IBM® BladeCenter® Advanced Management Module Protected Mode

Kenneth Corkins
System x™ Advanced Technical Support
kcorkins@us.ibm.com

Version 1.0
6/04/2007

Revision History

Version 1.0 – June 7, 2007	Initial Release

Notices:
This paper is intended to provide information regarding Protected Mode. It discusses findings based on configurations that were created and tested under laboratory conditions. These findings may not be realized in all customer environments, and implementation in such environments may require additional steps, configurations, and performance analysis. The information herein is provided "AS IS" with no warranties, express or implied. This information does not constitute a specification or form part of the warranty for any IBM or non-IBM products.

Information in this document was developed in conjunction with the use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

The information contained in this document has not been submitted to any formal IBM test and is distributed **as is**. The use of this information or the implementation of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

IBM may not officially support techniques mentioned in this document. For questions regarding officially supported techniques, please refer to the product documentation, announcement letters, or contact the IBM Support Line at 1-800-IBM-SERV.
This document makes references to vendor-acquired applications or utilities. It is the customer responsibility to obtain licenses of these utilities prior to their usage.

Table of contents

Protected mode overview

Protected mode (PM) is a feature of the IBM® BladeCenter® Advanced Management Module (AMM) to isolate management of the Cisco Intelligent Gigabit Ethernet Switch Module (IGESM) from the AMM in the IBM BladeCenter.

This feature is targeted at environments that have distinctly separate management teams for servers and networking, or where it is not desirable to permit the AMM to set or otherwise control certain attributes of the IGESM.

NOTE: If you do not have a specific requirement for management separation between the AMM and the IGESM, it is not necessary to implement this feature.

Table 1 compares the features of standard and protected modes:

Table 1: Feature comparison of standard and protected modes

Feature	Standard Mode	Protected Mode
AMM controls the IP address and mask for the primary management virtual local area network (VLAN) interface on the IGESM	Yes	No
Reset the IGESM back to factory default from the AMM	Yes	No
Enable/disable the external ports (17-20) from the AMM	Yes	No
AMM controls the ability for the IGESM to respond to ARP requests for its own IP address over its own uplink ports	Yes	No
Use the AMM to reload the switch and also turn it off and on	Yes	Yes
Use the AMM to set the switch to run advanced diagnostics during a reload	Yes	Yes
Shut down or reload the IGESM in the event of critical environment issues such as over temp or over current	Yes	Yes
Serial over LAN (SoL)	Yes	Yes

Note: Serial over LAN will still function with protected mode enabled.

Preparation

This section describes preparing the BladeCenter Advanced Management Module and the Cisco Intelligent Gigabit Ethernet Switch Module for protected mode.

Requirements

This section describes the requirements for the AMM and IGESM for protected mode.

BladeCenter Advanced Management Module

The Advanced Management Module must be at a minimum firmware level of ***1.26B.***

Cisco IGESM

The IGESM must be at a minimum Cisco code version of **12.1(22)EA9.**

Cisco console cable:

Configuring protected mode may require changing the management VLAN and IP address. A standard Cisco console cable is highly recommended to attach to the IGESM at least briefly during the configuration process. It is also important in case a mistake is made and management via telnet is lost during the migration. If the console cable is required, a workstation or notebook with some form of terminal emulator or a terminal server will be necessary to complete the migration process. For more information about the console cable and its use, see Appendix A.

Rules for deploying protected mode

Aside from the prerequisites listed in the previous section, certain rules apply to enabling and using this feature. Following these rules will help ensure success in a protected mode deployment.

Rules for AMM

To enable protected mode (PM) on the AMM, you must complete certain items before you actually enable PM for the desired switch bay. Before enabling protected mode, enable the following two items via the AMM user interface:

Enable “External management over all ports” for desired switch bay(s)
Enable “External ports” for desired switch bay(s)

Attempting to enable PM mode on the AMM without completing these two items will result in an error message, and the attempt to enable Protected Mode will be canceled. If this occurs, the operator must correct the condition and then rerun the PM enablement steps on the AMM to complete the process.

Rules for the IGESM

The management path for telnet, ping, etc., to IGESM via the AMM uplink is no longer available with PM enabled. One way the separation of management is created is by shutting down ports 15

and 16 on the IGESM (the ports that connect to the AMM inside the BladeCenter). Because the internal Ethernet path to the AMM is being disabled by the PM process, it will no longer be possible to send pings or telnet packets to the IGESM across the AMM. This means that the user will have two possible management paths for the IGESM after PM is enabled:

Path 1: This path carries the management VLAN of the IGESM over one or more of its uplink ports (17-20) and will most commonly be used in most production environments.

