **erpcd.conf** file contains the clear text RADIUS secret, the administrator must ensure that the file is located on a local disk and is edited from a local console or over a secure network link.

Server Information

The format of the **erpcd.conf** file is based on a single primary server. One RADIUS Authentication server and one RADIUS Accounting server may be specified for a particular ERPCD / ACP server.

Changing the erpcd.conf **File**

ERPCD reads the **erpcd.conf** file only at start-up. For the ERPCD to realize any changes to this file, it must be killed and re-started.

Default Values

If there is no configuration record for a RADIUS server, the following default values are used:

Attribute	Default Value
Secret	0x0
Timeout	4 seconds
Retries	10
Backup server	None

RADIUS Server and Accounting Server Format

erpcd.conf **File Format**

The **erpcd.conf** file format is:

```
radius default RADIUS=<RADIUS server>;
Accounting=<Accounting server>
```

- <*RADIUS server*> is the host name or Internet address of the RADIUS Authentication server.
- <*Accounting server*> is the host name or Internet address of the RADIUS Accounting server.

If no Accounting server is specified, it defaults to the RADIUS server. If no RADIUS server is specified, the RADIUS server defaults to the ACP server.

This entry must be contained on one line.

Response Timeout and Number of Retries Format

The format of the response timeout and number of retries specified in the **erpcd.conf** file is:

Syntax

```
radius server host=<val>;secret=<val>;timeout=<val>;
retries=<val>;backup=<val>
```

Fail-over occurs only if host is the original primary server.

This entry must be contained on one line.

host	The host name or Internet address of the RADIUS server or RADIUS Accounting server.
secret	The secret shared with the RADIUS server or RADIUS Accounting server.
timeout	The number of seconds to wait for a response before sending a retry.
retries	The number of times to retry before fail-over to the backup server.
backup	The host name or Internet address of the backup RADIUS server or RADIUS Accounting server.

Secret Format

The format for *secret* is an ASCII string or a hexadecimal string. The hexadecimal string format always starts with **0x** followed by a string of bytes, with each two hexadecimal digits indicating one byte.

Each entry in the **erpcd.conf** file must be contained on one line. Any amount of white space can exist between keywords, keyword / value pairs, and semi-colon delimeters. No white space can exist between the keyword and "=" or the value and "=".

erpcd.conf File Example

```
radius default RADIUS=132.245.66.11;Accounting=132.245.33.60
radius server host=132.245.66.11;secret=spikesecret;timeout=5;retries=5;backup=132.245.33.17
radius server host=132.245.33.17;secret=mysecretmysecret;timeout=6;retries=10
radius server host=132.245.33.60;secret=nottimesec;temeout=4;retries=10;backup=132.245.66.18
radius server host=132.245.66.18;secret=hpposecret;timeout=8;retries=12
```

Fail-over Algorithm Process

The following table describes the fail-over algorithm process for authentication and accounting.

Table 1. Fail–Over Algorithm Process

When or If...	The...
a user is to be authenticated,	RADIUS server first polled is specified in the "radius default" line of the **erpcd.conf** file (this server must have a "radius server" line).
There is no specification,	ACP server is treated as the RADIUS server.
an Access-Request packet is sent to the RADIUS server,	ERPCD / ACP waits the specified timeout value (4 seconds by default) for the response packet.
the time expires,	ERPCD / ACP retries the request.
the maximum number of retries (10 by default) is reached without a response from the server,	attempt to authenticate against the primary server fails and ERPCD / ACP attempts to authenticate against the backup server.
no response is received from the backup server,	user is rejected.
an accounting fail-over occurs, the server remains the same until,	restart of **erpcd.conf** or failure of the backup server.
both the accounting primary server and backup fail,	the **acp_logfile** records RADIUS accounting.

RADIUS Dictionary File

Included on the distribution kit is a reference RADIUS dictionary file which will be placed in the security files area. The **erpcd** server does not use this file, it is provided as documentation and a convenience. This file defines keywords, types, and values for RADIUS attributes and their corresponding code points. The file is in a format that is used as input by some RADIUS servers to parse messages, and write text output files. Customers may have existing dictionaries with differences in the keyword names, and may want to evaluate the impact to their databases and output reports.

The file that we provide includes the latest IETF definitions of the RADIUS protocol at the time of release. It includes all attributes and values that are needed to support our Remote Annex and **erpcd** implementation. It is not necessary that our definitions be used directly, but other dictionaries may have to be extended to cover our usage.

This file may be used as a reference to add or change existing RADIUS dictionaries as need be. Since it is in the format of some of the popular RADIUS servers, in some cases it may be used as a direct replacement. However, the network manager should review the dependencies and make a decisions on how to apply the differences.

The following is a partial example of the dictionary contents:

```
ATTRIBUTE       User-Name          1       string
ATTRIBUTE        Password          2       string
ATTRIBUTE       CHAP- Password     3       string
ATTRIBUTE       NAS-IP-Address     4       ipaddr
ATTRIBUTE       NAS-Port           5       integer
ATTRIBUTE       Service-Type       6       integer
ATTRIBUTE       Framed-Protocol    7       integer
ATTRIBUTE       Framed-IP-Address  8       ipaddr
<...>

#           User Service Types
VALUE      Service-Type       Login-User          1
VALUE      Service-Type       Framed-User         2
VALUE      Service-Type       Callback-Login-User 3
VALUE      Service-Type       Callback-Framed-    4
                              User
VALUE      Service-Type       Outbound-User       5
VALUE      Service-Type       Administrative-User 6
VALUE      Service-Type       NAS-Prompt          7
VALUE      Service-Type       Authenticate-Only   8
VALUE      Service-Type       Callback-NAS-Prompt 9
<...>
```

```
#         Framed Protocols
VALUE     Framed-Protocol   PPP               1
VALUE     Framed-Protocol   SLIP              2
VALUE     Framed-Protocol   ARAP              3
VALUE     Framed-Protocol   Gandalf-SL/MLP    4
VALUE     Framed-Protocol   IPX/SLIP          5
```