CHAPTER 10

Understanding Cisco IPICS Serviceability and Diagnostic Information

This chapter describes the serviceability and diagnostic information that is available for Cisco IPICS and contains the following sections:

Understanding the Serviceability Drawer

The Serviceability drawer is located in the Server tab of the Administration Console and contains the following windows:

- Dashboard—The Dashboard window provides you with Cisco IPICS system and resource information. For more information about the information that is included in this window, see the "Viewing the Information in the Dashboard Window" section on page 10-2.
- Diagnostics—This window contains summary information about the Cisco IPICS server and the components of the Cisco IPICS system that interact with the server. From this window, you can also execute a diagnostic

script and download the results of that diagnostic script and additional diagnostic information. For more information about the Diagnostics window, see the "Viewing Cisco IPICS Server Diagnostic Information" section on page 10-7

- System Logs—This window displays logging information for Cisco IPICS. This information can be useful for troubleshooting or debugging your system. For more information about the System Logs window, see the "Viewing the Cisco IPICS System Logs" section on page 10-12.

Viewing the Information in the Dashboard Window

The dashboard window displays current, real-time information regarding the overall status of your system. This window displays the resources that you have used in your system and the resources that you have available. These resources range from system resources, such as central processing unit (CPU) and memory usage, to entity resources, such as channel, VTG, user, license, and RMS details.

The format of this window includes multiple panes, one for each resource. Each pane is also known as a dashboard.

Tip To refresh the elements in this window and obtain the latest information, click **Refresh** at the top of the window.

This section contains the following topics:

Understanding the System Dashboard

The System Dashboard displays information about the Cisco IPICS policy engine, server memory and hard disk usage, and multicast address information. See Table 10-1 for all of the elements that are contained in this pane.

For related information about policy engine services and trace files, see the "Obtaining Information about Dial Engine Services" section on page 8-2 and the "Managing Tracing for the Policy Engine" section on page 8-4.

Table 10-1 Elements in the System Dashboard

Element	Description
Policy counts [multi-purpose, invitation]	The total number of policies (either active or inactive) that are available for the policy engine, grouped by multi-purpose and invitation policies. For more information about policy types, see the "Adding a Policy" section on page 7-6 and the "Managing Actions for a Policy" section on page 7-8.
Policy Engine status	The status of the policy engine. A status of Up indicates that the policy engine is active; a status of Down indicates that the policy engine is inactive.
Configured activity log size (in MB)	The maximum size of the activity log file. **Note** For more information about activity logs, see the "Managing Activity Logs" section on page 2-119.
Current activity log size (in MB)	The current size of the activity log file.
Free memory (in MB)	The amount of random access memory (RAM) that is available in the Cisco IPICS server. The RAM is obtained from the Dual Inline Memory Modules (DIMMs) in the Cisco IPICS server.
Used memory (in MB)	The amount of RAM that the server currently uses.
CPU - percent idle	The percentage of CPU resources that are idle and available. The CPU resources are obtained from the CPU in the server.

Table 10-1 Elements in the System Dashboard (continued)

Element	Description
Disk usage (in GB) [used / free / total]	The amount of disk space that is currently used in your server, the amount of free disk space that is currently available in your server, and the total amount of hard disk space that is available in your server.
Total/Available number of multicast addresses in pool	The total number of multicast addresses in the multicast address pool and the number of multicast addresses that are available. For more information about the multicast address pool, see the "Managing the Multicast Pool" section on page 2-83.

Understanding the Channel Dashboard

The Channel Dashboard displays information about the total number of channels, the number of enabled, disabled, active, and connected channels in your system, and the current status of those channels. For more information about channels and how they are used in Cisco IPICS, see the "Managing PTT Channels and Channel Groups" section on page 2-2.

See Table 10-2 for all of the elements that are contained in this pane.

