Nortel Networks 5399 and 8000 Access Switch Version 8.0 Software Release Notes

NORTEL NETWORKS™

Nortel Networks NA 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 NORTEL 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. Nortel Networks NA Inc. ("Nortel 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 Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA 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. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel 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 Nortel 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 Nortel 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. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel 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 Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel 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. Nortel Networks will replace defective media at no charge if it is returned to Nortel 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. Nortel 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. Nortel 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 Nortel 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 NORTEL 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 NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL 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 Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel 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 Nortel Networks the Software, user manuals, and all copies. Nortel 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 Nortel Networks, 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 NORTEL 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 NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Nortel Networks 5399 and 8000 Access Switch Version 8.0 Release Notes

These release notes apply to Version 8.0 of the Nortel Networks 5399 and 8000 Access Switch (formerly known as Model 8000 and Model 5399 Remote Access Concentrator (RAC)) software, which contains the following software releases:

- Remote Access Concentrator Operational Code Version R17.0

- DSP Digital Modem Code Version R3_56_56

    -- V.34/x2: Vx_00_56

    -- K56flex: Vk_00_56

- Host Tools for UNIX Version R17.0

- Server Tools for Windows NT R6.0.

➡ **Note:** Whenever the term Remote Access Concentrator (RAC) appears in this document, it refers to the Nortel Networks 5399 or 8000 Access Switch.

Disregard any IP Pooling information contained in the Access Switch product documentation. This information is out of date. For more information, see "IP Pooling Documentation"on page 31.

Version 8.0 does not support NFAS parameters and switches related to NFAS.

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

These release notes address the following topics:

- Supported remote access hardware

- Supported software and switch types

- New features in Version 8.0

- V.90 support in Version 8.0

- Known anomalies

- Bug fixes

- Modem support

- Acquiring software upgrades

- 24-hour unit replacement service

Supported Remote Access Hardware

Version 8.0 supports the Nortel Networks 5399 and 8000 Access Switches.

Supported Operating Systems

Binary files and source code are provided on the distribution media for each of the following operating systems except for Microsoft Windows NT.

- HP-UX 11.0

- HP-UX 10.20

- IBM RS/6000 AIX 4.2

- IBM RS/6000 AIX 4.3

- Microsoft Windows NT 4.0 for Intel (PDC/BDC Only)

- Red Hat LINUX 5.2, 2.0.36 kernel

- Solaris 2.6

- Solaris 7

Supported Compiler Versions

Version 8.0 supports the following compiler versions:

- Solaris 2.6: Workshop Compilers 4.2
- HP-UX 10.20: HP C Compiler (bundled)
- Red Hat Linux 5.2, 2.0.36 kernel: gcc version 2.7.2.3
- IBM RS/6000 AIX 4.3 AIX Compiler V3.1

RADIUS Server Information

The embedded RADIUS client in Remote Access Software Version 8.0 is known to be compatible with the following RADIUS servers:

- Any shipping BaySecure Access Control (BSAC) server
- Livingston 2.1
- USR 5.07
- Ascend 971222
- Merit RADIUS 3.6B
- SafeWord 4.

➡️ **Note:** As of Version 8.0, RADIUS Authentication Proxy via ERPCD/ACP is no longer supported.

SecurID/ACE Compatibility Information

5399 and 8000 Access Switch Software Version 80 is compatible with the SecurID/ACE Server Version 3.1.2.

SafeWord Compatibility Information

Remote Access Software Version 8.0 operates with Version 4.4 of the SafeWord server, and is compatible with Version 4.4 of the SafeWord UNIX client. There is no support for Windows NT.

Supported Switch Types

Table 1 lists the PRI switch types supported in Version 8.0.

Table 1.   PRI switch_type Values

Protocol	switch_type	Used In
T1/PRI	AT9 AT4 DMS NI2	North America; AT&T 5ESS#9 switch North America; AT&T 4ESS support North America; Nortel DMS100 switch North America; supports National ISDN2
E1/PRI	ETS ETS-NCRC4 ISR AU1 DGT SNG MTT MKT	Europe; ETSI Europe; ETSI without CRC Israel Australia Taiwan Singapore Japan Hong Kong

Table 2 lists the CAS switch types supported in Version 8.0.

