Doc. No. 78-4296-01 Rev. A0

CiscoWorks Windows 3.0(1) Release Notes

This document discusses the CiscoWorks Windows 3.0(1) release and includes the following information:

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Note This release note was produced on May 29, 1997. For more recent release note information, check Cisco Connection Online (CCO) for possible updates. Refer to the last section in this release note for access information.

What's New in this Release

CiscoWorks Windows 3.0(1) release includes support for Windows 95 and Windows NT 3.51 and 4.0. CiscoWorks Windows runs optionally on CastleRock SNMPc 4.1n and HP OpenView 7.2 (C.02.17) and 7.3 (D.0.2).

CiscoWorks Windows supports the following upgrade paths:

- Upgrade from CiscoWorks Windows 2.x
- Upgrade from CiscoVision 2.1

New devices are supported on all platforms unless otherwise noted. A *README* file describing device support is included on the Cisco Connection Online (CCO) service.

Note For the latest device support packages, refer to the Cisco Connection Online (CCO) service.

To mount and install devices from the support CD, refer to the special CD booklet included in the package. Be sure to read the *README* files on CCO.

Caution Before installing CiscoWorks Windows or CiscoView devices, read the caveats in "CiscoWorks Windows" on page 10.

CiscoWorks Windows Features

CiscoWorks Windows has the following features:

- Configuration Builder—An application that lets you configure the most common features in the Cisco Internetwork Operating System (IOS). Using this application, you can quickly and easily create configuration files for multiple routers, hubs, and access servers without knowing the router command-line language or syntax.
- Health Monitor—A dynamic fault and performance management tool that provides real-time statistics on device characteristics, interface status, and protocol information.
- Show Commands—An application that provides a simple way to display detailed information, including system, protocol, and traffic information for Cisco routers without having to enter complicated command-line language or syntax.
- CiscoView—A graphical network management application that provides a physical view of a Cisco device, its cards, and its ports. Available device data includes system status information; hardware type and software version number; and device, card, and port status. With CiscoView you can configure your Cisco devices, monitor network performance, quickly access vital device information, and troubleshoot minor network problems. Additional networking tools can be started from CiscoView. Additional device support is available on the Cisco Connection Online (CCO) or by ordering the Network Management Support CD.

  Additional CiscoView applications are supported (see Table 3).
- Online Help—A help system that provides information about using CiscoWorks Windows application tasks and finding product information.

CiscoWorks Windows IOS Information

This section contains the latest Cisco IOS (Internetwork Operating System) software version information at the time of printing.

Configuration Builder devices support Cisco IOS Software Releases 10.2 through 11.2, with the exception of access servers, which require a minimum of Cisco IOS Software Release 10.3. Cisco 3600 devices require Cisco IOS Software Release 11.1 or later. Cisco 4000 series devices require Cisco IOS Software Release 10.3 or later.

CiscoView, Show Commands, and Health Monitor devices support Cisco IOS Software Releases 10.2 through 11.2. Cisco 4000 series devices require Cisco IOS Software Release 10.3 or later.

Note CiscoView supports the Qualified Logical Link Control (QLLC) feature in Cisco IOS Software Release 10.3(7) or later and in Cisco IOS Software Release 11.0(2) or later. CiscoView supports the Synchronous Data Link Control (SDLC) feature in Cisco IOS Software Release 10.2 or later. CiscoView supports the CIP card in Cisco IOS Software Release 10.2 or later.

New devices and further specifics on Cisco IOS support will be updated as devices become supported. For the online release notes, refer to one of the following:

- Cisco Connection Online (CCO) in the Cisco Connection Documentation section (continually updated)
- Cisco Connection Documentation, Enterprise Series CD

Note The Cisco Connection Documentation, Enterprise Series CD was formerly called UniverCD.

Documentation Information

The documentation for CiscoWorks Windows includes this document, a CD-ROM booklet, incremental installation instructions, and online help. The primary documentation for CiscoWorks Windows is the online help. If you have documentation feedback, please forward comments to `bug-doc@cisco.com`

You can also refer to the CiscoWorks Windows registration/reference card for information on adding device support to CiscoView.

The documents shipped with this release include:

- *CiscoWorks Windows Getting Started Guide*
- *CiscoWorks Windows CD Installation Instructions*, which includes quick reference instructions for downloading device packages.
- *CiscoWorks Windows Release Notes*

Customer documentation can also be found on the Cisco Enterprise Customer Documentation CD or on CCO.

CiscoWorks Windows Device Information

Table 1 contains the list of supported CiscoView devices by product type.

