Doc. No. 78-3658-01

CWSI Version 1.0 on AIX Release Note

CiscoWorks for Switched Internetworks (CWSI) Version 1.0 on AIX is a set of three network management applications: CiscoView, VlanDirector, and TrafficDirector. This document contains the release notes for each of the CWSI Version 1.0 on AIX applications and information that applies to CWSI Version 1.0 on AIX product in general. This document contains the following sections:

- Release Notes for CWSI Version 1.0 on AIX
- Release Notes for CiscoView Version 3.1(1) on AIX
- Release Notes for VlanDirector Version 1.1 on AIX
- Release Notes for TrafficDirector Version 3.3 on AIX
- Cisco Connection Online

Release Notes for CWSI Version 1.0 on AIX

This section discusses the following CWSI Version 1.0 on AIX topics:

- Mounting from a Remote CD-ROM Drive
- Documentation Information

Mounting from a Remote CD-ROM Drive

You can install CWSI from a CD-ROM drive attached to your system or from a drive connected to a remote host. However, before installing CWSI from a CD-ROM, you must first use the System Management Interface Tool (SMIT) to mount the local or remote CD-ROM drive on the local AIX system.

This section describes mounting from a remote CD-ROM drive. For information on mounting from a local CD-ROM drive, refer to the *CWSI Version 1.0 on AIX Installation Guide*.

Note If you have already performed this procedure, or if another device is already mounted on the mount point, the following process will fail.

To mount the CD-ROM on the local filesystem from a remote CD-ROM drive, perform the following steps on the remote system to which the CD-ROM drive is physically connected:

Step 1 Log in as root user and start SMIT by entering the following at the command prompt:

```
hostname# smit
```

Step 2 On the System Management menu, select **Physical & Logical Storage**.

Step 3 Select **File Systems** and select **Add/Change/Show Delete File Systems**.

Step 4 Select **CDROM File Systems**.

Step 5 Select **Add a CDROM File System**.

Step 6 Click the "DEVICE name" **List** button and select the device name (such as */dev/cd0*) from the list that appears.

Step 7 In the "Mount point" field, enter the name of a mount point directory (such as */cdrom*).

Step 8 Click **Do**, read the output, and then click **Done**.

Step 9 Terminate SMIT by pressing **F12** or by clicking **Exit SMIT** on the Exit menu.

Step 10 Enter the following at the command prompt:

```
hostname# smit mountfs
```

Step 11 Click the "FILE SYSTEM name" List button and select a device name (such as */dev/cd0*) from the list that appears.

Step 12 In the "DIRECTORY over which to mount" field, enter the name of a mount point directory (such as */cdrom*).

Step 13 Click the "TYPE of file system" **List** button and select **cdrfs** as the file system type.

Step 14 Set the "Mount as Read-Only System" field to **Yes**.

Step 15 Click **Do**, read the output, and then click **Done**.

Step 16 Terminate SMIT by pressing **F12** or by clicking **Exit SMIT** on the Exit menu.

Step 17 At the command prompt, enter **smit mknfsexp**.

Step 18 Enter the "PATHNAME of directory to export" (such as */cdrom*).

Step 19 Using the arrow keys, change the "Mode to Export Directory" field to **read-only**.

Step 20 Enter information, if necessary, into any of the other fields.

Step 21 Click **Do**, read the output, and then click **Done**.

Step 22 Terminate SMIT by pressing **F12** or by clicking **Exit SMIT** on the Exit menu.

After completing the steps on the remote system, perform the following steps on the local system:

Step 1 Log in as the root user.

Step 2 Enter the following command at the command prompt:

```
hostname# mount
remote_hostname:remote_exported_filesystem_name
local_mount_point
```

For example, to mount a remote filesystem name /cdrom from a host named zen, enter:

```
hostname# mount zen:/cdrom /cdrom
```

The CD-ROM is now ready for CWSI to be installed.

Documentation Information

The documentation for CWSI Version 1.0 on AIX includes this release note, and:

- A CD-ROM booklet
- Online help
- VlanDirector User Guide
- TrafficDirector UNIX User Guide

Note The primary documentation for CiscoView on AIX is the online help. If you have feedback about the product or wish to send a query, send e-mail to: *cs-ciscoworks@cisco.com*. To report any problems with documentation, send your comments to *bug-doc@cisco.com*.

Release Notes for CiscoView Version 3.1(1) on AIX

This section includes the following information about the CiscoView Version 3.1(1) on AIX release:

- Supported Cisco IOS Software Features
- Installation and Configuration Results
- Getting Started with CiscoView Version 3.1(1) on AIX
- New Features in CiscoView Version 3.1(1) on AIX
- New Feature Caveats
- Maintaining CiscoView
- Troubleshooting
- CiscoView Version 3.1(1) on AIX Caveats

Note CiscoView Version 3.1(1) runs on AIX 4.1 *in addition* to AIX 3.2.5(1), and optionally with either NetView for AIX 4.1 or 3.1.

Supported Cisco IOS Software Features

This section contains the latest Cisco Internetwork Operating System (Cisco IOS) software version information at the time of printing. New devices and further specifics on Cisco IOS software support will be announced following this release. Refer to the online release notes on Cisco Connection Online (CCO), formerly called Cisco Information Online (CIO), or on the Cisco Connection Documentation, Enterprise Series CD, or Cisco Connection Documentation, CiscoPro Solutions CD, which are both accessible via CCO.

