



# NM-AIC-64, Contact Closure Network Module

## Feature History

Release	Modification
12.2(2)XG	This feature was introduced on the Cisco 2600 series and Cisco 3600 series platforms.
12.2(8)T	This feature was integrated into Cisco IOS Release 12.2(8)T and support for the Cisco 3631 was added.

This feature module describes the software support for the Network Module-Alarm Interface Controller-64 (NM-AIC-64), Contact Closure Network Module, commonly called the alarm interface controller (AIC). It includes information on the benefits of the new feature, supported platforms, and related documents.

This document includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 6](#)
- [Supported Standards, MIBs, and RFCs, page 6](#)
- [Configuration Tasks, page 7](#)
- [Monitoring and Maintaining the AIC, page 15](#)
- [Configuration Examples, page 16](#)
- [AIC CLI Syntax, page 20](#)
- [Command Reference, page 34](#)
- [Glossary, page 44](#)

## Feature Overview

The NM-AIC-64, Contact Closure Network Module (also known as the AIC) 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 data communications networks (DCNs) to IP-based DCNs. The AIC provides its users with a single box solution because it can be configured in the same router along with other operations, alarm administration, maintenance management, and provisioning (OAM&P) interfaces.

More than one AIC can be installed per router. For example, a Cisco 3662 can support up to six AICs. The Cisco 3640 can have up to three AICs, with the fourth slot reserved for communication, and so forth.

The AIC provides a total of 64 alarm inputs. Eight of the 64 points are software configurable for measuring either analog inputs or discrete inputs. The remaining 56 points are fixed to measure discrete points only. The AIC also provides 16 control relay outputs.

The discrete alarm input can be activated through ground or negative battery input. The negative battery range is -36 to -72V. The analog alarm is software configurable for either DC voltage or current. It can measure voltage from -60 to 60V or current from 0 to 20mA, but the configurable range is 4 to 20mA. The standard 16 control relays can be configured to turn on or turn off an external device.

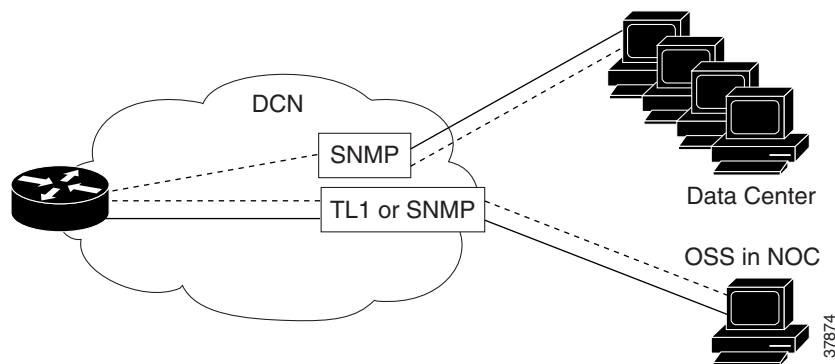
The AIC's 64 input contact points can control and monitor network elements and other nonintelligent interfaces, permitting the detection and report of alarms such as the following:

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

When an event occurs, such as a door alarm or an open gate, the AIC maps the simple discrete and analog alarms to preprogrammed intelligent messages and transports the messages to destinations in the IP network, typically to a network operations center (NOC). These messages are generated either in Transaction Language 1 (TL1) or in Simple Network Management Protocol (SNMP), which are used by a NOC's operations support system (OSS).

When the AIC is incorporated into the Cisco's DCN solution platforms, all the AIC's contact-closure alarms are routed and reported through the same network and systems as the intelligent network elements (NEs). This facilitates continued use of the existing OSS and its associated networks. A Cisco router with a AIC sends TL1 or SNMP messages to the OSS autonomously or in response to TL1 or SNMP commands from the OSS, as shown in Figure 1. TL1 supports two sessions, with the port numbers 5011 and 5012, respectively and SNMP supports four sessions.

**Figure 1 TL1 and SNMP Message Flow in a DCN Application**

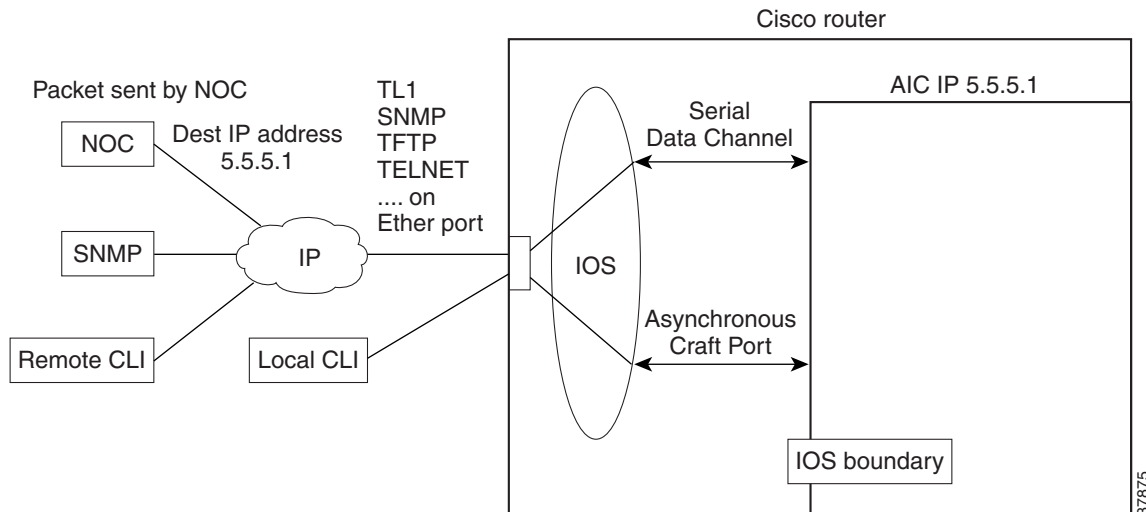


## Serial Communications Channels

As illustrated in [Figure 2](#), the AIC has two serial communications channels that provide different types of interfaces to the Cisco IOS:

- Serial data channel
- Asynchronous craft port

**Figure 2** OS Boundary into the AIC



## Serial Data Channel

The serial data channel supports all TCP/IP traffic to and from the AIC. This includes communication over IP with NOCs and data centers. The channel consists of one physical interface that provides support for the following applications:

- Telnet
- TL1
- TFTP
- SNMP

The Cisco IOS assigns an IP address to the AIC for use by the serial data channel. To route traffic, the serial data channel uses IP over synchronous high-level data link control (HDLC). All IP packets coming to the Cisco router with a destination IP address that matches the AIC's IP address are forwarded to the serial data channel using IP over HDLC.

## Asynchronous Craft Port

The asynchronous craft port supports Telnet to the AIC's port number. This Telnet method, called local-CLI, is useful for debugging when remote Telnet to the AIC's IP address (remote-CLI) is not applicable. For more information, see the [Configuring the NOC IP Address](#) section.

The asynchronous craft port also supports an AIC boot sequence, similar to the ROM monitor in Cisco IOS, which allows you to recover from a corrupted software image or configuration. See the [Override](#) section.

## Configuring the AIC

From a top-level view, AIC configuration involves assigning an IP address to the AIC using Cisco IOS commands and setting up alarm configurations with either TL1 or the AIC command-line interface (CLI). The flexible TL1 and AIC CLI permit a broad range of alarm configuration scenarios. The following are examples of four possible alarm configurations that can be programmed with the AIC CLI.

### Configuring a Discrete Alarm

```
enable
config terminal
alarm 1
description "west door"
normally closed
description normal "door closed"
description alarm "door open"
level 2
exit
```

### Configuring an Analog Alarm as an Analog Monitoring Voltage

```
enable
config terminal
alarm 57
analog voltage 2.5 30 60 60
description "tank level"
description normal "full"
description low "low"
description low-low "empty"
exit
```

### Configuring an Analog Alarm as a Discrete Monitoring Current

```
enable
config terminal
alarm 58
description "east door"
discrete current-loop 0.0 3.2 5.9 high
exit
```

### Configuring an Analog Alarm as a Discrete Monitoring Voltage

```
enable
config terminal
alarm 58
description "backup battery"
discrete voltage 9.0 high
exit
```

## Configuring an Analog Alarm to Act Like a Discrete Alarm (Minimal Configuration Method)

```
enable
config terminal
alarm 59
discrete
exit
```

## Benefits

### Increased Functionality and Versatility

The AIC increases the functionality and versatility of the Cisco 2600 series, Cisco 3640, Cisco 3660, and Cisco 3662, giving service providers and enterprises enhanced communications and connections between the OSS and the NOC.

