

Remote Access Software Version 5.4 Release Notes

Marketing Release 5.4

Part No. 303105-A Rev. 00
May 1998



Bay Networks

Copyright © 1998 Bay Networks, Inc.

All rights reserved. Printed in the USA. May 1998.

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.



SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).





Contents

Ordering Bay Networks Publications	ix
Bay Networks Customer Service	ix
How to Get Help	x
Supported Remote Access Hardware For Release 5.4	2
Supported Software and Switch Types For Release 5.4	3
Supported Operating Systems	3
Supported Compiler Versions	4
RADIUS Server Information	4
SecurID/ACE Compatibility Information	4
SafeWord Compatibility Information	5
Supported Switch Types	5
New Features in Release 5.4	6
Forcing the Download of Modem Code	6
Overriding the Nameserver	7
Specifying Separate RADIUS Accounting Servers	7
Allowing Login By Guest Users	8
Enabling 32-Bit Proxy ARP	8
Remote Access Software Release 5.4 Corrections	9
SPR 9308	9
SPR 9802	9
SPR 9805	9
SPR 11561	9
SPR 11722	9
SPR 11714	10
SPR 11604	10
SPR 10144	10
SPR 11563	10
SPR 11484	10
SPR 10926	11
Known Problems In Release 5.4	11
CLI Commands Added In R14.1.9	13
history	13
ppp -i	14
New admin/na Parameters in R14.1.9	14
RADIUS Filters	15
TMUX and TSTTY	17
Known Problems/Limitations in R14.1.9	17
Problems Resolved Since R14.1	17
SPR 11117	17
SPR 9594	17
SPR 10519	17
SPR 11019	18
SPR 11241	18
SPR 11253	18
SPR 11128	18
SPR 11246	18
SPR 11247	18
SPR 10954	19
SPR 10954	19



Contents

- Features in Release 5.1 19
 - AFD (Automatic Firmware Download) Changes 20
 - The afd Command 20
 - How AFD Works 21
 - Single Number ISDN Dial-Up 23
 - Obsolete option_key Parameter 23
 - Embedded RADIUS Client 24
 - Multi-System Multilink PPP 25
 - Long User Names 26
 - Corrections to Embedded RADIUS Client Documentation 26
 - RADIUS Attributes - Additional Information 27
 - CLI IP Host Filtering - Corrected Information 31
 - Remote Access Software Release 5.1 Corrections 31
 - SPR 10952 31
 - SPR 10229 31
 - SPR 10686 31
 - SPR 9824 31
 - SPR 9941 31
 - SPR 9937 32
 - SPR 9950 32
 - SPR 9955 32
 - SPR 8739 32
 - SPR 9977 32
 - SPR 10210 32
 - SPR 9936 32
 - SPR 10137 32
 - SPR 10255 33
 - SPR 9540 33
 - SPR 10434 33
 - SPR 9991 33
 - SPR 10483 33
 - SPR 10457 34
 - SPR 10568 34
 - SPR 10494 34
 - SPR 10525 34
- Changes to UNIX CLIs Release 14.1 34
 - Known Problems/Limitations 34
 - SPR 10025 38
 - SPR 10269, 10270, 10271 38
 - SPR 10367 38
 - SPR 10893 38
 - SPR 8482, 9901 38
 - SPR 10653 38
 - SPR 10585 38
 - SPR 10037 39
 - SPR 10380 39
- Changes to Annex Manager Release 3.1 39
 - System Requirements 39
 - Sun Requirements 39

HP Requirements	40
IBM Requirements	40
Remote Display Requirements	40
Known Problems/Limitations	40
Changes to Quick2Config Annex Release 3.1	41
System Requirements	41
Known Problems/Limitations	41
Correction to Quick2Config Annex Release 3.1: SPR 9155	42
Changes to the Network Administrator Utility (na) for Windows NT and Windows 95	42
Hardware/Software Requirements	42
Special Considerations	43
Changes to Remote Annex Server Tools for Windows NT R3.1	43
System Requirements	43
Installing Windows NT Server Tools	44
Manually Removing Remote Annex Server Tools for Windows NT	44
Known Problems/Limitations	46
24-Hour Unit Replacement Service	48
Saving the Unit Configuration	48
Restoring the Unit Configuration	51
Placing the File onto the Unit.	51
Using monitor Mode to Provide an IP Address for a New Unit	53

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 978-916-8880 (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

Remote Access Software Version 5.4 Release Notes

These release notes apply to Marketing Release 5.4 of Bay Networks[®] Remote Access software, which comprises these individual software releases:

- Remote Access Operational Code Version 14.2.15.
- Microcom Modem Code Version 2_4_81
- Host Tools for UNIX Version R14.2.15
- Server Tools for Windows NT[®] R3.1
- Quick2Config[®] Annex R3.1
- Annex Manager[™] R3.2

You can view the most current version of these release notes on the Bay Networks World Wide Web page at: <http://support.baynetworks.com/Library/tpubs>. Check this site for late information that is not included in this version of the release notes.

These Release Notes address the following topics:

- [Supported Remote Access Hardware For Release 5.4](#)
- [Supported Software and Switch Types For Release 5.4](#)
- [New Features in Release 5.4](#)
- [Remote Access Software Release 5.4 Corrections](#)
- [Known Problems In Release 5.4](#)
- [CLI Commands Added In R14.1.9](#)
- [New admin/na Parameters in R14.1.9](#)
- [TMUX and TSTTY](#)
- [Problems Resolved Since R14.1](#)
- [Features in Release 5.1](#)
- [Changes to UNIX CLIs Release 14.1](#)
- [Changes to Annex Manager Release 3.1](#)
- [Changes to Quick2Config Annex Release 3.1](#)

- [Changes to the Network Administrator Utility \(na\) for Windows NT and Windows 95](#)
- [Changes to Remote Annex Server Tools for Windows NT R3.1](#)
- [24-Hour Unit Replacement Service](#)

Supported Remote Access Hardware For Release 5.4

Release 5.4 supports the following platforms:

- RA2000
- RA4000
- RA6100
- RA6300
- RA5390
- RA5391
- RA5393



Throughout these release notes, the word “unit” is used as a synonym for “Remote Annex”.

Supported Software and Switch Types For Release 5.4

Release 5.4 supports or is compatible with a number of operating systems, compilers, switch types, and security servers.

Supported Operating Systems

The distribution media contain binary files for the supported operating systems. When the installation script detects that there are binary files for the host operating system, it gives you the option of installing the binary files or loading the source code and compiling the software at a later time. If there are no binary files available, the script loads the source code and uses a supported compiler on the host system to build the image. If the script does not identify a compiler on your system, it ends the installation session.

Binary files and source code are provided on the distribution media for each of the following operating system versions:

- HP-UX 10.10/10.20
- IBM RS/6000 AIX 4.1.4/4.1.5
- Microsoft® Windows NT 3.51 for Intel
- Microsoft Windows NT 4.0 for Intel
- Microsoft Windows NT 4.0 for DEC Alpha
- Red Hat V4.1 Linux (2.0.27 Kernel)
- Solaris 2.4/2.5/2.5.1
- Sun Microsystems SunOS 4.1.3/4.1.4

Supported Compiler Versions

Release 14.2.15 supports the following compiler versions:

- Solaris 2.4: Workshop Compilers 4.2
- HP-UX 10.10: HP C Compiler
- SunOS 4.1.4: Bundled SunOS C Compiler
- ITRA-Linux 2.0.18: Version 2.7.2

RADIUS Server Information

The embedded RADIUS client in Remote Access Software Release 5.4 is known to be compatible with the following RADIUS servers:

- Any shipping Bay Secure Access Control (BSAC) server
- Livingston 2.01
- Ascend 22497
- Merit RADIUS 2.4.23C

SecurID/ACE Compatibility Information

Remote Access Software Release 5.4 is compatible with SecurID/ACE Server Versions 2.3 and 3.0. Client software is supported on Windows NT versions 3.51 and 4.0, and on the following UNIX versions:

- HP-UX 10.10 and 10.20
- IBM AIX 4.1.x on RISC/6000
- Solaris 2.4, 2.5, and 2.5.1
- SunOS 4.1.3 and 4.1.4

SafeWord Compatibility Information

Remote Access Software Release 5.4 operates with Version 4.1 of the SafeWord server, and is compatible with Version 4.1 of the SafeWord UNIX client. There is no support for Windows NT.