Table 10-2 Elements in the Channel Dashboard

Element	Description
Total number of channels	The total number of channels that you have configured in the Cisco IPICS server.
Number of enabled channels	The number of channels that are enabled.
Number of disabled channels	The number of channels that are disabled.
Media Connection Count (for enabled channels)	This field represents the total number of media connection assignments that are mapped to enabled channels in the **Configuration > Channels** window. If any enabled channel has more than one media connection assignment, this number will be greater than the number of enabled channels.
Number of active channels	The number of enabled channels that are present in a virtual talk group (VTG).

Understanding the Virtual Talk Group Dashboard

The Virtual Talk Group Dashboard displays information about the number of VTGs and inactive VTGs in your system. For more information about VTGs, see the "Managing VTGs" section on page 4-2.

See Table 10-3 for all of the elements that are contained in this pane.

Table 10-3 Elements in the VIrtual Talk Group Dashboard

Element	Description
Number of VTG templates	The number of VTG templates, or inactive VTGs, that exist in the server.
Number of active VTGs	The number of VTGs that are currently active.

Understanding the User Dashboard

The User Dashboard displays information about the number of users who are logged in to the Administration Console, the number of users who are logged in to Cisco IPICS by using a Cisco Unified IP Phone, and the number of users who are logged in to Cisco IPICS by using the PMC. For more information about users, see the "Managing Users" section on page 3-2.

See Table 10-4 for all elements in the user dashboard.

Table 10-4 Elements in the User Dashboard

Element	Description
Number of users logged in to the administration console	The total number of users who are logged in to the Administration Console.
Number of Cisco Unified IP phone users logged in to Cisco IPICS	The total number of Cisco Unified IP Phone users who are logged in to the Cisco IPICS system.
Number of PMC users logged in to Cisco IPICS	The total number of PMC users who are logged in to the Cisco IPICS system.
Number of users dialed in to Cisco IPICS	The total number of users who are using the dial-in functionality of the Cisco IPICS system.

Understanding the License Dashboard

The License Dashboard displays information about the total and available number of ports that are licensed for use with Cisco IPICS. For more information about licenses, see the "Managing Licenses" section on page 2-107.

See Table 10-5 for all of the elements that are contained in this pane.

Table 10-5 Elements in the License Dashboard

Element	Description
Multicast Ports	The total number of multicast ports that your Cisco IPICS system is licensed to use and the number of multicast ports that are available for use.
Cisco Unified IP Phone Ports	The total number of Cisco Unified IP Phone ports that your Cisco IPICS system is licensed to use and the number of Cisco Unified IP Phone ports that are available for use.
LMR Ports	The total number LMR ports that your Cisco IPICS system is licensed to use and the number of LMR ports that are available for use.
Dial Ports	The total number of policy engine dial ports that your Cisco IPICS system is licensed to use and the number of dial ports that are available for use.
PMC Ports	The total number of PMC ports that your Cisco IPICS system is licensed to use and the number of PMC ports that are available for use.

Understanding the RMS Dashboard

The RMS Dashboard displays information about the available number of voice ports that your system is licensed to use. For more information about the RMS, see the "Managing the RMS" section on page 2-91.

See Table 10-6 for all of the elements that are available in this pane.

Table 10-6 Elements in The RMS Dashboard

Element	Description
Total/Available voice ports	The total number of voice ports that are configured for your server and the number that are available for use.

Viewing Cisco IPICS Server Diagnostic Information

The Diagnostics window displays diagnostic information for various components of the Cisco IPICS server.

When you access the Diagnostics window, Cisco IPICS runs a script to obtain the diagnostic information; this information displays in the Diagnostic Summary pane. To refresh the pane and display the most current diagnostic information for your server, click the **Execute Diagnostic Script** button, which is located on the lower left side of the window.

To download all diagnostic information that is included in this window, along with the ipics.log file, click the **Download Diagnostic Results** button. For more information about how to download the diagnostic results, see the "Downloading the Server Diagnostic Information" section on page 10-11.

