



# User's Guide

BladeCenter Open Fabric Manager with Nortel/BNT Extensions  
for Nortel Layer 2/3 GbE Switch Module  
Version 40.0

---

Part Number: BMD00005, March 2008

**BLADE**  
N E T W O R K  
T E C H N O L O G I E S

2350 Mission College Blvd.  
Suite 600  
Santa Clara, CA 95054  
[www.bladenetwork.net](http://www.bladenetwork.net)

Copyright © 2008 Blade Network Technologies, Inc., 2350 Mission College Blvd., Suite 600, Santa Clara, California, 95054, USA. All rights reserved. Part Number: BMD00005.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Blade Network Technologies, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

U.S. Government End Users: This document is provided with a “commercial item” as defined by FAR 2.101 (Oct. 1995) and contains “commercial technical data” and “commercial software documentation” as those terms are used in FAR 12.211-12.212 (Oct. 1995). Government End Users are authorized to use this documentation only in accordance with those rights and restrictions set forth herein, consistent with FAR 12.211- 12.212 (Oct. 1995), DFARS 227.7202 (JUN 1995) and DFARS 252.227-7015 (Nov. 1995).

Blade Network Technologies, Inc. reserves the right to change any products described herein at any time, and without notice. Blade Network Technologies, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Blade Network Technologies, Inc. The use and purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Blade Network Technologies, Inc.

Originated in the USA.

Alteon OS, and Alteon are trademarks of Nortel Networks, Inc. in the United States and certain other countries. Cisco® and EtherChannel® are registered trademarks of Cisco Systems, Inc. in the United States and certain other countries. Any other trademarks appearing in this manual are owned by their respective companies.

BLADE Network Technologies is the market-leading supplier of gigabit and 10G Ethernet, IP, and Application Switches for blade server systems globally. BLADE is the first vendor to focus exclusively on serving the network infrastructure needs of the rapidly growing blade server market. The company's end-users include Fortune 500 companies across 26 different industry segments.

# Contents

---

## **Preface 5**

Who Should Use This Guide 5

What You'll Find in This Guide 6

Typographic Conventions 7

How to Get Help 8

## **Chapter 1: Overview of BOFM Extensions Operation 9**

BOFM Extensions Quick Start 10

Configuring the BladeCenter Management Module 10

Configuring the Upstream Networking Device 10

Configuring the BladeCenter Processor Blades 11

## **Chapter 2: Using the BOFM Extensions BBI 13**

Requirements 13

Web Browser Set Up 13

Starting the BBI 14

Port Status 16

Link Status 16

Menu bar 17

Configuration window 18

Command Buttons 18

Updating the Software Image 19

Loading New Software 19

Selecting a Software Image to Run 21

Uploading a Software Image 21

Selecting a Configuration Block 22

Resetting the Switch 22

## **Chapter 3: Port Groups, VLANs, and Trunking 23**

- Port Groups 24
  - Port Group Characteristics 24
  - Configuring Port Groups 25
- VLANs 27
  - 802.1Q VLAN Tagging 27
  - Configuring VLANs 28
- Trunking 29
  - Statistical Load Distribution 30
  - Built-In Fault Tolerance 31
  - Trunk group configuration rules 31
  - Link Aggregation Control Protocol 31
  - Switch Failover 32
    - Setting the Number of Links to Trigger Failover 32
    - Configuring Switch Failover 33
- IGMP Snooping 34
- ServerMobilityTM 35
  - Configuring a backup server port 35
  - General Configuration 36
  - Port Configuration 37
  - DHCP Server Configuration 38

## **Chapter 4: Command Reference 41**

- CLI Menus 42
  - Menu Summary 42
- Viewing, Applying, and Saving Changes 45
  - Viewing Pending Changes 46
  - Applying Pending Changes 46
  - Saving the Configuration 46

## **Chapter 5: Configuring Switch Access 49**

- Management module setup 50
  - Factory default vs. MM assigned IP addresses 50
  - Configuring the default gateway 51
  - Configuring management module for switch access 51
- Using Telnet 54
  - Connect to the Switch via SSH 54
- Using the Browser-Based Interface 55

Access via HTTP	55
Access via HTTPS	55
Securing Access to the Switch	57
Setting Allowable Source IP Address Ranges	57
Configuring an IP Address Range for the Management Network	57
RADIUS Authentication and Authorization	59
Configuring RADIUS	59
User Accounts	60
RADIUS Attributes for Switch User Privileges	60
TACACS+ Authentication	61
TACACS+ Authentication Features	61
Authorization	61
Configuring TACACS+ Authentication	62
End User Access Control	62
Considerations for Configuring End User Accounts	63
Configuring End-User Access Control	64
Logging into an End User Account	65
Protected Mode	65
Secure Shell and Secure Copy	67
Configuring SSH/SCP features	68
Configuring the SCP Administrator Password	69
Using SSH and SCP Client Commands	69
To apply and save the configuration	70
SSH and SCP Encryption of Management Messages	71
Generating RSA Host and Server Keys for SSH Access	71
SSH/SCP Integration with Radius Authentication	72
SSH/SCP Integration with TACACS+ Authentication	72



# Preface

---

BladeCenter Open Fabric Manager with Nortel/BNT Extensions (BOFM Extensions) is a simplified software image that can be run on the Layer 2/3 GbE Switch Module for IBM BladeCenter. BOFM Extensions software provides an easy-to-use Graphical User Interface and a reduced function set to minimize networking mis-configuration.

This User's Guide describes how to configure and use the BOFM Extensions software. Refer to your Nortel Layer 2/3 GbESM *Installation Guide* for details about how to install the switch module in a BladeCenter chassis.

---

**NOTE** – When the term switch is used in this document, it specifically refers to a Nortel Layer 2/3 GbE Switch Module that is running BOFM Extensions software.

---

## 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 switch. The BOFM Extensions software'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 the BOFM Extensions software. Where possible, each section provides feature overviews, usage examples, and configuration instructions.

- [Chapter 1, “Overview of BOFM Extensions Operation,”](#) provides a general theory of operation for the BOFM Extensions.
- [Chapter 2, “Using the BOFM Extensions BBI,”](#) provides an overview of the Browser-Based Interface (BBI) that enables you to view and configure the BOFM Extensions.
- [Chapter 3, “Port Groups, VLANs, and Trunking,”](#) describes how to group multiple physical ports together to aggregate the bandwidth between large-scale network devices. This chapter also describes VLAN configuration, Switch Failover, IGMP Snooping, and Server Mobility.
- [Chapter 4, “Command Reference,”](#) provides an overview of menu commands that enable you to view information and statistics about the BOFM Extensions, and to perform any necessary configuration.
- [Chapter 5, “Configuring Switch Access,”](#) describes how to access the BOFM Extensions to configure, view information and run statistics. This chapter also discusses different methods to manage the BOFM Extensions for remote administrators using the management module, RADIUS authentication, Secure Shell (SSH), and Secure Copy (SCP).



