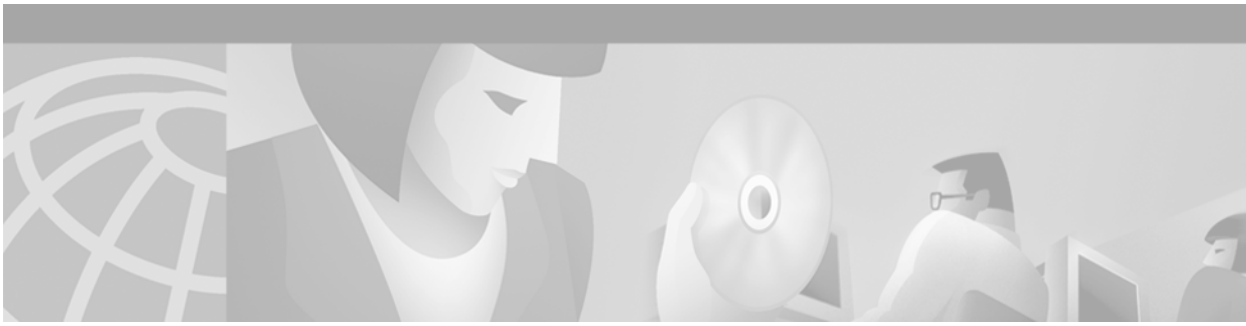

Release Notes for Network Module-Alarm Interface Controller-64 System Firmware on Cisco 2600 and Cisco 3600 Series Routers

April 25, 2002

These release notes describe the Network Module-Alarm Interface Controller-64 Contact Closure Network Module (NM-AIC-64) system firmware.

These release notes contain the following sections:

Network Module Firmware Overview

The Cisco NM-AIC-64 Alarm Interface Controller Network Module expands the capabilities of the Cisco data communications network (DCN) solution by providing remote alarm monitoring and remote control of network elements. By installing this network module into the Cisco 2600, 3640, or 3660 series routers, you have the capability of monitoring and controlling equipment in remote sites to provide enhanced network operations through added visibility into network elements, thereby increasing network security and reliability.

The AIC NM is an optional card that expands network management capabilities for customer-defined alarms. The AIC has its own CPU that communicates with the router and external media through serial communication channels. The AIC reduces service provider and enterprise operating costs by providing a flexible, low-cost network solution for migrating existing DCNs to IP-based DCNs.

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

The AIC can be configured in the same router along with other Operation, Alarm, Maintenance, and Provisioning (OAM&P) interfaces. More than one AIC can be installed per router. For example, a Cisco 366x can accommodate up to 6 AICs, monitor up to 384 network elements, and remotely control up to 96 network devices.

The AIC 64 input contact points can control and monitor network elements and other non-intelligent interfaces, permitting the detection and report of alarms such as the following:

- Network element alarm states
- Building security (door and window open and close)
- Fire and smoke indication
- Building environmentals (temperature and humidity)
- Utility power readings

For more information about the AIC, refer to the *NM-AIC-64, Contact Closure Network Module* feature module. Firmware will be available on Cisco.com in the near future.

Compatibility Requirements

The Cisco NM-AIC-64 is supported with Cisco IOS Release 12.2(2)XG and higher. The current firmware version is 4.5, module part number NM-AIC-64(=).

Supported Platforms

The Cisco NM-AIC-64 is supported on the following platforms:

- Cisco 2600 series routers
- Cisco 3640 and 3660
- Cisco 3600 series routers

Resolved Caveats

This section lists resolved caveats with Cisco NM-AIC-64 Alarm Interface Controller Network module firmware. If a workaround is not provided, a solution is being developed. (See the Error Messages section for further descriptions about some of the resolved caveats in this section.)

- CSCdt58949—**show alarm configuration** for point 64, SNMP trap: incomplete
- CSCdu58568—Cisco 3660 crash after 48 hours stress test.
- CSCdu60388—Need to exit alarm config mode to config multiple points.
- CSCdu60398—Need maximum length indication for text input.
- CSCdu60424—Need end command to exit from subconfig to privileged mode.
- CSCdu69768—Missing characters on Craft Port input.
- CSCdv02183—Analog alarm - unable to set description of alarm & normal state.
- CSCdv44780—Extra spaces present in CONDESCR field.
- CSCdv63010—The REPT^ALM and REPT^EVT messages missing OCRDAT and OCRTIM.

- CSCdv63915—AIC: REPT^ALM^EQPT does not include SA for service affecting alarms.
- CSCdw04806—AIC: Incorrect Control point status reported for normally closed case.
- CSCdu60409—AIC CLI not displaying <cr> at the end of **?** options.

If you have an account with Cisco.com, you can use Bug Navigator II on Cisco.com to find caveats of any severity for any Cisco software release.

Error Messages

The following section contains AIC error messages, causes, and some resolutions. If no workaround is provided, the error is being investigated.