Table 1 Supported CiscoView Devices

Small to Medium Business Products	Mid-Range Enterprise Products[1]	High-End Enterprise Products
Cisco and CiscoPro 761, 762, 765, 766, 771, 772, 775, 776	Catalyst and CiscoPro switch models[2] 1200, 1400, 1600, 1700, 1800, 1900, 2100, 2600, 2800, 2820, 2900, 3000, 3200, 5002, CPW2200, and Catalyst 3100	Catalyst 5000 and 5500
Cisco or CiscoPro 1003, 1004, and 1005	EtherSwitch Pro16,EPS2015, 1200, 1220, 1400, 1420	Cisco 7000, 7010, 7204, 7206, 7505, 7507, 7513 routers
Cisco and CiscoPro 1601, 1602, 1603, 1604	EtherSwitches: Pro16 and CPW16	LS1010[3]
Cisco 2501, 2502, 2503, 2504, 2505, 2507, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2520, 2521, 2522, 2523, 2524, and 2525	CiscoPro switch models CPW10-100, CPW500, CPW1200, CPW1220, and CPW1400	

Small to Medium Business Products	Mid-Range Enterprise Products[1]	High-End Enterprise Products
CiscoPro 2051, 2052, 2503, 2504, 2505, 2507, 2509, 2511, 2513, 2514, 2516, 2520, 2521, 2522, 2523, and 2524	Workgroup concentrators 1000, 1100, and 1400	
Cisco and CiscoPro 3600 series (includes 3620 and 3640)		
Cisco and CiscoPro 4000 series[4] (includes 4000, 4000-M, 4500, 4500-M, 4700, and 4700-M)		
AS5200 Access Server		
NetBeyond Fasthub 300 and Fasthub 100+ Series		
EPS-500, EPS-1500, EPS2115, CPW-500, and CPW-2115		

1. Adapters WA-C301TA, WA-C303TA, WA-C308TA, WA-C306TA, WA-C321T-PC, WA-C321T-UX, WA-C323T-PC, WA-C323T-UX, WA-C326T-PC, WAC326T-UX, WA-C328T-PC, WA-C328T-UX are no longer supported
2. Catalyst 1000 and 1100 are no longer supported.
3. LS100 and LS2020 are no longer supported.
4. Due to a fix made for the BRI port problem, the Cisco 4000 series devices now supports Cisco IOS 10.3 or later.

Note Check the Cisco World Wide Web site (`www.cisco.com`) periodically for download information on the latest device support and upgrades.

Table 2 provides a list of the CiscoWorks Windows applications and the devices each application supports.

Table 2 Supported CiscoWorks Windows Applications

Configuration Builder[1]	Show Commands	Health Monitor
Routers: 2500, 2501, 2502, 2503, 2509, 2510, 2511, 2514, 2512, 2515, 2520, 2521, 2522, 2523, 2524, 2525, 4000, 4500, 7000, 7010, 7204, 7206, 7505, 7507, and 7513	Routers: AccessPro, 2501-15, 4000, 4500, 7000, 7010, 7204, 7206, 7505, 7507, and 7513	Routers: AccessPro, 2501-15, 4000, 4500, 7000, 7010, 7204, 7206, 7505, 7507, and 7513
Hub/Router: 2505 and 2507	Hub/Router: 2505 and 2507	Hub/Router: 2505 and 2507
	Access Servers: 2509, 2510, 2511, and 2512	Access Servers: 2509, 2510, 2511, and 2512
	CiscoPro switch models CPW 10-100, CPW500, CPW 1200, CPW1400, and CPW2115	CiscoPro switch models CPW 10-100, CPW500, CPW 1200, CPW1400, and CPW2115

1. Configuration Builder devices support Cisco IOS Software Releases 10.0 through 11.2, with the exception of access servers, which require a minimum of Cisco IOS Software Release 10.2. Cisco 3600 devices require Cisco IOS Software Release 11.1 or later. Cisco 4000 series devices require Cisco IOS Software Release 10.3 or later.

Table 3 describes the applications supported by CiscoView.

Table 3 Supported CiscoView Applications

Application	Description	OS	IOS	Device Support
Threshold Manager 1.1.2	Threshold management application that monitors the availability and performance of Cisco devices	Windows 95, Windows NT 3.51 and 4.0	Cisco IOS 11.1 or 11.2 with RMON events and alarms group support	All devices with appropriate Cisco IOS or RMON features
StackMaker 1.0	StackMaker manages the device membership in a Cisco stack.	Windows 95 Windows NT 3.51, 4.0	10.0 through 11.2	Cisco and CiscoPro 1600, 3600, 3620, 3640, Catalyst 1900, Catalyst 2820, CPW1220, CPW1420, Fasthub 100+ and NetBeyond Fasthub 300
Flash File System	The Flash File System provides file copying and editing features for the 7000, 7010, 7204, 7206, 7505, 7507, 7513 routers.	Windows 95 Windows NT 3.51, 4.0	10.0 through 11.2	Cisco 7000, 7010, 7204, 7206, 7505, 7507, 7513 routers
AS5200 Manager	Modem management application used to monitor, configure, and troubleshoot the AS5200 Access Server	Windows 95 Windows NT 3.51 and 4.0	Cisco IOS 10.2 or later except for 3600 devices which require Cisco IOS 11.1 or later.	AS5200 Access Server

Note Check the Cisco World Wide Web site (www.cisco.com) periodically for download information on the latest device support and upgrades.

Incremental Installation Information

Customers can add new devices to CiscoView from CCO. For more information, refer to the "Downloading Device Packages" chapter in the *CiscoWorks Windows Getting Started Guide*. A quick reference version exists in the *CiscoWorks Windows CD Installation Instructions* booklet. For our partner initiated customers, refer to the section "Partner Initiated Customer Accounts."

