Server Connectivity Module for
IBM BladeCenter

User’s Guide

Version 1.1

Part Number: 31R1755, August 2006

Originated in the U.S.A.

Contents

Preface

The *Server Connectivity Module User's Guide* describes how to configure and use the software on the Server Connectivity Module for IBM BladeCenter. For documentation on installing the module physically, see the *Installation Guide* for your Server Connectivity Module (SCM).

Who Should Use This Guide

This *User's Guide* is intended for server administrators who need to connect the BladeCenter to a data network. The administrator does not require extensive knowledge of Ethernet or IP networking concepts to install and configure the SCM. The SCM's static configuration provides basic connectivity to the data network.

What You'll Find in This Guide

This guide will help you plan, implement, and administer Server Connectivity Module (SCM) software. Where possible, each section provides feature overviews, usage examples, and configuration instructions.

- Chapter 1, "Overview of Server Connectivity Module Operation," provides a general theory of operation for the SCM.
- Chapter 2, "Accessing the Server Connectivity Module," describes how to access the SCM to configure, view information and run statistics. This chapter also discusses different methods to manage the SCM for remote administrators using the management module, RADIUS authentication, Secure Shell (SSH), and Secure Copy (SCP).
- Chapter 3, "Port Groups, VLANs, and Trunking," describes how to group multiple physical ports together to aggregate the bandwidth between large-scale network devices.
- Chapter 4, "Command Reference," provides an overview of menu commands that enable you to view information and statistics about the SCM, and to perform any necessary configuration.

- Chapter 5, "Using the BBI," provides an overview of the Browser-Based Interface (BBI) that enables you to view and configure the SCM.

Typographic Conventions

The following table describes the typographic styles used in this book.

Table 1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	This type is used for names of commands, files, and directories used within the text.	View the `readme.txt` file.
	It also depicts on-screen computer output and prompts.	`Main#`
`AaBbCc123`	This bold type appears in command examples. It shows text that must be typed in exactly as shown.	`Main#` **`sys`**
<AaBbCc123>	This italicized type appears in command examples as a parameter placeholder. Replace the indicated text with the appropriate real name or value when using the command. Do not type the brackets.	To establish a Telnet session, enter: `host#` **`telnet`** *<IP address>*
	This also shows book titles, special terms, or words to be emphasized.	Read your *User's Guide* thoroughly.
[ ]	Command items shown inside brackets are optional and can be used or excluded as the situation demands. Do not type the brackets.	`host#` **`ls`** `[`**`-a`**`]`

How to Get Help

If you need help, service, or technical assistance, see the "Getting help and technical assistance" appendix in the *Server Connectivity Module for IBM BladeCenter Installation Guide*.

CHAPTER 1
Overview of Server Connectivity Module Operation

The Server Connectivity Module (SCM) provides a simple Ethernet interface option for connecting the IBM BladeCenter system to the network infrastructure. The administrative effort and network skills required to connect to the network are minimized. The number and type of configuration options on the SCM are restricted to reduce the initial setup complexity and to minimize the impact on upstream networking devices.

The SCM requires basic administration tasks similar to those required to connect a single multi-linked server to the network. Connecting the BladeCenter with up to fourteen (14) server blades becomes as easy as connecting a single server to the network.

The default network configuration of the SCM is consists of a single, untagged Virtual Local Area Network (VLAN). All of the uplink ports in each Port Group are aggregated together into a static Link Aggregation Group (LAG, or trunk group), which is fully compatible with Cisco EtherChannel technology. This configuration eliminates the need for Spanning Tree Protocol to prevent network loops, since the uplink ports act as a single link.

The SCM provides improved network reliability. All of the uplink ports in each Port Group participates in a static LAG, so if a link fails, the existing traffic is redirected to the other links.

The SCM software permits the copper TX uplink ports to auto-negotiate the speed (10/100/1000 Mbps), duplex (full/half) and flow-control settings of each link (the default setting). You can also fix these port characteristics to specified values. All of the uplink ports in each Port Group must be configured to the same port characteristics.

With Network Adaptor Teaming configured on the server blade Ethernet NICs, the servers can maintain redundant links to multiple SCMs within the BladeCenter chassis to provide enhanced reliability. The L2 Failover option allows the SCM to disable the server-blade ports when all of its external uplinks are inactive. This causes the Network Adaptor Teaming software to failover to the other SCM(s) in the BladeCenter chassis.

The SCM permits effective management of the server blades using the Serial Over LAN (SOL) feature over a VLAN dedicated to the BladeCenter management module. If no external ports are enabled, Layer 2 Failover must be disabled to use SOL.

Most users will find the Browser-based Interface (BBI) adequate for configuring and using the SCM. However, a command-line interface (CLI) is available for users familiar with the CLI, or who want to use scripting facilities.

Server Connectivity Module Quick Start

The Server Connectivity Module (SCM) is shipped with a default configuration that allows you to plug it into the BladeCenter Chassis and function correctly with no configuration changes. You must make some configuration changes to the upstream network device and the blades in the BladeCenter Chassis, as follows:

Configuring the BladeCenter Management Module

The link through the management module is used to connect to the SCM. The management module is also used to control several operational characteristics of the SCM:

- Plug the Ethernet cable into the management module and verify that you get link and can connect to the management module.
- Verify that the external ports are enabled.

NOTE – The SCM is supported by both the management module version 1 and the advanced management module.

Configuring the Upstream Networking Device

If only one link is required to the SCM, do the following:

- Plug in the Ethernet cable (straight through or crossover) that connects the SCM to the upstream networking device.
- Configure the upstream networking device to transmit the desired data on a single untagged (native) VLAN.
- Verify that the upstream networking device is configured to auto-negotiate the link's speed, duplex and flow control. If fixed port characteristics are desired, configure the SCM port characteristics using the appropriate BBI or CLI interfaces.

If more than one link is required to the SCM, configure a static link aggregation group (also referred to as a trunk group or EtherChannel) to include all of the ports that are being connected.

Configuring the BladeCenter Processor Blades

The operating system should be configured to have a single 802.1Q untagged interface. If two SCMs are used in the chassis, the blades can be configured to support Network Adaptor Teaming Failover (refer to the appropriate documentation for your operating system).

CHAPTER 2

Accessing the Server Connectivity Module

The Server Connectivity Module (SCM) software provides means for accessing, configuring, and viewing information and statistics about the SCM. This chapter discusses different methods of accessing the SCM and ways to secure it for remote administrators:

- "Management module setup" on page 14
- "Using Telnet" on page 20
- "Using the Browser-Based Interface" on page 20
- "Securing Access to the Server Connectivity Module" on page 22
  - "Setting Allowable Source IP Address Ranges" on page 23
  - "RADIUS Authentication and Authorization" on page 24
  - "TACACS+ Authentication" on page 28
  - "Secure Shell and Secure Copy" on page 32
  - "End User Access Control" on page 38

Management module setup

The BladeCenter Server Connectivity Module (SCM) is an integral subsystem within the overall BladeCenter system. The BladeCenter chassis includes a management module as the central element for overall chassis management and control.

NOTE – The SCM is supported by both the management module version 1 and the advanced management module. Refer to the appropriate section below.

The 100-Mbps Ethernet port on the management module is used to configure and manage the SCM. The SCM communicates with the management module through its internal port 15 (MGT1) or port 16 (MGT2), which is accessible through the 100 Mbps Ethernet port on the management module. The SCM will permit *only* management and control access to the SCM through the 10/100 Mbps Ethernet port on the management module. The six external 10/100/1000 Mbps Ethernet ports on the SCM cannot be used for management and control. Selecting this mode as an option through the management module configuration utility program has no effect (see the applicable *BladeCenter Installation and User's Guide* publications on the IBM *BladeCenter Documentation* CD for more information).

Management Module version 1

Factory default vs. MM assigned IP addresses

Each SCM must be assigned its own Internet Protocol address, which is used for communication with an SNMP network manager or other transmission control protocol/Internet Protocol (TCP/IP) applications (for example, BootP or TFTP). The factory-default IP address is 10.90.90.9x, where x corresponds to the number of the bay into which the SCM is installed (for additional information, see the *Server Connectivity Module for IBM BladeCenter Installation Guide)*. The management module assigns an IP address of 192.168.70.1*xx*, where *xx* corresponds to the number of the bay into which each SCM is installed, as shown in the following table:

Table 2-1 SCM IP addresses, based on switch-module bay numbers

Bay number	Factory-default IP address	IP address assigned by MM
Bay 1	10.90.90.91	192.168.70.127
Bay 2	10.90.90.92	192.168.70.128
Bay 3	10.90.90.94	192.168.70.129
Bay 4	10.90.90.97	192.168.70.130

NOTE – SCMs installed in Bay 1 and Bay 2 connect to server NICs 1 and 2, respectively. However, Windows operating systems show that SCMs installed in Bay 3 and Bay 4 connect to server NICs 4 and 3, respectively.

Configuring management module version 1 default gateway

The default Gateway IP address determines where packets with a destination address outside the current subnet should be sent. Usually, the default Gateway is a router or host acting as an IP gateway to handle connections to other subnets of other TCP/IP networks. If you want to access the SCM from outside your local network, use the management module to assign a default Gateway address to the SCM. Choose **I/O Module Tasks > Configuration** from the navigation pane on the left, and enter the default Gateway IP address (for example, 192.168.70.125). Click **Save**.

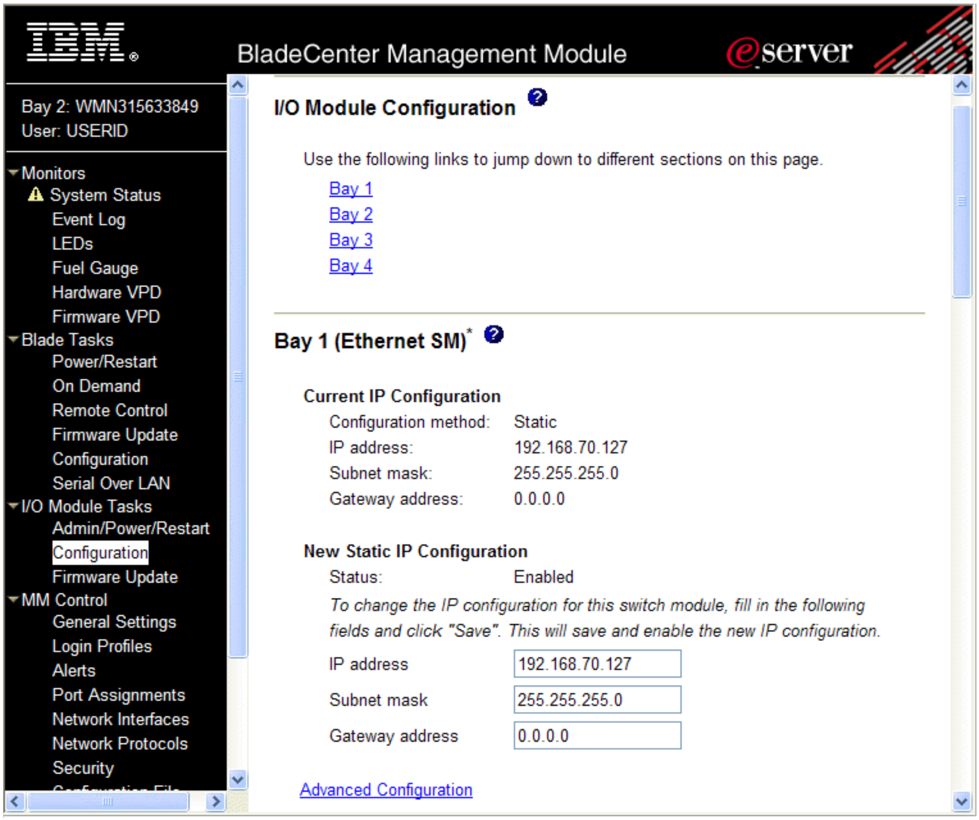
Configuring management module version 1 for switch access

Complete the following initial configuration steps:

1. **Connect the Ethernet port of the management module to a 10/100 Mbps network (with access to a management station) or directly to a management station.**

2. **Access and log on to the management module, as described in the *BladeCenter Management Module User’s Guide*. The management module provides the appropriate IP addresses for network access (see the applicable *BladeCenter Installation and User’s Guide* publications for more information).**

3. **Select** Configuration **on the** I/O Module Tasks **menu on the left side of the BladeCenter Management Module window. See** Figure 2-2.