Note The Cisco Connection Documentation, Enterprise Series CD, was formerly called UniverCD and the Cisco Connection Documentation, CiscoPro Solutions CD, was formerly called UniverCD for CiscoPro.

CiscoView Version 3.1(1) on AIX supports Cisco IOS Releases 10.0 through 11.1 with the exception of access servers, which require Cisco IOS Release 10.2.

Specifically, CiscoView on AIX supports the:

- Qualified Logical Link Control (QLLC) feature in Cisco IOS Release 10.3(7) and later and in Cisco IOS Release 11.0(2) and later
- Synchronous Data Link Control (SDLC) feature in Cisco IOS Release 10.2 and later
- Channel Interface Processor (CIP) card in Cisco IOS Release 10.2 and later

Installation and Configuration Results

When you install and configure CiscoView Version 3.1(1) on AIX, the following files are stored in the *$NMSROOT/install/bin* directory where the NMSROOT is set to */usr/nms*:

- Product configuration: *cv_configure*
- Device package install setup: *cv_pkgsetup*
- Device package installation: *cv_incrinstall*

A successful installation and configuration of the CiscoView Version 3.1(1) on AIX product results in the following files being present on your system:

- *$NSMROOT/install/ciscoview.ans*
- *$NMSROOT/bin/nmcview*

Absence of these files on your system indicates that the CiscoView Version 3.1(1) on AIX configuration was unsuccessful.

Getting Started with CiscoView Version 3.1(1) on AIX

This section provides information on getting started with CiscoView on AIX.

Discovering New or Changed IP Devices

The default IP Internet map includes all IP devices connected to NetView when NetView is started. To discover newly added or modified IP devices, use NetView's **Options> Manage Objects** command as follows:

Step 1 Click a device symbol on the default IP Internet map.

Step 2 Select **Options> Manage Objects**. NetView displays a submap of the selected device's children that are reachable in one hop. Newly appearing children could have been added to the network or explicitly unmanaged by a previous user. All newly appearing children devices are now accessible by CiscoView.

Step 3 Select **File> Save Map As** to save the database of devices you created.

For detailed information on how to run **Options> Manage Objects**, refer to the online help.

Using the CiscoView Online Help System

CiscoView's online help satisfies most of your information needs—there is no printed reference manual.

You can access CiscoView online help in the following ways:

- From the **Help** menu within CiscoView. You can select a contents page, a CiscoView overview, or help on the help system itself. Read the help system help for details on keyword searches.
- By clicking the **Help** button or pressing the **F1** key on any CiscoView window. This method presents context-sensitive help.
- By selecting **CW-Applications> CiscoView** on the NetView **Help** menu. This method presents the CiscoView contents page.

New Features in CiscoView Version 3.1(1) on AIX

CiscoView is a graphical user interface (GUI)-based device management software application that provides dynamic status, statistics, and comprehensive configuration information for Cisco Systems' switched internetworking products. CiscoView allows you to display a graphical representation of each network device, display configuration and performance information, and perform minor troubleshooting tasks.

The device packages provided with CiscoView Version 3.1.(1) on AIX software include support for the following Cisco devices:

- Catalyst switch models 1200, 1600, 1700, 2100, 2600, 2800, 3000, and 5000 series.
- Cisco ATM LightStream Switch models LightStream 100 (formerly called the Cisco HyperSwitch A100) running RTOS version 3.1(1) and LightStream 2020 running 2.1(2) and later.
- Kalpana EtherSwitches—EtherSwitch Pro16, EPS-500, EPS-1500, EPS2115, and EPS2015. Kalpana EtherSwitches EPS-500, EPS-2115, and Pro16 are managed by their CiscoPro equivalents: EtherSwitch CPW0500, EtherSwitch CPW2115, and EtherSwitch CPW16 respectively.

Note Refer to the "Switch Firmware" section in "Caveats for Workgroup Products" for firmware versions.

- CiscoPro EtherSwitch models—CPW10/100, CPW16, CPW0500, CPW1200, CPW1400, and CPW2115
- Workgroup Concentrators 1000, 1100, and 1400, and Workgroup FDDI/CDDI Adapters
- Cisco 4000 series (includes the Cisco 4000 and Cisco 4500)
- Catalyst 5000, 1600, and 1200 series running Catalyst software version 1.0 and later; Catalyst 3000 and Kalpana EPS 2015 switches (any firmware)
- Cisco 4000 series running Cisco IOS Releases 9.21 through 10.3, inclusive
- Cisco 2505 and 2507 running Cisco IOS Releases 10.0(6) through 10.3
- Cisco 2501, 2502, 2503, 2504, 2509, 2510, 2511, 2512, 2513, 2514, 2515, and 2516 running Cisco IOS Releases 10.2(1.3) through 10.3

- Cisco 7000 series (includes the Cisco 7000 and 7010) and Cisco 7500 series (includes Cisco 7505, 7507, and 7513) running Cisco IOS Releases 9.21 through 11.0(2)
- The following cards are supported by CiscoView Version 3.1(1) on AIX:
  - npm-4000-fddi-sas(200)
  - npm-4000-fddi-das(201)
  - npm-4000-1e(202)
  - npm-4000-1r(203)
  - npm-4000-2s(204)
  - npm-4000-2e1(205)
  - npm-4000-2e(206)
  - npm-4000-2r1(207)
  - npm-4000-2r(208)
  - npm-4000-4t(209)

Note CiscoView supports the Qualified Logical Link Control (QLLC) feature in Cisco IOS Release 10.3(7) and later, and in Cisco IOS Release 11.0(2) and later.

