296-1011-220
Document Revision 07.02

CVX Multi-Service Access Switch
Release 4.1
May 2001

CVX Multi-Service Access Switch

4.1 Release Notes

NORTEL NETWORKS™

Printed in the USA

Regulatory and Safety

Regulatory Information

U.S.A. Requirements

FCC Radio Frequency Class A Notice for CVX 1800 Access Switch

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission (FCC) rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

Do not attempt to repair or modify this equipment. All repairs must be performed by Nortel Networks, or an authorized Nortel Networks representative.

FCC Radio Frequency Class B Notice for CVX 600 Multi-Service Access Switch

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Part 68 General Information

This equipment complies with Part 68 of the FCC rules. This equipment uses the following USOC RJ-48 jacks:

Interface	Service Code	Facility Code
1.544 Mb/s superframe format (SF) without line power	6.0N	04DU9-BN
1.544 Mb/s superframe format (SF) and B8ZS without line power	6.0N	04DU9-DN
1.544 Mb/s ANSI extended superframe format (ESF) without line power	6.0N	04DU9-1KN
1.544 Mb/s ANSI extended superframe format (ESF) and B8ZS without line power	6.0N	04DU9-1SN

If you experience trouble with this equipment, please contact Nortel Networks for repair and warranty information. If there is a problem with the network, the telephone company may request that you remove the equipment from the network until the problem is resolved.

Nortel Networks recommends that you install an AC surge protector in the AC outlet to which the equipment is connected. This helps to prevent damage to the equipment caused by local lightning strikes or other electrical surges.

FCC and Telephone Company Procedures and Requirements

In order to connect this equipment to the network, you must provide the local telephone company with the registration number of this equipment, and you must order the proper connections.

To order the proper service, provide the telephone company with the following information:

- Number of required jacks and their USOC numbers
- Sequence in which the trunks are to be connected
- Facility interface codes, by position

UL Listing - U.S. and Canada

This equipment has been Listed by Underwriter Laboratories, Inc. for use in the U.S. and Canada to the requirements of UL 1950. Third Edition - Safety of Information Technology Equipment. Including Electrical Business equipment and Canadian Standards Association CAN/CSA C22.2 No. 950-95 Third Edition.

Australia Requirements

N441

The regulator for telecommunications and radio communications in Australia is the ACA (Australian Communications Authority). This equipment is labeled with the A-Tick mark, which indicates that the product complies with both EMC and Telecommunications requirements and establishes a traceable link between the

equipment and the manufacturer. It is also an indication to the user that the product can be connected to a telecommunications network.

Canada Requirements

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (CVX 1800) does not exceed the Class A limits for radio-noise emissions from digital apparatus, as documented in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (CVX 1800) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

Canada CS-03 Rules and Regulations

Note: The Canadian Department of Communications label identifies certified equipment. The certification means that the equipment meets certain telecommunications network protective, operational, and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, ensure that it is permissible to connect to the facilities of the local telecommunications company. You must install this equipment using an acceptable connection method.

Repairs to certified equipment should be made by a supplier-designated representative. If you make repairs or alterations to this equipment, or if the equipment malfunctions, the telecommunications company may request that you disconnect the equipment.

You should ensure, for your own protection, that the electrical ground connections for the power utility, telephone lines, and internal water-pipe system, if present, are connected. This precaution may be particularly important in rural areas.

Caution: You should not attempt to make such connections. You should contact the appropriate inspection authority or electrician.

Canada CS-03 Règles et règlements

Note: L'étiquette du ministère des Communications du Canada indique que l'appareillage est certifié, c'est-à-dire qu'il respecte certaines exigences de sécurité et de fonctionnement visant les réseaux de télécommunications. Le ministère ne garantit pas que l'appareillage fonctionnera à la satisfaction de l'utilisateur.

Avant d'installer l'appareillage, s'assurer qu'il peut être branché aux installations du service de télécommunications local. L'appareillage doit aussi être raccordé selon des méthodes acceptées.

Les réparations de l'appareillage certifié devraient être confiées à un service désigné par le fournisseur. En cas de réparation ou de modification effectuées par l'utilisateur ou de mauvais fonctionnement de l'appareillage, le service de télécommunications peut demander le débranchement de l'appareillage.

Pour leur propre sécurité, les utilisateurs devraient s'assurer que les mises à la terre des lignes de distribution d'électricité, des lignes téléphoniques et de la tuyauterie métallique interne sont raccordées ensemble. Cette mesure de sécurité est particulièrement importante en milieu rural.

Attention: Les utilisateurs ne doivent pas procéder à ces raccordements, mais doivent plutôt faire appel aux pouvoirs de réglementation en cause ou à un électricien, selon le cas.

Europe Requirements

EN 55 022 Statement

This certifies that the Nortel Networks CVX 1800 is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).

Warning: This is a Class A product. In a residential area, this product may cause radio interference, in which case the user may be required to take the appropriate measures.

EC Declaration of Conformity

This product conforms (or these products conform) to the provisions of Council Directive 89/336/EEC and 73/23/EEC, as amended by Directive 93/68/EEC.

Japan/Nippon Requirements Only

Voluntary Control Council for Interference (VCCI) Statement

この装置は、第一種情報装置（商工業地域において使用されるべき情報装置）で、商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会（VCCI）基準に適合しております。

従って、住宅地域、その隣接地域等で使用した場合、ラジオ、テレビ受信機等に障害を与えることがあります。

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the 1st category (information equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines that are aimed at preventing radio interference in commercial and/or industrial areas.

Consequently, when this equipment is used in a residential area or in an adjacent area thereto, radio interference may be caused to equipment such as radios and TV receivers.

JATE Requirements

This certifies that the Nortel Networks CVX 1800 conforms to the standards set by JATE (Japan Approvals Institute for Telecommunications Equipment) as of 02/25/99 with Approval Numbers T99-6007-0 and N99-N337-0.

Safety Warnings

General Warnings

The following safety warnings apply:

- Mechanical and electrical shock hazards are possible if you remove one or more of the modules. There are no operator-serviceable modules. Only qualified personnel should service this equipment.
- This equipment must be connected to a protective ground according to the instructions in the *CVX 1800 Access Switch Hardware Installation Guide*. Improper grounding may result in electrical shock.
- This equipment does not provide safety isolation between any port that is connected to a digital network termination point or any port to which terminal equipment is connected.
- The wall circuit breaker provides the main protection for this equipment. For -48 VDC operation, the equipment must reside on its own circuit with a breaker rated for 50 A.

DC Power Supply Warnings

The DC power supply must be installed in a restricted area, such as an equipment closet or room, in compliance with Articles 110-16, 110-17, and 110-18 of the National Electric Code, ANSI/NFPA 70. The DC power source must be isolated from the AC power source and must have a proper ground.

The grounded conductor of the DC supply circuit can be connected to the frame grounding conductor of the CVX Access Switch. In this case, the following conditions apply:

- The CVX switch must be connected to the DC power supply grounded conductor or bonding jumper from the grounding terminal bar or bus to which the DC power supply grounded conductor is connected.
- The CVX switch must be located in the same area as other equipment having a connection between the grounded conductor of the same DC supply circuit and the grounding conductor, and also the point of grounding of the DC system. The DC system must not be grounded elsewhere.
- For the CVX 1800 only, the DC power supply must be located on the same premises as the CVX 1800.
- You must not switch or disconnect devices in the grounded conductor between the DC power supply and the point of connection of the grounding electrode conductor.
- A readily accessible disconnect device may be provided in the fixed wiring for a DC power supply. The device must be rated for the voltage and current specified.

For safety purposes, the DC power supply requires connection to a grounded outlet. To prevent possible injury from voltages on the telecommunications network, disconnect all telecommunications network lines before disconnecting the DC power supply from the grounded outlet.

Lithium Battery Caution

Caution: Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Attention: Il y a danger d'explosion s'il y a remplacement incorrect de la batterie. Remplacer uniquement avec une batterie du même type ou d'un type recommandé par le constructeur. Mettre au rebut les batteries usagées conformément aux instructions du fabricant.

Contents

Contents

Chapter 4
Known Problems and Limitations

Chapter 5
User Information

Chapter 1
Upgrading to Release 4.1

Overview

The Nortel Networks CVX* Multi-Service Access Switch is a high-capacity, carrier-class, access switch that allows subscribers to connect to a public data network (PDN). You can access corporate network resources and the Internet from anywhere in the world through Integrated Services Digital Network (ISDN) lines or by modem over the public telephone network.

The CVX switch provides an interface between the telephone network and the data network. When the CVX switch validates and terminates a call, it passes the call to the designated customer, such as an Internet service provider (ISP), corporate host, or other network. The CVX switch's redundant architecture provides reliable carrier-class performance, which means high availability, maintainability, scalability, and compliance to carrier standards.

Release 4.1 Product Compatibility

Before performing any of the CVX switch upgrade procedures in this notice, make sure that the other CVX switch components are running software that is compatible with Release 4.1.

CVX Access Switch Family Compatibility Matrix

Table 1-1 indicates the compatibility of the CVX switch, CVX SS7 Gateway (CSG), CVX Policy Manager (CPM), and CVXView software versions as known on the release date of this document. Also indicated are the compatibility between CSG and SS7View software, and CPM and PolicyView software.

Table 1-1. CVX Access Switch Family Compatibility Matrix

		CPM					CSG			CVXView				
		2.0	3.0	3.1	3.6	4.0	3.0	3.6	4.0	2.0	3.0	3.1	3.6	4.0
CVX*	2.0	Y	Y	Y	N	N	Y	N	N	Y	Y	Y	N	N
	3.0	N	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y
	3.1	N	N	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y
	3.6	N	N	N	Y	Y	N	Y	Y	N	N	N	Y	Y
	4.0	N	N	N	N	Y	N	N	Y	N	N	N	N	Y
	4.1	N	N	N	N	Y	N	N	Y	N	N	N	N	N

* SCC II requires release 3.6.2 or later of the CVX switch software. CVX 600 hardware supports only release 4.0 or later of the CVX switch software. All other releases of the CVX switch software are supported on all CVX 1800 hardware.

CVX Switch Backward Compatibility

All CVX system software for the system control card (SCC), digital access card (DAC), and modem access card (MAC) is backward compatible with existing CVX switch hardware. Each respective firmware image automatically detects the hardware and its revision, and enables only the functionality supported by the installed hardware.

SCC-II Warning

Warning:
DO NOT USE any CVX switch software release prior to 3.6 or damage to the SCC-II will result. DO NOT COPY pre-3.6 versions of CVX switch software to any flash card installed in an SCC-II. If a CVX switch boot is attempted, the CVX switch will become nonfunctional until the corrupt SCC-II is removed and forwarded to Nortel Networks for reprogramming and returned to the customer site. The 3.6 software supplied with the SCC-II is required for normal operation.

Analog Modems

Analog Modems Supported by the CVX Switch

The CVX switch host digital modems support all known analog modem technologies. All versions of host digital modem software are tested for connection reliability, call longevity, and compatibility with various consumer modem technologies that lie beneath retail brand names and model numbers. Tests include representative retail samples of modem technologies offered by OEMs of Conexant Systems, Lucent Technologies, Texas Instruments, Analog Devices, Intel, Motorola, ESS Technology, PCTel, and others.

The CVX switch host digital modems are in compliance with all applicable ITU standards and recommendations.

In our testing however, we find that the supported consumer devices listed below *do not* meet our minimum standards for satisfactory connectivity. Compatibility and performance may improve with updated consumer modem software that now exists or will be issued in the future by the manufacturer, and users of these devices should upgrade as soon new software is available:

- V.90 Internal PCI-bus “winmodems” based on Lucent Technologies that are running under software versions earlier than version 5.49 tend to suffer from excessive failures to connect and unwanted disconnects. These issues were cleared with Lucent's 5.49 release. At the time of this report, the most recent Lucent version is 5.97. All users should update their modem software.
- V.90 Internal PCI-bus “winmodems” based on Conexant Systems HCF technologies running software versions earlier than version 2.1.2.161 tend to experience failures to connect and unwanted disconnects in excess of our minimum standards for satisfactory connectivity. All users should update their modem software.
- V.90 Internal PCI-bus softmodems based on Intel (Cirrus Logic) technology running software versions of 1.024 or earlier tend to experience failures to connect and unwanted disconnects that exceed our minimum standards. All users should update their modem software.