# 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.  It also depicts on-screen computer output and prompts.	View the <code>readme.txt</code> file.  Main#
<b>AaBbCc123</b>	This bold type appears in command examples. It shows text that must be typed in exactly as shown.	Main# <b>sys</b>
<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.  This also shows book titles, special terms, or words to be emphasized.	To establish a Telnet session, enter: host# <b>telnet</b> <i>&lt;IP address&gt;</i>  Read your <i>User's Guide</i> thoroughly.
[ ]	Command items shown inside brackets are optional and can be used or excluded as the situation demands. Do not type the brackets.	host# <b>ls</b> [-a]

## How to Get Help

---

If you need help, service, or technical assistance, see the "Getting help and technical assistance" appendix in the BOFM Extensions software for IBM BladeCenter *Installation Guide*.

## CHAPTER 1

# Overview of BOFM Extensions Operation

---

The BOFM Extensions software 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 BOFM Extensions software are restricted to reduce the initial setup complexity and to minimize the impact on upstream networking devices.

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

The BOFM Extensions 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 switches within the BladeCenter chassis to provide enhanced reliability. The L2 Failover option allows the BOFM Extensions software 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 switch(es) in the BladeCenter chassis.

The BOFM Extensions software 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 BOFM Extensions software. However, a command-line interface (CLI) is available for users familiar with the CLI, or who want to use scripting facilities.

## BOFM Extensions Quick Start

After you load the BOFM Extensions software, the default configuration allows the switch to 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 switch. The management module is also used to control several operational characteristics of the switch:

- 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 BOFM Extensions 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 switch, do the following:

- Plug in the Ethernet cable (straight through or crossover) that connects the switch 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 switch port characteristics using the appropriate BBI or CLI interfaces.

If more than one link is required to the switch, 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 switches 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

# Using the BOFM Extensions BBI

---

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

The BBI allows you to perform basic configuration tasks quickly and easily. The command line interface provides more detailed configuration options for the BOFM Extensions software (see [“Command Reference” on page 41](#)).

## Requirements

---

- Nortel Layer 2/3 GbE Switch Module for IBM BladeCenter
- Installed BOFM Extensions software
- PC or workstation with network access to the switch’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
  - Mozilla FireFox 1.0.4 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.

---

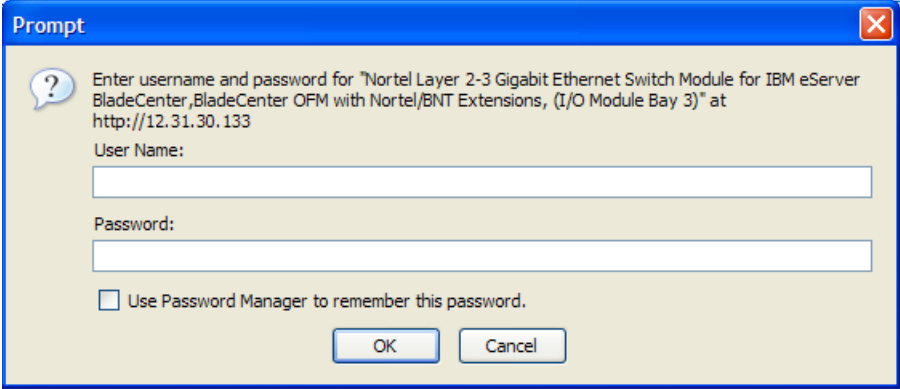
## Starting the BBI

---

When the switch and browser set up is done, follow these steps to launch the BOFM Extensions BBI:

1. **Access and log on to the management module, as described in the *BladeCenter Management Module User's Guide*.**
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 the switch. Click Advanced Configuration.**
4. **Click Start Web Session.**
5. **Log in to the switch.**

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



Enter the account name and password for the switch's administrator or user account. The default account name is *admin*, and the default password is *admin*.

---

**NOTE** – There may be a slight delay while the Port Group Mapping page is being initialized. Do 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 BOFM Extensions BBI appears in your Web browser's viewing window:

**Port Status**

**BLADE** *BladeCenter OFM with Nortel/BNT Extensions*  
 NETWORK TECHNOLOGIES

**Nortel L2/3 GbESM**  
[Help](#) [Logout](#)

**Bay 2**

Port Group Mapping  
 Internal Port Settings  
 External Port Settings  
 Non-Default Virtual LANs  
 System Settings

**Port Group Mapping**

**External Port**

EXT1	Group 1
EXT2	Group 1
EXT3	Group 1
EXT4	Group 1
EXT5	Group 1
EXT6	Group 1

**Server Port**

INT1	Group 1	INT2	Group 1
INT3	Group 1	INT4	Group 1
INT5	Group 1	INT6	Group 1
INT7	Group 1	INT8	Group 1
INT9	Group 1	INT10	Group 1
INT11	Group 1	INT12	Group 1
INT13	Group 1	INT14	Group 1

[Apply](#) [Save](#) [Revert/Apply](#)

**Menus** **Configuration window**

There are three main regions on the screen:

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

## Port Status

---

The Port Status area 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:

---

<b>Gray</b>	Disabled
<b>Green</b>	Link up
<b>White</b>	No link

---

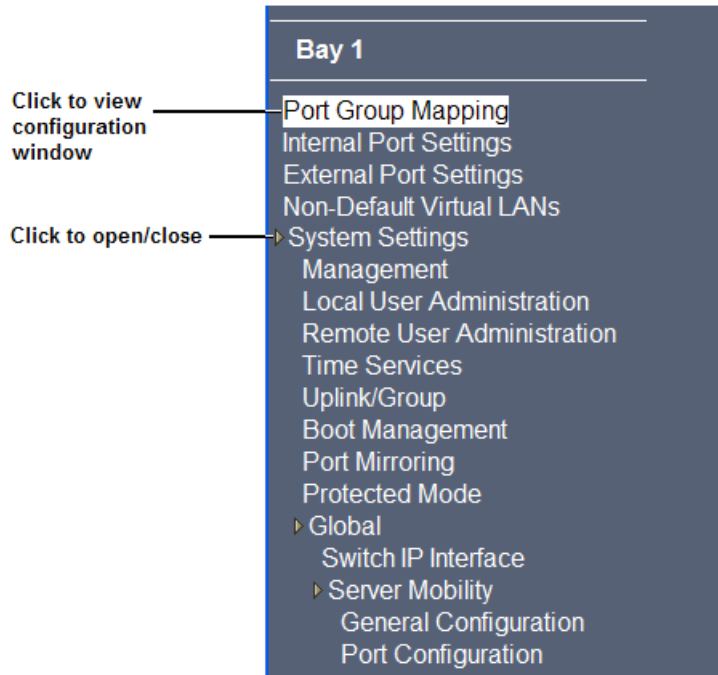
Click a port icon to display statistics for the port.

## Menu bar

---

Use the menu bar to select a particular feature to act upon. When you choose a menu item, the corresponding Configuration window is displayed.

The menu bar contains a tree of feature folders and names:



Click on the System Settings folder to open it and reveal its contents. Click it again to close it. Click on any feature name to view the Configuration window.