### Low Cost Migration to Cost-Effective Technology

The AIC provides a flexible, low-cost network solution for service providers and enterprises to migrate existing DCNs to IP-based DCNs and to bridge traditional operations networks to a more cost-efficient, next generation, IP-based operations network.

### Efficient, Single-Box Solution

The AIC provides discrete and analog alarms and initiated surveillance messages for central office and branch office network equipment (with nonintelligent interfaces) within the Cisco DCN solution products. By providing the contact closure network module in the same box as all the other OAM&P intelligent interfaces, customers benefit from the cost savings of a single-box solution that facilitates further DCN consolidation.

### Streamlines Management and Implementation

The AIC's single-box solution simplifies service providers' network management processes. It also streamlines the installation of a solution for contact closure alarms because it reduces the number of external elements required to carry out such a function. This is especially beneficial to competitive local exchange carriers (CLECs) entering into a central office co-location situation where space is at a premium.

## Restrictions

- The **no cdp enable** command is the only one that can be used on the AIC serial data channel. No other Layer 2 parameters on the AIC's serial data channel can be changed.
- Asynchronous communication parameters of the asynchronous craft port cannot be changed.

## Related Documents

### Cisco Documents

- [Update to the Cisco Network Module Hardware Installation Guide](#)
- [Release Notes for Network Module-Alarm Interface Controller-64 System Firmware on Cisco 2600 and Cisco 3600 Series Routers](#)

**Other Documents**

- Information about TL1 commands can be found in the Telcordia Technology (formerly Bellcore) document *Network Maintenance: Network Element and Transport Surveillance Messages*, GR-833-CORE, Issue 5, November 1996.
- For a reference of security-related commands (ACT-USER and CANC-USER), refer to Telcordia Technology's *Operations Applications Messages-Network Element and Network System Security Admin Messages*, TR-NWT-000835, Issue 2, January 1993.

## Supported Platforms

- Cisco 2600 series
- Cisco 3600 series (Cisco 3631, 3640, and 3660)

**Determining Platform Support Through Feature Navigator**

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check verifies that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password are e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

## Supported Standards, MIBs, and RFCs

**Standards**

No new or modified standards are supported by this feature.

**MIBs**

The AIC introduces a new MIB called CISCO-AIC-MIB. To support the AIC, an AIC object type and AIC ID were added to the following MIBs:

- OLD-CISCO-CHASSIS-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

#### RFCs

No new or modified RFCs are supported by this feature.

## Configuration Tasks

See the following sections for configuration tasks for the AIC feature:

- [Configuring the AIC](#) (required)
  - [Entering Alarm Configuration Mode and Configuring the AIC IP Address](#)
  - [Configuring the IP Route to the AIC](#)
- [Configuring the NOC IP Address](#) (optional)
- [Configuring Alarms](#) (optional)

## Configuring the AIC

Cisco IOS commands are used for configuring the AIC IP address and the IP routing to the AIC. After the IP address and the IP routing are set, alarm configurations can then be set up with either TL1 or the AIC command-line interface. See [Configuring the NOC IP Address](#) or [Configuring Alarms](#) sections for more information.

The following sections describe how to configure the AIC IP address and the IP routing to the AIC.

### Entering Alarm Configuration Mode and Configuring the AIC IP Address

Enter alarm configuration mode and configure the AIC IP address, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	Router# <b>show run</b>	Determines if the AIC is installed correctly in the router. If the AIC has been installed correctly, then the following appears:  <i>interface serial slot/port</i>  where the slot is the slot in which the AIC is inserted, and the port is 0.
Step 2	Router# <b>configure terminal</b>	Starts the configuration session.
Step 3	Router(config)# <b>alarm-interface slot-number</b>	Enters the AIC interface mode, specifying the slot number into which the AIC is installed.
Step 4	Router(config-aic)# <b>ip address ip-address</b>	Enters the IP address of the AIC.

	Command	Purpose
Step 5	Router(config-aic)# <b>reset</b>	Resets the AIC. Changing the IP configuration may not take until the next time the card is started. The <b>reset</b> command restarts the card.
Step 6	Router(config-aic)# <b>exit</b>	Exits the AIC interface mode.

## Configuring the IP Route to the AIC

There are many ways to configure IP routing to the AIC. The first method, shown below, uses an unnumbered IP address. An administrator uses this method to assign an IP address that is already known to the router, such as an address that is one of the addresses in the subnet of a Fast Ethernet IP address.

Configure IP routing to the AIC, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>ip route</b> <i>network-number network-mask</i> { <i>IP address</i>   <i>interface</i> } [ <i>distance</i> ] [ <b>name</b> <i>name</i> ]	Establishes the discrete IP route and mask on the router's serial interface. The arguments have the following meanings:  <i>network-number</i> —IP address of the target network or subnet.  <i>network-mask</i> —Network mask that lets you mask network and subnetwork bits.  <i>IP address</i> —Internet address of the next hop that can be used to reach that network in standard IP address notation. Example: 10.1.1.1.  <i>interface</i> —Network interface to use.  <i>distance</i> —(Optional) An administrative distance, which is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers.  <b>name name</b> —(Optional) Name of the user profile.  Example:  Router(config)# <b>ip route 5.5.5.1 255.255.255.255 serial12/0</b>
Step 2	Router(config)# <b>interface serial</b> <i>slot/port</i>	Enters the serial interface mode. Enter the slot in which the AIC is installed and the port 0.

	Command	Purpose
Step 3	Router(config-if)# <b>ip unnumbered</b> <i>type interface-number</i>	Enables IP processing on the serial interface to the AIC without assigning an explicit IP address to the interface. The <i>type</i> and <i>interface-number</i> arguments indicate another interface on which the router has an assigned IP address. The other interface cannot be an unnumbered interface, because only an interface that has its own IP address can be used to lend its IP to the serial port. Enter, for example:  Router(config-if)# <b>ip unnumbered FastEthernet 0/0</b>
Step 4	Router(config-if)# <b>exit</b>	Exits the serial interface mode.

The second method, shown below, does not use an unnumbered IP address and is used when there is a subnet available to the serial interface and to the AIC. Usually, this subnet is small with a subnet mask such as 255.255.255.252.

s

	Command	Purpose
Step 1	Router(config)# <b>interface serial</b> <i>slot/port</i>	Enters the serial interface mode. Enter the slot in which the AIC is installed and the port 0.
Step 2	Router(config-if)# <b>ip address</b> <i>ip-address network-mask</i>	Specifies the IP address and mask of the router's serial interface to the AIC. For example:  Router(config)# <b>ip address 5.5.5.2 255.255.255.252</b>
Step 3	Router(config-if)# <b>exit</b>	Exits the serial interface mode.

## Accessing the AIC

Remote-CLI and local-CLI are the two methods for accessing the AIC:

- Remote-CLI involves Telnetting to the IP address of the AIC. For example:

```
telnet 5.5.5.1
```

- Local-CLI involves accessing the asynchronous craft port by Telnetting to the IP address of the router and the AIC's TCP port number. For example:

```
telnet 10.2.130.105 2001
```

where 10.2.130.105 is the router's IP address and 2001 is on slot 0 of the router.

The AIC's TCP port number depends on the slot number in which the AIC is installed. As shown in [Table 1, Part 1](#), the Cisco IOS software reserves the first line of each slot for the asynchronous craft port.

**Table 1, Part 1** TCP Port Number Allocation for the AIC on the Cisco 2600 and Cisco 3600 Series

Slot Number	Terminal Line Number for the AIC's Asynchronous Craft Port	TCP Port Number
0	1	2001
1	33	2033
2	65	2065
3	97	2097
4	129	2129
5	161	2161
6	193	2193

## Configuring the NOC IP Address

Configure up to four NOC IP addresses to which the AIC sends SNMP messages, beginning in global configuration mode.



**Note** For a complete listing of AIC CLI commands, see the [AIC CLI Commands](#) section.

	Command	Purpose
<b>Step 1</b>	<code>aic(config)# snmp</code>	Enters the SNMP configuration mode.
<b>Step 2</b>	<code>aic(config-snmp)# noc ip-address {number} ip-address</code>	Enters an NOC IP address in which the AIC sends SNMP messages. The <i>number</i> argument can be the numbers 1 through 4.
<b>Step 3</b>	<code>aic(config-snmp)# exit</code>	Exits the SNMP configuration mode.