Partner Initiated Customer Accounts

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

You can also refer to "*Downloading New Cisco Devices and Applications*" for CiscoView for information on adding device support. It is ordered, or available on CCO or the Enterprise Customer Documentation CD.

Troubleshooting

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

- The Simple Network Management Protocol (SNMP) agent is not running 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.
- Check your device package and compare the date to the CCO device package version. Upgrade your device package to the latest version, if required.

CiscoWorks Windows Notes and Caveats

This section lists notes and restrictions that apply to the CiscoWorks Windows 3.0(1) release.

Note For your reference, identification numbers follow the description of the caveat; for example, [CSCdi00001]. If you need to contact Technical Support about one of the following caveats, refer to the identification number to speed up the resolution of any questions or situations you might encounter.

Installation Notes and Caveats

Installation notes and caveats for CiscoWorks Windows follow.

CastleRock SNMPc

SNMPc caveats include:

- The following bugs exist in SNMPc 4.1n. The fixes will be incorporated in 4.1q:
  - TrendWatch failed getting variables from SNMPc for MIB tables that have inaccessible indexes.
  - MIB tables with more than 80 columns crash.
  - The MIB compiler complains of a syntax error when a range is specified for Gauge32 types.

  Use the following URL to access the CastleRock SNMPc 4.1q release: **http://www.castlerock.com/update.htm.** If you plan to upgrade to 4.1q, do this before installing CiscoWorks Windows 3.0, or you will need to reinstall CiscoWorks Windows.

- After a new installation of SNMPc, you will need to reinstall CiscoWorks.
- When you run CiscoWorks Windows on SNMPc for the first time, you are prompted to compile MIB files. Select the **Yes** button. If you don't compile the MIB files, SNMPc might not properly discover and manage your Cisco devices, and CiscoWorks Windows applications might not execute properly.
- Autodiscovery finds either SNMP devices as ping nodes or finds nothing after clearing the discovery log. Verify that the read community string is correct. Start autodiscovery again to see if the problem persists. If it does, terminate autodiscovery and restart from the SNMPc Map menu. [CSCdi40648]

CiscoWorks Windows

The following notes and caveats should be followed:

- Shut down all applications prior to CiscoWorks Windows installation. CiscoWorks Windows installation might overwrite old Windows dynamic link libraries (DLLs) with newer versions and this might cause active applications to terminate.
- If the Kalpana SwitchVision application is installed on your system, deinstall the product before proceeding with the CiscoWorks Windows install.
- If CiscoWorks Windows fails to run immediately after an initial installation, exit and restart Windows.
- CiscoWorks Windows and CiscoVision should not be installed on the same workstation. This configuration is not currently supported, and results are unpredictable.
- CiscoWorks for Switched Internetworks (CWSI) 1.2 and CiscoWorks Windows 3.0 cannot coexist on the same machine. To upgrade CWSI 1.2 to CiscoWorks Windows 3.0, perform the following steps in the order specified here.

1. Remove VlanDirector by selecting Uninstall VlanDirector in the CiscoWorks Windows program group.
2. Remove CiscoWorks Windows by selecting Uninstall CiscoWorks in the CiscoWorks Windows program group.

3 Install CiscoWorks Windows. For details, refer to the *CiscoWorks Windows CD Installation Instructions* document.

Uninstalling only CiscoWorks Windows will remove the VlanDirector files, but will not remove the information in the registry.

Delay When Installing All Devices

If you select all the devices to be installed from the Device Install menu, it might take some time before there is an indication that the installation is progressing. Please standby, the installation will proceed.

Hardware Disk Space Requirements

The hardware disk space requirement for CiscoWorks Windows is 130 MB of free disk space with all packages installed.

HP OpenView for Windows MIB Compilation

There is a possibility that some of the MIBs may not load into the HP OpenView MIB database. MIB file compilation errors may occur when the *OVmibs.bat* file is run after the installation of CiscoView. This is because the MIB compilers are not consistent throughout all the platforms. [CSCdj01654]

Refer to the following pages on the Web to get more information on MIB compiler issues:

http://www.cisco.com/public/mibs/app-notes/mib-compilers

ftp://ftpeng.cisco.com/pub/mibs/app-notes/mib-compilers

Windows NT

CiscoWorks Windows 3.0(1) is not tested with Optivity on the same system. [CSCdi57009]

General Notes and Caveats

The general notes and caveats follow. They are divided into six sections:

- Notes and Caveats for Operating Systems and Other NMS, page 13

Notes and Caveats for Operating Systems and Other NMS

General notes and caveats for CiscoWorks Windows operating systems and optional Network Management Systems follow.

CastleRock SNMPc

The CastleRock SNMPc caveats include:

Changing the Device Community String for SNMPc

You can change the default device community string only once in Castle Rock SNMPc, by using the **Edit>Node Defaults** command, and you need to save and reload the network map before the new default community string takes effect. Performing this procedure again has no effect. You can use the following workaround to change community strings in the future.

Change the community strings for all devices at once, instead of one at a time, with the following procedure:

Step 1 Select one node.

Step 2 Select **Edit>Edit Object**.