For more information about the ipics.log file, refer to the "Understanding the Cisco IPICS Logs" chapter of the *Cisco IPICS Troubleshooting Guide, Release 2.1(1)*. For more information about the log severity information that is included in each message, see the "Understanding the System Log Severities" section on page 10-13.

See Table 10-7 for all of the elements that are contained in the Diagnostic Summary pane.

Table 10-7 Elements in the Diagnostic Summary Pane

Element	Description
Cisco IPICS Server Hostname:	The host name of the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **hostname**
Cisco IPICS Server Current Date and Time:	The current date and time of the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **date**
Cisco IPICS Server OS Version:	The version of the Cisco IPICS operating system that is currently installed on the server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat /etc/redhat-release**
Cisco IPICS Server Software Version:	The current version of the Cisco IPICS server software. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **grep -i "ipics.server.version=" ${TOMCAT_HOME}/webapps/ipics_server/WEB-INF/classes/resources/common.properties** **Note** Be sure to include the quotation marks when you enter this command; the **grep** command searches for the text string that is inside the quotation marks.
Cisco IPICS Server Software Version upgrade history:	The date and time that the current version of Cisco IPICS was installed and provides a history, with release versions, of the times that the software has been uninstalled or upgraded. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat /etc/ipics-release.history**

Table 10-7 Elements in the Diagnostic Summary Pane (continued)

Element	Description
Hardware Platform Details:	Detailed information for the hardware platform. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat /etc/hwprofile**
CPU Details:	Detailed information for the CPU. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat /proc/cpuinfo**
Cisco IPICS Server Network Interface Card Information:	The configuration of the Network Interface Cards (NICs), and the packets that have been transmitted and received on the NICs, that are installed on the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session. [root]# **ifconfig**
Uploaded License File Name(s):	The name of the license file(s) that have been uploaded onto the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **ls -l ${TOMCAT_HOME}/webapps/license/***
Uploaded License File Contents:	The contents of the license file(s) that have been uploaded onto the server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat ${TOMCAT_HOME}/webapps/license/***
Cisco IPICS Database Status:	The current status of the database. The database can be either online or offline. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **onstat -**

Table 10-7 Elements in the Diagnostic Summary Pane (continued)

Element	Description
Cisco IPICS Tomcat Web Server Status:	The current status of the Tomcat service. The Tomcat service functions as the Web server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **ps -ef | grep tomcat** **Note** If the Tomcat service is inactive (down), you may not be able to access the Administration Console. In specific situations, your Cisco technical support representative may direct you to manually run the **ps -ef | grep tomcat** script to gather details about the overall state of the system.
Cisco IPICS Server Hard Disk Utilization Information:	Usage information for the hard disks in the server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **df -a**
Cisco IPICS PMC Configuration File Contents:	The contents of the pmc.ini file. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session: [root]# **cat ${TOMCAT_HOME}/webapps/ipics_server/pmcdownloads/pmc.ini** **Note** Cisco IPICS uses the pmc.ini file to determine how to communicate with the Cisco IPICS server. The pmc.ini file is present only if you have generated a PMC installer. If you have not yet generated the PMC installer file, Cisco IPICS displays the following message: `Cannot find any pmc.ini files under the /opt/cisco/ipics/tomcat/current/webapps/ipics_files/store/installer folder.` For more information about the pmc.ini file, and how to generate a PMC installer, see the "Managing PMC Versions" section on page 2-142.

Downloading the Server Diagnostic Information

Cisco IPICS displays the diagnostic summary of your system in the Diagnostic Summary pane. You can download this diagnostic summary, along with the current system log information, to your PC.

When you download the diagnostic summary, Cisco IPICS creates a tar file that contains the diagnostic summary and the most current ipics.log file. For more information about the ipics.log file, see the "Understanding the System Log Severities" section on page 10-13.

To download the server diagnostic information, perform the following procedure.