Supported Switch Types

[Table 1](#) lists the PRI switch types supported in Release 14.2.15.

Table 1 Valid PRI switch_type Values

Protocol	switch_type	Description
T1/PRI	AT9	AT&T 5ESS Version 9 switch
	AT4	AT&T 4ESS support
	DMS	Nortel's DMS100 switch
	NI2	A switch supporting National ISDN2
E1/PRI	ETS	Used in Europe; ETSI
	ETS-NCRC4	Used in Europe; ETSI without CRC
	AU1	Used in Australia

[Table 2](#) lists the other switch types supported in Release 14.2.15.

Table 2 Valid switch_type Values

Protocol	switch_type	Description
Channelized T1	UST1	Used in North America
	HKT1	Used in Hong Kong

New Features in Release 5.4

Release 5.4 introduces five new features.

Forcing the Download of Modem Code

You can use the optional keyword **force** with the command to download Microcom modem code for Remote Annex 6100s and Remote Annex 6300s. By adding the **force** keyword to the end of the command line or configuration file entry, you can force the download of modem code to a modem that is not responding properly.

You can determine if a modem is not responding properly by issuing the **modem -v** command; any unresponsive modems on the RA 6100 or RA 6300 will be listed as having an unknown version.

In the Remote Annex's configuration file, the command to force the download of modem code is:

```
download mic <modem code filename> [force]
```

At the command line, the command to download modem code is

```
afd asy<portnum> <modem code filename> [force]
```



The **force** keyword should be used only as a final attempt to recover a Microcom modem used in an RA 6100 or an RA 6300. Using the **force** keyword will not enable you to recover a modem that has experienced a hardware failure.

Overriding the Nameserver

The annex parameter **nameserver_override** governs the unit's behavior when the unit and a remote host have different non-zero nameserver addresses configured during IPCP negotiations. If **nameserver_override** is set to **N** (its default value), the unit will acknowledge the remote host's nameserver address. If **nameserver_override** is set to **Y**, the unit will not acknowledge the remote host's nameserver address, and will return instead the nameserver address configured in the unit. Each of the four nameserver options are negotiated independently: primary DNS, secondary DNS, primary WINS, secondary WINS.

Specifying Separate RADIUS Accounting Servers

The parameters **radius_acct1_host** and **radius_acct2_host** enable you to specify RADIUS accounting servers that are separate from your RADIUS authentication servers. Set the values of these parameters to the IP addresses of the corresponding accounting servers. The default value for each of these parameters is **0.0.0.0**.

If one or more separate accounting servers have not been set, RADIUS will use the **pref_secure1_host** and **pref_secure2_host** as the accounting servers.

If a primary accounting server is specified, but no backup accounting server, RADIUS interprets this as meaning that no backup server is desired, and does not use either of the authentication servers as a backup accounting server.

Allowing Login By Guest Users

You can allow a guest user to log in to a unit without having to provide a password. You can enable this functionality through a unit's configuration file. For example:

```
%local_user
begin_user user_telnet
 clicmd telnet <hostname>
end_user
```

You can include multiple **%local_user** entries in the configuration file, which allows multiple users to log in to the unit without a password and then access a particular host on the network. Guest users may use any CLI command that does not require superuser privilege.

Enabling 32-Bit Proxy ARP

The port parameter **proxy_arp_enabled** allows the unit to proxy ARP all remote IP connections when it is set to **yes**. The default value, **no**, allows the unit to proxy ARP only those remote IP connections with the same subnet address as the unit.

When **proxy_arp_enabled** is set to **yes**, the unit will respond to ARP requests containing the IP address of the remote connection. The unit should send ARP replies with the source IP address of the remote connection and the source MAC address equal to the unit's MAC address.

Remote Access Software Release 5.4 Corrections

The following Remote Access Software problems have been fixed in Release 5.4.

SPR 9308

If **pref_secure1_host** is down, security now contacts **pref_secure2_host** properly.

SPR 9802

Filters that have been entered previously from the CLI **filter add** command and subsequently deleted are no longer restored when the unit is rebooted.

SPR 9805

Filters created using **interface=all** no longer create erroneous multiple entries in the filter list.

SPR 11561

Dialback is no longer granted if a user dials into a unit configured for outbound pools only.

SPR 11722

The unit now negotiates local IP addresses correctly for BayDVS users.

SPR 11714

The TMS field Authentication Protocol is no longer valid in versions of the image or **erpcd** subsequent to R14.1. A new TMS field, Server Location, determines if the BayDVS user is authenticated locally by the unit or remotely by the gateway.

In the case where an image subsequent to R14.1 is using a TMS (**erpcd**) from prior to R14.1, the Authentication Protocol field is used as follows: if it is set to ACP, authentication is performed locally by the unit; if it is set to RADIUS, authentication is performed remotely by the gateway.

SPR 11604

rtnet sessions can be opened with Remote Annex ports numbered higher than 64.

SPR 10144

Separate RADIUS accounting server functionality has been implemented.

SPR 11563

A new Nameserver parameter, **nameserver_override**, has been added to the unit's image. This parameter governs the unit's behavior when the unit and the remote host have different non-zero NS addresses configured during IPCP negotiations.

SPR 11484

CHAP now works correctly on sync PPP connections.

SPR 10926

The map3270 file now supports an entry “attention”. The format is similar to the other key mappings in map3270, for example:

```
attention = '\e[14~';
```

Key definitions in map3270 are no longer required to be in uppercase.

Known Problems In Release 5.4

- ARAP is not functional in Release 5.4; setting port mode to **arap** causes the unit to dump when a call is received by that port. The syslog may contain erroneous messages such as: Received attribute with incorrect length.
- An RA6100 with 4MB of RAM may dump when using DHCP.
- Sync PPP is unable to negotiate LCP when CHAP is configured in an SPB. An example SPB follows:

```
begin_session detect_me
call_action detect 15
end_session

begin_session V120_user
detected V120
call_action v120
set ppp_ncp all
##set ppp_ncp ipcp,ccp,mp,ipxcp,atcp
set ppp_security_protocol pap
end_session

#
#begin_session sync_user
#detected sync_ppp
#bearer data
call_action sync
set mode ppp
set ppp_ncp ipcp,ccp,mp,ipxcp,atcp
```

```
set mp_mrru 1500
set ppp_security_protocol chap
end_session

begin_session unmatched
call_action reject
end_session
```