Step 3 Select **Comm...**

Step 4 Change to the appropriate community string.

Step 5 Select **Change** in the Edit Node Attributes window.

Step 6 Select **Edit>Copy**.

Step 7 Select **Map>Select Nodes**.

Step 8 Select **All Agent Types and Entire Map**.

Step 9 Select **Edit>Paste**.

Step 10 Make sure only Community and In Map are selected before clicking **OK**.

This procedure sets the community string for all selected objects.

Debug SNMP Menu Option

When the SNMP Debug option is enabled, it pops up a separate console window which shows the SNMP traffic to and from the device. Do not close this window or it will cause CiscoView to exit also. If you close the console windows, CiscoView does not exit gracefully and may cause some undesirable side effects which may include an access violation general protection fault.

SNMPc Error Messages

Use the following recommended actions for dealing with error messages:

- If you receive the following message

  ```
  Unknown Node name
  ```

  when you double-click on an icon, exit and restart SNMPc.[CSCdi40732]

- If you receive the error message:

  ```
  WinSNMP Could not runC:CV4NTtrapx.exe [No TRAPs or IPX!]
  ```

  when you restart CiscoWorks Windows or SNMPc immediately after exiting a previous session, wait at least 20 seconds before attempting to restart CiscoWorks Windows and SNMPc. [CSCdi40713]

Refer to the *SNMPc Network Management Reference Guide* for more information about running CiscoWorks Windows/SNMPc.

HP OpenView for Windows

Closing debug SNMP window will cause the CiscoView application to terminate.[CSCdj08609]

Windows 95

Due to IPC (socket) problems in the TCL version used by CiscoView 4.0 on the Windows 95 operating system, the following features do not work properly and have been disabled on Windows 95 only:

- CV reuse window feature available in Options>Properties [CSCdi84212]
- Domain Configuration and Etherchannel Configuration applications [CSCdj02042]

On Windows 95 there appears to be different coloring shades in Grapher as port status is reset. You can refresh or redisplay the window as a work around. [CSCdi53523]

Windows NT

Under the Windows NT environment, running too many sessions of the CiscoWorks Windows applications (Health Monitor, Show Commands, and Configuration Builder) can cause a General Protection Fault (GPF) in the module *MFC250.dll*. This is a known Microsoft bug that can be avoided by running fewer sessions of the applications. [CSCdi31282, CSCdi34536]

Notes and Caveats for Enterprise Network Management Products

General notes and caveats for Enterprise Network Management products follow.

CiscoWorks for Switched Internetworks Community String

CiscoView 4.0 has some community string restrictions for composite devices. A composite device is a device that contains modules that have their own IP addresses. For example, the LS1010 ASP module that can reside within the Catalyst 5500. The restriction is that the community strings of all the composite modules must match the CiscoView defaults (read-only: public, read-write: private) for the modules to be manageable. [CSCdj11583].

Colormap Problems

Windows 95 has a known Microsoft colormap problem where some colors are mapped incorrectly when switching between applications.

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.

Dragging Ports

For this release, use the left mouse button to drag a port on Windows. Only certain devices (such as the CAT1200, CAT1600, CAT5000, CPW16) have defined their ports for dragging across devices.

IP Address

The Health Monitor, CiscoView, Show Commands, and Configuration Builder applications communicate with a device using its primary IP address. If the primary interface is down, these applications can not locate or attempt to reach the secondary IP address for that device. [CSCdi31320]

Popup Menu Titles

Popup menu titles are raised; users can mistake them for menu items. [CSCdi53475]

Starting CiscoView on Device Interfaces

If you start CiscoView on an expanded node's interface icon (for example, foo.cisco.com:1), you won't be able to telnet to that device—telnet thinks it should use port 1. Do not start CiscoView on device interfaces. [CSCdi56385]

Stripchart and Dials

Stripchart and dials do not get refreshed properly. This is especially true for Windows 95. [CSCdi51621]

TACACS

If you have TACACS or login security enabled on your router, the Show Commands application and the Configuration Builder Learn and Send features will not function. However, you can send configuration files generated by Configuration Builder using the standard TFTP transfer methods. [CSCdi31004][CSCdi76685]

CiscoView

This section contains notes and caveats for the CiscoView application.

CiscoView and Internationalization

CiscoView does not support internationalization.

CiscoView Times Out

In high traffic situations, you might experience timeouts. To increase the timeout period, select **Options>Properties** from the CiscoView menu and change the value for the Timeout field.

You should not reduce the physical view polling interval below (retries*timeout), especially if you experience timeouts; this can exhaust resources on Windows and result in a general error.

Configuration Builder

This section contains notes and caveats for the Configuration Builder application.

