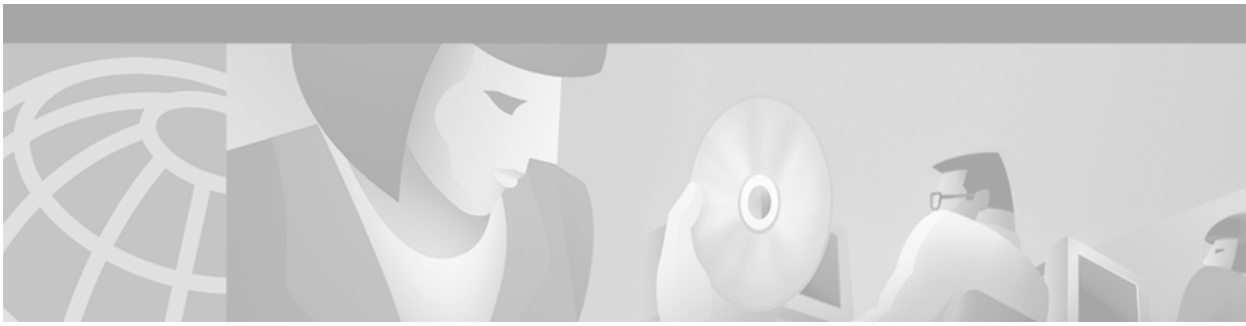

System Management Using System Controllers

The SC3640 System Controller runs Cisco IOS software and is designed to monitor and control up to seven Cisco AS5800 access servers (approximately 5000 ports) at a single location. The system controller can be installed at a remote facility so users can access multiple systems through a console port or Web interface. System administrators can download software configurations to any Cisco universal access server using Simple Network Management Protocol (SNMP) or Telnet. The system controller monitors Cisco equipment to provide performance data collection, accounting data collection, and logging.

For a complete description of the system controller and managed shelves commands in this chapter, refer to the "System Controller and Managed Shelves Commands" chapter of the *Cisco IOS Configuration Fundamentals Configuration Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online. For an overview of the SC3640 System Controller, see the "Cisco SC3640 System Controller" document on CCO at http://www.cisco.com/warp/public/cc/pd/as/as5800/prodlit/3640_ov.htm. For additional hardware configuration details, see the *Cisco SC3640 System Controller ICG* at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/sc3600dx/3640icg .

System Controller Configuration Task List

To configure the system controller and managed shelves, complete the tasks in the following sections:

- Configuring Shelf Discovery and Autoconfiguration
- Configuring the Virtual Console Feature
- Configuring the Health Monitor Feature
- Configuring Performance Data Collection
- Configuring Syslog Disk Logging
- Configuring the FTP Server Feature

See the end of this chapter for "System Controller and Managed Shelves Examples."

Configuring Shelf Discovery and Autoconfiguration

The Shelf Discovery and Autoconfiguration feature allows a system controller to automatically discover new shelves and properly configure them to interact with the system controller. The system controller communicates with its managed shelves through the Shelf Discovery Protocol (SDP), which runs on top of UDP.

The Shelf Discovery and Autoconfiguration features provide the following benefits:

- Control of multiple platforms from one location
- Easier method of configuring commands on all shelves
- Consolidated list of managed shelves and all interfaces on managed shelves

When the system controller detects that a shelf has been added or reloaded, it sends the following configuration commands to the shelf:

- SNMP configuration commands
  - Enables SNMP
  - Configures the community string to match the string used by the system controller
  - Configures the system controller as a target for traps
- Logging configuration commands
  - Enables logging
  - Configures the system controller as a target for logging
  - Configures timestamps on messages
- NTP configuration commands
  - Specifies the system controller as the time source
  - Updates the system calendar using the NTP time

Shelf Discovery and Autoconfiguration Task List

For a system controller to automatically discover and configure a shelf, both the system controller and the managed shelf must be configured. Perform the tasks described in the following sections:

- Configure the Shelf
- Configure the System Controller

Once you have configured the Shelf Discovery and Autoconfiguration feature on the system controller and managed shelves, you can increase the functionality of the system controller by configuring these additional features:

- Virtual Console
- Health Monitor
- Performance Data Collection
- Syslog Disk Logging
- FTP Server

Later sections in this chapter describe how to configure or use these features.