## Configuring Alarms

After the AIC and NOC IP addresses have been configured, you can configure alarms by programming the AIC's discrete and analog contact points. These tasks can be performed on-site or by Telnetting as described in the [Accessing the AIC](#) section.

Alarms are configured using either TL1 or AIC CLI. Information about TL1 commands can be found in the Telcordia Technology (formerly Bellcore) document *Network Maintenance: Network Element and Transport Surveillance Messages*, GR-833-CORE, Issue 5, November 1996. For a reference of security-related commands (ACT-USER and CANC-USER), refer to Telcordia Technology's *Operations Applications Messages-Network Element and Network System Security Admin Messages*, TR-NWT-000835, Issue 2, January 1993. The following TL1 messages and commands are supported by the AIC:

- TL1 Messages
  - REPT-ALM-ENV
  - REPT-ALM-EQPT
  - REPT-EVT
- TL1 Commands

- ACT-USER
- CANC-USER
- OPR-EXT-CONT
- RTRV-EXT-CONT
- RLS-EXT-CONT
- RTRV-ALM
- RTRV-ALM-ENV
- RTRV-ATTR
- RTRV-ATTR-CONT
- RTRV-ATTR-ENV
- RTRV-ATTR-LOG
- RTRV-HDR
- RTRV-LOG
- SET-ATTR-EQPT
- SET-ATTR-LOG
- SET-ATTR-ENV
- STA-LOG
- STP-LOG

## Programming the Analog Contact Points

Alarm points 57 through 64 are analog inputs, which are configurable as discrete inputs. When configured as an analog input, you must select whether the point is monitoring voltage or current. You must also define five ranges by selecting four values for a point-monitoring voltage or six ranges for a point-monitoring current. For current-monitoring points, the lowest and highest values define the range of possible values. (Valid values are from -99999.9 to 99999.9.) For voltage-monitoring alarms, the range of possible values is always -60 to 60V. The other four values must be within the defined range, and they partition the range into low-low, low, high, and high-high ranges. Except for the normal range, each range is associated with an alarm condition.

Analog points have four unique alarm states. Each alarm state has its own alarm description string. Only one alarm state per point may be active at any given time. In other words, when a threshold is crossed, the previous alarm state is cleared and the new alarm state is active.

When an analog input is configured as discrete, you must select whether the point is monitoring voltage or current. Similar to the analog configuration, you must also select the range of acceptable values for a current-monitoring alarm. (Valid values are from -99999.9 to 99999.9.) The voltage range is always -60 to 60V. You must define the threshold that causes the alarm condition and whether the normal state of the alarm is the higher or lower range.

**Note**

For the current analog point, the lower boundary is 4 mA and the upper boundary is 20 mA. For example,

```
analog current-loop 10 13 16 17 20 26
```

has 16 units between 10 and 26. If the AIC measures 4 mA, then it factors that the point is registering at the lower boundary. The AIC interprets 13 as 7 mA, 16 as 10 mA, 17 as 11 mA, 20 as 14 mA, and 26 as the upper boundary, which is 20 mA.

Following are examples:

Point 57 is monitoring ambient temperature of a building and the sensor range is -20 to 75 degrees Celsius. Below 0 degrees is a critical alarm, 0 to 10 degrees is a major alarm, 10 to 35 degrees is the normal range, 35 to 45 degrees is a minor alarm, and above 45 degrees is a major alarm. The configuration for this point follows:

```
alarm 57
analog current-loop -20 0 10 35 45 75
level low-low 1
level low 2
level high 3
level high-high 2
```

Point 58 is monitoring a fuel tank level with a resistive sensor. Below -46 volts is a critical alarm, -46 to -40 volts is a minor alarm, and above -40 volts is the normal range. This is a unidirectional alarm, so the high thresholds are set equal to the high bound (since this threshold cannot be crossed). The configuration for this point follows:

```
alarm 58
analog voltage -46 -40 60 60
level low-low 1
level low 3
```

Point 59 is monitoring a battery bank. Below -42 volts is a critical alarm and above -42 volts is the normal range. The configuration for this point follows:

```
alarm 59
discrete voltage -42 high
level 1
```

## Programming the Discrete Contact Points

The discrete alarms do not require as much programming as the analog alarms. The AIC CLI commands available are the following:

<b>no</b>	Reversal option
<b>exit</b>	Exits current mode
<b>description</b>	See <a href="#">Alarm Subconfiguration Mode</a> See <a href="#">Control Subconfiguration Mode</a>
<b>normally</b>	See <a href="#">Alarm Subconfiguration Mode</a>
<b>level</b>	See <a href="#">Alarm Subconfiguration Mode</a>

## Verifying the IP Address

To verify that the correct AIC IP address and IP route were entered, use the **show run** command. Below are samples of before-configuration and after-configuration **show run** outputs:

```
interface Serial5/0
ip unnumbered FastEthernet0/0
```

```
!
ip route 10.2.130.102 255.255.255.255 Serial5/0
!
alarm-interface 5
  ip address 10.2.130.102

*****before configuration show run output*****

version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uut2-3660
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
!
no ip finger
no ip domain-lookup
!
call rsvp-sync
cns event-service server
!
!
interface FastEthernet0/0
  ip address 10.2.130.2 255.255.0.0
  duplex auto
  speed auto
  no cdp enable
!
interface Serial5/0
  no ip address
!
ip kerberos source-interface any
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.0.1
ip http server
!
no cdp run
!
!
dial-peer cor custom
!
!
line con 0
  exec-timeout 0 0
  transport input none
line 161
  no exec
  transport preferred none
  transport input telnet
  transport output none
  stopbits 1
line aux 0
line vty 0 4
  password lab
  login
!
end
```

\*\*\*\*\*after configuration show run output\*\*\*\*\*

```

version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uut2-3660
!
logging rate-limit console 10 except errors
no logging console
!
ip subnet-zero
!
!
no ip finger
no ip domain-lookup
!
call rsvp-sync
cns event-service server
!
interface FastEthernet0/0
 ip address 10.2.130.2 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
!
interface Serial5/0
 ip unnumbered FastEthernet0/0
!
 ip kerberos source-interface any
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.2.0.1
 ip route 10.2.130.102 255.255.255.255 Serial5/0
 ip http server
!
no cdp run
!
!
alarm-interface 5
 ip address 10.2.130.102
!
dial-peer cor custom
!
!
!
line con 0
 exec-timeout 0 0
 transport input none
line 161
 no exec
 transport preferred none
 transport input telnet
 transport output none
 stopbits 1
line aux 0
line vty 0 4
 password lab
 login
!

```

end

## Troubleshooting Tips

If no alarm messages are sent for an unusually long period of time, **ping** the AIC address to check for connectivity.

For more information about error messages, refer to the [Release Notes for Network Module-Alarm Interface Controller-64 System Firmware on Cisco 2600 and Cisco 3600 Series Routers](#).

## Monitoring and Maintaining the AIC

The AIC provides a TFTP client for software upgrade and configuration image transfer. The methods for both actions, as well as how to override the existing software or configuration, are described below.

### Software Upgrade

When upgrading software, you must reset the AIC to run the new software. The AIC provides a protected (login required) command for software download. When you invoke this command with the TFTP server address as a parameter, the AIC connects to the IP address and, via TFTP, retrieves the software image file. After verifying that the software has been transferred successfully, the AIC replaces its running software with the newly downloaded software.

In the case of incompatible versions of IOS and AIC software, the IOS recognizes the difference and displays this information to you. You make the decision whether to upgrade or downgrade either the IOS or AIC software or to take no corrective action.

### Configuration Backup

The AIC CLI provides commands for storing and restoring configurations. Users can transfer the current configuration of the AIC to or from the TFTP server whose address is given as a parameter to the **put** or **get config** command. When a configuration file is transferred from the server to the AIC, the AIC takes on the new configuration.

The configuration is stored as a list of commands (script) that can be applied to the CLI of a AIC for configuration.

Two other useful commands are **get image** and **put config**. Use **get image** to get a new image, and **put config** to back up the configuration to the TFTP server.

Backup is not automatic, but the AIC reminds you, upon logout, to back up the configuration.