- V.90 Internal PCI-bus softmodems based on PCTel technology running version 7.61 or earlier tend to experience failures to connect rates that exceed our minimum standards. All users should update their modem software to the most current version offered.
- V.90 Internal ISA-bus modems based on ESS technology running version 6.73 or earlier suffer failures to connect and unwanted disconnect rates that exceed our minimum standards. All users should update modem software to the most current version.
- V.90 External USB-interface modems based on ST Microelectronics technology running version 2.76H or earlier suffer failures to connect that exceed our minimum standards. These devices should be upgraded to the most current version of modem software.

Specific Modems Tested

Below are listed the specific consumer modems that have been tested for performance and compatibility with the CVX switch as of the date of this document.

Make/Model
ActionTec Desk Link Pro PCI 56k (Lucent)
ActionTec 56k PCI PRO
Ambiant PCI 56k
Award Technology 56K V.90 Faxmodem (LT)
Best Data 56K Mach2 PCI (Conexant)
Best Data 56K Mach2 PCI (PCTel)
Boca Research Bocamodem 56K
Boca Research Fax Data PNP 33600
CNet Technology 5614CH 56K Voice/Fax
CNet Technology 5614XE 56K Voice/Fax
Conexant SofK56 HSF PCI
DGC 56K Fax/Modem (China)
Diamond Supra Express 56e
Diamond Supra Express 56e USB

Make/Model
Diamond SupraMax 56 PCI (Conexant)
Digicom 56K PCI Faxmodem
Digicom Modem Blaster PCI
Eiger Labs Eigercom 56K PCI (PCTel)
GVC V.90 Soft Modem (SoftK56)
HI-VAL LP USB Modem (STMicro)
HP 56K V.90 PCI (Conexant) HCF Winmodem
I/O Magic MagicSurfer 56K PCI (PCTel)
Intelliquis Total Fax w/LT Winmodem
Maxtech Netpacer Pro V.90 (LT Winmodem)
Microcom Compaq 415
Motorola SM56 PCI
Motorola UDS V34
New Media 56K USB Netsurfer
Pine VA7-AV MB Pctel HSP56MR
Sony WebTV Plus (Conexant)
TP-Link Data/Fax/Voice (China)
Unbranded V90 Winmodem (Lucent)
USR 56K Faxmodem (Sportster)
USR 56K PCI Winmodem
USR 56K Voice Pro USB
USR Courier 56K+V.Everything
USR Courier V.34+V.Everything
USR Sportster 336
Viking Comp 56LP-V (Lucent)
Zoom 56K Faxmodem (Conexant)
Zoom Faxmodem 56K (Conexant)
Zoom K56 (Conexant)
Zoom PC Card 56K (Lucent)
Zoom V.32bis
Zoom V.34 (Conexant)

Make/Model
Zoom V.90 USB (Lucent)
Zoom V.92 Faxmodem (Lucent)
Zoom V.92 LT Winmodem PCI

Minimum Configuration for Remote Access

The minimum chassis configuration for the CVX supports 96 or 102 modem or ISDN calls. In the minimum configuration, the chassis contains the following modules:

- One SCC-SM in front slot
  - CVX 1800 - slot 9 or 10
  - CVX 600 - slot 5 or 6
- One Nortel Networks flash memory card in PCMCIA slot 1 of the SCC-SM
- One SCC-RLTM in the corresponding rear slot
- One MAC-SM in any unused front slot
- One DS1-DAC-SM or one E1-DAC-SM in any unused front slot, usually installed in slot 2
- One DS1-DAC-LTM or one E1-DAC-LTM in the corresponding rear slot, usually installed in slot 2
- Blank filler panels in all unused front and rear slots

CVX Switch Pre-Upgrade Checklist

Before performing the CVX switch upgrade:

- Verify that all other CVX switch family devices have been successfully upgraded with compatible software (see "CVX Access Switch Family Compatibility Matrix" on page 1-2).
- Verify that all CVX switches are currently working properly, with no alarms. Check the LEDs to ensure proper operation.
- Create a backup copy of all files on your currently running CVX flash memory card.

  -- Retain the current release on the current flash card, or save all the contents to a backup directory.

  This step will allow you to restore your previous configuration, if necessary.
- Verify that you have the IP address of the CVX SCC (if you are performing a remote upgrade).
- Verify that you have the correct user name and password with Level 2 access privileges.
- Verify that a 3.6 or later release is running prior to upgrading hardware to SCC-II, double-density MAC, or double-density DAC.

Upgrading to Release 4.1 from Prior Releases

The following procedures describe how to install CVX Release 4.1 from a previous release or maintenance release. Use these procedures if you are performing either a local upgrade or a remote upgrade using FTP and Telnet.

This section contains the following procedures:

Note: Before upgrading the CVX switch to Release 4.1, be sure to save a copy of all the contents of your Release 2.0, 3.0, 3.1, 3.6, or 4.0 Nortel-supplied flash card. This step will allow you to restore your previous configuration should you experience problems with the upgrade.

Checking Your Flash Memory Card

Before you perform an upgrade, you must check your flash memory card to ensure that you have sufficient memory space to perform an upgrade. The minimum requirement for an upgrade is 45 Mb of available memory.

To check the amount of available flash memory, at the CVX> prompt, enter **dir**.

```
CVX> dir

   Directory of: c:\
.
. (list of directories and files)
.
   24 file(s)          18573814 bytes
                       29739836 bytes free
CVX>
```

Removing Unneccessary Files

Step	Action

1	At the CVX> prompt, enter cd <directory name>.
	
	`CVX> cd coredmp`
	`c:\coredmp`

2	At the coredmp directory, enter del *.* `CVX> del *.*`

3	At the CVX> prompt, enter **cd** to go back to the root (c:\) directory.
	
	`CVX> cd\` (Do not type **cd ..**)
	`c:\`
	`CVX>`

4	Repeat steps 1 through 3 for the crashes directory.

Backing Up the Current Release

This section describes the procedure for backing up the current CVX release prior to upgrading to CVX Release 4.1. Creating a backup copy will allow you to revert back to the older release if you experience problems with CVX Release 4.1.

Creating the Backup Directory on the Flash Memory Card

Step	Action
1	At the CLI, create a backup directory. Example: `CVX> mkdir backup` You can create the backup directory on the flash memory card in drive C:\.
2	Copy all files from the CVX root directory to the backup directory that you just created. Example: `CVX> copy [filename] c:\backup\[filename]`
3	Copy the 4.1 *cvx.dra* file to the CVX (using FTP or other file transfer method).

Performing a Local Upgrade

The *cvx.dra* file is a single bundled file that contains all the software images required for a CVX switch software upgrade. To upgrade, reboot the CVX switch with a flash memory card containing the following files:

- The Release 4.1 *cvx.dra* file
- The current *config.cvx* file that is running on the CVX switch
- The current *boot.ini* file that is running on the CVX switch

When the SCC starts up, it searches for a *cvx.dra* file. If this file is found, the SCC extracts all of the component files to the flash memory card. If a new *bepbr.elz* or *bepfr.els* file is found, the SCC automatically transfers these images to the flash memory card on board the SCC. After extracting all files and transferring images to SCC memory, the SCC deletes the *cvx.dra* file and restarts with the new software version; the extracted files reside on the flash memory card.

Note: Allow approximately 30 minutes for the CVX switch configure and reboot.

When booting from a *cvx.dra* file, the CVX switch does not overwrite the existing *boot.ini* file (instead, the *cvx.dra* file will copy the file called *boot.new* with a default version of the file). You can open and review the contents of the *boot.new* file, edit the file if necessary, and then copy it to the *boot.ini* file before restarting the CVX switch, as described in this section.

Note: The CVX switch must already be running Release 2.0 software or greater to support the automated upgrade procedure.

Note: If the CVX 1800 being upgraded contains a redundant SCC (slot 10), ensure that the CVX switch is running in slot 9 as the SCC master and the SCC in slot 10 is running as the slave before proceeding. If the CVX 600 being upgraded contains a redundant SCC (slot 6), ensure that the CVX switch is running in slot 5 as the SCC master and the SCC in slot 6 is running as the slave before proceeding. To check this, enter the following command:

```
CVX> scc -i
SCC is running in slot 9 as master.
Adjacent SCC detected!
```

Perform the following steps to upgrade to Release 4.1

Note: Issuing the **cold** command in this procedure drops all modem and trunk interfaces. Use the **quiesce** command so that no new calls are accepted before you start this procedure.

Step	Action
1	Ensure that the *cvx.dra*, *config.cvx*, and *boot.ini* files are present on the flash memory card in drive C:.
2	From the console, enter the cold command to reboot the CVX switch. `CVX> cold` To determine if the reboot is successful, proceed to "Determining Boot Results" on page 1-16.

Note: If the flash memory card does *not* contain the *boot.ini* file, the *cvx.dra* still extracts all the files. However, if the boot.ini file is missing, the CVX switch will boot into bootstrap mode.

Step	Action
3	From the console, press the [Return] key to display the user name: prompt.
4	Log in to the CVX switch.

5	After successfully logging on, enter the vinfo command at the CVX> prompt to display the software version.
	
	`CVX> vinfo`
	`Image Version Bld# BldDate Time Machine User Brd Branch`
	`fepmd 4.1 nnnn mm/dd/yyyy 03:20:53 BRICK2 Build scc v4.1.0`
	`CVX>`

Determining Boot Results

The CVX switch displays the results of the boot process on the local console. The following sections display the key messages in **bold** type for successful and unsuccessful boot results.

Successful Boot Results

When the CVX switch completes extracting files and moving them to the C:\ drive, the CVX switch starts the boot process. If the *boot.ini* file is present in flash memory after the default drive is mounted, the CVX switch displays the following messages:

```
CVX> cold     (step 5 of Performing a Local Upgrade (page 1-13)
.
.             (files are extracted)
.
...please wait for the system wide initialization
.
.             (waiting for default drive to mount)
.
Drive mounted ...found boot.ini ...
auto-loading BEP ...

Starting ... poweron boot ...
.
.
Slot n (DAC) pcc is ready ...
Slot n (DAC) dmm ready ...
```

Press the [Return] key. The user name: prompt is displayed.

Unsuccessful Boot Results

When the CVX switch completes extracting files and moving them to the C:\ drive, the CVX switch starts the boot process. If the *boot.ini* file is missing in flash memory after the default drive is mounted, the CVX switch displays the following messages:

```
CVX> cold     (step 5 of "Performing a Local Upgrade" starting on page 1-13)
.
.             (files are extracted)
.
...please wait for the system wide initialization
.
.             (waiting for default drive to mount)
.
Drive mounted ...
Starting the TDM Test control task  (the boot.ini file cannot be found)

Bootstrap shell starting ...
.
.
.
Slot n (DAC) pcc is ready ...
Slot n (DAC) dmm ready ...
Received ALIVE message from slot <#>
```

Press the [Return] key. The user name: prompt is displayed.

To restore the *boot.ini* file to flash memory, perform the following steps:

Step	Action
1	At the CVX> prompt, log on only as root (both user name and password). CVX> user name: **root** password: **root**
2	Enter the enable command or the set level 2 command to gain access to all CVX switch commands. CVX> **set level 2**

Step	Action
3	Enter the copy command to copy the *boot.new* file to *boot.ini*, as follows: `CVX> copy boot.new boot.ini`
4	Enter the cold command to reboot the CVX switch. `CVX> cold`

Performing a Remote Upgrade Using FTP and Telnet

You can upgrade your CVX switch to Release 4.1 remotely using FTP and Telnet. At the completion of the upgrade, the CVX switch uses the same configuration parameters as it did before the upgrade by retaining the previous *config.cvx* file and the previous *boot.ini* file.

Before you upgrade the CVX switch, be sure you have the following CVX switch information:

- IP address
- User name
- Password

Note: Before upgrading the CVX switch to Release 4.1, be sure to save a copy of all the contents of the 2.0, 3.0, 3.1, 3.6, or 4.0 Nortel-supplied flash card, either to a laptop PC or a network drive. This step will allow you to restore your previous configuration if you experience problems with the 4.1 upgrade. If the CVX switch is being upgraded from Release 3.6 or later, the **Backup** and **Revert** commands may be used to save the current load to a sub-directory of the flash card. See the *CVX Multi-Service Access Switch Administrator's Guide* for more information.

Note: Before upgrading the CVX switch with a redundant SCC, ensure that the primary SCC is running in the primary SCC slot. If it is not running, do not proceed with the upgrade procedures until you perform a failover from the secondary slot to the primary.

To upgrade the CVX switch remotely, perform the following steps:

Step	Action
1	Copy the *cvx.dra* file to your computer. **Note:** This file is approximately 16 MB.