Table 2.   CAS switch_type Values

Protocol	switch_type	Used In
Channelized T1	UST1 UST1FC UST1FD HKT1	North America North America - Feature Group C North America - Feature Group D Hong Kong
Channelized T1 - R1	TWT1R1	Taiwan
Channelized E1 - P7	SWE1P7	Sweden

(continued)

Table 2.   **CAS switch_type Values (continued)**

Protocol	switch_type	Used In
Channelized E1 - R2	ANE1R2	St.Martin
	ARE1R2	Argentina
	BBE1R2	CCITT BlueBookR2 (used in most of Europe); also used in Croatia, Chile, and South Africa
	BRE1R2	Brazil
	BR2E1R2	Brazil
	INE1R2-1	India
	INE1R2-2	India
	INE1R2-3	India
	INE1R2-4	India
	MOEIR2	Macao
	CNE1R2	China
	KRE1R2- 1	Korea
	KRE1R2- 2	Korea
	IDE1R2	Indonesia
	ILE1R2	Israel
	NZE1R2	New Zealand
	PHE1R2	The Philippines
	MYE1R2	Malaysia
	MXE1R2	Mexico
	THE1R2	Thailand
Channelized E1 - R2	TRE1R2	Turkey

New Features in Version 8.0

Version 8.0 introduces the following new features:

- Network Time Protocol

- Dual IP Address

- Multiple Security Levels

- Filtering Enhancements

- SNMP Additions

- 5399/8000 Support for CVX Policy Manager (CPM)

- Default Auto-detect Mode

- Calling Number Wildcarding in Session Parameter Blocks (SPBs)

- BayDVS Multilink Accounting

- Extensions to Framed-IP-Address RADIUS Accounting

- RADIUS Port Encoding Additions

- Persistent RADIUS Server

- Modem Call Quality Statistics in RADIUS

- IP Address Pooling.

➡ **Note:** Version 8.0 does not support NFAS parameters and switches related to NFAS.

Network Time Protocol (NTP)

Network Time Protocol (NTP), as defined in IETF RFC 1305, provides a mechanism to synchronize time on computers across an IP network.

Dual IP Addresses

This feature allows the 5399/8000 to assign up to two different source IP addresses to different types of packets.

Multiple Security Levels

Multiple security levels are now configurable on the 5399/8000. The "operator user" is a level with password protection and is above the user. You enter the operator mode from the user level by giving the command **operator**. From here, the operator user executes commands from the operator command set. Most of the commands gather available statistics on the RAC. Use the operator command at the operator prompt (annex%) to leave the operator mode and return to the RAC. The operator password is controlled at the superuser level with the CLI command (**oppasswd**).

SNMP Additions

Two additional SNMP traps are now supported on the 5399/8000 platforms. The first trap will be sent every time the blade boots up. It contains the code versions for the embedded image, the modem image and the wan image. The second trap will be sent when it is detected that the wan port is down (does not respond to commands).

5399/8000 Support for CVX Policy Manager (CPM)

CPM is a server-based product that facilitates the deployment and execution of multiple services in a remote access infrastructure. The 5399/8000 will inter-operate with CPM.

Default Auto-detect Mode

There are PPP clients that are entirely passive, and wait for the 5399/8000 to initiate PPP. In software releases prior to Version 8.0, the auto-detect process will time out after a configurable number of seconds (default 30), and drop into cli mode, which will fail to establish a PPP connection with these passive clients. In Version 8.0, a new port parameter, default_autodetect_mode, which will control the action of the auto-detect process after the timeout has expired, has been added. This parameter has two possible values: cli or ppp. The default value is cli, which makes the code behave as it currently does. If the value is sets to ppp, the auto-detect process will switch to ppp if the timeout expires.

Calling Number Wildcarding in Session Parameter Blocks (SPBs)

SPBs now allow wildcarding in the calling number processing. Two special characters have been added to the SPB syntax as follows:

? matches any single character

@ matches zero or more characters until end of string

For example, if a Service Provider is able to bill any numbers which start with 01,then the following SPB could be used:

```
Begin_session 01
  calling_no 01@
End_session

Begin_session no_cli
  Calling_no @
  Call_action drop
End_session
```

Alternatively, if all numbers can be billed, but subscribers have the ability to withhold the calling number information, then the following SPB could be used:

```
Begin_session with_cli
  calling_no ?@
End_session

Begin_session no_cli
  Calling_no @
  Call_action drop
End_session
```

BayDVS Multilink Accounting

BayDVS now sends RADIUS Accounting records to the remote RADIUS server for each link of a multilink call.

