# Release 5.1 Supplement for Remote Annexes

Marketing Release 5.1

Part No. 119346-A Rev. A
October 1997

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

## Copyright © 1997 Bay Networks, Inc.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

## Trademarks

Bay Networks is a registered trademark and Remote Annex, Quick2Config, RouterMan, SN, SPEX, Switch Node, System 5000, Bay Networks Press, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

## Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

## Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

## Bay Networks, Inc. Software License Agreement

**NOTICE:** Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price

**1. License Grant.** Bay Networks, Inc. (“Bay Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

**2. Restrictions on use; reservation of rights.** The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

**3. Limited warranty.** Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence.

THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

**4. Limitation of liability.** IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

**5. Government Licensees.** This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

**6. Use of Software in the European Community.** This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

**7. Term and termination.** This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

**8. Export and Re-export.** Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

**9. General.** If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

## Contents

## About This Guide

## Release 5.1 Supplement for Remote Annexes

# Tables

# About This Guide

This guide provides Release 5.1 supplement information for Bay Networks® Remote Annexes. The information in this guide discusses new or revised features supported in Release 5.1.

| If you want to | Go to |
|---|---|
| Configure RADIUS security. | page 1 |
| Learn about Release 5.1 features for the Model 5393 and Model 6300 Remote Annex. | page 36 |

## Before You Begin

When administering a Remote Annex, be sure to refer to this supplement for features supported in Release 5.1.

# Conventions

This manual uses the following printing conventions:

| Convention: | Represents: |
|---|---|
| `special type` | In examples, `special type` indicates system output. |
| **`special type`** | Bold **`special type`** indicates user input. |
| Return | In command examples, this notation indicates that pressing Return enters the default value. |
| **bold** | Bold indicates commands, pathnames, or filenames that must be entered as displayed. |
| *italics* | In the context of commands and command syntax, lowercase italics indicate variables for which the user supplies a value. |
| [ ] | In command dialog, square brackets indicate default values. Pressing Return selects this value. Square brackets appearing in command syntax indicate optional arguments. |
| { } | In command syntax, braces indicate that one, and only one, of the enclosed value must be entered. |
| \| | In command syntax, this character separates the different options available for a parameter. |
| ✎ | Notes provide important information. |
| ❗ | Warnings inform you about conditions that can have adverse effects on processing. |
| ⚡ | Cautions notify you about dangerous conditions. |

# Acronyms

| | |
|---|---|
| ACP | Access Control Protocol |
| AFD | Automatic Firmware Download |
| ATCP | Apple Talk Control Protocol |
| bfs | block file system |
| CHAP | Challenge Handshake Authentication Protocol |
| CLI | Command Line Interface |
| erpcd | expedited remote procedure call daemon |
| HDLC | High Level Data Link Control |
| IP | Internet Protocol |
| IPCP | Internet Protocol Control Protocol |
| IPXCP | IPX Control Protocol |
| ISDN | Integrated Services Digital Network |
| L2TP | Layer 2 Tunneling Protocol |
| MMP | Multi-system Multilink PPP |
| NAS | Network Access Server |
| PAP | Password Authentication Protocol |
| SPB | Session Parameter Block |
| PPP | Point-to-Point Protocol |
| PRI | Primary Rate Interface |
| SLIP | Serial Line Internet Protocol |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| VAS | Vendor-specific Attributes |
| WAN | Wide Area Network |

## Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers:

- Phone--U.S./Canada: 888-422-9773
- Phone--International: 510-490-4752
- FAX--U.S./Canada and International: 510-498-2609

The Bay Networks Press catalog is available on the World Wide Web at *support.baynetworks.com/Library/GenMisc*. Bay Networks publications are available on the World Wide Web at *support.baynetworks.com/Library/tpubs*.

## Bay Networks Customer Service

You can purchase a support contract from your Bay Networks distributor or authorized reseller, or directly from Bay Networks Services. For information about, or to purchase a Bay Networks service contract, either call your local Bay Networks field sales office or one of the following numbers:

| Region | Telephone number | Fax number |
|---|---|---|
| United States and Canada | 800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract<br>508-916-8880 (direct) | 978-916-3514 |
| Europe | 33-4-92-96-69-66 | 33-4-92-96-69-96 |
| Asia/Pacific | 61-2-9927-8888 | 61-2-9927-8899 |
| Latin America | 561-988-7661 | 561-988-7550 |

Information about customer service is also available on the World Wide Web at *support.baynetworks.com*.

# How to Get Help

If you purchased a service contract for your Bay Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Bay Networks service program, call one of the following Bay Networks Technical Solutions Centers:

| Technical Solutions Center | Telephone number | Fax number |
|---|---|---|
| Billerica, MA | 800-2LANWAN | 978-916-3514 |
| Santa Clara, CA | 800-2LANWAN | 408-495-1188 |
| Valbonne, France | 33-4-92-96-69-68 | 33-4-92-96-69-98 |
| Sydney, Australia | 61-2-9927-8800 | 61-2-9927-8811 |
| Tokyo, Japan | 81-3-5402-0180 | 81-3-5402-0173 |

# Release 5.1 Supplement for Remote Annexes

This supplement describes Remote Annex features supported in Release 5.1 as follows:

- Embedded RADIUS -- Describes how to configure RADIUS security on Remote Annexes.
- 5393 and 6300 Functions -- Release 5.1 functions that are supported only on the Model 5393 and Model 6300 Remote Annexes.

## Configuring RADIUS Security

RADIUS is an IETF-developed protocol that defines a communication standard between a Network Access Server (NAS), a Remote Annex in this case, and a host-based communication server.

RADIUS operates in three modes:

- 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 the authentication modes PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), and user name/password validation. Authorization is sent back by the server.
- 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.
- RADIUS Authorization; a user’s authorization information is supplied by the RADIUS server.

The Remote Annex software includes a native RADIUS client; a RADIUS server is available from Bay Networks separately, or you can use any other RADIUS server. You can use the RADIUS client independently, with the Remote Annex's security regime set to RADIUS, or you can use erpcd as a proxy RADIUS client running under the ACP security regime.

Note that the capabilities provided by the proxy RADIUS client running under the ACP security regime are a subset of those provided by the native RADIUS client; any transactions that take place between the proxy RADIUS client and ACP also take place when the security regime is RADIUS.

## Using erpcd As a Proxy RADIUS Client

To configure security using erpcd as a proxy RADIUS client:

1. **Set** enable_security **to** Y **and set** auth_protocol **to** acp**.**
2. **Configure the** erpcd.conf **file on the pref_secure1_host. This causes the Remote Annex to send ACP authentication and authorization requests to erpcd. erpcd converts these requests to RADIUS format, and sends the reformatted reports to the RADIUS server configured in the** erpcd.conf **file.**
3. **Reset the Remote Annex in order for these changes to take effect.**

## Using the Remote Annex's Native RADIUS Client

To configure security using the Remote Annex native RADIUS client:

1. **Set** enable_security **to** Y **and set** auth_protocol **to** radius**.**
2. **Reset the Remote Annex in order for this change to take effect.**

## RADIUS Parameters

The following **admin/na** parameters support the Remote Annex embedded RADIUS capability.

Refer to the *Remote Access Concentrator Software Reference* for a complete description of each parameter.