Note: Issuing the **cold** command in this procedure drops all modem and trunk interfaces. Use the quiesce command so that no new calls are accepted before you start this procedure.

Step	Action
2	Create a Telnet session from your computer to the CVX switch that you want to upgrade and ensure that the CVX switch displays the root directory. The CVX switch must be in the root (C:\) directory when you perform the FTP download. If using an FTP user friendly tool, please note that the CVX switch displays file names similiar to the Windows NT display.

3	Create an FTP session. For example, at the DOS prompt, enter **ftp**.
	
	`C:\> ftp`
	`ftp>`

4	At the ftp> prompt, enter open <CVX IP address>.
	
	`ftp> open 123.45.67.89`
	`Connected to 123.45.67.89.`
	`220 123.45.67.89 CVX FTP server (1.0) ready.`
	`User (123.45.67.89:(none)):`

5	Enter the user name.
	
	`User (123.45.67.89:(none)): <username>`
	`331 Password required for username.`
	`Password:`

6	Enter the password.
	
	`Password: <password>`
	`230 User <username> logged in.`
	`ftp>`

7	At the ftp> prompt, enter binary.
	
	`ftp> binary`
	`200 Type set to I.`
	`ftp>`

Step	Action
8	At the ftp> prompt, enter cd c:\ to go to the root directory. `ftp> cd\`

9	At the ftp> prompt, enter **put cvx.dra**.
	
	`ftp> put cvx.dra`
	`266 Transfer complete.`

10	When the file successfully transfers to the CVX switch, ensure that the *config.cvx*, *boot.ini*, and *cvx.dra* files are at the root directory on the flash card by initiating the dir command at the CVX prompt. If any of these files is missing, use FTP to transfer the missing file or files to the CVX switch.
11	Enter the **cold** command at the CVX prompt from a Telnet session. `CVX> cold` When you enter the **cold** command, the CVX switch reboots, the modem and trunk interfaces drop, the *cvx.dra* file expands into the CVX switch memory, and the Telnet session terminates. It takes approximately 30 minutes for the CVX switch to reconfigure and reboot.

12	Create another Telnet session. At the CVX> prompt, enter **vinfo**.
	
	`CVX> vinfo`
	`Image Version Bld# BldDate Time Machine User Brd Branch`
	`fepmd 4.1 nnnn mm/dd/yyyy 03:20:53 BRICK2 Build scc v4.1`
	`CVX>`

13	Ensure that the version number is 4.1.

Restoring the CVX Access Switch to the Backup Software Release

This section shows you how to restore the backup software release to the CVX switch. To restore the CVX switch to the backup software release, you will need to access the backup directory that you previously created.

Warning:
If you have upgraded to any double-density cards, DO NOT restore any CVX switch software release pior to 3.6 or damage to the SCC-II will result. You will have to reinstall your original hardware. If a CVX switch boot is attempted, the CVX switch will become nonfunctional due to a corrupted SCC-II and will not function until the corrupt SCC-II is removed.

To restore the CVX switch to a prior release, if the Revert command is available:

Step	Action
1	Use the Revert command to copy the files from the backup directory to the flash memory card in Drive C: Example: `CVX> revert c:\backup` This example copies all files from the backup directory in drive C: to the CVX switch root directory.
2	Enter the felf command to initialize the *bepbr.elz* file. `CVX> felf bepbr.elz`
3	Reboot the CVX switch. Example: `CVX> cold`

To restore the CVX switch to a prior release, if the Revert command is not available:

Step	Action

1	From the CLI, change to the backup directory and copy each file to the root directory on the flash memory card in drive C:. For example:
	
	`CVX> cd c:\backup`
	`CVX> copy [filename] c:\[filename]`
	
	This example copies the file specified by [filename] to the root directory. This must be done for every file in the c:\backup directory.

2	Enter the felf command to initialize the *bepbr.elz* file. `CVX> felf bepbr.elz`
3	Enter the cold command to restart the CVX switch using the backup software version. For example: `CVX> cold` The CVX switch reboots and installs the prior release software with the configuration associated with that software release.
4	Enter the vinfo command to verify the software version.

Upgrading to the Double-Density Hardware

Before upgrading to the new double-density DAC, MAC, and SCC-II hardware, ensure that the CVX switch is operating correctly before performing the upgrade. Any service problems need to be resolved before performing the upgrade.

The recommended slot locations for both 12xDS1 and 24xDS1 DAC cards are slots 2, 7, 12, 17.

If you are using CVXView and CPM, refer to Release 4.1 Product Compatibility (page 1-2) for upgrade compatiblities. If you do not perform upgrades to CVXView and to CPM, CVXView will not be able to monitor the CVX switch and CPM may not be able to communicate properly with the CVX switch.

Double-Density Upgrade Procedure

Step	Action
1	Upgrade to CVX Release 4.1.
2	Use the **vinfo** command to verify the correct version and operation of the CVX switch after the software upgrade is complete.
3	Remove all traffic from the CVX switch using the **shelf dry** command. On DAC cards, wait until all DS0s are removed from service before proceeding.
4	If changing the type of SCC being used, make sure to remove any configuration containers that will not be referenced by the new SCC-II. For example, if the SCC was the 3xENET+HSSI and the new SCC-II is the 5xENET, then delete all Frame Relay and HSSI containers prior to powering down the CVX switch. Also make any appropriate network design changes to your network to prevent the loss of routing to and from the CVX switch.
5	Power down the CVX switch.
6	Remove single density hardware and replace with the new double-density hardware in the same chassis slots, replacing the RLTM or LTM before inserting SCC-II. Install the double-double-density MACs into the same slots that occupied the single density MACs. Install the double-density DACs into the same slots that occupied the single density DACs. The master and redundant SCC-II hardware installs in the SCC slots. If using a 24xT1/E1 DAC, ensure that the LTM aligns with the DAC SM slot and the next higher slot. For example, if the DAC SM is installed in slot 2, the LTM should be installed in slots 2 and 3.
7	Recable the LTMs so that each T1/E1/T3 is replaced into the same port prior to the upgrade. This will ensure that the cabling matches the existing software configuration. For example, if a T3 was used, make sure to place the T3 cables into T3 1 (labeled TX1 and RX1) on the new 2 x DS3-DAC-LTM.
8	Remove the flash card from the master SCC and place it into the new master SCC-II.

Step	Action
9	Remove the flash card from the redundant SCC and place it into the new redundant SCCI-I, if used.
10	Apply power to the CVX switch. After the boot up sequence is complete, verify functionality of all new hardware and software and overall operation of the CVX switch.
11	From a console session, type **felf bepbr.elz**. If your CVX switch has a redundant SCC you will need to execute the command for the redundant SCC. To do this, type **vshell -r**, then type **felf bepbr.elz**. Type **cold** to reboot the redundant SCC. Exit the redundant SCC by pressing CTRL-C.
12	On the double-density DAC cards, provision the new DS1 and DS3 lines as needed onto the new hardware.
13	Increase the number of VPOPs or increase the IP pools so that you have enough IP addresses to assign to the increased number of calls.

Note: Ensure that the MAC port count is equal to or greater than the DS0 count enabled.

Post-Upgrade Tests

Perform the following tests to verify proper operation of the CVX switch.

- Verify IP connectivity between the CVX switch and other CVX switch family devices:
  - -- Use the **ping** and **traceroute** commands from the CLI.
- Verify that all analog and ISDN calls are successfully completing calls to the correct VPOPs.
- Verify that callers can reach the Internet.
- Ensure that the MAC port count is equal to or greater than the DS0 count enabled.

For information on configuring the CVX switch, refer to the CVX switch documentation set available on CD-ROM, or go to the Nortel Networks online customer support web site.

Operational Information

The following sections provide specific operational information that you need to know before using the CVX switch.

Nonredundant SCC Configurations on the CVX Switch

In a nonredundant SCC configuration on the CVX 1800, configure the SCC for slot 9 only. In a nonredundant SCC configuration on the CVX 600, configure the SCC for slot 5 only.

Redundant SCC Configurations

In redundant SCC configurations, the CVX switch automatically considers the SCC in the first SCC to be the master SCC upon initial power-up.

An example for the CVX 1800: if you have an SCC in slot 9 and an SCC in slot 10, the SCC in slot 9 will always be the master SCC and the SCC in Slot 10 will be the slave. Be sure to configure **shelf 1/slot 9** within *config.cvx*. Do not add configuration entries under **shelf 1/slot 10**.

An example for the CVX 600: if you have an SCC in slot 5 and an SCC in slot 6, the SCC in slot 5 will always be the master SCC and the SCC in Slot 6 will be the slave. Be sure to configure **shelf 1/slot 5** within *config.cvx*. Do not add configuration entries under **shelf 1/slot 6**.

Redundant DS3-DAC Configurations

In redundant DS3-DAC configurations, the main DS3-DAC must be configured for the lower of the two slots used. For example, if on a CVX 1800, there is a DS3-DAC in slot 4 and in slot 5, the DS3-DAC in slot 4 must be configured as the main card, and the DS3-DAC in slot 5 as the redundant card.

To create a redundant DS3 configuration, edit the *boot.ini* file on the flash memory card to include the following lines in the format:

```
[redundant]
  slotx=y
```

where *x* and *y* are adjacent CVX switch slots using two-digit numbers.

For example, the following entry creates a redundant configuration when you start the system.

slot04=05

Warning: When editing the *boot.ini* file, be sure to use a carriage return after the last line in the file. If you do not include the carriage return, the last character of the last line in the file will be truncated, resulting in an incorrect line entry and unpredictable system operation.

Configuration File (*config.cvx*)

When using the CLI to edit attributes in the configuration file, enter the **show** command to display the most current values for those attributes. When you use the **commit** command during a CLI session, the CVX switch applies any changes you made using the **set** command to the SCC memory buffer. It does not save the changes you made to the configuration file (*config.cvx*) on the flash memory card. To save your changes to the configuration file on the flash memory card, use the **save** command after you use the **commit** command. When you use CVXView to configure the CVX switch, the **commit** command automatically saves the configuration file on the flash memory card.

Ascend-Modem-Port-No Attribute (5212)

The value of the Ascend-Modem-Port-No attribute (for example, 262402) is a combination of the IOP, DMM, pack, and device, expressed in hexadecimal notation.

General Recommendations

We make the following recommendations for this CVX switch release:

- Before you modify the CVX switch configuration file, be sure to back up the current configuration file (*config.cvx*) to a network drive in case you need to install it again.
- Do not use embedded apostrophes in any commands at the command line interface. For example, do not name a system “John Doe’s CVX”. Embedded apostrophes will cause system errors.
- When you configure an E1 line for Channel Associated Signaling (CAS), the value you set for the **maxCalledDigits** attribute *must* match the value provisioned by the E1 service provider. If dial-up users cannot connect, or if 20 to 30 seconds pass before dial-up users connect, ensure that the maxCalledDigits value matches the maximum number of digits in the dialed number identification string (DNIS) received by the CVX switch.
- If you want to set up the IP interface for the first time without rebooting the CVX switch, enter the following commands:

  ```
  .../bic/ethernet 1/ethernetconfig> set ethernetenable disable
  .../ethernet 1/ip_interface/ip_circuit> set ip_local <n.n.n.n>
  .../bic/ethernet 1/ethernetconfig> set ethernetenable enable
  ```

- Nortel Networks recommends setting the system/ip_services/ip_service/ip_syslog> **priority** attribute to **disabled** (whether or not the system/ip_services/ip_service/ip_syslog> **filter_level** attribute is **enabled**). This allows the event message severity levels from the CVX switch to display properly in the system log.

Chapter 2
New Functionality

New Functionality in Release 4.1

This chapter describes the new functionality for the CVX Multi-Service Access Switch Release 4.1.