Path 2: Use the serial console port on the rear of the IGESM and attach it to either a terminal server (for remote access) or a local system/notebook's serial port for direct access. This tends to be the secondary path used when path 1 is not available.

The VLAN associated with a VLAN interface on the IGESM must be allowed on at least one of the uplink ports (17-20). This can be in the form of a trunk port that allows the VLAN to exist on one or more of the uplinks, or an access port that is set to the specific VLAN This is necessary for path 1 above to operate. If this rule is not followed, a warning message to this effect will be displayed, and the PM command will be rejected until the issue is resolved. This design reduces the likelihood that users will lock themselves out of path 1 after PM is fully enabled.

Note: Unlike Standard Mode, in which it is important to follow certain rules for VLAN isolation (documented in section 5.3 of the IGESM Redpaper) with protected mode, any VLAN can be used for any purpose. Best practices still are to isolate management from data traffic, but with protected mode, it is not a necessity -- just a best practice.

Subnet recommendation

The recommended method for assigning the management interface of the IGESM for protected mode is to configure the interface to be in a different subnet than that of the AMM. This is a recommendation, not a requirement. If the address of the IGESM is in the same subnet as the AMM interface, the following error message will be displayed on the IGESM:

```
WARNING: IP Address of the Mgmt vlan = XXX falls in the same
subnet as that of the Management Module. Change the IP address on
the mgmt vlan to some other subnet.
```

The IGESM and AMM will still function properly if both management interfaces are in the same subnet.

Configuring protected mode

After all prerequisites are met, enabling protected mode is a two-step process. Step 1 is to enable protected mode on the AMM. Step 2 is to enable it on the IGESM.

> **NOTE:** To activate protected mode on the IGESM, you must reload the device. Reloading the IGESM is a disruptive action. During the time it takes for the device to reload, no network traffic will pass through the device. The reload will also disconnect the network interfaces on the servers. It may also cause the Spanning tree protocol to recalculate.

The following sections provide the steps necessary to complete this process.

Configuring protected mode on the Advanced Management Module

Take the following steps to enable the protected mode feature on the Advanced Management Module:

1. Update AMM firmware to the correct version.
2. Enable external ports for desired switch bays.
3. Enable external management for desired switch bays.
4. Enable protected mode for desired switch bays.

1. Update AMM firmware to the correct version.

A. Obtain the latest version of AMM firmware from the IBM Support Web site (refer to appendix B on page 17 for the URL for AMM firmware). Version 1.26B (Build ID: BPET26B) is the earliest version that supports the protected mode feature. Versions later than 1.26B will also support protected mode.

B. Install the firmware on the AMM by following the instructions in the README file listed on the download page. The final step in the AMM upgrade process will require restarting the AMM.

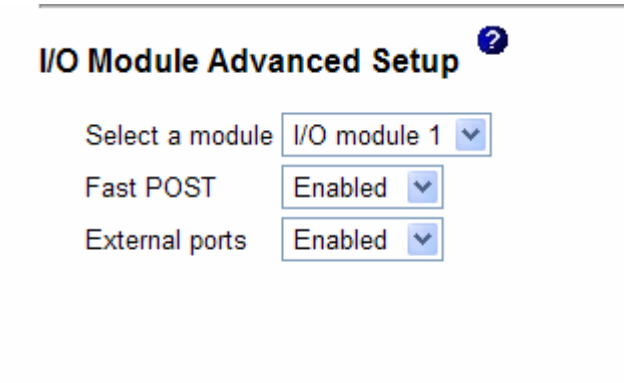
> **NOTE:** Restarting the AMM does not affect the operation of the blade servers. The servers will continue to operate while the AMM is restarting.
>
> Restarting the AMM does not affect the operation of the switch modules in the BladeCenter, but will affected the management of the modules during the time the AMM is restarting.

2. Enable external ports.

A. From the AMM Management interface, navigate to: **I/O Module Tasks → Admin/Power/Restart**.

B. At the bottom of the page, in the I/O Module Advanced Setup section, choose the module to configure for protected mode. Ensure that the **External ports** drop-down box is showing **Enabled**.

