

SmartConnect™

# User's Guide

HP 1:10Gb Ethernet BL-c Switch for c-Class BladeSystem®

Version 41.1

---

Part Number: BMD00083, July 2009

**BLADE**  
NETWORK TECHNOLOGIES

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

Copyright © 2009 BLADE Network Technologies, Inc., 2350 Mission College Blvd., Suite 600, Santa Clara, California, 95054, USA. All rights reserved. Part Number: BMD00083.

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.

BLADE OS, BLADE, and ServerMobility are trademarks of BLADE Network Technologies, Inc. in the United States and certain other countries. Cisco<sup>®</sup> and EtherChannel<sup>®</sup> 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.

Originated in the USA.

# Contents

---

## **Preface 9**

- Who Should Use This *User's Guide* 9
- What You'll Find in This *User's Guide* 10
- Typographic Conventions 11
- How to Get Help 11

## **Part 1: Basic Concepts & Configuration 13**

---

### **Chapter 1: SmartConnect Software Operation 15**

- SmartConnect Software Overview 15
- SmartConnect Software Quick Start 17
  - Configuring the Chassis Management System 17
  - Configuring the Upstream Networking Device 17
  - Configuring the Chassis Processor Blades 17

### **Chapter 2: Getting Started with the Browser-Based Interface 19**

- Requirements 19
- Web Browser Set Up 19
- Starting the BBI 20
- Updating the Software Image 22
  - Loading the New Software Image 22
  - Transferring the New Image to the Switch 22
  - Selecting a Software Image to Run 24
  - Uploading a Software Image from the Switch 24
- Selecting a Configuration Block 25
- Resetting the Switch 26

### **Chapter 3: Switch Virtualization 27**

Virtual Switch Groups	28
Port Groups	28
Virtual Machine Groups	28
Link Aggregation	29
VLANs	30
Network Segmentation	30
Port Access	30
Port-Based VLAN Tagging	30
Defined VLANs	31
Trunking	32
External Trunks	32
Internal Trunks	37
IGMP Snooping	38
ServerMobility	39
Configuring a Backup Server Port	39
General Configuration	40
Port Configuration	41
DHCP Server Configuration	42

### **Chapter 4: Stacking 45**

Stacking Overview	45
Stacking Requirements	46
Stack Membership Roles	46
The Master Switch	47
Backup Switch Selection	48
Stack Member Numbers	50
Best Configuration Practices	50
Configuring Each Switch in a Stack	51
Additional Master Configuration	53
Master Configuration via the CLI	53
Master Configuration via the BBI	56
Managing a Stack	59
Upgrading Stack Software	62
Replacing a Switch in an Existing Stack	64

**Chapter 5: Command Reference 67**

CLI Menus 68

Viewing, Applying, and Saving Changes 71

Viewing Pending Changes 71

Applying Pending Changes 71

Saving the Configuration 72

**Chapter 6: Configuring Switch Access 73**

Using Telnet 74

Connect to the Switch via SSH 74

Using the Browser-Based Interface 75

Access via HTTP 75

Access via HTTPS 75

Securing Access to the Switch 77

Setting Allowable Source IP Address Ranges 78

RADIUS Authentication and Authorization 79

TACACS+ Authentication 81

End User Access Control 82

Secure Shell and Secure Copy 84

**Part 2: BBI Reference 93**

---

**Chapter 7: Understanding the Browser-Based Interface 95****Chapter 8: Virtual Switch Groups 101**

Virtual Switch Groups Membership 103

Virtual Switch Groups Settings 105

Virtual Switch Groups ACL QoS 107

**Chapter 9: Switch Policies 109**

Internal Port Settings 110

External Port Settings 111

Management Port Settings 112

Port Mirroring 113

Access Control Lists 114

ACL Configuration Table 114

Add or Edit ACLs 116

Access Control List Sets 119

- Quality of Service 120
  - IEEE 802.1p for MAC-Level QoS 120
  - DiffServ Code Point QoS 121
- ServerMobility 122
  - ServerMobility General Configuration 123
  - ServerMobility Port Configuration 124

## **Chapter 10: System Settings 125**

- Management Settings 126
- General Settings 127
- Local User Administration 128
- Remote User Administration 130
- Time Services Settings 132
- ErrDisable System Settings 133
- Management Network Settings 133
- Bootstrap Protocol Settings 134
- SSH/Telnet Settings 135
- Virtual Machine Group Settings 136
- Syslog Settings 137
- Stacking Configuration 138
  - Stack Switch Configuration 138
  - Stack IP Interfaces 139

## **Chapter 11: Boot Management 141**

- General Boot Settings 142
- Boot Schedule 144

## **Chapter 12: Switch Information 145**

- Access Control List Information 146
- Access Control List Sets Information 146
- ARP Cache Information 147
- Bootstrap Protocol Relay Information 148
- Forwarding Database Information 148
- Virtual Switch Group Information 150
- IGMP Information 151
- IP Information 152
- Link Status Information 153

ServerMobility	154
ServerMobility General Information	154
ServerMobility Port Information	155
SNMPv3 Information	156
Syslog Messages	158
Port Transceiver Status	159
Trunk Groups Information	159
User Information	160
Virtual Machine Group Information	160
<b>Chapter 13: Switch Statistics</b>	<b>161</b>
Access Control List Statistics	161
FDB Statistics	162
Layer 3 Statistics	162
IGMP Group Snooping Statistics Summary	166
IP Statistics	167
MP-Specific Information	168
CPU Utilization	169
MP Packet Statistics	169
Network Time Protocol Statistics	170
Port Statistics	170



# Preface

---

BLADE Network Technologies' SmartConnect software is a simplified software image that can be run on the HP 1:10Gb Ethernet BL-c Switch for c-Class BladeSystem. SmartConnect software provides an easy-to-use graphical user interface (GUI) and a reduced function set to minimize networking mis-configuration.

This *User's Guide* describes how to configure and use the SmartConnect software. Refer to the blade server chassis *Installation Guide* for details about how to install the switch module hardware.

---

**Note** – When the term *switch* is used in this document, it specifically refers to the HP 1:10Gb Ethernet BL-c Switch for c-Class BladeSystem that is running SmartConnect software.

---

## Who Should Use This *User's Guide*

---

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

## What You'll Find in This *User's Guide*

---

This *User's Guide* will help the administrator plan, implement, and administer the SmartConnect software. Where possible, each section provides feature overviews, usage examples, and configuration instructions.

### *Part 1: Basic Concepts and Configuration*

Part 1 of this *User's Guide* contains fundamental information necessary to use the SmartConnect software. Chapters are arranged in the best order for making quickest use of the SmartConnect software.

[Chapter 1, “SmartConnect Software Operation,”](#) provides a general theory of operation for the SmartConnect software.

[Chapter 2, “Getting Started with the Browser-Based Interface,”](#) provides an overview of the browser-based interface (BBI), the primary tool used to view and configure the SmartConnect software.

The remaining chapters in this part describe key SmartConnect software features, providing detail for their use and configuration. Features covered include switch virtualization for port groups, VLANs, trunking, failover, and stacking, the command-line interface, and methods for remote administration.

See [“Basic Concepts & Configuration” on page 13](#) for the complete description of the chapters in this part of the *User's Guide*.

### *Part 2: BBI Reference*

Part 2 of this *User's Guide* contains information about the settings and controls on each page of the browser-based interface (BBI) used for configuring and monitoring the switch.

[Chapter 7, “Understanding the Browser-Based Interface,”](#) starts Part 2 of this *User's Guide* and provides information about the BBI screen layout, menu system, and basic operation.

The remaining chapters are arranged in hierarchical order, as they appear in the BBI menu bar.

See [“BBI Reference” on page 93](#) for the complete description of the sections in this part of the *User's Guide*.

# 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> <IP address>  Read the <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]
AaBbCc123	This block type depicts menus, buttons, and other controls that appear in Web browsers and other graphical interfaces.	Click the <b>Save</b> button.

## How to Get Help

If help, service, or technical assistance is needed, see the blade server chassis software *Installation Guide* for the appropriate contact information.



# Part 1: Basic Concepts & Configuration

The chapters in this part of the *User's Guide* cover the following information:

- [Chapter 1, “SmartConnect Software Operation,”](#) provides a general theory of operation for the SmartConnect software.
- [Chapter 2, “Getting Started with the Browser-Based Interface,”](#) provides an overview of the browser-based interface (BBI) that enables the administrator to view and configure settings on the switch.
- [Chapter 3, “Switch Virtualization,”](#) describes how to use virtualization features to combine multiple ports to aggregate bandwidth between large-scale network devices, or segregate ports or virtual machines to form smaller, independent switch entities.
- [Chapter 4, “Stacking,”](#) describes how to configure the switch for stacking, which allows multiple switches to work together as a single unit.
- [Chapter 5, “Command Reference,”](#) provides an overview of menu commands that enable the administrator to view information and statistics about the switch, and to perform any necessary configuration.
- [Chapter 6, “Configuring Switch Access,”](#) describes different methods to access and manage the switch, including remote administration using the management system, RADIUS authentication, Secure Shell (SSH), and Secure Copy (SCP).



## CHAPTER 1

# SmartConnect Software Operation

---

## SmartConnect Software Overview

---

The BLADE Network Technologies' SmartConnect software provides a simple Ethernet interface option for connecting a blade server chassis 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 SmartConnect software are restricted to reduce the initial setup complexity and to minimize the impact on upstream networking devices.

The SmartConnect software requires basic administration tasks similar to those required to connect a single multi-linked server to the network. Connecting the blade server chassis with up to sixteen (16) server blades becomes as easy as connecting a single server to the network.

The default network configuration of the SmartConnect software consists of a single Virtual Switch Group (VSG). As the switch is configured, additional VSGs may be created, and switch resources (internal ports, external ports, and virtual machines) may be reassigned to take advantage of various switch virtualization features.

By default, all of the external uplink ports in each VSG are aggregated together into a static Link Aggregation Group (LAG, or trunk), which is fully compatible with Cisco EtherChannel technology. This configuration eliminates the need for Spanning Tree Protocol to prevent network loops among the individual links, since the uplink ports act as a single link.