## Configuration window

---

Use the Configuration window to configure settings for BOFM Extensions software.

When you choose a menu item, the corresponding Configuration window is displayed. The Configuration window provides information and allows you to make configuration changes to BOFM Extensions settings.

### Command Buttons

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

---

<b>Apply</b>	Pending configuration changes do not take effect until the Apply command is selected. Once applied, all changes take effect on the BOFM Extensions immediately. If you do not save the changes, however, they will be lost the next time the switch is rebooted.
<b>Save</b>	Writes applied configuration changes to non-volatile flash memory on the switch.
<b>Revert Apply</b>	Remove pending and applied changes made since the last <b>Save</b> command was issued.

---

## Updating the Software Image

---

The software image is the executable code running on the switch. The latest version of the BOFM Extensions software can be downloaded from the BladeCenter support website:

<http://www.ibm.com/support>

In the BBI, choose menu **System Settings > Boot Management**.

Upgrading the software image on the switch typically involves the following actions:

- Load the new image onto a FTP or TFTP server on your network, or on a local computer.
- Transfer the new image to the switch.
- Select the new software image to be loaded into the switch the next time it is rebooted/reset.

## Loading New Software

The switch 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 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 the software download, to validate that the image is compatible. If the image is incompatible, an error message is displayed.

---

You can use the BBI to load software onto the switch. The software image to load can reside in one of the following locations:

- FTP server
- TFTP server
- Local computer

Perform the following steps to load a software image:

1. In the menu bar, select System Settings > Boot Management.

The Boot Management page appears.

**Boot Management**

Reboot the Module  Next boot config block

Image to boot  Image to transfer

**Current Image Information**

Image 1 - version 1.4.3, downloaded 3:26:40 Tue Jan 6, 2007 NormalConnect  
 Image 2 - version 40.0.1, downloaded 0:52:49 Thu Jan 1, 2007 BladeCenter  
 OFM with Nortel/BNT Extensions  
 Boot kernel - version 1.4.3

**Update Image/Cfg**

Method to use for transfer

Settings for using FTP or TFTP Server

Server Address   
 Remote File Name

2. Select the Image to transfer.
3. In the Update Image/Cfg section, select the Method to use for transfer.
  - If you are loading software from a TFTP server, enter the Server IP Address, and the Remote File Name. Click Get Image.
  - If you are loading software from a FTP server, enter the Server IP Address, and the Remote File Name. Enter the FTP Username and FTP Password. Click Get Image.
  - If you are loading software from your computer (HTTP), click Browse. In the File Upload Dialog, select the file and click OK. Click Get Image.

Once the image has loaded, the page refreshes to show the new software.

## Selecting a Software Image to Run

Perform the following steps to select which software image (image1 or image2) you want to run after the next reboot.

1. **In the menu bar, select System Settings > Boot Management.**

**The Boot Management page appears.**

2. **Select the Image to boot.**
3. **Click Reboot the Module to activate the new software image.**

The switch can store two different types of software image, as follows:

- Normal Layer 2/3 software image
- BOFM Extensions software image

You can use this procedure to switch from one image type to the other. However, the configuration block for one image type is not compatible with the other type.

If you change the software type, you must load a compatible configuration block, or reset the configuration to factory defaults. It is recommended that both the active configuration and the backup configuration remain compatible with the active image type. For example, if BOFM Extensions image is in the active config, do not store a normal image in the backup config.

## Uploading a Software Image

Perform the following steps to upload a software image from the switch to a FTP or TFTP server.

1. **In the menu bar, select System Settings > Boot Management.**  
**The Boot Management page appears.**
2. **Select the Image to transfer.**
3. **In the Update Image/Cfg section, select the Method to use for transfer.**
  - **If you are loading software to a TFTP server, enter the Server IP Address, and the Remote File Name. Click Put Image.**
  - **If you are loading software to a FTP server, enter the Server IP Address, and the Remote File Name. Enter the FTP Username and FTP Password. Click Put Image.**

## Selecting a Configuration Block

---

When you make configuration changes to the switch, you must save the changes so that they are retained beyond the next time the switch 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 of the BOFM Extensions software. Under certain circumstances, it may be desirable to reset the switch software to its default configuration.

Perform the following steps to select which configuration block you want the switch to load the next time it is reset:

1. **In the menu bar, select System Settings > Boot Management.**  
**The Boot Management page appears.**
2. **Select the Next boot config block.**
3. **Click Reboot the Module to activate the new configuration block.**

## Resetting the Switch

---

You can reset the switch to make your software image file and configuration block changes occur.

---

**NOTE** – Resetting the switch causes the date and time to revert to default values.

Use the Time Services configuration window (**System Settings > Time Services**) to re-enter the current date and time, unless you have configured an NTP server.

---

To reset the switch module:

1. **In the menu bar, select System Settings > Boot Management.**  
**The Boot Management page appears.**
2. **Click Reboot the Module.**



## CHAPTER 3

# Port Groups, VLANs, and Trunking

---

This chapter describes the port, VLAN, and trunking configuration of the BOFM Extensions software.

Most of the configuration is static, and cannot be changed.

- [Port Groups](#)
- [VLANs](#)
- [Trunking](#)
- [IGMP Snooping](#)
- [ServerMobility™](#)

## Port Groups

---

Switch ports can be combined into Port Groups. Up to six Port Groups are available. 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

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 menu **Port Group Mapping** to select the Port Group for each of the external ports and server blade ports. Click **Apply** to make your changes active.

### Port Group Mapping

External Port

EXT1 Group 1 ▾

EXT2 Group 1 ▾

EXT3 Group 1 ▾

EXT4 Group 1 ▾

EXT5 Group 2 ▾

EXT6 Group 2 ▾

Server Port

INT1 Group 1 ▾

INT2 Group 1 ▾

INT3 Group 1 ▾

INT4 Group 1 ▾

INT5 Group 1 ▾

INT6 Group 1 ▾

INT7 Group 1 ▾

INT8 Group 1 ▾

INT9 Group 1 ▾

INT10 Group 1 ▾

INT11 Group 2 ▾

INT12 Group 2 ▾

INT13 Group 2 ▾

INT14 Group 2 ▾

Apply

Save

RevertApply

Choose menu **Internal Port Settings** to configure server blade ports (enable or disable).

Choose menu **External Port Settings** to configure external ports, as follows:

- Port name
- Operational status (enable or disable)
- Port speed
- Flow control (rx, tx, both, none))

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

### Uplink/Group Settings

Group	Switch Failover	Number of Links to Trigger Failover	Link Aggregation Control Protocol	IGMP Snooping
Group 1	disable ▼	all ▼	disable ▼	enable ▼
Group 2	disable ▼	all ▼	disable ▼	enable ▼
Group 3	disable ▼	all ▼	disable ▼	enable ▼
Group 4	disable ▼	all ▼	disable ▼	enable ▼
Group 5	disable ▼	all ▼	disable ▼	enable ▼
Group 6	disable ▼	all ▼	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 BOFM Extensions 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.