### Override

In the case that bad software is resident on the AIC or that the configured administrator password is lost, the AIC provides a method for recovering the card. Upon booting, the AIC begins a countdown, visible at the AIC local CLI (craft port). If an ASCII character is received on that local CLI channel (DSCC4 channel 2) during this countdown, the AIC enters a mode in which a limited CLI is available. At this

limited CLI, available over the craft port only, no login is necessary. You may execute commands for software upgrade or restore the configuration to its default. The restored default configuration takes effect upon a reset of the AIC card. See [reset \(alarm-interface\)](#) for more information.

After interrupting the countdown, you see an “[AIC Boot]:” prompt. From this prompt, you can enter “?” to see the available commands, “g” to **get** a new application image, or “d” to **delete** the current configuration and return to the defaults. (All commands require a carriage return.) In the case of the **get** command, you are prompted for the name of the file, the IP address of the TFTP server, and a confirmation.

## Show Commands

The Cisco IOS **show** commands can be used to display AIC configuration settings and the information sent to the IOS by the AIC. The **ping** command is useful for verifying asynchronous line connectivity.

The following Cisco IOS **show** command can be used to monitor and maintain alarms:

Command	Purpose
Router# <b>show alarm-interface</b> [ <i>slot-number</i> ] [ <i>summary</i> ]	Displays AIC configuration setting and the information sent to the IOS by the AIC.

A list of the AIC CLI **show** commands can be found in the [User Mode](#) section.

## Configuration Examples

This section provides the following configuration examples:

- [Configuring the AIC IP Address](#)
- [Configuring IP Route to the AIC](#)
  - [With an Unnumbered IP Address](#)
  - [Without an Unnumbered IP Address](#)
- [AIC CLI Configuration for Alarms](#)

### Configuring the AIC IP Address

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
!
hostname router
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
interface FastEthernet0/0
ip address 10.2.130.5 255.255.0.0
duplex auto
speed auto
no cdp enable

```

```
!  
interface Serial1/0  
ip address 172.128.12.1 255.255.255.252  
!  
ip kerberos source-interface any  
ip classless  
no ip http server  
!  
!  
alarm-interface 1  
ip address 172.128.12.2  
!  
dial-peer cor custom  
!  
line con 0  
exec-timeout 0 0  
transport input none  
line 33  
no exec  
transport preferred none  
transport input telnet  
transport output none  
stopbits 1  
line aux 0  
line vty 0 4  
password lab  
login  
!  
no scheduler allocate  
!  
end
```

## Configuring IP Route to the AIC

### With an Unnumbered IP Address

```
version 12.1  
no service single-slot-reload-enable  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname uut2-3660  
!  
logging rate-limit console 10 except errors  
no logging console  
!  
ip subnet-zero  
!  
!  
no ip finger  
no ip domain-lookup  
!  
call rsvp-sync  
cns event-service server  
!  
interface FastEthernet0/0  
ip address 10.2.130.2 255.255.0.0  
duplex auto  
speed auto
```

```

no cdp enable
!
interface Serial5/0
 ip unnumbered FastEthernet0/0
!
ip kerberos source-interface any
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.0.1
ip route 10.2.130.102 255.255.255.255 Serial5/0
ip http server
!
no cdp run
!
alarm-interface 5
 ip address 10.2.130.102
!
dial-peer cor custom
!
!
!
line con 0
 exec-timeout 0 0
 transport input none
line 161
 no exec
 transport preferred none
 transport input telnet
 transport output none
 stopbits 1
line aux 0
line vty 0 4
 password lab
 login
!
end

```

## Without an Unnumbered IP Address

```

uut5-2621#s run
Building configuration...

Current configuration :1318 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uut5-2621
!
logging rate-limit console 10 except errors
no logging console
!
ip subnet-zero
!
no ip finger
no ip domain-lookup
!
no ip dhcp-client network-discovery
!
interface FastEthernet0/0

```

```
ip address 10.2.130.5 255.255.0.0
duplex auto
speed auto
no cdp enable
!
interface Serial1/0
ip address 172.128.12.1 255.255.255.252
!
router rip
network 10.0.0.0
!
ip kerberos source-interface any
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.0.1
no ip http server
!
no cdp run
!
snmp-server packetsize 4096
snmp-server manager
!
!
alarm-interface 1
ip address 172.128.12.2
call rsvp-sync
!
dial-peer cor custom
!
line con 0
exec-timeout 0 0
transport input none
line 33
no exec
transport preferred none
transport input telnet
transport output none
stopbits 1
line aux 0
line vty 0 4
password lab
login
!
no scheduler allocate
!
end
```

## AIC CLI Configuration for Alarms

These examples are output from the command **show alarm config #** command.

### Discrete Alarm

```
description:west door
normally closed
normal state description:door closed
alarm state description:door open
alarm Level: 4
SNMP trap:enabled
```

## Analog Alarm Monitoring Current

```
description: thermostat
high-high state description: very hot
high-high Level: 4
high state description: hot
high Level: 4
normal state description: just right
low state description: cold
low Level: 4
low-low state description: very cold
low-low Level: 4
current-loop -5.2 5.4 15.0 25.0 35.1 45.6
SNMP trap: enabled
```

## Analog Alarm Monitoring Current Configured as a Discrete

```
description: east door
configured as discrete
normal state description: door closed
alarm description: door open
alarm Level: 4
current-loop 0.0 3.2 5.9
normally high
SNMP trap: enabled
```

## AIC CLI Syntax

The AIC CLI operates in four separate modes as described below. The mode currently in use determines the prompt used and the commands that are available. The modes are designed to mimic the modes available at the Cisco CLI:

- |                        |  |
|------------------------|--|
| <b>User Mode</b>       | The interface begins in user mode. This mode is not password-protected, by default, although it may be configured to be. In user mode, commands that show information are available. Also available is the command for entering privileged mode. The prompt in user mode is the AIC name followed by a right angle bracket (>).  |
| <b>Privileged Mode</b> | In privileged mode, configuration may be viewed and all user mode commands are available. Also available are the commands for reentering user mode and entering configuration modes. The prompt in privileged mode is the AIC name followed by a pound sign (#).<br><br>Upon entrance to privileged mode, if one or more users are already using privileged mode (or any configuration mode), the entering user is warned that those other users may be configuring the AIC. |

<b>Global Configuration Mode</b>	Global configuration mode allows configuration of global options and allows you to enter the subconfiguration modes. The commands available here are not available in other modes. The prompt in this mode is the AIC name followed by (config)#.
<b>Subconfiguration Modes</b>	The subconfiguration modes are used for configuring specific parts of the AIC. Commands available in this mode are not available in other modes. Four subconfiguration modes are available: alarm, control, TL1, and SNMP. The prompts in these modes are the AIC name followed by (config-alarm)#, (config-control)#, (config-tl1)#, and (config-snmp)#.

## AIC CLI User Levels

The AIC allows for three levels of users. For purposes of generality, in this document, the levels are referred to by number, where 1 is the most privileged level and 3 is the least privileged. Level 3 users are allowed to enter user mode only. Level 1 and 2 users are able to access all modes, but not all commands are available to level 2 users. The command descriptions indicate to which levels of users the command is available.

Login requirements are configurable. By default, login is required for privileged users (levels 1 and 2), but not for level 3 users. Login requirements can be configured so that login is required for users of all levels.

## AIC CLI Error Handling

If an AIC CLI command is entered incorrectly, an error message is displayed one line below the input, with a caret (^) indicating the invalid parameter.

## AIC CLI Commands

The command syntax and description for each command is shown below, organized by the mode in which the command is available.

The syntax of the commands includes the following symbols:

- #—number, validated according to requirements
- #.#.#.#—IP address
- \$—string surrounded by double “ ”, validated according to requirements
- <>—optional part of command

### User Mode

#### **enable**

Enters privileged mode. This command is available to level 1 and 2 users.

**exit**

Exits the AIC CLI. This command is available to level 1, 2, and 3 users.

**show tl1 alarm**

Displays TL1 attributes for every alarm point in the following format. This command is available to level 1, 2, and 3 users.