The SmartConnect software provides improved network reliability. By default, uplink ports participate in a static trunk so that if an individual link fails, the existing traffic is redirected to the remaining links. In addition to default static trunks, VSGs may be configured to use dynamic Link Aggregation Control Protocol (LACP) for their trunks.

The SmartConnect software permits the uplink ports to auto-negotiate the flow-control settings of each link (the default setting). Port characteristics can also be configured to specified values. All of the trunked uplink ports in each VSG must be configured to the same port characteristics in order to participate (form an active link) in the trunk.

---

**Note** – In the default switch configuration in which all external ports (even those of different physical types) belong to one trunk, some external ports may be automatically disabled by the switch to satisfy general trunking restrictions. See [“Trunking Rules” on page 33](#) for details.

---

With Network Adaptor Teaming configured on the server blade Ethernet NICs, the servers can maintain redundant links to multiple switches within the blade chassis to provide enhanced reliability. The L2 Failover option allows the SmartConnect 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 blade server chassis.

Most administrators will find the Browser-based Interface (BBI) adequate for configuring and using the SmartConnect software. However, a command-line interface (CLI) is available for users familiar with the CLI, or who want to use scripting facilities. Other interface products, such as the Blade Harmony Manager, may also be used for managing some or all switch functions.

# SmartConnect Software Quick Start

---

When SmartConnect software is loaded, the default configuration allows the switch to function correctly with no configuration changes. The administrator must make some configuration changes to the upstream network device and the blades in the blade chassis, as described in the following sections.

## Configuring the Chassis Management System

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

- Plug the Ethernet cable into the management system and verify the link.
- Verify access to the management system.
- Verify that the external ports are enabled.

## 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 Chassis 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 server blades can be configured to support Network Adaptor Teaming Failover. For details, refer to the appropriate documentation for the operating system.



## CHAPTER 2

# Getting Started with the Browser-Based Interface

---

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 the administrator to perform basic configuration tasks quickly and easily. The command line interface provides more detailed configuration options for SmartConnect software (see [“Command Reference” on page 67](#)).

## Requirements

---

- HP 1:10Gb Ethernet BL-c Switch for c-Class BladeSystem
- Installed SmartConnect software
- PC or workstation with HTTP access to the switch’s management IP interface as configured using the management system
- Frame-capable Web browser, 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 the Web browser

## Web Browser Set Up

---

Most modern Web browsers work with frames and JavaScript by default, and require no additional set up. However, check the 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 the Web browser.

---

## Starting the BBI

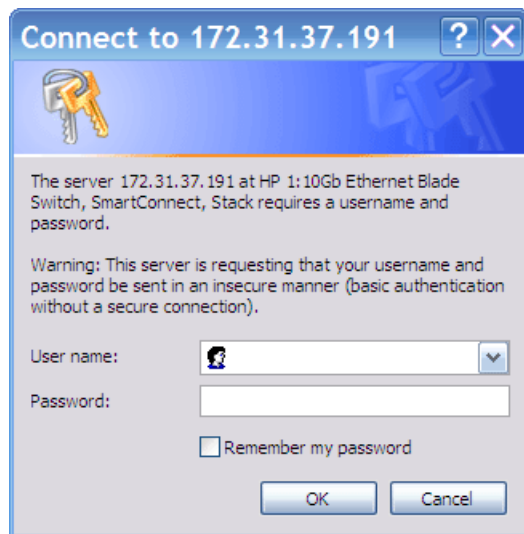
---

When the SmartConnect software and browser set up is done, follow these steps to launch the SmartConnect software BBI:

1. **Start the Web browser.**
2. **In the browser URL address window, specify the IP address of the target switch.**  
If the switch is configured correctly for BBI access, the login prompt will appear.
3. **Log in to the switch.**

If the switch and browser are properly configured, the password prompt will appear:

**Figure 2-A** SmartConnect Login Prompt



---

**Note** – The sample screens that appear in this *User's Guide* might differ slightly from the screens displayed in any given system. Screen content varies based on the type of blade server chassis being used, the firmware versions and options that are installed, and the specific hardware and software of the system used for accessing the switch.

---

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 main BBI page is being initialized. Do not stop the browser while loading is in progress.

---

Once the administrator is properly logged in, the SmartConnect software BBI appears in the Web browser's viewing window:

**Figure 2-B** BBI Startup Screen

The screenshot shows the BBI interface for 'Bay 1'. At the top right, the 'Port Status' section displays a grid of 25 port icons, with ports 17-25 highlighted in green. Below this is the 'Virtual Switch Groups Membership' configuration window. It contains three main sections: 'External Port' (ports 17-25), 'Management Port' (port 18), and 'Server Port' (ports 1-16). Each port has a dropdown menu for 'Group' and 'Trunk'. The 'VM Preprovisioning' section includes a table with columns for 'VM Mac Address', 'Group', and 'Delete'. The 'Management Port' section has a dropdown menu for 'Management Group'. At the bottom of the configuration window are 'Apply', 'Save', and 'RevertApply' buttons. A left sidebar contains a 'Menus' section with a list of navigation options: 'Virtual Switch Groups', 'Policies', 'System Settings', 'Boot Management', 'Information', and 'Statistics'. Callouts with blue lines point to the 'Port Status' area, the 'Menus' sidebar, and the 'Configuration Window'.

There are three main regions on the BBI 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 view and configure switch features.

See “BBI Reference” on page 93 for general details on using the BBI.

## Updating the Software Image

---

The software image is the executable code running on the switch. Upgrading the software image on the switch typically involves the following actions:

- Load a new software image onto a FTP or TFTP server on the network, or onto a local computer.
- Transfer the newly loaded software image to the switch.
- Select the new software image to be run when the switch is next reset.
- Reset the switch.

### Loading the New Software Image

Use the BBI to determine which version of software is currently installed on the switch. On the BBI menu, choose **System Settings > Boot Management > General**. The resulting window displays the current software information.

If the switch requires a software update, the latest version of the SmartConnect software is available from the support website. Download the switch image and place it on a FTP or TFTP server, or on a local computer.

### Transferring the New Image to the Switch

The switch can store up to two different software images, called *image1* and *image2*, as well as boot software, called *boot*. When loading new software, the administrator must specify where it should be placed: either into *image1*, *image2*, or *boot*.

For example, if the active image is currently loaded into *image1*, best practice is to load the new software into *image2*. This allows the administrator to 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.

---

The BBI may be used for loading 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. On the BBI, choose menu **System Settings > Boot Management > General**.

The *Boot Management* window appears.

**Figure 2-C** Boot Management Window (shown with Stacking enabled)

The screenshot shows the 'Boot Management' window with the following elements:

- Reboot the Module:** Three buttons labeled 'Reboot Stack', 'Reboot Master', and 'Reboot Switches'.
- Next boot config block:** A dropdown menu currently set to 'active config'.
- Image to boot:** A dropdown menu set to 'Image 1'.
- Image to transfer:** A dropdown menu set to 'Image 1'.
- Current Image Information:** A text area listing:
  - Image 1 - version 41.1.0.106, downloaded 14:46:53 Sat Apr 21, 2000 SmartConnect
  - Image 2 - version 41.1.0.106, downloaded 6:11:13 Sun Apr 22, 2000 SmartConnect
  - Boot kernel - version 1.0.0
- Update Image/Cfg:** A section containing:
  - Method to use for transfer:** A dropdown menu set to 'TFTP'.
  - Settings for using FTP or TFTP Server:** Two input fields for 'Server Address' and 'Remote File Name'.
  - Buttons:** 'Get Image', 'Put Image', 'Get Cfg', 'Put Cfg', 'Put TS Dump', 'Put Crash Dump', 'Clear Crash Dump', 'Apply', 'Save', and 'Revert apply'.
- Switches:** A small box in the top right corner labeled 'Switch 1' and 'Switch 2'.

2. Use the **Image to transfer** drop-down list to select the desired image.
3. In the **Update Image/Cfg** section, use the **Method to use for transfer** drop-down list to specify the desired method (such as TFTP, FTP, or HTTP).
4. **Get the image from the appropriate source:**
  - If transferring software from a TFTP server, enter the Server IP Address, and the Remote File Name. Then click **Get Image**.
  - If transferring software from a FTP server, enter the Server IP Address, and the Remote File Name. Also enter the FTP Username and FTP Password. Then click **Get Image**.
  - If transferring software from a local computer (HTTP), click **Browse**. In the File Upload dialog, select the desired file and click **OK**. Then click **Get Image**.

Once the image is transferred, 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*) desired to run after the next reboot.

1. **On the BBI, choose menu **System Settings > Boot Management > General**.**
2. **In the **Boot Management** page, use the **Image to boot** drop-down list to select the desired image.**

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

- SmartConnect software image
- HP 1:10Gb Ethernet BL-c Switch for c-Class BladeSystem image

This procedure can be used to change from one image type to the other. However, the configuration block for one image type is not compatible with the other type.

3. **If necessary, select an option from the **Next boot config block** drop-down list.**

If the software image type is changed, a compatible configuration block must be loaded or the configuration must be reset to factory defaults. It is recommended that both the active and backup configurations remain compatible with the active image type. For example, if a SmartConnect software configuration file is in the *active config*, do not store a normal configuration file in the *backup config*.

---

**Note** – When resetting the switch to its factory default configuration, the switch will retain its stacking settings. To reconfigure or disable stacking, see [“Stacking” on page 45](#).

---

4. **Click **Apply** to submit the image and configuration changes to the switch.**  
The changes will remain pending until the switch is next reset.
5. **Click **Reboot the Module** to activate the new image file and configuration block.**

## Uploading a Software Image from the Switch

Software images can also be uploaded from the switch to a FTP or TFTP server. The same software can then be transferred to other compatible switches.