I/O Module Configuration

Use the following links to jump down to different sections on this page.

Bay 1 (Ethernet SM)*

Current IP Configuration

Configuration method: Static
IP address: 192.168.70.127
Subnet mask: 255.255.255.0
Gateway address: 0.0.0.0

New Static IP Configuration

Status: Enabled

To change the IP configuration for this switch module, fill in the following fields and click "Save". This will save and enable the new IP configuration.

IP address: 192.168.70.127
Subnet mask: 255.255.255.0
Gateway address: 0.0.0.0

4. **You can use the default IP addresses provided by the management module, or you can assign a new IP address to the SCM through the management module. You can assign this IP address through one of the following methods:**

   - Manually through the management module
   - Automatically through the IBM Director Configuration Wizard (available in Director release 4.21)

NOTE – If you change the IP address of the SCM, make sure that the SCM and the management module both reside on the same subnet.

5. **Enable the following features in the management module:**

   - External Ports **(I/O Module Tasks > Admin/Power/Restart > Advance Setup)**

The default value is **Disabled**. If this feature is not already enabled, change the value to **Enabled**, then **Save**.

NOTE – In **Advanced Configuration > Advanced Setup**, enable "Preserve new IP configuration on all switch resets," to retain the SCM's IP interface when you restore factory defaults. This setting preserves the management port's IP address in the management module's memory, so you maintain connectivity to the management module after a reset.

You now can start a Telnet session, Browser-Based Interface (Web) session, a Secure Shell session, or a secure HTTPS session to the SCM.

Advanced Management Module

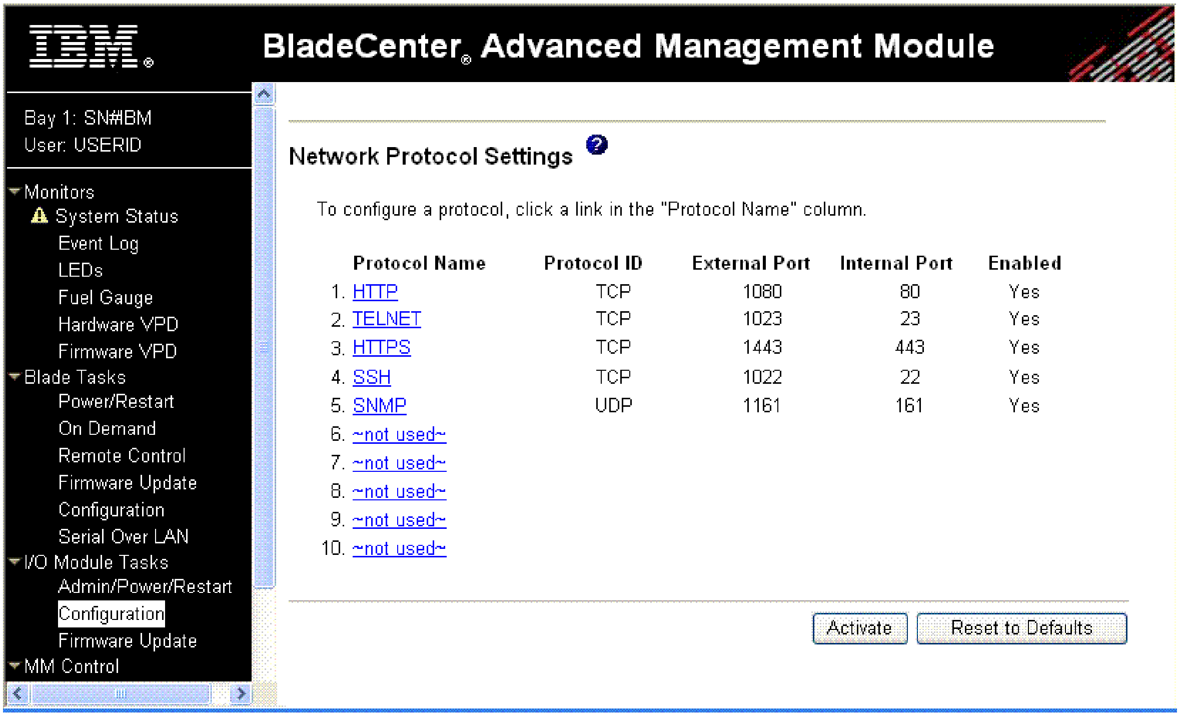
Assigned IP Addresses

Each SCM's Internet Protocol address is mapped from the management module IP address, using Network Address Translation (NAT). For additional information, see the *Server Connectivity Module for IBM BladeCenter Installation Guide*. The management module uses network protocol ports to provide access to each SCM (see Figure 2-1).

CAUTION—Do not change the internal port numbers in the advanced management module's Network Protocol Settings, as shown in Figure 2-1. If the internal port numbers change, you will lose the connection to the Server Connectivity Module.

For example, to Telnet to the SCM in Bay 1, enter the following from the Telnet window:

```
telnet <management module IP address> 1023
```



Network Protocol Settings

To configure a protocol, click a link in the "Protocol Name" column.

	Protocol Name	Protocol ID	External Port	Internal Port	Enabled
1.	HTTP	TCP	1080	80	Yes
2.	TELNET	TCP	1023	23	Yes
3.	HTTPS	TCP	1443	443	Yes
4.	SSH	TCP	1022	22	Yes
5.	SNMP	UDP	1161	161	Yes
6.	~not used~				
7.	~not used~				
8.	~not used~				
9.	~not used~				
10.	~not used~				

Figure 2-1 SCM network protocol settings in the advanced management module

NOTE – Server Connectivity Modules (SCMs) installed in Bay 1 and Bay 2 connect to server NICs 1 and 2, respectively. However, Windows operating systems show that SCMs installed in Bay 3 and Bay 4 connect to server NICs 4 and 3, respectively.

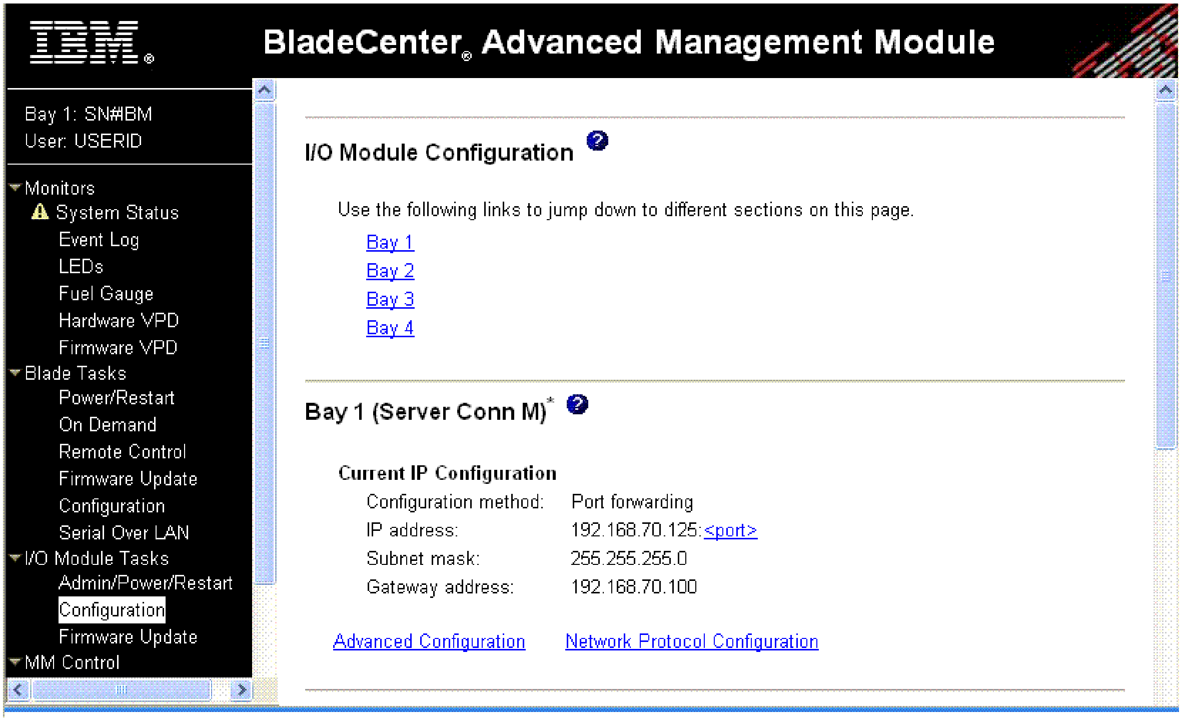
Configuring advanced management module for access

Complete the following initial configuration steps:

1. **Connect the Ethernet port of the management module to a 10/100 Mbps network (with access to a management station) or directly to a management station.**

2. **Access and log on to the management module, as described in the *BladeCenter Management Module User’s Guide* on the IBM *BladeCenter Documentation* CD. The management module provides the appropriate IP addresses for network access (see the applicable *BladeCenter Installation and User’s Guide* publications on the IBM *BladeCenter Documentation* CD for more information).**

3. **Select** Configuration **on the** I/O Module Tasks **menu on the left side of the BladeCenter Advanced Management Module window. See** Figure 2-2.



I/O Module Configuration

Use the following links to jump down to different sections on this page.

Bay 1 (Server Conn M)*

Current IP Configuration

Configuration method: Port forwarding
IP address: 192.168.70.125:<port>
Subnet mask: 255.255.255.0
Gateway address: 192.168.70.100

Figure 2-2 Server Connectivity Module management on the BladeCenter management module

You can now start a Telnet session, Browser-Based Interface (Web) session, a Secure Shell session, or a secure HTTPS session to the SCM. For TCP/IP applications to work with the SCM, a route path must exist between your workstation and the management module.

NOTE – SCM access through the USB serial port is not supported.

Using Telnet

Telnet is used to access the SCM’s command-line interface. Telnet can be launched from the management module interface, or by using a local Telnet application on your workstation.

NOTE – If you cannot access the Server Connectivity Module (SCM) using Telnet or the Browser-Based Interface (web), try to ping the SCM’s IP address from management module. If the ping fails, the management module is not configured correctly.

To use Telnet from the management module, choose **I/O Module Tasks** > **Configuration** from the navigation pane on the left. Select a bay number and click **Advanced Configuration** > **Start Telnet/Web Session** > **Start Telnet Session**. A Telnet window opens a connection to the SCM (requires Java 1.4 Plug-in).

To establish a Telnet connection with the SCM from your workstation, you can run the Telnet program and issue the Telnet command, followed by the management module IP address and the Telnet port for the SCM. For example:

```
telnet <management module IP address> 1023
```

Connect to the Server Connectivity Module via SSH

The SSH (Secure Shell) protocol enables you to securely log into another computer over a network to execute commands remotely. As a secure alternative to using Telnet to manage Server Connectivity Module (SCM) configuration, SSH ensures that all data sent over the network is encrypted and secure. For more information, see “Secure Shell and Secure Copy” on page 32. For more information on the CLI, see *“Command Reference” on page 51*.