Access Server Dialog Boxes

For access server dialog boxes, the cursor will not provide feedback for incorrect data entry in fields, nor is the field with incorrect data highlighted. Font resizing at various screen resolutions may cause the incorrect sizing of text or limit the visible selections in pull-down combo-boxes. You can select invisible combo-box selections by holding down the right mouse button while in the combo-box, then scrolling up or down. [CSCdi34066]

Access Server Features

For access server features, the Chat Script Manager dialog box may create

```
expect null/send null lines
```

in a chat script. If you inadvertently create empty lines under the Expect and Send fields, you receive error messages about your chat script. Delete and recreate the chat script. [CSCdi34038]

Context-Sensitive Help

Selecting a menu item with the mouse and pressing the **F1** key opens the Configuration Builder Help Contents main window instead of starting context-sensitive help. However, context-sensitive help is supported for all Configuration Builder dialog boxes. [CSCdi34304]

Dialog Box Margins

Dialog box margins may not align on some monitor resolutions. [3D-look]

Invalid OS Error

On the NT platform, if an incorrect model is selected in the Model field of the New Configuration File dialog or the Cisco IOS field is empty or incorrectly filled in, you may encounter the following error message: `Invalid OS Specified. OS version should be greater than 10.2.‘`

The workaround is to enter the device’s correct Cisco IOS version number into the Cisco IOS field. This Cisco IOS version should be greater than 10.2. [CSCdj12523]

ISDN Interfaces

Configuration Builder learns extra ISDN interfaces on routers running Cisco IOS 11.2. The workaround is to delete the extra interfaces reported after the learn operation. [CSCdi79442]

Sending Configuration Files

Configuration Builder is designed for initial configuration and subsequent modifications of routers. A configuration sent by Configuration Builder may not completely overwrite a manually created or modified existing configuration. To simplify configuration, Configuration Builder supports the most common configuration options and uses defaults when possible. You are encouraged to view configurations before sending them to a router to ensure that the generated configuration commands and defaults meet your expectations.

If you receive a banner command timeout error message when sending a configuration file, remove the banner command from the configuration file and resend the file. If you receive other command timeout error messages when sending files, select **File>Communication Timeouts**. In the Communication Timeouts dialog box, increase the long and short timeout values, and try sending the file again. [CSCdi20708]

Spreadsheet Control

Spreadsheet control has the following caveats:

- If you use the **F1** key often while the input focus is within a dialog box, Configuration Builder spreadsheet controls can lose track of certain pointers. To release memory and refresh the pointers, log out of Windows and log in again. [CSCdi34671]
- When you use the keyboard to navigate spreadsheet style controls, you must press the spacebar twice to modify a checkbox. [CSCdi15204]
- The **Esc** key does not close the window when the input focus is in the spreadsheet style controls. Use the window menu or move the input focus out of the spreadsheet controls to close the window. [CSCdi15891]

Health Monitor

The **F1** key context-sensitive help feature is not supported for Health Monitor menu items. Context-sensitive help is supported for all Health Monitor dialog boxes. [CSCdi32448]

Show Commands

Show Commands features are not supported by all device types. However, Show Commands' unsupported features can still be selected.

If you select an unsupported feature, you see an error message. For example, if you select the show controllers CxBus feature for a Cisco CPA2509, you see the following error message. [CSCdi30902]

```
This command is not supported by this IOS image.
```

StackMaker

StackMaker caveats include:

Internal Debugging

When the StackMaker Debug option is set to **On**, debug messages print to the StackMaker Debug Log file. The default is Off. The StackMaker Debug Log file stores messages that are useful in troubleshooting problems. This log file is *smDebugLog* in *c:\CWW* or the install directory.

When the StackMaker Debug SNMP option is set to **On**, SNMP debug messages print to the console on the PC. The messages show the SNMP packets that have been sent and received. The default is Off.

Log File from Apply Operations

The StackMaker log file stores the results of a saved stack configuration (Actions>Apply Stack Configuration). The log file is *$NMSROOT\etc\cview\devices\stackmkr\sm.log*. When the log file exceeds 1 MB, it automatically resets to 0 bytes.

Threshold Manager

Threshold Manager caveats include:

Threshold Settings

Some agents, most notably the Catalyst switches, impose a limit on the number of alarm and event entries that can be created. Applying a large number of thresholds to these devices will likely fail. In this case, some alarm

entries might be successfully created but their associated event entries are not. These failed creations are marked as *Failed* in the Current Threshold Settings pane. If you attempt to delete those settings, Threshold Manager reports that the deletion failed (because it cannot delete nonexistent event entries). In this case, you can ignore the error message, and can verify that the deletion occurred by retrieving the threshold settings after the deletion.

Policies

New policies are always added to the display list.To view the new policies, exit from the Configure Thresholds window, then reopen it. [CSCdi62741]

Policy file names won't match if IP address is used. To correct this, use the hostname instead of the IP address when saving host-specific policies. [CSCdi62739]

Duplicate global/device/host policies may be allowed, depending on which window is used. When creating a custom policy, you can only save it once, either as global, device, or host. But after saving the policy, you can use the Modify Threshold Policy window to modify the saved custom policy and save it as all three. [CSCdi68329]

Notes and Caveats for Workgroup Products

General notes and caveats for Workgroup products follow.

Catalyst 1900, Catalyst 2820, CPW 1220, and CPW 1420

To delete an entry from the Set Managers configuration, enter an IP address of 0.0.0.0. The agent on the devices will not accept a blank entry for an IP address. [CSCdj03444]

Catalyst 116 and CPW 316

To delete an entry from the Set Managers configuration, enter a blank field. The IP address of 0.0.0.0 will not remove the entry from the Set Manager Table.