Extensions to Framed-IP-Address RADIUS Accounting

The Framed-IP-Address is now reported in a RADIUS START accounting message for MP calls.

RADIUS Port Encoding Addition

A new annex security parameter, radius_port_encoding, has been added. This annex parameter specifies the format used to report the RADIUS accounting information to the RADIUS server. Valid values are device and channel. The default is device. When set to channel, both the port number and the wan/channel are sent in the Access Request/Accounting Request packet for every call. When set to device, this parameter displays the number of the port.

Persistent Radius Server

A new annex parameter, persistent_primary_server, modifies the Access Switch so that it will always send every packet to a user-designated primary RADIUS server first. If no response is received from the primary server, the packet is then sent to a user-designated secondary server. The values are Y and N. The default is N.

When the value is set to Y, the Access Switch always looks for the primary server first and sends packets to it. Even if the primary server does not respond, all subsequent packets are sent to the primary server and then to the secondary server. When set to N, the Access Switch sends all received packets to the user-designated primary RADIUS server first. If no response is received from the primary server, the packet is then sent to a user-designated secondary server. All subsequent packets are sent to the secondary server.

Modem Call Quality Statistics in Radius

Several VSAs that relate to the assessment of Modem Call Quality have been added to RADIUS accounting.

IP Address Pooling

This feature allows the 5399/8000 to store IP addresses locally where it can function as an IP address "server" for the rest of the chassis or for a series of 8000s located on a single subnet.

Documentation for IP Address Pooling may be found on Nortel Networks World Wide Web page at *http://support.baynetworks.com/Library/tpubs*.

V.90 Support in Version 8.0

The following sections summarizes the numerous improvements made to the BayDSP digital modem code in Version R3_56_56.

V.90 Dial-Out Feature

This feature enhancement permits the 5399 to originate a call to a client Analog modem and establish an asymmetrical V.34-V.90 connection with the remote modem. By design, originating calls to remote access server digital modems will establish an asymmetrical V.34-V.34 connection.

The feature addition has no impact on the typical Service Provider environment in which the remote modem is originating calls to the concentrator.

Phase 2 Handshake Algorithms

Changes were made to Phase 2 to improve dial-out connectivity with certain client modem types by influencing their transmit power levels. The digital modem may now signal the client to reduce its transmit power level. Not all client modems implement this feature, and therefore the improved performance may or may not be visible to customers that use the V.34 or V.90 dial-out feature.

Phase 3 Handshake Algorithms

Changes were made to Phase 3 to increase the retrain timeout from 5.1 to 6 seconds. This improvement was incorporated to accommodate increased V.90 connectivity on extreme local loop conditions (EIA Loop 6) with certain client modem types (3Com/USR 56K Fax/modem, for example) that require additional time during this phase of t7he handshake before falling back to V.34.

This increase in the timeout period is beyond the requirements of the V.90 recommendation; however, no negative repercussions have been observed with other V.90 modems.

Additional Call Statistics

Call statistics have been enhanced and now include received signal quality measurements in Phase 3 and 4 of handshake, a trace of the most recent six pump states, and the residual echo level in V.90, x2, K56Flex, V.34, and V.32 modes. In addition, the pump states reported to 5399 Host have been expanded. These additional statistics have no effect on performance or operations, but will be of use in engineering debug activities.

V.34 Performance

General, on-going improvements were implemented in V.34 mode that should improve connectivity with older-generation V.34 consumer modems. The incremental gain may not be visible to the customer.

V.90 Performance

Previously, the upstream speed on V.90 calls (Vx-code variant only) was limited to 28.8 Kbps by design. This maximum rate has now been extended to 31.2 Kbps; however, achieving 31.2 Kbps in the upstream direction is contingent upon suitable line conditions.

V.42 Performance

Improvements in V.42 detection were added to accommodate network conditions that trigger certain client modems to initiate rate renegotiation requests immediately following data mode establishment. Expected results are increased successful V.42 negotiations with IBM Thinkpad internal modems under these conditions.

Other

Changes to μ-Law compression rounding and to V.34 pre-emphasis filter rounding were incorporated. These changes were housekeeping in nature, and have no effect whatever on digital modem code performance. An additional safeguard was implemented to improve the host to BayDSP 'Ready'-state communications.

Known Anomalies

This section describes known anomalies in Version 8.0.