- **address_origin -** This parameter specifies the server from which the dial-in user receives a network address.
- **auth_protocol -** This parameter indicates which authentication regime will be used, **acp** (the default) or **radius**. This parameter must be set to **acp** for erpcd to be used as a proxy RADIUS client.
- **enable_radius_acct -** This parameter, when set to **Y**, enables RADIUS accounting when security is enabled and the security regime is RADIUS. The RADIUS accounting server runs on the same host as the RADIUS authentication server.
- **enable_security -** This parameter must be set to **Y** for any security regime to work. The parameter's default value is **N**.
- **pref_secure1_host -** This parameter must be set to the IP address of the primary RADIUS and RADIUS accounting server.
- **pref_secure2_host -** This parameter must be set to the IP address of the secondary RADIUS and RADIUS accounting server.
- **radius_acct_level -** This parameter indicates the level of RADIUS accounting used (**basic** or **advanced**).
- **radius_acct_port -** This parameter specifies the number of the UDP port on which the RADIUS accounting server listens. The default value is **1813**. (Older RADIUS servers use port **1646**.)
- **radius_auth_port -** This parameter indicates the number of the UDP port on which the RADIUS server listens. The default value is **1812**. (Older RADIUS servers use port **1645**.)

- **radius_port_encoding -** This parameter controls the format in which RADIUS accounting information is reported to the RADIUS server. The possible values for this parameter are **device** (the default) and **channel**.
- **radius_retries -** This parameter indicates the number of times the RADIUS client retries sending access-request/accounting-request packets before trying the secondary host. The default value is **10**.
- **radius_secret -** This string defines the RADIUS shared secret for the Remote Annex. By default, the shared secret is unset.

The value of **radius_secret** should not be exposed on the network in clear text form.

- **radius_timeout -** This parameter specifies the retransmission timer for RADIUS access-request/accounting-request packets. The default value is **4**.

## RADIUS Attributes

RADIUS tracks various pieces of data using attributes. The Remote Annex supports a number of standard RADIUS attributes, plus a number of Bay Networks vendor-specific attributes (VSAs) that are equivalent to entries in various files used by the ACP security regime.

## Supported RADIUS Standard Attributes

The standard RADIUS attributes are:

- **User-Name (1)**
- **User-Password (2)**
- **CHAP-Password (3)**
- **NAS-IP-Address (4)**
- **NAS-Port (5)**
- **Service-Type (6)**
- **Framed-Protocol (7)**
- **Framed-IP-Address (8)**
- **Framed-IP-Netmask (9)**
- **Framed-Routing (10)**
- **Filter-Id (11)**
- **Framed-MTU (12)**
- **Framed-Compression (13)**
- **Login-IP-Host (14)**
- **Login-Service (15)**
- **Login-TCP-Port (16)**
- **Unassigned (17)**
- **Reply-Message (18)**
- **Callback-Number (19)**
- **Callback-Id (20)**
- **Unassigned (21)**
- **Framed-Route (22)**
- **Framed-IPX-Network (23)**
- **State (24)**
- **Class (25)**
- **Vendor-Specific (26)**
- **Session-Timeout (27)**

- **Idle-Timeout (28)**
- **Termination-Action (29)**
- **Called-Station-Id (30)**
- **Calling-Station-Id (31)**
- **NAS-Identifier (32)**
- **Proxy-State (33)**
- **Login-LAT-Service (34)**
- **Login-LAT-Node (35)**
- **Login-LAT-Group (36)**
- **Framed-AppleTalk-Link (37)**
- **Framed-Apple-Talk-Network (38)**
- **Framed-AppleTalk-Zone (39)**
- **CHAP-Challenge (60)**
- **NAS-Port-Type (61)**
- **Port-Limit (62)**
- **Login-LAT-Port (63)**

## Supported RADIUS Accounting Attributes

The RADIUS accounting attributes are:

- **Acct-Status-Type (40)**
- **Acct-Delay-Time (41)**
- **Acct-Input-Octets (42)**
- **Acct-Output-Octets (43)**
- **Acct-Session-Id (44)**
- **Acct-Authentic (45)**
- **Acct-Session-Time (46)**
- **Acct-Input-Packets (47)**
- **Acct-Output-Packets (48)**
- **Acct-Terminate-Cause (49)**
- **Acct-Multi-Session-Id (50)**
- **Acct-Link-Count (51)**

### Bay Networks Vendor-Specific Attributes (VSAs)

These attributes enable RADIUS to emulate the behavior of the ACP security regime:

- **Annex-Filter (VSA Bay Networks 28)**
- **Annex-CLI-Command (VSA Bay Networks 29)**
- **Annex-CLI-Filter (VSA Bay Networks 30)**
- **Annex-Host-Restrict (VSA Bay Networks 31)**
- **Annex-Host-Allow (VSA Bay Networks 32)**
- **Annex-Product-Name (VSA Bay Networks 33)**
- **Annex-SW-Version (VSA Bay Networks 34)**
- **Annex-Local-IP-Address (VSA Bay Networks 35)**
- **Annex-Tunnel-Type (VSA Bay Networks 36)**
- **Annex-Tunnel-Medium-Type (VSA Bay Networks 37)**
- **Annex-Tunnel-Client-Endpoint (VSA Bay Networks 38)**
- **Annex-Tunnel-Server-Endpoint (VSA Bay Networks 39)**
- **Annex-Tunnel-Id (VSA Bay Networks 40)**
- **Annex-Tunnel-Connection-Id (VSA Bay Networks 41)**
- **Annex-Callback-Port-List (VSA Bay Networks 42)**

## The RADIUS Dictionary File

A reference RADIUS dictionary file is included in the distribution kit and is placed in the security files area. The dictionary 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. You may have existing dictionaries with differences in the keyword names, and you may want to evaluate the impact to your databases and output reports.

The file that Bay Networks provides 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 the Bay Networks Remote Annex implementation. You do not need to use our definitions directly, but other dictionaries may have to be extended to cover our usage.

Use this file as a reference when adding or changing existing RADIUS dictionaries as needed. Because this file is in the format of some of the popular RADIUS servers, in some cases it can be used as a direct replacement. However, you should review the dependencies and make a decision on how to apply the differences.

A partial listing of the dictionary contents is shown below:

```
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
<...>
```

*(continued on next page)*

```
#          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-User 4
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
```

## Configuring Remote Annex Functions Using RADIUS

You can configure Remote Annex functions by setting the values of RADIUS attributes on the RADIUS server. This section details what RADIUS attributes must be set to enable various Remote Annex functions.

In the descriptions that follow, note that numbers for packet types appear in braces **{1}**, numbers for attributes appear in parentheses **(1)**, and numbers for enumerations appear in brackets **[1]**.

### End User and Session Identification

The Remote Annex provides identification information to the RADIUS server via attributes included in Access-Request packets. Access-Request packets includes the following RADIUS attributes:

- **User-Name (1)**
- **User-Password (2)**
- **CHAP-Password (3)**
- **NAS-IP-Address (4)**
- **NAS-Port-Type (61)**
- **NAS-Port (5)**
- **Service-Type (6)**
- **Framed-Protocol (7)**
- **Called-Station-Id (30)**
- **Calling-Station-Id (31)**
- **Annex-Product-Name (VSA Bay Networks 33)**
- **Annex-SW-Version (VSA Bay Networks 34)**

## Automatic Connection

You can configure RADIUS to connect a user to a specific service automatically when the user calls in. The Remote Annex port must be in CLI mode (through the port parameter **mode** set to **cli** or **auto_detect**). The RADIUS attributes **Service-Type (6)**, **Framed-Protocol (7)**, and **Login-Service (15)** determine the service to which the user is connected.