- A proxy RADIUS dialup client will have an IPX node number assigned to it even if the profile specifies only an IP address.
- The **na** utility in R14.2.15 does not recognize the following parameters; to modify their values, you must use the **admin** utility:
 - **ipcp_unnumbered**
 - **ppp_ipx_network** (RA 6300 and RA 5393)
 - **ppp_ipx_node** (RA 6300 and RA 5393)
- The **admin** utility in R14.2.15 does not recognize the **radius_port_encoding** parameter; to modify its value, you must use the **na** utility.
- The **na** utility in R14.2.15 supports all the new parameters that have been added in maintenance releases subsequent to R14.1, but does not recognize them in units that are running the maintenance software versions X14.1.1 thru X14.1.17, including R14.1.9. The **na** utility will recognize these parameters in maintenance versions starting with X14.2.18. The affected parameters are:
 - **nameserver_override**
 - **pref_nbns1_addr**
 - **pref_nbns2_addr**
 - **proxy_arp_enabled**
 - **radius_acct1_host**
 - **radius_acct2_host**
 - **radius_acct1_port**
 - **radius_acct2_port**

- **radius_acct1_secret**
- **radius_acct2_secret**
- **radius_auth1_port**
- **radius_auth2_port**
- **radius_auth1_secret**
- **radius_auth2_secret**

CLI Commands Added In R14.1.9

Four commands were added to the command line interface in R14.1.9: **history**, **ppp -i**, **reset annex filter**, and **list -r**. Descriptions of **history** and **ppp -i** follow; refer to [RADIUS Filters](#) on page 15 for descriptions of **reset annex filter** and **list -r**.

history

The **history** CLI command is similar to the UNIX **history** command. By default, **history** displays the last 25 CLI commands, the maximum number of commands that can be shown. The command's syntax is:

history n - Display *n* previous CLI commands, up to a maximum of 25.

The **history** command incorporates four companion commands:

- **!!** - Re-issue the most recent CLI command.
- **!n** - Re-issue the *n*th CLI command.
- **Ctrl-p** - Display the previous CLI command, up to the 25th.
- **Ctrl-n** - Display the succeeding CLI command, if there is one (otherwise, nothing is displayed).

Ctrl-p and **Ctrl-n** work without a <CR>; use them to scroll backward and forward through the command history.

ppp -i

The **-i** argument now may be used with the **ppp** command. This argument displays the locally configured local and remote addresses.

New admin/na Parameters in R14.1.9

Four configuration parameters were added in R14.1.9.

Two parameters have been added to the Annex category to enable the unit to negotiate the addresses of the primary and secondary NetBIOS name servers (per RFC 1877):

- **pref_nbns1_addr** - The IP address of the primary NetBIOS name server. The default value is 0.0.0.0.
- **pref_nbns2_addr** - The IP address of the secondary NetBIOS name server. The default value is 0.0.0.0.

Two parameters have been added to the Security category to enable an administrator to change the prompts for RADIUS user and RADIUS password. These prompts are used only when **auth_protocol** is set to **radius**, and are not used for local authentication, or when **auth_protocol** is set to **acp**.

- **radius_user_prompt** - The unit's RADIUS login prompt string. The default string is **Annex%susername%c**.
- **radius_pass_prompt** - The unit's RADIUS password prompt string. The default string is **Annex%spassword%c**.

RADIUS Filters

RADIUS filters now reside on the unit, rather than on the RADIUS server.

The unit reads these filters when it boots, and stores the filters in memory, applying them only to Framed PPP or SLIP users. This is achieved through the use of a **%filters** section in the unit's configuration file. An example **%filters** section follows:

```
%filters
begin_filter blockhost
output include ip dst_addr 132.245.33.8 discard
end
```

The **%filters** section begins with the keyword **%filters** and ends with the beginning of the next keyword section or with the end of the file. One or more **%include** statements can be used in the section to include filter definitions from other configuration files on the boot server or the local system.

The keyword **begin_filter**, followed by the filter's name, introduces each individual filter definition. The filter's name is case-sensitive and can be up to 23 characters long. The keyword **end** terminates each filter definition.

Each line of the filter definition is the same as a RADIUS VSA Annex-Filter string. (This is the same as the **filter** subcommand **add** in the CLI, but without the **add** command or the interface specification.)

A filter definition consists of these arguments, which are explained in [Table 3](#):

```
<direction> <scope> <family> <criteria> <actions>
```

Table 3 Filter Definition Arguments

Argument	Valid Values	Description
direction	input, output	This value specifies the direction of packets to which to apply the filter.
scope	include, exclude	This value causes the filter to be inclusive or exclusive.
family	ip	In Release 5.4, only IP is available for this argument.
criteria	dst_addr, dst_port, src_port, src_address, address_pair, port_pair, protocol	These are the conditions on which the filter accepts or rejects packets.
actions	discard, icmp, syslog	The action which may be performed upon meeting the criteria.

The **reset annex filters** command causes the unit to discard the filter definitions in memory and read them again from the **%filters** section of the configuration file. This also happens if you issue the **reset annex all** command.

The **filter** subcommand **list** now accepts the argument **-r**; this displays the loaded filters.

TMUX and TSTTY

As of Release 5.3, support for TMUX and TSTTY is discontinued. This is an issue only for customers who are using Remote Annexes.

Known Problems/Limitations in R14.1.9

- Setting the port mode to **ARAP** causes the unit to dump a core file when it receives a call.
- ATCP works only if the port mode is set to **ppp**. ATCP will not work if the port mode is set to **auto_adapt** or **auto_detect**.

Problems Resolved Since R14.1

SPR 11117

Tunnel key decryption of the RADIUS received encrypted attribute is now supported on the unit.

SPR 9594

The unit should no longer panic when receiving CHAP challenges.

SPR 10519

LAT HIC printing should no longer skip the last few characters of a file.

SPR 11019

CCP should no longer panic.

SPR 11241

The unit now supports the use of the Domain Name Server Option (option 6) and NetBIOS over TCP/IP Name Server Option (option 44) from DHCP for the DNS and NBNS address requests during IPCP negotiations.

SPR 11253

RADIUS filters now reside on the unit, reducing additional network traffic and making them easier to manage.

SPR 11128

The unit no longer responds to ICMP router solicitations when **routed** is set to **no**.

SPR 11246

The event log parsing function now parses the log correctly.

SPR 11247

The parameters **pref_nbns1_addr** and **pref_nbns2_addr** have been added for primary and secondary NBNS (WINS) addresses per RFC 1877.

SPR 10954

You can change the unit's username and password prompts via embedded RADIUS using the parameters **radius_user_prompt** and **radius_pass_prompt**.

SPR 10954

The **ppp -i** command has been added.

Features in Release 5.1

The following sections describe the features supported in Release 5.1:

- [*AFD \(Automatic Firmware Download\) Changes*](#)
- [*Single Number ISDN Dial-Up*](#)
- [*Obsolete option key Parameter*](#)
- [*Embedded RADIUS Client*](#)
- [*Multi-System Multilink PPP*](#)
- [*Long User Names*](#)
- [*Corrections to Embedded RADIUS Client Documentation*](#)
- [*RADIUS Attributes - Additional Information*](#)

[Table 4](#) summarizes new feature support by platform.

Table 4 New Feature Support

		Platform						
		RA2000	RA4000	RA5390	RA5391	RA5393	RA 6100	RA 6300
Feature	Automatic Firmware Download				X	X	X	X
	Single number dial-up					X		X
	Obsolete option_key	X	X	X	X	X	X	X
	Embedded RADIUS client	X	X	X	X	X	X	X
	Multi-System Multilink PPP					X		X
	Long user names	X	X	X	X	X	X	X

AFD (Automatic Firmware Download) Changes

This section describes a new superuser CLI command, **afd**, and other changes to AFD not reflected in the Release 5.1 UNIX documentation.