The default configuration for the BOFM Extensions 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 1022 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	Group 1	Group 2	Group 3	Group 4	Group 5	Group 6
VLANs							
2	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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 switch modules 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.

Trunk groups are static link aggregation groups that are compatible with Cisco's EtherChannel technology. This section describes trunk group operation.

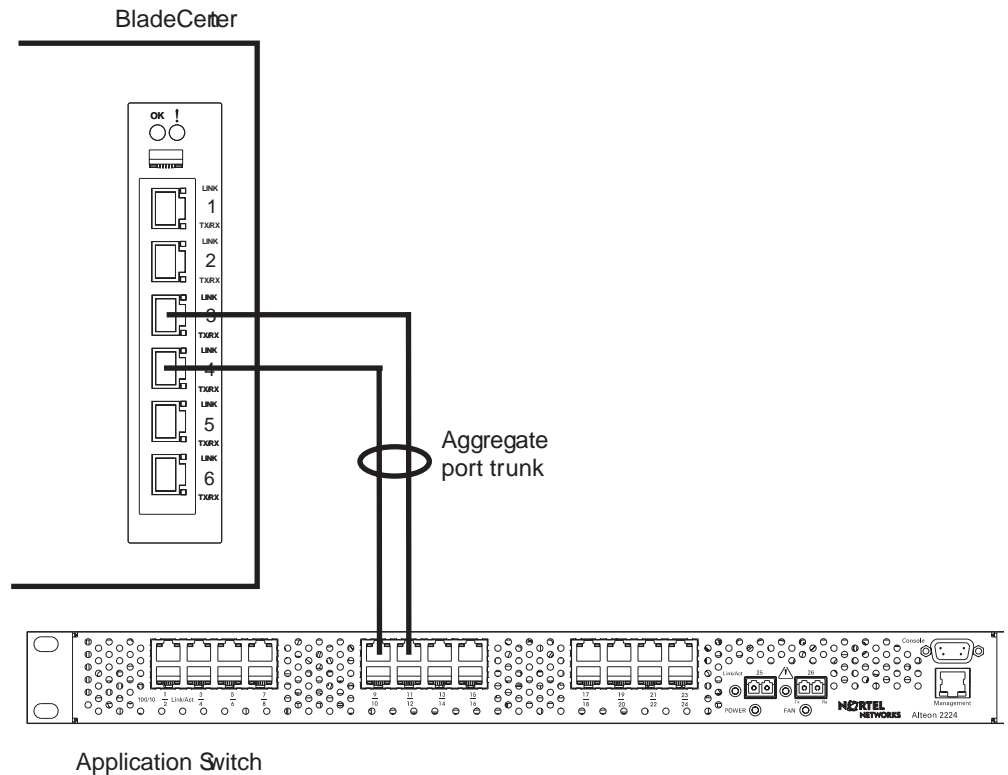
BOFM Extensions software is statically configured to place each Port Group into a separate trunk group.

---

**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 switch's external ports, unless that is the only device plugged into the ports.

---

When using port trunk groups between the switch module and other network devices, 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 switch module 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 switch'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 switch 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 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<sup>®</sup> EtherChannel<sup>®</sup> 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 reasigned dynamically to the remaining link/s of the dynamic trunk group.

On the BBI, choose **System 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.

## Switch Failover

The primary application for Switch 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.

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

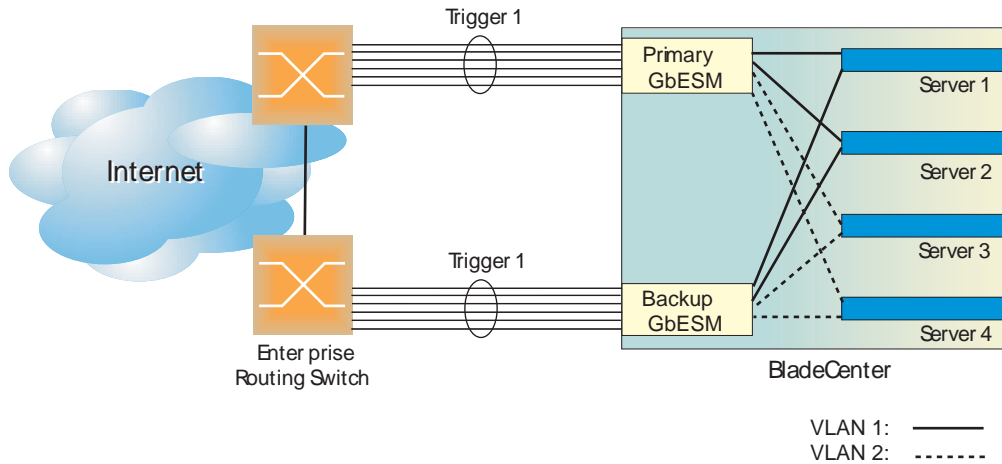
- If some (or all) of the links fail in the failover trigger, the switch disables all internal ports in the Port Group. When the internal ports are disabled, it causes the NIC team on the affected server blades to failover from the primary to the backup NIC. This process is called a failover event.
- When the appropriate number of links return to service, the switch enables the internal ports in the Port Group. This causes the NIC team on the affected server blades to fail back to the primary switch (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 Number of Links to Trigger Failover

The Number of Links to Trigger Failover specifies the minimum number of operational links in the Port Group that triggers 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 number of links to zero (0), the switch triggers a failover event only when no links in the Port Group are operational.

## Configuring Switch Failover

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



**Figure 3-2** Basic Switch Failover

On the BBI, choose **System Settings > Uplink/Group** to enable Switch Failover, and configure the Number of Links to Trigger Failover.

## IGMP Snooping

---

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

By default, the BOFM Extensions floods unregistered IP multicast (IPMC) packets to all ports.

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

## ServerMobility™

---

The ServerMobility feature allows you to assign server IP addresses based on their physical location in a BladeCenter Chassis. If a server fails, a replacement server can assume the identity of the failed unit. The replacement can be new blade server placed into the slot of the failed unit, or it can be a backup server in another slot, that is activated to take over for the failed server.

The ServerMobility feature uses DHCP option 82 to support fixed server address allocation. When the switch relays a server's DHCP request, it inserts the chassis ID, slot number, and port number into the request, as follows:

- The chassis ID is encoded in the Agent circuit ID sub-option, in hexadecimal format, as follows:  
59:49:00:c1:56:5f:11:db:a8:dd:ca:d0:a4:b3:de:4a
- The slot number and port number are encoded in the Agent remote ID sub-option, in hexadecimal format. The following example shows how slot 1 and port number 2 are configured in the Agent remote ID:  
01:0:0:0:02

The DHCP server must be configured to supply a reserved IP address for each server, based on the option 82 information.

---

**NOTE** – The ServerMobility feature operates independently of the BladeCenter Open Fabric Manager (OFM) features that may be installed on the chassis Advanced Management Module. ServerMobility should not be enabled on the switch if you have already enabled BladeCenter OFM server failover features on the chassis Management Module.