C. Save the setting if required.



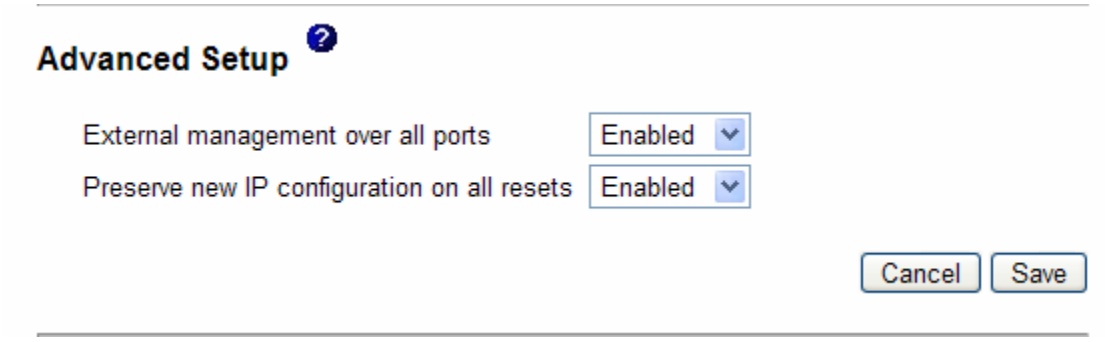
3. Enable management over external ports.

A. From the AMM Management interface, navigate to: **I/O Module Tasks → Configuration**.

B. Navigate to the switch module you need to configure for protected mode.

C. Select the **Advanced Configuration** link. In the **Advanced Setup** section, ensure that the **External management over all ports** drop-down box is showing **Enabled**.

D. Save the setting if required.



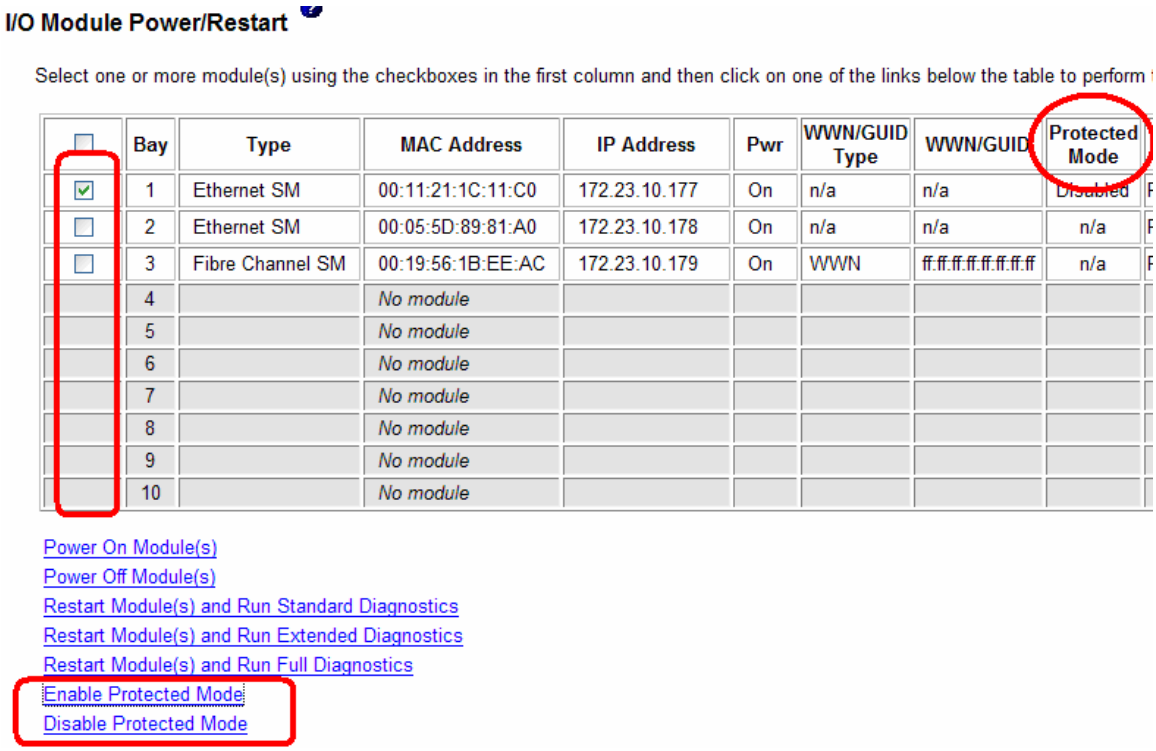
4. Enable protected mode.

A. From the AMM management interface, navigate to **I/O Module Tasks → Admin/Power/Restart**.

B. Place a check mark next to the switch module you need to enable for protected mode.

C. At the bottom of the table, select the option to enable Protected Mode.

If all of the previous steps have been completed successfully, the Protected Mode indication in the table will change from **Disabled** to **Pending**.



At this point, the AMM is ready for protected mode. The IGESM must be configured next.