Catalyst 1200

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. To see the Short-Term or Long-Term history from Traffic Monitor, use the Domain Manager to configure the Short-Term and Long-Term group manually or use Segment Zoom to view the port first.

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. For the Catalyst 5000 it is Statistics, Short-Term history, and Long-Term history.

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 may not be matched with the device. If the community string is matched and the problem still happens, use the CiscoView Configure Device menu to see if the RMON capability is enabled or not.

If you launch Switch/Port Zoom from CiscoView and then delete one of the RMON Agents using TrafficDirector, you must re-launch CiscoView before attempting to launch Switch/Port Zoom again.

If you see "IP address is not set in sysIpAddr MIB variable," it is because the Catalyst 1200 SNMP agent does 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.

TrafficDirector 3.3 cannot be launched for interfaces with ifIndex values greater than 1000.

Catalyst 1800

The device agent does not update the IP Address Table of MIB-II properly and does not reflect the correct IP Address information of all the device interfaces. So, the user will not be able to view the correct IP Address information of the device through **Device>Configure>IP Address Table**.

The user will not be able to create new static entries for IP Route Table and ARP Table through CiscoView.

In the interface configuration (**Port>Config>Interface**), modification of the IP parameters always results in an error message being displayed, but the modification is done successfully.

The user will not be able to change the bridge type of the FDDI port to sr-only or srt.

The user will not be able to change the bridge type of the Token Ring port to srtb or tb-only.

The system time configuration is not included as part of device configuration.

Catalyst 1900, Catalyst 2100, Catalyst 2800, EtherSwitch 1200, and EtherSwitch 1400 Series Devices

CPW1200, CPW1220, CPW1400, CPW1420, Catalyst 1900, Catalyst 2100, Catalyst 2800, and Catalyst 2820—The General Bridge window shows the bridge information for VLAN1 only. Bridge information for other VLANs is not available.

CPW1220, CPW1420, Catalyst 1900, and Catalyst 2820—In the CDP Configuration Dialog, changing the transmission time of one port will change the transmission time of all ports. This is a feature of the implementation of the corresponding MIB objects in the device firmware. [CSCdi83959]

CPW1200, CPW1220, CPW1400, CPW1420, Catalyst 1900, Catalyst 2100, Catalyst 2800, and Catalyst 2820—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.

CPW 1420 and Catalyst 2820

On the front panel display of the device, the Connect and Disabled LEDs on FDDI modules do not reflect the appropriate status.

Although there is a **Monitor** menu option available for both FDDI and repeater ports this feature is not supported on these modules.

The **Configure>Module** option is only supported for one module type, even though it can be invoked for multiple module types.

Catalyst 2600

The Catalyst 2600 device package contains two versions of the enterprise MIBs for the Catalyst 2600 switch:

- *C2600_cisco.my*—This MIB file is installed to support devices with image versions prior to 2.2.1.
- *C2600.my* —This MIB file is installed to support devices with image version 2.2.1 or later.

If you are using a MIB browser tool, you will see the MIB variables defined in each of the above, under different branches, at the same time, though any particular Catalyst 2600 switch will respond to queries on only one of the MIBs based upon the release of software in the device. Cisco recommends that you upgrade your Catalyst 2600 switches to version 2.2.1 or later.

CPW 2200 and Catalyst 2900

Under a heavy load condition, SNMP responses are slow. You may see an "`error, no response since...`" message in the CiscoView status window. Select **Options>Properties** and increase the Polling Frequency and Timeout values. [CSCdi57962]

If the number of the embedded RMON agent is over 50,you cannot create any 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.

If you launch Switch/Port Zoom from CiscoView and then delete one of the RMON Agents using TrafficDirector, you must re-launch CiscoView before attempting to launch Switch/Port Zoom again.

TrafficDirector 3.3 cannot be launched for interfaces with ifIndex values greater than 1000.

When multiple ports are selected, the Port>Configure window will not display the Broadcast Suppression category. This is only available for single port selection.

When enabling port security administration on a port, there may be timeouts. If this happens, increase the SNMP timeout value to approximately 10 seconds.

The WS-X2901 module will only show the speed LED lighted when the speed is configured as 100Mbps and the port is connected.

The Port Utilization tool has been removed from the Tools menu and is now available only on a per module basis on the **Config>Module** menu.

Catalyst 3000 Series

When installing CiscoView 4.0 and integrating with HP OpenView 4.1.1, you will see an error relating to the *C3_2_0.my* MIB file display. This error is due to duplicate definitions in the Catalyst 3000 MIB files. To correct this problem, download a new copy of the *C3_2_0.my* MIB and README files from CCO at the following location:
ftp://www.cisco.com/cisco/netmgmt/ciscoview/temp-smu/CSCdj03981.README and CSCdj03981.tar.Z [CSCdi03981]

When the Catalyst 3200 is viewed using CiscoView it does not follow the traditional real-life display model for CiscoView device support. The display shows all Catalyst 3200 modules compacted into a two slot chassis, with module numbers increasing from left to right and top to bottom.

When accessing a stack with six or more devices, there may be some significant performance problems. The performance can be improved by increasing the SNMP timeout settings.