```
point 1
sid: router 3
aid: slot 2
cond: point 1
eqpt: eqpt
env: false
srveff: nsa
dirn: trmt
locn: nend
```

```
point 2
sid: router 3
aid: slot 2
cond: point 2
eqpt: eqpt
env: false
srveff: nsa
dirn: trmt
locn: nend
```

...

**show tl1 alarm #**

Displays TL1 attributes for the specified alarm point in the following format. This command is available to level 1, 2, and 3 users. The output format for alarms 1 to 56 is followed by the output format for alarms 57 to 64.

```
sid: router 3
aid: slot 2
cond: point 16
eqpt: eqpt
env: false
srveff: nsa
dirn: trmt
locn: nend
```

```
sid: router 3
aid: slot 2
cond: point 60
eqpt: eqpt
env: false
srveff: nsa
dirn: trmt
locn: nend
```

**show tl1 control**

Displays TL1 attributes for every control in the following format. This command is available to level 1, 2, and 3 users.

```
point 1
sid: router 3
```

```
aid: slot 2
cond: point 1
durn: 3.0 sec

point 2
sid: router 3
aid: slot 2
cond: point 2
durn: 3.0 sec

...
```

### show tl1 control #

Displays TL1 attributes for the specified control in the following format. This command is available to level 1, 2, and 3 users.

```
sid: router 3
aid: slot 2
cond: point 1
durn: 3.0 sec
```

### show snmp config

Displays the GET and TRAP community names and the SNMP global option, alarm-off trap. This command is available to level 1, 2, and 3 users.

```
GET community name: public
TRAP community name: public
SNMP alarm-off trap: enabled
```

### show snmp noc address list

Displays the four IP addresses to which SNMP traps are sent. This command is available to level 1, 2, and 3 users.

```
noc 1: 10.1.43.55
noc 2: 10.1.43.54
noc 3: 172.12.37.12
noc 4: 172.26.9.25
```

### show snmp noc address #

Displays the specified IP address to which SNMP traps are sent. This command is available to level 1, 2, and 3 users.

```
noc 3: 172.16.37.12
```

### show ip-address

Displays the AIC's IP address. This command is available to level 1, 2, and 3 users.

```
172.12.37.12
```

### show clock

Displays the current date and time. This command is available to level 1, 2, and 3 users.

```
14:12:34 06/23/01
```

**show history**

Displays the last ten input commands, as shown below. If fewer than ten commands have been entered since reboot, only those are displayed. Commands are shown in order of input. The most recent command is at the bottom. This command is available to level 1, 2, and 3 users.

```
show clock
enable
configure terminal
alarm 1
description "west door"
description normal "door closed"
description alarm "door open"
normally closed
no normally closed
exit
```

**show alarm state**

Displays the states of every alarm. Points in the alarmed state are indicated by a number (1 to 4), indicating the level (1 is critical, 4 is status), as shown. This command is available to level 1, 2, and 3 users.

```
1.....8 9.....16 17....24 25....32 33....40 41....48 49....56 57....64
----- --13----- --4-44-- 3---2--- ---4432- ----- --1----- --444--4
```

**show alarm state #**

Displays descriptions of the specified alarm point and the alarm state. This command is available to level 1, 2, and 3 users.

```
west door
normal
```

**show alarm config**

Displays the configuration of every alarm point. This command is available to level 1, 2, and 3 users.

```
point 1
description: alarm 1
normally open
normal state description: normal
alarm state description: alarm
alarm Level: 4
SNMP trap: enabled

point 2
description: alarm 2
normally closed
normal state description: normal
alarm state description: alarm
alarm Level: 4
SNMP trap: disabled

point 57
description: alarm 57
high-high state description: high-high
high-high Level: 4
high state description: high
high Level: 4
normal state description: normal
low state description: low
```

```

low Level: 4
low-low state description: low-low
low-low Level 4: low-low
current-loop 4.0 7.0 10.0 13.0 16.0 20.0
SNMP trap: enabled

```

### show alarm config #

Displays the configuration of the specified alarm. This command is available to level 1, 2, and 3 users. The output format for alarms 1 to 56 is followed by the output formats for alarms 57 to 64.

```

description: alarm 1
normally open
normal state description: normal
alarm state description: alarm
alarm Level: 4
SNMP trap: enabled

description: alarm 2
high-high state description: high-high
high-high Level: 4
high state description: high
high Level: 4
normal state description: normal
low state description: low
low Level: 4
low-low state description: low-low
low-low Level: 4
current-loop 4.0 7.0 10.0 13.0 16.0 20.0
SNMP trap: enabled

```

### show control state

Displays information about the logical and physical states of all the control points. This command is available to level 1, 2, and 3 users.

```

1.....8 9.....16
----- ----- logical (-RELEASED, ^OPERATED)
----- ----- physical (-OPEN, ^CLOSED)

```

### show control state #

Displays the logical and physical (in parentheses) states of the specified control point. This command is available to level 1, 2, and 3 users.

```

control 1
released latched (physically open)

```

### show control config

Displays the configuration of every control point. This command is available to level 1, 2, and 3 users.

```

point 1
description: generator 1
enabled
normally open
momentary duration: 3.2 seconds

point 2
description: generator 2
enabled

```

```
normally open
momentary duration: 40.2 seconds
...
```

### show control config #

Displays the configuration of the specified control. This command is available to level 1, 2, and 3 users.

```
description: generator 2
enabled
normally open
momentary duration: 3.2 seconds
```

### ping #.#.#.#

Sends a series of five ICMP echo request packets to the specified IP address and displays the results. Sample output is shown below. This command is available to level 1, 2, and 3 users.

```
aic# ping 10.2.0.1
Pinging IP address 1.2.0.1
Failure
Success
Success
Success
Success
Success rate is 80 percent (4/5)
aic#
```

## Privileged Mode

All commands available in user mode are available in privileged mode.

### exit

Reenters user mode. This command is available to level 1 and 2 users.

### show users

Displays usernames and levels of access. Currently logged-in users are indicated by an asterisk (\*). The user invoking this command is indicated by a right angle bracket (>). This command is available to level 1 and 2 users.