Table 1 AIC Error Messages

AIC Error Message	Cause	Resolution
CSCdu61680—AIC sends wrong HDLC header.	The correct high-level data link control (HDLC) header is 0x0F000800. However, AIC might send the wrong HDLC header (such as 0x0 or any random number). The problem happens in AIC builds 42, 41, 40, and 39; it might also happen before build 39.	Not resolved.
CSCdu58568—Cisco 3660 crash after 48 hours AIC stress test.	The wrong HDLC header sent by AIC (CSCdu61680) makes the Cisco 3660 crash. This problem was found after 48 hours of AIC stress testing.	Resolved. Fix on Cisco router prevents the router from crashing when the wrong HDLC header is received.
CSCdu69753—When commands are issued on the craft or data port, there is a delay between the time that something is typed and when it is accepted and appears in the CLI.	The delay results from an AIC resource problem and no handshaking on the craft port.	Not resolved.

CSCdu69768—Missing characters on craft port input.	All characters of “alarm” are not fully accepted by the command-line interface (CLI), as shown in the following output example:
	
	`aic#`
	`--- 11:12:55 ---`
	`+++ 11:12:55 +++`
	`show tl1 aarm 1`
	`^`
	`% Invalid input detected at '^' marker.`
		Resolved.

Table 1 AIC Error Messages (continued)

AIC Error Message	Cause	Resolution
CSCdu73518—AIC FAULT does not change cardOperStatus: The status LED only turns orange when the AIC fails POST, which does not indicate if the AIC is healthy enough to report the problem to the Cisco IOS software. Also, modification of management message between AIC and Cisco IOS software is needed to allow the AIC to report failure of POST and the status LED is orange.	The cardOperStatus selection shows DOWN only if the card cannot be initialized; the hardware on the card cannot be set up. There was no design requirement for the AIC to send the LED status to Cisco IOS software.	Not resolved. Use the **show alarm-interface** command in privileged EXEC mode to check if the AIC is running.

CSCdv02183—AIC analog alarm is not able to set description of alarm and normal state.	The alarm or normal state option is missing in alarm configuration.	This problem is resolved in AIC build 43. The words, "normal" and "WORD" have been added to the description, as in the following output example:
		
		`Router(config-alarm)# description ?`
		
		`high High state`
		`high-high High-high state`
		`low Low state`
		`low-low Low-low state`
		`normal Normal state`
		`WORD Description of the state`
		
		`Router(config-alarm)# description battery_level`
		`Router(config-alarm)# description normal good`

CSCdt58949—**show alarm configuration** for point 64, SNMP trap is incomplete.
 	
When issuing a **show alarm config** command on the local CLI (craft port), the command output for point 64 is incomplete for the SNMP field, as shown in the following example:
 	
`point 64`
`description: alarm 64`
`configured as discrete`
`normal state description:`
`normal`
`alarm state description:`
`discrete`
`alarm Level: 4`
`voltage 0.0`
`normally high`
`SNMP t`
	A bug found in the Cisco IOS driver for the AIC craft channel resulted in this symptom.	Resolved.

Table 1 AIC Error Messages (continued)

AIC Error Message	Cause	Resolution
CSCdu54724—The AIC name goes back to lower case after reset. After changing the AIC module name from "aic" to "AIC" and resetting the AIC module, the name changed to "aic" instead of "AIC."	Changed information is not stored.	Not resolved.
CSCdu60498—AIC name is missing in configuration backup file.	The configuration backup file created by entering the **put config file_location tftp_server_address** command does not have the name of the AIC.	Not resolved.

CSCdt92276—The AIC [AIC Boot]: prompt does not start with a new line when interrupting the AIC boot process to access the [AIC Boot]: prompt.
After showing the help menu, the [AIC boot] prompt should start with a new line, as in the following example:
`[AIC Boot]: ?`
 	
`d - delete current configuration and replace with default configuration`
`g - get image from tftp server`
`? - print this list[AIC Boot]:`
	The prompt is missing the <cr> after showing the content of the help menu.	Not resolved.

CSCdu35883—The AIC needs an **exit** command to terminate a telnet session.	The **exit** command option is missing.	An **exit** command is added in build 43.
CSCdu09556—The AIC needs any new CLI to read analog value for an analog alarm point; not able to show value of selected analog alarm point.	The **show alarm value** command needs to have the number 57 and others added.	Not resolved.
CSCdu48808—The AIC needs a crash dump feature to be added.	The crash dump feature is missing.	Not resolved.
CSCdu60382— The AIC CLI needs page-by-page output.	There is no page break option at the end of the page. Press the space bar to display more information on the following pages.	Not resolved.

Table 1 AIC Error Messages (continued)

AIC Error Message	Cause	Resolution
CSCdu60411—The AIC CLI needs control key functionality to move around on the same line.	Control keys and arrow keys cannot traverse the same line of input as implemented in Cisco IOS software. Ctrl-B moves the cursor back one character; Ctrl-F moves the cursor ahead one character.	Not resolved.
CSCdu60388—The AIC CLI needs to exit alarm config mode to configure multiple points.	The CLI does not allow the second alarm to be configured when in first alarm configuration mode. You must exit alarm configuration mode before going back into the configuration mode for the second alarm.	Resolved. The system now allows you to configure the second alarm without having to exit from first alarm configuration mode.