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

1. **On the BBI, choose menu **System Settings > Boot Management > General**.**  
In the Boot Management window, page appears.
2. **Use the **Image to transfer** drop-down list to select the desired image.**

3. In the **Update Image/Cfg** section, use the **Method to use for transfer** drop-down list to specify the desired method.
4. **Get the image from the appropriate source:**
  - If loading a software image to a TFTP server, enter the Server IP Address, and the Remote File Name. Then click **Put Image**.
  - If loading a software image to a FTP server, enter the Server IP Address, and the Remote File Name. Also enter the FTP Username and FTP Password. Then click **Put Image**.
  - If loading a software image to a local computer (HTTP), click **Browse**. In the File Upload dialog, select the desired file and click **OK**. Then click **Put Image**.

## Selecting a Configuration Block

---

When configuration changes are made to the switch, the administrator must save the changes so that they are retained beyond the next time the switch is reset. When the **save** command is issued, the 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 Smart-Connect 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 the switch will load the next time it is reset:

1. On the BBI, choose menu **System Settings > Boot Management > General**.
2. In the **Boot Management** window, select an option in the **Next boot config block** (*active*, *backup*, or *factory*).

---

**Note** – When resetting the switch to its factory default configuration, the switch will retain its stacking settings. To reconfigure or disable stacking, see [“Stacking” on page 45](#).

---

3. **Click Apply to submit the configuration block changes to the switch.**

The changes will remain pending until the switch is next reset.
4. **Click Reboot the Module to activate the new configuration block.**

## Resetting the Switch

---

The switch must be reset to make the software image file and configuration block changes active. To reset the switch module:

1. **On the BBI, choose menu System Settings > Boot Management > General.**

The Boot Management page appears.

2. **Click Reboot the Module.**

## CHAPTER 3

# Switch Virtualization

---

The following virtualization features are included in the SmartConnect software:

- VMready

The switch's VMready software makes it *virtualization aware*. The switch automatically discovers the Virtual Machines (VMs) of hypervisors connected to internal ports on the switch. The SmartConnect software accepts up to 1024 VMs.

- Virtual aggregation

Switch resources can be pooled together, combining their capacity while at the same time simplifying their management. This can be accomplished on a number of levels:

- *Grouping* multiple internal and external switch ports into a single, logical switching entity with shared bandwidth capacity. Up to 32 such Virtual Switch Groups (VSGs) can be configured on the switch or stack.
- *Trunking* multiple switch ports into a single, high-bandwidth link to other networking devices. Each VSG supports up to two external trunks which can be used independently, or as a primary and backup.
- *Stacking* multiple switches from the same or different chassis into a single super-switch. SmartConnect software supports one stack with up to eight switches. Stacking also permits the use of up to 56 internal port trunks.

- Virtual segmentation

VSGs act as independent logical units. Traffic assigned to different VSGs is thoroughly separated within the switch, essentially dividing the switch into smaller switch entities.

VSG segmentation occurs internally within the switch, requiring no support changes to the broader network configuration (such as VLANs). Internal and external switch ports, as well as any attached VMs, can be independently assigned to VSGs.

- ServerMobility™

The ServerMobility feature allows server IP addresses to be assigned based on their physical location in a blade server chassis. Then, if a server fails, a replacement server (in the same or different slot) can assume the identity (and configuration) of the failed unit.

By combining virtualization features, SmartConnect software provides a highly-flexible framework for allocating and managing switch resources.

## Virtual Switch Groups

---

Switch resources can be assigned to VSGs. Up to 32 VSGs are available. Each VSG behaves independently, which allows for segmenting the switch into smaller logical entities. Within each VSG, member ports can be aggregated into trunks, combining their bandwidth.

Two different types of resources can be assigned to VSGs:

- Ports (internal and external)
- VMs

### Port Groups

Each internal and external port can be independently assigned to one of the 32 available VSGs. Each VSG can contain multiple ports, but each port can belong to only one VSG.

VSGs for port groups must have the following characteristics:

- It is recommended that each VSG contain internal server ports *and* external ports for proper network operation.
- By default, all external ports in the same VSG are placed into one trunk to aggregate their bandwidth. For more information, see [“Trunking” on page 32](#).

For VSG port group and trunk configuration, see [“Assigning Ports to VSGs” on page 103](#).

### Virtual Machine Groups

The switch automatically discovers VMs that reside in the hypervisor directly connected to the switch. As with ports, VMs can be independently assigned to VSGs in order to group or separate them. Optionally, uplink ports can also be assigned to VSGs that include VMs.

The switch will accept a maximum of 1024 VMs. Once this limit is reached, the switch will reject additional VMs.

---

**Note** – In some rare situations, the switch may reject the addition of new VMs prior to reaching the 1024 VM limit. This can occur when the hash bucket corresponding to the new VM is already full. If this occurs, change the virtual machine's MAC address and retry the operation. The MAC address can usually be changed from the virtualization platform's management console (such as the VMware Virtual Center). This limitation is independent of whether switches are acting alone or as part of a stack.

---

VSGs containing VMs have the following characteristics:

- The VSG may consist of VMs and (optionally) external ports.
- Internal ports cannot be added to VSGs which contain VMs, and VMs cannot be added to VSGs which contain internal ports.
- The switch allows communication between VMs in the same group.
- The switch does not allow communication between VMs which are not in the same group. However, VMs which are in the same hypervisor may still communicate with each other even if they are not assigned to the same VSG on the switch.

For information on configuration, see [“Assigning Virtual Machines to VSGs” on page 103](#).

## Link Aggregation

The default network configuration of the SmartConnect software places all ports into a single VSG, and aggregates all external ports together into a static Link Aggregation Group (LAG), also known as a *trunk* (see [“Trunking” on page 32](#)).

This configuration eliminates the need for Spanning Tree Protocol to prevent network loops, since the uplink ports act as a single link. Also, since all of the uplink ports in each VSG participate in a static LAG, if a link fails, the existing traffic is redirected to the other links.

To override default VSG assignments and trunk settings, see [“Assigning Ports to VSGs” on page 103](#)).

# VLANs

---

## Network Segmentation

Virtual Local Area Networks (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.

Switches with SmartConnect software are VLAN-transparent. This allows traffic from all VLANs to be supported on all SmartConnect VSGs without the need to configure VLANs on the switch or to configure VSGs on the broader network, greatly simplifying network management.

Network segmentation within the SmartConnect switch is provided using VSGs. Each VSG acts as an independent Layer 2 switch. By default, VSGs treat all VLAN traffic as regular, untagged traffic, and do not use VLAN information for making decisions on whether to forward, drop, or segment traffic. However, VLAN tags are preserved by default, allowing VLANs to be enforced as configured throughout the network.

Though VSG numbers do not technically correlate to specific VLAN IDs, if VSGs are used as a way to emulate VLANs in the switch, for ease of management, the administrator can set the name of the VSG to reflect the equivalent VLAN identity.

## Port Access

VLAN security policies can be enforced for ports within VSGs by using Access Control Lists (ACLs). Port ACLs can be configured to consider a packet's VLAN ID for making decisions on whether to permit or deny packet ingress.

ACLs can be configured in the BBI through the Switch Policy menus (see [“Access Control Lists” on page 114](#) and [“Access Control List Sets” on page 119](#)), and applied to ports through the Virtual Switch Groups menu (see [“Virtual Switch Groups ACL QoS” on page 107](#)).

## Port-Based VLAN Tagging

Each internal and external port can be independently configured with a Port VLAN ID (PVID) for VLAN tagging purposes. Under specific circumstances, the configured VLAN ID will be added to or stripped from traffic passing through the switch.

- Upon the ingress of untagged packets:
  - If the PVID on the port is 0 (the default), the packets will remain untagged.
  - If the PVID on the port is set to any value other than 0, the switch will tag the packets, placing the port's VLAN identifier into the frame headers. One application of this feature is to set a VLAN for traffic outbound from servers that do not perform their own VLAN tagging.
- Upon the ingress of tagged packets:
 

Packets which are already tagged for specific VLANs prior to reaching the switch are unchanged (retain their original tag), regardless of the PVID setting on the ingress port.
- Upon the egress of untagged packets:
 

After ingress processing, if the packet is still untagged, it will remain untagged when egressing the port, regardless of the PVID setting on the egress port.
- Upon the egress of tagged packets (whether tagged prior to ingress, or as a result of ingress processing):
  - If the PVID on the egress port is different than that of packet's tag, the packet will remain unchanged upon egress, retaining it's current tag.
  - If the PVID on the egress port matches the packet's tag, the VLAN tag will be stripped from the packet header. One application of this feature is to remove tags on traffic bound for servers that are not configured to support multiple VLANs.

PVIDs can be configured in the BBI through the *Switch Policy* menus (see [“Internal Port Settings” on page 110](#) and [“External Port Settings” on page 111](#)).

## Defined VLANs

The SmartConnect software uses the following VLANs:

- The default VLAN is an untagged VLAN used for data traffic, and contains all external ports and internal server-blade ports.
- Individual VLANs can be specified for switch IP Interfaces and stack interface.
- If the stacking feature is enabled, VLAN 4090 is reserved for segmenting inter-switch stacking traffic. Though the default stacking VLAN can be changed, it is strongly recommended that the default VLAN 4090 be used and reserved solely for stacking.
- 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.

## Trunking

Trunks provide super-bandwidth, multi-link connections between switch modules or other trunk-capable devices. A trunk is a group of ports that act together, combining their bandwidth to create a single, larger virtual link.

In the SmartConnect software, trunks function as static Link Aggregation Groups (LAGs) that are compatible with Cisco's EtherChannel technology.