PPP Callback Feature

The PPP callback feature does not function under the following condition. A PPP dial-in client negotiates MutiLink (MP) and Callback (CBCP) and logs in as a tunnel user (either a Bay DVS tunnel user or a L2TP tunnel user). When all three conditions exist, the RAS disconnects the PPP dial-in client. The syslog reports the following messages:

```
terminating: Success
No such device
```

NSF Support

Currently NSF is supported only on the 5ESS switch. On other switch types, dialout calls will fail with the following message:

```
calling wan 1 b channel disconnecting 96: mandatory information
element missing handle 1: dial_request state.
```

V.90

The BayDSP V.90 digital modem technology has been extensively tested with all popular V.90, x2, K56flex, and V.34 client modems. The V.90 implementation is subject to some interpretation differences during the coding process by the variety of organizations that are releasing products for the client modem user.

Consequently, incompatibilities exist between the central site V.90 modem releases and certain client modem implementations, as follows:

- V.FC (Fast Class) modems are not supported by BayDSP digital modems.

- The version of BayDSP Digital Modem code included in this release does not support MNP modems. As most other modem types do, the BayDSP modem supports the more robust ITU-T V.42 and V.42bis recommendations. If the originating modem supports only MNP, the connection will be made in a non-error-correcting mode.

- V.32terbo operation (a 19.2 Kb/s mode of operation similar to V.FC) may operate with some modems but is not supported in this release.

- The version of BayDSP Digital Modem code included in this release supports speeds from 2400 (V.22bis) up to 33.6 Kb/s (V.34 with extended rates). Support for 300 b/s (Bell 103) and 1200 b/s (Bell 212A) may be added to a future release.

- The following modems are known to exhibit connection reliability problems with the BayDSP Digital Modems:

  -- AT&T Paradyne Comsphere 3810

  -- AT&T Paradyne 3740-A1-201

  -- Motorola Codex 3261

  -- UDS V.3225

  -- Racal V.34 models 3292 and 3264

  -- RCV56DPF-PLL L8571A Rev 33.00/33.00

  -- Motorola PCI SM56 softmodem

Ongoing client modem flash upgrades resolve many of these issues; however, the following chipsets/client modems have been found to exhibit limited compatibility with the BayDSP V.90 modem implementation.

ESS x2 Chipset

The ESS x2 chipset previously had a bug that affected transmission and detection of the x2 signature within the handshake. Consequently, connections with the BayDSP modem would fall back to V.34 mode. ESS has since fixed the x2 signature requirements; however, not all manufacturers that use the ESS chipset have not incorporated these changes in their client modem releases. One client modem in this category is the Netcom ESS56K.

Cirrus Logic Chipset

The Cirrus Logic chipset previously had a bug affecting x2 training sequence timings. Consequently, connections with the BayDSP modem would fall back to V.34 mode. Cirrus Logic has since fixed this problem; however, not all manufacturers that use the Cirrus Logic chipset may have incorporated these changes in their client modem releases. Client modem manufacturers who use the Cirrus Logic chipset in some of their modem models are Digicom, GVC, Atlas, and Zoltrix.

Racal ALM 3239

The Racal ALM 3239 modem does not connect with the BayDSP modem. During the handshake sequence, INFO sequences are incompatible between the 3239 and the BayDSP digital modem. Consequently, the handshake sequence does not progress to data mode and the modems disconnect the line. It is very important that the client modem user check the client modem manufacturer's Web site for any upgrades that may be available. A good site for links to client modem manufacturers is *http://modems.rosenet.net/*.

SecurID Version 3.1.2 Support

When using SecurID version 3.1.2, whether as an ACE proxy server or as a primary RADIUS server, you need to set the following parameters.

If using SecurID as a primary RADIUS server:

```
radius_retries 6
radius_auth_timeout 5
```

If using SecurID proxied from another RADIUS server:

```
radius_retries 4
radius_auth_timeout 8
```

These values may seem high, but the authentication engine in the SecurID server takes longer than a regular security server to process login information, especially if there are many checklist attributes.

Also, SecurID Version 3.1.2 does NOT perform RADIUS Accounting properly, and it is recommended that a separate accounting server be configured if SecurID will be the primary RADIUS server.

Insufficient Contiguous Memory

If an insufficient contiguous memory to reload modem code message appears in the syslog file, you must reboot the 5399 or 8000 RAC to load new modem code.