Configure the Shelf

To configure the shelf to use the system controller, use the following commands in global configuration mode:

Command	Purpose
syscon address *ip-address password*	Start the SDP process on the shelf. This command causes the shelf to start looking for a system controller at the specified address.
syscon shelf-id *number*	If the shelf does not already have a shelf ID, configure a shelf ID for the system controller to use.

To monitor the SDP process, use the **show syscon sdp** and **debug syscon sdp** commands.

Configure the System Controller

To configure the system controller, use the following commands in global configuration mode:

Command	Purpose
syscon community *string*	Specify the SNMP community string. During shelf autoconfiguration, this community string is automatically set on the shelf.
syscon password *password*	Specify the password used in authenticating messages between the system controller and managed shelves. This password must match the password configured on shelves.

Use the following commands to monitor SDP events and status:

Command	Purpose
show syscon discover [**brief** | **full**]	Display information about managed shelves.
show syscon sdp	Display information about SDP.
debug syscon sdp	Debug SDP.

Configuring the Virtual Console Feature

The Virtual Console feature allows you to access dial and router shelves connected to a system controller. During a system controller session, you can connect to a router or dial shelf at the same privilege level as the current system controller session. By entering one command, you can Telnet directly to a shelf, provide a username and password, and then go to the same privilege level as the system controller.

The Virtual Console feature allows you to connect to all managed shelves through one session and switch between sessions easily. You do not have to reenable privileged EXEC mode every time you switch to another shelf session.

This feature is useful when you need to do quick tasks on different managed shelves.

The Virtual Console feature has the following security aspects:

- The system controller and managed shelves typically communicate over a private network. Thus, unauthorized access is limited.

- Shelf units will only allow **attach shelf** commands from the IP address for the system controller, as specified in the **syscon address** command.
- The system controller will only accept requests from the connected shelf.

To use the Virtual Console feature, you must first configure the Shelf Discovery and Autoconfiguration feature. Refer to the "Configuring Shelf Discovery and Autoconfiguration"section for these tasks.

To use the Virtual Console feature, complete the tasks in the section that follows.

Using the Virtual Console Feature

To use the virtual console feature, use the following command beginning in user EXEC or privileged EXEC mode:

Command	Purpose
attach shelf *shelf-id*	On the system controller, connect to the managed shelf.
	Enter commands on the managed shelf.

You are connected to the managed system until one of the following occurs:

- You enter another **attach shelf** command.
- You enter the **exit** or **quit** commands at the EXEC prompt.
- You leave the session idle for a length of time (determined by the **exec-timeout** command on the shelf).
- You locally terminate the connection (^^x). (In a Telnet connection, ^^x will suspend the connection. With the **attach shelf** command, ^^x will break the connection.)

In every case except the first, control is returned to the system controller. In the first case, the connection to the current shelf is closed and a new connection to the specified shelf is opened.

Configuring the Health Monitor Feature

The Health Monitor feature monitors key performance attributes of the shelves managed by the system controller.

The Health Monitor feature continually polls its managed shelves to obtain the information stored in the Health Monitor MIB. Management stations collect information for all the shelves from the system controller rather than by polling each shelf individually.

In addition, you can configure specific performance thresholds for all managed shelves through simple commands on the system controller. The system controller uses SNMP to automatically configure the following on each managed shelf:

- Expressions in the EXPRESSION-MIB to calculate the attributes
- RMON alarms to poll the attributes at specific intervals
- RMON events to send traps to the system controller when an attribute exceeds its specified threshold

When threshold traps are received by the system controller, they are converted to Health Monitor traps and sent to trap destinations configured in the system controller.

The Health Monitor feature provides the following benefits:

- Simplified configuration of SNMP-based monitoring functions. Entering a few commands on the system controller configures all of the managed shelves to send traps.
- Management systems poll only the system controller to get Health Monitor MIB data. The management systems do not have to poll the individual shelves. Thus, this feature reduces network traffic and system resources used by management systems.