---

### Configuring a backup server port

If you configure one server as the backup to another server, you may want the two servers to use the same IP address, even though they are in different slots. To address this issue, configure a port as the backup port of another (active) port on the BOFM Extensions. The agent remote ID sub-option for packets received on the backup port will use the port number of its active port. When the active server goes down, the backup server will receive the same IP address as the active server.

The following configuration guidelines apply to ServerMobility backup ports:

- Both the active port and the backup port must have the ServerMobility feature enabled.
- The active port and the backup port must be in the same Port Group.

## General Configuration

To configure the ServerMobility feature, choose **System Settings > Global > Server Mobility > General Configuration**.

**Server Mobility General Configuration**

**Bootstrap Protocol Relay**

BOOTP Server IP Address: 0.0.0.0

Secondary BOOTP Server IP Address: 0.0.0.0

BOOTP State: Disabled

**Server Mobility**

Server Mobility State: Disabled

Relay on Non-Server-Mobility Ports: Enabled

Set Server Mobility configuration to factory default: ☐

Apply Save Revert Apply

**Figure 3-3** ServerMobility™ general configuration

The following table describes the general options for the ServerMobility feature.

**Table 2** ServerMobility™ - General Configuration fields

Field	Description
	<b>Bootstrap Protocol Relay</b>
BOOTP Server IP Address	Sets the IP address of the BOOTP server.
Secondary BOOTP Server IP Address	Sets the IP address of the secondary BOOTP server (optional).
BootP State	Enables or disables BOOTP Relay on the switch.

**Table 2** ServerMobility™ - General Configuration fields (Continued)

Field	Description
	<b>ServerMobility</b>
ServerMobility State	Enables or disables the ServerMobility feature on the switch.
Relay on Non-Server-Mobility Ports	Enables or disables BOOTP Relay for all ports that have the ServerMobility feature disabled.
Set ServerMobility configuration to factory default	Resets ServerMobility parameters to factory default values.

## Port Configuration

To configure ports for the ServerMobility feature, choose **System Settings > Global > ServerMobility > Port Configuration**.

Port	Port Server Mobility Mode	Port DHCP request filtering Mode	Backup Port
INT1	enabled ▼	disabled ▼	None ▼
INT2	disabled ▼	disabled ▼	None ▼
INT3	disabled ▼	disabled ▼	None ▼
INT4	disabled ▼	disabled ▼	None ▼
INT5	disabled ▼	disabled ▼	None ▼
INT6	disabled ▼	disabled ▼	None ▼
INT7	disabled ▼	disabled ▼	None ▼
INT8	disabled ▼	disabled ▼	None ▼

**Figure 3-4** ServerMobility™ port configuration

The following table describes the ServerMobility feature options for each port on the switch.

**Table 3** ServerMobility™ - Port Configuration fields

Field	Description
Port	Identifies each port in the switch.
Port ServerMobility Mode	Enables or disables the ServerMobility feature on the port. When enabled, DHCP option 82 information is forwarded to the DHCP server.
Port DHCP request filtering mode	Enables or disables filtering DHCP request information on the port. When enabled, DHCP requests from the blade server are filtered, so that the DHCP server receives only DHCP requests from the switch. <b>Note:</b> If the ServerMobility feature is enabled on a port, it is recommended that you also enable DHCP request filtering.
Backup port	Selects a backup port. The blade server connected to the backup port acts as a backup to the server connected to this port. The backup server uses the same IP address as the active server.

## DHCP Server Configuration

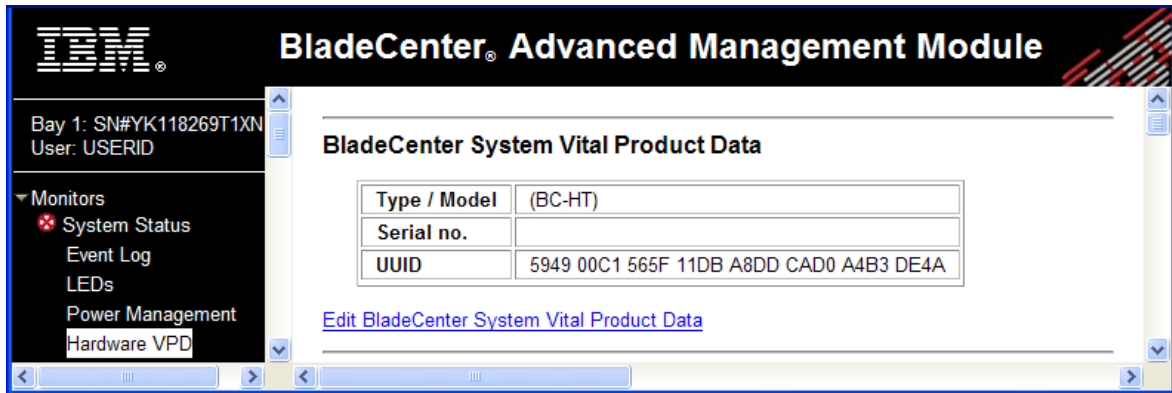
To modify the DHCP server configuration, open the configuration file (**dhcpcd.conf**), and add new classes for server ports. Then define an IP address for each class.

For Linux DHCP servers, option 82 information is referenced by the following variables:

- `option agent.circuit-id`
- `option agent.remote-id`



You can use these variables in any expression allowed within a DHCP configuration file. To declare an explicit chassis, configure the chassis ID in **agent.circuit-id**. In the advanced management module, the chassis ID is displayed in the UUID field on the System Vital Product Data window (**Monitors > Hardware VPD**).



**Figure 3-5** Chassis UUID field on management module VPD window

This configuration declares a class for the server connected to port INT8 of a switch in slot 1 of chassis 5949 00C1 565F 11DB A8DD CAD0 A4B3 DE4A

```
class "class-chassis1-slot1-port8"
{
  match if option agent.circuit-id =
  59:49:00:c1:56:5f:11:db:a8:dd:ca:d0:a4:b3:de:4a
  and option agent.remote-id = 01:0:0:0:08; }

```

This configuration associates an IP address with the class declared above.

```
subnet 10.70.70.0 netmask 255.255.255.0 {
  pool
  {
    allow members of " class-chassis1-slot1-port8"; range 10.70.70.10; }
  }
}

```

In the following example, one new class is added to define server port INT8, then an IP address is associated with the new class:

```
*****CLASS*****
# in this class I have defined a switch in chassis with ID
# 59:49:00:c1:56:5f:11:db:a8:dd:ca:d0:a4:b3:de:4a
# placed in slot 1 and blade server is connected in port 8(INT8)

class "class-chassis1-slot1-port8"
{
match if option agent.circuit-id =
59:49:00:c1:56:5f:11:db:a8:dd:ca:d0:a4:b3:de:4a
and option agent.remote-id = 01:0:0:0:08; }

*****Range for that class*****
# for class-chassis1-slot1-port8 only one IP
# is defined (10.70.70.10)

subnet 10.70.70.0 netmask 255.255.255.0 {
pool
{
allow members of " class-chassis1-slot1-port8"; range 10.70.70.10; }
}
```

This example was performed with Internet Systems Consortium DHCP Server, version 3.0.4

## CHAPTER 4

# Command Reference

---

Your BOFM Extensions software provides a default configuration that is ready to perform basic switching functions. Some of the more advanced features, however, require administrative configuration before they can be used effectively.