Using the Browser-Based Interface

Use the management module to access the Server Connectivity Module (SCM) through a Web session. Choose **I/O Module Tasks** > **Configuration** from the navigation pane on the left. Select a bay number and click **Advanced Configuration** > **Start Telnet/Web Session** > **Start Web Session**. A browser window opens a connection to the SCM.

The Browser-based Interface (BBI) provides access to the common configuration, management and operation features through your Web browser.

By default, BBI access is enabled.

Access via HTTP

BBI access is enabled by default. To access the SCM via the Browser-Based Interface, open a Web browser window and type in the URL using the IP interface address of the management module IP address and the HTTP port for the SCM. For example:

```
http://<management module IP address>: 1080
```

Access via HTTPS

BBI access via HTTPS is disabled by default. Use the following CLI command to enable HTTPS access:

```
>> /cfg/sys/access/https/access ena
```

Before you can access the BBI via HTTPS, you must generate a certificate to be used during the key exchange. Use the CLI command below to generate the HTTPS certificate. A default certificate is created the first time you enable HTTPS, but you can create a new certificate defining the information you want to be used in the various fields.

```
>> /cfg/sys/access/https/generate
Country Name (2 letter code) [  ]:  <country code>
State or Province Name (full name) []:  <state>
Locality Name (eg, city) []:  <city>
Organization Name (eg, company) []:  <company>
Organizational Unit Name (eg, section) []:  <org. unit>
Common Name (eg, YOUR name) []:  <name>
Email (eg, email address) []:  <email address>
Confirm generating certificate? [y/n]: y
Generating certificate. Please wait (approx 30 seconds)
restarting SSL agent
```

To access the SCM via the Browser-Based Interface, open a Web browser window and type in the URL using the IP interface address of the management module IP address and the HTTPS port for the SCM. For example:

```
https://<management module IP address>: 1443
```

You can save the certificate to flash for use if the SCM is rebooted. To save the certificate, use the following command: `/cfg/sys/access/https/certsave`.

When a client (e.g. web browser) connects to the SCM, the client is asked to accept the certificate and can verify that the fields are what the client expected. Once BBI access is granted to the client, you can use the BBI as described in “Using the BBI.”

Securing Access to the Server Connectivity Module

Secure management is needed for environments that perform significant management functions across the Internet. The following are some of the functions for secured management:

- Limiting management users to a specific IP address range. See "Setting Allowable Source IP Address Ranges" on page 23
- Authentication and authorization of remote administrators: see "RADIUS Authentication and Authorization" on page 24
- Encryption of management information exchanged between the remote administrator and the Server Connectivity Module: see "Secure Shell and Secure Copy" on page 32

The following sections are addressed in this section:

- "Setting Allowable Source IP Address Ranges" on page 23
- "RADIUS Authentication and Authorization" on page 24
- "TACACS+ Authentication" on page 28
- "Secure Shell and Secure Copy" on page 32

Setting Allowable Source IP Address Ranges

To limit access to the SCM, you can set a source IP address (or range) that will be allowed to connect to the SCM IP interface through Telnet, SSH, or the Browser-Based Interface (BBI). This also helps to prevent spoofing or attacks on the SCM's TCP/IP stack.

When an IP packet reaches the SCM, the source IP address is checked against the range of addresses defined by the management networks and masks, (`/cfg/sys/access/mgmt`). If the source IP address of the host or hosts are within the defined ranges, they are allowed to attempt to log in. Any packet addressed to a SCM IP interface with a source IP address outside these ranges are discarded.

Configuring an IP Address Range for the Management Network

Configure Management network IP address and mask from the System menu in the Command Line Interface (CLI).

```
>> Main# /cfg/sys/access/mgmt/add
Enter Management Network Address:  192.192.192.0
Enter Management Network Mask:  255.255.255.128
```

In this example, the management network is set to 192.192.192.0 and management mask is set to 255.255.255.128. This defines the following range of allowed IP addresses: 192.192.192.1 to 192.192.192.127. The following source IP addresses are granted or not granted access to the SCM:

- A host with a source IP address of 192.192.192.21 falls within the defined range and would be allowed to access the SCM.
- A host with a source IP address of 192.192.192.192 falls outside the defined range and is not granted access. To make this source IP address valid, you would need to shift the host to an IP address within the valid range specified by the **`mgmt`** setting, or modify the management address to be 192.192.192.128. This would put the 192.192.192.192 host within the valid range allowed by the configured management network (192.192.192.128-255).

RADIUS Authentication and Authorization

The Server Connectivity Module (SCM) supports the RADIUS (Remote Authentication Dial-in User Service) method to authenticate and authorize remote administrators for managing the Server Connectivity Module. This method is based on a client/server model. The Remote Access Server (RAS)—the Server Connectivity Module—is a client to the back-end database server. A remote user (the remote administrator) interacts only with the RAS, not the back-end server and database.

RADIUS authentication consists of the following components:

- A protocol with a frame format that utilizes UDP over IP (based on RFC 2138 and 2866)
- A centralized server that stores all the user authorization information
- A client, in this case, the Server Connectivity Module (SCM)

The SCM—acting as the RADIUS client—communicates to the RADIUS server to authenticate and authorize a remote administrator using the protocol definitions specified in RFC 2138 and 2866. Transactions between the client and the RADIUS server are authenticated using a shared key that is not sent over the network. In addition, the remote administrator passwords are sent encrypted between the RADIUS client (SCM) and the back-end RADIUS server.

How RADIUS Authentication Works

1. **Remote administrator connects to the SCM and provides user name and password.**
2. **Using Authentication/Authorization protocol, the SCM sends request to authentication server.**
3. **Authentication server checks the request against the user ID database.**
4. **Using RADIUS protocol, the authentication server instructs the SCM to grant or deny administrative access.**

Configuring RADIUS

On the BBI, choose **Miscellaneous Settings > Remote User Administration** to configure RADIUS authentication.

On the command-line interface, use the following procedure to configure RADIUS authentication on the Server Connectivity Module (SCM).

1. **Turn RADIUS authentication on, then configure the Primary and Secondary RADIUS servers.**

```
>> Main# /cfg/sys/radius                         (Select the RADIUS Server menu)
>> RADIUS Server# on                             (Turn RADIUS on)
Current status: OFF
New status:     ON
>> RADIUS Server# prisrv 10.10.1.1               (Enter primary server IP)
Current primary RADIUS server:     0.0.0.0
New pending primary RADIUS server: 10.10.1.1
>> RADIUS Server# secsrv 10.10.1.2               (Enter secondary server IP)
Current secondary RADIUS server:     0.0.0.0
New pending secondary RADIUS server: 10.10.1.2
```

2. **Configure the RADIUS secret.**

```
>> RADIUS Server# secret
Enter new RADIUS secret: <1-32 character secret>
```

3. **If desired, you may change the default UDP port number used to listen to RADIUS.**

   The well-known port for RADIUS is 1645.

```
>> RADIUS Server# port
Current RADIUS port: 1645
Enter new RADIUS port [1500-3000]: <port number>
```

4. **Configure the number retry attempts for contacting the RADIUS server, and the timeout period.**

```
>> RADIUS Server# retries
Current RADIUS server retries: 3
Enter new RADIUS server retries [1-3]:     < server retries>
>> RADIUS Server# time
Current RADIUS server timeout: 3
Enter new RADIUS server timeout [1-10]: 10 (Enter the timeout period in minutes)
```

RADIUS Authentication Features

The SCM supports the following RADIUS authentication features:

- Supports RADIUS client on the SCM, based on the protocol definitions in RFC 2138 and RFC 2866.
- Allows RADIUS secret password up to 32 bytes and less than 16 octets.

- Supports *secondary authentication server* so that when the primary authentication server is unreachable, the SCM can send client authentication requests to the secondary authentication server. Use the `/cfg/sys/radius/cur` command to show the currently active RADIUS authentication server.
- Supports user-configurable RADIUS server retry and time-out values:
  - □ Time-out value = 1-10 seconds
  - □ Retries = 1-3

  The SCM will time out if it does not receive a response from the RADIUS server in 1-3 retries. The SCM will automatically retry connecting to the RADIUS server before it declares the server down.
- Supports user-configurable RADIUS application port.
  The default is 1645/UDP-based on RFC 2138. Port 1812 is also supported.
- Allows network administrator to define privileges for one or more specific users to access the SCM at the RADIUS user database.
- SecurID is supported if the RADIUS server can do an ACE/Server client proxy. The password is the PIN number, plus the token code of the SecurID card.

User Accounts

The user accounts listed in Table 2-2 can be defined in the RADIUS server dictionary file.

Table 2-2 User Access Levels

User Account	Description and Tasks Performed	Password
User	The User has no direct responsibility for SCM management. The User can view all status information and statistics but cannot make any configuration changes to the SCM.	`user`
Operator	The Operator manages all functions of the SCM. The Operator can reset ports or the entire SCM.	`oper`
Administrator	The Administrator has complete access to all menus, information, and configuration commands on the SCM, including the ability to change both the user and administrator passwords.	`admin`

RADIUS Attributes for SCM User Privileges

When the user logs in, the SCM authenticates his/her level of access by sending the RADIUS access request, that is, the client authentication request, to the RADIUS authentication server.

If the remote user is successfully authenticated by the authentication server, the SCM verifies the *privileges* of the remote user and authorize the appropriate access. The administrator has an option to allow *backdoor* access via Telnet. The default is `disable` for Telnet access.

NOTE – To obtain the RADIUS backdoor password for your Server Connectivity Module, contact your IBM Service and Support line.

All user privileges, other than those assigned to the Administrator, have to be defined in the RADIUS dictionary. RADIUS attribute 6 which is built into all RADIUS servers defines the administrator. The file name of the dictionary is RADIUS vendor-dependent. The following RADIUS attributes are defined for SCM user privileges levels:

Table 2-3 SCM-proprietary Attributes for RADIUS

User Name/Access	User-Service-Type	Value
User	*Vendor-supplied*	255
Operator	*Vendor-supplied*	252
Admin	*Vendor-supplied*	250

TACACS+ Authentication

The Server Connectivity Module (SCM) supports authentication and authorization with networks using the Cisco Systems TACACS+ protocol. The SCM functions as the Network Access Server (NAS) by interacting with the remote client and initiating authentication and authorization sessions with the TACACS+ access server. The remote user is defined as someone requiring management access to the SCM either through a data or management port.

TACACS+ offers the following advantages over RADIUS:

- TACACS+ uses TCP-based connection-oriented transport; whereas RADIUS is UDP-based. TCP offers a connection-oriented transport, while UDP offers best-effort delivery. RADIUS requires additional programmable variables such as re-transmit attempts and time-outs to compensate for best-effort transport, but it lacks the level of built-in support that a TCP transport offers.
- TACACS+ offers full packet encryption whereas RADIUS offers password-only encryption in authentication requests.
- TACACS+ separates authentication, authorization and accounting.

How TACACS+ Authentication Works

TACACS+ works much in the same way as RADIUS authentication as described on page 24.

1. **Remote administrator connects to the SCM and provides user name and password.**
2. **Using Authentication/Authorization protocol, the SCM sends request to authentication server.**
3. **Authentication server checks the request against the user ID database.**
4. **Using TACACS+ protocol, the authentication server instructs the SCM to grant or deny administrative access.**

During a session, if additional authorization checking is needed, the SCM checks with a TACACS+ server to determine if the user is granted permission to use a particular command.