CVX Multi-Service Access Switch Software Features for 4.1

The following list highlights the software enhancements in this release:

- X.75 dial-in support for ISDN (LAPB)
- V.110 Rate Adaptation support for 14.4 and 28.8 kbps enhanced data rates
- V.92 support for modems (CSM6 MACs only, at this time)
- V.44 support for modems (CSM6 MACs only)
- Vrouter support for L2TP and ClearTCP
- DVS Tunnel Local Authentication
- Compressed CVX .dra binaries

New Features

X.75 Dial-In Support for ISDN (LAPB)

X.75 dial-in support is implemented for the German ISDN dial-in remote access market. “X.75”, as used here, refers specifically to layer two of the protocol (LAPB). The following are supported:

- Auto-detection of X.75 calls, versus Synchronous PPP calls in ISDN B-channel
- PPP over X.75
- ClearTCP over X.75
- Auto-detection of PPP versus TTY connection over X.75
- Shell login over X.75
- Call type override for configuring X.75 VPOP

You may see X.75 references in statistics for this release. For example:

```
CVX>show session table

 sess Id L1 DS1 DS0 L2         type  stat      IP address    Called# username
00000001  9   0   0  9     ethernet activ  132.245.15.183
00000002  9   0   0  9     ethernet activ      15.2.20.40
00000003  1   1  19  2      isdnX75 inact     15.2.20.170 5082302102  wmcshaw
00000004  1   1  19  2      isdnX75 inact         0.0.0.0 5082302101 cyrus_ow
00000005  1   1  19  2      isdnX75 inact         0.0.0.0 5082302101 cyrus_ow
00000006  1   1  19  2      isdn64K inact     15.2.20.171 5082302102  wmcshaw
00000007  1   1  20  2      isdn64K inact     15.2.20.171 5082302102  wmcshaw
00000008  1   1  21  2     modemV34 inact     15.2.20.172 5082302102    rward
00000009  1   1  22  2      isdnX75 inact         0.0.0.0 5082302101 cyrus_ow
0000000A  1   1  19  2      isdnX75 activ     15.2.20.173 5082302102  wmcshaw
CVX>
```

```
CVX>show session detail A
                    sessionID: 0000000A
                        state: active
                permanentFlag: switched
                        vpopId: 2
                          name: x75
                     remoteIP: 15.2.20.173
                  remoteIPMask: 255.255.255.255
                       localIP: 0.0.0.0
                   localIPMask: 0.0.0.0
                   linkService: isdnX75
                   serviceMode: ppp
                     startTime: 931570
                      stopTime: 0
              timeOfModemSync: 0
                timeOfService: 931573
          terminatingComponent: none
              terminationCause: 0
                 lastComponent: ppp
                    layer1Slot: 1
                    layer2Slot: 2
                  calledNumber: 5082302102
                 callingNumber: 5082366103
                 originateMode: answer
                      octetsIn: 0
                     octetsOut: 0
                     packetsIn: 0
                    packetsOut: 0
                   multiLinkId: 00000000
                          port: 1
                      timeslot: 19
                     linkCount: 1
               txStartDataRate: 64000
               rxStartDataRate: 64000
                 txEndDataRate: 64000
                 rxEndDataRate: 64000
                 txMinDataRate: 64000
                 rxMinDataRate: 64000
                 txMaxDataRate: 64000
                 rxMaxDataRate: 64000
                           iop: 1
                           dmm: 0
                          pack: 0
                        device: 1
                     tdmStream: 0
                   tdmTimeSlot: 0
             terminationReason: n/a
```

```
                    duration: 182
                 durationHMS:      0:03:02.000
               ss7SessionId: 00000000000000000000
                modemNumber: 1
                 tunnelType: none
            tunnelMediumType: unknown
         tunnelServerAddress: 0.0.0.0
                   callClass: 0
                  tandemPort: 0
              tandemTimeslot: 0
              callClassArray:
                callClassLen: 0
            actualAuthMethod: local
             ModemModulation: None
        ModemErrorCorrection: None
        ModemDataCompression: None
               ModemTxBlocks: 0
           ModemRetransmits: 0
                   ModemSNR: 0
         ModemLocalRetrains: 0
        ModemRemoteRetrains: 0
     ModemLocalRenegotiations: 0
    ModemRemoteRenegotiations: 0
        ModemReceiveLineLevel: 0
             cleartcpRemoteIP: 0.0.0.0
          cleartcpRemotePort: 0
                   tunnelId: 00000000
                     linkId: 00000000

CVX>show session vpop 2
 Datalink   Transport   Current     Total    Current-ELPT   Total--ELPT
 Call-Type   Protocol  Sessions   Sessions    HOURS:MN:SC   HOURS:MN:SC
 ---------  ---------  --------  ----------  ------------   -----------
     other      setup         0           0       0:00:00       0:00:00
     other      other         0           0       0:00:00       0:00:00
     other      trunk         0           0       0:00:00       0:00:00
     other        ppp         0           0       0:00:00       0:00:00
     other   cleartcp         0           0       0:00:00       0:00:00
     other  tunnelled         0           0       0:00:00       0:00:00
     trunk      setup         0           0       0:00:00       0:00:00
     trunk      other         0           0       0:00:00       0:00:00
     trunk      trunk         0           0       0:00:00       0:00:00
     trunk        ppp         0           0       0:00:00       0:00:00
     trunk   cleartcp         0           0       0:00:00       0:00:00
     trunk  tunnelled         0           0       0:00:00       0:00:00
     modem      setup         0           1       0:00:00       0:00:17
     modem      other         0           0       0:00:00       0:00:00
```

```
modem      trunk         0           0       0:00:00       0:00:00
modem        ppp         0           1       0:00:00      64:04:30
modem   cleartcp         0           0       0:00:00       0:00:00
modem  tunnelled         0           0       0:00:00       0:00:00
 isdn      setup         0           2       0:00:00       0:00:00
 isdn      other         0           0       0:00:00       0:00:00
 isdn      trunk         0           0       0:00:00       0:00:00
 isdn        ppp         0           2       0:00:00      91:41:21
 isdn   cleartcp         0           0       0:00:00       0:00:00
 isdn  tunnelled         0           0       0:00:00       0:00:00
 v110      setup         0           0       0:00:00       0:00:00
 v110      other         0           0       0:00:00       0:00:00
 v110      trunk         0           0       0:00:00       0:00:00
 v110        ppp         0           0       0:00:00       0:00:00
 v110   cleartcp         0           0       0:00:00       0:00:00
 v110  tunnelled         0           0       0:00:00       0:00:00
 v120      setup         0           0       0:00:00       0:00:00
 v120      other         0           0       0:00:00       0:00:00
 v120      trunk         0           0       0:00:00       0:00:00
 v120        ppp         0           0       0:00:00       0:00:00
 v120   cleartcp         0           0       0:00:00       0:00:00
 v120  tunnelled         0           0       0:00:00       0:00:00
  x75      setup         0           2       0:00:00       0:00:00
  x75      other         0           0       0:00:00       0:00:00
  x75      trunk         0           0       0:00:00       0:00:00
  x75        ppp         1           2       0:04:19       0:04:50
  x75   cleartcp         0           0       0:00:00       0:00:00
  x75  tunnelled         0           0       0:00:00       0:00:00
```

V.110 Rate Adaptation Support

V.110 rate adaptation is supported for 14.4 and 28.8 kbps enhanced data rates. Specific supported functions include:

- V.110 14.4 and 28.8 kbps in the CVX switch through the PRI ISDN signaling
- V.110 14.4 and 28.8 kbps in the CVX switch through SS7
- The IOP interface to modems for 14.4 and 28.8 kbps speeds
- CallType override in VPOP configuration

In addition to the above, statistics correctly display the speeds where needed.

V.92 support for modems (CSM6 MACs only, for this release)

Although *V.92 modem code is not included in this release*, the 4.1 release is V.92 ready. V.92 modem code is available for Beta testing, and has the following new features:

- **QuickConnect** gives reduced modem handshake time, resulting in up to 40% faster connections, by remembering call setup details of the previous call. Remembered details include digital impairments, channel frequency response, and other characteristics that determine modulation and initial connect speed.
- **Modem-On-Hold** allows the user to resume their connection to the Internet without re-authentication or modem negotiation after taking or placing a voice call.

You may see V.92 references in statistics for this release. For example:

```
CVX> show session detail
             linkService: modemV92
             serviceMode: ppp
    terminatingComponent: ppp
       terminationReason: Remote user closed LCP
         modemModulation: V90
    modem ataCompression: V44

CVX> show modems session
connectString:                          CONNECT 57600/V92/LAPM/V44/54667:TX/24000:RX
disconnectReason:                       Normal Local Hangup
retrain/reneg reason:                   None
modulation protocol:                    V90 (234)
EC/DC protocols:                        LAP-M/V44
SNR value:                              -7.0 dB
SNR min/max:                            -7.0 dB/-7.0 dB
retrains local/remote:                  0/0
Remote V92 capability:                  Yes
Handshake time (secs):                  10
V92 fallback to V90?                    No
Is Quick Connect attempted?             Yes
Is the call connected with Quick Connect? Yes
Modem On Hold sessions requested:       0
Granted Modem On Hold sessions:         0
```

Note: For installation and configuration information for V.92, see the *V.92 Modem Code Upgrade and Release Notes* (NTP 296-1011-233).

```
CVX> show modems call

Collecting modem statistics...done.

Found 408 modems in 2 slots.  Summary of modems by slot:
--------------------------------------------------------------------------------
Slot Modems |   Calls  Connect Auth | V.90   K56  V.34  V.32  V.92  ErrC  Comp
--------------------------------------------------------------------------------
   4    204 |      13    100%   92% |  92%    7%    0%    0%    0%  100%  100%
   6    204 |      19     94%   89% |  77%    5%   16%    0%    0%  100%  100%
--------------------------------------------------------------------------------
 All    408 |      32     96%   90% |  83%    6%    9%    0%    0%  100%  100%
--------------------------------------------------------------------------------
Type 'show modems ?' for help on detailed modem displays.
```

Note: V.92 references may also be seen in show_session_table and show_session_log.

PCM Upstream is also part of the V.92 protocol, but is not not supported in the first round of V.92 code.

V.44 support for modems (CSM6 MACs only)

This feature is not visible to the user and there are no new parameters.

V.44 uses a new compression scheme that compresses HTML (and other data with similar patterns) for faster downloads. The result is an average of 30-40% faster throughput over older algorithms.

V.44 is a third compression scheme, supplementing use of ITU standard V.42bis and the old MNP scheme.

You will see V.44 references in statistics for this release. For examples, see "V.92 support for modems (CSM6 MACs only, for this release)" on page 2-6.

Note: Although V.44 may appear in the same examples used for V.92, it is not tied to V.92. Either may be implemented independent of the other.

Note: Due to hardware limitations, V.44 will not be supported on the CSM3 MAC cards.

Vrouter support for L2TP and ClearTCP

The CVX switch previously supported the use of vrouters for PPP calls, but now also supports L2TP and ClearTCP calls. This eliminates the need to add routes for L2TP and ClearTCP in the default routing table.

All traffic for an L2TP or ClearTCP call will be routed using the vrouter specified in the VPOP for the call. In addition, all RADIUS traffic for the call will also be routed using the vrouter.

The vrouter will work with whatever network type is used to connect the CVX switch to the wholesale customer's network, including frame relay and Ethernet.

For configuration of vrouters, see "Configuring the IP_Vrouter Objects" (page 5-29), in the *CVX Multi-Service Access Switch Configuration Guide*.

Note: Before the changes in vrouter functionality, RADIUS traffic was routed using the default router and not the vrouter for the VPOP. With the changes made in the vrouter functionality, RADIUS traffic is now sent using vrouters. Changes may be required in the default routing table and vrouter routes. The vrouter configured for a VPOP should have routes which allow it to get to the RADIUS servers used for the VPOP.

Add a route to the vrouter that points to the interface that the RADIUS server in question is on. It need only be a host route, if the only destination is the RADIUS server, or it can be a wider route, if necessary. If the RADIUS server is on the same segment as the CVX interface, the next hop value of the route can be anything on that segment, and is best set to the RADIUS server itself.

DVS Tunnel Local Authentication

This release supports the DVS Local Authentication feature on the CVX switch. This feature is not visible to the user and there are no new configuration parameters on the CVX switch. DVS local Authentication is enabled by using the enhanced support for the DVS CPM (Radius) return list attribute, Annex-User-Server-Location. When DVS Local Authentication is configured, the second DVS user authentication now goes to a locally configured authentication server, as defined on the CVX switch, instead of a remote user authentication server, as defined by the returned tunnel attributes.

DVS Local Authentication still uses the DVS two-step user authentication process. The first user authentication (after pre-auth, if enabled) identifies the user as a DVS user, with the CPM (Radius) server returning DVS tunnel attributes. The attribute Annex-User-Server-Location can now return one of three valid values: 0 for none, 1 for local, or 2 for remote. (Previously only 0 and 2 were supported). If a value of 1 is returned for Annex-User-Server-Location, any remote authentication attributes also returned are ignored.