Health Monitor Task List

To use this feature, you must first configure the Shelf Discovery and Autoconfiguration feature. Refer to the "Configuring Shelf Discovery and Autoconfiguration" section for these tasks.

In addition, the SNMP Manager feature should be configured on the system controller. Use the **snmp-server manager** command to enable this feature. For details, see the "Configuring the Router as an SNMP Manager" section in the "Monitoring the Router and Network" chapter of this book.

To configure the Health Monitor feature, complete the tasks in the following sections:

- Using the Health Monitor
- Monitoring Shelf Attributes
- Supported MIBs and RFCs

Using the Health Monitor

When the Shelf Discovery and Autoconfiguration feature is enabled, the system controller automatically polls its managed shelves for Health Monitor MIB data. The system controller polls all the discovered shelves once a minute to obtain this data. Use the **show syscon mibpoll** EXEC command to display the current Health Monitor MIB data.

Optionally, you can configure the managed shelves to monitor certain attributes and notify the system controller when the attribute thresholds are exceeded, as described in the following section.

Monitoring Shelf Attributes

To configure monitored attributes for the managed shelves, use the following commands in global configuration mode on the system controller:

Command	Purpose
syscon monitor {**io-mem** *percent* | **modem** *percent* | **trunk** *percent*}	Specifies attributes for the system controller to monitor.
syscon monitor traps	Enables Health Monitor MIB trap forwarding on the system controller.
snmp-server host *host-addr* [*traps* | *informs*] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]	Specifies where the system controller sends the traps.
snmp-server enable traps	Enables trap generation on the system controller.

The Health Monitor MIB traps sent by the system controller are more readable than the traps sent to the system controller from the managed shelves. To send Health Monitor MIB traps to a management station, you should configure the **syscon monitor traps** command, the **snmp-server enable traps** command, and the appropriate **snmp-server host** command.

To view the status of the monitoring process, use the **show syscon monitor** EXEC command.

Supported MIBs and RFCs

This feature implements the Health Monitor MIB and utilizes MIB2 and POP-MGMT-MIB on the managed shelves.

Configuring Performance Data Collection

The Performance Data Collection feature allows a Cisco 3640 system controller to collect and store SNMP MIB data from its managed router and dial shelves. The system controller then serves as a central point for network management data collection.

The system controller collects the raw data from the managed shelves periodically, saves the data, and provides a single access point for a central network management application. The data can then be uploaded to a network management station using FTP or TFTP.

Performance data is stored on a disk local to the system controller. The files are located at disk0:/performance/shelf-*shelfid*/*pollgroupname*.*unixtimestamp*. A new file is created each time the system controller collects data from a shelf.

The Performance Data Collection feature provides the following benefits:

- Remote network management stations can get performance data from one place, as a single file transferred via FTP or TFTP. This benefit reduces network traffic and resources in the management station because the station does not have to poll each individual shelf.
- The bulk transfer method of collecting data generates less traffic on the network than collecting the same amount of information using SNMP requests. The bulk transfer method also impacts the managed shelves less than SNMP polling.

Performance Data Collection Task List

To use this feature, you must first configure the following features:

- Shelf Discovery and Autoconfiguration. See the "Configuring Shelf Discovery and Autoconfiguration" section for these tasks.
- FTP Server. See the "Configuring the FTP Server Feature" section for these tasks.
- SNMP Manager. See the "Configuring the Router as an SNMP Manager" section in the "Monitoring the Router and Network" chapter of this book for configuration details.

In addition, the system clock should be set to the current time before the data collection starts. For system clock configuration details, see the "Performing Basic System Management" chapter in this book. Network Time Protocol (NTP) is the recommended method for obtaining the time.