Configuring protected mode on the Cisco Intelligent Ethernet Switch Module

The following steps must be taken to enable the Protected Mode feature on the Cisco IGESM:

1. Upgrade the IGESM IOS to the correct version.
2. Create VLANs and management interfaces.
3. Allow VLANs on upstream ports.
4. Enable protected mode.
5. Save the configuration and reload the IGESM.

1. Upgrade the IGESM IOS.

Upgrade the IOS firmware on the IGESM by following the instructions in the README file located with the IGESM software download page (refer to appendix B on page 17 for the URL for IGESM) firmware). Version 12.1(22)EA9 is the earliest version that supports the protected mode feature. Versions later than 12.1(22)EA9 will also support protected mode.

NOTE: In order to upgrade the firmware on the IGESM the device must be reloaded. Reloading the IGESM is a disruptive action. During the time it takes for the device to reload no network traffic will pass through the device. The reload will also disconnect the network interfaces on the servers. It may also cause the Spanning tree protocol to recalculate.

.

2. Create VLANs and management interfaces.

While it is possible that a user may want to manage the IGESM using the same IP subnet and VLAN that had been used for management in standard mode, in most cases it is assumed the goal will be to set the IGESM to a different VLAN/IP subnet. It is acceptable to allow the IGESM to remain on the default management VLAN interface of VLAN 1 and still utilize the PM feature. This document assumes this will not be the case, but using VLAN 1 for management is fully supported.

Note: Once protected mode is enabled, the AMM can no longer provide a path for IGESM management traffic through its own uplink.

The VLAN selected must be available on the upstream network, to allow the necessary management traffic a path out of the IGESM.

Changing to a new management VLAN can be done in one of two ways. One way is to create a new management VLAN interface and configure the IGESM to use it, leaving the old management VLAN interface in place but not used. The second way is to make that new management VLAN interface the one tied to the “management” keyword. The latter is a bit cleaner, as it means only a single management VLAN interface will exist, but either method will work.

A. To create this new interface, first create the VLAN (assuming “vtp transparent” mode) and then configure the new interface to use this VLAN.

B. Starting in enable mode, switch to config mode, create the new VLAN (where X = the VLAN number to be used) and then the new interface to the VLAN as follows:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan X
Switch(config-vlan)#int vlan X
```

C. To shut down the old interface and use the new one, issue the keyword “management” on the interface (this is optional but results in fewer operational logical interfaces and may be cleaner than leaving the old management interface operational). While still in the int vlan x mode from above, issue the following command:

```
Switch(config-if)#management
```

When the keyword management is issued, the old management VLAN interface is shut down and the old IP address is moved over to this new interface.

Note: When you issue this command, a TELNET session to the IGESM will become disconnected while the switch moves the MANAGEMENT function to the new vlan. TELNET can reconnect after approximately 40 seconds. If you are using the console port to issue this command, the console session will not be disconnected.

3. Allow VLANs on upstream ports.

Before the IGESM will accept the command to enable protected mode, the management VLAN must be carried over at least one (or more -- depending on the upstream connectivity) of the IGESM uplink ports, 17-20.

A. **If using a port in access mode** (only a single VLAN permitted) for this purpose, ensure that the port is configured for access mode and is using the management VLAN as the allowed VLAN.

You can accomplish this using the following commands from config terminal mode, in interface config mode:

```
Switch(config)#int g0/Y
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan X
```

(Where X is the desired management VLAN and where Y is the physical port 17 through 20).

B. I**f the uplink(s) being used to carry the management interface are to be trunks** (carrying multiple VLANs), the command on the interface would be as follows:

```
Switch(config)#int g0/Y
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add X
```

(Where X is the desired management VLAN, and where Y is the physical port 17 through 20).

C. **If using aggregation to bind ports together on the uplinks** (port-channel), you may need to run these commands on the logical port channel interface as well:

```
Switch(config)#int poY
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add X
```

(Where X is the desired management VLAN and where Y is the port channel number 1 through 6).

Note: There are other ways to allow the management VLAN on the uplink ports, and the above should be considered as possible examples.

4. Enable protected mode.

After you have completed the preceding steps, the IGESM is ready to take the command to turn on protected mode. From configure terminal mode, run the following command:

```
Switch(config)# platform chassis-management protected-mode
```

At this point, the feature will be enabled, but not yet operational. To complete this process the configuration must be saved to NVRAM and the IGESM must be reloaded.

5. Save the configuration to NVRAM and reload the IGESM.

A. From enable mode (# prompt), run the command:

```
Switch# copy running-config startup-config
```

Note: The ***write*** command is still supported as well.

As noted elsewhere in this document, reloading the IGESM will affect traffic flow for servers using this switch. Reloading the switch may require scheduling an outage window to complete this process.

B. From enable mode (# prompt), run the command:

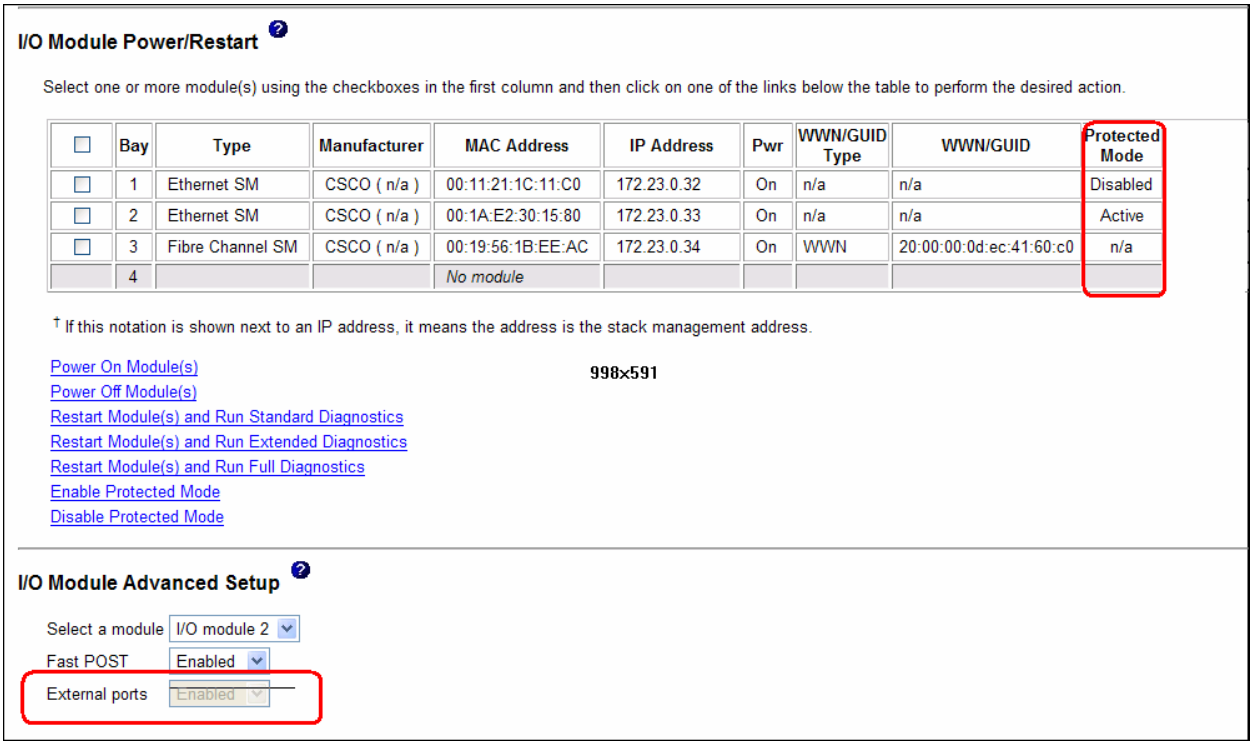
```
Switch# reload
```

C. Answer **yes** when prompted to perform a reload.

Allow the switch several minutes to reload. The AMM interface can be used to check the status of the reload.

Verifying that protected mode is operational

On the AMM, the status of protected mode is displayed in the I/O Module Power/Restart screen. Additionally, the External ports Enable/Disable function is no longer changeable from the AMM.



I/O Module Power/Restart

Select one or more module(s) using the checkboxes in the first column and then click on one of the links below the table to perform the desired action.

	Bay	Type	Manufacturer	MAC Address	IP Address	Pwr	WWN/GUID Type	WWN/GUID	Protected Mode
☐	1	Ethernet SM	CSCO (n/a)	00:11:21:1C:11:C0	172.23.0.32	On	n/a	n/a	Disabled
☐	2	Ethernet SM	CSCO (n/a)	00:1A:E2:30:15:80	172.23.0.33	On	n/a	n/a	Active
☐	3	Fibre Channel SM	CSCO (n/a)	00:19:56:1B:EE:AC	172.23.0.34	On	WWN	20:00:00:0d:ec:41:60:c0	n/a
	4			*No module*					

† If this notation is shown next to an IP address, it means the address is the stack management address.

Power On Module(s)
Power Off Module(s)
Restart Module(s) and Run Standard Diagnostics
Restart Module(s) and Run Extended Diagnostics
Restart Module(s) and Run Full Diagnostics
Enable Protected Mode
Disable Protected Mode

998x591

I/O Module Advanced Setup

Select a module: I/O module 2
Fast POST: Enabled
External ports: Enabled

The IP configuration screen is also disabled. The operator cannot change the IP address of the IGESM from the AMM. The AMM will show the pre-protected mode address and the currently configured address of the IGESM. The Advanced Configuration link no longer works in the AMM.

Bay 2 (Ethernet SM)*

Current IP Configuration

Configuration method: Static
IP address: 172.23.0.99
Subnet mask: 255.255.255.0
Gateway address: 172.23.0.6

New Static IP Configuration

Status: Enabled

This I/O Module is currently in protected mode and these properties cannot be changed

IP address: 172.23.0.33
Subnet mask: 255.255.255.0
Gateway address: 172.23.0.6

Advanced Configuration

On the IGESM, the status of protected mode can be confirmed with the ***show platform summary*** command. An example output from this command is shown below.