TACACS+ Authentication Features

Authentication is the action of determining the identity of a user, and is generally done when the user first attempts to log in to a device or gain access to its services. The SCM supports ASCII inbound login to the device. PAP, CHAP and ARAP login methods, TACACS+ change password requests, and one-time password authentication are not supported.

Authorization

Authorization is the action of determining a user’s privileges on the device, and usually takes place after authentication.

The mapping between TACACS+ authorization levels and SCM management access levels is shown in Table 2-4. The authorization levels must be defined on the TACACS+ server.

Table 2-4 SCM-proprietary Attributes for TACACS+

User Access Level	TACACS+ level
`user`	0
`oper`	3
`admin`	6

If the remote user is successfully authenticated by the authentication server, the SCM verifies the *privileges* of the remote user and authorize the appropriate access. The administrator has an option to allow *backdoor* access via Telnet. The default is `disable` for Telnet access.

NOTE – To obtain the TACACS+ backdoor password for your Server Connectivity Module, contact your IBM Service and Support line.

Accounting

Accounting is the action of recording a user's activities on the device for the purposes of billing and/or security. It follows the authentication and authorization actions. If the authentication and authorization is not performed via TACACS+, there are no TACACS+ accounting messages sent out.

You can use TACACS+ to record and track software logins, configuration changes, and interactive commands.

The SCM supports the following TACACS+ accounting attributes:

- protocol (console/telnet/ssh/http)
- start_time
- stop_time
- elapsed_time
- disc-cause

NOTE – When using the Browser-Based Interface, the TACACS+ Accounting Stop records are sent only if the **`Quit`** button on the browser is clicked.

Command Authorization and Logging

When TACACS+ Command Authorization is enabled (`/cfg/sys/tacacs/cauth ena`), SCM configuration commands are sent to the TACACS+ server for authorization. When TACACS+ Command Logging is enabled (`/cfg/sys/tacacs/clog ena`), SCM configuration commands are logged on the TACACS+ server.

The following examples illustrate the format of SCM commands sent to the TACACS+ server:

```
authorization request, cmd=cfgtree, cmd-arg=/cfg/sys/access/user/uid
accounting request, cmd=/cfg/sys/access/user/uid, cmd-arg=1
authorization request, cmd=cfgtree, cmd-arg=/cfg/sys/access/user/
uid/ena
accounting request, cmd=/cfg/sys/access/user/uid/ena
authorization request, cmd=cfgtree, cmd-arg=/cfg/access/user/uid/
name
accounting request, cmd=/cfg/sys/access/user/uid/name, cmd-arg=bill

authorization request, cmd=apply
accounting request, cmd=apply
```

The following rules apply to TACACS+ command authorization and logging:

- Only commands from Telnet or SSH connection are sent for authorization and logging. BBI or file-copy commands (for example, TFTP or sync) are not sent.
- Only leaf-level commands are sent for authorization and logging. For example, `/cfg` is not sent, but `/cfg/sys/access/user/uid` is sent.
- The full path of each command is sent for authorization and logging. For example, `/cfg/sys/tacacs/cauth`.
- Command arguments are not sent for authorization. For `/cauth ena`, only `/cauth` is authorized. The command and its first argument are logged, if issued on the same line.
- Only executed commands are logged.
- Invalid commands are checked by the software, and are not sent for authorization or logging.
- Authorization is performed on each leaf-level command separately. If the user issues multiple commands at once, each command is sent separately as a full path.

- Only the following global commands are sent for authorization and logging:
  ```
  apply
  diff
  ping
  revert
  save
  telnet
  traceroute
  ```

Configuring TACACS+ Authentication

On the BBI, choose **Miscellaneous Settings > Remote User Administration** to configure TACACS+ authentication.

On the command-line interface, use the following procedure to configure TACACS+ authentication on the Server Connectivity Module (SCM).

1. **Turn TACACS+ authentication on, then configure the Primary and Secondary TACACS+ servers.**

```
>> Main# /cfg/sys/tacacs+                 (Select the TACACS+ Server menu)
>> TACACS+ Server# on                     (Turn TACACS+ on)
Current status: OFF
New status:     ON
>> TACACS+ Server# prisrv 10.10.1.1       (Enter primary server IP)
Current primary TACACS+ server:     0.0.0.0
New pending primary TACACS+ server: 10.10.1.1
>> TACACS+ Server# secsrv 10.10.1.2       (Enter secondary server IP)
Current secondary TACACS+ server:     0.0.0.0
New pending secondary TACACS+ server: 10.10.1.2
```

2. **Configure the TACACS+ secret and second secret.**

```
>> TACACS+ Server# secret
Enter new TACACS+ secret: <1-32 character secret>
>> TACACS+ Server# secret2
Enter new TACACS+ second secret: <1-32 character secret>
```

3. **If desired, you may change the default TCP port number used to listen to TACACS+.**

The well-known port for TACACS+ is 49.

```
>> TACACS+ Server# port
Current TACACS+ port: 49
Enter new TACACS+ port [1-65000]: <port number>
```

4. **Configure the number retry attempts and the timeout period.**

```
>> TACACS+ Server# retries
Current TACACS+ server retries: 3
Enter new TACACS+ server retries [1-3]:    < server retries>
>> TACACS+ Server# time
Current TACACS+ server timeout: 5
Enter new TACACS+ server timeout [4-15]: 10(Enter the timeout period in minutes)
```

5. **Apply and save the configuration.**

Secure Shell and Secure Copy

Secure Shell (SSH) and Secure Copy (SCP) use secure tunnels to encrypt and secure messages between a remote administrator and the Server Connectivity Module (SCM). Telnet does not provide this level of security. The Telnet method of managing a SCM does not provide a secure connection.

SSH is a protocol that enables remote administrators to log securely into the SCM over a network to execute management commands.

SCP is typically used to copy files securely from one machine to another. SCP uses SSH for encryption of data on the network. SCP is used to download and upload the SCM configuration via secure channels.

The benefits of using SSH and SCP are listed below:

- Authentication of remote administrators
- Identifying the administrator using Name/Password
- Authorization of remote administrators
- Determining the permitted actions and customizing service for individual administrators
- Encryption of management messages
- Encrypting messages between the remote administrator and the SCM
- Secure copy support

The SCM supports SSH versions 1.5 and 2.0. and supports SSH clients version 1.5 - 2.x. The following SSH clients have been tested:

- SSH 1.2.23 and SSH 1.2.27 for Linux (freeware)
- SecureCRT 3.0.2 and SecureCRT 3.0.3 for Windows NT (Van Dyke Technologies, Inc.)
- F-Secure SSH 1.1 for Windows (Data Fellows)
- Putty SSH
- Cygwin OpenSSH

- Mac X OpenSSH
- Solaris 8 OpenSSH
- AxeSSH SSHPro
- SSH Communications Vandyke SSH A
- F-Secure

Configuring SSH/SCP features

SSH and SCP are disabled by default. Before you can use SSH commands, you must turn on SSH/SCP. Begin a Telnet session from the management module and enter the following CLI command:

```
>> # /cfg/sys/sshd/on                     (Turn SSH on)
Current status: OFF
New status: ON
```

NOTE – You cannot turn SSH off from your Telnet connection. SSH can be turned off only through a direct connection to the serial console port from a technical support representative, or by resetting the SCM to factory defaults.

To enable or disable SCP apply and save:

Enter the following commands from the CLI to enable the SCP `putcfg_apply` and `putcfg_apply_save` commands:

```
>> # /cfg/sys/sshd/ena                     (Enable SCP apply and save)
SSHD# apply                                (Apply the changes to start generating RSA
                                            host and server keys)
RSA host key generation starts
.............................................................
......................................................
RSA host key generation completes (lasts 212549 ms)
RSA host key is being saved to Flash ROM, please don't reboot
the box immediately.
RSA server key generation starts
............................................................
RSA server key generation completes (lasts 75503 ms)
RSA server key is being saved to Flash ROM, please don't reboot
the box immediately.
------------------------------------------------------------------
Apply complete; don't forget to "save" updated configuration.

>> # /cfg/sys/sshd/dis                     (Disable SSH/SCP apply and save)
```

Configuring the SCP Administrator Password

To configure the `scpadm` (SCP Administrator) password, first connect to the SCM via the management module. For security reasons, the scpadm password may only be configured when connected through the management module.

To configure the password, enter the following command via the CLI. At factory default settings, the current SCP administrator password is `admin`.

```
>> /cfg/sys/sshd/scpadm
Changing SCP-only Administrator password; validation required...
Enter current administrator password: <password>
Enter new SCP-only administrator password: <new password>
Re-enter new SCP-only administrator password: <new password>
New SCP-only administrator password accepted.
```

Using SSH and SCP Client Commands

This section shows the format for using some client commands. The examples below use 205.178.15.157 as the IP address of the management module, and 1022 as the SSH port number.

To log in to the SCM:

Syntax:

```
ssh <MM IP address> or ssh -l <login-name> <MM IP address>
```

Example**:**

```
>> # ssh 205.178.15.157 1022
>> # ssh -l <login-name> 205.178.15.157 1022 (Login to the SCM)
```

To download the SCM configuration using SCP:

Syntax**:**

```
scp <MM IP address> 1022:getcfg <local filename>
```

Example:

```
>> # scp 205.178.15.157 1022:getcfg ad4.cfg
```

To upload the configuration to the SCM:

Syntax:

```
scp <local filename> <MM IP address> 1022:putcfg
```

Example:

```
>> # scp ad4.cfg 205.178.15.157 1022:putcfg
```

To apply and save the configuration

The `apply` and `save` commands are still needed after the last command (`scp ad4.cfg 205.178.15.157 1022:putcfg`). Or, instead, you can use the following commands:

```
>> # scp ad4.cfg 205.178.15.157 1022:putcfg_apply
>> # scp ad4.cfg 205.178.15.157 1022:putcfg_apply_save
```

- The `diff` command is automatically executed at the end of `putcfg` to notify the remote client of the difference between the new and the current configurations.
- `putcfg_apply` runs the `apply command` after the `putcfg` is done.

- `putcfg_apply_save` saves the new configuration to the flash after `putcfg_apply` is done.
- The `putcfg_apply` and `putcfg_apply_save` commands are provided because extra `apply` and `save` commands are usually required after a `putcfg`; however, an SCP session is not in an interactive mode at all.

SSH and SCP Encryption of Management Messages

The following encryption and authentication methods are supported for SSH and SCP:

Server Host Authentication:	Client RSA authenticates the SCM at the beginning of every connection
Key Exchange:	RSA
Encryption:	3DES-CBC, DES
User Authentication:	Local password authentication, RADIUS, `SecurID` (via RADIUS, TACACS+, for SSH only—does not apply to SCP)

Generating RSA Host and Server Keys for SSH Access

To support the SSH server feature, two sets of RSA keys (host and server keys) are required. The host key is 1024 bits and is used to identify the SCM. The server key is 768 bits and is used to make it impossible to decipher a captured session by breaking into the SCM at a later time.

When the SSH server is first enabled and applied, the SCM automatically generates the RSA host and server keys and is stored in the FLASH memory.

NOTE – To configure RSA host and server keys, first connect to the Server Connectivity Module through the management module (commands are not available via external Telnet connection), and enter the following commands to generate them manually.

```
>> # /cfg/sys/sshd/hkeygen                    (Generates the host key)
>> # /cfg/sys/sshd/skeygen                    (Generates the server key)
```

These two commands take effect immediately without the need of an `apply` command.

When the SCM reboots, it retrieves the host and server keys from the FLASH memory. If these two keys are not available in the flash and if the SSH server feature is enabled, the SCM automatically generates them during the system reboot. This process may take several minutes to complete.