Procedure

Step 1 From the Administration Console, navigate to **Serviceability** > **Diagnostics**.

Step 2 Click **Download Diagnostic Results**.

The File Download dialog box displays.

Step 3 Click **Open** to open the tar file or save it to your PC.

Note The machine to which you download the zipped file must have an application, such as WinZip, installed to be able to open and extract the files from a tar file archive.

The tar file opens and displays the following files:

- The **tacout** file contains the latest diagnostic summary information.
- The **ipics.log** file contains the latest log information for Cisco IPICS.
- The **lmgrd.log** file contains log information for the license manager.

Step 4 To save the tar file to your PC, click **Save**.

A Save As dialog box displays.

Step 5 Navigate to the location on your PC where you want to save the tar file.

Step 6 Click **Save**.

The system unpacks the **tacout**, **ipics.log** and **lmgrd.log** files from the tar file, saves the files to the location that you specified, and closes the Save As dialog box.

Step 7 Use a text file viewer on your PC to view the log files.

Note You must use a text file viewer that can understand UNIX new-line characters, such as WordPad. If you use Notepad, the file will not display properly.

Viewing the Cisco IPICS System Logs

Cisco IPICS provides the ability to view the latest server log information in the System Logs window. The Recent System Log Entries pane in the **Serviceability > System Logs** window contains the log information that shows you the processes that have occurred in the different components of the Cisco IPICS system. For example, you can view the recent Tomcat service or policy engine entries. The information that is contained in these logs can help you to troubleshoot problems that you might encounter with Cisco IPICS.

Tip To refresh this window and see updated status information, click **Refresh**.

You can view the log information by using the Administration Console or you can save the log to a file and download it to your PC.

Note Cisco IPICS provides you with other logs that are not available in the **System Logs window**. You can view and download logs such as the Activity Log in the Administration Console. Cisco IPICS provides additional logs that are available by accessing the server with a console terminal. For a full list of the logs that Cisco IPICS provides, refer to the "Understanding the Cisco IPICS Logs" chapter of the *Cisco IPICS Troubleshooting Guide, Release 2.1(1)*.

This section includes the following topics:

Understanding the System Log Severities

The system log entries include messages of different severities. These messages range from informational-level messages to messages that indicate that a fatal error has occurred with Cisco IPICS.

Table 10-8 describes the types of system log entries that can display in the Recent System Log Entries pane.

Table 10-8 System Log Entry Types

Log Entry Type	Purpose
TRACE	Detailed debug information about the programmatic steps that Cisco IPICS performs to fulfill a request.
DEBUG	Debug information that is less detailed than TRACE information.
INFO	Informational messages about noteworthy events, such as the start of a scheduled policy.
WARN	Warning messages about occurrences such as incorrect user input or requests that Cisco IPICS cannot fulfill.

Table 10-8 System Log Entry Types (continued)

Log Entry Type	Purpose
ERROR	Messages that are similar to a WARN message, but with higher severity, such as in the case of insufficient licenses. ERROR messages display in red in the Recent System Log Entries pane.
FATAL	An unrecoverable error that requires your attention, such as a failed database connection or a router initialization failure. Often a FATAL error requires you to take immediate action to fix the specified error. When a FATAL error occurs, Cisco IPICS generates an error notification message and displays the message prominently in the current window of any user with system administrator or All privileges. Also, FATAL messages display in red in the Recent System Log Entries pane. If you continue to encounter FATAL errors, or if you experience unexpected system failures, contact your Cisco technical support representative for further analysis.

Note By default, Cisco IPICS does not capture the TRACE and DEBUG messages in the system logs. Cisco recommends that you do not activate these logging levels unless you are specifically instructed to do so by your Cisco technical support representative.

Sorting the System Logs By ERROR or WARNING Messages

To visually identify the type of status messages that display in the Recent System Log Entries pane, Cisco IPICS displays log entries of differing severities in the following text colors:

- Red—Red messages indicate that an ERROR-level error has occurred.