DMS 100

If your switch type is a DMS 100 and one of your WAN interfaces is set to switch_type disable, upon rebooting, the CO returns busy to all inbound calls. The RAC is therefore unavailable for use. Manually resetting the WAN modules brings the WANs back online. Or, you can change the switch type from disable to a valid switch type. The WAN reports a red alarm, but other WANs will come out of yellow alarm.

Australian DSP Configuration

For Australian users, please make the following changes to the %digital_modem section of the *config.annex* file:

```
config_bytes 25=128 config_bytes 24=12
```

Rtelnet

There is no rtelnet support for Linux.

Switch Types

Unconfigured switch types will default to AT9 for E1 PRI.

NA

The system administrator cannot set remote_address, IPX_network, and IPX_node in the same command string. The command format used is parameter_name value <increment>. Since the increment is an optional number, it is impossible to tell whether there will be one or two tokens following a parameter name. Therefore, these three parameters need to be the last or only parameters on any one command line.

Setting the ipx_network WAN Parameter

Setting the ipx_network WAN parameters by **admin** switches the digits on wan2. For example, set the following using the **admin** command:

```
set wan=all b=all ipx_network 00000001
```

The command output is as follows:

For wan 1:

```
ipx_network:*00000001 00000002 00000003 00000004

00000005 00000006 00000007 00000008
00000009 0000000a 0000000b 0000000c
0000000d 0000000e 0000000f 00000010
11000000 12000000 13000000 14000000
00000015 00000016 00000017
```

For wan 2:

```
ipx_network:*01000000 02000000 03000000 04000000

05000000 06000000 07000000 08000000
09000000 0a000000 0b000000 0c000000
0d000000 0e000000 0f000000 10000000
11000000 12000000 13000000 14000000
15000000 16000000 17000000
```

To work around this problem, set the ipx_network parameters for each WAN (for example, wan=1 or wan=2).

Versalar Dialout Client (VDC)

The VDC does not work with any Windows NT program that requires a dialer. This includes dial-up networking under Windows NT, Compuserve, and AOL. The modem does connect with the remote end, but the dialers under Windows NT do not recognize this. However, you can use telnet to access the rotary and make manual dialout calls to a BBS using AT commands. Note that VDC is a separate product that works with Version 8.0. A workaround is available in the form of a new .inf file. This file is available at:

ftp://ftp-support.baynetworks.com/outgoing/RA/

The file is called:

mdmnortel.inf.

Use this file instead of the standard windows modem file in the VDC modem setup.

Using Local RADIUS Security

The RAC does not use the Authentication server address in the TMS entry for authentication. It uses the address that is configured on the RAC.

netstat -IP

The **netstat -IP** command may provide misleading information for L2TP tunnels. PPP is not terminated on the annex and this information may be incorrect. The **netstat -IP** command displays last received and last sent before final establishment.

netstat -i

The **netstat -i** command output should list tunnels as VPN-tunnel, not DVS tunnel, for a l2tp connection. For example:

```
Annex# n -i

Name Mtu Network Address Ipkts Ierrs Opkts Oerrs
Collis
en0 1500 132.245.81 132.245.81 1606251 0 1295865 2 0
en0 1500 0 - 65534 65394.157 1606251 0 1295865 2 0
lo0 1536 127 127 0 0 0 0 0
syn63 1524 DVS-tunnel DVS-tunnel 5 1 586856 0 0
syn50 1524 DVS-tunnel DVS-tunnel 4 0 586659 0 0
en0 576 00000000 0000000000001665370 0 1299446 2 0
```

Bug Fixes

The bugs in this section have been fixed in Version 8.0.

CR 111740

The annex parameter 'timezone_minuteswest' can now be set to a value less than -720.

CR 98415

The dialback feature of ACP now works correctly with ISDN terminal adapters.

CR 101927

CBCP no longer syslogs erroneous entries when callback fails.

CR 103568

The Radius Annex-Host-Restrict attribute no longer allows telnet to the restricted host during dialup.

CR 106230

Telnetting to an Annex with filters installed now functions properly.

CR 108069

A security issue with BayDVS tunnels and telnet has been corrected.

CR 108705

The anxt1BusiedOutChannels MIB now correctly reports the number of busiedout channels.

CR 108706

The anxt1TotalChannel MIB now correctly reports the number of active WANS.

CR 109083

An SNMP walk (getnext) from anxt1Total is now working properly.

CR 109519

The MIB object, callHistWANUnitNumber, within the callHistTable (xylo-callmgt.mib) is now returning the correct values.