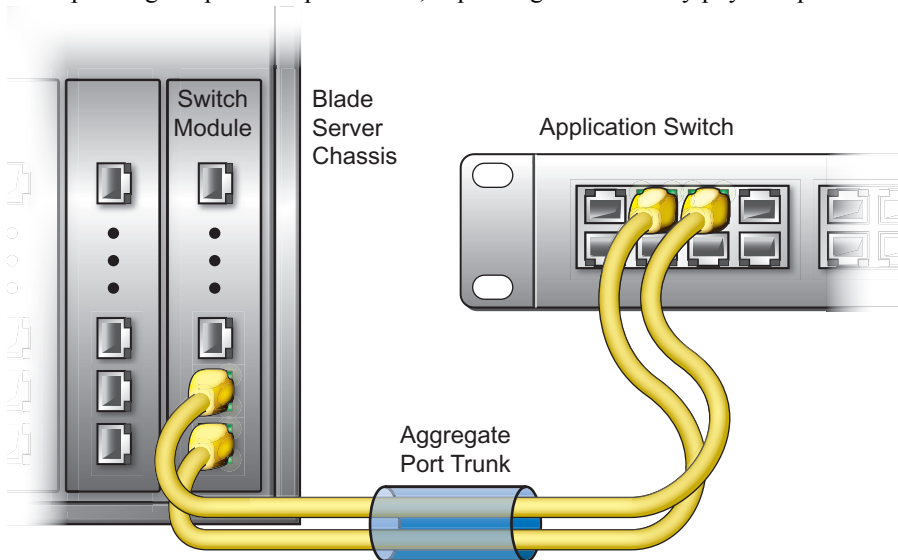
SmartConnect software supports the following trunk types:

- Up to 64 external trunks (2 independent trunks for each of 32 VSGs)
- Up to 56 internal trunks are available when multiple switches are placed in a stacked configuration (see [“Stacking” on page 45](#)).

For additional limits, see [“Trunking Rules” on page 33](#).

### External Trunks

When using a VSG with multiple external ports, a trunk can be created between the switch module and another switch. A simple example is shown in [Figure 3-A](#). This provides a virtual link operating at up to 30G per second, depending on how many physical ports are combined.



**Figure 3-A** Trunking External Ports

The trunk 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 trunking technology is compatible with these devices when they are configured manually.

Each VSG can have up to two external port trunks. Each of these trunks may consist of as many external ports as are available in the VSG. By default, the external ports for each VSG are placed into one of the VSG's available trunks. If all the switch ports belong to the same VSG (as with the factory default configuration), all external ports will be placed into the same trunk, though it is possible that not all links will be active (see [“Trunking Rules” on page 33](#)).

---

**Note** – Because all external ports in a VSG belong to the same trunk by default, external ports should not be used as regular IEEE 802.3 network links. Do not plug a workstation directly into one of the switch's active external ports unless it is the only device attached to these ports, or unless the port has been explicitly assigned to a VSG or trunk with no other active external ports.

---

To reconfigure the trunk assignment for each external port, see [“Virtual Switch Groups Membership” on page 103](#).

## Trunking Rules

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

- Trunking to third-party devices must comply with Cisco<sup>®</sup> EtherChannel<sup>®</sup> technology.
- For any specific trunk, only one physical port type can be active at any given time. If ports of different types (such as 1G ports and 10G ports) are mixed in a trunk (as occurs in the default configuration), the switch uses the Best Link algorithm to select the best port type for trunk operation. The lower-speed trunk ports will be automatically disabled while the higher-speed ports are in operation.
- For any specific trunk, although any number of ports can be assigned to the trunk, a maximum of eight ports may have an active link at any given time. If more than eight ports are included in a trunk, the switch will automatically disable links on the extra trunk ports while eight ports are in operation.
- Each trunk may consist of internal ports only, or external ports only. Internal and external ports cannot be mixed in the same trunk.
- Each external trunk must consist of member ports belonging to only one VSG. External ports for different VSGs cannot be trunked together.

- Each external trunk must originate from one logical device (one switch or different switches in the same stack), and lead to one logical destination device (such as a switch, stack, or other network device).
- Internal trunks require that stacking is enabled.
- Internal trunks may have member ports belonging to one VSG or multiple VSGs.
- Each internal trunk may group internal ports from the same switch or multiple switches in a stack, and may lead to one or more network devices.
- Internal trunks do not support VMs that are assigned to VSGs. Trunking ports that include VSG-assigned VMs, or assigning VSGs to VMs on ports that are already part of an internal trunk, may cause unexpected behavior.

These rules apply to any switch when operating independently, or to the set as a whole when multiple switches are placed in a stacked configuration.

## Statistical Load Distribution

Network traffic is statistically distributed between external ports in a trunk. 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 for data transmission. If there are enough devices feeding the trunked lines, then traffic distribution becomes relatively even.

## Built-In Fault Tolerance

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

Statistical load distribution is maintained when a port in a trunk is lost or returned to service.

## 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). If a link in a LACP trunk group fails, traffic is reassigned dynamically to the remaining link or links of the dynamic trunk.

To configure LACP for a VSG, choose **Virtual Switch Groups > Settings** in the BBI. The Link Aggregation Control Protocol field can be used to enable or disable LACP. When enabled, external ports in the VSG participate in LACP. When disabled (as by default), external ports in the VSG's external trunk act as a static trunk.

## 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. For details, refer to “Configuring Teaming” in the *Broadcom NetXtreme™ Gigabit Ethernet Adapter User Guide*.

Switch failover is disabled by default, but can be enabled for any VSG. When enabled, switch failover works as follows:

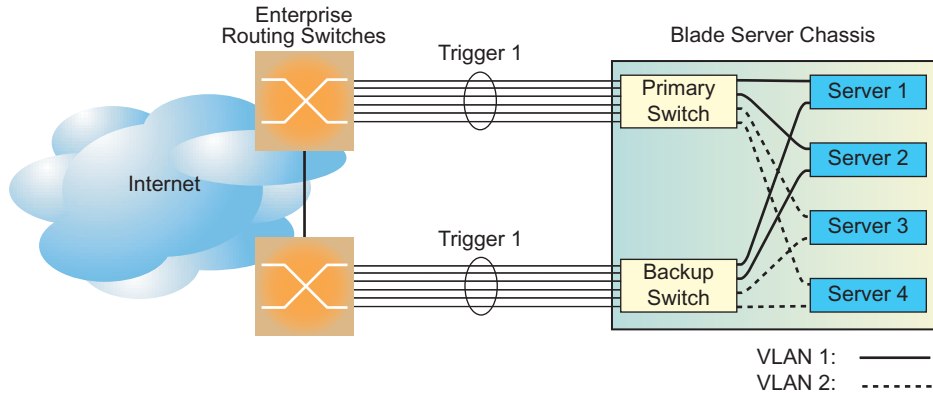
- If some (or all) of the links fail in the failover trigger, the switch disables all internal ports in the VSG. This causes the NIC team on the affected server blades to failover from the primary to the backup NIC. This process is called a failover event.
- When the appropriate number of links return to service, the switch enables the internal ports in the VSG. 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 VSG 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. If the trigger number is set to zero (0), the switch triggers a failover event only when no links in the VSG are operational.

## Configuring Switch Failover

Figure 3-B 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 VSG 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-B** Basic Switch Failover

On the BBI, choose **Virtual Switch Groups > Settings** to enable Switch Failover and to configure the Number of Links to Trigger Failover.

## Preventing Loops

In cases where both external trunks of a VSG lead either to a single device or to two devices in the same Spanning Tree Protocol (STP) domain (such as for redundancy applications), a potential network loop exists.

STP devices use Bridge Data Protocol Unit (BPDU) packets to exchange information required for selecting or blocking specific network paths. To prevent loops, SmartConnect software supports a variety of BPDU options. By default, BPDU Flooding is enabled for all SmartConnect VSGs. As such, BPDUs received on a particular VSG port are flooded to all member ports in the VSG. By distributing BPDU information to upstream devices with STP enabled, those devices can block the appropriate SmartConnect switch link and prevent a loop with no further configuration on the SmartConnect switch.

If upstream devices are not able to block one of the VSG's trunked links, BPDU Guard can be enabled on the VSG. When enabled, if BPDUs are received on the port in the VSG, BPDU Guard disables that port. Alternately, the switch can be configured to drop all BPDU packets.

To configure the BPDU policy, see [“BPDU Policy” on page 106](#).

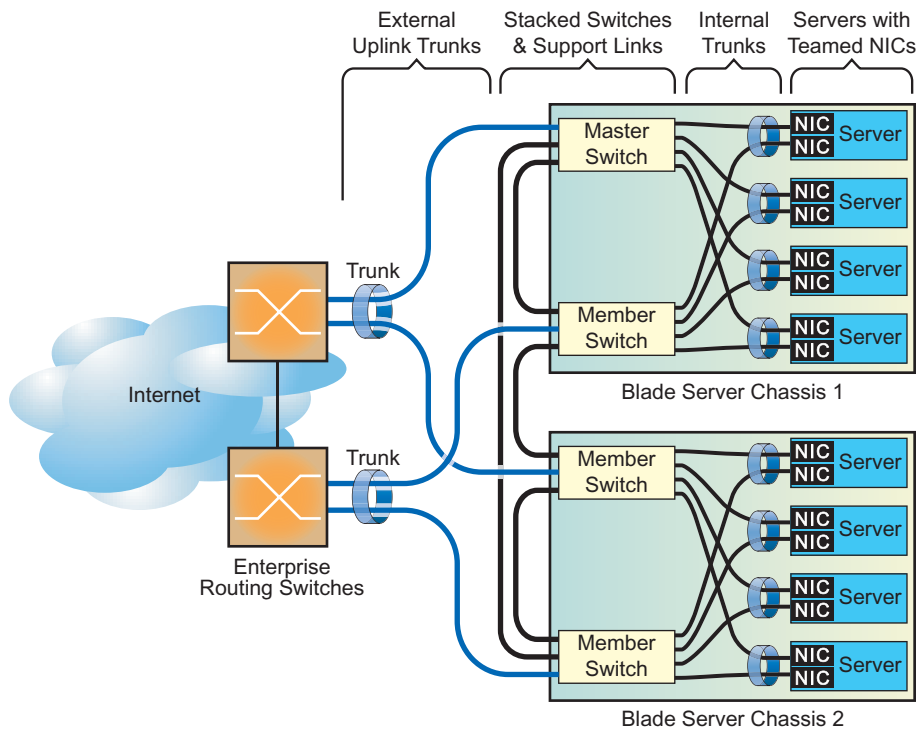
## Internal Trunks

Internal trunks allow for more granular high-availability options for the links between the servers and switches within a blade server chassis. Internal trunks have the following requirements:

- One or more blade servers in the blade chassis must be installed with multiple NICs and be configured for NIC Teaming. The actual number of supported NICs depends on the specific server and chassis model, and the capabilities of the NIC Teaming software.
- Multiple SmartConnect switches in the same blade chassis as the servers must be linked together as part of a stacked configuration (see [“Stacking” on page 45](#)). The number of SmartConnect switches installed in the chassis (and their slot locations) must coincide with the slots targeted by the blade servers' NICs.