New Feature Caveats

With CWSI, CiscoView support has been extended for the CPW16, Catalyst 1200, Catalyst 3000, and Catalyst 5000. Support has also been added for the Catalyst 2900. The following are caveats for these devices in CiscoView:

- Catalyst 3000—Because of a bug in the Catalyst 3000 1.0A software, the ATM Virtual Channel Aging menu always displays default values for all three parameters. The changes you make through this menu take effect correctly, but the values read from the device are always the default values.
- Catalyst 5000/2900—Under a heavy load condition, Catalyst 5000/2900 SNMP responses are slow. You might see an “error, no response since....” message in the CiscoView status window. Select **Options>Properties** and increase the Polling Frequency and Timeout values. [CSCdi57962]
- Catalyst 1200, 5000/2900—When using the Switch Zoom menu from CiscoView to view multiple switch ports, the default configuration for the Catalyst 1200 is to configure Statistics, Short-Term History, Long-Term History, and Host group. For the Catalyst 5000/2900, the default configuration is to configure Statistics only. To see the Short-Term or Long-Term History from traffic monitor, use the Domain Manager to configure the Short-Term and Long-Term groups manually or use Segment Zoom to view the port first.
- Catalyst 1200, 5000/2900—When using the Segment Zoom menu from CiscoView to view the port segment, the default configuration for the Catalyst 1200 is to configure the Statistics, Short-Term History, Long-Term History and Host group. The default configuration for the Catalyst 5000/2900 is Statistics, Short-Term History, and Long-Term History.
- Catalyst 5000/2900—If the number of the embedded RMON agent is over 50, you cannot create a new embedded RMON agent group for the new port. Use the Domain Manager to de-install the agent group from the unused port to free the memory resource.

- Catalyst 5000/2900—When you select the repeater module port on a Catalyst 5000/2900, it always uses the first port of the selected segment to create the RMON agent group.
- Catalyst 1200—If you see “IP address is not set in sysIpAddr Mib variable,” the Catalyst 1200 SNMP agent did not store the correct IP address in the sysIpAddr MIB variable, so you have to use CiscoView to correct it. Go to **Configure>Device**, enter the correct IP address in the corresponding field, and click **Modify**.
- Do not use the Grapher in the CiscoView Monitor “10BaseT Group Switching Ethernet” window. Use the Monitor or Traffic Director tools to see graphical views of the selected repeater ports.
- The IP Route device configuration window is not scrollable. Use the numbered arrow keys to scroll the window.
- If you get the “Error: Entry or Group not present in Agent” message when invoking Segment Zoom, Switch Zoom, or Data Capture, the “write” community string might not be matched with the device. If the community string is matched and the problem still occurs, try checking the CiscoView Configure Device menu to verify that the RMON capability is enabled.

Maintaining CiscoView

You can perform the following routine maintenance functions for CiscoView:

- Loading MIBs into NetView
- Rebuilding All CiscoView Files

You can also add new device and application support to CiscoView, by performing incremental installations.

The following procedures require that you use the IBM AIX system administrator facility, SMIT.

Loading MIBs into NetView

If you experience any corruption of your MIB database or the MIBs are not usable, you might want to consider reloading MIBs into NetView. The amount of time it takes to load MIBs into NetView depends on the number of MIBs being loaded.

To load MIBs into NetView:

Step 1 If you have not already done so, start SMIT by entering the following at the command prompt:

```
hostname# smit
```

Step 2 On the System Management menu, click **Communications Applications and Services**.

Step 3 On the next menu, click **Cisco Network Management Applications for AIX**.

Step 4 On the next menu, click on **CiscoView**.

Step 5 In the CiscoView dialog box, click **Maintenance**.

Step 6 In the Maintenance dialog box, click **Load all MIBs into NetView**.

Step 7 In response to the confirmation dialog box, click **OK**.

If the MIB files load successfully, an *OK* status is displayed. If loading failed, a *Failed* status is displayed. If loading failed, contact a TAC representative.

Step 8 Terminate SMIT by pressing **F12** or by clicking **Exit SMIT** on the Exit menu.

Rebuilding All CiscoView Files

You can rebuild all CiscoView Version 3.1(1) on AIX configuration files if:

- You are not sure which device packages or files reside on your system.
- You wish to troubleshoot and rebuild existing CiscoView files because of suspected corruption or deletion of CiscoView configuration files.

To rebuild all CiscoView files, follow this procedure:

Step 1 Enter the following at the command prompt:

```
hostname# smit
```

Step 2 On the System Management menu, click **Communications Applications and Services**.

Step 3 On the next menu, click **Cisco Network Management Applications for AIX**.

Step 4 On the next menu, click on **CiscoView**.

Step 5 In the CiscoView dialog box, click **Maintenance**.

Step 6 In the Maintenance dialog box, click **Rebuild**.

Step 7 In response to a confirmation dialog box, click **OK**.

If the rebuilding process is successful, an *OK* status is displayed. If the process failed, a *Failed* status is displayed. If the rebuilding process fails, contact a TAC representative.

Step 8 Terminate SMIT by pressing **F12** or by clicking **Exit SMIT** on the Exit menu.