Table 1 shows the services to which a user can be connected automatically based on a given value of **Service-Type (6)** and **Framed-Protocol (7)** or **Login-Service (15)**.

Table 1. Remote Annex Automatic Services

| Service-Type (6) | Framed-Protocol (7) | Login-Service (15) | Automatic Service |
|---|---|---|---|
| **Login [1]/Callback [3]** | n/a | **Telnet [0]** | telnet |
| **Login [1]/Callback [3]** | n/a | **Rlogin [1]** | rlogin |
| **Login [1]/Callback [3]** | n/a | **LAT [4]** | connect |
| **Login [1]/Callback [3]** | n/a | any except telnet, rlogin, or LAT | CLI |
| **Framed [2]/Callback [4]** | **PPP [1]** | n/a | ppp |
| **Framed [2]/Callback [4]** | **SLIP [2]** | n/a | slip |
| **Framed [2]/Callback [4]** | **ARAP [3]** | n/a | arap |
| **Administrative [6]** | n/a | n/a | CLI super-user |
| **NAS Prompt [7]/Callback [9]** | n/a | n/a | CLI |

## Telnet/rlogin

The **Login-IP-Host (14)** attribute specifies the Internet address to be connected to via telnet or rlogin. If **Login-IP-Host (14)** is set to **0xff**, the user is prompted for a host. If **Login-IP-Host (14)** is set to **0**, the user is connected to the address stored in the Remote Annex port parameter **dedicated_arguments**. If the latter method is used, the **Login-TCP-Port (16)** attribute is ignored.

The **Login-TCP-Port (16)** attribute specifies the destination TCP port for the telnet or rlogin session. The default port for telnet is 23, and the default port for rlogin is 513.

## LAT/connect

The **Login-LAT-Node (35)** attribute specifies the LAT node to connect to via the CLI **connect** command. Alternatively, you can specify the **Login-LAT-Service (34)** attribute to restrict the user to a particular service pool. Use the **Login-LAT-Port (63)** attribute to specify the LAT port to connect to on the remote node or service. The **Login-LAT-Group (36)** attribute is a bit mask of the LAT groups the user can access.

## Service Hint and Restriction

If the Remote Annex port is not in CLI mode (whether the Remote Annex port auto-detected a framing protocol/slave or the port was configured for framing/slave), then the user is restricted to the profile returned by RADIUS. If the RADIUS server returns a specific **Service-Type (6)** or **Framed-Protocol (7)**, but the port is not running that service or protocol, the user is rejected and the reason is logged by RADIUS Accounting.

Table 2 shows the required port modes or services that correspond to particular combinations of values for **Service-Type (6)** and **Framed-Protocol (7)**.

Table 2. Remote Annex Port Mode/Service Restrictions

| Service-Type (6) | Framed-Protocol (7) | Required Port Mode/ Service |
|---|---|---|
| **Login [1]/Callback [3]** | any | cli |
| **Framed [2]/Callback [4]** | **PPP [1]** | ppp |
| **Framed [2]/Callback [4]** | **SLIP [2]** | slip |
| **Framed [2]/Callback [4]** | **ARAP [3]** | arap |
| **Framed [2]/Callback [4]** | unspecified | ppp, slip, or arap |
| **Outbound [5]** | any | slave |
| **Administrative [6]** | any | cli |
| **NAS-Prompt [7]/Callback [9]** | any | cli |
| unspecified | any | unrestricted |

Note that if **Service-Type (6)** = **Callback-Framed[4]**, the user is granted access but will not be called back.

## Dialback Services

For the Callback service types (**Service-Type (6) = Callback-Login [3]**, **Callback-NAS-Prompt [9]**), the Remote Annex will dial back the user with the phone number specified in the **Callback-Number (19)** attribute. If this attribute is not returned by the RADIUS server, the user is prompted for the number. Specifying the callback number in the RADIUS server is more secure than having the user provide it at the prompt.

The Remote Annex dials back the user on the same channel on which he or she dialed in. Dialback calls are reauthenticated (and reauthorized) as if they were new calls.

### Session Timeout

You can restrict the user to a specified dial-in length using the **Session-Timeout (27)** attribute. The value of **Session-Timeout (27)** is equal to the number of seconds the user is allowed to be dialed in before the Remote Annex unilaterally terminates the user's session. This feature is identical to the *max_logon* feature in ACP.

### Idle Timeout

You can use the **Idle-Timeout (28)** attribute to time out the user's session once the corresponding port stops receiving or transmitting data. The value of the **Idle-Timeout (28)** attribute is equal to the number of seconds the session can be idle before the Remote Annex unilaterally terminates the session. This feature is identical to that provided by the Remote Annex port parameter *inactivity_timer.*

## CLI Scripting

You can configure the user through RADIUS to execute a CLI script upon gaining access. This feature uses the **Annex-CLI-Command (VSA Bay Networks 29)** attribute to specify a list of CLI commands to run, with each command in a separate attribute. The commands are executed in the order in which they are received. Note that protocol commands (PPP, SLIP, ARAP) end the script, even if later commands are specified. Note also that the **...** command also ends the script, and is interpreted to mean that the user remains at the NAS prompt. This feature is identical to the **clicmd** entry in the **acp_userinfo** file used with the ACP security regime.

## CLI Command Filtering

You can make certain CLI commands unavailable to the user. This feature uses the **Annex-CLI-Filter (VSA Bay Networks 30)** attribute to specify a list of CLI commands that the user cannot access. You must specify each filtered command in a separate attribute. Entering filtered commands generates the error message "CLI: Command not found." This feature is identical to the **climask** entry in the **acp_userinfo** file used with the ACP security regime.

## CLI IP Host Filtering

You can prevent the user from gaining access, via rlogin or telnet, to a specific host or host-transport port combination. You can do this with a list of **Annex-Host-Restrict (VSA Bay Networks 31)** and **Annex-Host-Allow (VSA Bay Networks 32)** attributes. The values of each of these attributes is a composite string value. The first four bytes contain, in network order, the IP address that the user should be specifically restricted from using or allowed to use. Trailing bytes that are zero are interpreted to match all values of that byte. Thus, 132.245.0.0 means everything on the 132.245.0.0 subnet, while 0.0.0.0 means every host on the entire WAN. The remainder of the string is a printable comma-delimited list or dash-delimited range of TCP or UDP ports that the user is restricted from using or allowed to use. For example, "23,101" would restrict/allow usage of ports 23 and 101, while "17-105" would restrict/allow usage of ports 17 to 105. This feature is identical to the acp_restrict file used with the ACP security regime.

To determine if a user can gain access to a host-port, each attribute is processed in the order in which it was received. Processing stops when a host-port match is found. The user is restricted access if the attribute that matched was an **Annex-Host-Restrict (VSA Bay Networks 31)** attribute. Otherwise, the user is allowed access.

## Raw Outbound Service

The Remote Annex is capable of allowing raw outbound access to a Remote Annex port via telnet. In order to use this feature, the user must either have no **Service-Type (6)** specified or have **Service-Type (6)** = **Outbound**. This is analogous to the slave port mode.

## Framed Protocol Service

The Remote Annex is capable of providing a dial-in user with framed protocol service (PPP, SLIP, or ARAP). In order to use this feature, the user must either have no **Service-Type (6)** specified or have **Service-Type (6) = Framed [2]**.