For additional restrictions, see [“Trunking Rules” on page 33](#).

[Figure 3-C](#) shows a high-availability network combining external and internal trunks in a stacked switch configuration.



**Figure 3-C** Trunking Internal Ports

In [Figure 3-C](#), the two external trunks provide aggregation to the exterior network, and also high-availability in case any single uplink cable, external port, switch module, or blade chassis fails. On the service side of the network, each server includes two NICs which are automatically connected to each of the switch modules within its blade chassis. Both internal switch ports leading to each specific server are trunked together, despite belonging to different switches in the stack. Each server is configured for NIC Teaming so that if either NIC or switch module fails, the connection to the other switch is maintained using the same server IP address.

Alternate configurations are possible. Internal trunks do not require that trunked ports belong to the same VSG. Also, internal trunks may include multiple ports from any specific switch (individually or as part of the stack).

By default, all internal ports are excluded from trunks. To assign internal ports to trunks, see [“Internal Trunk ID” on page 110](#).

## 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 switch floods unregistered IP multicast (IPMC) packets to all ports.

On the BBI, choose **Virtual Switch Groups > Settings** to enable IGMP Snooping for the desired VSG. The default value for all VSGs is **enabled**.

## ServerMobility

---

The ServerMobility™ feature allows server IP addresses to be assigned based on their physical location in a blade server chassis. If a server fails, a replacement server can assume the identity of the failed unit. The replacement can be a 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 SmartConnect features that may be installed on the chassis. ServerMobility should not be enabled on the switch if SmartConnect server failover features have already been enabled on the chassis management system.

---

## Configuring a Backup Server Port

If one server is configured as the backup to another server, the administrator may wish 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 switch. The agent remote ID sub-option for packets received on the backup port will use the port number of its active port. If 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 VSG.

## General Configuration

To configure the ServerMobility feature, choose Policies > Server Mobility > General Configuration.

**Server Mobility General Configuration**

Server Mobility

Server Mobility State Disabled

Relay on Non-Server-Mobility Ports Enabled

Auto-Recovery State Disabled

Auto-Recovery Failover Time (1-255)  sec

Set Server Mobility configuration to factory default

**Figure 3-D** ServerMobility General Configuration Window

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

**Table 3-1** ServerMobility General Configuration Fields

Field	Description
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 Policies > Server Mobility > Port Configuration.

Port	Port Server Mobility Mode	Port DHCP request filtering Mode	Backup Port
1	enabled	disabled	None
2	disabled	disabled	None
3	disabled	disabled	None
4	disabled	disabled	None
5	disabled	disabled	None
6	disabled	disabled	None
7	disabled	disabled	None
8	disabled	disabled	None

**Figure 3-E** ServerMobility Port Configuration Window

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

**Table 3-2** 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 DHCP request filtering also be enabled.
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.

**Note –** For port numbers, if the switch is part of a multi-switch stack, the displayed number indicates the Configured Switch number (*csnum*) followed by the port number. See “[Stacking Port Numbers](#)” on page 60 for more information.

## 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`

These variables can be used in any expression allowed within a DHCP configuration file. To declare an explicit chassis, configure the chassis ID in `agent.circuit-id`.

This configuration declares a class for the server connected to port 8 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 8, 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

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

# Stacking

---

### Stacking Overview

---

A *stack* is a group of up to eight switches with SmartConnect software that work together as a unified system. A stack has the following properties, regardless of the number of switches included:

- The network views the stack as a single entity, and the stack is identified by a single network IP address.
- The stack is managed through one Master switch in the stack, using the command-line interface (CLI) or Browser-Based Interface (BBI).
- Switches in a stack may reside within a single blade server chassis, or in multiple chassis.
- The number of ports in a stack equals the total number of ports of all the switches that are part of the stack.
- The maximum number of Virtual Switch Groups (VSGs) remains 32 (the same as for a non-stacked switch), though the number of ports which can be placed in any VSG is equal to the total number of ports in the stack.
- The maximum number of Virtual Machines (VMs) remains 1024 (the same as for a non-stacked switch).
- The maximum number of external trunks remains 64 (2 for each of the 32 VSGs) though the number of ports which can participate in any trunk is equal to the total number of ports in the stack.
- The maximum number of internal trunks is 56.

## Stacking Requirements

---

Before switch modules can form a stack, they must meet the following requirements:

- All switch modules must be the same type.
- All blade server chassis must be the same type or have the same number of server slots (for example, BCE and BCH chassis types are compatible for stacking).
- Each switch must be installed with SmartConnect software. The same release version is not required, as the Master switch will push a firmware image to each differing switch in the stack.
- It is recommended that two 10Gb external ports on each switch are dedicated to stacking. External ports 19 and 20 are used by default, though this can be changed during configuration if necessary. The cables used for connecting the switches in a stack carry low-level, inter-switch communications critical to shared switching functions. Always maintain the stability of stack links in order to avoid internal stack reconfiguration.

## Stack Membership Roles

---

A stack contains up to eight switches, interconnected by a stack trunk in a local ring topology (see [Figure 4-A on page 52](#)). With this topology, only a single stack link failure is allowed.

An operational stack must contain one Master and one or more Members, as follows:

- **Master**

One switch controls the operation of the stack and is called the Master. The Master provides a single point to manage the stack. A stack must have one and only one Master. The firmware image, configuration information, and run-time data are maintained by the Master and pushed to each switch in the stack as necessary.
- **Member**

Member switches provide additional port capacity to the stack. Member switches can reside within a single blade server chassis or across multiple chassis. Members receive configuration changes, run-time information, and software updates from the Master.
- **Backup**

One member switch can be designated as a Backup to the Master. The Backup takes over control of the stack if the Master fails. Configuration information and run-time data are synchronized with the Master.

## The Master Switch

An operational stack can have only one active Master at any given time. In a normal stack configuration, one switch is configured as a Master and all others are configured as Members.

When adding new switches to an existing stack, the administrator should explicitly configure each new switch for its intended role as a Master (only when replacing a previous Master) or as a Member. All stack configuration procedures in this chapter depict proper role specification.

However, although uncommon, there are scenarios in which a stack may temporarily have more than one Master switch. Should this occur, one Master switch will automatically be chosen as the active Master for the entire stack. The selection process is designed to promote stable, predictable stack operation and minimize stack reboots and other disruptions.

### Splitting and Merging One Stack

If multiple stack links or stack Member switches fail, thereby separating the Master and Backup into separate sub-stacks, the Backup automatically becomes an active Master for the partial stack in which it resides. Later, if the topology failures are corrected, the partial stacks will merge, and the two active Masters will come into contact.

In this scenario, if both the (original) Master and the Backup (acting as Master) are in operation when the merger occurs, the original Master will reassert its role as active Master for the entire stack. The Backup will reboot and return to its role as Backup.

However, if the original Master switch is disrupted (powered down or in the process of rebooting) when it is reconnected with the active stack, the Backup (acting as Master) will retain its acting Master status in order to avoid disruption to the functioning stack. The deferring Master will temporarily assume a role as Backup.

If both the Master and Backup are rebooted, the switches will assume their originally configured roles.

If, while the stack is still split, the Backup (acting as Master) is explicitly reconfigured to become a regular Master, then when the split stacks are finally merged, the Master with the lowest MAC address will become the new active Master for the entire stack.

## Merging Independent Stacks

If switches from different stacks are linked together in a stack topology without first reconfiguring their roles as recommended, it is possible that more than one switch in the stack might be configured as a Master.

Although all switches which are configured for stacking and joined by stacking links are recognized as potential stack participants by any operational Master switches, they are not brought into operation within the stack until explicitly assigned (or “bound”) to a specific Master switch.

Consider two independent stacks, Stack A and Stack B, which are merged into one stacking topology. The stacks will behave independently until the switches in Stack B are bound to Master A (or vice versa). In this example, once the Stack B switches are bound to Master A, Master A will automatically reconfigure them to operate as Stack A Members, regardless of their original status within Stack B.

However, for purposes of future Backup selection, reconfigured Masters retain their identity as configured Masters, even though they otherwise act as Members and lose all settings pertaining to their original stacks.

## Backup Switch Selection

An operational stack can have one optional Backup at any given time. Only the Backup specified in the active Master's configuration is eligible to take over current stack control when the Master is rebooted or fails. The Master automatically synchronizes configuration settings with the specified Backup to facilitate the transfer of control functions.

The Backup retains its status until one of the following occurs:

- The Backup setting is deleted or changed using the following command from the active Master:

```
>> # /cfg/stack/backup
-or-
>> # /cfg/stack/backup <csnum>
```

- A new Master assumes operation as active Master in the stack, and uses its own configured Backup settings.
- The active Master is rebooted with the boot configuration set to factory defaults (clearing the Backup setting).

## Master Failover

When the Master switch is present, it controls the operation of the stack and pushes configuration information to the other switches in the stack. If the active Master fails, then the designated Backup (if one is defined in the Master's configuration) becomes the new acting Master and the stack continues to operate normally.

## Secondary Backup

When a Backup takes over stack control operations, if any other configured Masters (acting as Member switches) are available within the stack, the Backup will select one as a secondary Backup. The primary Backup automatically reconfigures the secondary Backup, and specifies itself (the primary Backup) as the new Backup in case the secondary fails. This prevents the chain of stack control from migrating too far from the original Master and Backup configuration intended by the administrator.

## Master Recovery

If the prior Master recovers in a functioning stack where the Backup has assumed stack control, the prior Master does not reassert itself as the stack Master. Instead, the prior Master will assume a role as a secondary Backup to avoid further stack disruption.

Upon stack reboot, the Master and Backup will resume their regular roles.

## No Backup

If a Backup is not configured on the active Master, or the specified Backup is not operating, then if the active Master fails, the stack will reboot without an active Master.