For the second user authentication, the CVX switch now uses a locally configured authentication server. This authentication server is configured on the CVX switch like any other local authentication server, and referenced via the DVS users configured VPOP. This authentication server must be reachable directly from the CVX switch, and not across any DVS tunnels.

All other DVS tunnel negotiations remain unchanged.

Note: The CPM can be configured for DVS local authentication using the domain-based strategy or the dial-number based strategy.

The following example sets up an ip_aaa_group for CPM.

```
CONFIG> configure system
system> configure ip_services
system/ip_services> configure ip_aaa_remote
../ip_aaa_remote> configure ip_aaa_group 1
/ip_aaa_remote/ip_aaa_group 1> configure ip_aaa_radius_config
../ip_aaa_radius_config> set nas_id hanscvx
../ip_aaa_radius_config> set session_id_style hex
../ip_aaa_radius_config> set session_id_size 32_bit
../ip_aaa_radius_config> commit
../ip_aaa_radius_config> return

../ip_aaa_remote> configure ip_aaa_set 1
../ip_aaa_remote/ip_aaa_set 1> configure ip_aaa_server 1
../ip_aaa_set 1/ip_aaa_server 1> set index 1
../ip_aaa_server 1> set ip_addr 132.245.70.21 ---> CPM address
../ip_aaa_server 1> set ip_port 1645 --> CPM authentication port
../ip_aaa_server 1> set retries 5
../ip_aaa_server 1> set key pw1/7jwat9y
../ip_aaa_server 1> set trace true
../ip_aaa_server 1> commit
../ip_aaa_server 1> return
```

The following example sets up a CVX VPOP to authenticate using the above AAA Group:

```
sessions> configure vpop 1
sessions/vpop 1> configure ppp_modem_config
.../vpop 1/ppp_modem_config> set authserverprotocol1 pap
.../vpop 1/ppp_modem_config> set authserverprotocol2 chap
.../vpop 1/ppp_modem_config> set authclientprotocol1 pap
.../vpop 1/ppp_modem_config> set authclientprotocol2 chap
.../vpop 1/ppp_modem_config> commit
.../vpop 1/ppp_modem_config> return

sessions/vpop 1> configure ppp_isdn_config

.../vpop 1/ppp_isdn_config> set authserverprotocol1 pap
.../vpop 1/ppp_isdn_config> set authserverprotocol2 chap
.../vpop 1/ppp_isdn_config> set authclientprotocol1 pap
.../vpop 1/ppp_isdn_config> set authclientprotocol2 chap
.../vpop 1/ppp_isdn_config> commit
.../vpop 1/ppp_isdn_config> return
```

```
sessions/vpop 1> configure vpop_config
sessions/vpop 1/vpop_config> set authentication_server_group 1
sessions/vpop 1/vpop_config> set authorization_server_group 1
sessions/vpop 1/vpop_config> set accounting_server_group 2
sessions/vpop 1/vpop_config> set auth_method remote_first
sessions/vpop 1/vpop_config> set sourceipaddress 135.234.70.51
sessions/vpop 1/vpop_config> commit
sessions/vpop 1/vpop_config> return
sessions/vpop 1> return
sessions>
```

For dialed-number strategy turn on pre-authentication. For domain-based strategy set up VPOP 0 to handle PAP or CHAP.

Memory Management Improvements

To help debug memory problems, code has been added to track configuration, Gmalloc/gfree, and Pbuf.

Compressed cvx.dra Binaries

The CVX binaries (.els files) are now compressed by approximately a 2:1 ratio. This change ensures that upgrades can easily be performed when using 48MB flash cards. In addition, the upgrade and reboot time is significantly reduced by approximately 50%.

Vinfo runs more slowly on the compressed files. The CLI will print a message indicating the fact that the file is compressed while it is finding the version info.

Unsupported Features

Voice over IP is documented in the customer documentation but is not supported in Release 4.1.

V.92 modem code is not included in this release, but this release will support V.92 modem code when it is available. Of the V.92 features, PCM Uplink will not be supported until a later date.

Configuration Changes Since Release 4.0

Changes and Additions

The following table lists the CVX switch configuration file changes and additions that occurred since Release 4.0. Refer to the *CVX Multi-Service Access Switch Objects and Attributes* for description details.

MIB object identifiers and the MIB path are documented in the *CVX Multi-Service Access Switch Objects and Attributes*.

CLI Path	Add/Change Description
system/ip_services/ip_aaa_remote/ip_aaa_group/ ip_aaa_radius_config>	**Added**: nas_ip_address attribute **Changed:** default from enable to disable for tier1_enable attribute
system/Tunnels/TunnelGroup/DVSGateway>	**Changed**: UserName attribute default from “Up to 64 characters” to “Up to 128 characters”.
sessions/VPOP/hdlc_config>	**Added**: the following attributes to the hdlc_config object: DetectProtocol (true/false, default is true) DetectDefault (ppp/shell, default is shell) DetectTimeout (range of 500 to 30000, default is 3500)
system/ip_vrouter	**Changed**: ip_vrouter object range from “1 to 65535” to “1 to 32”.

CLI Path	Add/Change Description
sessions/session_table_format>	**Added**: the following values to the linkService option under param1 through param10 attributes: • isdnX75 • modemV92 the following value to the ModemDataCompression option under param1 through param10 attibutes: • V44
sessions/VPOP/call_type_override>	**Added**: the following options to presented_call_type attribute: • V110_ASYNC_14400 • V110_ASYNC_28800 • X75_64K • X75_56K the following options to override_call_type attribute: • V110_ASYNC_14400 • V110_ASYNC_28800 • X75_64K • X75_56K
sessions/VPOP/vpop_config>	**Changed**: valid range of vrouter_id attribute is now “0 to 32”.
system/ip_services/ip_service>	**Changed**: valid range of ip_dns_ns is now “0” to “2”

Route Aggregation for IP Pools

Note: The information in this section is not fully documented in the *CVX 1800 Access Switch Command Reference* for CVX Release 4.0. Use this information in conjunction with your documentation CD-ROM.

The CVX switch applies route aggregation to local IP address pools when possible. Route aggregation is a method of collecting a large number of host routes into one encompassing network route to save routing table space and streamline RIP and/or OSPF updates.

When you set the count attribute (under the ip_address_block object) to an even power of two (that is, **2, 4, 8, 16**, etc.) and set a start attribute which would be the beginning of the associated subnet, the CVX switch converts the IP pool to include a "mask" that encompasses the same address range.

```
 count        mask
-----   ---------------
  2     255.255.255.254
  4     255.255.255.252
  8     255.255.255.248
 ...    ...
```

This reduces the availability of one IP address from the pool. This is because the CVX switch can never assign the network address of an IP subnet.

```
CVX> config sessions/vpop 1/ip_pool 1/ip_address_block 1
Entering Configuration Mode
.../VPOP 1/ip_pool 1/ip_address_block 1> set start 10.10.10.1
.../VPOP 1/ip_pool 1/ip_address_block 1> set count 4
.../VPOP 1/ip_pool 1/ip_address_block 1> commit
```

The above example indicates the configuration of four IP addresses available to the users in VPOP 1, IP pool 1.

However, the following **show vpop pool** command output indicates there are only three IP addresses available in VPOP 1, IP pool 1.

```
CVX> show vpop pool
VPOPs:
   # auth-srvr-grp acct-srvr-grp adv-type addr-mode VRtr-id
--- ------------ ------------ -------- --------- -------
   1             0            0 adv-pool remote          0
   pool 1: (PUBLIC)
     blk  start            len  next             free  status
     ---  ---------------  ---  ---------------  ----  --------
     1    10.10.10.1       3    10.10.10.1       3     enabled
```

The free count for this range is 3, even though the count was set to 4. The CVX switch converts the start/count pair to a subnet/mask of 10.1.1.0/255.255.255.252, removing what would be the network address of the next IP subnet, 10.10.10.4, and leaving three IP addresses available for assignment.

If you set the start attribute to the first IP address of a subnet, route aggregation does not occur and the CVX switch does not modify the count attribute.

For example:

```
CVX> config sessions/vpop 1/ip_pool 2/ip_address_block 1
Entering Configuration Mode
.../VPOP 1/ip_pool 2/ip_address_block 1> set start 10.10.10.8
.../VPOP 1/ip_pool 2/ip_address_block 1> set count 4
.../VPOP 1/ip_pool 2/ip_address_block 1> commit
```

The above example indicates the configuration of four IP addresses available to the users in VPOP 1, IP pool 2. The following **show vpop pool** command output indicates there are four IP addresses available in VPOP 1, IP pool 2.

```
CVX> show vpop pool
VPOPs:
   # auth-srvr-grp acct-srvr-grp adv-type addr-mode VRtr-id
--- ------------ ------------ -------- --------- -------
   1             0            0 adv-pool remote          0
   pool 2: (PUBLIC)
     blk  start            len  next             free  status
     ---  ---------------  ---  ---------------  ----  --------
     1    10.10.10.8       4    10.10.10.8       4     enabled
```

Creating IP Pool With Route Aggregation

There are two methods for creating an IP pool with route aggregation on the CVX switch:

- Using the start/mask method
- Using the start/count method

The following examples show a configuration that allows the CVX switch to aggregate IP pools when required.

Note: To configure the CVX switch to aggregate IP pools when required, set the route_advertise attribute (at the path *sessions/VPOP/vpop_config*) to **advertise_pool.**

The following Example 1 and 2 configurations both result in the CVX switch assigning the first IP address of 10.10.10.1 to dial-in users as shown in the outputs of the **show routes** command.

Example 1- Using the Start/Mask Method

```
.../VPOP 1/ip_pool 1/ip_address_block 1> show
   Members currently configured at this level:
             start 10.10.10.1
             count 0
             mask 255.255.255.252
             range_in_use false
             admin_status enabled


CVX> show routes
Routing table display

IP Routes:
D = default, P = private, I = internal, E = external
D           0.0.0.0/0  cid 1   gw 192.168.1.2     igp   static/low    1
         10.10.10.0/30 cid 100                    igp   static/high   1
P      192.168.1.0/24  cid 1                      igp   local cfg     1
```

Example 2- Using the Start/Count Method

```
.../VPOP 1/ip_pool 1/ip_address_block 1> show
   Members currently configured at this level:
             start 10.10.10.1
             count 4
             mask 0.0.0.0
             range_in_use false
             admin_status enabled


CVX> show routes
Routing table display

IP Routes:
D = default, P = private, I = internal, E = external
D           0.0.0.0/0  cid 1   gw 192.168.1.2     igp   static/low    1
         10.10.10.0/30 cid 100                    igp   static/high   1
P      192.168.1.0/24  cid 1                      igp   local cfg     1
```

Creating IP Pool Without Route Aggregation

The following is an example of an IP pool configuration where the CVX switch does not use route aggregation, as shown in the output of the **show routes** command.

Example - Using the Start/Count Method

```
.../VPOP 1/ip_pool 1/ip_address_block 1> show
   Members currently configured at this level:
             start 10.10.10.7
             count 4
             mask 0.0.0.0
             range_in_use false
             admin_status enabled


CVX> show routes
Routing table display

IP Routes:
D = default, P = private, I = internal, E = external
D           0.0.0.0/0  cid 1   gw 192.168.1.2     igp   static/low    1
         10.10.10.7/32 cid 100                    igp   static/high   1
         10.10.10.8/32 cid 100                    igp   static/high   1
         10.10.10.9/32 cid 100                    igp   static/high   1
        10.10.10.10/32 cid 100                    igp   static/high   1
P      192.168.1.0/24  cid 1                      igp   local cfg     1
```

Chapter 3
Corrected Problems

BEP Corrected Problems

This table contains a brief description of each Change Request (CR) completed for this CVX switch release for the BEP.

CR Number	Category	Release Note
Q00047989	BEP	The CVX BEP no longer goes into event logging loop when secondary BEP fails during file syncing. The event logging loop depleted BEP memory and caused it to crash with “DMM unable to allocate memory” panic reason.
Q00047983	BEP	The CVX BEP no longer goes into reboot loop when it crashes.
Q00047853	BEP	The CVX CLI command “CrashBEP” now reliably crashes BEP.

FEP Corrected Problems

This table contains a brief description of each Change Request (CR) completed for this CVX switch release for the FEP.

CR Number	Category	Release Note
Q00046305	FEP	The CVX FEP will no longer hang due to a race condition in TCP code.
Q00047654	FEP	The CVX FEP will no longer crash when incorrectly formatted pbufs are received from MAC.
Q00047729	FEP	A telnet hang caused by pre-maturely releasing telnet UDP port is now fixed. This type of telnet hang was caused by S-Monitor and NMAP scripts.