- Blue—Blue messages indicate that a WARNING-level error has occurred.
- Black—Black messages indicate that an INFO-level error has occurred.

Cisco IPICS displays the total number of ERROR, WARNING and INFO messages in the Status Summary area, directly below the Recent System Logs pane.

You can also view each ERROR or WARNING message by performing the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **Serviceability > System Logs**.

Step 2 Determine if there are any ERROR or WARNING messages in the log by viewing the Status Summary area, which is indicated by colored dots.

The Status Summary area provides you with the total number of messages that appear in the Recent System Log Entries pane.

If the number of red (ERROR) or blue (WARNING) messages is greater than zero, proceed to the next step.

Step 3 From the drop-down list box that is located in the upper right of the window, choose one of the following options:

- **Errors—**To find ERROR-level messages
- **Warnings—**To find WARNING-level messages

Step 4 Click on the arrow buttons to navigate and view each ERROR or WARNING message:

- Click | < to find the first message in the System Log.
- Click < to move backward one message in the System Log.
- Click > to move forward one message in the System Log.
- Click > | to move to the last message in the System Log.

Note If you are viewing the first message in the System Log, the | < and < arrow buttons appear dimmed. If you are viewing the last message in the System Log, the > and > | arrow buttons appear dimmed.

Downloading System Logs

Cisco IPICS displays the most current system log information in the Recent System Log Entries pane and allows you to download all of the system logs to your PC.

Cisco IPICS saves the log information in sequential log files, starting with ipics.log and continuing with ipics.log.1 through ipics.log.10.

- Cisco IPICS records system log information in the ipics.log file and continues to add data to it until the file reaches a maximum size of approximately 5.2 MB.
- When the ipics.log file reaches its maximum size, Cisco IPICS renames the file with an incremental number (starting at 1) and creates a new ipics.log file to capture the most current log data.

  This process of filling and incrementing files continues until you have ten system log files that range from ipics.log.1 to ipics.log.10, in addition to the most recent ipics.log file.
- When you have accumulated ten files, Cisco IPICS automatically purges the oldest file.

When you download your system logs, Cisco IPICS creates a zip file of all the ipics.log files.

The system logs are located in the following directory:

/opt/cisco/ipics/tomcat/current/logs

To download the system logs, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **Serviceability > System Logs**.

Step 2 Click **Download** at the bottom of the window, under the **Recent System Log Entries** pane.

The File Download dialog box displays.

Step 3 Click **Open** to open the ipics_logs.zip file or save it to your PC.

Note The machine to which you download the zipped file must have an application, such as WinZip, installed to be able to open and extract the files from a tar file archive.

The zip file opens and displays the list of ipics.log files.

Note To view the log file, you must use a text file viewer that can understand UNIX new-line characters, such as WordPad. If you use Notepad, the file will not display properly.

Step 4 To save the zip file to your PC, click **Save**.

A Save As dialog displays, from which you can navigate to the location to save the zip file on your PC.

Step 5 If you chose to save the zip file, click **Save**.

The system unzips the files from the zip file, saves the files to the location you specified, and closes the Save As dialog box.

SNMP Support for Cisco IPICS

The Cisco IPICS server software includes read-only support for Simple Network Management Protocol Version 3 (SNMPv3). SNMPv3 is a protocol that facilitates the secure exchange of management information between network devices.

Note Cisco IPICS does not support SNMP traps.

This section describes how you configure and use SNMP with Cisco IPICS and includes the following topics:

Supported MIBs and RFCs

The server software provides a set of management information base (MIB) files and Request for Comments (RFC) documents to support SNMPv3.

The MIBs are divided into the following types:

- MIBs that provide you with information about the Cisco Media Convergence Server (MCS) hardware. Table 10-9 lists the Cisco MCS hardware MIBs that Cisco IPICS supports and the object ID (OID) for each MIB.