CR 109960

Transparent telnet now functions correctly.

CR 95667 and CR 101469

Fixed a problem with interrupts which caused 5399s to stop responding to inbound network traffic, such as pings and finger commands.

CR 101180

The anxt1ChanState MIB now correctly provides a value of 1 (available), 2 (busied-out), or 3 (auto-busied-out).

CR 101182

The anxt1ChanState MIB no longer erroneously indicates a channel is busied-out.

CRS 102926 and CR 103855

TCP Clear functionality has been added for normal and pre-auth users. This was done by adding the Radius Attribute, Login-Service, value TCP Clear.

CR 103909

A security problem, which allowed CHAP authentication when the Radius Security Server was not in service, has been fixed.

CRS 104687, 105440,105452 and 106581

A problem with activated dialout routes not being properly installed or removed from the Annexes routing table has been resolved.

CR 105459

Dialout routes now properly send RIP routes when variable subnet masks are used in the dialout definition.

CR 105689

Actcall/histcall no longer display 'Diagnostic Disconnect Code nn' in the Begin(end) Rx speed record.

CRS 105962 and 104247

MMP calls no longer fail to authenticate on a busy network.

CR 106119

A problem in DHCP that caused terminated calls to display in the **who** command and resulted in the modem still being allocated has been resolved.

CR 106516

The cli wan busyout command now functions properly.

CR 107162

Dialout routes are no longer poisoned on Annexes configured for wan type UST1.

CR 88674

Nokia Cellular PCMCIA cards will now properly run PPP over V.110.

CR 92611

MP connections no longer fail if the Annex parameter mmp_enabled is set to Y and the port parameters mp_endpoint_address and mp_endpoint_class are set to the default values.

CR 92660

The Annex's CallBack Control Protocol (CBCP) implementation is now RFC (Draft) Compliant. Now when a user hits <Esc> or otherwise cancels out of the Callback Number dialog box, the call will proceed as a normal PPP call.

CR 92880

A problem in DHCP that caused terminated calls to display in the **who** command and resulted in the modem still being allocated has been resolved.

CR 95679

MMP connections now log the RADIUS Accounting attributes Called-Station-ID and Calling-Station-ID.

CR 96838

When a RADIUS user configured with a Service-Type of Callback-Login and a Login-Service of Telnet issue the **logout** command, the user is now disconnected rather than dropped to a CLI prompt.

CR 97183

Outbound connections are no longer allowed when the port parameter Mode is set to **auto_detect**.

CR 100103

The Annex now properly sends Connect-Info to Radius for both sync and async calls.

CR 101068

When ATCP is negotiated, the Annex now properly sees AppleTalk Zones and Servers.

CR 101497

The Modem Disconnect Reasons as displayed in the **histcall** command have been updated to be more descriptive of the actual end-user condition. Table 3 shows the new values.

Table 3.   Histcall Command Modem Disconnect Reasons

EXISTING DEFINITIONS	ENHANCED DEFINITIONS
Unknown	Undetermined Disconnect Reason
Local Host Disconnect	Disconnect Command Rec'd From Host

(continued)

Table 3.   Histcall Command Modem Disconnect Reasons (continued)

EXISTING DEFINITIONS	ENHANCED DEFINITIONS
CD Timer Expired	No Carrier Detected, Timed Out
Protocol Disconnect	Client Failed Error Detection Protocol
Protocol Disconnect	Client Failed Error Correction Due to Remote Modem Protocol
Cleardown	Cleardown Signal Rec'd From Client
Long Space Disconnect	Long Space Disc Red From Client
Carrier Lost	Carrier Dropped by Client or Telco
Retrain Timeout	No Client Response to Retrain Request

CR 101925

Exclude filters now work properly when combined with include filters.

CR 101978

The Annex now allows **callback_enable** and **auto_busyout_enable** to be set to **Y** on the same WAN interface.

CR 102041, 103497, and 104477

A new feature has been added to automatically stop syslog output to the console after 500 messages. Syslogging can be manually started and stopped by using the console monitor syslog command. Additionally, syslog messages can be displayed on the console even if host-based logging is being used. Console monitor syntax:

syslog on - starts console syslog for another 500 messages

syslog off - stops console syslog immediately

CR 104110

SPBs now allow wildcarding in the calling number processing.

CR 104112

After the autodetect process times out, the 5399 now switches to PPP mode, rather than CLI.

