Server Connectivity Module for
IBM BladeCenter

Release Notes

May 2006

Reference Number: 322574-A

Originated in the U.S.A.

Release Notes

These release notes provide the latest information regarding the Server Connectivity Module (SCM) for the IBM BladeCenter. This supplement modifies information found in the complete documentation:

- *SCM User's Guide*
- *SCM Installation Guide*

The publications listed above are available from http://www.ibm.com/pc/support. Please keep the Release Notes with your product manuals.

Hardware support

The Server Connectivity Module (SCM) is a high performance interface option for connecting the IBM BladeCenter system to the network infrastructure (see Figure 1). The SCM supports six Gigabit Ethernet external ports, 14 Gigabit Ethernet internal ports and two Fast Ethernet management ports. The SCM also features tight integration with IBM BladeCenter's management module.

NOTE – The SCM is not supported by the management module version 1. You must use the advanced management module to work with the SCM.

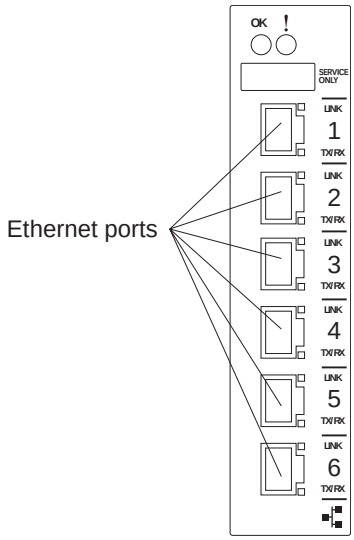

Figure 1 SCM faceplate

Software support

The Server Connectivity Module (SCM) provides a simple Ethernet interface option for connecting the IBM BladeCenter system to the network infrastructure. The SCM's default configuration allows you to plug it into the BladeCenter Chassis and function correctly with no configuration changes. The configuration options are restricted to reduce the initial setup complexity and to minimize the impact on upstream networking devices.

For more detailed information about SCM's features and capabilities, please refer to the *User's Guide* for the *Server Connectivity Module for IBM BladeCenter.*

Supplemental Information

This section provides additional information about configuring and operating the Server Connectivity Module.

Management Module

- The “Fast POST=Disabled/Enabled” inside the IBM management module Web interface “I/O Module Admin/Power/Restart” does not apply to the SCM.

  Solution: To boot with Fast or Extended POST, go to the “I/O Module Admin/Power/Restart” window. Select the SCM, and then choose “Restart Module and Run Standard Diagnostics” or “Restart Module and Run Extended Diagnostics.”

- The following table correlates the Firmware Type listed in the IBM management module’s Web interface “Firmware VPD” window to the SCM software version:

  Table 1 Firmware Type list

Firmware Type	Description
Boot ROM	SCM Boot code version
Main Application 1	Image 1 SCM software version
Main Application 2	Image 2 SCM software version

- Within the IBM management module Web interface, the Java applets of “Start Telnet Session” and “Start Web Session” do not support changing of default known ports 23 and 80 respectively.

  The internal ports on the SCM cannot be changed. If you change the internal ports on the the management module, you lose the connection to the SCM.

Management Module-SCM Connectivity

Currently, the IBM management module is designed to provide one-way control of the SCM. As a result, the SCM may lose connectivity to the management module via the management port under the following conditions:

- If you execute the `/boot/reset` CLI command on the SCM or the SCM resets itself, the management module might not push the IP attributes to the switch, and connectivity may be lost.

Solution: Use the ***Admin/Power/Restart*** window on the management module's Web interface to restart the switch module in question.

Secure Management Network

The following SCM attributes are reserved to provide secure management access to and from the IBM management module:

- VLAN 4095
- IP Interface 128
- Gateway 132
- MGT1 (Port 15)
- MGT2 (Port 16)

NOTE – The external uplink ports (EXT1-EXT6) cannot be members of the management VLAN (4095).

Secure Shell (SSH)

Because SSH key generation is CPU intensive, the SCM attempts to avoid unnecessary key generation. The process generates three server keys:

1. One key is generated to replace the current server key, if used.
2. A second key is generated as a spare, in case the current server key is used and the specified interval expires.
3. A third key is generated for use at the next reboot.

Therefore, if you never login via SSH, you will only see two key generation events. You may see all three events directly following a reboot. If you want to witness the key generation after the specified interval has expired, then you must login via SSH at least once during each expiration interval.

Trunk Group Configuration Tip

Configure all ports in a trunk group to the same speed. You cannot aggregate 10/100Base-TX module ports with gigabit ports.

Syslog Configuration Tip

The *facility* parameter traditionally is used to correlate services (e.g. IP, CLI, etc.) to messages. This is done to distinguish between the different services that are running in the network/ device. However, for the SCM, there is a single configured facility value (0-7) used on all messages. By configuring a unique facility value for each switch, a single SYSLOG server can distinguish between the various SCMs in the network.

BBI Configuration Tip

Users with an access level of *operator* (`oper`) cannot make any changes in the BBI. Operators cannot enable or disable ports from the BBI. Operators can enable or disable ports from the CLI.

Known issues

This section describes known issues for the SCM.

Interoperability with Older Hubs

The command-line interface might display **link up** and **link down** messages continuously for an external port that is connected to certain older hub models configured for 100 Mbps half-duplex. The display might show **link up** erroneously. This behavior has been observed when connecting the SCM with the following devices:

- NetGear FE104 100 hub
- SBS 1000Base-T NIC
- 3Com Linkbuilder FMS100 Hub 3C250 TX/I
- 3Com SuperStack II 100TX 3C250C-TX-24/12
- Nortel Baystack 204 Hub

If the SCM is connected to an Application Switch which requires a link speed of 100 Mbps half-duplex, then enable auto negotiation on the SCM port with port speed=any, mode=any, fctl=both, and auto=on.

Linking at 10/100MB

When the link speed for an external connection is forced (i.e. no Auto-Negotiation) to 100 Mbps and then changed to 10 Mbps, if the external device is changed first, the external device may erroneously report the link as DOWN even after the SCM is changed to 10 Mbps.

Solution: At the external device, disconnect and reconnect the cable.

RADIUS with SSHv2

With RADIUS turned on, users might see a duplicate login prompt for SSHv2 clients, if the RADIUS server is too slow to respond or if the RADIUS server is not available. In this case, users must re-type the username and password to login.

Trunk Traffic

Multicast, broadcast and DLF (Destination Lookup Failed, which are unknown destination MAC packets) traffic is sent to the lowest numbered port in the trunk. If this port is down, then the traffic is sent to the next lowest-numbered port. If the port that was down comes up again, the traffic is not re-hashed back to the recovered port.

BBI software download

Some versions of Microsoft Internet Explorer version 6.x do not perform HTTP download efficiently. If you have one of these versions, HTTP software download might take much longer than expected (up to several minutes).

Other browsers or release levels are known to perform the download more efficiently. Use another browser, such as Netscape or Firefox, if download times are excessive.

FTP/TFTP subdirectory for CLI uploads and downloads

When you use the CLI to upload or download files, and enter the entire command on a single line, the target file cannot reside in a subdirectory on the FTP/TFTP server. If the target is in a subdirectory, use the CLI prompts to perform the task. For example:

```
Boot Options# gtimg
Enter name of switch software image to be replaced
 ["image1"/"image2"/"boot"]: image1
Enter hostname or IP address of FTP/TFTP server: 10.4.12.1
Enter name of file on FTP/TFTP server: my00022_os_cpu/
my00022_os_cpu.img
```