Note Cisco IPICS does not supply you with the hardware MIBs. If your SNMP management console (such as, a MIB browser) does not contain these MIBs, you can search for the MIBs by accessing the Hewlett-Packard web site at http://www.hp.com and downloading them to your SNMP management console. You can search for the MIBs by specifying either the MIB name or OID.

- MIBs that provide you with information about network and system status. Table 10-10 lists the network status MIBs.

  These MIBs are the standard MIBs that are installed with the Net-SNMP package for the Cisco IPICS operating system. The MIBs are located in the following directory in the Cisco IPICS server:

  /usr/share/snmp/mibs

  If your SNMP management console does not contain these MIBs, you can download the MIBs from the server to your SNMP management console:

Cisco IPICS also includes RFCs with SNMP. RFCs provide you with definitions for MIBs and other SNMP elements. See Table 10-11 for the RFCs.

Table 10-9 lists the MIBs that are used for monitoring the status of the Cisco MCS hardware.

Table 10-9 Supported MIBs for Cisco MCS Hardware

Name	OID	Description
CPQIDA-MIB	1.3.6.1.4.1.232.3	This MIB module provides you with information about the Intelligent Drive Array.
CPQHOST-MIB	1.3.6.1.4.1.232.11	This MIB module provides you with host operating system information, including free memory, total memory size, free disk space, and total disk size.
CPQSTDEQ-MIB	1.3.6.1.4.1.232.1	This MIB module provides you with information about the standard equipment configuration for your server.
CPQTHRSH-MIB	1.3.6.1.4.1.232.10	This MIB module provides you with information about threshold management functions.
CPQSTSYS-MIB	1.3.6.1.4.1.232.8	This MIB module provides you with information about the files that are on the system.
CPQSINFO-MIB	1.3.6.1.4.1.232.2	This MIB module provides you with general system information.
CPQSM2-MIB	1.3.6.1.4.1.232.9	This MIB module provides you with information about the Remote Insight and Integrated Lights-Out Drivers and Agents (hprsm) service. This MIB also displays information about the network interface card (NIC), including NIC model, NIC type, NIC location, and the maximum transmission unit for the NIC.
CPQNIC-MIB	1.3.6.1.4.1.232.18	This MIB module provides you with information about the NIC.
CPQIDE-MIB	1.3.6.1.4.1.232.14	This MIB module provides you with information about the disk, including the disk model, its capacity, and its condition.

Table 10-10 lists the Net-SNMP MIBs that are used for monitoring the network.

Table 10-10 MIBs for Cisco IPICS Network and System Status

Name	Description
AGENTX-MIB.txt	This is the MIB module for the SNMP Agent Extensibility Protocol (AgentX).
DISMAN-EVENT-MIB.txt	The MIB module defines event triggers and actions for network management purposes.
DISMAN-SCHEDULE-MIB.txt	This MIB module defines a set of objects that provides mechanisms to schedule SNMP set operations periodically or at specific points in time.
DISMAN-SCRIPT-MIB.txt	This MIB module defines a set of objects that allow delegating management scripts to distributed managers.
EtherLike-MIB.txt	This MIB module describes generic objects for Ethernet-like network interfaces.
HCNUM-TC.txt	This MIB module contains textual conventions for high capacity data types.
HOST-RESOURCES-MIB.txt	This MIB module defines a uniform set of objects that are useful for the management of host computers. Host computers are independent of the operating system, network services, or any software application.
HOST-RESOURCES-TYPES.txt	This MIB module registers type definitions for storage types, device types, and file system types.
IANA-ADDRESS-FAMILY-NUMBERS-MIB.txt	This MIB module defines the AddressFamilyNumbers textual convention.
IANAifType-MIB.txt	This MIB module defines the IANAifType Textual Convention, and the enumerated values of the ifType object that is defined in the MIB-II ifTable.
IANA-LANGUAGE-MIB.txt	This MIB module registers object identifier values for well-known programming and scripting languages.
IANA-RTPROTO-MIB.txt	This MIB module defines the IANAipRouteProtocol and IANAipMRouteProtocol textual conventions, which are used in MIBs that need to identify unicast or multicast routing mechanisms.