Incremental Installations

To add new device and application support to CiscoView, access the Cisco Systems online support channel, Cisco Connection Online (CCO), formerly Cisco Information Online (CIO).

You must be running CiscoView Version 3.1 and later to do incremental installations. Open CiscoView and select **Help>About CiscoView** to check the version number.

CCO Registered User

To register on CCO, enter the following URL into your WWW browser:

```
http://www.cisco.com
```

If you are already registered, enter the following URL:

```
http://www.cisco.com/kobayashi/Library_root_shtml
```

Enter your CCO username and password. Continue to the section “Installing from CCO.”

CCO Guest User

If you are not registered on CCO or do not have a SmartNet contract, you will need a special access code. Phone the Technical Support team for CiscoView at 800 553-2447 or 408 526-7209, or email *tac@cisco.com*, then enter:

```
http://www.cisco.com/public/library/spc_req.shtml
```

Enter the special access code and click **Execute**. Go to the section “Installing from CCO” before proceeding.

FTP User

If you have a SmartNet contract, enter the following URL into your WWW browser:

ftp://[*userid*]**@www.cisco.com/cisco/netmgmt/ciscoview/3.1.1/packages**

For userid, substitute your own userid.

If you are not registered on CCO or do not have a SmartNet contract, you need a special access code. Phone the Technical Access Center (TAC) for CiscoView at 800 553-2447 or 408-526-7209, or *email@cisco.com*; then enter:

ftp://*[special_access_code]***@www.cisco.com/coded/**

For special_access_code, substitute your own special access code.

For FTP server access, enter your email address as the password, for example, *myname@net.com*.

To get more information about the Partner Initiated Customer Accounts (PICA) program before accessing CCO for device package files, use the following URL:

```
http://www.cisco.com/acs/info/pica.html
```

Installing Devices Incrementally

To install devices incrementally on CiscoView Version 3.1(1) on AIX, use either of the following methods:

- Install from the CiscoView CD-ROM
- Install from Cisco Connection Online (CCO). Instructions on how to download additional device support for CiscoView are on CCO and on the Cisco FTP server. The instructions are in the Software Image Library Enterprise Network Management section under CiscoView.

Step 1 If you have not already done so, start SMIT by entering the following at the command prompt:

```
hostname# smit
```

Step 2 On the System Management menu, click **Communications Applications and Services**.

Step 3 On the next menu, click **Cisco Network Management Applications for AIX**.

Step 4 On the next menu, click **CiscoView**.

Step 5 On the CiscoView menu, click **Device Package Install Setup**.

Step 6 In the field “Directory Containing Device Packages,” enter the path where the device packages reside.

Step 7 In the “Load MIBs into NetView” field, the default is **No**. If you want to load MIBs, click the **List** button.

Step 8 If you performed Step 7, click **Yes** in the Single Select List dialog box to load MIBs into NetView.

Note Loading MIBs may take a significant amount of time depending on the number of MIBs being loaded.

Step 9 Click **Do**, wait for the process to complete, and read the output.

If the process was successful, an *OK* status is displayed. If the process failed, a *Failed* status is displayed. If the process failed, contact a TAC representative.

Step 10 Click **Done** and then **Cancel**.

Troubleshooting

This section provides information to help you troubleshoot problems associated with CiscoView Version 3.1(1) on AIX.

Log File for Incremental Installation of Device Packages

When you perform an incremental installation of a CiscoView device package, the following log file is created on your system: *$NMSROOT/cvinstall.log*. Reviewing this log file may enable you to troubleshoot problems associated with the incremental installation.

If You Cannot Open a Device in CiscoView

If you cannot open a device in CiscoView, you will receive a message indicating that the device is unmanageable. This message indicates one of the following conditions:

- The Simple Network Management Protocol (SNMP) server is not set in the device. You can still ping the device from the management station.
- You have entered an incorrect community string in the **File>Open Device** window.
- The management station cannot reach or successfully ping the device.
- CiscoView will fail to come up after an interface processor card is removed from the router because the ifTable still contains information on the card. Reinsert the card or reload the routing image after removing the card to allow CiscoView to work. [CSCdi42488]

CiscoView Version 3.1(1) on AIX Caveats

This section lists notes and restrictions that apply to the CiscoView Version 3.1(1) on AIX release.

- Installation Caveats
- De-installation Caveats
- General Caveats

Installation Caveats

This section provides installation caveats.

HyperHelp Resource File

The CiscoView installation puts the X Window System^{TM} resource file for HyperHelp in the */usr/lib/X11/app-defaults* directory. Because different systems have different types of X installations, the CiscoView application does not always read this resource file. When the resource file is not read, the HyperHelp viewer text may be unreadable on your screen. Do one of the following tasks to make sure that this resource file is read:

- Run the following command each time you log in to your system:

  ```
  xrdb -merge /usr/lib/X11/app-defaults/HyperHelp
  ```

- Put this command in your *.cshrc* or *.profile* file so that it is run automatically every time you log in to your system. Move the HyperHelp X resource file to another directory, such as each user’s home directory. [CSCdi41126] [CSCdi33830]

Path Environment Variables

The following error message indicates that the program (for example, xrdb) is not in your path. Check your path environment variable. [CSCdi57661]

```
couldn't execute "xrdb": no such file or directory
```

Loading Device Packages from a Remotely Mounted CD-ROM

If you are working off a remotely mounted CD-ROM drive in a directory other than */cdrom*, you may have to set the environment variable I_CDROM_PATH to the directory to which the CD-ROM filesystem is mounted when loading device packages in CiscoView.