The Catalyst 3000 software does not support RMON on either a stack or an ATM port.

The coloring of ports on the router module according to port status is not supported in this release. If you wish to manage the router module, use the right mouse button and select the “CiscoView Router” menu then use the left mouse button to launch another CiscoView session to manage the router. The Catalyst 3000 software does not allow the modification of the Parent VLAN number. [CSCdi76775]

You may notice timeout messages and SNMP Set Failed messages when using the EtherChannel Configuration tool. If this happens, increase the SNMP timeout values for better performance.

If you are running version 2.0(1) of the Catalyst 3000 software, you will not be able to drag a port to a VLAN that does not already have ports assigned to it. This problem can be fixed by upgrading to a later release of Catalyst 3000 software.

If you are running version 2.0(1) of the Catalyst 3000 software, changes to Full/Half Duplex settings will not always be reported correctly. This problem can be fixed by upgrading to a later release of Catalyst 3000 software.

If you are running version 2.0(1) of the Catalyst 3000 software, the SAID value entered when creating a new VLAN will be redisplayed as a different value. However, the VLAN will have been created with the SAID value you specified. This problem can be fixed by upgrading to a later release of Catalyst 3000 software.

The Domain Configuration and EtherChannel Configuration tools are not supported on Windows 95.

The VLAN & Bridge application does not highlight ISL ports.

Due to restrictions in the Catalyst 3000 software, the WS-X3006B is displayed in CiscoView as a WS-X3006A.

If you launch Switch/Port Zoom from CiscoView and then delete one of the RMON Agents using TrafficDirector, you must re-launch CiscoView before attempting to launch Switch/Port Zoom again. TrafficDirector only works in CWSI is installed.

Catalyst 5000 Series

ATM, FDDI, and CDDI do not support Broadcast Suppression.a

For machines that do not have a */tftpboot* directory (such as a PC) an error will be displayed whenever the Upload/Download feature is invoked on a Catalyst 5000 module.

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.

When using the Switch Zoom menu from CiscoView to view multiple switch ports, the default configuration for the Catalyst 5000 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 group manually or use Segment Zoom to view the port first.

When using the Segment Zoom menu from CiscoView to view the port segment, the default configuration for the Catalyst 5000 it is Statistics, Short-Term history, and Long-Term history.

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 may not be matched with the device. If the community string is matched and the problem still happens, use the CiscoView Configure Device menu to see if the RMON capability is enabled or not.

When you select the repeater module port on a Catalyst 5000, it always uses the first port of the selected segment to create the RMON agent group.

If all Catalyst 5500 slots are populated with modules and you experience timeouts, increase the SNMP timeout value to 15 seconds.

The WS-X5213 and WS-X5213A modules only show the 100Mbps speed LED lighted if the speed is configured at 100Mbps and the port is connected.

Opening the FDDI/Ethernet Bridge category under **Configure>Device** can give an "unknown error." This is due to a problem with the device software.

If a general error (genErr) is displayed when changing vlanPortIslStatus, the selected port may not support ISL.

The values ifAdminStatus and ifLinkUpDownTrapEnable cannot be changed on an ATM port.

Port duplex settings cannot be changed on ATM and FDDI ports.

The value portSpanTreeFastStart cannot be changed on ATM and FDDI ports.

Configuring ports to unsupported speeds returns a general error (genErr). This is due to a problem in the device software.

The following list details the availability of Broadcast Suppression in terms of pps (packets per second) or % (percentage) for modules on Catalyst 5000 series switches. A plus sign (+) indicates available, while a minus sign (-) indicates not. Modules not on this list do not have Broadcast Suppression. The Broadcast Suppression feature is not available on ATM and FDDI. [CSCdi90909]

Module	Packets per Second (pps)	Percentage	Note
WS-X5013	+	+	
WS-X5011	+	-	

Module	Packets per Second (pps)	Percentage	Note
WS-X5010	+	+	% available with newer hardware only
WS-X5113	+	-	
WS-X5111	+	-	
WS-X5213	+	-	
WS-X5020	+	-	
WS-X5114	+	-	
WS-X5223	+	+	
WS-X5224	+	+	
WS-X5213A	+	-	

NetBeyond Fasthub 100+ and 300 Series

For devices that have an expansion module, the port numbering is not consistent with the management console. Ports 17 through 32 are listed in CiscoView as Repeater 2: Port 1 through 16. [CSCdi77159]

After the first reset of the device, the user must set the rptrReset MIB variable to noReset (default value) before the next reset can be performed. This is due to a problem on the device software and will be fixed in a later release. [CSCdi77452]

CDP and CGMP Protocols Unsupported

The CPW 1200/1400 and Cat 2100/2800 devices do not support the CDP and CGMP protocols. The CiscoView dialogs for these will return errors.

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.

Dragging Ports

For this release, use the middle mouse button to drag on a PC. Only Catalyst devices (such as the CAT1200, CAT1600, CAT5000, CPW16) have defined their ports for dragging across devices.

Duplicate Categories

When multiple ports of different types are selected, **Port>Config** may show duplicate categories.