To configure and use the Performance Data Collection feature, complete the tasks in the following sections:

- Configure Performance Data Collection on the System Controller

- What to Do Next

Configure Performance Data Collection on the System Controller

To configure Performance Data Collection on the system controller, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# syscon poll-group` *name*	Specifies the name of the performance data set and enters poll-group configuration mode. Poll-group configuration mode is indicated by the (config-poll-gr) router prompt.
Step 2	`Router(config-poll-gr)# oid` *object-id*	Specifies the MIB variables to collect. Repeat this command for each MIB variable.
Step 3	`Router(config-poll-gr)# transfer-mode {bulk | poll}`	Sets the data collection method.
Step 4	`Router(config-poll-gr)# shelf-type` *sysObjectID*	(Optional) Specifies the shelf types for the data collection. Repeat this step for each shelf type. The default is all shelf types.
Step 5	`Router(config-poll-gr)# poll-interval` *minutes*	(Optional) Sets the data collection interval, in minutes. The default is 10 minutes.
Step 6	`Router(config-poll-gr)# samples` *number*	(Optional) Specifies the maximum number of stored data sets. The default is 10.
Step 7	`Router(config-poll-gr)# enable`	Enables Performance Data Collection.
Step 8	`Router(config-poll-gr)# exit`	Exits poll-group configuration mode. This step ends the configuration of the performance data set.
Step 9		(Optional) Repeat steps 1 through 8 for each additional poll group.
Step 10	`Router(config)# end`	Returns the CLI to privileged EXEC mode.
Step 11	`Router# more system:running-config` `Router# show syscon perfdata`	Shows current configuration information so that you can verify that performance data is correctly configured.
Step 12	`Router# copy system:running-config nvram:startup-config`	Saves the configuration.

Configure the system controller to collect all the MIB variables that your network management station uses. Thus, the network management station can obtain all the information from the system controller without ever polling a managed shelf.

What to Do Next

After the system controller has collected the data, you must copy data from the system controller's disk (via FTP or TFTP) to the network management station. Use the **poll-interval** and **samples** commands to determine how long the data is stored on the disk before it is erased.

Configuring Syslog Disk Logging

The Syslog Disk Logging feature allows you to collect, store, and retrieve all managed shelf syslog (system log) messages through the system controller. The system controller receives syslog messages from managed shelves and stores these messages in subfiles on its disk.

Each syslog message stored in a subfile contains the following information:

- Host IP address
- Facility
- Severity
- Timestamp (date and time) set by the managed shelf
- Message text

In addition, this feature provides an enhanced method of viewing messages in the logging history table. Messages can be displayed based on host IP address, time received, and order received.

The Syslog Disk Logging feature provides the following benefits:

- The system controller provides one storage and retrieval location for syslog messages from multiple hosts on the network.
- You can display syslog messages based on time, hostname, or order received.
- Subfiles can store a large number of messages.
- Messages are preserved across system reloads. Without this feature, messages are stored in syslog history tables, which are lost when the system reboots.

Subfiles

Subfiles provide additional storage space for syslog messages. They contain the large logging history tables and preserve the tables even when the machine is reloaded.

The system controller creates subfiles using the same name as the root and a different extension for each subfile:

- The current subfile is called *name*.cur.
- The first archived subfile is *name*.1.
- The second is *name*.2.
- The last (oldest) archived subfile's extension is one less than the maximum number of subfiles (*number*-1). The complete subfile name is *name.number*-1.

The file space is preallocated before any messages are received to provide deterministic disk space allocation. When the system controller receives a new syslog message, the following events occur:

- The router determines if there is enough room in the current file (*name*.cur) to add the new data.
- If there is enough room, the data is added to the end of the current file.
- If there is not enough room, the last subfile is deleted (*name.number*-1).
  - The renaming subfiles are renamed to use the next (higher) extension.
  - A new *name*.cur is created.
  - The data is placed in the new current file.

Syslog Disk Logging Task List

To use this feature, you must first configure the Shelf Discovery and Autoconfiguration feature, which automatically configures the managed shelves to send syslog messages to the system controller. In addition, the **service timestamp log datetime** command is configured on all the shelves. Refer to the "Configuring Shelf Discovery and Autoconfiguration" section for these tasks.

If you want messages generated by the system controller to be stored in the subfiles along with messages received from managed shelves, configure the system controller as the syslog server for its own messages using the **logging** *host* command.