Tables Show All Categories

Multiple selections show all categories, whether they apply to a specific group of selections or not. If the category does not apply, the configuration table will show "N/A" in the cells. [CSCdi48854]

Installing CiscoView Version 3.1(1) on CiscoWorks 3.0.3

If you install CiscoView Version 3.1(1) on a machine where CiscoWorks 3.0.3 is already loaded, you *must* de-install CiscoView and then install CiscoView Version 3.1(1).

Installing CiscoView Version 3.1(1) when CiscoView Version 3.0(3) Exists

If CiscoView 3.0(3) exists on your system, you must de-install it first and then install CiscoView Version 3.1(1).

De-installation Caveats

This section provides deinstallation caveats.

De-installing CiscoView Version 3.1(1) on AIX

Before de-installing CiscoView Version 3.1(1) on AIX, the NMSROOT environment variable must be set on your system.

General Caveats

The general caveats are divided into six sections:

- Caveats for Enterprise Network Management Products (including CiscoView 3.(1) on AIX and other products)
- Caveats for Workgroup Products
- Caveats for Access Products
- Caveats for High-End Business Products (including the Cisco 7000 and Cisco 7500 series and ATM switches)
- Caveats for Online Help

Caveats for Enterprise Network Management Products

General notes and caveats for Enterprise Network Management products are described below.

Dragging Ports—For this release, use the middle mouse button to drag on UNIX. Only certain devices (such as the Catalyst 1200, Catalyst 1600, Catalyst 5000, CPW 16) have defined their ports for dragging across devices.

NetView Discovery Issue—When a switch is configured as two or more domains, NetView discovery may not work properly and may discover only one of the domains. If this occurs, use CiscoView to manage the domain directly rather than launching it from the map.

NetView Error Message—The *xnmloadmib* program in NetView may have problems reloading MIB files into their database. The definition of CiscoNetworkProtocol in *CISCO-TC-V1SMI.my* and OwnerString in *IF-MIB-V1SMI.my* will display an error message similar to the following when you run **cvinstall -f**:

```
Error detected while loading MIB file: /net/cv311/etc/cview/mibs/CISCO-TC-V1SMI.my
This MIB cannot be loaded until the following problem is corrected:
Line 44613: Error defining ASN.1 Type: dupliCatalyste type with conflicting definition
‘CiscoNetworkProtocol’
```

The workaround is to invoke *xnmloadmib* manually, select and unload all Cisco-specific MIB files from the list box in the *xnmloadmib* GUI, then run the command **cvinstall -f** to load all Cisco specific MIB files. [CSCdi56399]

Running CiscoView with Too Little Swap Space—If the server or display workstation is running out of swap space, you will see a message such as “X error: Couldn’t allocate color cell,” and CiscoView will core dump. If you are running other applications, you might want to check your swap space occasionally.

To check swap space on an AIX system, enter the following:

```
hostname% lsps -a
```

If your system is running out of swap space (for example, only 200 KB of swap space remains), quit some of the other applications you are running, or increase your swap space if possible. [CSCdi37063]

Running Out of Colors—CiscoView can run out of colors. If this occurs, CiscoView will continue to run, but all the colors it cannot allocate will dither to black or white. You can avoid this by starting CiscoView before starting color-intensive applications, or by using a private color map for the color-intensive applications (such as **application_name -install**).

Popup Menu Titles—Popup menu titles are raised; users may mistake them for menu items. [CSCdi53475]

Stripchart and Dials—The stripchart and CPU busy dials for 1 minute and 5 minutes are not drawn clearly for the 7513 router. [CSCdi51621]

Caveats for Workgroup Products

Following are general notes and caveats that apply to the Cisco Workgroup family of products including the Catalyst 2800, Catalyst 2100, EtherSwitch 1200, and EtherSwitch 1400

- In the front panel display of the Catalyst 2800 and EtherSwitch 1400, the Connect and Disabled LEDs on FDDI modules do not reflect the appropriate status.
- CPW1200, CPW1400, Catalyst 2100, Catalyst 2800—In the General Bridge Window, the Last Topology Change field does not apply when the Spanning-Tree protocol is disabled.

- CPW1400, Catalyst 2800—Do not attempt to invoke the Monitoring menu for an FDDI port or a repeater port. There is no monitoring function provided for these ports, although the pull-down menu is enabled when such ports are selected.
- CPW1400, Catalyst 2800—The Configure Module Windows do not work when more than one module type is selected. Select only one module type before opening these windows.
- CPW1200, CPW1400, Catalyst 2100, Catalyst 2800—The General Bridge window shows the bridge information for VLAN1 only. Bridge information for other VLANs is not available.
- CPW1200, CPW1400, Catalyst 2100, Catalyst 2800—The Spanning-Tree Protocol Window for switched ports is available for ports in VLAN1 only. This window does not show valid information for ports not in VLAN1.
- The WG-Concentrator, CPW10/100, and WG_Adapter do not show version information in the About CiscoView dialog box. In these cases, the About CiscoView dialog box displays the package version only. However, the version information is displayed in the "Packages Installed" list.

Community String Mismatching—When the user enters values for the "read-only," "write-only," and "read-writeId" with the command-line interface (CLI) commands, these values must match. A mismatch results in "noSuchName" or "timeout" errors. To avoid these error conditions, use identical community strings in CiscoView and corresponding agents.