The **afd** Command

The new superuser **afd** command allows manual downloading of firmware for a designated module. The syntax is:

afd *device* [*filename*]

[Table 5](#) describes the arguments.

Table 5 Arguments for the **afd** Command

Argument	Description
<i>device</i>	Specifies the module firmware to be downloaded.
<i>filename</i>	<p>Specifies the name of the load host file containing the firmware to be downloaded. If this argument is omitted, afd checks /usr/spool/erpcd/bfs/afd_list to determine the file to be downloaded.</p> <p>If you specify <i>filename</i>, the firmware in that file is downloaded once. When you reboot, the firmware file downloaded reverts to one of those listed in afd_list.</p> <p>Additional information on AFD and afd_list follows this table and is also contained in the manual <i>Managing Remote Access Concentrators Using Command Line Interfaces</i>.</p>

How AFD Works

The Automatic Firmware Download software starts when the unit boots or when the **afd** command is issued. The software reads the **/usr/spool/erpcd/bfs/afd_list** file, which is a text file listing the firmware file names, hardware-type strings, switch types, and version strings. AFD uses this file to validate the image(s) stored in the module(s).

The contents of the **afd_list** file follow. Each line contains two fields, a file name and version information, separated by white space. The version information is divided into three fields, separated by semicolons (;). The first field is the hardware type; the second field is the switch type (as set by the **switch_type** parameter); and the third field is the version string.

```
# This file is generated automatically. Do not edit.
#
# Any "PRI X1" image can go on any "PRI X1" or "CAS X1" module.
# "CAS X1" images may go only on "CAS X1" modules or on "PRI X1"
# modules where the DSP presence has been detected.
#
pri_t1-1_128 PRI T1 USA|PRI T1;DMS|AT5|AT9|NI2;VERSION A MGR=1.128
pri_e1-1_68 PRI E1 ETSI|PRI E1;ETS|ETS-NCRC4;VERSION A MGR=1.68
```

```
pri_csu-1_222 CAS T1 CSU|PRI T1 USA CSU|PRI T1 CSU;AT9|DMS|NI2;VERSION A MGR=1.222

pri_4ess-1_13 PRI T1 4ESS CSU;AT4;VERSION A MGR=1.13

pri_aus-1_35 PRI E1 AUSTEL;AU1;VERSION A MGR=1.35

pri_sng-1_3 PRI E1 SINGAPORE;SNG;VER=VERSION A MGR=1.3

cas_elt1-1_39 CAS T1 CSU|CAS
E1;UST1|TWT1R1|HKT1|KRE1R2|BRE1R2|BBE1R2|SWE1P7|IDE1R2|TWT1|NZE1R2|PHE1R2|
THE1R2|MYE1R2|ARE1R2|CNE1R2|MXE1R2|ANE1R2|TRE1R2|ILE1R2|UST1FD;
VERSION CAS-E1T1-1.39

mod_mic-2_4_812880;;2.4.81/85

pri_dgt-1_2 PRI T1 TAIWAN CSU;DGT;VERSION AMGR=1,2

pri_hkt-1_3 PRI T1 HONGKONG CSU;HKT;VERSION AMGR=1.3
```

AFD interprets **afd_list** as follows:

- If the switch type set via the **switch_type** parameter does not match any of the switch types in **afd_list**, no firmware is downloaded. If the switch type *does* match an entry in **afd_list**, AFD checks the entry's hardware type.
 - If the hardware type is "CAS T1.*" or "CAS E1.*" and the firmware in the WAN module is "CAS T1.*" or "CAS E1.*", the version is checked. If the version in **afd_list** does not match the version in the module, the firmware is downloaded.
 - If the hardware type is "CAS T1.*" or "CAS E1.*" and there is no firmware in the module, the switch type is ignored, and the firmware image downloaded is the one appropriate for the first hardware type (CAS T1 or CAS E1) in **afd_list** that matches the hardware type of the module. Subsequently, AFD checks to see whether or not the module can run the CAS image appropriate for the switch type. If so, the firmware for that image is downloaded.



An empty module is rare and is usually the result of an interrupted download.

Single Number ISDN Dial-Up

The single number ISDN dial-up feature allows you to configure the unit to discriminate automatically between the various protocols that may be used for dial-up over ISDN. This allows you to lower operating costs by purchasing a single dial-in number to cover all remote access needs, rather than having separate numbers for TA (V.120), synchronous PPP, and modem users. The design of this method great flexibility to determine how to handle calls because it does not require any particular disposition of a call solely based on the protocol in use. Instead, the session parameter block (SPB) mechanism is used to determine how to handle the call after the protocol has been detected, and a set of carefully chosen defaults allows simple configuration.

Obsolete `option_key` Parameter

As of Release 5.1, all Remote Annexes are shipped with IP, IPX, AppleTalk, and TN3270 keys included. Although not reflected in the Release 5.1 documentation, setting the **option_key** parameter is no longer required for enabling these features; now they are enabled by default.

LAT is the only software protocol available that is optional and that requires a key.

Since the features now enabled by default consume a significant amount of memory, you may want to disable those that you do not use. To do so, use the Annex parameter **disabled_modules**.



The **lat_key** parameter must be set in order to enable LAT.

Embedded RADIUS Client

Release 5.1 includes an embedded RADIUS client. This feature enables you to use a Remote Annex in conjunction with the following RADIUS servers:

- Any shipping BSAC server
- Livingston 2.01
- Ascend 22497
- Merit RADIUS 2.4.23C

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 to the client 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.

You can use the embedded RADIUS client independently, with the unit's authentication protocol set to RADIUS, or you can use erpcd as a proxy RADIUS client running under the ACP authentication protocol.

Note that the capabilities provided by the proxy RADIUS client running under the ACP authentication protocol 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 authentication protocol is RADIUS.

Multi-System Multilink PPP

Release 5.1 supports multi-system Multilink PPP (MMP) on Remote Annexes that support PRI connections: RA 6300 and RA 5393.

MMP is a superset of Multilink PPP, allowing MP links belonging to the same MP bundle to terminate on multiple units. The units 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. An MMP group is a set of one or more units that act as a single entity for any MP links that terminate on any of the units in the group; all members of an MMP group must reside on the same Ethernet segment. MMP groups usually are organized to correspond to telco hunt groups.

Bay Networks units 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 unit terminates a given MP link. The location of the MP bundle head is determined by the bundle discovery protocol. Layer 2 Tunneling Protocol (L2TP) tunnels MP links to remote MP bundle heads, ensuring that successive links on one unit in an MMP group are combined into the same bundle as the primary link on another unit.

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.

Long User Names

Release 5.2 supports user names of up to 128 characters.

Corrections to Embedded RADIUS Client Documentation

This section contains corrections to the Embedded RADIUS Client information appearing in the manual *Managing Remote Access Concentrators Using Command Line Interfaces*.

The **radius_acct_level** parameter value **basic** has been renamed to **standard**. (The other available value for this parameter is **advanced**.)

The default value of the **radius_acct_port** parameter has been changed to **1646**. (Previously, the default value was **1813**.)

The default value of the **radius_auth_port** parameter has been changed to **1645**. (Previously, the default value was **1812**.)

The unit of measure associated with the **radius_timeout** parameter is seconds.

The RADIUS attributes **Unassigned(17)**, **Unassigned(21)**, **Termination-Action(29)**, **Proxy-State(33)**, **Login-LAT-Group(36)**, **Framed-AppleTalk-Link(37)**, **Framed-AppleTalk-Network(38)**, and **Framed-AppleTalk-Zone(39)** are not supported in this release.