You can use the BOFM Extensions BBI to perform most basic configuration tasks. However, the command line interface is the most direct method for collecting information and making configuration changes. Using a basic terminal, you are presented with a hierarchy of menus that enable you to view information and statistics about the switch, 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 switch in both the user and administrator command modes. This chapter discusses how to use the command line interface for the BOFM Extensions software.

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 switch.

[Information Menu]	
sys	- System Information Menu
l2	- Layer 2 Information Menu
l3	- Layer 3 Information Menu
link	- Show link status
port	- Show port information
transcvr	- Show Port Transceiver status
group	- Show group information
dump	- Dump all information

## ■ Statistics Menu

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

```
[Statistics Menu]
port      - Port Stats Menu
clrports  - Clear stats for all ports
l2        - Layer 2 Stats Menu
l3        - Layer 3 Stats Menu
mp        - MP-specific Stats Menu
ntp       - Show NTP stats
dump      - Dump all stats
```

## ■ Configuration Menu

The Configuration Menu (/cfg) allows an administrator to configure switch 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
global    - Global Menu
group     - Group Menu
pmirr     - Port Mirroring 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 switch is reset, the port returns to its normally configured operation.

```
[Operations Menu]
port      - Operational Port Menu
prm       - Protected Mode Menu
passwd    - Change current user password
clrlog    - Clear syslog messages
ntpreq    - Send NTP request
```

## ■ Boot Options Menu

The Boot Options menu (/boot) is used for upgrading switch software, selecting configuration blocks, and for resetting the switch 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 FTP/TFTP
  ptimg - Upload selected software image via FTP/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 switch is next reset
- ☐ Selecting a configuration block to be used when the switch is next reset
- ☐ Downloading or uploading a new software image to the switch 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    - Uencode 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 switch 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** and **diff flash** commands are global commands. Therefore, you can enter them 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
```

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.

---

**NOTE** – The **apply** command and the **diff flash** command are global commands. 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 switch.

---

**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 BOFM Extensions. Your options include:

- The active configuration block
- The backup configuration block
- Factory default configuration



## CHAPTER 5

# Configuring Switch Access

---

The BOFM Extensions software provides detailed commands for configuring system access and system management, and for viewing information and statistics. This chapter discusses switch access features, and how to secure the switch for remote administrators:

- “Management module setup” on page 50
- “Using Telnet” on page 54
- “Using the Browser-Based Interface” on page 55
- “Securing Access to the Switch” on page 57
  - “Setting Allowable Source IP Address Ranges” on page 57
  - “RADIUS Authentication and Authorization” on page 59
  - “TACACS+ Authentication” on page 61
  - “End User Access Control” on page 62
  - “Protected Mode” on page 65
  - “Secure Shell and Secure Copy” on page 67

## Management module setup

The switch module 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 switch 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 switch. The switch 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.

You can manage the switch through the management module, or through any of the internal or external ports. Use the following command to create an additional interface for accessing the switch:

```
/cfg/global/sif
```

This interface provides access to a management application (e.g., Telnet/HTTP) located on a blade server or on a host station connected to the switch through one of the external ports.

### Factory default vs. MM assigned IP addresses

Each switch 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 switch is installed (for additional information, see your *Installation Guide*). The management module assigns an IP address of 192.168.70.1xx, where xx corresponds to the number of the bay into which each switch is installed, as shown in the following table:

**Table 5-1** Switch 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** – Switch modules installed in Bay 1 and Bay 2 connect to server NICs 1 and 2, respectively. However, Windows operating systems using older I/O expansion adapters might show that switch modules installed in Bay 3 and Bay 4 connect to server NIC 4 and NIC 3, respectively.

---

## Configuring the 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 switch connections to other subnets of other TCP/IP networks.

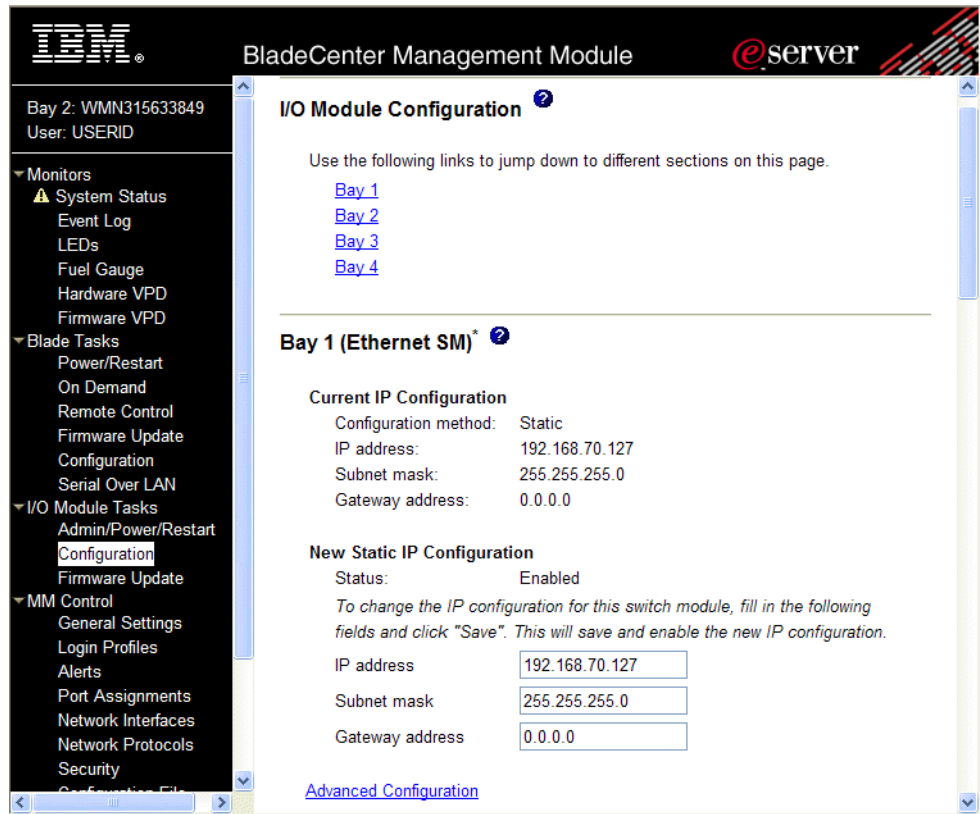
If you want to access the switch from outside your local network, use the management module to assign a default Gateway address to the switch. Choose **I/O Module Tasks > Configuration** from the navigation pane on the left, and enter the default Gateway IP address (for example, 192.168.70.125). Click **Save**.

## Configuring management module 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.



**Figure 5-1** Switch configuration on the BladeCenter management module

4. You can use the default IP addresses provided by the management module, or you can assign a new IP address to the switch 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

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

In **Advanced Configuration > Advanced Setup**, enable “Preserve new IP configuration on all switch resets,” to retain the switch’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 BOFM Extensions. For HTTPS access, you must enable HTTPS on the BOFM Extensions (`/cfg/sys/access/https/access e`). For more information about SSH access, refer to [“Secure Shell and Secure Copy” on page 67](#).

## Using Telnet

---

Telnet is used to access the switch'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 switch using Telnet or the Browser-Based Interface (web), try to ping the switch'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 switch (requires Java 1.4 Plug-in).

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