When a group of stacked switches are rebooted without an active Master present, then all switches in the stack are placed in a `WAITING` state until a Master appears. During this `WAITING` period, all the external ports and internal server ports of these Member switches are placed into operator-disabled state. Without the Master, a stack cannot respond correctly to networking events.

## Stack Member Numbers

---

Each switch in the stack has two numeric identifiers, as follows:

- **Attached Switch Number** (*asnum*)  
This is automatically assigned by the Master switch and is not user-configurable. The *asnum* identifies each switch based on its physical connection in relation to the Master.
- **Configured Switch Number** (*csnum*):  
The *csnum* is configured by the stack administrator in order to create a logical grouping of switches and ports.

It is recommended that *asnum* 1 and *csnum* 1 be used for identifying the Master switch.

---

**Note** – By default, *csnum* 1 is assigned to the Master. If *csnum* 1 is not available, the lowest available *csnum* is assigned to the Master.

---

## Best Configuration Practices

---

The following are guidelines for building an effective switch stack:

- Always connect the stack switches in a complete ring topology (see [Figure 4-A on page 52](#)).
- Optimal stack performance occurs in a stack of three switches, as each switch is then directly connected to all others in the stack.
- For stacks with more than three switches, the Backup switch should be adjacent to the Master in the stacking topology.
- Avoid disrupting the stack connections unnecessarily while the stack is in operation.
- For best redundancy, use DMLT.
- Avoid altering the stack *asnum* and *csnum* definitions unnecessarily while the stack is in operation.
- Stacking uses one of the QoS priority queues for management and control traffic. Therefore, only seven priority queues will be available for regular QoS use.
- Configure only as many QoS levels as necessary. This allows best use of packet buffers.

## Configuring Each Switch in a Stack

---

This section provides procedures for creating a stack of switch modules. The high-level procedure is as follows:

- Enable stacking on each switch.
- Designate one switch as the Master.
- Reboot all stack switches.
- Connect the stack trunk as shown in [Figure 4-A](#).
- Configure the Master interface.
- Configure additional stacking parameters on the Master.

To pre-configure each Member switch for stacking, use the CLI to perform the following steps.

### 1. Enable stacking on each switch in the stack.

```
>> # /boot/stack/enable
```

### 2. Configure the Stack Trunk ports (optional).

Dedicate two external 10Gb ports on each switch to support stacking. It is recommended that the default stack ports be used (shown below).

```
>> Boot Stacking# stktrnk
Enter ports one per line, NULL at end:
> 19
> 20
>
A Reboot is required for the new settings to take effect
```

### 3. Configure the stacking VLAN (optional).

Although any VLAN (except VLAN 1) may be defined for stack traffic, it is highly recommended that the default, VLAN 4090, be reserved for stacking (shown below).

```
>> Boot Stacking# vlan 4090
```

#### 4. Set the stacking mode.

By default, each switch is set to member mode. However, one (and only one) switch must be set to master mode. Use the following CLI command on only the designated Master switch:

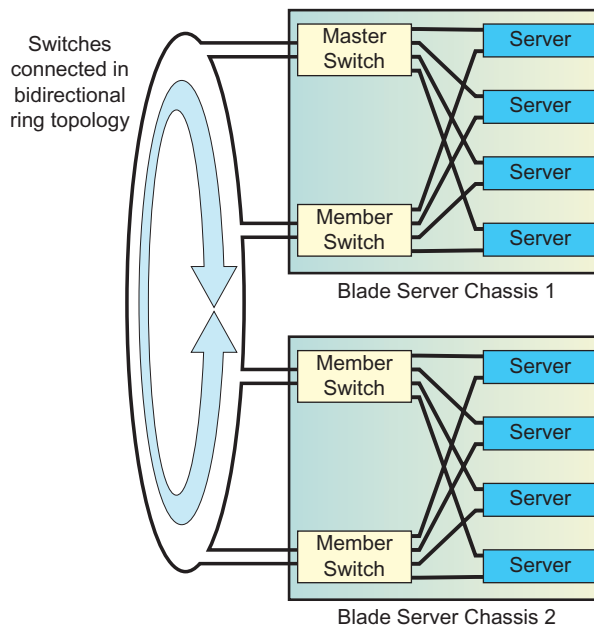
```
>> Boot Stacking# mode master
```

**Note** – If any Member switches are incorrectly set to master mode, use the mode member command to set them back to Member mode.

#### 5. Reboot all of the stack switch modules.

#### 6. Physically connect the Stack Trunks in a bidirectional ring topology.

It is recommended that two 10Gb external ports on each switch are dedicated to stacking. As shown in Figure 4-A, starting with the Master switch, connect each switch in turn to the next. Connect the last Member switch back to the Master to complete the ring.



**Figure 4-A** Example of Stacking Connections

Once the stack trunks are connected, the switches perform low-level stacking configuration.

**Note** – It is recommended not to disconnect and reconnect the stack links after the stack is formed. If the stack links are disconnected, stack operation can become unstable as the stack reconfigures, and traffic can be disrupted, causing data loss.

## 7. On the designated Master switch, configure the Master interface for the stack.

```
>> # /cfg/stack/mif
>> Master Switch Interface# addr <interface IP address>
>> Master Switch Interface# mask <subnet mask>
>> Master Switch Interface# gw <gateway IP address>
```

**Note** – The `mif` menu is available only on the Master switch once the stacking mode has been set (Step 4) and the switch has been rebooted (Step 5).

## Additional Master Configuration

Once the Master switch interface has been defined, access the internal management IP interface of the Master switch, and complete the configuration. This can be done using either the CLI or the Browser-Based Interface (BBI).

### Master Configuration via the CLI

Use the following procedures to complete the stack configuration using the CLI. To use the BBI instead, see “[Master Configuration via the BBI](#)” on page 56.

### Locating the Master Switch Internal Management IP Interface via CLI

Use Telnet to connect to the Master interface IP address configured in [Step 7 on page 53](#) (the final step of the previous procedure), or log in to the Master switch and execute the following command:

```
>> # /info/stack/ip

Master switch IP:
-----
   for Data Interface           - 172.24.0.200
   for Int Mgmt Interface      - 10.100.120.8
```

## Viewing Stack Connections via CLI

To view information about the switches in a stack, execute the following command:

```
>> # /info/stack/switch

Stack name:
Local switch is the master.

Local switch:
  csnum - 1
  MAC - 00:00:00:00:01:00
  Switch Type - 9
  Chassis Type - 99
  Switch Mode (cfg) - Master
  Priority - 225
  Stack MAC - 00:00:00:00:01:1f

Master switch:
  csnum - 1
  MAC - 00:00:00:00:01:00

Backup switch:
  csnum - 2
  MAC - 00:22:00:ad:43:00

Configured Switches:
-----
csnum          MAC              asnum
-----
C1  00:00:00:00:01:00  A1
C2  00:22:00:ad:43:00  A3
C3  00:11:00:af:ce:00  A2

Attached Switches in Stack:
-----
asnum          MAC              csnum  State
-----
A1  00:00:00:00:01:00  C1    IN_STACK
A2  00:11:00:af:ce:00  C3    IN_STACK
A3  00:22:00:ad:43:00  C2    IN_STACK
```

## Binding Members to the Stack via CLI

You can bind Member switches to a stack `csnum` using either their MAC address or `asnum`:

```
>> # /cfg/stack/bind <csnum> mac <MAC address>
or
>> # /cfg/stack/bind <csnum> asnum <asnum>
```

To remove a Member switch, execute the following command:

```
>> # /cfg/stack/bind <csnum>
```

## Assigning a Stack Backup Switch via ISCLI

To define a Member switch as a Backup (optional) which will assume the Master role if the Master switch should fail, execute the following command:

```
>> # /cfg/stack/backup <csnum>
```

## Configuring an External IP Address for the Stack via ISCLI

Configure the following information for the Master switch interface:

- Master interface IP address and subnet mask
- Default gateway IP address
- VLAN number used for external access to the stack (rather than the internal VLAN 4090 used for inter-stack traffic)

Use the following commands:

```
>> # /cfg/stack/mif
>> Master Switch Interface# addr <interface IP address>
>> Master Switch Interface# mask <subnet mask>
>> Master Switch Interface# gw <gateway IP address>
>> Master Switch Interface# vlan <VLAN 2-4094>
```

When the Master switch interface is defined, configuration is complete.

## Master Configuration via the BBI

As an alternative to the CLI (“[Master Configuration via the CLI](#)” on page 53), you may complete the Master switch configuration using the BBI as shown in the following procedures.

### Locating the Master IP Interface via Browser

To launch the BBI for the Master switch, use a Web browser to access the Master interface IP address configured in [Step 7 on page 53](#).

### Viewing Stack Connections via BBI

From the Master switch BBI menu, choose **Information > Stack** and locate the Attached Switch Information. Make sure all of the stack switches are listed. If a switch is not listed, check the cables on the stack links, and make sure all stacking requirements are met, as listed in “[Stacking Requirements](#)” on page 46.

<b>Attached Switch Information</b>					
<b>Attached Switch Number (asnum)</b>	<b>UUID</b>	<b>Bay Number</b>	<b>Configured Switch Number (csnum)</b>	<b>MAC</b>	<b>State</b>
1	594900c1565f11dba8ddcad0a4b3de4a	1	1	00:17:ef:cf:e5:00	IN_STACK
2	594900c1565f11dba8ddcad0a4b3de4a	2	Not configured	00:16:60:f9:33:00	ATTACH
3	d65f11a8ddcad0a17efcfe57efc3fbfcfe	1	Not configured	00:17:ef:c3:fb:00	ATTACH
4	d65f11a8ddcad0a17efcfe57efc3fbfcfe	2	Not configured	00:17:ef:cf:e2:00	ATTACH

**Figure 4-B** Attached Switch Information Window

## Binding Members to the Stack via BBI

Choose menu System Settings > Stacking > Switch Configuration. The Stack Switch Configuration window appears, as shown in [Figure 4-C](#).