RADIUS Attributes - Additional Information

After changing the setting of the **auth_protocol** parameter, you must reboot the unit in order for the change to take effect.

The **Annex-System-Disconnect** attribute (Bay Networks VSA 44) is supported. This integer attribute describes the system disconnect code, and is logged in RADIUS Accounting Stop messages. The reported values are shown in [Table 6](#).

Table 6 RADIUS Attributes

Value	Description
0	Unknown
1	Telephone disconnect: caller hung up
2	Dial failed
3	WAN manager error
4	Disconnect reset
5	Error from adm_notify()
6	Modem down from adm_notify()
7	PPP protocol disconnect
8	Inactivity timer (port data)
9	CLI “hangup” command
10	CLI last-job
11	Max logon or Session-Timeout timer
12	Normal slave termination (net disc)
13	Abnormal termination (TCP RST, other)
14	DCD wait (probably modem conn) failed
15	param cli_inactivity
16	Port was reset, probably by admin
17	CLI authentication failed

Table 6 RADIUS Attributes (Continued)

Value	Description
18	Slave port authentication failed
19	PPP PAP failed
20	PPP CHAP failed
21	We reset modem
22	Modem dead
23	PPP LCP negotiation failure
24	PPP last NCP failure (IPCP)
25	PPP last NCP failure (IPXCP)
26	PPP last NCP failure (ATCP)
27	PPP last NCP failure (CCP)
28	PPP last NCP failure (MP)
29	PPP last NCP timeout (IPCP)
30	PPP last NCP timeout (IPXCP)
31	PPP last NCP timeout (ATCP)
32	PPP last NCP timeout (CCP)
33	PPP last NCP timeout (MP)
34	PPP initialization failed
35	PPP unknown disconnect reason code
36	PPP dialback
37	PPP address in use
38	PPP no device
39	PPP modem hangup signal received
40	PPP hangup signal received
41	PPP termination signal received

Table 6 RADIUS Attributes (Continued)

Value	Description
42	PPP kill signal received
43	PPP time signal received
44	PPP no memory
45	PPP connection abort
46	PPP VPN LCP phase failure
47	PPP VPN AUTH phase failure
48	PPP MP invalid port configuration
49	PPP invalid operation for device type
50	PPP MMP bundle discovery failure
51	DVS registration failure
52	DVS home agent deregistration
53	DVS tunnel no renew
54	DVS tunnel expired

Annex-Modem-Disconnect (Bay Networks VSA 45): This integer attribute describes the disconnect reason reported by the modem. The reported values are shown in [Table 7](#).

Table 7 Modem Disconnect Reasons

Value	Description
0	Unknown
1	Local host disconnect (unit hang-up)
2	CD timer expired
3	Reserved
4	Protocol disconnect by remote modem
5	Clear-down

Table 7 Modem Disconnect Reasons (Continued)

Value	Description
6	Long space disconnect
7	Carrier lost
8	Retrain timeout

Annex-Disconnect-Reason (Bay Networks VSA 46): This integer attribute describes the composite disconnect reason reported by the unit. Essentially, this attribute is the more important of the **Annex-System-Disconnect** and **Annex-Modem-Disconnect** reasons. Its values are the same as those from **Annex-System-Disconnect** with the addition of those listed in [Table 8](#).

Table 8 Unit Disconnect Reasons

Value	Description
100,002	Local host disconnect
100,003	CD timer expired
100,004	Reserved
100,005	Protocol disconnect by remote modem
100,006	Long space disconnect
100,007	Carrier lost
100,008	Retrain timeout

Annex-Transmit-Speed (Bay Networks VSA 50): This integer equals the modem transmit speed (user download speed) in b/s.

Annex-Receive-Speed (Bay Networks VSA 51): This integer equals the modem receive speed (user upload speed) in b/s.

CLI IP Host Filtering - Corrected Information

The correct format for the values of the Bay Networks vendor-specific RADIUS attributes **Annex-Host-Restrict** and **Annex-Host-Allow** is **a.b.c.d n,n,n-n**, where **a.b.c.d** is the affected host's IP address and **n,n,n-n** is the list of affected ports on that host. The host's IP address and the list of ports must be separated by a single space. A "0" in any of the IP address fields matches any host on the corresponding subnet.

Remote Access Software Release 5.1 Corrections

SPR 10952

The calling number is included now in **erpcd** proxy RADIUS accounting messages.

SPR 10229

erpcd RADIUS class attributes now work with the Bay Networks Secure Access Control (BSAC) address pool.

SPR 10686

erpcd RADIUS now supports user names of up to 128 characters.

SPR 9824

The framed IP address is now included in the RADIUS accounting file.

SPR 9941

A PPP termination with data enqueued for output on a busy unit no longer causes mbuf corruption.

SPR 9937

The **stats -T** command now handles current PRM correctly.

SPR 9950

CCP BSD Compress now complies with RFC 1977.

SPR 9955

Handling of V.120 for dialback has been added.

SPR 8739

Port server connections show the username instead of “---” when the **who** command is executed.

SPR 9977

PPP termination with data enqueued for output on a busy box no longer causes mbuf corruption.

SPR 10210

DOS CR/LF handling functions only on non-macro entries; macro entries are treated as is.

SPR 9936

Log-in and log-out mechanisms are available for Annex web pages.

SPR 10137

The default port mode on all PRI products has changed from **cli** to **auto_adapt**.

SPR 10255

RIP updates should no longer stop on PPP interfaces.

SPR 9540

Annex printing no longer causes the Annex to panic.

SPR 10434

The **reset annex all** command now correctly updates modem type definitions in Annex memory, depending on the new list of session parameter blocks.

SPR 9991

The **rip_force_newrt** parameter allows you to tune the amount of time the RAS allows a primary router to send periodic RIP updates. If the RAS does not hear from the primary router within this timeout period, and a secondary router broadcasts a valid replacement route, the replacement route takes precedence regardless of the metric. The default state for this parameter is 0 (off), which disables the feature. The parameter can be set for 1 to 255 seconds (the real internal minimum is 5 seconds).

SPR 10483

The **answer_delay** keyword is available for SPBs. This keyword takes a single decimal argument in seconds. The keyword specifies the delay for answering the call to putting the modem or other resource (sync, TA) on the channel. The default value is 2 seconds for SPBs that set **call_action modem** when **call_action detect** is not in use for that call. The default is 0 for all other SPBs.

SPR 10457

USR 28.8 and 33.6 Sportster modems now work with the RA2000/4000 product line.

SPR 10568

The **pool** keyword in **acp_userinfo** now recognizes **ta**.

SPR 10494

Annex prompts are no longer displayed with CLI hooks.

SPR 10525

Autodetect mode now works for Trumpet and other PPP clients.

Changes to UNIX CLIs Release 14.1

This section describes changes to the UNIX command line interfaces for Release 14.1 of the Remote Annex operational code.

Known Problems/Limitations

- If you are using acp logging, you need to be certain that you have sufficient disk space available for log messages. If both the primary and secondary acp hosts run out of disk space, the unit will cache acp messages while it waits for space on the host to be freed. The unit will hang if it uses all of its storage space.
- In order to install the host tool sources for Linux and compile successfully, a preliminary step is required if you are running a release of Linux that includes the Linux 2.0 kernel (such as Redhat Linux or Slackware 3.1).

Under these releases of Linux, a bug in one of the system include files will prevent the remote access software from compiling successfully on your host, and must be repaired before the remote access software is installed.