Switch Firmware

The following firmware versions must be used in the switches:

- Catalyst 2100 and 2800—v. 3.63 or higher
- EtherSwitch 1200 and 2800—v. 3.63 or higher
- EtherSwitch 10/100—v. 1.38 or higher
- Catalyst 1700—v. 1.38 or higher
- Grand Junction FastSwitch 10/100—v. 1.37 or higher
- Grand Junction FastSwitch 2100 and 2800—v. 3.62 or higher

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

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 STP before you attempt to reconfigure. This problem is fixed in version 9.1 of the device firmware. [CSCdi41317]

Notes and Caveats for Access Products

General notes and caveats for the Cisco Access family of products follow.

Card Support for Cisco 1600 Series Routers

The following WAN interface cards are supported:

- wic-serial-1t
- wic-s-t-2186
- wic-u-2091

Card Support for 3600 Series Routers

The following Combo Port Modules (cpm) are supported:

- pm-cpm-1e2w
- pm-cpm-2e2w
- pm-cpm-1e1r2w

The following Port Modules (pm) are supported:

- pm-ct1-csu
- pm-ct1-dsx1
- pm-2ct1-dsx1
- pm-ce1-balanced
- pm-2ce1-balanced
- pm-ce1-unbalanced
- pm-2ce1-unbalanced
- pm-4bri-u
- pm-4bri-st
- pm-cpm-8bri-u
- pm-cpm-8bri-st
- pm-4A/S
- pm-cpm-8A/S

The following WAN interface cards are supported:

- wic-serial-1t
- wic-s-t-3420
- wic-u-3420

Card Support for Cisco 4000, 4500, and 4700 Series

The following network processor modules (npm) are supported:

- npm-4000-fddi-sas
- npm-4000-fddi-das
- npm-4000-1e
- npm-4000-1r
- npm-4000-2s
- npm-4000-2e1
- npm-4000-2e
- npm-4000-2r1
- npm-4000-2r
- npm-4000-4t
- npm-4000-2t16s (for 4500 and 4700 routers only)
- npm-4000-4b
- npm-4000-8b
- npm-4000-ct1
- npm-4000-ce1
- npm-4000-1a
- npm-4000-6e
- npm-4000-1fe

FDDI Port Status Functionality

For 4000 series routers running Cisco IOS Release 10.2 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 or 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

Notes and Caveats for High-End Business Products

General notes and caveats for High-End Business products follow.

Can't Read DD(port-23.port-26.pos) for Fast Ethernet PA

When you try to open a horizontal-chassis device such as the 7204, 7206, or 7505 with a Fast ethernet port adapter installed, the error message "can't read 'DD(port-23.port-26.pos)': no such element in array" is displayed. To fix this bug, upgrade to the latest 7000 CiscoView package at http://www.cisco.com/cgi-bin/tablebuild.pl/cview40 [CSCdj16247]

Displayed ATM Connector Type

CiscoView always displays the multimode fiber SC type of ATM connector on AIPs, even when the media interface is of another type. [CSCdi53420]

FDDI Port Status Functionality

For 7000/7500 series routers running Cisco IOS Release 10.2 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 or 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

Flash File System

When performing the Squeeze operation on a flash card, the error "Failed to Squeeze. Try increasing the timeout property under Options in the Main window" may be observed even though the operation succeeds. [CSCdj03172]

High System Availability (HSA)

On the 7513 and 7507 chassis, when the master rsp (route switch processor) is in use, the console port changes color on the CiscoView 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]

LightStream1010

To configure an LECS address for LS1010 from CiscoView, **ServiceId** needs to be the following: **10.1.3.6.1.4.1.353.1.5.1.<*Index*>**, where Index is the row differentiator for configuring multiple LECS addresses. Index is an integer.

From CiscoView for LS1010, ATM Traffic Descriptor table does not show any rows. This is an agent bug. [CSCdj00685]

Power Supply Display

By default, CiscoView displays two power supplies for a 7000 running Cisco IOS Release 10.2 or earlier. With Cisco IOS Release10.3 or later, power supplies are displayed based on ciscoEnvMonSupplyState values.

Notes and Caveats for Online Help

General notes and caveats for CiscoWorks Windows online help follow.

Find Tab

The creation of the full-text search database (Find option) in online help may take several minutes, depending on the number of devices you have installed.

4000 Series Help Error

The Cisco 4000 Series help incorrectly states that they are stack devices. There is also a link to the StackMaker help that does not work. To reach StackMaker help, ensure the StackMaker help package is installed and select Help>Contents to locate the StackMaker help topics. [CSCdj01872]

Obtaining Service and Support

For service and support for a product purchased from a reseller, contact the reseller. Resellers offer a wide variety of Cisco service and support programs, which are described in the section “Service and Support” in the information packet that shipped with your chassis.

Note If you purchased your product from a reseller, you can access Cisco Connection Online (CCO) as a guest. CCO is Cisco Systems’ primary, real-time support channel.Your reseller offers programs that include direct access to CCO’s services.

For service and support for a product purchased directly from Cisco, use CCO.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information 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, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

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, and Internet e-mail, and it 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
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.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 connection rates up to 28.8 kbps.

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

If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, 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 *CiscoWorks Windows Getting Started Guide* publication.

974(2)R