CSCdu60398—The AIC CLI needs maximum length indication for text input.	Missing maximum length of text input.
	The CLI used now:
	`Router(config-tl1)# ala 1 sid ?`
	Proposed CLI:
	`Router(config-tl1)# ala 1 sid ?`
	`WORD SID 5 character maximum string`
		Resolved.

CSCdu60409—The AIC CLI does not display the carriage return symbol <cr> at the end of **?** options. If there are not any more options, entering **?** should show <cr>.	The **show control configuration 1** command does not show <cr> when no more options exist. The CLI used now: `Router# show control configuration 1?` Proposed CLI: `Router# show control configuration 1?` <cr>	Resolved.

CSCdu60424—The AIC CLI needs the **end** command to exit from subconfiguration to privileged mode.	The **end** command does not work in configuration mode, as in the following example:
	`Router(config)# end`
	`^`
	`% Invalid input detected at '^' marker.`
	`Router(config)# alarm 1`
	`Router(config-alarm)# end`
	`^`
	`% Invalid input detected at '^' marker.`
		Resolved.

Downloading Firmware

To download firmware to the AIC, use the following steps:

Step 1 Connect to the router on which the AIC resides. The following prompt appears:

```
Router#
```

Step 2 Verify the present firmware build that is running on the AIC by entering the **show alarm-interface** command in privileged EXEC mode. The slot number is the slot in which the AIC is installed. In the following example, information in **bold** shows the current numbering (version) scheme:

```
Router# show alarm-interface slot-number

               Alarm Interface Card in Slot 0:
Status:HARDWARE NOT PRESENT

               Alarm Interface Card in Slot 1:
Configured IP address:1.2.134.105
Status:RUNNING
Timer expires in < 10 min.
Reported version:00 00 00 01
Expected version:00 00 00 01
Last Self Test result:READY
Last Start-Up message:
----------
<AIC>:Hardware Version 1, Revision A Software Version 1, Revision A 1.0.0 Installed and
running, POST passed.
----------
Last Status severity:0
Last Status message:
----------
Status
----------
```

Step 3 Connect to the AIC by entering the **telnet** command in privileged EXEC mode. The line number value corresponds to the slot in which the AIC is installed:

```
Router# telnet router ip-address line-number
```

Step 4 Log on to the AIC by typing **enter** at the AIC login prompt and then entering your login ID and password:

```
aic>
aic> enter
LOGIN:*****
PASSWORD:*****
aic#
```

Step 5 To retrieve the software image from the specified IP address using TFTP, enter the **get image** command in privileged EXEC mode. The *filename* argument must be a complete path, as shown in the following example:

```
aic# get image filename tftp server ip-address

Getting a new image will destroy the old one.
Proceed? [confirm 'y' or 'n'] y
.............................................................
 command successful
aic#
```

Step 6 Return to the router prompt, and configure the AIC by entering the **alarm-interface** command in configure interface mode. Then reset the CPU in the AIC by entering the **reset** (AIC) command in alarm-interface mode, as shown in the following example:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# alarm-interface slot-number
Router(config-aic)# reset

Alarm Interface Card in slot x restarted

Router(config-aic)# end
Router#
```

The router takes a few minutes to build the configuration.

Step 7 Verify the configuration on the AIC by entering the **show alarm-interface** command in privileged EXEC mode. The slot number is the slot in which the AIC is installed. In the following example, information in **bold** shows the change in the numbering (version) scheme:

```
Router# show alarm-interface slot-number

                Alarm Interface Card in Slot 0:
Status:HARDWARE NOT PRESENT

                Alarm Interface Card in Slot 1:
Configured IP address:1.2.134.105
Status:RUNNING
Timer expires in < 10 min.
Reported version:00 00 00 01
Expected version:00 00 00 01
Last Self Test result:READY
Last Start-Up message:
----------
<AIC>:Hardware Version 1, Revision A Software Version 2, Revision A 1.0.1 Installed and
running, POST passed.
----------
Last Status severity:0
Last Status message:
----------
Status
----------
```

For more information about downloading firmware, refer to the *NM-AIC-64, Contact Closure Network Module* feature module and the *Software Configuration Guide for Cisco 3600 Series and Cisco 2600 Series Routers*.

Related Links

For further information about AIM firmware, refer to the following related sources:

- Cisco IOS Release 12.2 Configuration Guides and Command References
- Cisco IOS Release 12.2 Master Indexes
- NM-AIC-64, Contact Closure Network Module
- *Update to the Cisco Network Module Hardware Installation Guide*

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the **Fax** or **Email** option under the “Leave Feedback” at the bottom of the Cisco Documentation home page.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.

- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the Related Links section.