## Disabling Routing

The framed protocol user can disable routing packets across the link with the **Framed-Routing (10)** attribute. The default behavior is to send and listen for routing packets across a link to a different subnet, but not a link to the same subnet. Note that because this attribute does not specify a network layer protocol or framing protocol, the Remote Annex assumes that the attribute applies to all framing protocols (PPP, SLIP) but only IP.

## IP Network Mask

When IP is running over the link, you can configure the IP network mask for the dial-in side with the **Framed-IP-Netmask (9)** attribute. In this way, the Remote Annex can know when a packet should be forwarded across the dial-up link. The default is for the Remote Annex to assume that the network mask of the remote link is identical to the Remote Annex network mask.

## IP Static Route Configuration

When IP is running over the link, you can configure static routes for that link with the **Framed-Route (22)** attribute. Note that the Remote Annex will accept the nonstandard format for this attribute used by the Nautica RADIUS server as well as the standard format.

## Filtering Services

The Remote Annex supports filtering of IP, TCP, and UDP packets.

The **Annex-IP-Filter (VSA Bay Networks 28)** attribute allows the RADIUS server to specify a packet filter in the Remote Annex packet filter format, because RADIUS does not define a specific filter format. You can then configure the RADIUS server to upload specific packet filters based on the user's profile.

The Remote Annex also supports the **Filter-Id (11)** attribute in conjunction with the **Annex-Filter (VSA Bay Networks 28)** attribute. Upon receiving a **Filter-Id (11)** attribute, the Remote Annex initiates another Access-Request. The Remote Annex then waits for an **Access-Accept {2}** with the list of the actual filters supplied in **Annex-Filter (VSA Bay Networks 28)** attributes. This method requires a corresponding "pseudo-user" in the RADIUS server. **Nested Filter-Id (11)** attributes are not permitted.

The algorithm for applying filters is: the **Access-Accept {2}** packet is parsed. If an **Annex-Filter (VSA Bay Networks 28)** attribute is present, the filter is applied to the user's session. If a **Filter-Id (11)** attribute is present, then the Remote Annex makes a "pseudo-user" request as described earlier. The response to the "pseudo-user" request MUST contain only **Annex-Filter (VSA Bay Networks 28)** attributes; other attributes are ignored by the Remote Annex. Note that the order of processing the filter attributes is not important, because the order of the Remote Annex filters is not important.

## Maximum Transmission Unit

You can set the size of the maximum transmission unit (MTU) from the Remote Annex to the remote peer with the **Framed-MTU (12)** attribute, which is supported for SLIP and PPP, but not for ARAP. The value of this attribute is overridden by PPP, however, if the Remote Annex receives a *ppp_mru* value from the remote peer. Note that **Framed-MTU (12)** must be at least 576 bytes for IPX traffic and 599 bytes for AppleTalk traffic.

## Network Layer Compression Protocols

Network layer compression protocols can be configured using the **Framed-Compression (13)** attribute. Only Van-Jacobson TCP/IP header compression is supported by the Remote Annex.

## PAP

PAP works as described in RFC 2058.

## CHAP

CHAP works as described in RFC 2058. Note that the Remote Annex sends the CHAP challenge in *both* the **CHAP-Challenge (60)** attribute and the authenticator.

## MP

You can configure the maximum number of MP links allowed for the user with the **Port-Limit (62)** attribute. If not specified, the default number of links allowed is one. This attribute is recognized only for the first link of an MP bundle. For subsequent links, this attribute is ignored.

## L2TP

L2TP tunnels a user’s PPP session to another node where it is treated as if it were a local PPP session. L2TP is used to implement both DVS and MMP.

L2TP uses CHAP for its peer authentication. Operation of this is the same as for regular PPP CHAP but with one exception: the CHAP Identifier is set to be the low order byte of the CHAP challenge. Thus RADIUS can be used to authenticate L2TP tunnels using its existing CHAP mechanism. The L2TP Access-Request contains the following attributes:

- **User-Name (1)**
- **CHAP-Password (3)**
- **NAS-IP-Address (4)**
- **NAS-Port (5)** = VPN[5000] + index
- **Service-Type (6)**
- **Acct-Delay-Time (41)**
- **CHAP-Challenge (60)**
- **Annex-Product-Name (VSA Bay Networks 33)**
- **Annex-SW-Version (VSA Bay Networks 34)**
- **Annex-Tunnel-Type (VSA Bay Networks 36)**
- **Annex-Tunnel-Medium-Type (VSA Bay Networks 37)**
- **Annex-Tunnel-Client-Endpoint (VSA Bay Networks 38)**
- **Annex-Tunnel-Server-Endpoint (VSA Bay Networks 39)**
- **Annex-Tunnel-Id (VSA Bay Networks 40)**

## IPCP

You can configure the user’s IP address (the remote peer’s address) using the **Framed-IP-Address (8)** attribute if the *address_origin* port parameter is set to *acp* or *auth_server*. If an address is returned by the RADIUS server, then the Remote Annex *insists* on using that address, or it does not allow IPCP to come up. If, however, 255.255.255.255 is specified, then the Remote Annex allows the peer to set the address. If 255.255.255.254 is specified, then the Remote Annex gets the address using DHCP. If the attribute is not specified, then the Remote Annex falls back to the *remote_address* admin port parameter.

You can configure the local port IP address using the **Annex-Local-IP-Address (VSA Bay Networks 35)** attribute if the admin *address_origin* port parameter is set to *acp* or *auth_server*. If an address is returned by the RADIUS server, then the Remote Annex *insists* on using that address, or it does not allow IPCP to come up. If, however, **255.255.255.255** is specified, then the Remote Annex allows the peer to set the address. If **255.255.255.254** is specified, then the Remote Annex gets the address using DHCP. If the attribute is not specified, then the Remote Annex falls back to the *local_address* port parameter.

## IPXCP

You can configure the user’s IPX network number the **Framed-IPX-Network (23)** attribute. Note that the Remote Annex *insists* on using the address returned by RADIUS, or it does not allow IPXCP to come up. If, however, **4294967294** is specified, the Remote Annex assigns an address from the local port parameter *ppp_ipx_network*.

## SLIP

You can configure the user’s IP address (the remote peer’s address) using the **Framed-IP-Address (8)** attribute if the admin *address_origin* port parameter is set to *acp* or *auth_server*. If an address is returned by the RADIUS server, then the Remote Annex uses that address. If, however, **255.255.255.254** is specified, then the Remote Annex gets the address using DHCP. If the attribute is not specified, then the Remote Annex falls back to the *remote_address* admin port parameter.

You can configure the local port IP address using the **Annex-Local-IP-Address (VSA Bay Networks 35)** attribute if the admin *address_origin* port parameter is set to *acp* or *auth_server*. If an address is returned by the RADIUS server, then the Remote Annex uses that address. If, however, **255.255.255.254** is specified, then the Remote Annex gets the address using DHCP. If the attribute is not specified, then the Remote Annex falls back to the *local_address* admin port parameter.