CR Number	Category	Release Note (continued)
149219-1	FEP	The FEP no longer crashes when more than three DNS servers are configured. Previously, there was no limit enforced by configuration, which caused memory corruption. Now, the number of DNS servers has been limited to three. If more than three DNS server are configured, error messages are written to the event logs while the system is rebooting. Valid container IDs are 0, 1, and 2.
148309-1	FEP	The core dump utility now copies the full 64MB of memory when doing a core dump on the SCC-II. Prior to this release, the core dump utility occasionally dumped only 32MB.
147538-1	FEP	A Telnet hang caused by the NMAP port scan utility has been corrected.
147447-1	FEP	The FEP no longer crashes when the input and output queues do not release allocated memory.
147209-1	FEP	The CVX now sends Ascend Multilink attributes (Ascend-Multilink-ID and Ascend-Num-In-Multilink) in an accounting stop request only if multilink is enabled.
146871-1	FEP	The Ethernet will no longer show sluggishness due to DNS. The problem was caused by the invalid use of UDP ports.
146478-1	FEP	The Ascend dictionary file is now imported into the aptis.dct file.
146196-2	FEP	The FEP no longer crashes with the message "DMM: unable to allocate memory." The queue size for syslog messages has been limited, and DTRACE calls have been removed from the syslog function.
146172-1	FEP	The FEP no longer hangs when receiving unknown types of MobileIP packets, which caused it to run out of size0 pbufs. This problem was caused by a denial of service attack.
146162-2	FEP	A Telnet hang caused by race conditions when running the NMAP port scan utility repeatedly has been corrected.
146062-1	FEP	The FEP no longer crashes when issuing the command **radius -v 89 -c 30**. The use of this command caused the FEP to reference an uninitialized RADIUS tracing structure.
146041-1	FEP	The FEP no longer hangs during a Telnet session while a CLI task is waiting for user input. A 30-minute timer has been added to clear the wait state.
145581-1	FEP	The SCC-I is now compatible with the 64MB 96-modem CSM6 MAC card (NTDY40KA). Prior to this release, the FEP reported "Invalid link ID" after taking 128 calls.
145426-1	FEP	The FEP no longer crashes due to the disabling of an Ethernet port which allowed associated pointers to persist.

CR Number	Category	Release Note (continued)
145417-2	FEP	The FEP no longer crashes in the Ethernet driver code. The problem occurred when two processes tried to access a structure at the same time, causing memory corruption.
145307-3	FEP	The FEP no longer crashes during FTP due to a problem with the TCP idle timer. The socket level timeout was reduced to one minute.
144944-1	FEP	The CVX no longer displays the "No Server" message on the FEP console when there is no accounting server.
144884-2	FEP	The FEP no longer crashes due to excessive memory being consumed by L2F-related events. The number of events per L2F tunnel has been reduced to 256.
144882-2	FEP	The CVX now takes into account variable length subnet masking while making updates to the routing table.
144866-1	FEP	The FEP no longer crashes due to memory corruption caused by an increase in banner length.
144862-1	FEP	The FEP no longer crashes when printing large amounts of data collected in an rsh RADIUS query. A short delay has been added while printing data.
144646-2	FEP	VPOP Strategy Organization Name will now work with the OutputStyle set to **name** and the VPOP_config parameter address_mode set to **local**. New parameters have been added for this release.
144521-2	FEP	The **show access-list** command now properly displays the access-lists in a sorted order.
144468-2	FEP	During configuration, the CVX now reports an error if an alphanumeric character is entered when an integer is expected.
144355-2	FEP	The CVX switch no longer allows the configuration of vrouters with an id greater than 32. Prior to this release, the vrouters could be configured with an ID greater than 32, but were ignored.
144272-3	FEP	The CVX switch no longer reports 100% CPU utilization caused by one CLI task. Associated socket and shell sessions are now properly cleaned up.
144095-2	FEP	The FEP no longer crashes under high OSPF loads. The problem occurred when two processes tried to access a global data structure at the same time. Conditions have been added to correctly restore a process state.
144064-2	FEP	During a telnet session, the **vinfo -h** command now properly displays its output. The output was originally directed to the FEP console and appeared to be lost.
143753-2	FEP	The **show t1 slot x ds1 y rfc** command now displays the correct value for the CircuitID field.

CR Number	Category	Release Note (continued)
143183-2	FEP	The FEP no longer crashes with a machine check exception during local authentication due to a null pointer.
143153-2	FEP	In a failed session, the CVX now passes the actual user name in the Accounting Stop packet. It had previously been passed as an unknown user name.
143126-2	FEP	The FEP no longer crashes with a machine check exception while processing a RADIUS RPC message.
143108-2	FEP	The FEP no longer crashes when receiving IP packets with incorrect IP header options.
143007-2	FEP	The CVX switch passes the *nas_ip_address*, rather than the management address, in the RADIUS packet, when the *nas_ip_address* has a value and the nas_id is not set.
142849-2	FEP	Configuration changes to the vrouter parameters are now dynamic. Changes no longer require a reboot.
142772-3	FEP	Truncation of the username during a Telnet session no longer occurs. The UserName attribute maximum length has been increased from 15 characters to 32 characters.
142664-1	FEP	The **show session detail** command now displays the correct number for DVS multilink bundles.
142574-1	FEP	A type of Telnet hang is now prevented by properly releasing allocated resources when sessions are terminated.
142367-2	FEP	The CVX switch now displays the DSx3IntervalTable for all T3 cards during an SNMP walk. Previously, only the first T3 card was displayed.
141746-2	FEP	The FEP no longer hangs when a RADIUS request packet is sent to an incorrectly configured VPOP.
141718-1	FEP	The session manager fields for both called number and calling numbers have been expanded to accommodate 32 digits. The **show session table** command displays all the numbers.
141650-2	FEP	When a new VPOP is assigned to a call by the CPM during preauthentication, the DSByte value will be determined by the new VPOP.
138499-2	FEP	The **vinfo** command now works properly during Telnet sessions, and vinfo's error messages have been clarified.
138376-2	FEP	Two users dialed into the same VPOP can now communicate with one another.

CR Number	Category	Release Note (continued)
137570-1	FEP	Active and inactive DVS sessions are now recognized correctly in DVS-specific CLI commands. Previously, with multilink bundles, all sessions were shown under the dvs active CLI command as inactive when any of the slave links were terminated.
137568-2	FEP	Multilink connections no longer fail after more than two links with bogus VPOP.
136765-2	FEP	The **show modem** command correctly identifies available commands.
136763-2	FEP	The **show ethernet stats all** command now only provides results for existing Ethernet ports. In prior releases, non-existent Ethernet ports were reported as "undiscovered…"
136726-2 139209-1 140416-1	FEP	The **show route** command now displays a complete routing table. Prior to this release, some routes were occasionally missed.
136313-2	FEP	Event filtering now works correctly when a filter is defined for a card in slot 11 through 18. The culprit was a mismatch caused by the difference in the way the card numbers were determined in the filter record and the card source.

MAC Corrected Problems

This table contains a brief description of each Change Request (CR) completed for this CVX switch release that affects the MAC.

CR Number	Category	Release Note
Q00046842	MAC	The MAC no longer crashes when closing ClearTCP calls due to improper calling of tcp_close function or memory block header block corruption.
Q00046251	MAC	The CVX MAC will no longer go into a state causing Ethernet frame discards while handling error conditions.
148799-1	MAC	The MAC no longer crashes due to a corrupt queue pointer caused by a race condition. The resources associated with a session are now freed when the session is cleared.
148616-1	MAC	The MAC no longer crashes due to race conditions caused by ClearTCP sessions running over the X.75 interface. Instead of clearing the resources in three steps, all resource associations are now cleared at the same time, preventing the race condition.

CR Number	Category	Release Note (continued)
148123-1	MAC	The problem of the MAC crashing while bringing up 1,344 L2TP calls was corrected by masking interrupts before checking the value of a session pointer.
146882-1	MAC	The MAC no longer crashes due to queuing race conditions which caused over-allocation of ClearTCP sessions. ClearTCP was creating new sessions after the maximum number of sessions had already been reached on the MAC.
146872-1	MAC	The MAC no longer crashes due to a watchdog timer expiration. This was caused by receiving prolonged bursts of data from the SCC. It was corrected by adding a limit on the number of frames to be processed in a continuous transmission.
146672-1	MAC	The MAC no longer hangs while receiving data during error conditions. The hang condition caused Ethernet frames to be discarded.
146304-1	MAC	The MAC no longer crashes with an "ipstub session exhausted" error. The number of sessions was extended from 256 to 408. Also, the allocation and freeing of new sessions are now synchronized to avoid a race condition.
146159-2	MAC	The MAC no longer crashes due to bad packet length calculated by the Compression Control Protocol (CCP) decompressor.
146042-1	MAC	Modems will no longer hang and cause repeated "Fail to Awaken" termination codes. Modems were hanging because the IOP image was issuing modem commands without waiting for the modem to be fully disconnected after terminating the previous call.
145738-1	MAC	Multiple IOP reboots in L2TP environments no longer cause the MAC to crash. L2TP failed to fully release the MAC's memory when an IOP crashed or was manually rebooted. This condition depleted the memory pool on the MAC, eventually leading to the crash.
145341-1	MAC	VJCompression of packets with identical IP identification fields is now handled properly. Users of Prodigy's Odigo 3.0 instant messaging no longer have problems contacting the server.
145241-1	MAC	Termination causes are correctly encoded in the MIP DVS tunnel deregistration, link down packets, and accounting stop requests.
145096-2	MAC	The MAC no longer crashes due to memory allocation failures while creating an IP access list.
144827-3	MAC	The MAC no longer crashes after more than 64 DVS multilink sessions are closed.
144661-3	MAC	ClearTCP now supports up to 204 sessions for double-density MAC cards.
144415-2	MAC	The CVX no longer writes multiple core dump files for a single failure on a MAC. Events are now logged for crashes and core dumps.

CR Number	Category	Release Note (continued)
144383-3	MAC	The maximum number of terminated L2TP sessions kept in the log buffer has been reduced from 256 to 128 to increase available memory.
144323-3	MAC	The MAC no longer crashes due to race conditions in queing routines while under a heavy ClearTCP load.
144252-3	MAC	A timer has been added before the end of a ClearTCP session to give enough time to tasks to perform a proper cleanup.
144028-2	MAC	The MAC no longer crashes under extreme load conditions. The crash occurred because of an announcement queue overflow caused by queue service delays.
143466-3	MAC	The MAC no longer hangs or crashes when there is traffic stalled in the transmit (Tx) direction. The hang resulted in the failure to forward traffic to the IOPs or the failure to report statistics, and associated crashes were caused by the watchdog timeout.
143236-2	MAC	The MAC no longer crashes when message processing takes too long, causing the watchdog timer to expire.
137818-2	MAC	The **card dry** command now brings the MAC down after all sessions have terminated. Previously, the card was not brought down when multilink calls were involved.
137601-2	MAC	The CVX switch now sends the Field Inspection Notice (FIN) and ACK at the end of the ClearTCP session, which allows the session to properly terminate.
136827-6	MAC	The MAC no longer hangs due to resource depletion. Data movement on the MAC in both Tx and Rx directions are no longer stalled.
136382-4	MAC	Host modems no longer become permanently hung (non-responsive) and report "fail to awaken modem" termination codes until the MAC is rebooted. Modems in a hung state are now reset and restored without user intervention.

DAC Corrected Problems

This table contains a brief description of each Change Request (CR) completed for this CVX switch release that affects the DAC.

CR Number	Category	Release Note
Q00046695	DAC	Individual E1 will no longer bounce and go into red alarm. Hardware jitter attenuation is now turned on the receive side which reduces noise on the line.
146827-2	DAC	The CVX will not drop calls under heavy load. The CVX was rejecting RBS calls if the call was coming in on a line that was still recovering from a previous call.
145715-2	DAC	The DAC FP no longer crashes when a process exits. The order in which memory was freed when the process exited was changed.
143625-2	DAC	The interface ID under the Q.931 standard is now properly calculated.
142958-2	DAC	The DAC-II DS3 RLTMs (NTDY39BB) now correctly report statistics and errors.
141137-4	DAC	The ds1 index mapping of E1/R2 calls on DS0s greater than channel 15 now correctly maps on the Rx TDM stream. This allows for a complete data path between the client modem and the CVX modem.
136302-2	DAC	The DAC no longer generates traps after being disabled administratively.