```
Switch#show platform summary
Platform Summary:

Switch Slot: 2
Chassis Type: BladeCenter
Current IP Addr: 172.23.0.33, 255.255.255.0,  gw: 172.23.0.6
Default IP Addr: 10.10.10.92, 255.255.255.0,  gw: 0.0.0.0
IP Fields read from VPD: 0.0.0.0, 0.0.0.0,  gw: 0.0.0.0
Static IP Fields in VPD: 172.23.0.33  255.255.255.0  172.23.0.6
IP Acquisition Method used: user-config

Active Mgmt Module in Mgmt Slot: 1
Native Vlan for Mgmt Module Ethernet ports: 360
External Mgmt over Extern ports Enabled
Mgmt Module Protected Mode: Operational
Mgmt Module Protected Mode configured on switch: TRUE
Mgmt Module supports Protected Mode: TRUE
```

Interfaces G0/15 and G0/16 (the AMM connections) will show as disabled in the IGESM.

```
Port      Name    Status   Vlan  Duplex  Speed Type
Gi0/15    mgmt1  disabled  360   full    100 10/100/1000BaseTX
Gi0/16    mgmt2  disabled  360   full    100 10/100/1000BaseTX
```

Check to make sure that the IGESM can ping out to upstream devices by pinging the default gateway and/or any necessary upstream management devices.

Disabling protected mode

Disable protected mode on the IGESM

This section describes the process to disable protected mode on the IGESM and the AMM. The steps to disable protected mode are essentially the opposite of enabling the feature.

Protected mode must be disabled on the IGESM first, and then disabled in the AMM.

A. From configuration mode, enter the command:

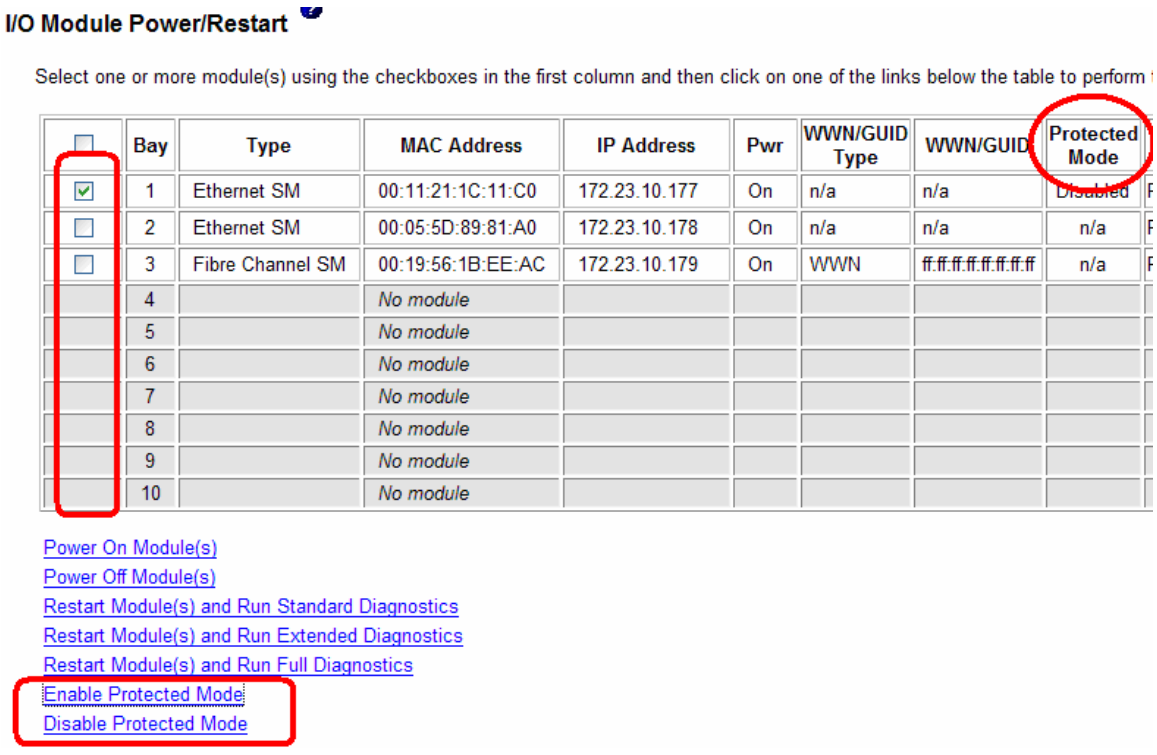
```
Switch(config)#no platform chassis-management protected-mode
```

B. As before, disabling protected mode on the IGESM requires that you save the configuration and reload the IGESM.

Disable protected mode on the AMM

After the IGESM has reloaded, the protected mode status indicator in the AMM will show Pending.

To disable protected mode in the AMM, place a checkmark next to the module, and select **Disable Protected Mode** from the list of actions.

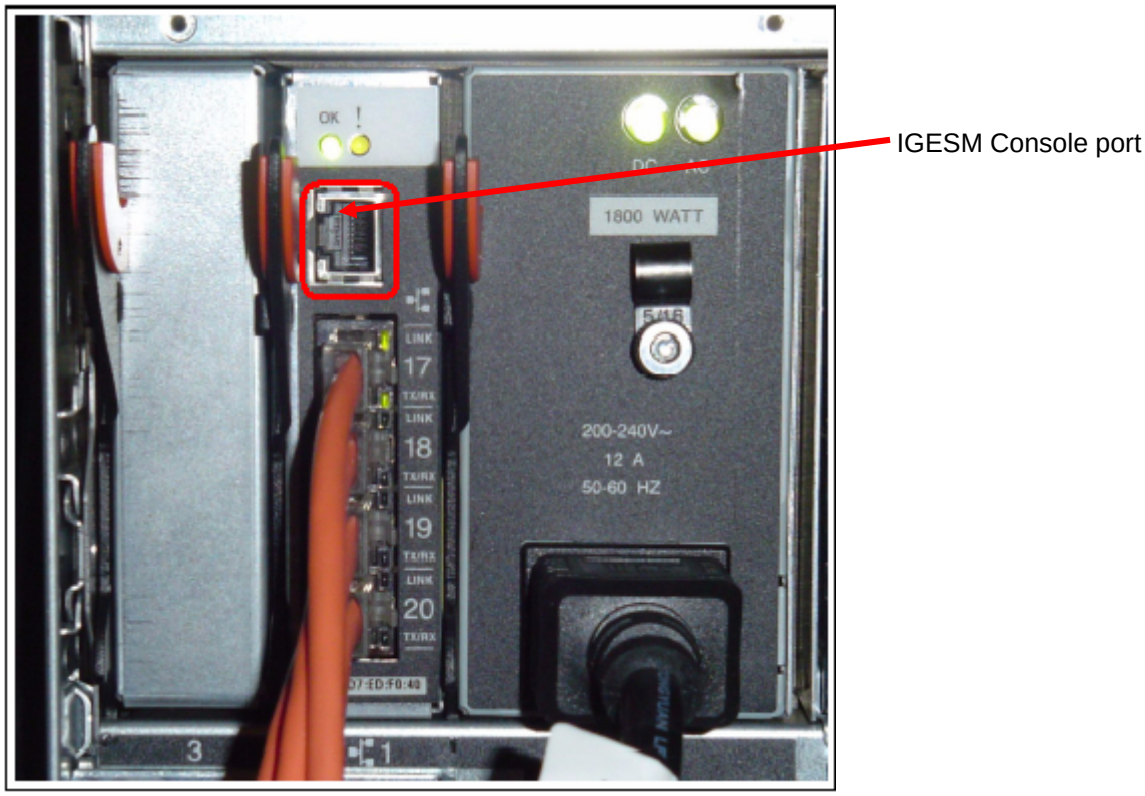


Appendix A – Cisco console cable

This section contains information on using the console port of the IGESM.