```
telnet 192.168.70.127
```

## Connect to the Switch 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 switch 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 67](#). For more information on the CLI, see [“Command Reference” on page 41](#).



## Using the Browser-Based Interface

---

Use the management module to access the switch through a Web session. Choose menu **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 BOFM Extensions interface on the switch.

The BOFM Extensions 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 switch via the BOFM Extensions BBI, open a Web browser window and type in the URL using the IP interface address of the switch. For example:

```
http:// 192.168.70.127
```

### 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 switch via the Browser-Based Interface, open a Web browser window and type in the URL using the IP interface address of the switch. For example:

```
https:// 192.168.70.127
```

You can save the certificate to flash for use if the BOFM Extensions 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 switch, the client is asked to accept the certificate and can verify that the fields are what the client expected.

## Securing Access to the Switch

---

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 57](#)
- Authentication and authorization of remote administrators: see [“RADIUS Authentication and Authorization” on page 59](#)
- Encryption of management information exchanged between the remote administrator and the BOFM Extensions: see [“Secure Shell and Secure Copy” on page 67](#)

The following sections are addressed in this section:

- [“Setting Allowable Source IP Address Ranges” on page 57](#)
- [“RADIUS Authentication and Authorization” on page 59](#)
- [“TACACS+ Authentication” on page 61](#)
- [“Secure Shell and Secure Copy” on page 67](#)

### Setting Allowable Source IP Address Ranges

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

When an IP packet reaches the switch, 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 switch 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 switch:

- A host with a source IP address of 192.192.192.21 falls within the defined range and would be allowed to access the switch.
- 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 switch supports the RADIUS (Remote Authentication Dial-in User Service) method to authenticate and authorize remote administrators for managing the BOFM Extensions software. This method is based on a client/server model. The Remote Access Server (RAS)—the switch—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.

### Configuring RADIUS

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

### Remote User Authorization

Radius

Radius	<input type="button" value="enable"/>	Port	<input type="text" value="1645"/>
Radius Primary Server	<input type="text" value="10.10.1.1"/>	- Radius Secret	<input type="text" value="*****"/>
Radius Secondary Server	<input type="text" value="10.10.1.2"/>	- Radius Secret	<input type="text" value="*****"/>

Tacacs+

Tacacs+	<input type="button" value="disable"/>	Port	<input type="text" value="49"/>
Tacacs+ Primary Server	<input type="text" value="0.0.0.0"/>	- Tacacs+ Secret	<input type="text"/>
Tacacs+ Secondary Server	<input type="text" value="0.0.0.0"/>	- Tacacs+ Secret	<input type="text"/>

**Figure 5-2** RADIUS configuration on the BOFM Extensions BBI

In the Radius section, enter the Primary Radius Server IP address and Radius secret. Select **enable**.

Click **Apply**.

## User Accounts

The user accounts listed in [Table 5-2](#) can be defined in the RADIUS server dictionary file.

**Table 5-2** User Access Levels

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

## RADIUS Attributes for Switch User Privileges

When the user logs in, the switch 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 switch 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 switch, 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 BOFM Extensions user privileges levels:

**Table 5-3** Switch-proprietary attributes for RADIUS

User Name/Access	User-Service-Type	Value
User	<i>Vendor-supplied</i>	255
Operator	<i>Vendor-supplied</i>	252
Admin	<i>Vendor-supplied</i>	250

# TACACS+ Authentication

The switch supports authentication and authorization with networks using the Cisco Systems TACACS+ protocol. The switch 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 switch either through a data or management port.

## 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 switch 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 switch management access levels is shown in [Table 5-4](#). The authorization levels must be defined on the TACACS+ server.

**Table 5-4** Switch-proprietary attributes for TACACS+

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

## Configuring TACACS+ Authentication

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

### Remote User Authorization

**Radius**

Radius	<input type="text" value="disable"/>	Port	<input type="text" value="1645"/>
Radius Primary Server	<input type="text" value="0.0.0.0"/>	- Radius Secret	<input type="text" value="*****"/>
Radius Secondary Server	<input type="text" value="0.0.0.0"/>	- Radius Secret	<input type="text" value="*****"/>

**Tacacs+**

Tacacs+	<input type="text" value="enable"/>	Port	<input type="text" value="49"/>
Tacacs+ Primary Server	<input type="text" value="10.10.1.1"/>	- Tacacs+ Secret	<input type="text"/>
Tacacs+ Secondary Server	<input type="text" value="10.10.1.2"/>	- Tacacs+ Secret	<input type="text"/>

**Figure 5-3** TACACS+ configuration on the BOFM Extensions BBI

In the Tacacs+ section, enter the Primary TACACS+ Server IP address and TACACS+ secret. Select **enable**.

Click **Apply**.

## End User Access Control

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



## Considerations for Configuring End User Accounts

- A maximum of 10 end-user IDs are supported on the switch.
- The switch does not automatically validate configurations.
- Switch software supports end user support for Telnet access to the switch. As a result, only very limited access is granted to the primary administrator under the BBI mode of access.
- If RADIUS authentication is used, the user password on the Radius server overrides the user password on the switch. Also note that the password change command only modifies the BOFM Extensions 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 switch.
- Passwords can be up to 15 characters in length for TACACS, RADIUS, Telnet, SSH, and Web access. Passwords for end-user accounts can be up to 128 characters.

## Configuring End-User Access Control

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

### Local User Administration

Built-in Users

Username	Password	User Type	Enabled
admin	*****	administrator ▼	enable ▼
oper		operator ▼	disable ▼
user	*****	user ▼	enable ▼

User Configuration

	Username	Password	User Type	Enabled
User1 :	dan	*****	user ▼	enable ▼
User2 :			user ▼	disable ▼
User3 :			user ▼	disable ▼
User4 :			user ▼	disable ▼
User5 :			user ▼	disable ▼
User6 :			user ▼	disable ▼
User7 :			user ▼	disable ▼
User8 :			user ▼	disable ▼
User9 :			user ▼	disable ▼
User10 :			user ▼	disable ▼

**Figure 5-4** Configuring end-user accounts on the BOFM Extensions BBI

Use the following procedure to configure an end-user account.

1. **In the User Configuration section, enter a Username and Password for the account.**
2. **Select the User Type.**  
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 5-2 on page 60](#).
3. **Select enable to allow the new user to access the switch.**
4. **Click Apply.**

## 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 Class of Service configured for the end-user account.

## Protected Mode

Protected Mode settings allow the switch administrator to block the management module from making configuration changes that affect switch operation. The switch retains control over those functions.

The following management module functions are disallowed when Protected Mode is turned **on**:

- External Ports: Enabled/Disabled
- External management over all ports: Enabled/Disabled
- Restore Factory Defaults
- New Static IP Configuration

In this release, configuration of all functions listed above are restricted to the local switch when you turn Protected Mode **on**. In future releases, individual control over each function may be added.

---

**NOTE** – Before you turn Protected Mode on, make sure that external management (e.g., Telnet) access to the switch's IP interface is enabled:

**System Settings > Global > Switch IP Interface**

---

To configure Protected Mode, enable the functions for which you wish to secure local control, and set Local protected mode to **on**.

**Switch Protected Mode Configuration**

Local control of external management	Disabled
Local control of external ports	Disabled
Local control of factory default reset	Disabled
Local control of Mgmt VLAN interface	Disabled
Local protected mode	On <input type="button" value="v"/>

**Figure 5-5** Configuring Protected Mode on the BOFM Extensions BBI

If you lose access to the switch through the external ports, use the console port to connect directly to the switch, and configure an IP interface for management access.

## 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 switch. Telnet does not provide this level of security. The Telnet method of managing a BOFM Extensions does not provide a secure connection.

**SSH** is a protocol that enables remote administrators to log securely into the switch 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 switch 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 switch
- Secure copy support

The switch 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
```