## Challenge-Response Mechanisms

The Remote Annex supports the standard RADIUS Challenge-Response Mechanisms through the use of the **Access-Challenge {4}** packet type and the **Reply-Message (18)** and **State (24)** attributes. That is, if the Remote Annex receives an **Access-Challenge {4}** response, it prompts the user for information, with the prompt as the string value of the **Reply-Message (18)** attribute. The Remote Annex then sends a new **Access-Request {1}** packet, with the user’s response encoded in the **User-Password (2)** attribute, and with the **State (24)** attribute returned unmodified. This dialog may continue indefinitely until the RADIUS server determines that the user should be allowed access.

## Accounting

This section describes the RADIUS Accounting features that the Remote Annex supports. Note that the RADIUS **Accounting-Request {4}** packets include the actual values of RADIUS attributes used, and not necessarily the values returned in the **Access-Accept {2}** packet. For example, this means that for a PPP user, the **Framed-IP-Address (8)** attribute is the address actually negotiated during IPCP startup, and not necessarily the address returned by RADIUS. Note that this address is included in the **Accounting-Request {4}** packet when **Acct-Status-Type (40)** = **IPCP-Start [VSE Bay Networks 3]**, because the actual negotiated address is not known at authentication time.

## Events

This section describes the events that trigger RADIUS Accounting from the Remote Annex. Each RADIUS Accounting log is queued for transmission, and once transmitted, requeued for acknowledgment. When the Remote Annex receives the corresponding Accounting-Response, the Accounting-Request log is purged. Periodically, the Remote Annex retransmits the Accounting-Request logs that have been sitting on the acknowledgment queue. Once the Remote Annex determines that it has too many logs, the Remote Annex starts syslogging the oldest ones and purging them from memory, clearing room for newer events to be held in buffers.

## User Login

The Remote Annex creates a log entry whenever a user is granted access to the Remote Annex. In this case, **Acct-Status-Type (40)** = **Start [1]**. The Remote Annex also includes the following attributes, when applicable, in this log:

- **User-Name (1)**
- **NAS-IP-Address (4)**
- **NAS-Port (5)**
- **Service-Type (6)**
- **Framed-Protocol (7)**
- **Login-IP-Host (14)**
- **Login-Service (15)**
- **Login-TCP-Port (16)**
- **Callback-Number (19) -** Only if this starts a dialback session
- **Class (25)**
- **Called-Station-Id (30)**
- **Calling-Station-Id (31)**
- **Login-LAT-Service (34)**
- **Login-LAT-Node (35)**
- **Login-LAT-Group (36)**
- **Acct-Delay-Time (41)**
- **Acct-Session-Id (44)**
- **Acct-Authentic (45)**
- **Acct-Multi-Session-Id (50)**
- **Acct- Link-Count (51)**
- **NAS-Port-Type (61)**
- **Login-LAT-Port (63)**
- **Annex-CLI-Command (VSA Bay Networks 29)**

## User Logout

The Remote Annex create a log entry whenever a user's Remote Annex session completes. In this case, **Acct-Status-Type (40)** = **Stop [2]**. The Remote Annex also includes the following attributes, when applicable, in this log:

- **User-Name (1)**
- **NAS-IP-Address (4)**
- **NAS-Port (5)**
- **Service-Type (6) -** Use Callback type if the user will be called back next, otherwise normal
- **Framed-Protocol (7)**
- **Callback-Number (19) -** Only if the user will be called back next
- **Class (25)**
- **Acct-Delay-Time (41)**
- **Acct-Input-Octets (42)**
- **Acct-Output-Octets (43)**
- **Acct-Session-Id (44)**
- **Acct-Session-Time (46)**
- **Acct-Input-Packets (47)**
- **Acct-Output-Packets (48)**
- **Acct-Terminate-Cause (49)**
- **Acct-Multi-Session-Id (50)**
- **Acct-Link-Count (51)**
- **NAS-Port-Type (61)**

## NAS Reboot Up

The Remote Annex creates a log entry whenever the Remote Annex has booted and has come up. In this case, **Acct-Status-Type (40)** = **Accounting-On [7]**. The Remote Annex includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **Acct-Delay-Time (41)**
- **Annex-Product-Name (VSA Bay Networks 33)**
- **Annex-SW-Version (VSA Bay Networks 34)**

## NAS Reboot Down

The Remote Annex creates a log entry whenever the Remote Annex is about to go down and reboot. In this case, **Acct-Status-Type (40)** = **Accounting-Off [8]**. The Remote Annex includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **Acct-Delay-Time (41)**
- **Annex-Product-Name (VSA Bay Networks 33)**
- **Annex-SW-Version (VSA Bay Networks 34)**

## NAS Accounting Start

The Remote Annex creates a log entry whenever the Remote Annex starts RADIUS Accounting. This occurs when security is turned on and reset after initially being off. In these cases, **Acct-Status-Type (40)** = **Accounting-Restart [VSE Bay Networks 6]**. The Remote Annex includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **Acct-Delay-Time (41)**
- **Annex-Product-Name (VSA Bay Networks 33)**
- **Annex-SW-Version (VSA Bay Networks 34)**

## NAS Accounting Stop

The Remote Annex creates a log entry whenever the Remote Annex stops RADIUS Accounting. This occurs when security is turned off and reset after initially being on. In these cases, **Acct-Status-Type (40)** = **Accounting-Shutoff [VSE Bay Networks 7]**. The Remote Annex includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **Acct-Delay-Time (41)**
- **Annex-Product-Name (VSA Bay Networks 33)**
- **Annex-SW-Version (VSA Bay Networks 34)**

## User Reject

The Remote Annex creates a log entry whenever the Remote Annex rejects the user based on security criteria. In this case, **Acct-Status-Type (40)** = **User-Reject [VSE Bay Networks 1]**. The Remote Annex also includes the following attributes in this log:

- **User-Name (1)**
- **NAS-IP-Address (4)**
- **NAS-Port (5)**
- **Service-Type (6)**
- **Framed-Protocol (7)**
- **Class (25)**
- **Called-Station-Id (30)**
- **Calling-Station-Id (31)**
- **Acct-Delay-Time (41)**
- **Acct-Authentic (45)**
- **NAS-Port-Type (61)**
- **Annex-Product-Name (VSA Bay Networks 33)**
- **Annex-SW-Version (VSA Bay Networks 34)**

## Call Start

The Remote Annex creates a log entry whenever a 5399, 5393, or RA6300 accepts an incoming call. In this case, **Acct-Status-Type (40)** = **Call-Start [4]**. The Remote Annex also includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **NAS-Port (5)**
- **Called-Station-Id (30)**
- **Calling-Station-Id (31)**
- **Acct-Delay-Time (41)**
- **NAS-Port-Type (61)**

## Call Reject

The Remote Annex creates a log entry whenever it rejects an incoming call before user authentication. In this case, **Acct-Status-Type (40)** = **Call-Reject [VSE Bay Networks 2]**. The Remote Annex also includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **NAS-Port (5)**
- **Called-Station-Id (30)**
- **Calling-Station-Id (31)**
- **Acct-Delay-Time (41)**
- **NAS-Port-Type (61)**

## Call Stop

The Remote Annex creates a log entry whenever it detects an end to a call. In this case, **Acct-Status-Type (40)** = **Call-Stop [5]**. The Remote Annex also includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **NAS-Port (5)**
- **Class (25)**
- **Called-Station-Id (30)**
- **Calling-Station-Id (31)**
- **Acct-Delay-Time (41)**
- **NAS-Port-Type (61)**