While it is possible under certain conditions to completely move an IGESM into protected mode without using a console cable, it is very likely that one will be needed at some point in the process. Based on this, it is strongly recommended that a console cable be available for this migration process.

The console port on the IGESM is located just above port 17 on the rear of the IGESM



The console cable used by the IGESM currently does not ship with the IGESM, but is the same cable used by other Cisco products. If a console cable is available from other Cisco equipment, that cable can be used.

A console cable can be ordered from Cisco using this part number:

ACS-DSBUASYN=

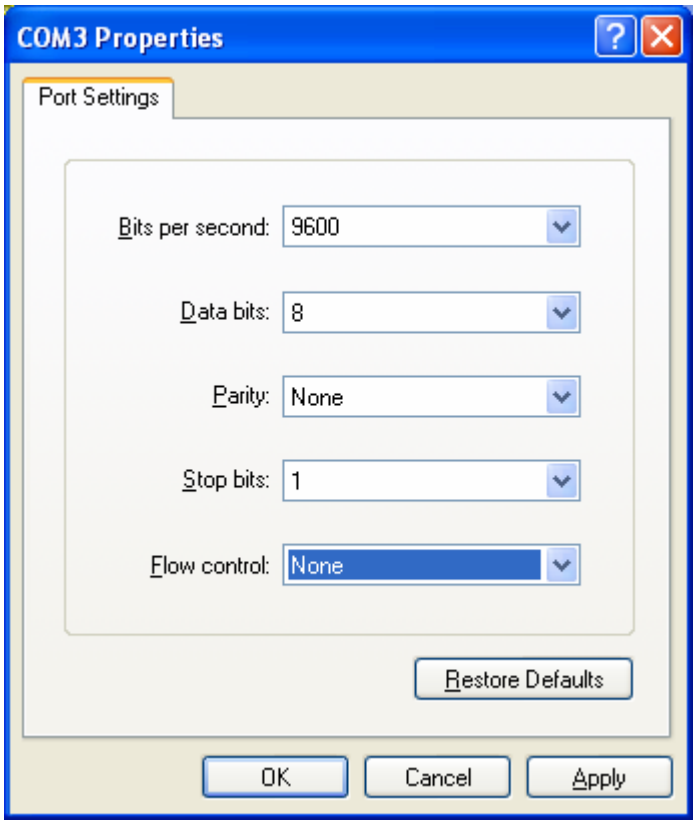
Information for making a cable can be found at the following link:

http://www.cisco.com/warp/public/473/9.html

After a working console cable has been acquired, a serial connection must be made from the management workstation to the IGESM. You can use any terminal emulator. HyperTerminal, the free terminal emulator included with all Windows® products, can be used. Ensure that the emulator has the following settings:

Speed:	9600
Bits:	8
Parity:	None
Stop bits:	1
Flow control:	None

The following are the settings as shown from a HyperTerminal session:



Appendix B – Firmware locations

Advanced Management Module

The AMM must be at a minimum firmware level of 1.26B. The latest version of the AMM firmware is available at this location:

http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/docdisplay?brandind=5000008&lndocid=MIGR-5070708

Cisco IGESM

The IGESM must be at a minimum code level of **12.1(22)EA9.** The latest version can be obtained at the following URL:

http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-64460&brandind=5000020

References

This section contains links to documentation and important information.

Advanced Management Module and Management Module User's Guide

http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-45153&brandind=5000008

IBM IGESM Deployment Redpaper

http://www.redbooks.ibm.com/abstracts/redp3869.html

IGESM Software Configuration Guide

http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-55261&brandind=5000020