**Stack Switch Configuration - Bind to Attached Switch Number (asnum)**

Stack Name

Master Switch 1

Backup Switch

Switch	Bind asnum	UUID	Bay Number	Delete
Switch 1	1	594900c1565f11dba8dd	1	<input type="checkbox"/>
Switch 2	4	594900c1565f11dba8dd	2	<input type="checkbox"/>
Switch 3	2	d65f11a8ddcad0a17efcf	3	<input type="checkbox"/>
Switch 4	3	d65f11a8ddcad0a17efcf	4	<input type="checkbox"/>

**Figure 4-C** Stack Switch Configuration Window

Each switch in the stack is represented by an Attached Switch Number (asnum) and a Configured Switch Number (cnum) as explained in [“Viewing Stack Connections via BBI” on page 56](#). Both asnum 1 and cnum 1 are reserved for the Master.

- Select an attached switch in the Bind asnum drop-down list to bind the switch to its associated cnum.
- In the Backup Switch drop-down list, select a cnum for a Backup switch (optional) which will assume the Master role if the Master switch should fail.
- In the Stack Name field, enter a name for the stack (optional).

The UUID and Bay Number fields display information about the location of configured switches and are not configurable. The UUID is the Unit ID number of the blade server chassis where the switch resides, and the Bay Number is the switch's physical bay within the chassis.

Click **Apply** to make the changes active, and **Save** to retain changes beyond reboot cycles.

## Configuring an External IP Address for the Stack via BBI

Choose menu **System Settings > Stacking > IP Interfaces**. Use the Stack IP Interfaces window to configure a single IP interface for the stack. This interface is known at the Master interface and is shared by all switches in the stack.

**Stack IP Interfaces**

Master Switch Interface

IP Address	192.168.150.200
Subnet Mask	255.255.255.0
Group (1 - 32)	1
Smvlan (0 - 4094)	0
Default Gateway Address	192.168.150.254
Delete Interface	<input type="checkbox"/>

Backup Switch Interface

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Group (1 - 32)	1
Smvlan (0 - 4094)	0
Default Gateway Address	0.0.0.0
Delete Interface	<input type="checkbox"/>

Management IP Interface

**Figure 4-D** Stack IP Interfaces Configuration Window

Enter the following information for the Master Switch Interface:

- Master interface IP address and subnet mask
- Virtual Switch Group number
- VLAN number used for external access to the stack (rather than the internal VLAN 4090 used for inter-stack traffic)
- Default gateway IP address

Click **Apply** to make the changes active, and **Save** to retain changes beyond reboot cycles.

**Note** – The Backup switch interface is provided for historical purposes only and should be left unconfigured. If a Backup switch interface is defined in this window, and the Master fails, the stack IP address will change to the IP address configured for the Backup switch interface.

## Managing a Stack

The stack is managed through the Master switch. The Master switch then pushes configuration changes and run-time information to the Member switches.

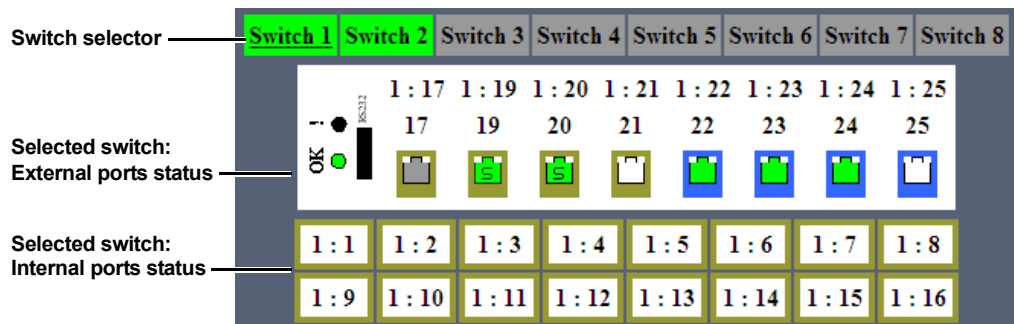
Use Telnet or the Browser-Based Interface (BBI) to access the Master, as follows:

- On any switch in the stack, connect to any external port that is not part of an active trunk (see the note on [page 33](#)).
- Use the management IP address assigned to the Master by the management system.

When switches are configured into a stack, the BBI displays information for the stack.

The BBI menu area displays the `csnum` for the Master and the Backup (if configured). The port status area display includes a switch selector and enhanced port displays, as shown below:

**Figure 4-E** Port Status with Stacking

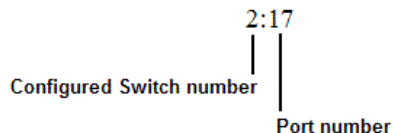


Click a highlighted switch in the switch selector to display status information about ports in that switch. Click a port icon to display port statistics.

The following additional BBI configuration changes occur when switches are stacked.

### Stacking Port Numbers

Once a stack is configured, the manner in which port numbers are displayed changes throughout the BBI. Instead of the single number, the `csnum` appears in front of each port number. For example:



This numbering change appears in the port status area at the top of the BBI, as well as on numerous configuration pages. For example:

- Virtual Switch Groups > Membership
- Policies > External Port Settings
- Policies > Internal Port Settings
- Policies > ServerMobility > Port Configuration

On these BBI configuration pages, the administrator can also select whether to display all ports for all switches, all present switches, all defined switches, or a specific `csnum`. To do this, make the appropriate selection from the View Ports drop-down list.

### Stacking Internal Port Settings

For each port in a stack, the following command is added to the Internal Port Settings window:

**Table 4-1** Additional Internal Port Settings for Stacking

Field	Description
Internal trunk id <1-56, 0 = none>	Configures the trunk ID for internal ports. Ports in the same VSG that have the same internal trunk ID form a trunk.

### Stacking VLANs

VLAN 4090 is the default VLAN reserved for stacking ports.

---

**Note** – Do not use VLAN 4090 for any purpose other than stacking.

---

## Stacking Boot Management

The Boot Management General window provides controls that allow the administrator to perform a reboot of individual switches in the stack, or the entire stack. The following table describes the stacking Reboot commands.

**Table 4-2** Stacking Boot Management buttons

Field	Description
Reboot Stack	Performs a software reboot/reset of all switches in the stack. The software image specified in the Image To Boot drop-down list becomes the active image.
Reboot Master	Performs a software reboot/reset of the Master switch. The software image specified in the Image To Boot drop-down list becomes the active image.
Reboot Switches	Performs a reboot/reset on selected switches in the stack. Select one or more switches in the drop-down list, and click <b>Reboot Switches</b> . The software image specified in the Image To Boot drop-down list becomes the active image.

The Update Image/Cfg section of the window applies to the Master. When a new software image or configuration file is loaded, the file first loads onto the Master, and the Master pushes the file to all other switches in the stack, placing it in the same software or configuration bank as that on the Master. For example, if the new image is loaded into image 1 on the Master switch, the Master will push the same firmware to image 1 on each Member switch.

## Upgrading Stack Software

---

Upgrade all stacked switches at the same time. The Master controls the upgrade process. Use the following procedure to perform a software upgrade.

1. **Load new software on the Master. Refer to “Transferring the New Image to the Switch” on page 22.**

The Master pushes the new software image to all Members in the stack, as follows:

- If the new software is loaded into image 1, the Master pushes the software into image 1 on all Members.
- If loaded into image 2, the Master pushes the software into image 2 on all Members.

The software push can take several minutes to complete.

2. **Verify that the software push is complete. Use either the CLI or the BBI:**

- From the BBI, go to **Information > Stack** and view the Image Push Status Information at the bottom of the page, or
- From the CLI, use following CLI command to verify the software push:

```
>> # /info/stack/pushstat
Image 1 transfer status info:
  Switch 00:16:60:f9:33:00:
    last receive successful
  Switch 00:17:ef:c3:fb:00:
    not received - file not sent or transfer in progress

Image 2 transfer status info:
  Switch 00:16:60:f9:33:00:
    last receive successful
  Switch 00:17:ef:c3:fb:00:
    last receive successful

Boot image transfer status info:
  Switch 00:16:60:f9:33:00:
    last receive successful
  Switch 00:17:ef:c3:fb:00:
    last receive successful

Config file transfer status info:
  Switch 00:16:60:f9:33:00:
    last receive successful
  Switch 00:17:ef:c3:fb:00:
    last receive successful
```

**3. Reboot all switches in the stack. Use either the BBI or the CLI.**

- From the BBI, select System Settings > Boot Management. Click Reboot Stack.
- From the CLI, use the following command:

```
>> # /boot/reset
```

**4. Once the switches in the stack have rebooted, verify that all of them are using the same version of firmware. Use either the BBI or the CLI.**

- From the BBI, go to Information > Stack and view the Switch Firmware Versions Information.
- From the CLI, use following command:

```
>> # /info/stack/vers
```

```
Switch Firmware Versions:
```

```
-----
asnum csnum      MAC          S/W  Version  Serial #
-----
A1     C1    00:00:00:00:01:00 image1 0.0.0.0 CH4909005L
A2     C2    00:11:00:af:ce:00 image1 0.0.0.0 CH4909005F
A3           00:22:00:ad:43:00 image1 0.0.0.0 CH4909005T
```

## Replacing a Switch in an Existing Stack

Stack switches may be replaced while stack is in operation. However, the following conditions must be met in order to avoid unnecessary disruption:

- If removing an active Master switch, make sure that a valid Backup exists in the stack.
- It is best to replace only one switch at a time.
- If replacing multiple switches, once one switch has been properly disconnected (see the procedures that follow), any adjacent switch can also be removed.
- Removing any two, non-adjacent switches will divide the ring and disrupt the stack.

Use the following procedures to replace a stack switch.

### *Preparing the New Switch*

1. **Make sure the new switch meets the stacking requirements on [page 46](#).**
2. **Enable stacking on the new switch.**

```
>> # /boot/stack/enable
```

3. **Configure the stack trunk ports (optional).**

Dedicate two external 10Gb ports on each switch to support stacking. It is recommended that the default stack ports be used (shown below).

```
>> Boot Stacking# stktrnk
Enter ports one per line, NULL at end:
> 19
> 20
>
A Reboot is required for the new settings to take effect
```

4. **Configure the stacking VLAN, of use the default setting.**

Although any VLAN may be defined for stack traffic, it is highly recommended that the default, VLAN 4090, be reserved for stacking (shown below).

```
>> Boot Stacking# vlan 4090
```

## 5. Set the stacking mode.

By default, each switch is set to Member mode. However, if the incoming switch has been used in another stacking configuration, it may be necessary to ensure the proper mode is set.