## IPCP Start

The Remote Annex creates a log entry whenever a PPP session starts IPCP. The log contains the negotiated IP address. In this case, **Acct-Status-Type (40)** = **IPCP-Start [VSE Bay Networks 3]**. The Remote Annex also includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **NAS-Port (5)**
- **Service-Type (6)**
- **Framed-Protocol (7)**
- **Framed-IP-Address (8)**
- **Class (25)**
- **Acct-Delay-Time (41)**
- **Acct-Session-Id (44)**
- **Acct-Multi-Session-Id (50**)
- **NAS-Port-Type (61)**
- **Annex-Local-IP-Address (VSA Bay Networks 35)**

## IPXCP Start

The Remote Annex creates a log entry whenever a PPP session starts IPXCP. The log contains the negotiated IPX address. In this case, **Acct-Status-Type (40)** = **IPXCP-Start [VSE Bay Networks 4]**. The Remote Annex also includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **NAS-Port (5)**
- **Framed-IPX-Network (23)**
- **Class (25)**
- **Acct-Delay-Time (41)**
- **Acct-Session-Id (44)**
- **Acct-Multi-Session-Id (50)**
- **NAS-Port-Type (61)**

## ATCP Start

The Remote Annex creates a log entry whenever a PPP session starts ATCP. In this case, **Acct-Status-Type (40)** = **ATCP-Start [VSE Bay Networks 5]**. The Remote Annex also includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **NAS-Port (5)**
- **Class (25)**
- **Acct-Delay-Time (41)**
- **Acct-Session-Id (44)**
- **Acct-Multi-Session-Id (50)**
- **NAS-Port-Type (61)**

## Tunnel Start

The Remote Annex creates a log entry whenever an L2TP tunnel is established with another node. When an L2TP tunnel is established, the log contains **Acct-Status-Type (40)** = **Tunnel-Start [VSE Bay Networks 8]**. The Remote Annex also includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **Acct-Delay-Time (41)**
- **Annex-Tunnel-Type (VSA Bay Networks 36)**
- **Annex-Tunnel-Medium-Type (VSA Bay Networks 37)**
- **Annex-Tunnel-Client-Endpoint (VSA Bay Networks 38)**
- **Annex-Tunnel-Server-Endpoint (VSA Bay Networks 39)**
- **Annex-Tunnel-Id (VSA Bay Networks 40)**

## Tunnel Stop

The Remote Annex creates a log entry whenever an L2TP tunnel is destroyed. When an L2TP tunnel is destroyed, the log contains **Acct-Status-Type (40)** = **Tunnel-Stop [VSE Bay Networks 9]**. The Remote Annex also includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **Acct-Delay-Time (41)**
- **Annex-Tunnel-Type (VSA Bay Networks 36)**
- **Annex-Tunnel-Medium-Type (VSA Bay Networks 37)**
- **Annex-Tunnel-Client-Endpoint (VSA Bay Networks 38)**
- **Annex-Tunnel-Server-Endpoint (VSA Bay Networks 39)**
- **Annex-Tunnel-Id (VSA Bay Networks 40)**

## Tunnel Reject

The Remote Annex creates a log entry whenever it rejects L2TP tunnel establishment with a peer. When an L2TP tunnel is rejected, the log contain **Acct-Status-Type (40)** = **Tunnel-Reject [VSE Bay Networks 10]**. The Remote Annex also includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **Acct-Delay-Time (41)**
- **Annex-Tunnel-Type (VSA Bay Networks 36)**
- **Annex-Tunnel-Medium-Type (VSA Bay Networks 37)**
- **Annex-Tunnel-Client-Endpoint (VSA Bay Networks 38)**
- **Annex-Tunnel-Server-Endpoint (VSA Bay Networks 39)**
- **Annex-Tunnel-Id (VSA Bay Networks 40)**

## MP Start

The Remote Annex creates a log entry whenever an MP bundle is created. For MMP, this will be logged only on the LNS. In this case, **Acct-Status-Type (40)** = **MP-Start [VSE Bay Networks 13]**. The Remote Annex also includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **NAS-Port (5)** = **MP [6000]** + index
- **Acct-Delay-Time (41)**
- **Acct-Multi-Session-Id (51)**
- **NAS-Port-Type (61)** = **Virtual [5]**

## MP Stop

The Remote Annex creates a log entry whenever an MP bundle is destroyed. For MMP, this will be logged only on the LNS. In this case, **Acct-Status-Type (40)** = **MP-Stop [VSE Bay Networks 14]**. The Remote Annex also includes the following attributes, when applicable, in this log:

- **NAS-IP-Address (4)**
- **NAS-Port (5)** = **MP [6000]** + index
- **Acct-Delay-Time (41)**
- **Acct-Multi-Session-Id (51)**
- **NAS-Port-Type (61) = Virtual [5]**

## Time Stamps and Session Duration

Each RADIUS Accounting record is queued with a timestamp indicating when the event occurred. Whenever a RADIUS Accounting-Request is issued by the Remote Annex, the Remote Annex records the difference in time (now - occurrence) and places the result in the **Acct-Delay-Time (41)** attribute.

Each session in the Remote Annex retains a timestamp of the start of the session. When the session ends, the Remote Annex records the difference in time (finish - start) and places the result in the **Acct-Session-Time (46)** attribute.

## Session Throughput

Each session in the Remote Annex tracks the packet and byte throughput of each session associated with a physical line. When the session ends, the Remote Annex records these statistics and places the results in the **Acct-Input-Octets (42)**, **Acct-Output-Octets (43)**, **Acct-Input-Packets (47)**, and **Acct-Output-Packets (48)** attributes.

## Session Tagging

Each session in the Remote Annex has a unique Session Identifier. This identifier is an eight-digit uppercase hexadecimal number. For the initial session, the first four digits are random, the next three digits are zero, and the final digit is one. Subsequent sessions increments the previously used session ID as its own. This identifier is placed in the **Acct-Session-Id (44)** attribute.

Each MP bundle also has a unique MP Bundle Identifier equal to the Session Identifier of the first link of the bundle. This identifier is placed in the **Acct-Multi-Session-Id (50)** attribute.

## MultiSession Link Count

Each MP session records the number of links it has used in the **Acct-Link-Count (51)** attribute.

## Authentication Method

RADIUS Accounting logs only users that are authenticated via RADIUS. This means that **Acct-Authentic (45)** = **RADIUS [1]** in each **Accounting-Request {4}** packet when **Acct-Status-Type (40)** = **Start [1]**.

## Termination Reason

Termination reason reporting is supported by the **Acct-Terminate-Reason (49)** attribute. Refer to the *Remote Access Concentrator Software Reference* for a complete description of this attribute.

### Access State

The Remote Annex supports the RADIUS standard way to preserve RADIUS server state from the **Access-Accept {2}** to the **Accounting-Request {4}** packets. That is, if the Remote Annex receives a **Class (25)** attribute in the **Access-Accept {2}**, then the Remote Annex echoes the attribute in its **Accounting-Request {4}** packet. In this way, the RADIUS server maintains a state relationship from when it granted access to when it gets recorded access.

## 5393 and 6300 Functions

The following functions have been implemented for the Model 5393 and Model 6300 Remote Annexes:

- Default Call Configuration
- Session Parameter Blocks (SPBs)
- Automated Firmware Download (AFD)
- Multi-System Multilink PPP

### Using the Default Call Configuration

When delivered to you, the Remote Annex is configured to detect automatically the type of call - TA (V.120, V.110, or X.75), synchronous PPP, or modem - arriving on an ISDN PRI B channel. Any calls not recognized within a (modifiable) 5-second timeout period are treated as modem calls. This automatic detection feature allows you to keep operating costs low by purchasing a single dial-in number for all your remote access users.