Table 10-10 MIBs for Cisco IPICS Network and System Status (continued)

Name	Description
IF-INVERTED-STACK-MIB.txt	This MIB module provides the Inverted Stack Table for interface sub-layers.
IF-MIB.txt	This MIB module describes generic objects for network interface sublayers. This MIB is an updated version of the MIB-II ifTable, and incorporates the extensions defined in Request for Comments (RFC) 1229.
INET-ADDRESS-MIB.txt	This MIB module defines textual conventions for representing Internet addresses. An Internet address can be an IPv4 address, an IPv6 address, or a domain name system (DNS) name. This module also defines textual conventions for Internet port numbers, autonomous system numbers, and the length of an Internet address prefix.
IP-FORWARD-MIB.txt	This MIB module provides information regarding Classless Inter-Domain Routing (CIDR) multi-path IP routes.
IP-MIB.txt	This MIB module manages IP and Internet Control Message Protocol (ICMP) implementations, excluding the management of IP routes.
IPV6-ICMP-MIB.txt	This MIB module is used for entities that implement ICMP version 6 (ICMPv6).
IPV6-MIB.txt	This MIB module is used for entities that implement IP version 6 (IPv6).
IPV6-TC.txt	This MIB module is used for entities that implement the IPv6 TC protocol.
IPV6-TCP-MIB.txt	This MIB module is used for entities that implement TCP over IPv6.
IPV6-UDP-MIB.txt	This MIB module is used for entities that implement the User Datagram Protocol (UDP) over IPv6.
NET-SNMP-AGENT-MIB.txt	This MIB module defines control and monitoring structures for the Net-SNMP agent.
NET-SNMP-EXAMPLES-MIB.txt	This MIB module provides example MIB objects for agent module example implementations.

Table 10-10 MIBs for Cisco IPICS Network and System Status (continued)

Name	Description
NET-SNMP-EXTEND-MIB.txt	This MIB module defines a framework for scripted extensions for the Net-SNMP agent.
NET-SNMP-MIB.txt	This MIB module provides information about the top-level infrastructure of the net-SNMP project enterprise MIB tree.
NET-SNMP-TC.txt	This MIB module provides textual conventions and enumerations for the Net-SNMP project.
NOTIFICATION-LOG-MIB.txt	This MIB module MIB module is used for logging SNMP notifications (traps and informs).
RMON-MIB.txt	This MIB module contains standard information relating to remote network monitoring.
SMUX-MIB.txt	This MIB module describes SNMP Multiplexing (SMUX) protocol management objects.
SNMP-COMMUNITY-MIB.txt	This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2c, and SNMPv3.
SNMP-FRAMEWORK-MIB.txt	This MIB module is used for SNMP management architecture.
SNMP-MPD-MIB.txt	This MIB module is used for message processing and dispatching.
SNMP-NOTIFICATION-MIB.txt	This MIB module defines MIB objects that provide mechanisms to remotely configure the parameters that are used by an SNMP entity for the generation of notifications.
SNMP-PROXY-MIB.txt	This MIB module defines MIB objects that provide mechanisms to remotely configure the parameters that are used by a proxy forwarding application.
SNMP-TARGET-MIB.txt	This MIB module defines MIB objects that provide mechanisms to remotely configure the parameters that are used by an SNMP entity for the generation of SNMP messages.
SNMP-USER-BASED-SM-MIB.txt	This MIB module provides definitions for the SNMP user-based security model.
SNMP-USM-AES-MIB.txt	This MIB Defines object identities for the advanced encryption standard (AES) by the SNMP user-based security model.