### *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 SCP Administrator password, first connect to the switch 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 `PASSWORD`.

```
>> /cfg/sys/sshd/scpadmin
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. For the examples below, the IP address of the BOFM Extensions is 205.178.15.100, the IP address of the management module is 205.178.15.157, and 1022 as the SSH port number.

*To log in to the switch:*

Syntax:

```
ssh -l <username> <switch IP address>
or
ssh -p <SSH port number> -l <username> <Advanced MM IP address>
```

Example:

```
>> # ssh -l scpadmin205.178.15.100
or
>> # ssh -p 1022 -l scpadmin@205.178.15.157
```

*To download the switch configuration using SCP:*

Syntax:

```

scp <username>@<switch IP address>:getcfg <local filename>
or
scp -p <SSH port number> <username>@<Advanced MM IP address>:getcfg <local filename>

```

Example:

```

>> # scp scpadmin@205.178.15.100:getcfg ad4.cfg
or
>> # scp -p 1022 scpadmin@205.178.15.157:getcfg ad4.cfg

```

*To upload the configuration to the switch:*

Syntax:

```

scp <local filename> <username>@<switch IP address>:putcfg
or
scp -p <SSH port number> <local filename> <username>@<Advanced MM IP address>:putcfg

```

Example:

```

>> # scp ad4.cfg scpadmin@205.178.15.100:putcfg
or
>> # scp -p 1022 ad4.cfg scpadmin@205.178.15.157:putcfg

```

**To apply and save the configuration**

The **apply** and **save** commands are still needed after the last command (**scp ad4.cfg scpadmin@205.178.15.100:putcfg**).

Or, instead, you can use the following commands:

```

>> # scp ad4.cfg scpadmin@205.178.15.157 1022:putcfg_apply
>> # scp ad4.cfg scpadmin@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 BOFM Extensions 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 switch. The server key is 768 bits and is used to make it impossible to decipher a captured session by breaking into the BOFM Extensions at a later time.

When the SSH server is first enabled and applied, the switch 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 switch through the management module (commands are not available via external Telnet connection), and enter the following commands to generate them manually.

---

>> # <code>/cfg/sys/sshd/hkeygen</code>	<i>(Generates the host key)</i>
>> # <code>/cfg/sys/sshd/skeygen</code>	<i>(Generates the server key)</i>

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

When the switch 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 switch automatically generates them during the system reboot. This process may take several minutes to complete.

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

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

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

---

**NOTE** – The BOFM Extensions 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 BOFM Extensions 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 switch, 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 switch, 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 switch 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 switch will recognize him as the SCP-only administrator. The switch allows only the administrator access to SCP commands.

---



# Index

---

## Symbols

[ ] ..... 7

## Numerics

802.1Q VLAN tagging ..... 27

## A

accessing the switch

    defining source IP addresses ..... 57

    RADIUS authentication ..... 59

    security ..... 57

    using the Browser-based Interface ..... 55

active configuration block ..... 22, 46

administrator account ..... 60

apply (global command) ..... 46

applying configuration changes ..... 46

## B

backup configuration block ..... 22, 46

broadcast domains ..... 27

## C

Cisco EtherChannel ..... 31

command conventions ..... 7

configuration

    apply changes ..... 46

    save changes ..... 46

    view changes ..... 46

configuration block

    active ..... 22

    backup ..... 22

    factory ..... 22

    selection ..... 22

configuration rules

    port mirroring ..... 31

    Trunking ..... 31

    VLANs ..... 31

## D

default password ..... 60

diff (global) command, viewing changes ..... 46

downloading software ..... 19

## E

EtherChannel ..... 29, 30

    as used with port trunking ..... 31

## F

factory configuration block ..... 22

Failover ..... 32

fault tolerance

    port trunking ..... 31

frame tagging. *See* VLANs tagging.

## I

IGMP Snooping ..... 34

image

    downloading ..... 19

    software, selecting ..... 21

IP subnets

    VLANs ..... 27

ISL Trunking ..... 30

## L

LACP ..... 31

Link Aggregation Control Protocol ..... 31

logical segment. *See* IP subnets.

**M**

Main Menu	
summary .....	42
management module.....	50
Management Processor (MP)	
use in switch security .....	57
manual style conventions .....	7
multi-links between switches	
using port trunking.....	29

**P**

password	
administrator account .....	60
default.....	60
user account.....	60
port mirroring	
configuration rules .....	31
port trunking .....	30
EtherChannel .....	29, 30
fault tolerance .....	31

**Q**

Quick Start .....	10
-------------------	----

**R**

RADIUS	
authentication.....	59
SSH/SCP.....	72
routers	
port trunking .....	30
RSA keys .....	71

**S**

save (global command) .....	46
noback option .....	46
save command .....	22

SecurID .....	72
security	
allowable SIP addresses .....	57
RADIUS authentication .....	59
switch management.....	57
VLANs.....	27
segmentation. <i>See</i> IP subnets.	
segments. <i>See</i> IP subnets.	
software	
image .....	19
spoofing, prevention of .....	57
SSH	
RSA host and server keys.....	71
SSH/SCP	
configuring .....	68
statistical load distribution .....	30
switch	
resetting .....	22
switch management	
security.....	57

**T**

TACACS+ .....	61
tagging. <i>See</i> VLANs tagging.	
text conventions .....	7
Trunking	
configuration rules .....	31
typographic conventions.....	7

**U**

user account .....	60
--------------------	----

**V**

VLANs	
broadcast domains.....	27
multiple VLANs .....	27
security.....	27