Exiting CiscoView Version 3.1(1) Causes Applications to Close—If you are using the CPW16 or Catalyst 3000 and close the CiscoView window, any application window that was launched from it will automatically close. Remember to close the EtherChannel and Domain Configuration application windows before you open another CiscoView application or exit from the CiscoView application. There is no limitation on the number of CiscoView applications that you can run.

False Error Reported After Setting Parameters—On the CPW16 and Catalyst 3000, when you try to set parameters for the EtherChannel/Domain application under moderate- to high-traffic situations, the application incorrectly displays an error window indicating that the operation was not successful. In reality, the command was successful, and you should dismiss the error dialog. The application should continue to function properly.

Next Button—If you rapidly press the Next button on the Catalyst 5000 port configuration dialog box, you may see some category names repeated twice. Redisplay the window to remove the duplicate names. [CSCdi57910]

ProStack Power Supply Link Problem—The rear view of the ProStack matrix power supply does not indicate whether the connector link is up or down (for example, the connector does not come up green if there is a link).

Switch Firmware—The following firmware versions must be used in the switches:

- Catalyst 2100 and Catalyst 2800 version 3.63 or higher
- EtherSwitch 1200 and EtherSwitch 2800 version 3.63 or higher
- Grand Junction FastSwitch 2100 and FastSwitch 2800 version 3.62 or higher

Note The Grand Junction FastSwitch 2100 and FastSwitch 2800 are managed the same as the Catalyst 2100 and Catalyst 2800, respectively.

- EtherSwitch 10/100—version 1.38 or higher

- Catalyst 1700—version 1.38 or higher
- Grand Junction FastSwitch 10/100—version 1.37 or higher

Switches—If you configure EtherChannel or Virtual Domains in Kalpana switch models EPS2015RS, EPS2115RSM, and Pro16 while running version 9.0 firmware with STP active, the map icons become red, and you receive the following error message:

```
No response from the device
```

After restarting the system, deactivate the shielded twisted-pair (STP) before you attempt to reconfigure. This problem is fixed in version 9.1 of the device firmware. [CSCdi41317]

Caveats for Access Products

Following are general notes and caveats for Cisco access products.

FDDI Port Status Functionality—The Cisco 4000 series devices with dual attachment station (DAS) FDDI ports show status on only the lower one of the two connectors. The status color is determined from the port's administrative status (ifAdminStatus) and operational status (ifOperStatus) values. [CSCdi28566]

Read-Only MIB Variables—The administrative status (ifAdminStatus) value "testing" and the ring speed (dot5RingSpeed) variable are implemented as "read only" in all Cisco IOS software versions and cannot be set through popup menus on CiscoView Configure Port screens. However, Configure Port tables (with multiple ports) offer popup windows that permit attempts to set these variables. Such attempts result in "Permission Denied" messages. [CSCdi50635]

Tunnel Interface—A "can't read 'port': no such variable" message appears at the bottom of the configuration port dialog box when a tunnel interface is encountered while you click up through the ports. This message can be ignored. [CSCdi55765]

Caveats for High-End Business Products

Following are general notes and caveats for the Cisco high-end business suite of products (including the Cisco 7000 and Cisco 7500 series and ATM switches).

Displayed ATM Connector Type—CiscoView Version 3.1(1) on AIX always displays the multimode fiber SC type of ATM connector on ATM Interface Processors (AIPs), even when the media interface is another type. [CSCdi53420]

FDDI Port Status Functionality—For the Cisco 7000 and Cisco 7500 series routers running Cisco IOS Release10.2 or earlier, the displayed status color is determined from the port's administrative status (ifAdminStatus) and operational status (ifOperStatus) values. This status color will be the same on each connector. For devices running Cisco IOS Release 10.3 and later, the displayed status color is determined from the Port Connect State (fddimibPORTConnectState) for each connector. The possible values for this status and the corresponding status colors are listed below [CSCdi28566].

Status	Status color
Disabled	Brown
Standby	Brown
Connecting	Blue
Active	Green

High System Availability (HSA)—On the Cisco 7513 and Cisco 7507 chassis, when the master RSP (Route Switch Processor) is in use, the console port changes color on the CiscoView Version 3.1(1) display. However, when a slave RSP is installed, its console port mirrors that of the master, regardless of whether or not it is in use. [CSCdi49049]

In the HSA (dual RSP) configuration, invoking the Admin File Systems function gives an error message caused by a duplicate flash partition name (“slaveslot0”) on the router. This error makes the File Systems functionality unavailable. The user should acknowledge the error message and close the “File Systems” window. [CSCdi54831]

LightStream 2020 MIB Support—For the LightStream 2020 there is currently no MIB support for the “LNS OK,” “LN FLT,” “BITS OK,” and “TCS SEL” LEDs on front linecards. These LEDs appear blank. In addition, the “TX” and “RX” LEDs on front linecards blink too rapidly for SNMP polling purposes and also appear blank.

Lightstream 2020 Software Releases Supported—The LightStream 2020 supports Release 2.1(2) and later.

Online Insertion and Removal (OIR) Support—Hot swap is supported only on devices running Cisco IOS Release 11.0 and later. [CSCdi53447]

Power Supply Display—By default, CiscoView Version 3.1(1) on AIX displays two power supplies for a Cisco 7000 running Cisco IOS Release10.2 and earlier. With Release 10.3 and later, power supplies are displayed based on *ciscoEnvMonSupplyState* values (ENVIRONMENTAL MIB).