To enable and use the Syslog Disk Logging feature, perform the following tasks:

- Creating the Syslog-Server Subfiles
- Displaying Syslog Messages

Creating the Syslog-Server Subfiles

Normally, the system controller just stores messages in the logging history table. However, to store a larger number of messages and preserve the messages across reboots of the machine, you need to create syslog server subfiles. To create these subfiles, use the following commands in global configuration mode:

Command	Purpose
logging syslog-server *size number dir-name*	Creates the syslog-server subfiles.
dir disk0:	Verifies that the files have been created.

A typical subfile configuration is five subfiles with a size of 500 KB. This configuration stores significant volumes of syslog data but still allows efficient searching. If the subfiles are too large or numerous, the **show syslog-server** command might be slow.

Displaying Syslog Messages

To view syslog messages stored in subfiles, use the following command in EXEC mode:

Command	Purpose
show syslog-server [**last** *number* | **since** [*date*] *hh*:*mm*:*ss*] [**source** *ip-address*]	Displays syslog messages.

Configuring the FTP Server Feature

The FTP Server feature configures a router to act as an FTP server. FTP clients can copy files to and from certain directories on the router. In addition, the router can perform many other standard FTP server functions. For example, the FTP Server allows you to retrieve files, such as syslog files, from the disk file system on the router.

Supported FTP Commands

When the router receives a request for an FTP connection, the FTP Server process is started. The FTP Server prompts for a username and password.

After you supply a valid username and password, you can enter various commands. Not all FTP commands are supported by this FTP Server implementation. The FTP Server responds to the following FTP client commands:

!	cr	image	nmap	reset	sunique
append	debug	lcd	ntrans	rhelp	system
ascii	dir	ls	open	rstatus	tenex
binary	disconnect	macdef	prompt	runique	trace
bye	get	mdir	put	send	type
case	glob	mkdir	pwd	sendport	user
cd	hash	mls	quit	site	verbose
chmod	help	mode	quote	size	
close	idle	nlist	reget	status	

Refer to the documentation for your FTP client for detailed information on these commands. For example, if you are using a UNIX workstation as the FTP client, enter the **man ftp** command for descriptions of these commands.

To use the FTP Server feature, complete the task in the section that follows.

Enabling the FTP Server

To enable the FTP Server, use the following commands in global configuration mode:

Command	Purpose
ftp-server enable	Enables the FTP Server.
ftp-server topdir *directory*	Restricts the region where the FTP clients can read or write files.

System Controller and Managed Shelves Examples

The following sections provide system controller and managed shelves examples:

- Shelf Discovery and Autoconfiguration Examples
- Virtual Console Examples
- Health Monitor Examples
- Performance Data Collection Examples
- Syslog Disk Logging Examples
- FTP Server Examples

Shelf Discovery and Autoconfiguration Examples

The following sample configuration enables a device to begin serving as a system controller. The system controller waits to be contacted by shelves and then provides them with the appropriate configuration.

```
syscon password syspassword
syscon community public
```

The follow example configures a shelf to use the system controller at 172.23.66.111. The shelf ID is 99. If you are using a Cisco AS5800, you do not need to specify a shelf ID with the **syscon shelf-id** command.

```
syscon address 172.23.66.111 syspassword
syscon shelf-id 99
```

After the shelf has contacted the system controller through SDP, the system controller configures the managed shelf with the following commands:

```
snmp-server community public RW
snmp-server enable traps
snmp-server host 172.23.66.111 traps version 2c public
snmp-server packetsize 1480
ntp server 172.23.66.111
ntp update-calendar
service timestamps log datetime msec
logging 172.23.66.111
logging trap
```

The following sample **debug syscon sdp** output on the managed shelf shows the shelf contacting the system controller. The shelf sends a Hello packet to the system controller at 172.23.66.111. The system controller responds with the autoconfiguration commands. The remaining lines show the Hello packets exchanged between the shelf and the system controller.

```
Shelf# debug syscon sdp

SYSCTLR: Hello packet sent to the SYSCTLR at 172.23.66.111
SYSCTLR: Command packet received from SYSCTLR
Feb 24 17:24:16.713: %SHELF-6-SYSCTLR_ESTABLISHED: Configured via system controller
located at 172.23.66.111
SYSCTLR: Rcvd HELLO from SYSCTLR at 172.23.66.111
SYSCTLR: Hello packet sent to the SYSCTLR at 172.23.66.111
SYSCTLR: Rcvd HELLO from SYSCTLR at 172.23.66.111
```