Chapter 4
Known Problems and Limitations

SCC-II Warning

Warning: Use ONLY the Release 3.6 or later software with the SCC-II. (Ref: SR 60327405)

DO NOT USE any CVX software release lower than 3.6 or damage to the SCC-II will result. DO NOT COPY pre-3.6 versions of CVX software to any flash card installed in an SCC-II. If a CVX switch boot is attempted, the CVX switch will become nonfunctional until the corrupt SCC-II is removed and forwarded to Nortel Networks for reprogramming and returned to the customer site. The 3.6 software supplied with the SCC-II is required for normal operation.

If you wish to load a release prior to 3.6 with the SCC-II, you must install an SCC-I and its corresponding LTM before using the older CVX software.

Table of Known Problems

CR Number	Description
5335	Permanent virtual circuits are listed as active instead of active-wait when they are disconnected from the far end router. Also, the ARP table has only the first entry correct for the Frame Relay information.
139208-1	OSPF routes are not summarized when an OSPF Range is configured.
139248-1	When using local authentication in VPOP 0/ppp_modem_config, if you set AuthServerProtocol1 to CHAP and AuthServerProtocol2 to PAP, AuthServerProtocol2 never goes down to PAP and the connection fails. To work around this, set AuthServerProtocol1 to PAP and AuthServerProtocol2 to CHAP.
139252-1 139253-1	Attempts to configure and walk the following Aptis-Monitoring MIBs have been unsuccessful: pppDeadLogEntryTable pppDeadSessionStatsTable dvsStatusDeadTable L2FLinkStatusTable L2FLogEntryTable
139257-1	The SNMP Get Bulk action returns results for 100 instances regardless of the table being queried.
139259-1	The **session components** command and an SNMP walk of **sessioncomponentsIndex** display different counts. The counts for both should be the same.
139260-1	A MIB walk of sessionTraceTable in the Aptis-monitoring MIB displays information for the first session only.
139274-1	Session Detail Timestamps Do Not Contain Clock Time The following session attributes show a value representing the number of seconds relative to system start time, instead of showing actual clock time (date and time): startTime stopTime timeOfModemSync time OfService
147737-1	The **show modems** command fails to find modems with an IOP of 3 and a DMM of 6. For example, **show modems 13/3/6/2/3** does not display performance information about slot 13/IOP 3/DMM 6/pack 2/modem 3.
149443-1	When CPM is configured for monitor mode and the primary CPM server is not available, the FEP will crash during pre-authentication of a dial up client.

Known Limitations in Release 4.1

The following are descriptions of the known limitations of the CVX Multi-Service Access Switch.

Open Shortest Path First (OSPF)

Note: CVX switch operating as an autonomous system boundary router (ASBR) within a not-so-stubby area (NSSA).

Note: IP Pools within the CVX switch are flooded through the OSPF area as type 2 external routes. The CVX switch must be configured as an ASBR in order to propagate the IP pools. To reduce the number of LSA's generated by a CVX switch, all IP pools configured on that switch should consist of a subnet address and a mask rather than a starting address and a count. In addition, the route_advertise parameter in the CVX switch configuration under *sessions/ vpop #/vpop_config* must be set to **advertise_routes.** This ensures that IP pool addresses are summarized into one LSA per pool rather that one LSA per individual host address.

Limitations on Configurations

The following are known OSPF limitations for the CVX switch:

- There is a limit of 15 on the maximum number of adjacencies reliably supported.
- The link state database can be no greater that 300 link state advertisements (LSAs).

- The following chart shows the relationship between supported LSA routes and neighbors within an OSPF area. This chart is valid for all SCC hardware.

Number of Neighbors in Area	Number of LSA Routes per host
1	300
2	150
3	100
4	75
5	60
6	50
7	42
8	37
9	33
10	30
11	27
12	25
13	23
14	21
15	20

Unsupported OSPF Items

The following OSPF items are not supported for this release:

- CVX switch operating in stub areas or as part of backbone area 0
- CVX switch configured as a designated router (DR), area border router (ABR), or backup designated router (BDR)
- OSPF range parameters ip_ospf_range
- Virtual links parameters, including auto_virtual_link_enabled and ip_ospf_virtual_link
- OSPF commands associated with an ABR or ASBR generating default routes: generate_default_enabled, generate_default_metric, and generate_default_metric_type

- Stub area related parameters under ip_ospf_area: stub_area_enabled set to true, stub_area_default_cost, and stub_area_no_summary_enabled

Dynamic Configuration of Frame Relay (CR 139241)

When you configure an IP interface, the changes should be dynamic. The only way to effect the changes has been to use a reboot.

Dynamic configuration of Frame Relay requires an orderly startup. FEP memory will be depleted if the Frame Relay configuration is not edited in a certain sequence. This happens when you change and **commit** the *FrLogicalIF 1/ ip_interface/ip_ifnumber/if_index* member value after committing the *ip_circuit* members.

Make sure the order of committing configuration changes is done in the order of containers in the FR hierarchy. The only exception is that the *FrLogicalIF_config/ frLIFenable* member should be set to **enable** when all Frame Relay containers and members are present and set to the desired values.

The following procedure explains how to configure Frame Relay for port 1 on a T1 interface. For other Frame Relay configuration procedures, see the *CVX Multi-Service Access Switch Startup Guide*. For detailed descriptions of the commands used in these instructions, see the *CVX Access Switch Objects and Attributes*.

Example: Configuring Frame Relay for Port 1 on a T1 Interface

The following CLI session configures Frame Relay on a CVX switch using T1 ports on two SCC-LTM-T1 cards. Use the following detailed CLI session to configure T1 port 1, or go to the CLI Path Summary at the end of this procedure. The CLI Path Summary shows a summary of the commands that you enter in this procedure. Repeat this process to configure T1 port 2.

Notes:

1. All IP addresses shown in these instructions are examples only. Do not use them in your configuration.

2. Do not confuse the **return** command with the [Return] key on the keyboard. You must type the word “return” on the command line.

Step	Action

1	Go to the T1 level of the CLI hierarchy.
	
	`CVX> config`
	`Entering Configuration Mode`
	`CONFIG> configure shelf 1/slot 9/scc/bic/t1 1`

2	Enter the configure leasedline and configure virtuallink commands. The number that you enter following the **configure virtuallink** command is the T1 port number. Only one virtual link is allowed for each T1.
	
	`shelf 1/slot 9/SCC/BIC/T1 1> configure leasedline`
	`.../BIC/T1 1/LeasedLine> configure virtuallink 1`
	`.../BIC/T1 1/LeasedLine/VirtualLink 1>`

3	**Enter the configure frinterface command, followed by a number.** The number following the **configure frinterface** command is the virtual link port number. Only one FrInterface per virtual link is allowed. `.../T1 1/LeasedLine/VirtualLink 1> configure frinterface 1`

4	**Enter the configure frinterface_config command to access and set the Frame Relay configuration parameters.**
	
	The **set frDlcmiLMIType** command used in this step specifies the data link connection management identifier (DLCMI) scheme on the Frame Relay interface. Your carrier can tell you which DLCMI type to specify.
	
	`.../VirtualLink 1/FrInterface 1> configure frinterface_config`
	`.../FrInterface_config> set frDlcmiLMIType annexd`
	`.../FrInterface_config> commit`
	`.../FrInterface_config> return`
	`.../T1/LeasedLine/VirtualLink 1/FrInterface 1>`

Step	Action

5	**At the FRInterface 1 level of the CLI hierarchy, enter the configure frlogicalif command.**
	
	The number that you enter following the **configure frlogicalif** command is the Frame Relay logical interface number. The number that you enter following the **configure frcircuit_config** command is the number that indicates the DLCI to be used on this interface. You should use unique DLCI values for the entire Frame Relay interface.
	
	`.../VirtualLink 1/FrInterface 1> **configure frlogicalif 1**`
	`.../FrInterface 1/FrLogicalIF 1> **configure frcircuit_config 16**`
	`.../FrInterface 1/FrLogicalIF 1/FrCircuit_config 16> **return**`
	`.../FrInterface 1/FrLogicalIF 1>`

Step	Action

6	Enter the configure ip_interface command to access the IP configuration objects that you need to set for Frame Relay, as follows:
	• ip_ifnumber
	• ip_circuit
	`.../FrInterface 1/FrLogicalIF 1> **configure ip_interface**`
	`.../FrLogicalIF 1/ip_interface> **configure ip_ifnumber**`
	`.../FrLogicalIF 1/ip_interface/ip_ifnumber> **set if_index 1**`
	The if_index value is the same as the local_if_index value under ip_route.
	`.../FrLogicalIF 1/ip_interface/ip_ifnumber> **set class protocol**`
	`.../FrLogicalIF 1/ip_interface/ip_ifnumber> **set subclass fr**`
	`.../FrLogicalIF 1/ip_interface/ip_ifnumber> **set instance 1**`
	`.../FrLogicalIF 1/ip_interface/ip_ifnumber> **commit**`
	`.../FrLogicalIF 1/ip_interface/ip_ifnumber> **return**`
	`.../FrLogicalIF 1/ip_interface> **configure ip_circuit**`
	`.../FrLogicalIF 1/ip_interface/ip_circuit> **set ip_index 1**`
	`.../ip_interface/ip_circuit> **set ip_local 134.177.66.21**`
	`.../ip_interface/ip_circuit> **set ip_mask 255.255.255.0**`
	`.../ip_interface/ip_circuit> **set inverse_arp_enabled true**`
	`.../ip_interface/ip_circuit> **commit**`
	`.../ip_interface/ip_circuit> **return**`
	`.../FrInterface 1/FrLogicalIF 1/ip_interface> **return**`
	`.../FrInterface 1/FrLogicalIF 1> **configure frlogicalif_config**`
	`.../FrLogicalIF 1/frLogicalIF_config> **set frLIFEnable enable**`
	`.../FrLogicalIF 1/frLogicalIF_config> **commit**`
	`.../FrLogicalIF 1/frLogicalIF_config> **return**`
	`.../VirtualLink 1/FrInterface 1/FrLogicalIF 1> **return**`
	`.../VirtualLink 1/FrInterface 1> **return**`
	`.../T1 1/LeasedLine/VirtualLink 1>`

Step	Action
7	**Enter the configure virtuallink_config command to access the virtual link parameters.** `.../T1 1/LeasedLine/VirtualLink 1>` **`configure virtuallink_config`**
8	Set the channelenable command to enable, and then return to the virtuallink_config object. `.../VirtualLink 1/VirtualLink_config>` **`set ChannelEnable enable`** `.../VirtualLink 1/VirtualLink_config>` **`commit`** `.../VirtualLink 1/VirtualLink_config>` **`return`**
9	Go back to the T1 level of the CLI hierarchy. Accept the default settings for the T1_trunkconfig configuration object. `shelf 1/slot 9/SCC/BIC/T1 1>` **`configure t1_trunkconfig`** `shelf 1/slot 9/SCC/BIC/T1 1/T1_trunkconfig>` **`commit`** `shelf 1/slot 9/SCC/BIC/T1 1>` **`exit`** `There are outstanding changes to the running configuration: Save the running configuration as the saved configuration? [Y/N]` **`y`** `CVX>`