Once the call type is detected, calls are handled as follows:

- TA and modem calls are placed in protocol-detection mode and directed accordingly to a PPP, ARAP, or terminal emulation (CLI) process. Because of its inherent lack of security, SLIP cannot be detected; it must be started by issuing the **slip** command at the CLI prompt.
- Synchronous PPP calls are directed to a PPP process.

For the Remote Annex to be operational with this default configuration, the only requirements are that you set the switch type and any other interface parameter whose factory defaults do not match the service options provided by the telco for your ISDN PRI lines.

## Configuring Session Parameter Blocks

You define SPBs in the **%pri** section of the configuration file on the host you use to download Remote Annex software. By default, the file is named **config.annex** and is located in the **/usr/spool/erpcd/bfs** directory.

### SPB Sections

Each SPB in the **%pri** section must be defined within **begin_session** and **end_session** fields. The **begin_session** field lets you name an SPB within the configuration file.

An SPB has three sections:

- A section presenting call setup criteria. If the SETUP message that starts an incoming call meets *all* of these criteria, or if no criteria are specified, the call is handled by this SPB.
- A call handling section that manages all calls meeting the SPB setup criteria. This section specifies an action to be taken for the calls.
- A section containing per-session port parameter settings. All global port parameters can be overridden (as appropriate for the specific type of call) in this SPB section. If you do not need to change the value of a global port parameter, do not specify it here - that is, if no parameter values are special to this session, you can omit this section of the SPB.

## How SPBs Are Scanned

When it receives a call, the Remote Annex tries to match the SETUP information elements of the call with setup criteria values defined in the SPBs. The Remote Annex searches SPBs in the order that they appear in the configuration file, so the sequence in which you specify SPBs is important. You should order your SPBs from the most specific to the most generic.

When it scans the SPBs, the Remote Annex uses the first SPB whose setup criteria are met by the incoming call. All criteria in an SPB must be met by the SETUP information elements in order for the Remote Annex to consider the SPB a match.

Once the Remote Annex finds a matching SPB setup criteria section for a particular call, it:

- Handles the call as specified in the call-handling section.
- Uses the per-session port parameter settings to form the dynamic parameter values that will be applied to the call.

If no SPBs are defined, or no matching SPBs are found, the Remote Annex handles a call as described in *Using the Default Call Configuration on page -36*.

## SPB Fields

Use the following format when entering an SPB into the configuration file. Table 3 describes all possible SPB fields. Unless otherwise noted, each field is optional.

```
# this is a comment line

begin_session                  <session_name>
calling_no                     <phone number>
called_no                      <phone number>
called_subaddress              <number>
bearer                         <voice or data>
detected                       <detection keyword>
call_action                    <action>
max_number_of_calls            <integer>
acp_log                        <yes or no>
rate56k                        <yes or no>
set                            <parameter_name setting>
end_session
```

Table 3. SPB Field Definitions

| Field | Definition |
|---|---|
| begin_session | (Mandatory)<br>Marks the beginning of an SPB and names it. The session name is an alphanumeric string of up to 12 characters. (The Remote Annex accepts longer strings, but 12 characters is the recommended limit.) You can use this string with the CLI superuser **sessions** command to display an SPB. |
| calling_no | Specifies the telephone number that identifies the origin of the ISDN call. *Specify the entire number, including the area code, even if it would not normally be required to make the call.* Separate the area code from the rest of the phone number with a dash, or enclose the area code in parentheses. No wild card symbols (*) are permitted and white space is ignored. If this field is omitted, any calling number is permitted.<br>Sometimes the calling number is not available in the SETUP information, either because the telco did not have the equipment to deliver it or because the number is private. If **calling_no** is specified, but no number is contained in the SETUP information, the SPB is not a match. |

*(continued on next page)*

Table 3. SPB Field Definitions (continued)

| Field | Definition |
|---|---|
| called_no | Specifies the number the user entered to dial into the Remote Annex. *Specify the entire number, including the area code, even if it would not normally be required.* Separate the area code from the rest of the phone number with a dash, or enclose the area code in parentheses. No wild cards (*) are permitted. White space is ignored.<br>Note: The ACP log file shows the called number delivered by the switch (for PRI protocols). The log file may contain only the final digits of the number.<br>If this field is omitted, any called number matches this SPB. |
| called_subaddress | This field is appropriate only for end-to-end calls using an ISDN PRI line that the telco has provisioned for subaddressing. |
| bearer | Specifies the bearer capability of the call. Valid values are **voice** and **data**. |

*(continued on next page)*

Table 3. SPB Field Definitions (continued)

| Field | Definition |
|---|---|
| detected *keyword* | Specifies a keyword indicating how to handle calls detected as a result of a **call_action** field set to **detect** in another SPB.<br>Permissible *keyword* values are:<br>**valid**, which matches when either TA or synchronous PPP calls are detected.<br>**modem**, which matches when neither TA nor synchronous PPP calls are detected during the *timeout* period defined in a **call action detect** field in a separate SPB.<br>**v120**, which matches when TA calls (V.120 over HDLC) are detected.<br>**sync_ppp**, which matches when synchronous PPP calls (PPP LCP Configure-Request over HDLC) are detected.<br>**56**, which matches all calls when the line speed is 56 Kb/s.<br>**64**, which matches when the line speed is 64 Kb/s.<br>**any**, which matches any call, whether or not a **call_action** field is set to **detect** in another SPB. This is the default.<br>You can combine keywords to produce a less restrictive SPB than one containing a single keyword. For example, specifying **v120, modem** matches both V.120 and modem calls.<br>To create a more restrictive scenario than you can in one SPB, use separate SPBs. For example, if you specify **v120** in one SPB, then **56** in a second SPB, and **sync_ppp** in a third, V.120 calls will be handled by the first SPB, 56Kb/s PPP calls will be handled by the second SPB, and 64Kb/s will be handled by the third SPB. |

*(continued on next page)*

Table 3. SPB Field Definitions (continued)

| Field | Definition |
|---|---|
| call_action *keyword* | Defines how to handle the call. This field is mandatory, unless a **detect** action is already in effect for this call. Valid values for *keyword* are:<br>**detect** [*timeout*], which attempts to recognize V.120 or synchronous PPP frames in the raw digital data delivered by the telco. If neither frame type is recognized in the number of seconds specified for *timeout*, which defaults to 5 seconds, the connection type is assumed to be analog modem. After detection, the SPBs are searched again for a **detected** field entry that matches the detected frame type and indicates how to handle the call.<br>Do not use the **rate56k** or **set** fields (see below) in an SPB containing a **call_action** of **detect**.<br>**reject**, which rejects the call.<br>**modem**, which handles the call as a modem call.<br>**v120**, which handles the call as a V.120 call.<br>**sync**, which handles the call as a synchronous PPP call.<br>The default is **detect**, which means that all calls are accepted; it is impossible to reject a call beyond this point. |
| max_number_of_ calls | Defines the maximum number of calls that this session handles simultaneously. Valid PRI values are **1** to **23** (in the U.S.) and **1** to **30** (in Europe). The defaults are the upper limits (23 and 30). |
| acp_log | Specifies whether or not the Remote Annex forwards a call’s SETUP information elements and status to the ACP log file. Valid values are **yes** and **no** (the default). Status is logged as *call accept*, *call reject*, or *call disc* (disconnect). |