```
Level Username
>1   admin
  2   sue
*2   george
  2   noc1
  2   noc2
  2   noc3
  3   alvin
  3   simon
  3   ted
  3   unused4
  3   unused5
```

### configure terminal

Enters global configuration mode. This command is available to level 1 and 2 users.

**operate control # momentary**

Operates the specified control momentarily, according to the configured length of operation. This command is available to level 1 and 2 users.

**operate control # latch**

Operates the specified control. This command is available to level 1 and 2 users.

**release control # momentary**

Releases the specified control momentarily according to the configured length of release. This command is available to level 1 and 2 users.

**release control # latch**

Releases the specified control. This command is available to level 1 and 2 users.

**get image \$###**

Retrieves the software image from the specified IP address, according to the path and filename specified, via TFTP. This command is available to level 1 and 2 users.

**put image \$###**

Transfers the running software image to the specified IP address, according to the path and filename specified, via TFTP. This command is available to level 1 and 2 users.

**get config \$###**

Retrieves the configuration file from the specified IP address, according to the path and filename specified, via TFTP. This command is available to level 1 and 2 users.

**put config \$###**

Transfers the configuration file to the specified IP address, according to the path and filename specified, via TFTP. This command is available to level 1 and 2 users.

**Global Configuration Mode****exit**

Reenters privileged mode. This command is available to level 1 and 2 users.

**alarm #**

Enters alarm subconfiguration mode to configure the specified alarm number. This command is available to level 1 and 2 users.

**control #**

Enters control subconfiguration mode to configure the specified control number. This command is available to level 1 and 2 users.

**tl1**

Enters TL1 subconfiguration mode. This command is available to level 1 and 2 users.

**snmp**

Enters SNMP subconfiguration mode. This command is available to level 1 and 2 users.

**<no> name \$**

Configures the AIC's name to the specified string. If the <no> option is used, the name is set to the default value ("aic"). This command is available to level 1 and 2 users.

**<no> user #1 #2 \$1 \$2**

Assigns the first string as the username and the second string as the password for the specified user (second number) of the specified level (first number). If the <no> option is used, the string fields are not used and the username and password return to default values. The default string for both username and password for the level 1 user is "admin". The default strings for both username and password for level 2 users are "unused1", "unused2", and so on. The default strings for both username and password for level 3 users are "unused101", "unused102", and so on. This command is available to level 1 users.

**<no> early-login**

Requires login at entry to the AIC CLI (user mode) instead of at entry into privileged mode. If the <no> option is used, login is required at entry into privileged mode instead of at entry into user mode. This command is available to level 1 users.

## Alarm Subconfiguration Mode

**exit**

Reenters global configuration mode. This command is available to level 1 and 2 users.

**<no> description \$**

Sets the alarm's description to the specified string. If the <no> option is used, the string field is not required and the description is set to "alarm #", where # is the number of the alarm being configured. This command is available to level 1 and 2 users.

**<no> description normal \$**

Sets the alarm's description of its normal state to the specified string. If the <no> option is used, the string field is not required and the description is set to "normal". This command is available to level 1 and 2 users.

**<no> description alarm \$**

Sets the alarm's description of its alarm state to the specified string. If the <no> option is used, the string field is not required and the description is set to "alarm". While this string applies to points 57 to 64 only if configured as discrete, the command is always accepted. This command is available to level 1 and 2 users.

**<no> description high-high \$**

Sets the alarm's description of its high-high alarm state to the specified string. If the <no> option is used, the string field is not required and the description is set to "high-high". While this string applies only to points 57 to 64 configured as analog alarms, the command is always accepted. This command is available to level 1 and 2 users.

**<no> description high \$**

Sets the alarm's description of its high alarm state to the specified string. If the <no> option is used, the string field is not required and the description is set to "high". While this string applies only to points 57 to 64 configured as analog alarms, the command is always accepted. This command is available to level 1 and 2 users.

**<no> description low \$**

Sets the alarm's description of its low alarm state to the specified string. If the <no> option is used, the string field is not required and the description is set to "low". While this string applies only to points 57 to 64 configured as analog alarms, the command is always accepted. This command is available to level 1 and 2 users.

**<no> description low-low \$**

Sets the alarm's description of its low-low alarm state to the specified string. If the <no> option is used, the string field is not required and the description is set to "low-low". While this string applies only to points 57 to 64 configured as analog alarms, the command is always accepted. This command is available to level 1 and 2 users.

**<no> normally closed**

Sets the alarm's normal state to closed. If the <no> option is used, the normal state is set to open. This command applies only to points 1 to 56. This command is available to level 1 and 2 users.

**<no> level #**

Sets the alarm's level to the specified level. If the <no> option is used, the level field is not used and the level is set to the default level (4). While this level applies to points 57 to 64 only when configured as discrete, the command is always accepted. This command is available to level 1 and 2 users.

**<no> level high-high #**

Sets the alarm's high-high state level to the specified level. If the <no> option is used, the level field is not used and the level is set to the default level (4). While this level applies only to points 57 to 64 configured as analog, the command is always accepted. This command is available to level 1 and 2 users.

**<no> level high #**

Sets the alarm's high state level to the specified level. If the <no> option is used, the level field is not used and the level is set to the default level (4). While this level applies only to points 57 to 64 configured as analog, the command is always accepted. This command is available to level 1 and 2 users.

**<no> level low #**

Sets the alarm's low state level to the specified level. If the <no> option is used, level field is not used and the level is set to the default level (4). While this level applies only to points 57 to 64 configured as analog, the command is always accepted. This command is available to level 1 and 2 users.

**<no> level low-low #**

Sets the alarm's low-low state level to the specified level. If the <no> option is used, the level field is not used and the level is set to the default level (4). While this level applies only to points 57 to 64 configured as analog, the command is always accepted. This command is available to level 1 and 2 users.

**analog current-loop #1 #2 #3 #4 #5 #6**

This command is only for alarm points 57 to 64. It configures the alarm points as a current-loop monitoring analog alarm, where #1 and #6 represent the low and high bounds of the range of current, respectively, and where #2, #3, #4, and #5 represent thresholds. These values may be no less than -9999999.9 and no more than 9999999.9. The values specified must be in increasing order. (#1 is less than or equal to #2, #2 is less than or equal to #3, and so on.) This command is available to level 1 and 2 users.

**analog voltage #1 #2 #3 #4**

This command is only for alarm points 57 to 64. It configures the alarm points as voltage monitoring analog alarms, where #1, #2, #3, and #4 represent thresholds. The values specified must be in increasing order. (#1 is less than or equal to #2, #2 is less than or equal to #3, and so on.) This command is available to level 1 and 2 users.

**discrete current-loop #1 #2 #3 high**

This command is only for alarm points 57 to 64. It configures the alarm points as discrete, where #1 and #3 represent the low and high bounds of the range, respectively; #2 represents the threshold that indicates the alarm; and the normal state is high. This command is available to level 1 and 2 users.

**discrete current-loop #1 #2 #3 low**

This command is only for alarm points 57 to 64. It configures the alarm points as discrete, where #1 and #3 represent the low and high bounds of the range, respectively; #2 represents the threshold that indicates the alarm; and the normal state is low. This command is available to level 1 and 2 users.

**discrete voltage #1 high**

This command is only for alarm points 57 to 64. It configures the alarm points as discrete alarm points, where #1 represents the threshold that indicates the alarm, and the normal state is high. The bounds of the range are always -60.0 and 60.0 volts. This command is available to level 1 and 2 users.

**discrete voltage #1 low**

This command is only for alarm points 57 to 64. It configures the alarm points as discrete alarm points, where #1 represents the threshold that indicates the alarm, and the normal state is low. The bounds of the range are always -60.0 and 60.0 volts. This command is available to level 1 and 2 users.

**discrete**

This command is only for alarm points 57 to 64. It configures the alarm points as discrete alarm points so that they resemble the discrete alarm points 1 to 56. This allows users a simple way to configure an analog alarm as discrete, so that it acts like other discrete points. To reverse the alarm or change the threshold, another command must be used. This command is available to level 1 and 2 users.

**Control Subconfiguration Mode****exit**

Reenters global configuration mode. This command is available to level 1 and 2 users.

**<no> description \$**

Sets the control's description to the specified string. If the <no> option is used, the string field is not required and the description is set to "control #", where # is the number of the alarm being configured. This command is available to level 1 and 2 users.

**<no> normally closed**

Sets the control's normal state to closed. If the <no> option is used, the normal state is set to "open." This command is available to level 1 and 2 users.

**<no> disable**

Disables the control. If the <no> option is used, the control is enabled. This command is available to level 1 and 2 users.

**<no> momentary timer #**

Sets the control's momentary duration to the specified number of seconds. Valid values range from 0.1 to 600.0, in increments of tenths. If the <no> option is used, the momentary duration is set to 3.0 seconds. This command is available to level 1 and 2 users.

**TL1 Subconfiguration Mode****Note**

The TL1 parameters have limits on the number of characters that you can enter. To find the limits for a particular parameter, enter "?"

**exit**

Reenters global configuration mode. This command is available to level 1 and 2 users.

**<no> alarm # sid \$**

Sets the TL1 source identifier (SID) of the specified alarm to the specified string. If the <no> option is used, the SID is set to "AIC". This command is available to level 1 and 2 users.

To find the limits for this parameter:

```
Router(config-t11)# alarm 1 sid ?
```

WORD SID string (20 character max)

**<no> alarm # aid \$**

Sets the TL1 access identifier (AID) of the specified alarm to the specified string. If the <no> option is used, the AID is set to "UNDEFINED". This command is available to level 1 and 2 users.

**<no> alarm # cond \$**

Sets the TL1 condition (COND) of the specified alarm to the specified string. If the <no> option is used, the COND is set to "POINT #", where # is the specified alarm number. This command only applies to points 57 to 64 when they are configured as discrete alarm points. This command is available to level 1 and 2 users.

**<no> alarm # eqpt \$**

Sets the TL1 equipment (EQPT) of the specified alarm to the specified string. If the <no> option is used, the EQPT is set to "EQPT". This command is available to level 1 and 2 users.

**<no> alarm # env**

Sets the specified alarm as an environmental alarm (ENV = TRUE). If the <no> option is used, it is set as not an environmental alarm (ENV = FALSE). This command is available to level 1 and 2 users.

**<no> alarm # srveff**

Sets the specified alarm as service-affecting (SRVEFF = SA). If the <no> option is used, it is set as not service-affecting (SRVEFF = NSA). This command is available to level 1 and 2 users.

**alarm # dirn trmt**

Sets the TL1 direction (DIRN) of the specified alarm to transmit (TRMT). This command is available to level 1 and 2 users.

**alarm # dirn rcv**

Sets the TL1 direction (DIRN) of the specified alarm to receive (RCV). This command is available to level 1 and 2 users.

**alarm # dirn na**

Sets the TL1 direction (DIRN) of the specified alarm to NA. This command is available to level 1 and 2 users.

**alarm # locn nend**

Sets the TL1 location (LOCN) of the specified alarm to near-end (NEND). This command is available to level 1 and 2 users.

**alarm # locn fend**

Sets the TL1 location (LOCN) of the specified alarm to far-end (FEND). This command is available to level 1 and 2 users.

**alarm # locn line**

Sets the TL1 location (LOCN) of the specified alarm to line (LINE). This command is available to level 1 and 2 users.

**<no> control # sid \$**

Sets the TL1 source identifier (SID) of the specified control to the specified string. If the <no> option is used, the SID is set to "AIC". This command is available to level 1 and 2 users.

**<no> control # aid \$**

Sets the TL1 access identifier (AID) of the specified control to the specified string. If the <no> option is used, the AID is set to "UNDEFINED". This command is available to level 1 and 2 users.

**<no> control # cond \$**

Sets the TL1 condition (COND) of the specified control to the specified string. If the <no> option is used, the COND is set to "POINT #", where # is the specified control number. This command is available to level 1 and 2 users.

## SNMP Subconfiguration Mode

**exit**

Reenters global configuration mode. This command is available to level 1 and 2 users.

**<no> community \$**

Sets the SNMP community name to the specified string. Community names for other operations are set to "public" and cannot be changed. If the <no> option is used, the community name is set to "aic snmp". This command is available to level 1 and 2 users.

**<no> noc ip-address #.#.#.#**

Sets the specified number NOC address to the specified IP address. This also enables this NOC address. If the <no> option is used, the IP address is not used and the specified number NOC address is disabled. This command is available to level 1 and 2 users.

**<no> disable alarm #**

Disables the sending of traps upon change of state of the specified alarm. If the <no> option is used, the traps are enabled for this alarm.

**<no> disable alarm-off-trap**

Disables the sending of traps upon change of state to the inactive state for all alarms. If the <no> option is used, the traps are enabled.

# Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

## New Commands

- [alarm-interface](#)
- [debug alarm-interface](#)
- [reset \(alarm-interface\)](#)
- [show alarm-interface](#)

## Modified Commands

- [show diag](#)

# alarm-interface

To enter the alarm interface mode and configure the AIC, use the **alarm-interface** command in configuration interface mode. To leave the **alarm-interface** mode, use the **exit** command.

**alarm-interface** *slot-number*

<b>Syntax Description</b>	<i>slot-number</i>	Number of the port in which the AIC is installed.
---------------------------	--------------------	---

**Defaults** No default behavior or values.

**Command Modes** Configuration interface

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(2)XG	This command was introduced for the Cisco 2600 series and the Cisco 3600 series.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

**Examples** The following example shows how the **alarm-interface** command is used in conjunction with the **ip address** and the **reset** commands:

```
Router(config)# alarm-interface 5
Router(config-aic)# ip address 10.2.130.105
```

A change in an AIC's IP configuration may not take effect until the next time the card is started. Use the **reset** command to restart the card.

```
Router(config-aic)# reset
Alarm Interface Card in slot 5 restarted

Router(config-aic)# end
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip address</b>	Sets a primary or secondary IP address for an interface.
	<b>reset (alarm-interface)</b>	Resets the AIC CPU.

# debug alarm-interface

To show real-time activities in the data channel or the management channel of the AIC, use the **debug alarm-interface** command in privileged EXEC mode. To turn off the output, use the **undebug alarm-interface** command.

```
debug alarm-interface slot-number {data | management}
```

```
undebug alarm-interface slot-number {data | management}
```

## Syntax Description

<i>slot-number</i>	Router chassis slot where the AIC network module is installed.
<b>data</b>	Displays AIC serial data channel and asynchronous craft port communication activity.
<b>management</b>	Displays IOS-to-AIC communication activity.

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(2)XG	This command was introduced for the Cisco 2600 series and the Cisco 3600 series.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

## Usage Guidelines

This command allows you to observe the management channel activity from the AIC in the specified slot. Such activity shows that the software running on the AIC CPU has reached a minimum level of working order.

## Examples

The following example shows sample output for the **debug alarm-interface 1 management** command:

```
AIC Slot 1:STATUS received
```

The following is sample output for the **debug alarm-interface 1 data** command:

```
AIC Slot 1:STATUS received
aic_fastsend:particle count=1, len=1504
aic_pak_to_txring:scattered particle count=1, tx bytes=1504, leftover=0
aic_interrupt:# 30419 gstar=0x1000000
aic_safe_start:particle count=1, len=524
aic_pak_to_txring:scattered particle count=1, tx bytes=524, leftover=0
aic_process_TXivq:ivq - 0x42040000 at 15, slice 1
aic_interrupt:# 30420 gstar=0x1000000
aic_process_TXivq:ivq - 0x42040000 at 16, slice 1
aic_interrupt:# 30421 gstar=0x10000000
aic_scc_rx_intr:sts_dlen=0xC5E10000, len=1504, RSTA=0xA0
aic_serial_RX_interrupt:rxttype=1, len=1504, aic_scc_rx_intr:last_rxbd has aged, 2
```

```

aic_process_RXivq:ivq - 0x60000    at 13, slice 1
aic_interrupt:# 30422  gstar=0x10000000
aic_scc_rx_intr:sts_dlen=0xC20D0000, len=524, RSTA=0xA0
aic_serial_RX_interrupt:rxttype=1, len=524, aic_process_RXivq:ivq - 0x60000    at 14, slice
1
aic_interrupt:# 30423  gstar=0x20000000
aic_scc_rx_intr:sts_dlen=0xC00D0000, len=12, RSTA=0xA0
aic_mgmt_RX_interrupt:len=12
aic_mgmt_fastsend:particle count=1, len=20 / 20
aic_pak_to_txring:scattered particle count=1, tx bytes=20, leftover=0
aic_scc_rx_intr:last_rxbd has aged, 2
aic_process_RXivq:ivq - 0x10060000 at 37, slice 1
aic_interrupt:# 30424  gstar=0x20000000
aic_process_TXivq:ivq - 0x52040000 at 24, slice 1
    
```


**Related Commands**

Command	Description
<a href="#">alarm-interface</a>	Enters the alarm interface mode and configures the AIC.
<a href="#">reset (alarm-interface)</a>	Resets the AIC CPU.

# reset (alarm-interface)

To reset the CPU in the AIC, use the **reset** command in alarm interface mode.

**reset**

**Syntax Description** There are no keywords or arguments for this command.

**Defaults** No default behavior or values.

**Command Modes** Alarm interface

Command History	Release	Modification
	12.2(2)XG	This command was introduced for the Cisco 2600 series and the Cisco 3600 series.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

**Examples** The following message is returned after inputting the **reset** command:

```
Selected card in slot 1 restarted
```

Related Commands	Command	Description
	<a href="#">alarm-interface</a>	Enters the alarm interface mode and configures the AIC.

# show alarm-interface

To display the AIC configuration setting and the information sent to the IOS by the AIC, use the **show alarm-interface** command in privileged EXEC mode.

```
show alarm-interface [slot-number] [summary]
```

Syntax Description		
<i>slot-number</i>		Selects AIC by entering the slot number into which the AIC was placed.
<i>summary</i>		Selects the summary format for the output message.

**Defaults** Displays verbose message output and displays all AICs in all slot numbers on the router.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(2)XG	This command was introduced for the Cisco 2600 series and the Cisco 3600 series.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

**Examples** The following example provides a **show alarm-interface summary** display:

```
Router# show alarm-interface 5 summary
      Alarm Interface Card in Slot 5:
Configured IP address:10.2.130.102
Status:KEEPALIVE TIMER EXPIRED
Alarm Interface Card in Slot 5:
Configured IP address:10.2.130.102
Status:KEEPALIVE TIMER EXPIRED
```

The following is an example of a verbose **show alarm-interface** display:

```
Router# show alarm-interface 4
      Alarm Interface Card in Slot 4:
Configured IP address: 10.10.10.2
Status: RUNNING
Timer expires in < 11 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
```

show alarm-interface

-----

The following table describes the fields shown in the **show alarm-interface** displays.