The following sample **debug syscon sdp** output on the system controller shows the system controller discovering the managed shelf. In the first few lines, the system controller receives a Hello packet from shelf 99 at 172.23.66.106. The system controller responds with a Hello packet. When the shelf sends another Hello packet, the system controller resets the timer and sends another packet.

```
Syscon# debug syscon sdp

SYSCTLR: Hello packet received via UDP from 172.23.66.106
%SYSCTLR-6-SHELF_ADD: Shelf 99 discovered located at address 172.23.66.106
Hello packet sent to the RS located at 172.23.66.106
SYSCTLR: Hello packet received via UDP from 172.23.66.106
Timer for shelf 99 updated, shelf is alive
Hello packet sent to the RS located at 172.23.66.106
```

Virtual Console Examples

In the following example, a user connects to a managed shelf from the system controller from user EXEC and privileged EXEC modes. Notice that the user connects to the shelf at the current user privilege level.

```
systemcont> show syscon
Shelf# 2  172.23.66.102 SDB update  09:09:16 PST Jan 27 1998
systemcont> attach shelf 2
Trying 172.23.66.102 ... Open

shelf2> show syscon
Current uptime 09:10:00 PST Jan 27 1998, system controller 172.23.66.100
Last hello packet received at 09:09:16 PST Jan 27 1998
8625 Total SDP packets
    0 packets with bad MD5 hash
    4311 Hello packets received
    4314 Hello packets sent
    0 Command packets received
    0 Command packets sent
shelf2> quit

[Connection to 172.23.66.102 closed by foreign host]
systemcont> enable
Password:
systemcont# attach shelf 2
Trying 172.23.66.102 ... Open

shelf2# show syscon sdp
Current uptime 09:10:45 PST Jan 27 1998, system controller 172.23.66.100
Last hello packet received at 09:10:14 PST Jan 27 1998
8627 Total SDP packets
    0 packets with bad MD5 hash
    4312 Hello packets received
    4315 Hello packets sent
    0 Command packets received
    0 Command packets sent
shelf2# exit

[Connection to 172.23.66.102 closed by foreign host]
systemcont#
```

Health Monitor Examples

The following system controller sample configuration monitors three attributes and forwards traps to myhost.cisco.com.

```
! The following commands are configured as part of the Shelf Discovery and
! Autoconfiguration feature.
!
syscon password syspassword
syscon community syscommunity
!
! The following lines configure the shelves to monitor IO memory on all the shelves and
! total modem and trunk utilization.
! If IO memory utilization exceeds 10%, the shelf sends a trap to the system controller.
! If the total utilization of all modems or trunk on all shelves exceeds 5%, the system
! controller generates a trap.
!
```

```
syscon monitor modem 5
syscon monitor trunk 5
syscon monitor io-mem 10
!
! The following commands enable forwarding of traps. When the system controller receives
! a trap from a managed shelf or generates one itself, it forwards the trap to the host
! called myhost using the community string public.
!
syscon monitor traps
snmp-server host myhost.cisco.com public
snmp-server enable traps
!
! The following line enables the SNMP manager process.
!
snmp-server manager
```

You can view the current configuration of Health Monitor on the system controller with the **show syscon monitor** command.

```
nnm3640-2# show syscon monitor

Health Monitor setup status on the shel(f,ves):
Shelf#  Shelf IP Address        Monitoring Type Threshold Value Status
    3   172.23.66.109           IO-Mem            10            Active

Health Monitor setup status on the system controller:
Monitoring Type Threshold Value Status
 Trunk            5             Active
 Modem            5             Active
```

The system will automatically configure each shelf to monitor its IO memory utilization. You can check the RMON configuration using the **show rmon alarms** and **show rmon events** commands on a managed shelf.

```
nnm7206-6# show rmon alarms

Alarm 596 is active, owned by IOMem
 Monitors ciscoExperiment.22.1.4.1.1.2.1.0.0.0 every 120 second(s)
 Taking absolute samples, last value was 66
 Rising threshold is 10, assigned to event 514
 Falling threshold is 0, assigned to event 0
 On startup enable rising or falling alarm

nnm7206-6# show rmon events

Event 514 is active, owned by IOMem
 Description is Send snmp trap to health_monitor
 Event firing causes trap to community syscommunity, last fired 00:04:02
```