Table 10-10 MIBs for Cisco IPICS Network and System Status (continued)

Name	Description
SNMP-USM-DH-OBJECTS-MIB.txt	This MIB module lists definitions for providing forward secrecy for key changes to the usmUserTable, and provides a method to kick-start access to the agent via a Diffie-Helman key agreement.
SNMP-VIEW-BASED-ACM-MIB.txt	This MIB module provides definitions for the View-based Access Control Model for SNMP.
SNMPv2-CONF.txt	This MIB module includes definitions for conformance groups.
SNMPv2-MIB.txt	This MIB module defines MIB objects for SNMPv2 entities.
SNMPv2-SMI.txt	This MIB module defines MIB objects for the Structure of Management Information (SMI).
SNMPv2-TC.txt	This MIB module defines MIB objects for SNMPv2 textual conventions.
SNMPv2-TM.txt	This MIB module defines MIB objects for SNMPv2 over UDP over IPv4.
TCP-MIB.txt	This MIB module manages TCP implementations.
TRANSPORT-ADDRESS-MIB.txt	This MIB module provides commonly used transport address definitions.
UCD-DEMO-MIB.txt	This MIB module is used for the University of California, Davis (UCD) demonstration.
UCD-DISKIO-MIB.txt	This MIB module defines objects for disk input and output (I/O) statistics.
UCD-DLMOD-MIB.txt	This MIB module defines the MIB objects for dynamic loadable MIB modules.
UCD-IPFWACC-MIB.txt	This MIB module defines the MIB components for reading information from the accounting rules IP firewall.
UCD-SNMP-MIB.txt	This MIB defines the private UCD SNMP MIB extensions.
UDP-MIB.txt	This MIB module manages UDP implementations.

Table 10-11 lists the RFCs that are part of the Cisco IPICS SNMP infrastructure.

Table 10-11 RFCs for Cisco IPICS SNMP

Name	Description
RFC-1215.txt	This RFC specifies a straightforward approach to defining traps that are used with SNMP.
RFC1155-SMI.txt	This RFC provides the common definitions for the structure and identification of management information for TCP/IP-based internets.
RFC1213-MIB.txt	This RFC defines the second version of the Management Information Base (MIB-II) that are used with network management protocols in TCP/IP-based internets.

Configuring an SNMP Management Console and MIB Browser for Use with Cisco IPICS

To configure a MIB browser for Cisco IPICS on your SNMP management console, perform the following procedure:

Procedure

Step 1 (Optional) If your SNMP management console does not contain the MIBs, download the MIBs to your SNMP management console by performing the following actions:

- Download the hardware status MIBs by downloading them from the Hewlett-Packard web site at http://www.hp.com.

  See Table 10-9 for a list of the system hardware status MIBs.

- Download the Net-SNMP MIBs that provide overall network status by performing the following steps:

  a. Log in to the Cisco IPICS server by using the root user ID.

  b. Navigate to the **/usr/share/snmp/mibs** directory by entering the following command:

     [root]# **cd /usr/share/snmp/mibs**

  c. Locate the MIB file(s) that you want to use.

d. Use a secure FTP program to download the MIB file(s) from the Cisco IPICS server to your SNMP management console.

   See Table 10-10 for a list of the Net-SNMP MIBs.

Step 2 From your SNMP management console, open a MIB browser that supports SNMPv3.

Step 3 Create a profile in the SNMP management console with the following information:

- Host: The IP address of the Cisco IPICS server
- User name: **ipics_snmp_user**
- Authentication password: **access_snmp**
- Authentication protocol (MD5 or Secure Hash Algorithm (SHA)): **MD5**
- Privacy/encryption password: **access_snmp**
- Privacy protocol (DES or AES): **DES**

Note The authentication protocol and privacy protocol are used to authenticate SNMPv3 messages.

Step 4 Use the supported MIB browser from your SNMP management console to perform read-only SNMP queries from the Cisco IPICS server.