To repair the file, follow these steps:

1. Edit the file **/usr/include/time.h**.
2. Go to line 121.
3. Change the first instance of the keyword "const" to "**__const**", as it is in all the other uses of the keyword in this file.

Line 121 as shipped:

```
extern int nanosleep __P((const struct timespec
    *__rqtp,
```

Line 121 after editing:

```
extern int nanosleep __P((__const struct timespec
    *__rqtp,
```

4. Save the file and exit the editor.
- The current alarm status for PRI/T1 isn't reported through SNMP.
 - V.terbo operation (a 19.2 Kb/s mode of operation similar to V.FC) may operate with some modems but is not supported with this release.
 - The ISDN TAs listed below are known to have compatibility problems running Multilink PPP with the RA 6300 and RA5393. However, running single-link PPP with these TAs on those models is supported:
 - Courier I-Modem (firmware version 2.1.4)
 - Zyxel2864I (firmware version 2.05)
 - When a voice call is placed to a unit (PRI) and no modems are available, the caller will get a ring-no-answer signal rather than a busy signal.

- If you are using a BitSurfer PRO, the BitSurfer Configuration Manager software does not set all the parameters necessary to make async PPP or MP connections. They must be set manually to the following:

```
AT&F&C1&D2\Q3%A2=95@M2=P@B0=1%A4=0
```

(put this in the **setup** string in your dialer).

Change **B0=1** to **B0=2** for 2-channel MP.

- In Release 14.1, TMS is not backward-compatible with the Release 14.0 database. You must run the convert utility in order to make the database compatible.
- Security does not work on the VCI type CLI.
- The UNIX installation script currently recognizes and installs software on many platforms other than those that are officially supported by this release. Please see the section [Supported Remote Access Hardware For Release 5.4](#) for the list of officially supported platforms.
- In some instances, AFD does not update the Microcom modem firmware properly. If this happens, use **admin** to issue the **modem all** command, then the **set modem busy_out n** command, and reboot the unit.
- When using the **cli** option from the Console monitor prompt to start a CLI session, always close the session (hang-up) and return to the Console monitor before rebooting or resetting the unit. Otherwise, it is possible to get the unit's Console monitor into an inaccessible state, which will then require the unit to be physically removed/reinserted in the 5000 hub. This is especially likely if the Hub Supervisory **Reset module** command is executed when a CLI session is left open from the Console monitor.

- IPX dialup addressing is completely rearranged when **address_origin** is set to **local** and the addresses are to be selected from the WAN; the remote addresses are set to 0.0.0.0. An example of the WAN setup follows (the format of the screen text has been altered slightly to fit the page):

```

WAN B/DS0 Channel Parameters

remote_address:
  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0

ipx_network:*
  a00000ab a00000b7 a00000c3 a00000cf
  a00000db a00000e7 a00000f3 a00000ff
  a000000b a0000017 a0000023 a000002f
  a000003b a0000047 a0000053 a000005f
  a000006b a0000077 a0000083 a000008f
  a000009b a00000a7 a00000b3 a00000bf

ipx_node:*
  00-00-00-00-00-aa 00-00-00-00-01-54 00-00-00-00-01-fe
  00-00-00-00-02-a8 00-00-00-00-03-52 00-00-00-00-03-fc
  00-00-00-00-04-a6 00-00-00-00-05-50 00-00-00-00-05-fa
  00-00-00-00-06-a4 00-00-00-00-07-4e 00-00-00-00-07-f8
  00-00-00-00-08-a2 00-00-00-00-09-4c 00-00-00-00-09-f6
  00-00-00-00-0a-a0 00-00-00-00-0b-4a 00-00-00-00-0b-f4
  00-00-00-00-0c-9e 00-00-00-00-0d-48 00-00-00-00-0d-f2
  00-00-00-00-0e-9c 00-00-00-00-0f-46 00-00-00-00-0f-f0

  THESE ARE THE NEGOTIATED ADDRESSES:

*** NCP (IPXCP) Status ***

Options          Local:          Remote:
Network No       a0              a0000083
Node No          00802d054ac4   000000000c9e
Compression      Telebit 15/ 0   Telebit 15/ 0
Routing Prot     RIP/SAP         None
Router Name      LM054AC4        None
  
```

SPR 10025

The UNIX installation can install the host tool sources on nonsupported UNIX platforms.

SPR 10269, 10270, 10271

Deficiencies in the help for the **admin** CLI.

SPR 10367

Compiling the UNIX host tools on Solaris 2.5 generates nonfatal compiler warnings.

SPR 10893

The Ascend RADIUS server does not authenticate SecurID users when it receives authentication requests from the embedded RADIUS client.

SPR 8482, 9901

SNMP does not report input or output frame or byte counts for the T1 and E1 interfaces.

SPR 10653

You cannot expire old passwords and enter new passwords using the Windows NT **erpcd** server.

SPR 10585

The Windows NT install shield appears to hang during server tool installation. Please be patient; it will complete the installation.

SPR 10037

The RA 6300 and RA 5393 support the **actcall/histcall** CLI commands, but not all modem information is available with those commands.

SPR 10380

If you boot a unit from another unit, issuing the **stats** command on the booted unit displays corrupted statistics.

Changes to Annex Manager Release 3.1

System Requirements

Annex Manager Release 3.1 runs on several popular UNIX systems. The following sections list the hardware and software requirements for installing and running Annex Manager.

For all systems, a minimum of 10MB of free disk space must be available prior to installation. A minimum of 32 MB of RAM is recommended, although specific memory requirements will vary, depending on the type of workstation and the other tasks that may be concurrent with Annex Manager. In all cases, a color monitor or X Windows terminal is recommended, although Annex Manager is usable with a monochrome X Windows terminal.

Sun Requirements

Annex Manager runs under Sun OS releases 4.1.3c and 4.1.4 and Solaris releases 2.4 and 2.5.1 on SPARC systems. The following patches are required for SunOS versions earlier than 4.1.3c:

- Patch number 100444-48 OpenWindows 3.0: OpenWindows V3.0 Server Patch 3000-86.

- Patch number 100492-01_09 OpenWindows 3.0: jumbo patch for olwm 3.0.

HP Requirements

Annex Manager runs under HP-UX 10.10 and 10.20 on HP 9000 Series 700 Workstations.

IBM Requirements

Annex Manager runs on IBM RS/6000 workstations under AIX 4.1.4 and 4.1.5.

Remote Display Requirements

If you use Annex Manager on an X Windows terminal, Bay Networks recommends that you have more than 2MB of RAM to avoid problems when you have multiple windows open simultaneously.

Known Problems/Limitations

The following items are problems and limitations of Annex Manager Release 3.1:

- If you select a PRI-supporting unit (RA 6300 or RA 5393) and you change the switch type, you should ignore the resulting error message:

```
<annex_name (node port 0)> anxt1CasDnisDigits :  
Parameter cannot be set: it does not exist or is read-  
only.  
There was an error setting one or more parameters.  
This may be due to a timeout.
```
- There is no online help available for the Reset options, which follow editing the configuration file. If you change the configuration file using Annex Manager, a dialog box appears with the various Reset options that you can select.

- Annex Manager will crash occasionally if you try to go into Setup mode when running SunOS 2.5.1.
- On AIX UNIX platforms, in the Setup>Security screen, the Security/Incoming On/Off buttons are misaligned with the text fields. This may be due to fonts not being installed on the system.
- Customize mode is not supported for this release.