Performance Data Collection Examples

The following partial sample configuration file configures Performance Data Collection on a system controller:

```
! Enable the FTP Server on the system controller and specify the top-level directory
! for FTP operations.
!
ftp-server enable
ftp-server topdir disk0:/performance
!
! Configure the device to act as a system controller and specify the passwords.
!
syscon password semtest
syscon community private
!
! Configure and enable the different poll groups.
!
syscon poll-group popmgmt
 oid cpmDS0Usage.1.*
 oid cpmActiveCallSummary.1.*
 oid cpmCallHistorySummary.3.*
 transfer-mode bulk
 poll-interval 25
 samples 5
 enable
syscon poll-group cmlineinfo
 oid cmLineInfo.1.*
 oid cmLineInfo.2.*
 oid cmLineInfo.3.*
 oid cmLineInfo.4.*
 transfer-mode bulk
 poll-interval 20
 samples 5
 enable
syscon poll-group cpmds0usage
 oid cpmDS0Usage.2.0
 oid cpmDS0Usage.3.0
 oid cpmDS0Usage.4.0
 oid cpmDS0Usage.5.0
 oid cpmDS0Usage.6.0
 oid cpmDS0Usage.7.0
 transfer-mode poll
 poll-interval 15
 samples 10
 enable
syscon poll-group callfailure
 oid cpmCallFailure.1.0
 oid cpmCallFailure.2.0
 oid cpmCallFailure.3.0
 oid cpmCallFailure.4.0
 oid cpmCallFailure.5.0
 oid cpmCallFailure.6.0
 oid cpmCallHistorySummary.1.0
 oid cpmCallHistorySummary.2.0
 transfer-mode poll
 poll-interval 20
 samples 10
 enable
syscon poll-group cmsysteminfo
 oid cmSystemInfo.1.0
 oid cmSystemInfo.2.0
 oid cmSystemInfo.3.0
```

```
 oid cmSystemInfo.4.0
 oid cmSystemInfo.5.0
 oid cmSystemInfo.6.0
 oid cmSystemInfo.7.0
 oid cmSystemInfo.8.0
 oid cmSystemInfo.9.0
 oid cmSystemInfo.10.0
 transfer-mode poll
 poll-interval 25
 shelf-type 108
 samples 12
 enable
syscon poll-group iftable
 oid ifEntry.3.*
 oid ifEntry.4.*
 oid ifEntry.5.*
 oid ifEntry.8.*
 transfer-mode poll
 poll-interval 20
 samples 10
 enable
```

The following **show syscon perfdata** output indicates that the system controller is collecting data from shelf 0:

```
SysCont# show syscon perfdata

Performance Data Collection:

          Poll        Last     Total     Get    GetBulk  Bulk Xfer
Shelf#    Group       File    Requests Requests Requests Requests  Errors
    0  popmgmt      891873300       5        0        0        5       0
       cmlineinfo   891873600       5        0        0        5       0
       cpmds0usage  891873000       1        1        0        0       0
       callfailure  891873600       1        1        0        0       0
       cmsysteminfo 891873300       1        1        0        0       0
       iftable      891873647     651        1      650        0       0
```

Use the **dir** command to view the data sets. Note that the file extension corresponds to the “Last File” time in the **show syscon perfdata** command.

```
SysCont# dir disk0:/performance/shelf-0
Directory of disk0:/performance/shelf-0/

128  -rw-         238   Apr 06 1998 14:29:59  cpmds0usage.891873000
192  -rw-         402   Apr 06 1998 14:34:59  cmsysteminfo.891873300
194  -rw-         385   Apr 06 1998 14:39:59  callfailure.891873600
196  -rw-      119967   Apr 06 1998 14:40:59  iftable.891873647

219791360 bytes total (218087424 bytes free)
```