Read-Only MIB Variables—The administrative status (ifAdminStatus) value “testing” and the ring speed (dot5RingSpeed) variable are implemented as “read only” in all Cisco IOS software versions and cannot be set through popup menus on CiscoView Configure Port screens. However, Configure Port tables (with multiple ports) offer popup menus that permit attempts to set these variables. Such attempts result in “Permission Denied” messages. [CSCdi50635]

Caveats for Online Help

The following caveats are for online help.

Glossary Links—Some device-specific help files may not have links to the glossary file. To view the glossary, select **Help>Using CiscoView** in the help window.

Options Menu—The following information was omitted from the online help information for the **Options** menu:

```
Options>Set HyperHelp Defaults sets the HyperHelp resources so that the HyperHelp viewer
text is readable on the screen.

Options>Debug records trace information into a file loCatalysted in /tmp/.cvlog.
```

Release Notes for VlanDirector Version 1.1 on AIX

The VlanDirector Version 1.1 on AIX release works as documented in the *VlanDirector User Guide* with the exception of the items documented in the following sections:

- Known Defects
- Features that Might Not Exhibit Expected Behavior

For detailed information on VlanDirector, refer to the *VlanDirector User Guide*.

Known Defects

VlanDirector Version

To find the version of VlanDirector, use the **-V** option instead of **-v**. The **-v** option is no longer available, as it is used internally by the TCL subsystem.

Starting VlanDirector

To save your customized views, you must start VlanDirector from a shell whose current working directory is one for which you have read-write access.

The online help for the VlanDirector Startup dialog box reverses the default values for community strings. It says ‘private’ for Read and ‘public’ for Read/Write, when the reverse is true.

Ports Window Scroll Bar

The Ports window scroll bar does not always operate as expected, as shown in this example:

Step 1 Select a VLAN with at least one port, such as vlanX.

Step 2 Bring up the VLAN Ports window.

Step 3 Select the default VLAN or some other VLAN with many more ports than vlanX.

The scroll bar of the window does not change to reflect the greater number of ports in the newly selected VLAN.

Workaround: Either close the window and reopen it, resize the window, or turn Show: VLAN Ports off, then on again. The scroll bar then correctly reflects the number of objects displayed.

Using Help

The initial size of the Help window is not wide enough to display the **Find** button.

Workaround: Resize the help window at least 0.75 inches wider to display the **Find** button.

The Find window is displayed directly on top of the Help window and completely obscures it. This makes it appear that the **Go To** button in the Find window does not work.

Workaround: Move the Find window away from the Help window.

VLAN Names

VlanDirector allows VLAN names up to 32 characters long, except when there are Catalyst 3000s in the network. (Catalyst 3000s only accept VLAN names up to 16 characters long.) VlanDirector does not take this into consideration when validating the length of a VLAN name.

Workaround: Make sure VLAN names do not exceed 16 characters in length if you have Catalyst 3000s in your network.

Undo

If you are running in a known network and you try to undo an action before a previous undo action is complete, you get this error message:

```
Immediate Network Operation Failed
```

If you click **Help** on this message, you get this further explanation:

```
Operation not the last in the undo list
```

Further, you can no longer open the undo list.

Workaround: Do not begin a second undo until the first one is complete.

Features that Might Not Exhibit Expected Behavior

Community Strings

In VlanDirector Version 1.0, the Read and Write community strings defaulted to ‘public’ and ‘private’ respectively. In VlanDirector Version 1.1, only the Read community string has a default value (‘public’). Therefore, when you start VlanDirector without specifying a CSF or -wr, VlanDirector uses ‘public’ for both the Read and Write community strings.

Upcoming Features

The following features will appear in the VlanDirector Version 1.2 release, to be used with Catalyst 5000 2.2 and Catalyst 3000 1.3:

- FDDI 802.10 support
- FDDI-Ethernet translation bridging

Release Notes for TrafficDirector Version 3.3 on AIX

The TrafficDirector Version 3.3 on AIX release works as documented in the *TrafficDirector Windows User Guide* with the exception of the items documented in the following sections:

- Product Overview
- Licensing
- Configuration Limits
- Cisco RMON Agents
- Catalyst 5000 Group Switching Ethernet Module
- Catalyst 1200 RMON Agent Configuration Guidelines

For detailed information on TrafficDirector, refer to the *TrafficDirector UNIX User Guide*.

Product Overview

TrafficDirector is an RMON console software application that lets you monitor, troubleshoot, and record information about your network’s operation. TrafficDirector helps you analyze network traffic patterns and identify and isolate a wide variety of fault conditions in data communications networks.

TrafficDirector works as a distributed system. It uses a central management console running TrafficDirector software in conjunction with data-gathering agents located at various points on a network. It can simultaneously collect wide-ranging statistical data, display selectively captured and fully decoded network traffic, set user-defined alarm conditions, and obtain real-time updates from all segments of a widely dispersed internetwork. TrafficDirector accomplishes this from a centralized, SNMP-compatible network management console.

TrafficDirector is based on two standards that enable it to operate in a multitopology, multivendor environment:

- The Simple Network Management Protocol (SNMP), which defines the protocol for all intercommunications between TrafficDirector, SwitchProbe devices, and Cisco Internetwork Operating Systems (Cisco IOS) RMON agents.
- The Remote Monitoring Management Information Base (RMON-MIB), which defines the type of information that is to be gathered and made available to the user for each network segment.