The SCM can also automatically regenerate the RSA server key. To set the interval of RSA server key autogeneration, use this command:

```
>> # /cfg/sys/sshd/intrval <number of hours (0-24)>
```

A value of 0 denotes that RSA server key autogeneration is disabled. When greater than 0, the SCM autogenerates the RSA server key every specified interval; however, RSA server key generation is skipped if the SCM is busy doing other key or cipher generation when the timer expires.

NOTE – The Server Connectivity Module (SCM) performs only one session of key/cipher generation at a time. Thus, an SSH/SCP client will not be able to log in if the SCM is performing key generation at that time, or if another client has logged in immediately prior. Also, key generation will fail if an SSH/SCP client is logging in at that time.

SSH/SCP Integration with Radius Authentication

SSH/SCP is integrated with RADIUS authentication. After the RADIUS server is enabled on the SCM, all subsequent SSH authentication requests will be redirected to the specified RADIUS servers for authentication. The redirection is transparent to the SSH clients.

SSH/SCP Integration with TACACS+ Authentication

SSH/SCP is integrated with TACACS+ authentication. After the TACACS+ server is enabled on the SCM, all subsequent SSH authentication requests will be redirected to the specified TACACS+ servers for authentication. The redirection is transparent to the SSH clients.

SecurID Support

SSH/SCP can also work with SecurID, a token card-based authentication method. The use of SecurID requires the interactive mode during login, which is not provided by the SSH connection.

NOTE – There is no Browser-Based Interface (BBI) support for SecurID because the SecurID server, ACE, is a one-time password authentication and requires an interactive session.

Using SecurID with SSH

Using SecurID with SSH involves the following tasks.

- To log in using SSH, use a special user name, “ace,” to bypass the SSH authentication.
- After an SSH connection is established, you are prompted to enter the user name and password (the SecurID authentication is being performed now).
- Provide your user name and the token in your SecurID card as a regular Telnet user.

Using SecurID with SCP

Using SecurID with SCP can be accomplished in two ways:

- Using a RADIUS server to store an administrator password.

  You can configure a regular administrator with a fixed password in the RADIUS server if it can be supported. A regular administrator with a fixed password in the RADIUS server can perform both SSH and SCP with no additional authentication required.
- Using an SCP-only administrator password.

  Use the command, `/cfg/sys/sshd/scpadm` to bypass the checking of SecurID.

  An SCP-only administrator’s password is typically used when SecurID is used. For example, it can be used in an automation program (in which the tokens of SecurID are not available) to back up (download) the SCM configurations each day.

NOTE – The SCP-only administrator’s password must be different from the regular administrator’s password. If the two passwords are the same, the administrator using that password will not be allowed to log in as an SSH user because the Server Connectivity Module (SCM) will recognize him as the SCP-only administrator. The SCM allows only the administrator access to SCP commands.

End User Access Control

The administrator can define user accounts that permit end users to access the Server Connectivity Module (SCM) using the CLI commands. Once end-user accounts are configured and enabled, the SCM requires user name/password authentication.

Considerations for Configuring End User Accounts

- A maximum of 10 end-user IDs are supported on the Port Aggregator (SCM).
- The SCM does not automatically validate configurations.

- SCM software supports end user support for Telnet access to the SCM. As a result, only very limited access is granted to the primary administrator under the BBI/SSH1 mode of access.
- If RADIUS authentication is used, the user password on the Radius server overrides the user password on the SCM. Also note that the password change command only modifies the SCM password and has no effect on the user password on the Radius server. RADIUS authentication and user password cannot be used concurrently to access the SCM.
- Passwords can be up to 128 characters in length for TACACS, RADIUS, Telnet, SSH, and Web access.

Configuring End-User Access Control

On the BBI, choose **Miscellaneous Settings** > **Local User Administration** to configure user accounts.

On the command-line interface, enter the following command to display the end user access control menu.

```
>> # /cfg/sys/access/user
```

The following command allows you to configure one of the 10 end-user IDs.

```
/cfg/sys/access/user/uid 1
```

The following command sequence allows you to define a user name and password.

```
>> User ID 1 # name bill                          (Assign name “bill” to user ID 1)
Current user name:
New user name:     bill
```

The following command sequence allows you to change the user’s password.

```
>> User ID 1 # pswd
Changing user password; validation required:
Enter current admin password: <current administrator password>
Enter new user password: <new user password>
Re-enter new user password: <new user password>
New user password accepted.
```

Defining a User’s Access Level

By default, the end user is assigned to the user access level (also known as Class of Service, or CoS). CoS for all user accounts have global access to all resources except for User CoS, which has access only to view resources that the user owns. Refer to Table 2-2 on page 27.

To change the user’s access level, enter the `cos` command, and select one of the available options:

```
>> User ID 1 # cos <user|oper|admin>
```

Validating a User’s Configuration

```
User ID 2 # cur
     name jane    , dis, cos user    , password valid, offline
```

Listing Current Users

The `cur` command displays defined user accounts and whether or not each user is currently logged into the SCM.

```
# /cfg/sys/access/user/cur

Usernames:
  user     - Enabled
  oper     - Disabled
  admin    - Always Enabled

Current User ID table:
  1: name bill    , ena, cos user, password valid, online

  2: name jane    , ena, cos user, password valid, online
```

Enabling or Disabling a User

An end user account must be enabled before the SCM recognizes and permits login under the account. Once enabled, the SCM requires any user to enter both user name and password.

```
>> # /cfg/sys/access/user/uid <#>/ena
>> # /cfg/sys/access/user/uid <#>/dis
```

Logging into an End User Account

Once an end user account is configured and enabled, the user can login using the username/ password combination. The level of access is determined by the CoS established for the end-user account.

CHAPTER 3

Port Groups, VLANs, and Trunking

This chapter describes the port, VLAN, and trunking configuration of the Server Connectivity Module (SCM). Most of the configuration is static, and cannot be changed.

Port Groups

SCM ports can be combined into Port Groups. Up to six Port Groups are available in the SCM. Each Port Group should contain both internal server ports (INT1-INT14) and external ports (EXT1-EXT6).

NOTE – The port references that appear in this document might differ slightly from your system. The number of ports is based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

VLANs and Link Aggregation Groups (trunks) are configured automatically for the Port Group. No network loops are allowed in the configuration. All external ports in the Port Group form a trunk group (static trunk or Link Aggregation Group).

Port Group Characteristics

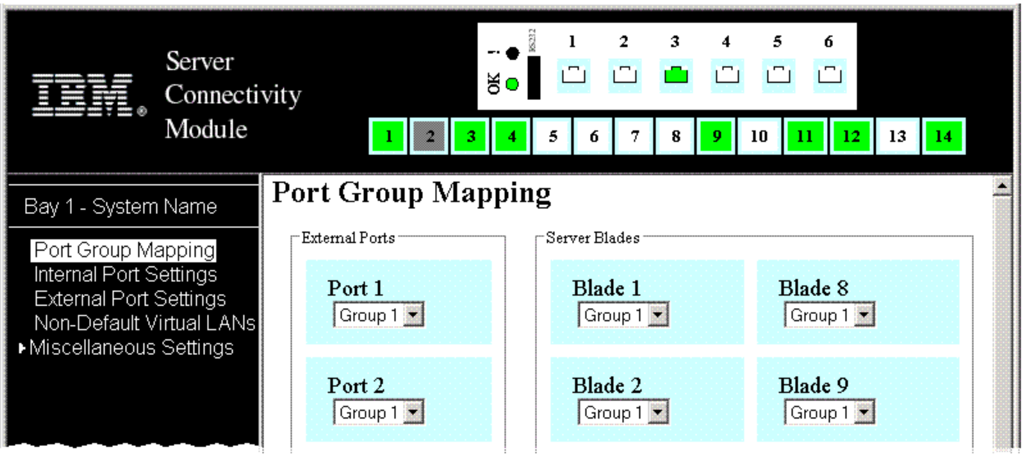
SCM Port Groups must have the following characteristics:

- Each Port Group must contain at least one external port (EXT1-EXT6) and one internal server blade port (INT1-INT14).
- All ports in a Port Group must have the same configuration.

- Each port in the Port Group is a member of a unique, untagged VLAN.
- Tagged VLANs (1-4094) can be assigned to each Port Group. Tagged VLANs cannot be configured across multiple Port Groups.

Configuring Port Groups

On the BBI, choose **Port Group Mapping** to select the Port Group for each of the external ports and server blade ports. Click **`Apply`** to save the configuration.



Port Group Mapping

External Ports

Port 1: Group 1

Port 2: Group 1

Server Blades

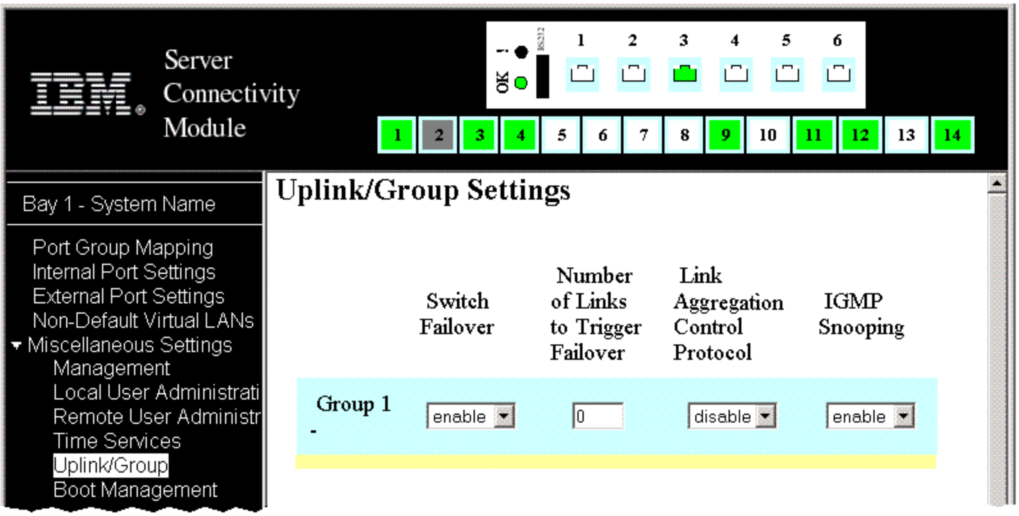
Blade 1: Group 1

Blade 8: Group 1

Blade 2: Group 1

Blade 9: Group 1

To enable Layer 2 Failover, LACP, or IGMP Snooping for the Port Group, choose **Miscellaneous Settings** > **Uplink/Group**.



Uplink/Group Settings

	Switch Failover	Number of Links to Trigger Failover	Link Aggregation Control Protocol	IGMP Snooping
Group 1	enable	0	disable	enable

VLANs

Virtual LANs (VLANs) are commonly used to split up groups of network users into manageable broadcast domains, to create logical segmentation of workgroups, and to enforce security policies among logical segments.

The default SCM configuration has two VLANS:

- The default VLAN is an untagged VLAN used for data traffic, and contains both external ports and internal server-blade ports.
- VLAN 4095 is used by the management network, which includes the management ports and (by default) the internal blade ports. This configuration allows Serial over LAN (SoL) management, a feature available on certain server blades. VLAN 4095 configuration cannot be modified.

802.1Q VLAN Tagging

802.1Q VLAN *tagging* provides standards-based VLAN support for Ethernet systems. This standard permits multiple VLANs to be transmitted over a single Ethernet connection.