You can watch the details of the data collection using the **debug syscon perfdata** command:

```
SysCont# debug syscon perfdata

PERF: Start 'cmlineinfo' timer, next cycle in 5 mins, 31 secs
PERF: Timer event: 'popmgmt', 15 minutes
PERF: Bulk file create: 'popmgmt', shelf 0, pc 60ACBB10
PERF: SNMP resp: Type 4, 'popmgmt', shelf 0, error_st 0
PERF: FTP transfer: 'popmgmt', shelf 0, pc 60ACBB10
PERF: SNMP resp: Type 5, 'popmgmt', shelf 0, error_st 0
PERF: Deleted disk0:/performance/shelf-0/popmgmt.891809700
PERF: Timer event: 'cpmds0usage', 15 minutes
PERF: Polling 'cpmds0usage', shelf 0, pc 60ADE004
PERF: SNMP resp: Type 6, 'cpmds0usage', shelf 0, error_st 0
PERF: Logged polled data to disk0:/performance/shelf-0/cpmds0usage.891873900
PERF: Timer event: 'iftable', 12 minutes
PERF: Bulk file create: 'iftable', shelf 0, pc 60BE16AC
PERF: SNMP resp: Type 4, 'iftable', shelf 0, error_st 0
PERF: FTP transfer: 'iftable', shelf 0, pc 60BE16AC
PERF: SNMP resp: Type 5, 'iftable', shelf 0, error_st 0
PERF: Deleted disk0:/performance/shelf-0/iftable.891883559
```

Syslog Disk Logging Examples

The following example creates five subfiles. Each subfile has a maximum size of 2000 KB; thus, the total available size is 10000 KB. The subfiles are named mysyslog.cur, mysyslog.1, mysyslog.2, mysyslog.3, and mysyslog.4.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# logging syslog-server 2000 5 mysyslog
Router(config)# end
%SYS-5-CONFIG_I: Configured from console by console
Router# dir disk0:
Directory of disk0:/
  3  drw-           0   Jan 17 1998 07:03:53  syslogd.dir
  4  drw-           0   Jan 12 1998 11:02:29  performance
 12  drw-           0   Jan 12 1998 11:56:37  configs
242  drw-           0   Jan 21 1998 17:51:29  mysyslog.dir
340492288 bytes total (336560128 bytes free)
Router# dir disk0:/mysyslog.dir
Directory of disk0:/mysyslog.dir/
  0  -rw-           0   Jan 21 1998 17:51:29  mysyslog.1
  0  -rw-           0   Jan 21 1998 17:51:29  mysyslog.2
  0  -rw-           0   Jan 21 1998 17:51:29  mysyslog.3
  0  -rw-           0   Jan 21 1998 17:51:31  mysyslog.4
  0  -rw-           0   Jan 21 1998 17:51:31  mysyslog.cur
340492288 bytes total (336560128 bytes free)
```

FTP Server Examples

The following example enables the FTP Server and limits client access to the syslogd.dir directory on disk0:

```
ftp-server enable
ftp-server topdir disk0:/syslogd.dir
```

After these commands have been entered, you can FTP to the router. In the following example, a user connects to the router and gets the file syslogd.1. Notice that the user starts in the directory specified by the **ftp-server topdir** command.

```
FTPclient% ftp FTProuter
Connected to FTProuter.cisco.com.
220 FTProuter IOS-FTP server (version 1.00) ready.
Name (FTProuter:me): aa
331 Password required for 'aa'.
Password:
230 Logged in.
Remote system type is Cisco.
ftp> pwd
257 "disk0:/syslogd.dir/" is current directory.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
syslogd.1
syslogd.2
syslogd.3
syslogd.4
syslogd.5
syslogd.6
syslogd.7
syslogd.8
syslogd.9
syslogd.cur
226 Transfer complete.
ftp> bin
200 Type set to I.
ftp> get syslogd.1
200 PORT command successful.
150 Opening BINARY mode data connection for syslogd.1 (607317 bytes).
226 Transfer complete.
607317 bytes received in 7.7 seconds (77 Kbytes/s)
ftp>
```

Use the **debug ftpserver** command to observe the process on the router.