Changes to Quick2Config Annex Release 3.1

System Requirements

- Hardware/software requirements - 80486 100MHz recommended
- Monitor - VGA or SVGA
- RAM - 8MB minimum; 16MB recommended for Windows 95; 32MB recommended for Windows NT
- Free space on hard drive - 6MB for Windows 95 and Windows NT
- Mouse - Microsoft compatible
- Communications stack - compatible with the standard TCP/IP stacks included with Windows NT and Windows 95

Known Problems/Limitations

The following items are problems and limitations of Quick2Config Annex Release 3.1:

- If you select a T1-supporting unit (RA 6100 or RA 5391) in the tree, then select the WAN Interface tab, you should ignore the resulting error message:

```
<annex name> 1.3.6.1.4.1.15.2.11.2.1.15.2 Error:MIB  
Variable doesn't exist
```

- You should ignore the following erroneous error message:
MSVCR_T40.dll can not be found
- PRI in and out statistics show no activity even though PRI has been in use.
- Clicking on the <http://www.baynetworks.com> URL in the World Wide Web help page brings up an error message.
- In the Basic Dial Access tab, if an inappropriate or out of range value is applied, a MIB error appears on the screen instead of an appropriate error message.
- If there is a device in the list that has become unreachable, selecting it can cause Quick2Config to crash occasionally. This happens rarely and randomly, and only if the device is unreachable and is in an unknown state.

Correction to Quick2Config Annex Release 3.1: SPR 9155

You can use Quick2Config Annex to set all valid combinations of PPP interface protocols.

Changes to the Network Administrator Utility (na) for Windows NT and Windows 95

Hardware/Software Requirements

You must use the following hardware and operating system version to use the **na** utility on Windows NT or Windows 95:

- Personal computer - 80486 100MHz recommended
- Monitor - VGA or SVGA
- RAM - 8MB minimum; 16MB recommended for Windows 95; 32MB recommended for Windows NT

- Free space on hard drive - 1MB
- Microsoft-compatible Mouse
- CD-ROM (required for initial installation)
- Windows 95, Windows NT 3.51, or Windows NT 4.0

Special Considerations

The **na** utility no longer requires that you have administrator privileges on an NT host to make changes to the unit's configuration. You should set the superuser password on the unit to prevent unauthorized access.

Changes to Remote Annex Server Tools for Windows NT R3.1

System Requirements

You will need the following to install and run Remote Annex Server Tools for Windows NT Release 3.1:

- A 486 or greater CPU with a minimum of 32MB of RAM, or a DEC Alpha CPU with a minimum of 32MB of RAM
- A server running Windows NT Version 4.0, configured to support TCP/IP
- Administrative privileges on the server
- At least 10MB of free disk space on an NTFS drive
- Four or more formatted 3.5 inch 1.44MB floppy disks, if you choose to create a set of installation diskettes
- A CD-ROM drive for installation of the software

Installing Windows NT Server Tools

The installation instructions for Windows NT Server Tools state that you must run the **setup.exe** file for both Windows NT 3.51 and 4.0. This is true only for Windows NT 3.51; if you are using Windows NT 4.0, the **setup.exe** file will run automatically.

Manually Removing Remote Annex Server Tools for Windows NT

Presently, there is no uninstall program included in this release. You will have to manually remove the program and files if you want to uninstall them. Use the following procedure to remove the program:

1. **Go to the** Control Panel > Services **and stop Annex** erpcd, Annex syslogd, **and** Annex timed.
2. **Start the registry editor:**
 - a) For **Windows NT 3.51**, you can find the registry in **\windows_install_dir\system32\regedt32.exe**. Remove the following keys:

HKEY_LOCAL_MACHINE (on the local machine)

SOFTWARE

Bay Networks

Remote Annex Server Tools (and all subkeys)

HKEY_LOCAL_MACHINE (on the local machine)

SOFTWARE

RAPProduct

HKEY_LOCAL_MACHINE (on the local machine)

SYSTEM

CurrentControlSet

Services

erpcds, syslogd, timed (three separate keys)

HKEY_LOCAL_MACHINE (on the local machine)

SYSTEM

CurrentControlSet

Services

EventLog

Application

ANNEX syslog, Annex_ACP, Annex_syslog (three separate keys)

HKEY_LOCAL_MACHINE (on the local machine)

SOFTWARE

PROGRAM GROUPS

Bay Networks (To avoid removing Q2CAnnex or NA icons, go to the group and delete the icons for the Remote Annex Server Tools for Windows NT)

b) For **Windows NT 4.0**, you can find the registry file in **\windows_install_dir\regedt.exe**. Remove the following keys:

HKEY_LOCAL_MACHINE (on the local machine)

SOFTWARE

Bay Networks

Remote Annex Server Tools (and all subkeys)

HKEY_LOCAL_MACHINE (on the local machine)

SOFTWARE

RAProduct

HKEY_LOCAL_MACHINE (on the local machine)

SYSTEM

CurrentControlSet

Services

erpcds, syslogd, timed (three separate keys)

HKEY_LOCAL_MACHINE (on the local machine)

SYSTEM

CurrentControlSet

Services

EventLog

Application

ANNEX syslog, Annex_ACP, Annex_syslog (three separate keys)

Go to Settings > Taskbar > Start Menu Programs > Advanced and delete the Bay Networks Remote Annex programs.

3. Go to the File Manager or Explorer and delete the following files/directories:

Delete the installation directory **c:WIN32APP\BayNet\RAnnex** and its files.

Delete the installation backup directory **c:WIN32APP\BayNet\RAnnex.bak** and its files.

Delete the directory **c:\bfs** and its files.

Delete the directory **c:\etc** and its files.

4. Reboot the system.

Known Problems/Limitations

- You should halt all **erpcd** processes running in debug mode prior to installing Remote Annex Server Tools for Windows NT.
- Installing Remote Annex Server Tools for Windows NT on a system that has **erpcd** running causes the following error:

An application error has occurred and an application log is being opened erpcd.exe

Exception: access violation (0xc0000005), Address: 0x004152276

- In order to run the **erpcd** authentication function under debug mode, you need special privileges. Use “Act as operation system” from the Windows NT user manager to resolve the problem.
- You must use care when transferring **acp_files**, etc. from UNIX hosts to Windows NT hosts, because the end-of-line characters are different. To avoid this problem, use a utility such as **unix2dos** (available on the World Wide Web).
- Remote Annex Server Tools for Windows NT do not support the following UNIX utilities:
 - **aprint** - the Remote Annex printer utility
 - **ch_passwd** - the Remote Annex user password change utility
 - **ien116d** - the IEN-116 name server
 - **rtelnet** - remote telnet
- This release of the Remote Annex Server Tools for Windows NT supports up to two units booting or dumping from/to a server simultaneously and up to 10 user login requests per minute per server.
- Remote Annex Server Tools for Windows NT R3.1 does not allow the **config.annex** file to be correctly uploaded to the unit during booting. A workaround for this problem is to use **ftp** to put the **config.annex** file on the EEPROM on the Annex and set the **load_dump_seq** to **net,self**.
- Occasionally, installation will not be able to shut down the Annex time service in an existing installation of the Remote Annex Server Tools for Windows NT R3.1. This is exhibited by a long pause before the file copying process starts and an error message in writing the registry after files are copied. The installation fails. One workaround is to reinstall. The second install succeeds. A second option is to use control panel services to shut down the Annex processes manually and then install.

- During the installation of Remote Annex Server Tools on Windows NT 4.0, the install shield appears to hang. The wizard asks you twice for the appropriate geographic location, and when you click the “Next” button, the application appears to hang, not responding to mouse-clicks or keystrokes. After a few minutes, the installation process proceeds normally.