IGESM Command Reference

http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-55260&brandind=5000020

IGESM Message Guide (all error messages)

http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-55259&brandind=5000020

Troubleshooting Cisco Systems IGESM issues

http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-59637&brandind=5000008

Copper IGESM Install Guide

http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-57858&brandind=5000020

SFP IGESM Install Guide

http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-59200&brandind=5000020

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

BladeCenter®
IBM®
System x

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml.

Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, EtherChannel are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Windows is a trademark of Microsoft Corporation in the U.S. and other countries.

Other company, product and service names may be trademarks or service marks of others.

Notices

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply. For a copy of applicable product warranties, write to: Warranty Information, P.O. Box 12195, RTP, NC 27709, Attn: Dept. JDJA/B203. IBM makes no representation or warranty regarding third-party products or services including those designated as ServerProven or ClusterProven.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

MB, GB, and TB = 1,000,000, 1,000,000,000 and 1,000,000,000,000 bytes, respectively, when referring to storage capacity. Accessible capacity is less; up to 3GB is used in service partition. Actual storage capacity will vary based upon many factors and may be less than stated. Some numbers given for storage capacities give capacity in native mode followed by capacity using data compression technology. Maximum internal hard disk and memory capacities may require the replacement of any standard hard drives and/or memory and the population of all hard disk bays and memory slots with the largest currently supported drives available.

The information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.