CR 104216

BayDVS now sends RADIUS Accounting records to the remote RADIUS server for each link of a multilink call.

Modem Support

The BayDSP V90 Digital Modem Compatibility List may be found at:

http://support.baynetworks.com/library/tpubs/pdf/remote/rac70/DMCL.PDF.

Acquiring Software Upgrades

Check the Nortel Networks Customer Support page on the World Wide Web for the latest software updates (point your browser to *http://upport.baynetworks.com*, then access the software tab at the top of the page). Also, check your modem vendor's World Wide Web page or BBS for the latest release of your modem's firmware.

24-Hour Unit Replacement Service

Nortel Networks Customer Service offers a purchasable contract (Next Day with Labor - BJ 2300) that provides next day parts replacement. For the Next Day with Labor Service Agreement to be honored, you must follow the procedures in the sections "Saving the RAC Configuration:" and "Restoring the RAC Configuration").

Saving and Restoring the RAC Configuration

When you have finished configuring your RAC, Nortel Networks recommends that you save your configuration to a host file. This ensures that you will have the configuration if the configuration file becomes damaged or otherwise needs to be replaced. Keeping a backup of the configuration file greatly simplifies the reconfiguration process, if you need to reconfigure the RAC. 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. See "Supported Operating Systems" on page 2 for more information.

➡ **Note:** Passwords and option keys (except for the 56K password) 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. 56K passwords are an exception to this rule; these passwords are saved and cannot be changed.

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.

➡ **Note:** You must have root permission on the host.

Saving the RAC Configuration:

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

    ```
    command: annex <IP_address>
    ```

    IP_address identifies the RAC to which you will issue subsequent commands.

➡ **Note:** The next prompt might not be a command prompt. You will be prompted for a password if one is specified for the RAC.

2. **You now see the RAC IP address, the RAC 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 and places the file in the same directory from which you are running **na**. The file name should identify the RAC 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_recv_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 the file will not be corrupted or otherwise changed when you upgrade the RAC.

Restoring the RAC Configuration

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

Placing the File onto the RAC

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

➡️ **Note:** The new unit must have an IP address already assigned to it. For more information, see the hardware installation manual. 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 RAC, 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.

➡️ **Note:** You must have root permission on the host.

To restore a RAC's configuration:

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

    ```
    command: annex <IP_address*>
    ```

    IP_address identifies which RAC you want for subsequent commands.

2. **Enter one of the following commands:**

    For UNIX:

    read <filename.param >

    For Windows NT:

    read <filename.txt>

    This copies the filename.param file to the RAC that you specified and change the parameters to those specified in the file.

3. **Enter:**

    command: **quit**

    This exits **na.**

➡️ **Note:** 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 the IP addresses specified for 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 RAC, you must use the monitor prompt to assign an IP address to the RAC. You need the following equipment to do this:

- A terminal (VT100, laptop, and so on).

- A straight-through RJ45 cable.

- A console terminal adapter. If you are using a laptop, you typically need aDB25-to-DB9 converter, straight-through.

To assign an IP address to a RAC:

1. **Insert the RJ45 connector in the console port of the RAC.**

2. **Set your terminal to the following settings: 9600 baud, 8 data, 1 stop, no parity, and XON/XOFF.**

3. **Insert the other end other end of the RJ45 connector into the console adapter and connect the console adapter to your laptop.**

4. **Turn on the RAC.**

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 Return. The monitor prompt appears.**

7. **At the monitor prompt, set the IP address and the initial configuration parameters. Enter addr to make these initial configuration settings.**

8. **Check the boot sequence by entering seq. Because you are booting from the network, set the sequence to net, self. You can specify self only if the option was purchased for that particular unit.**

9. **Enter image to verify that you are using the correct operational image.**

10. **Enter boot, then press Return to boot the RAC. 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 RAC.**

Documentation Changes

This section describes changes affecting the 5399 and 8000 Access Switch product documentation. These changes are the result of changes made to the Version 8.0 software after the these documents went to print.

NFAS Documentation

The documentation for Version 8.0 contains information on NFAS. Disregard this information. Version 8.0 does *not* support NFAS parameters and switches related to NFAS.

IP Pooling Documentation

Disregard any IP Pooling information contained in the documentation. This information is out of date. Nortel Networks will release a Supplement covering IP Pooling at a later date. You can find the Supplement on the Web at *support.baynetworks.com/library/tpubs/*.