24-Hour Unit Replacement Service

This service is named “Next Day With Labor - BJ 2300.” You must follow the procedures in this section in order for the Next Day With Labor Service Agreement to be honored.

Saving the Unit Configuration

When you have finished configuring your unit, Bay Networks recommends that you save your configuration to a host file. This ensures that you will have the configuration at your disposal in the event that the configuration file becomes damaged in any way, or otherwise needs to be replaced. Keeping a backup of the configuration file greatly simplifies the reconfiguration process, should you need to do it.

This procedure guides you through saving the configuration using the **na** utility. By default, **na** is installed in the **/usr/annex** directory for UNIX and in the **win32app\Annex** directory for Windows NT. You can change this location from its default during the installation process. Supported platforms and requirements are listed in [Known Problems/Limitations](#) on page 34.



Passwords and option keys are not saved when you save the configuration file using the **na write** command. These values must be restored individually if the unit is replaced or the configuration is changed or erased.

On a UNIX host, you can start **na** by typing **./na** from the directory in which you installed **na**. On a Windows NT host, you can either double-click on the **na** icon or use File Manager and click on **na.exe**.



You must have root permission on the host.

To save a unit's configuration:

1. At the command prompt, issue this command:

```
command: annex <IP address>
```

This identifies the unit to which you will issue subsequent commands.



The next prompt might not be a command prompt. You will be prompted for a password if one is specified for the unit.

2. You now see the unit IP address, the unit type, and the version of code that it is running. To save the configuration to a file: for UNIX:

```
command: write <IP address> <filename.param>
```

for Windows NT):

```
command: write <IP address> <filename.txt>
```

This creates a file with a file name you specify. It places this file in the same directory from which you are running **na**. The file name should identify the unit for which you are saving the configuration.

The **write** command for Windows NT works the same as the UNIX **write** command, but it puts the file in a form that Notepad can read.

3. To exit the utility, enter:

```
quit
```

The following is a typical login procedure prompting you for a password (on Windows NT, only the first line is different):

```
# /usr/annex/na
command: Annex 192.32.30.49
Password for 192.32.30.49 <unknown>: abc
192.32.30.49: Micro-Annex-UX R11.1, 8 async ports
```

```
command: write 192.32.30.49 annex.param
command: quit
```

Excerpts from a sample **annex.param** file follow:

```
# Annex 192.32.30.49
echo setting Annex parameters
set annex subnet_mask 255.255.255.0
set annex pref_load_addr 192.32.30.30
set annex pref_dump_addr 192.32.30.30
set annex load_broadcast N
set annex broadcast_addr 192.32.30.255
set annex load_dump_gateway 0.0.0.0
set annex load_dump_sequence net,self
set annex image_name "oper.56.enet "
set annex motd_file "motd"
set annex config_file "config.Annex"
set annex authoritative_agent Y
set annex routed Y
set annex server_capability none
set annex disabled_modules atalk,ipx,vci
set annex tftp_load_dir "10.0 //"
set annex tftp_dump_name ""
set annex ipencap_type ethernet
set annex ip_forward_broadcast N
.
.
.
echo setting parameters for interface asy8
set interface=asy8 rip_send_version compatibility
set interface=asy8 rip_rcv_version both
set interface=asy8 rip_horizon poison
set interface=asy8 rip_default_route off
set interface=asy8 rip_next_hop needed
set interface=asy8 rip_sub_advertise Y
set interface=asy8 rip_sub_accept Y
set interface=asy8 rip_advertise all
set interface=asy8 rip_accept all
```

You may want to create a backup directory elsewhere and copy this file into that directory. This ensures that there is no chance of the file being corrupted or otherwise changed when you upgrade the unit.

Restoring the Unit Configuration

This process is necessary for restoring a configuration to a unit.

Placing the File onto the Unit

If you have previously saved a unit configuration in a file on a UNIX or Windows NT host, you can use that file to configure a new unit.



The new unit must have an IP address assigned to it already. See [Using monitor Mode to Provide an IP Address for a New Unit](#) on page 53 for basic instructions on booting a unit. Complete instructions are in the hardware installation manual for your unit.

Also, passwords and keys are not saved, and must be restored individually.

If you plan to edit the configuration file that you are going to place on another unit, copy the file and rename it before you start making changes. Pay special attention to unit-specific parameters such as **local_address** and **remote_address**.

On a UNIX host, you can start **na** by entering **./na** from the directory in which you installed **na**. On a Windows NT host, you can either double-click on the **na** icon or use File Manager and click on **na.exe**.



You must have root permission on the host.

To restore a unit's configuration:

1. **At the command prompt, enter the following:**

command: **annex** <IP address*>

This identifies which unit you want for subsequent commands.

2. **(For UNIX)** command: **read** <filename.param >
(For Windows NT) command: **read** <filename.txt>

This copies the **filename.param** file to the unit that you specified and changes the parameters to ones specified in the file.

3. command: **quit**

This exits **na**.



The script file does not contain the IP address of the unit; this allows you to transfer the file from one unit to another. However, you must be careful if you have specified IP addresses specified for the ports; they will be copied to the new unit. Remember that you cannot have the same IP addresses across different units; IP addresses must be unique.

The following is a sample of **login** and **read** commands on a UNIX host (on Windows NT, only the first line is different):

```

#/usr/annex/na
command: Annex 192.32.30.49
Password for 192.32.30.49 <unknown>: abd
192.32.30.49: Micro-Annex-UX R11.1, 8 async ports
command: read annex.param
setting annex parameters
setting parameters for async port 1
setting parameters for async port 2
setting parameters for async port 3
setting parameters for async port 4
setting parameters for async port 5
setting parameters for async port 6
setting parameters for async port 7
setting parameters for async port 8
setting parameters for interface en0
setting parameters for interface asy1

```

```
setting parameters for interface asy2
setting parameters for interface asy3
setting parameters for interface asy4
setting parameters for interface asy5
setting parameters for interface asy6
setting parameters for interface asy7
setting parameters for interface asy8
command: quit
```

Using monitor Mode to Provide an IP Address for a New Unit

If you are configuring a new unit, you must use the monitor prompt to assign an IP address to the unit. You need the following equipment to do this:

- A terminal (VT100, laptop, etc.).
- A straight-through RJ45 cable.
- A console terminal adapter. If you are using a laptop, you typically need a DB25 to DB9 converter, straight-through.

To assign an IP address to a unit:

1. **Insert the RJ45 connector in the console port of the unit.**
2. **Set your terminal to the following settings:** 9600 baud, 8 data, 1 stop, no parity, **and** XON/XOFF.
3. **Insert the other end of the RJ45 connector into the console adapter and connect the console adapter to your laptop.**
4. **Turn on the unit.**
5. **As soon as the unit powers up, all of the LEDs come on; wait for any one of the LEDs to go out, then press the Test button.**
6. **Wait approximately one to two minutes and press the <Return> key. The monitor prompt resumes.**
7. **At the monitor prompt you can start setting the IP address and the initial configuration parameters. Enter `addr` to make these initial configuration settings.**

8. **Check the boot sequence by typing seq. Since you are booting from the network, set it to net,self. self can be set only if the option was purchased for that particular unit.**
9. **Check the image to make sure that it is the correct operational image. Enter image to verify this.**
10. **Enter boot, then press <Return> to boot the unit. A steady stream of dots appears on the screen and eventually ends at the eof.**
11. **At the eof, press <Return> to access the console monitor or annex: prompt, depending on the type of unit you are working with.**
12. **Use na to configure the unit.**