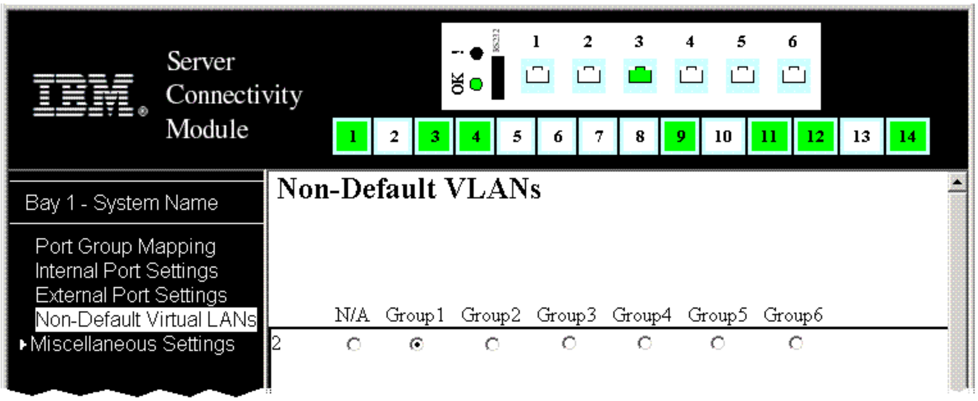
Tagging places the VLAN identifier in the frame header of a packet, allowing each port to belong to multiple VLANs. When you add a port to multiple VLANs, you must also enable tagging on that port.

NOTE – The Server Connectivity Module does not permit configuration of tagged VLANs across multiple Port Groups.

The default configuration for the SCM has all ports set as untagged members of the default VLAN. In this configuration, all incoming packets are assigned to the default VLAN. You can create up to 255 additional tagged VLANs (1-4094), and assign them to Port Groups.

Configuring VLANs

On the BBI, choose **Non-Default Virtual LANs** to create VLANs and assign them to Port Groups.



Non-Default VLANs

	N/A	Group1	Group2	Group3	Group4	Group5	Group6
2	○	●	○	○	○	○	○

1. **Click** Add VLAN **to configure a new VLAN.**
2. **Select the corresponding radio button to assign the VLAN to a Port Group.**
3. **Click** `Apply` **to make the changes active. Click** Save **to write the configuration to flash memory.**

Trunking

Trunk groups provide super-bandwidth, multi-link connections between Server Connectivity Modules (SCMs) or other trunk-capable devices. A trunk group is a group of ports that act together, combining their bandwidth to create a single, larger virtual link.

SCM trunk groups are static link aggregation groups that are compatible with Cisco’s Ether-Channel technology. This section describes the SCM trunk groups.

The SCM is statically configured to place each Port Group into a separate trunk group.

NOTE – Because all ports in a Port Group belong to the same trunk group, individual external ports cannot be used as a regular 802.3 link. Do not plug a workstation directly into one of the SCM’s external ports, unless that is the only device plugged into the ports.

When using port trunk groups between the SCM and a switch, as shown in Figure 3-1, you can create a virtual link, operating at up to 6 Gig per second, depending on how many physical ports are combined.

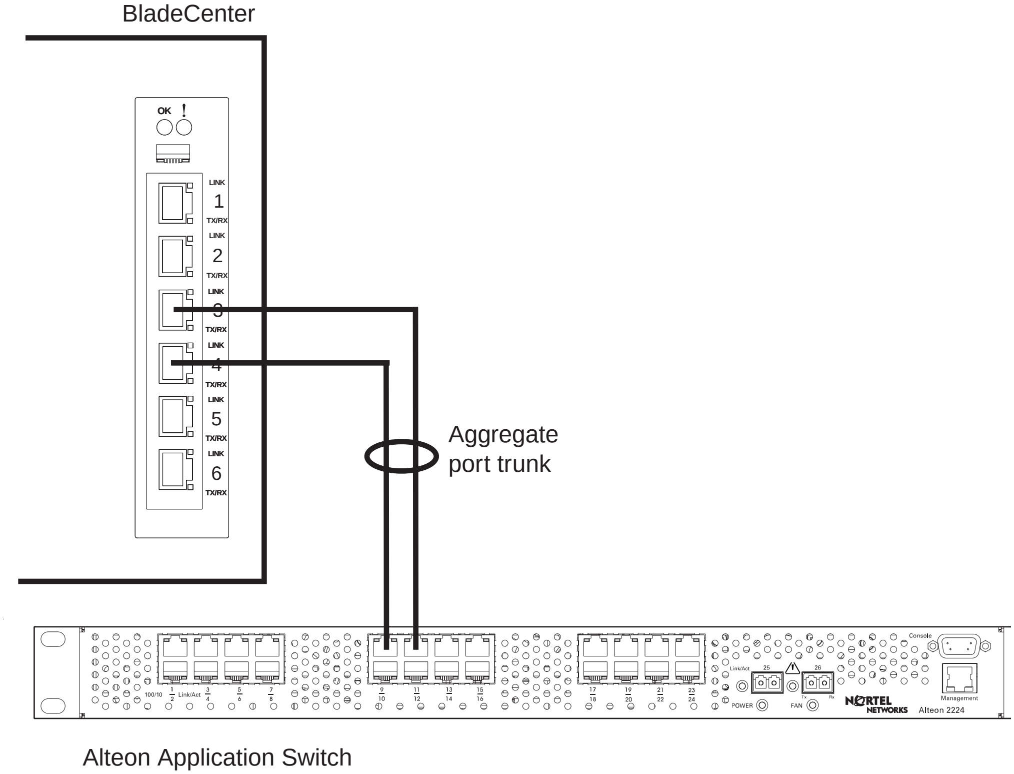


Figure 3-1 Port Trunk Group

The trunk group is also useful for connecting a SCM to third-party devices that support link aggregation, such as Cisco routers and switches with EtherChannel technology (*not* ISL trunking technology) and Sun's Quad Fast Ethernet Adapter. The SCM's trunk group technology is compatible with these devices when they are configured manually.

Statistical Load Distribution

Network traffic is statistically distributed between ports in a trunk group. The SCM uses the source and destination IP address information present in each transmitted IP frame to determine load distribution. If the frame is not an IP frame, then Layer 2 MAC addresses are used.

Each packet's particular combination of source and destination addresses results in selecting one line in the trunk group for data transmission. If there are enough devices feeding the trunk lines, then traffic distribution becomes relatively even.

Built-In Fault Tolerance

Since trunk groups are comprised of multiple physical links, each trunk group is inherently fault tolerant. As long as one connection is available, the trunk remains active.

Statistical load balancing is maintained whenever a port in a trunk group is lost or returned to service.

Trunk group configuration rules

The trunking feature operates according to specific configuration rules. When working with trunks, consider the following rules that determine how the a trunk group reacts in any network topology:

- All trunks must originate from one device, and lead to one destination device.
- Trunking from third-party devices must comply with Cisco® EtherChannel® technology.
- All ports in a Port Group must have the same configuration.
- Only external ports in a Port Group are trunked.

Link Aggregation Control Protocol

Link Aggregation Control Protocol (LACP) is an IEEE 802.3ad standard for grouping several physical ports into one logical port (known as a dynamic trunk group or Link Aggregation Group) with any device that supports the standard. Please refer to IEEE 802.3ad-2002 for a full description of the standard.

The 802.3ad standard allows standard Ethernet links to form a single Layer 2 link using the Link Aggregation Control Protocol (LACP). Link aggregation is a method of grouping physical link segments of the same media type and speed in full duplex, and treating them as if they were part of a single, logical link segment. If a link in a LACP trunk group fails, traffic is reassigned dynamically to the remaining link/s of the dynamic trunk group.

On the BBI, choose **Miscellaneous Settings > Uplink/Group** to configure LACP. When enabled, external ports in the Port Group participate in LACP. When disabled, external ports in the Port Group act as a static trunk group.

Layer 2 Failover

The primary application for Layer 2 Failover is to support Network Adapter Teaming. With Network Adapter Teaming, the NICs on each server all share the same IP address, and are configured into a team. One NIC is the primary link, and the other is a standby link. For more details, refer to “Configuring Teaming” in the Broadcom NetXtreme™ Gigabit Ethernet Adapter User Guide (http://www.ibm.com/pc/support/site.wss/MIGR-43152.html).

Layer 2 Failover is disabled by default. You can enable Layer 2 Failover on a Port Group. When enabled, Layer 2 Failover works as follows:

- If some (or all) of the links fail in the failover trigger, the SCM disables all internal ports. When the internal ports are disabled, it causes the NIC team on the affected server blades to failover from the primary to the backup NIC. This process is called a failover event.
- When the appropriate number of links return to service, the SCM enables the internal ports. This causes the NIC team on the affected server blades to fail back to the primary SCM (unless Auto-Fallback is disabled on the NIC team). The backup processes traffic until the primary's internal links come up, which takes up to five seconds.

Setting the Failover Limit

The failover limit lets you specify the minimum number of operational links required within the failover trigger before the trigger initiates a failover event. For example, if the limit is four, a failover event occurs when the number of operational links in the trigger is four or fewer. When you set the limit to zero, the SCM triggers a failover event only when no links in the trigger are operational.

Layer 2 Failover Configuration

Figure 3-2 is a simple example of Layer 2 Failover. One SCM is the primary, and the other is used as a backup. In this example, all external ports on the primary SCM belong to a single Port Group, with Layer 2 Failover enabled, and Failover Limit set to 2. If two or fewer links in trigger 1 remain active, the SCM temporarily disables all internal server-blade ports. This action causes a failover event on Server 1 and Server 2.

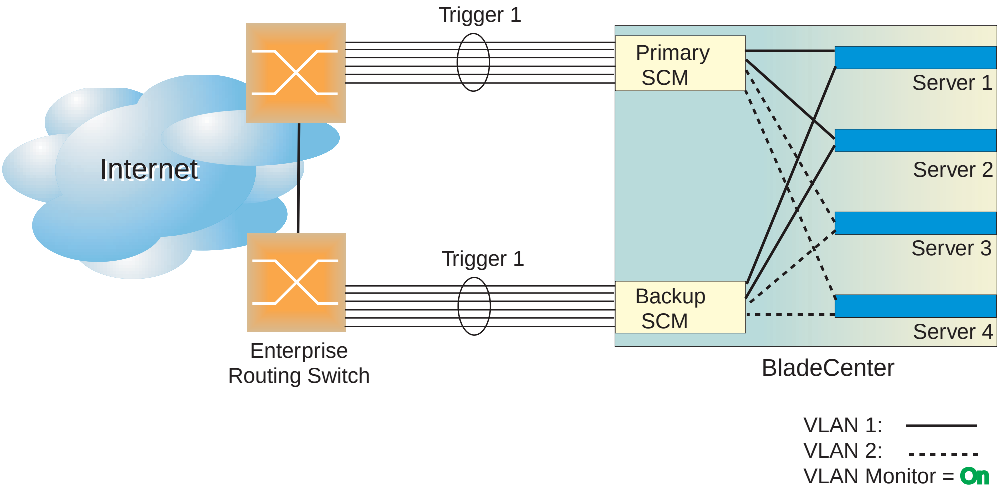


Figure 3-2 Basic Layer 2 Trunk Failover

On the BBI, choose **Miscellaneous Settings** > **Uplink/Group** to enable Layer 2 Failover, and configure the Failover Limit.

IGMP Snooping

IGMP Snooping allows the SCM to forward multicast traffic only to those ports that request it. IGMP Snooping prevents multicast traffic from being flooded to all ports. The SCM learns which server hosts are interested in receiving multicast traffic, and forwards it only to ports connected to those servers.

On the BBI, choose **Miscellaneous Settings** > **Uplink/Group** to enable IGMP Snooping. The default value is **`enabled`**.

CHAPTER 4
Command Reference

Your Port Aggregator (SCM) is ready to perform basic switching functions right out of the box. Some of the more advanced features, however, require some administrative configuration before they can be used effectively.