TrafficDirector has four main functions:

- Monitoring network traffic, and measuring the flow of data.
- Capturing network traffic and recording it for later examination.
- Interpreting raw network data and translating it into a graphic form that you can then view and analyze.
- Setting limit conditions on network traffic and generating alarms if those limits are exceeded.

TrafficDirector gathers and analyzes network information using SwitchProbes and Cisco IOS software RMON agents attached to network segments.

Licensing

TrafficDirector requires a serial number and password to unlock the software for use. A temporary evaluation serial number and password are attached to the shipping box. This serial number allows you to begin using TrafficDirector as soon as you receive it. However, you will need to request a permanent password before the evaluation expiration date. If you change the IP address of the host, or if you move the software to another machine, you must contact Cisco for a new password.

Note The license agreement requires a separate license for each machine on which you intend to use TrafficDirector.

You can obtain a permanent license agreement through Cisco Connection Online (CCO) or by sending a fax to Cisco Systems.

Getting a License through the CCO Web Server

To obtain a permanent license agreement through Cisco Connection Online, follow these steps:

Step 1 Access Cisco Connection Online at http://www.cisco.com.

Step 2 Access the Software Library. Enter the required information to generate your permanent password. Be sure to use the registration serial number and the registration password shipped with the software package.

Getting a License by Fax

To obtain a permanent license agreement by fax send a fax to Cisco Systems at 408 526-8898 addressed to “Attention: Software Licensing.” Include the IP address of the machine on which you will be using TrafficDirector as well as your registration serial number and registration password shipped with the software package and a return fax number. You will receive your permanent password within 48 hours.

Configuration Limits

TrafficDirector for UNIX (Solaris, SunOS, HP/UX and IBM-AIX) has the following configuration limitation:

Configuration Parameter	Maximum Number Supported
Agents	1000
Agent groups	100
Agents per agent group	60
Interface number (ifIndex number)	999

Cisco RMON Agents

The Catalyst 1200 series switch embedded RMON agent and the SwitchProbe agents provide full seven-layer monitoring for all RMON groups. The Catalyst 2900 and Catalyst 5000 embedded RMON agents provide four groups of RMON (statistics, history, alarms and events) on all Ethernet and Fast Ethernet ports. The Cisco 2500 series routers with Cisco IOS Release 11.1 provide all nine groups of RMON as specified in RFC 1757.

Catalyst 5000 Group Switching Ethernet Module

The Group Switching Ethernet Module of the Catalyst 5000 supports 1 RMON agent on each of its 12-port segments for a total of 4 agents. Use only the ifIndex of the first port in each 12-port segment group when configuring the RMON agent from TrafficDirector.

Catalyst 1200 RMON Agent Configuration Guidelines

The Catalyst 1200 DMP and NMP version 3.1 or higher include an embedded EnterpriseRMON agent. You need to purchase an agent license from Cisco before enabling this RMON agent. The embedded RMON agent *cannot* be configured to monitor the FDDI interface.

To use RMON within the Catalyst 1200 switch you must first create an agent and install domains for each interface that you wish to monitor. When configuring a new agent be sure to set the Interface Number field to a port number between 3 and 10, indicating which Ethernet port/segment you want to monitor. Also, be sure that the SNMP community strings in the Catalyst 1200 match those configured in TrafficDirector for each agent. Cisco ships the Catalyst 1200 with the following default community strings: Read = *public*,Write = *private*.

The Catalyst 1200 series switch reserves slightly less than 1 MB of RAM for use by the embedded RMON agent. Each enabled agent group within an installed domain consumes both memory and CPU cycles on the NMP to monitor that domain. You should remove any unused domains and only install the groups and domains that you plan to monitor. Use the following memory consumption guidelines when configuring groups and domains:

RMON Groups	Memory Used (bytes)	Assumptions
Statistics	100	
Short History	5 K	For 50 buckets
Long History	5 K	For 50 buckets
Host Table	25 K	For fewer than 256 hosts
Conversations (Metric Table)	30 K	For fewer than 1024 conversations
Fully enabled domain	75 K	Maximum (not including data capture buffer)

Note If you receive the error message “Error: No resources in agent” or experience other problems when using the Catalyst 1200 RMON agent, check to make sure that the above memory guidelines have not been exceeded. Most customer problems are caused by the installation of too many domains and groups.

Cisco Connection Online

Cisco Connection Online (CCO), formerly Cisco Information Online (CIO), is the Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional content and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

To obtain access to CCO's software library as part of the PICA (Partner Initiated Customer Accounts) program, use the following URL:

- `http://www.cisco.com/acs/info/pica.html`

  and see this control panel to automate the process: Post Software for Customers under Temporary Special File Access, at:

- `http://www.cisco.com/acs/admin/cseesd.shtml`

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously—a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, Internet e-mail, and fax download options, and is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: `http://www.cisco.com`
- Telnet: `cco.cisco.com`
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and baud rates up to 14.4 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact `cco-help@cisco.com`. For additional information, contact `cco-team@cisco.com`.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contractor, contact Cisco's Technical Assistance Center (TAC) at 800 553 2447, 408 526-7209, or `tac@cisco.com`. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408-526-7208, or `cs-rep@cisco.com`.

This document is to be used in conjunction with the *CiscoView CD Installation Instructions* publiCatalystion.