(continued on next page)

Table 3. SPB Field Definitions (continued)

| Field | Definition |
|---|---|
| rate56k | If set to **yes**, specifies a data rate of 56 Kb/s for the B channels, even if the bearer information in the incoming ISDN SETUP messages indicates a different rate. The default is **no**, which sets the data rate to the rate provided in the SETUP message. *Do not change this default unless you are in Europe or Australia and are having problems receiving calls from the U.S. In this situation, the telco sometimes fails to specify the correct data rate. In all other situations, specify* **no**. |
| set | Specifies a port parameter setting that is applied to the session. The syntax is:<br>**set** [*parameter parameter_value*]<br>You can specify multiple **set** commands. These settings override the values in nonvolatile memory while the session is active, but they do not change the actual values in nonvolatile memory. Any parameters not specified in *set* fields are determined by the actual global (nonvolatile memory) settings. |
| end_session | Mandatory; ends the SPB. |

# Automated Firmware Download (AFD)

The Remote Annex uses automated firmware download (AFD) to obtain the correct firmware it requires for operation. The Remote Annex downloads the version of the firmware that is appropriate to the switch type and hardware platform in use.

AFD is enabled or disabled by entries in the **%gateway** section of the **config.annex** file. AFD is enabled by default; therefore, no entry in the **%gateway** section is necessary. AFD executes in normal download mode by default.

AFD has two modes of operation: normal download and never download. When normal download is enabled, AFD attempts to download if the current revision of the firmware is outdated or if it is inappropriate for the switch type in use. Also, AFD attempts to download firmware if a Remote Annex module is marked as failed by diagnostics, regardless of what mode is specified. AFD does not attempt any download in never download mode.

## Creating %gateway Entries for AFD

Settings for AFD are included in the **%gateway** section of the configuration file. If no entries are present in the **%gateway** section, the default AFD behavior is normal download mode.

In the event that two or more entries in the **%gateway** section indicate conflicting or overlapping instructions, the latest entry has precedence.

Normal Download Mode

Normal download mode downloads firmware if it determines that the current firmware revision is outdated, or the current firmware does not support the switch type in use.You can use the following entry to enable AFD in normal mode:

```
%gateway
download pri /* download pri module */
```

Never Download Mode

Never download mode disables AFD, preventing it from downloading firmware. You can use the following entry to disable AFD. Note that **download pri never** and **download wan never** perform the same function; **download pri never** has been retained to ensure backward compatibility with earlier releases of the software.

```
%gateway
download pri never /* prevent download of pri module */
```

## Console Port Status Messages

Various status messages may be displayed in the console window during AFD.

Unsolicited Status

The following messages are displayed in the console if AFD downloads firmware to any valid device:

```
Downloading firmware, may take up to 5 mins, type afd for
status
Downloading firmware completed
```

## Solicited Status

Entering the console port command **afd** displays the status of AFD. Following is the list of messages that may be displayed, depending on the status of AFD:

- afd not started yet

  ```
  AFD not invoked:
  ```

- afd started, no download in progress

  ```
  AFD executing:
  view syslog for status, version strings or
  error(s)
  ```

- download in progress

  ```
  AFD executing:
  LOADING internal pri module firmware
  view syslog for status, version strings or
  error(s)
  ```

- afd done with no download attempted

  ```
  AFD completed:
  view syslog for status, version strings or
  error(s)
  ```

- afd done with download completed

  ```
  AFD completed:
  ABORTED loading internal pri module firmware
  ```

  or

  ```
  SUCCESS loading internal pri module firmware
  view syslog for status, version strings or
  error(s)
  ```

## Using Multi-System Multilink PPP

Multi-system Multilink PPP (MMP), a superset of Multilink PPP, allows MP links belonging to the same MP bundle to terminate on multiple Remote Annexes. The Remote Annexes are combined together in an MMP group to use all of the incoming channels in the group, increasing the potential bandwidth of an MP bundle. Bay Networks Remote Annexes support MMP for incoming calls only. The locations of the MP links are completely transparent to remote users; users need (and receive) no information about which Remote Annex terminates a given MP link. The location of the MP bundle head is determined by the bundle discovery protocol. The Layer 2 Tunneling Protocol (L2TP) is used to tunnel MP links to remote MP bundle heads, ensuring that successive links on one Remote Annex in an MMP group are combined into the same bundle as the primary link on another Remote Annex.

MMP is disabled by default, through the annex parameter **mmp_enabled** set to **n**. To enable MMP, you must set **mmp_enabled** to **y** and configure the global port or inbound channels for MP, if you have not done so already. MMP relies on three other features, which are enabled when MMP is enabled:

- MP bundle discovery
- Virtual MP links
- Layer 2 Tunneling Protocol (L2TP)

## MMP Groups

An MMP group is a set of one or more Remote Annexes that act as a single entity for any MP links that terminate on any of the Remote Annexes in the group. MMP groups usually are organized to correspond to telco hunt groups. All Remote Annexes in an MMP group must reside on the same Ethernet segment and, where applicable, on the same IP subnet. A Remote Annex can belong to a single MMP group only. Otherwise, Remote Annexes can be grouped any way, with multiple groups allowed on the same Ethernet segment.

MMP groups are identified by their end point discriminator, which comprises the port parameters **mp_endpoint_class** and **mp_endpoint_address**. All the Remote Annexes in an MMP group must have the same **mp_endpoint_class** and the same **mp_endpoint_address**. When MMP is enabled and **mp_endpoint_class** is set to **loc** or **psndn**, the **mp_endpoint_address** parameter indicates an endpoint discriminator address, which is the number of the hunt group or the name of the rotary served by the MMP group. *Refer to the* Remote Access Concentrator Software Reference *for complete descriptions of these parameters.*

## Establishing MMP Connections

When a remote user dials the number for a hunt group, a Remote Annex belonging to the MMP group assigned to that hunt group answers the call. The remote user can use any type of line: BRI, PRI, or asynchronous. The answering Remote Annex detects the type of call automatically and answers it appropriately, creating an MP link.

While the MP link is in the authentication phase, the Remote Annex initiates the Bundle Discovery Protocol to determine if an MP bundle head for the user exists. The MP bundle head is the Remote Annex that contains the first (primary) link of an MP bundle. The Bundle Discovery Protocol searches first the current Remote Annex for an MP bundle, then the other Remote Annexes in the MMP group. If the Bundle Discovery Protocol does not find an existing MP bundle, the current MP link becomes the primary MP link and creates an MP bundle, and the current Remote Annex becomes the MP bundle head. If the Bundle Discovery Protocol locates an existing MP bundle for the remote user, the current MP link becomes a secondary MP link. If the MP bundle head is a different Remote Annex, the current link is tunnelled to that MP bundle head via L2TP and becomes a virtual link; virtual links are always secondary links. Secondary MP links are combined with the primary MP link to form an MP bundle; all MP fragments are reassembled by the MP bundle head.

MP bundles handle links terminating on the MP bundle head and virtual links equally, without preference. A primary link always resides on the MP bundle head and is never a virtual link.

The maximum possible number of MP links permitted on any Remote Annex is the maximum number of actual channels plus an equal number of virtual links.