The command line interface is the most direct method for collecting information and performing configuration tasks. Using a basic terminal, you are presented with a hierarchy of menus that enable you to view information and statistics about the SCM, and to perform any necessary configuration.

The various commands have been logically grouped into a series of menus and sub-menus. Each menu displays a list of commands and sub-menus that are available, along with a summary of each command. Below each menu is a prompt where you can enter appropriate commands.

You can view configuration information for the SCM in both the user and administrator command modes. This chapter discusses how to use the command line interface for the SCM.

This chapter provides an overview of menu commands.

CLI Menus

The Main Menu appears after a successful connection and login. The following table shows the Main Menu for the administrator login. Some features are not available under the user login.

```
[Main Menu]
      info    - Information Menu
      stats   - Statistics Menu
      cfg     - Configuration Menu
      oper    - Operations Command Menu
      boot    - Boot Options Menu
      maint   - Maintenance Menu
      diff    - Show pending config changes  [global command]
      apply   - Apply pending config changes [global command]
      save    - Save updated config to FLASH [global command]
      revert  - Revert pending or applied changes [global command]
      exit    - Exit  [global command, always available]
```

Menu Summary

- **Information Menu**

  The Information Menu (`/info`) allows you to display information about the current status of the SCM.

```
[Information Menu]
     sys      - System Information Menu
     l2       - Layer 2 Information Menu
     l3       - Layer 3 Information Menu
     link     - Show link status
     port     - Show port information
     geaport  - Show system port and gea port mapping
     group    - Show group information
     dump     - Dump all information
```

- **Statistics Menu**

  The statistics menu (`/stats`) allows you to view performance statistics for the SCM.

```
[Statistics Menu]
     port     - Port Stats Menu
     l2       - Layer 2 Stats Menu
     l3       - Layer 3 Stats Menu
     mp       - MP-specific Stats Menu
     dump     - Dump all stats
```

Configuration Menu

The Configuration Menu (`/cfg`) allows an administrator to configure SCM parameters. Configuration changes are not active until explicitly applied. You can save changes to non-volatile memory.

```
[Configuration Menu]
     sys      - System-wide Parameter Menu
     port     - Port Menu
     group    - Group Menu
     dump     - Dump current configuration to script file
     ptcfg    - Backup current configuration to FTP/TFTP server
     gtcfg    - Restore current configuration from FTP/TFTP server
```

Operations Command Menu

The Operations Command menu (`/oper`) is used for making immediate and temporary changes to the configuration. For example, you can immediately disable a port (without the need to apply or save the change), with the understanding that when the SCM is reset, the port returns to its normally configured operation.

```
[Operations Menu]
     port     - Operational Port Menu
     passwd   - Change current user password
     clrlog   - Clear syslog messages
```

Boot Options Menu

The Boot Options menu (`/boot`) is used for upgrading SCM software, selecting configuration blocks, and for resetting the SCM when necessary.

```
[Boot Options Menu]
        image - Select software image to use on next boot
        conf  - Select config block to use on next boot
        gtimg - Download new software image via TFTP
        ptimg - Upload selected software image via TFTP
        reset - Reset switch
        cur   - Display current boot options
```

To use the Boot Options Menu, you must be logged in as the administrator. The Boot Options Menu provides options for:

- Selecting a software image to be used when the SCM is next reset
- Selecting a configuration block to be used when the SCM is next reset
- Downloading or uploading a new software image to the SCM via FTP/TFTP

- **Maintenance Menu**

The Maintenance menu (`/maint`) allows you to generate a dump of the critical state information, and to clear entries in the forwarding database and the ARP and routing tables.

```
[Maintenance Menu]
     sys       - System Maintenance Menu
     fdb       - Forwarding Database Manipulation Menu
     debug     - Debugging Menu
     arp       - ARP Cache Manipulation Menu
     igmp      - IGMP Multicast Group Menu
     uudmp     - Uuencode FLASH dump
     ptdmp     - Upload FLASH dump via FTP/TFTP
     cldmp     - Clear FLASH dump
     tsdmp     - Tech support dump
     pttsdmp   - Upload tech support dump via FTP/TFTP
```

Viewing, Applying, and Saving Changes

As you use the configuration menus to set parameters, the changes you make do not take effect immediately. All changes are considered “pending” until you explicitly apply them. Also, any changes are lost the next time the SCM boots unless the changes are explicitly saved.

NOTE – Some operations can override the settings in the Configuration menu. Therefore, settings you view in the Configuration menu (for example, port status) might differ from run-time information that you view in the Information menu or on the management module. The Information menu displays current run-time information of parameters.

While configuration changes are in the pending state, you can do the following:

- View the pending changes
- Apply the pending changes
- Save the changes to flash memory

Viewing Pending Changes

You can view all pending configuration changes by entering **`diff`** at the menu prompt.

NOTE – The `diff` command is a global command. Therefore, you can enter **`diff`** at any prompt in the CLI.

Applying Pending Changes

To make your configuration changes active, you must apply them. To apply configuration changes, enter **`apply`** at any prompt in the CLI.

```
# apply
```

NOTE – The `apply` command is a global command. Therefore, you can enter **`apply`** at any prompt in the administrative interface.

Saving the Configuration

In addition to applying the configuration changes, you can save them to flash memory on the Port Aggregator.

NOTE – If you do not save the changes, they will be lost the next time the system is rebooted.

To save the new configuration, enter the following command at any CLI prompt:

```
# save
```

When you save configuration changes, the changes are saved to the *active* configuration block. The configuration being replaced by the save is first copied to the *backup* configuration block. If you do not want the previous configuration block copied to the backup configuration block, enter the following instead:

```
# save n
```

You can decide which configuration you want to run the next time you reset the SCM. Your options include:

- The active configuration block

- The backup configuration block
- Factory default configuration

You can view all pending configuration changes that have been applied but not saved to flash memory using the `diff flash` command. It is a global command that can be executed from any menu.

Updating the Software Image

The software image is the executable code running on the Port Aggregator (SCM). A version of the image ships with the SCM, and comes pre-installed. As new versions of the image are released, you can upgrade the software running on the SCM. To get the latest version of software available, go to:

```
http://www.ibm.com/support
```

Click on Downloads and Drivers. Use the `/boot/cur` command to determine the current software version.

Upgrading the software image on the SCM requires the following:

- Loading the new image onto a FTP or TFTP server on your network
- Transferring the new image from the FTP or TFTP server to the SCM
- Selecting the new software image to be loaded into the SCM the next time it is reset

Loading New Software

The SCM can store up to two different software images, called `image1` and `image2`, as well as boot software, called `boot`. When you load new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot`.

For example, if your active image is currently loaded into `image1`, you probably want to load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

NOTE – The switch image type is checked during download onto the Server Connectivity Module, to validate that the image is compatible. If the image is incompatible, an error message is displayed.

Using the CLI

To load a new software image to the SCM, you need the following:

- The image or boot software loaded on a TFTP server on your network
- The IP address of the TFTP server
- The name of the new software image or boot file

When the above requirements are met, use the following procedure to download the new software to the SCM.

1. **At the `Boot Options#` prompt, enter:**

```
Boot Options# gtimg
```

2. **Enter the name of the software to be replaced:**

```
Enter name of switch software image to be replaced
 ["image1"/"image2"/"boot"]: <image>
```

3. **Enter the IP address of the FTP or TFTP server.**

```
Enter hostname or IP address of FTP/TFTP server: <IP address>
```

4. **Enter the name of the new software file on the server.**

```
Enter name of file on FTP/TFTP server: <filename>
```

The exact form of the name will vary by server. However, the file location is normally relative to the FTP or TFTP directory (usually `/tftpboot`).

5. **Enter your username for the server, if applicable.**

```
Enter username for FTP server or hit return for TFTP server:
<username> or <Enter>
```

6. **The system prompts you to confirm your request.**

You should next select a software image to run, as described below.

Selecting a Software Image to Run

You can select which software image (`image1` or `image2`) you want to run after the next reboot.

1. **At the `Boot Options#` prompt, enter:**

```
Boot Options# image
```

2. **Enter the name of the image you want the SCM to use upon the next boot.**

The system informs you of which image is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use switch software "image1" on next reset.
Specify new image to use on next reset ["image1"/"image2"]:
```

Uploading a Software Image from the Server Connectivity Module

You can upload a software image from the Server Connectivity Module (SCM) to a FTP or TFTP server.

1. **At the `Boot Options#` prompt, enter:**

```
Boot Options# ptimg
```

2. **The system prompts you for information. Enter the desired image:**

```
Enter name of switch software image to be uploaded
["image1"|"image2"|"boot"]: <image> <server filename>
```

3. **Enter the IP address of the FTP or TFTP server:**

```
Enter hostname or IP address of FTP/TFTP server: <IP address>
```

4. **Enter the name of the file into which the image will be uploaded on the FTP or TFTP server:**

```
Enter name of file on FTP/TFTP server: <filename>
```

5. **The system then requests confirmation of what you have entered. To have the file uploaded, enter Y.**

```
image2 currently contains Software Version 90.0.1
Upload will transfer image2 (1889411 bytes) to file "test"
 on TFTP server 192.1.1.1.
Confirm upload operation [y/n]: y
```

Selecting a Configuration Block

When you make configuration changes to the Port Aggregator (SCM), you must save the changes so that they are retained beyond the next time the SCM is reset. When you perform the `save` command, your new configuration changes are placed in the *active* configuration block. The previous configuration is copied into the *backup* configuration block.

There is also a *factory* configuration block. This holds the default configuration set by the factory when your SCM was manufactured. Under certain circumstances, it may be desirable to reset the configuration to the default.

Use the following procedure to set which configuration block you want the SCM to load the next time it is reset:

1. **At the `Boot Options#` prompt, enter:**

```
Boot Options# conf
```

2. **Enter the name of the configuration block you want the SCM to use:**

The system informs you of which configuration block is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use active configuration block on next reset.
Specify new block to use ["active"/"backup"/"factory"]:
```

Resetting the Server Connectivity Module

You can reset the Server Connectivity Module (SCM) to make your software image file and configuration block changes occur.

NOTE – Resetting the SCM causes the date and time to revert to default values. Use `/cfg/sys/date` and `/cfg/sys/time` to reenter the current date and time, unless you have configured an NTP server.

To reset the SCM, at the `Boot Options#` prompt, enter:

```
>> Boot Options# reset
```

You are prompted to confirm your request.

CHAPTER 5
Using the BBI

This chapter briefly describes the software features and requirements for the Browser-Based Interface (BBI), and explains how to access the BBI.

Requirements

- Server Connectivity Module (SCM)
- Installed SCM software
- PC or workstation with network access to the SCM's management interface as configured using the management module
- Frame-capable Web-browser software, such as the following:
  - Netscape Navigator 4.7x or higher
  - Internet Explorer 6.0x or higher
- JavaScript enabled in your Web browser

Web Browser Set Up

Most modern Web browsers work with frames and JavaScript by default, and require no additional set up. However, you should check your Web browser’s features and configuration to make sure frames and JavaScript are enabled.

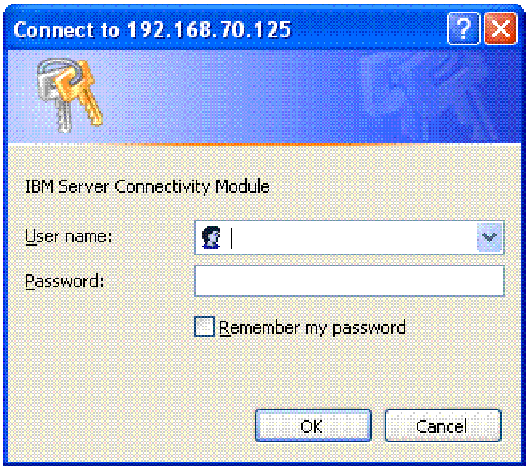
NOTE – JavaScript is not the same as Java. Please make sure that JavaScript is enabled in your Web browser.