Field	Description
Alarm Interface Card in Slot 4	Identifies the card type and slot number.
Configured IP address	Identifies the configured IP address.
Status	Identifies AIC card status. Can be one of the following: HARDWARE DETECTED RUNNING HARDWARE NOT PRESENT KEEPALIVE TIMER EXPIRED
Timer expires in	Identifies the current value of the KEEPALIVE TIMER, or states if the timer has been disabled. This line is only active when the status line reads HARDWARE DETECTED or RUNNING.  Used in troubleshooting to detect operational failures of the AIC.
Reported version	Indicates the active software version number.  Comparing the reported version to the expected version may reveal possible incompatibilities between the AIC's software and the IOS image.
Expected version	Indicates the expected software version number.  Comparing the reported version to the expected version may reveal possible incompatibilities between the AIC's software and the IOS image.
Last Self Test result	Indicates the result of the AIC's power on self-test (POST).
Last Start-Up message	Identifies any startup messages.
<AIC>	Identifies the AIC. Includes version and activity information.
Last Status severity	Rates the severity of the status message. Any number, other than 0 indicates a need for intervention. The number 1 indicates the most severe condition.
Last Status message	Indicates the last status message.

**Related Commands**

Command	Description
<a href="#">alarm-interface</a>	Enters the alarm interface mode and configures the AIC.

# show diag

To display the revision level information for cable modem cards, and hardware information regarding the AIC, use the **show diag** command in privileged EXEC mode.

**show diag**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.1 CA	This command was introduced.
	11.2 P	This command was modified to update the sample display for the port adapters PA-12E/2FE, PA-E3, and PA-T3.
	11.3 XA	This command was made available for Cisco IOS Release 11.3 XA.
	12.0(5)XQ	This command was enhanced and made available for the Cisco 1750 router.
	12.2(2)XG	This command was made available for the AIC on the Cisco 2600 series and the Cisco 3600 series.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

**Usage Guidelines** If the slot contains a cable modem card or an AIC network module, the information displayed is the electrically erasable programmable read-only memory (EEPROM) contents of that card or module.

**Examples** The following shows sample output from the **show diag** command for a 2611 with the NM-AIC-64 installed.

```
Router# show diag
Slot 0:
C2611 2E Mainboard Port adapter, 2 ports
Port adapter is analyzed
Port adapter insertion time unknown
EEPROM contents at hardware discovery:
Hardware Revision : 2.3
PCB Serial Number : JAD044808SG (1090473337)
Part Number : 73-2840-13
RMA History : 00
RMA Number : 0-0-0-0
Board Revision : C0
Deviation Number : 0-0
EEPROM format version 4
EEPROM contents (hex):
0x00: 04 FF 40 00 92 41 02 03 C1 18 4A 41 44 30 34 34
```

show diag

```
0x10: 38 30 38 53 47 20 28 31 30 39 30 34 37 33 33 33
0x20: 37 29 82 49 0B 18 0D 04 00 81 00 00 00 00 42 43
0x30: 30 80 00 00 00 00 FF FF FF FF FF FF FF FF FF
0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

```
Slot 1:
NM_AIC_64 Port adapter, 3 ports
Port adapter is analyzed
Port adapter insertion time unknown
EEPROM contents at hardware discovery:
Hardware Revision : 1.0
Part Number : 74-1923-01
Board Revision : 02
PCB Serial Number : DAN05060012
EEPROM format version 4
EEPROM contents (hex):
0x00: 04 FF 40 02 55 41 01 00 82 4A 07 83 01 42 30 32
0x10: C1 8B 44 41 4E 30 35 30 36 30 30 31 32 FF FF FF
0x20: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x30: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

The following is sample output from the **show diag** command displaying hardware-related information about the AIC:

```
Slot 1:
NM_AIC_64 Port adapter, 4 ports
Port adapter is analyzed
Port adapter insertion time unknown
EEPROM contents at hardware discovery:
Hardware Revision :1.0
Part Number :74-1923-01
Board Revision :02
PCB Serial Number :DAN05060038
EEPROM format version 4
EEPROM contents (hex):
0x00:04 FF 40 02 55 41 01 00 82 4A 07 83 01 42 30 32
0x10:C1 8B 44 41 4E 30 35 30 36 30 30 33 38 FF FF FF
0x20:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x30:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x40:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x50:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x60:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x70:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

The following table describes the fields shown in the **show diag** displays.

Field	Description
C2611 2E Mainboard Port adapter, 2 ports	Line card type; number of ports available.
Port adapter is analyzed	The system has identified the Cisco 2611 series port adapter.
Port adapter insertion time	Elapsed time since insertion.
Hardware Revision	Version number of the Cisco 2611 series port adapter.

Field	Description
PCB Serial Number	Serial number of the printed circuit board.
Part Number	The part number of the port adapter.
RMA History	Counter indicating how many times the port adapter has been returned and repaired.
RMA Number	Return material authorization number, which is an administrative number assigned if port adapter needs to be returned for repair.
Board Revision	Revision number (signifying a minor revision) of the Cisco uBR 7200 series port adapter.
Deviation Number	Revision number (signifying a minor deviation) of the Cisco uBR7200 series port adapter.
EEPROM format version	Version number of the EEPROM format.
EEPROM contents (hex)	Dumps of EEPROM programmed data.

# Glossary

**AIC**—Alarm Interface Controller.

**CiscoFusion**—Cisco internetworking architecture that fuses together the scalability, stability, and security advantages of the latest routing technologies with the performance benefits of ATM and LAN switching, and the management benefits of VLANs. See also Cisco IOS.

**Cisco IOS**—Cisco system software that provides common functionality, scalability, and security for all products under the CiscoFusion architecture. Cisco IOS allows centralized integrated, and automated installation and management of internetworks, while ensuring support for a wide variety of protocols, media, services, and platforms. See also CiscoFusion.

**CLEC**—Competitive local exchange carrier, CAP Competitive Access Provider. In the U.S., the Telecommunications Act of 1996 allowed competitive local exchange carriers / competitive access providers (CLECs) to compete with the RBOCs for local traffic. CLECs frequently partner with Tier 2/3 ISPs. The CLEC provides the access portion of the network and delivers bulk traffic to the ISP. CLECs tend to focus on business customers.

**DCE**—Data circuit-terminating equipment (ITU-T expansion). Devices and connections of a communications network that comprise the network end of the user-to-network interface. The DCE provides a physical connection to the network, forwards traffic, and provides a clocking signal used to synchronize data transmission between DCE and DTE devices. See DTE.

**DTE**—Data terminal equipment. Device at the user end of a user-network interface that serves as a data source, destination, or both. DTE connect to a data network through a DCE device and typically uses clocking signals generated by the DCE. See DCE.

**FTP**—File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.

**HDLC**—High-level data link control. Bit-oriented synchronous data link layer protocol developed by ISO. Derived from Synchronous Data Link Control (SDLC), HDLC specified a data encapsulation method on synchronous serial linked using frame characters and checksums. See SDLC.

**IP**— Internet Protocol. A connectionless protocol that operates at the network layer (Layer 3) of the OSI model. IP provides features for addressing, type-of-service specification, fragmentation and reassemble, and security. Defined in RFC 791. This protocol works with TCP and is usually identified as TCP/IP. See TCP/IP.

**ITU-T**—International Union Telecommunication Standardization Sector. International body that develops worldwide standards for telecommunications technologies.

**SDLC**—Synchronous Data Link Control. Systems Network Architecture (SNA) data layer communications protocol. SDLC is bit-oriented, full-duplex serial protocol that has spawned numerous similar protocols, including HDLC and LAPB. See SNA.

**SNA**—Systems Network Architecture. Large, complex, feature-rich network architecture developed in the 1970s by IBM. Similar in some respects to the OSI reference model, but with a number of differences. SNA is essentially composed of seven layers: data flow control layer, data-link control layer, path control layer, physical control layer, presentation services layer, transaction service layer, and transmission control layer.

**SNMP**— Simple Network Management Protocol. A TCP/IP protocol built to serve as a communications channel for internetwork management operating at the application layer of the IP stack.

**TCP**—Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmissions. TCP is part of the TCP/IP protocol stack. See TCP/IP and IP.

**TCP/IP**—Transmission Control Protocol/Internet Protocol. Common name for the suite of protocols developed by the U.S. Department of Defense in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best known protocols in the suite. See TCP and IP.

**Telnet**— Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connections, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.

**TFTP**—Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network.

**TL1**— Translation Language 1. A widely-used management protocol for telecommunications developed by Telcordia Technologies (formerly Bellcore) under the GR-833-CORE specification.