CLI Path Summary for Setting Frame Relay Parameters for T1 Port 1

```
CVX> config
CONFIG> configure shelf 1/slot 9/scc/bic/t1 1
shelf 1/slot 9/SCC/BIC/T1 1> configure leasedline
.../BIC/T1 1/LeasedLine> configure virtuallink 1
.../T1 1/LeasedLine/VirtualLink 1> configure frinterface 1
.../VirtualLink 1/FrInterface 1> configure frinterface_config
.../FrInterface 1/FrInterface_config> set frDlcmiLMIType annexd
.../FrInterface 1/FrInterface_config> commit
.../FrInterface 1/FrInterface_config> return
.../VirtualLink 1/FrInterface 1> configure frlogicalif 1
.../FrInterface 1/FrLogicalIF 1> configure frcircuit_config 16
.../FrInterface 1/FrLogicalIF 1/FrCircuit_config 16> return
.../FrInterface 1/FrLogicalIF 1> configure ip_interface
.../FrLogicalIF 1/ip_interface> configure ip_ifnumber
.../FrLogicalIF 1/ip_interface/ip_ifnumber> set if_index 1
.../FrLogicalIF 1/ip_interface/ip_ifnumber> set class protocol
.../FrLogicalIF 1/ip_interface/ip_ifnumber> set subclass fr
.../FrLogicalIF 1/ip_interface/ip_ifnumber> set instance 1
.../FrLogicalIF 1/ip_interface/ip_ifnumber> commit
.../FrLogicalIF 1/ip_interface/ip_ifnumber> return
.../FrLogicalIF 1/ip_interface> configure ip_circuit
.../FrLogicalIF 1/ip_interface/ip_circuit> set if_index 1
.../ip_interface/ip_circuit> set ip_local 134.177.66.21
.../ip_interface/ip_circuit> set ip_mask 255.255.255.0
.../ip_interface/ip_circuit> set inverse_arp_enabled true
.../ip_interface/ip_circuit> commit
.../ip_interface/ip_circuit> return
.../FrInterface 1/FrLogicalIF 1/ip_interface> return
.../FrInterface 1/FrLogicalIF 1> configure frlogicalif_config
.../FrLogicalIF 1/frLogicalIF_config> set frLIFEnable enable
.../FrLogicalIF 1/frLogicalIF_config> commit
.../FrLogicalIF 1/frLogicalIF_config> return
.../VirtualLink 1/FrInterface 1/FrLogicalIF 1> return
.../VirtualLink 1/FrInterface 1> return
.../T1 1/LeasedLine/VirtualLink 1> configure virtuallink_config
.../VirtualLink 1/VirtualLink_config> set ChannelEnable enable
.../VirtualLink 1/VirtualLink_config> commit
.../VirtualLink 1/VirtualLink_config> return
.../T1 1/LeasedLine/VirtualLink 1> return
.../BIC/T1 1/LeasedLine> return
```

```
shelf 1/slot 9/SCC/BIC/T1 1> configure t1_trunkconfig
shelf 1/slot 9/SCC/BIC/T1 1/T1_trunkconfig> commit
shelf 1/slot 9/SCC/BIC/T1 1/T1_trunkconfig> exit
There are outstanding changes to the running configuration: Save
the running configuration as the saved configuration? [Y/N] y
CVX>
```

Alarm State Indication (CR 139219)

If you set the AdminState of a T3 or of an individual T1 in the T3 to **disabled**, the Alarm State displayed by a **show ds1 slot *n*** command incorrectly indicates OK for the disabled T3 or T1.

Accounting Stop Packet (CR 139223)

The Accounting Stop packet functionality should be used specifically for failed connections that specifically have the user name set to Unknown. The Accounting Stop functionality has been incorrectly extended to the RADIUS diagnostics command **radius -a**, causing the packets to be sent to the RADIUS server with user names of Unknown.

CVX-SS7-Session-Id-Type (CR 139231)

The CVX-SS7-Session-Id-Type attribute may appear in accounting stop and start packets.

Login-Service Attribute (CR 139232)

The Login-Service attribute is implemented only for clearTCP connections. The attribute shows up in other instances where it has no relevance, such as in regular PPP calls and L2F/L2TP calls. (For clearTCP connections, the Login-Service value of 2 (TCP Clear) is correct.)

Trunk Value Counting (CR 139250)

After a fresh reboot of the CVX switch, the **show session summary** command displays a Trunk value of 100 percent. When calls are brought into the CVX switch, the percent value changes, eventually decreasing to 0.

Session Accounting (CR 139261)

The **show session vpop 1** command does not account for all sessions. Although a session is generated and is accounted for when you execute the **show session table** command, the session does not appear as a type “Other” call when you execute the **show session vpop 1** command.

File into Wrong Directories (CR 139269)

Multiple ftp sessions to the CVX switch may result in files from one session going to the wrong directory.

Also, multiple telnet and/or ftp sessions through the same ip-address may result in files being placed in the wrong directory.

UDP Checksum (CR 140388)

The CVX switch does not compute a UDP checksum on outgoing packets.

Call_type_override Parameter (CR 145190)

The **call_type_override** parameter is not supported for X.75 sessions.

Entering Commands Through Vshell

If you use Vshell to enter a command such as **ping** on the FEP, you cannot use Ctrl-C to terminate execution of the command. Instead, by pressing Ctrl-C, you exit the FEP and go back to the BEP.

Telnetting from UNIX Platforms

Example of a Telnet connection to the CVX switch from certain UNIX platforms causes the following:

```
Connected to cvx.sample.net.
Escape character is '^]'.
Nortel Networks CVX-1800
login: rroot
password:
CVX>
```

This occurs on the following platforms:Linux Slackware 4.0, Kernel Version 2.2.12, SunOS 4.1.3_U1, SunOS 4.1.4.

Time Counters

The value returned for the object instance of systemTimeFixedBootTime is the number of clock ticks since 1/1/1900.

Table Values Difference

CVX switch MIBs that have tables with instances (for example, systemSummaryTable and systemVersionTable) contain instance values that differ from the table Index value. These values should be the same.

Ascend-Require-Auth Parameter

The Ascend-Require-Auth parameter is not supported.

The **radius trace** command displays the Ascend-Require-Auth parameter (sent from the RADIUS server) as “unknown.” (In the CVX switch, use **preauth radius** for tier 2 authentication.)

The CVX switch does not support this parameter because the CVX switch does not support CLID preauthentication. The functionality of Ascend-Require-Auth is duplicated by Ascend-Recv-Auth, which the CVX switch does support.

Get Command on Multiple Objects

If you issue an SNMP **get** command on multiple objects, for example, sysDescr.0 and sysObjectId.0, sysObjectID.0 returns different results depending on whether you specified it first or not.

If you ask for...	...then...	Results
sysDescr.0	sysObjectID.0	the sysObjectId is returned incorrectly.
sysObjectID.0	sysDescr.0	the sysObjectId is returned correctly.

Buffer Size Limitation for RADIUS Packets

There is a buffer size limitation on the CVX switch for receiving RADIUS authentication packets and creating RADIUS accounting packets. The limitation is 1024 bytes, which includes the 20-byte RADIUS header in addition to RADIUS data (attributes).

Analog PPP Multilink

Analog PPP multilink is only supported over L2TP and L2F.

Multiple Ethernet on Same Subnet

CVX supports a maximum of two Ethernet interface on the same subnet. The routing protocols have to be disabled on those interfaces.

Chapter 5
User Information

Flash Memory Card Contents

The following table lists the files on the CVX Multi-Service Access Switch Release 4.1 flash memory card:

Filename	Description
SYNC.INI	File defining all files requiring synchronization with a redundant SCC. Also defines which files are to be saved in a backup operation.
BOOT.NEW	Updated copy of *boot.ini.* Any customizations in the existing *boot.ini* file should be merged into a *boot.new. Boot.new* should then replace *boot.ini* on the flash card.
BEPBR.ELZ	FELF boot loader for 860 processor (BEP) on SCC
BEPMR.ELS	Runtime image for 860 processor (BEP) on SCC
FEPGR.ELS	Diagnostic image for 603 processor (FEP) on SCC
FEPMD.ELS	Runtime image for 603 processor (FEP) on SCC
FPGD.ELS	Diagnostic image for 603 processor (FP) on DAC
FPMD.ELS	Runtime image for 603 processor (FP) on DAC
IOPBR.ELS	Boot loader for 860 processor (IOP) on MAC
IOPDR.ELS	Preload image for 860 processor (IOP) on MAC
IOPGD.ELS	Diagnostic image for 860 processor (IOP) on MAC
IOPMD.ELS	Runtime image for 860 processor (IOP) on MAC
LPPGD.ELS	Diagnostic image for 603 processor (LPP) on MAC
LPPMD.ELS	Runtime image for 603 processor (LPP) on MAC

Filename	Description (continued)
SPBR.ELS	Boot loader for 860 processor (SP) on DAC
SPDR.ELS	Preload image for 860 processor (SP) on DAC
SPGD.ELS	Diagnostic image for 860 processor (SP) on DAC
SPMD.ELS	Runtime image for 860 processor (SP) on DAC
SIXPACK.MDM	Modem firmware for CSM/6 chipset on MAC
TRIPACK.MDM	Modem firmware for CSM/3 chipset on MAC (SRAM version)
TRIPACKD.MDM	Modem firmware for CSM/3 chipset on MAC (DRAM version)
TRIPACKV.MDM	Modem firmware for CSM/3v chipset on MAC
VINFO.LST	General information about the build, such as where done, time, version, build number
VERSION.TXT	Vinfo data for each image in the bin directory
DTE.HLP	Online help for **edit** command*
*The dte command line editor and the dte.hlp file are written by Douglas Thomson.	

Technical Documentation

Note: CVX release 4.1 uses the 4.0 documentation set, supplemented with these release notes.

For more information about the CVX switch, see the following documents:

- *CVX Multi-Service Access Switch Product Description* (NTP 296-1011-100)
- *CVX 1800 Multi-Service Access Switch Hardware Installation Guide* (NTP 296-1011-200)
- *CVX Multi-Service Access Switch Startup Guide* (NTP 296-1011-210)
- *CVX Multi-Service Access Switch Configuration Guide* (NTP 296-1011-300)
- *CVX Multi-Service Access Switch Objects and Attributes* (NTP 296-1011-305)
- *CVX Multi-Service Access Switch Termination Codes, SNMP Traps, and Events* (NTP 296-1011-320)
- *CVX Multi-Service Access Switch RADIUS Reference* (NTP 296-1011-902)
- *CVX Multi-Service Access Switch Troubleshooting Guide* (NTP 296-1011-901)
- *CVX 600 Multi-Service Access Switch Hardware Installation Guide* (NTP 296-1011-202)
- *V.92 Modem Code Upgrade and Release Notes* (NTP 296-1011-233)

For more information about CVXView, see the following documents:

- *CVXView Network Management Products Release Notes* (NTP 296-1011-230)
- *CVXView Installation and Upgrade Guide* (NTP 296-1011-251)
- *CVXView Administrator's Guide* (NTP 296-1011-340)
- *CVXView Configuration Guide* (NTP 296-1011-310)

- *CVXView NMS Monitoring Guide* (NTP 296-1011-311)
- *CVXView CNM User's Guide* (NTP 296-1011-330)
- *CVX PolicyView User's Guide* (NTP 296-1022-100)

For more information about CVX Policy Manager, see the following documents:

- *CVX Policy Manager Release Notes* (NTP 196-1012-101)
- *CVX Policy Manager User's Guide* (NTP 296-1012-100)
- *CVX Policy Manager Installation Guide* (NTP 296-1012-200)

Technical Support/Customer Service

In the USA: Dial 1-800-758-4827 to contact a Technical Support engineer.

Outside the USA: Contact your Regional Nortel Networks Support Prime.

For information about the Nortel Networks Network Access Division, go to the World Wide Web (WWW) site at http://www.nortelnetworks.com.

Accessing Nortel Networks Documentation and Software Updates

Documentation and software updates are available through the World Wide Web at http://www.nortelnetworks.com. Product information and technical bulletins are available to all customers with valid user accounts. These accounts are provided at the time of system purchase. Access to software upgrades, technical documentation, and other support information is restricted to customers with support contracts. Contact your Nortel Networks account representative for more information about support contracts or gaining access to documentation and software updates.

Equipment Problems

If your equipment is not working properly, you should immediately remove it from the telephone line to prevent any possible damage to the telephone network. If the telephone company identifies a problem, they may notify you prior to discontinuing telephone service. After notification, you will be given an opportunity to correct the problem. You will also be informed of your right to file a complaint with the Federal Communications Commission (FCC).

If repair or modification is required in order for your equipment to operate properly, contact Technical Support. All repairs or modifications must be completed by Nortel Networks or an authorized Nortel Networks representative.

Using the Adobe Acrobat Master Index

The CVX Documentation CD includes a master index for performing full-text searches of all the documents on the CD. To use the index, you must add it to your index selection in Acrobat Reader.

1. Open the Index Selection dialog box:

If you are using...	Then select...
Acrobat Reader 3.0	**Tools > Search > Indexes**
Acrobat Reader 4.0	**Edit > Search > Select Indexes**

2. If no index appears in the Index Selection dialog box:
   a. Click **Add**.
   b. Click the file *Index**Index.pdx*.
   c. Click **Open**.
3. Click the index name in the Index Selection dialog box.
4. Click **OK**.

Note: If the Search feature does not exist in your copy of Acrobat Reader, uninstall your copy and install Acrobat Reader from the CD.

CVX Multi-Service Access Switch

4.1 Release Notes

Printed in the USA

296-1011-220
CVX Multi-Service Access Switch Release 4.1, Document Revision 07.02
May, 2001

NORTEL NETWORKS™