Starting the BBI

When the Server Connectivity Module (SCM) and browser set up is done, follow these steps to launch the BBI:

1. **Access and log on to the management module, as described in the *BladeCenter Management Module User’s Guide* on the IBM *BladeCenter Documentation* CD.**
2. **Select** Configuration **on the** I/O Module Tasks **menu on the left side of the BladeCenter Management Module window.**
3. **Click a Bay number to select an SCM. Click** Advanced Configuration**.**
4. **Click** Start Web Session**.**
5. **Log in to the SCM.**

If the SCM and browser are properly configured, you will be asked to enter a password:



Connect to 192.168.70.125

IBM Server Connectivity Module

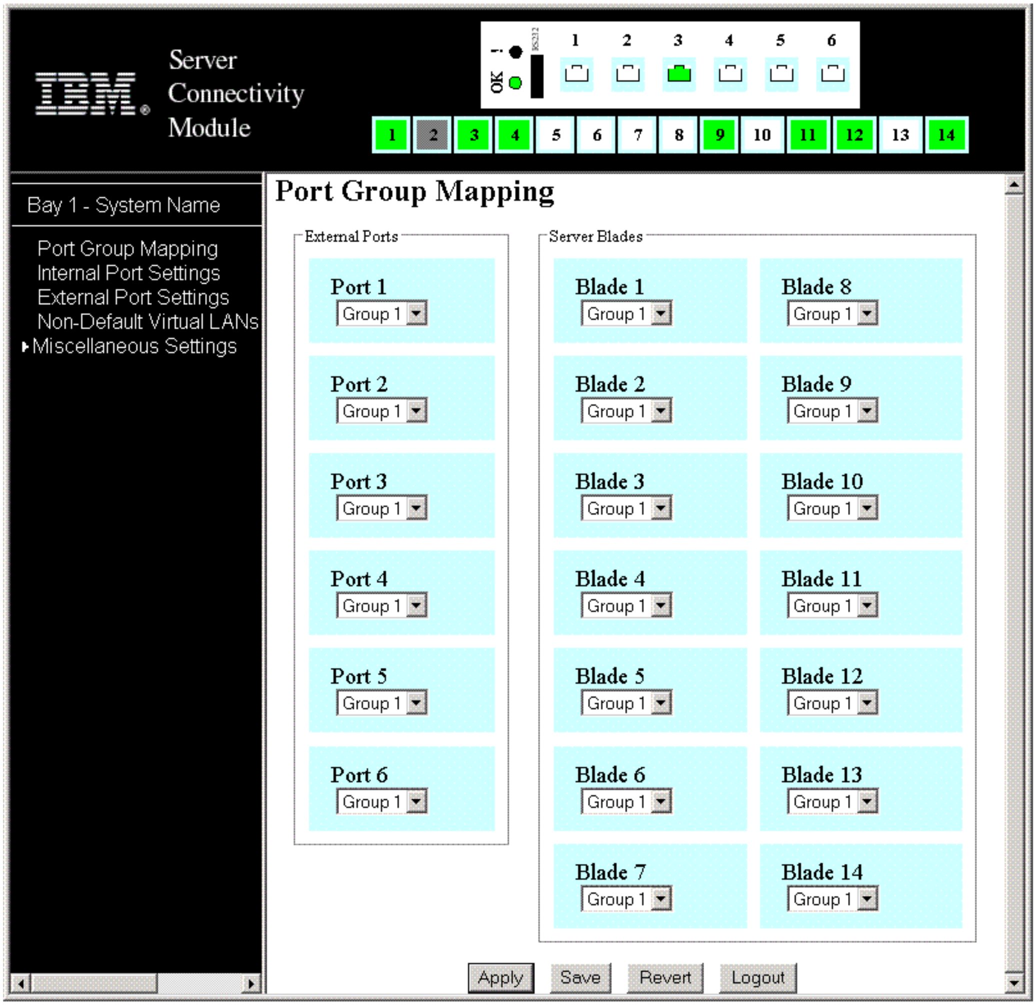
User name: |

Password:

Enter the account name and password for the SCM's administrator or user account. The default account name is *USERID*, and the default password is *PASSW0RD* (with zero "0", not "O").

6. **Allow the Port Group Mapping page to load.**

   When the proper account name and password combination is entered, the Port Group Mapping page is displayed in your browser's viewing area:



Port Group Mapping

External Ports

Port 1 Group 1
Port 2 Group 1
Port 3 Group 1
Port 4 Group 1
Port 5 Group 1
Port 6 Group 1

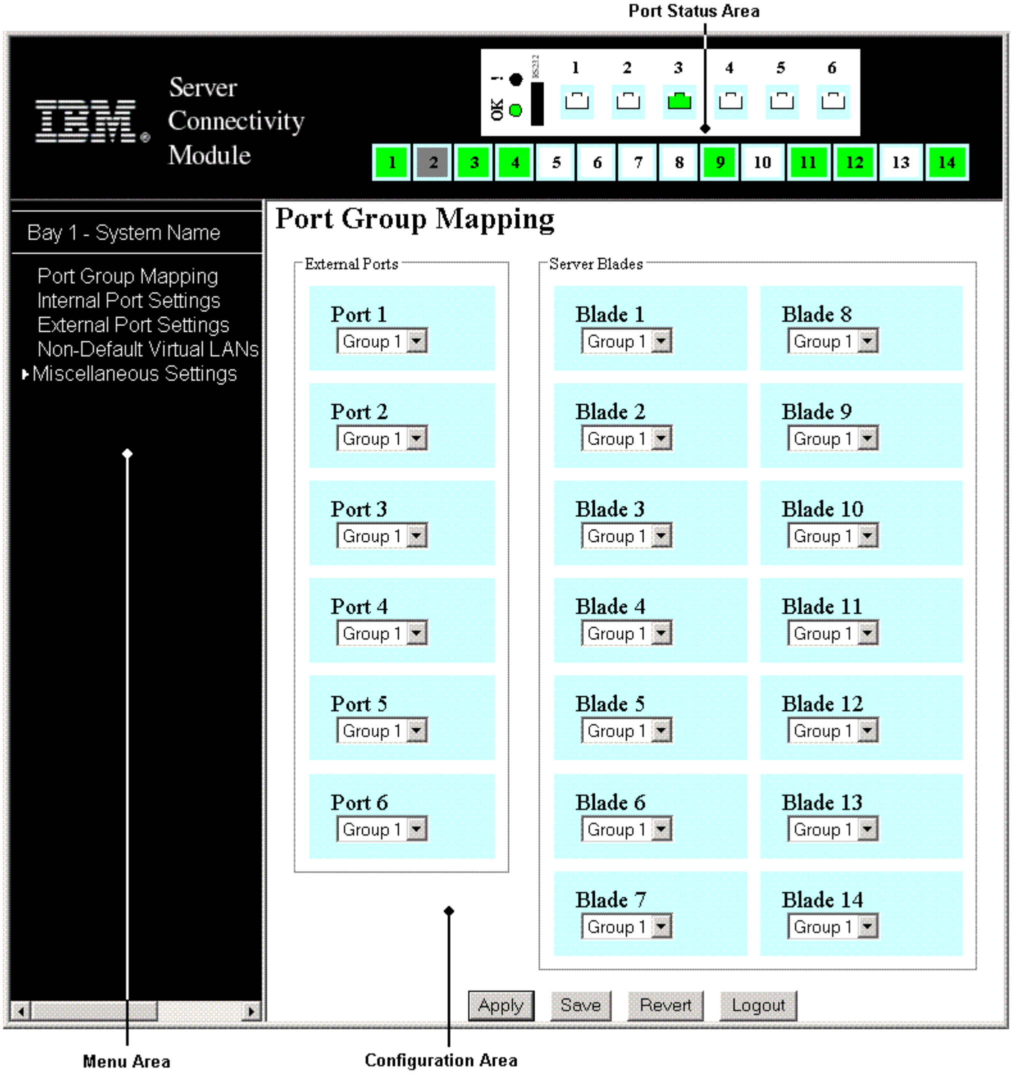
Server Blades

Blade 1 Group 1
Blade 8 Group 1
Blade 2 Group 1
Blade 9 Group 1
Blade 3 Group 1
Blade 10 Group 1
Blade 4 Group 1
Blade 11 Group 1
Blade 5 Group 1
Blade 12 Group 1
Blade 6 Group 1
Blade 13 Group 1
Blade 7 Group 1
Blade 14 Group 1

NOTE – There may be a slight delay while the Port Group Mapping page is being initialized. You should not stop the browser while loading is in progress.

NOTE – The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

Once you are properly logged in, the Browser-Based Interface (BBI) appears in your Web browser's viewing window:



Port Group Mapping

External Ports

- Port 1: Group 1
- Port 2: Group 1
- Port 3: Group 1
- Port 4: Group 1
- Port 5: Group 1
- Port 6: Group 1

Server Blades

- Blade 1: Group 1
- Blade 2: Group 1
- Blade 3: Group 1
- Blade 4: Group 1
- Blade 5: Group 1
- Blade 6: Group 1
- Blade 7: Group 1
- Blade 8: Group 1
- Blade 9: Group 1
- Blade 10: Group 1
- Blade 11: Group 1
- Blade 12: Group 1
- Blade 13: Group 1
- Blade 14: Group 1

There are three main regions on the screen:

- The Port Status Window is used to view port status. Click a port icon to view details.
- The Menu Window is used to select particular items or features to act upon.
- The Configuration Window is used to configure selected items.

Status Window

The Status Window contains port icons that display status information about each port. Click a port icon to display detailed information about the port.

A color box indicates the Port Group in which each port resides.

Link Status

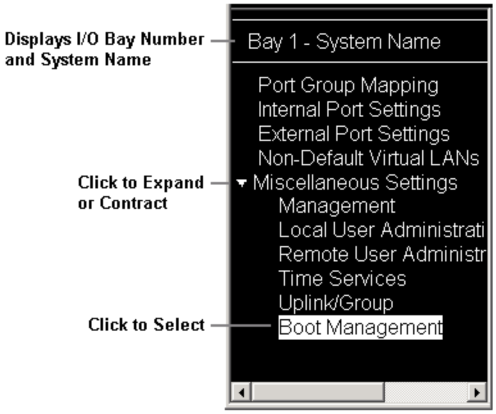
A port icon’s color indicates its link status, as follows:

Green	Link up
White	No link
Gray	Disabled

Menu Window

The Menu Window is used for selecting a particular feature to act upon. Configuration forms for the selected item appear in the Configuration Window.

The Menu Window contains a tree of feature folders and names:



Click on the Miscellaneous Settings folder to open it and reveal its contents. Click it again to close it. Click on any feature name to load the configuration form in the Configuration Window.

Configuration Window

Use the Configuration Window to configure SCM settings.

When a feature is selected on the Menu Window, a configuration form is displayed in the Configuration Window. The exact nature of the form depends on the type of information available.

Configuration forms display information and allow you to make configuration changes to SCM parameters.

Command Buttons

The following general commands are available at the bottom of the Configuration Window:

Apply	Pending configuration changes do not take effect until the Apply command is selected. Once applied, all changes take effect on the SCM immediately. If you do not save the changes, however, they will be lost the next time the SCM is rebooted.
Save	Writes applied configuration changes to non-volatile flash memory on the SCM.
Revert	Remove pending configuration changes between **Apply** commands. Use this command to restore configuration parameters set since last **Save** command.
Logout	Log off the SCM and exit the BBI.