- If replacing a Member or Backup switch:

```
>> Boot Stacking# mode member
```

- If replacing a Master switch:

```
>> Boot Stacking# mode master
```

## 6. Apply and save your configuration changes.

## 7. Turn the new switch off.

### *Removing the Old Switch*

#### 1. Make sure the stack is configured in a ring topology.

---

**Note** – When an open-ended daisy-chain topology is in effect (either by design or as the result of any failure of one of the stacking links), removing a stack switch from the interior of the chain can divide the chain and cause serious disruption to the stack operation.

---

2. **If removing a Master switch, make sure that a Backup switch exists in the stack and then turn the Master switch off. This will force the Backup switch to assume Master operations for the stack.**
3. **Remove the stack link cables from the old switch only.**
4. **Disconnect all network cables from the old switch only.**
5. **Turn off only the old switch (if not already off), and remove it.**

### *Install the New Switch*

1. **Install the new switch in its determined place according to the *RackSwitch G8000 Installation Guide*.**
2. **Attach the required stack link cables to the ports configured in [Step 3 on page 64](#).**
3. **Attach the desired network cables to the new switch.**
4. **Turn the new switch on.**

Once the new switch boots, it will join the existing stack. Wait for this process to complete.

### *Bind the New Switch to the Stack*

- 1. Log in to the Master switch interface.**

---

**Note** – If replacing the Master switch, be sure to log in to the Master switch interface (hosted temporarily on the Backup switch) rather than logging in directly to the newly installed Master.

---

- 2. From the Master switch interface, assign the `csnum` for the new switch.**

You can bind switches to a stack `csnum` using either their MAC address or `asnum`:

```
>> # /cfg/stack/bind <csnum> mac <MAC address>
or
>> # /cfg/stack/bind <csnum> asnum <asnum>
```

- 3. Apply and save your configuration changes.**

---

**Note** – If replacing the Master switch, the Master will not assume control from the Backup unless the Backup is rebooted or fails.

---

## CHAPTER 5

# Command Reference

---

The SmartConnect 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.

The administrator can use the SmartConnect software 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, the administrator is presented with a hierarchy of menus that enable one 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 SmartConnect 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 Menu

The Operations Menu (/oper) is used for making immediate, temporary changes to the operational configuration of the switch. 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
  gting - Download new software image via FTP/TFTP
  pting - 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 system. 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
```

---

**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 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 switch. Your options include:

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

---

**Note** – When resetting the switch to its factory default configuration, the switch will retain its stacking settings. To reconfigure or disable stacking, see [“Stacking” on page 45](#).

---

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.

## CHAPTER 6

# Configuring Switch Access

---

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

- “Using Telnet” on page 74
- “Using the Browser-Based Interface” on page 75
- “Securing Access to the Switch” on page 77
  - “Setting Allowable Source IP Address Ranges” on page 78
  - “RADIUS Authentication and Authorization” on page 79
  - “TACACS+ Authentication” on page 81
  - “End User Access Control” on page 82
  - “Secure Shell and Secure Copy” on page 84

## Using Telnet

---

Telnet is used to access the switch's command-line interface. Telnet can be launched from the management system 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 (BBI), try to ping the switch's IP address from management system. If the ping fails, the management system is not configured correctly.

---

To use Telnet from the management system, 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 84](#). For more information on the command line interface (CLI), see [“Command Reference” on page 67](#).

## Using the Browser-Based Interface

---

Use the management system 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 Web browser window opens a connection to the SmartConnect software interface on the switch.

The switch's Browser-Based Interface (BBI) provides access to the common configuration, management and operation features through the Web browser.

### Access via HTTP

BBI access is enabled by default. To access the switch via the 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) []: <organizational 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 BBI, 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 switch is rebooted. To save the certificate, use the following command:

```
>> /cfg/sys/access/https/certsave
```

When a client (such as a 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 78](#)
- Authentication and authorization of remote administrators: see [“RADIUS Authentication and Authorization” on page 79](#)
- Encryption of management information exchanged between the remote administrator and the switch: see [“Secure Shell and Secure Copy” on page 84](#)

The following sections are addressed in this section:

- [“Setting Allowable Source IP Address Ranges” on page 78](#)
- [“RADIUS Authentication and Authorization” on page 79](#)
- [“TACACS+ Authentication” on page 81](#)
- [“Secure Shell and Secure Copy” on page 84](#)

## 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 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 (as defined in the `/cfg/sys/access/mgmt` menu).

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 the management network IP address and mask in the System Access Management Menu.

```
>> 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, 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 SmartConnect software supports the RADIUS (Remote Authentication Dial-in User Service) method to authenticate and authorize remote administrators for managing the switch. 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

1. In the BBI, choose **System Settings > Remote User Administration** to configure RADIUS authentication.
2. In the Radius section of the window, enter the **Primary Radius Server IP address** and **Radius secret**.
3. Select **enable** for the Radius option.
4. Click **Apply** to make your changes active, and **Save** to retain changes beyond reboot.

### User Accounts

The user accounts listed in [Table 6-1 on page 79](#) can be defined in the RADIUS server dictionary file.

**Table 6-1** 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 SmartConnect Software User Privileges

When the user logs in, the switch authenticates the appropriate level of access by sending the RADIUS access request (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. By default, Telnet access is disabled.

---

**Note** – To obtain the RADIUS backdoor password for your switch, contact your 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 (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 switch user privileges levels:

**Table 6-2** SmartConnect-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 6-3 on page 81](#). The authorization levels must be defined on the TACACS+ server.

**Table 6-3** SmartConnect-Proprietary Attributes for TACACS+

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

### Configuring TACACS+ Authentication

1. **On the BBI, choose `System Settings > Remote User Administration` to configure TACACS+ authentication.**
2. **In the TACACS+ section of the window, enter the TACACS+ Primary Server IP address and TACACS+ Secret.**
3. **Select `enable` for the TACACS+ option.**
4. **Click `Apply` to make your changes active, and `Save` to retain changes beyond reboot.**

## 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.
- SmartConnect 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 switch 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

1. On the BBI, choose **System Settings > Local User Administration**.

### 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 :	<input type="text"/>	<input type="text"/>	user ▼ disable ▼
User2 :	<input type="text"/>	<input type="text"/>	user ▼ disable ▼
User3 :	<input type="text"/>	<input type="text"/>	user ▼ disable ▼
User4 :	<input type="text"/>	<input type="text"/>	user ▼ disable ▼
User5 :	<input type="text"/>	<input type="text"/>	user ▼ disable ▼
User6 :	<input type="text"/>	<input type="text"/>	user ▼ disable ▼
User7 :	<input type="text"/>	<input type="text"/>	user ▼ disable ▼
User8 :	<input type="text"/>	<input type="text"/>	user ▼ disable ▼
User9 :	<input type="text"/>	<input type="text"/>	user ▼ disable ▼
User10 :	<input type="text"/>	<input type="text"/>	user ▼ disable ▼

**Figure 6-A** Local User Administration Window

2. In the **User Configuration** section, enter a **Username** and **Password** for the account.
3. 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 6-1 on page 79](#).

4. Select **enable** to allow the new user to access the switch.
5. Click **Apply** to make your changes active, and **Save** to retain changes beyond reboot.

## Logging in to 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.

## 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 switch 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 system and enter the following CLI command:

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

### Enabling or Disabling 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 system. For security reasons, the `scpadm` password may only be configured when connected through the management system.

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 switch is 205.178.15.100, the IP address of the management system 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

```

## 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, a 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 switch 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 SmartConnect. The server key is 768 bits and is used to make it impossible to decipher a captured session by breaking into the SmartConnect at a later time.

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

To configure RSA host and server keys, first connect to the switch through the management system or 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 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 also can regenerate the RSA server key. To set the interval of RSA server key auto-generation, use this command:

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

A value of 0 (zero) denotes that RSA server key autogeneration is disabled. When greater than 0, the switch automatically generates 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 SmartConnect performs only one session of key/cipher generation at a time. Thus, a SSH/SCP client will not be able to log in if the switch is performing key generation at that time, or if another client has logged in immediately prior. Also, key generation will fail if a 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 SmartConnect, 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 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 a 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 a SCP-only administrator password.

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

A 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 a SSH user because the switch will recognize him as the SCP-only administrator. The switch allows only the administrator access to SCP commands.

---



# Part 2: BBI Reference

SmartConnect software provides a graphical user interface that lets you remotely configure and manage switches through a Web browser.

Using the SmartConnect software browser-based interface (BBI), you can:

- Divide the switch into multiple virtual switches.
- Group multiple physical ports together to aggregate the bandwidth between large-scale network devices.
- Set properties for internal and external switch ports and management ports.
- Configure Access Control Lists (ACLs), port mirroring, and other switch features.
- Examine a variety of switch information and statistics.

The following sections of this *User's Guide* contain information about the settings and controls on each page of the BBI used for configuring and monitoring the switch:

- [Chapter 7, “Understanding the Browser-Based Interface,”](#) provides information about the BBI screen layout and menu system, and describes how to make and save configuration settings.
- [Chapter 8, “Virtual Switch Groups,”](#) provides information for virtualizing the switch: dividing it into multiple virtual switches, defining VLANs, and grouping ports to aggregate bandwidth.
- [Chapter 9, “Switch Policies,”](#) provides information for configuring internal and external ports, port mirroring, and defining Access Control Lists (ACLs), quality of service (QoS), and ServerMobility.

- [Chapter 10, “System Settings,”](#) provides information for configuring management capabilities, local and remote user administration, time services, BOOTP, SSH and Telnet access, Syslog, and more.
- [Chapter 11, “Boot Management,”](#) provides information for loading switch software images, and for selecting which image and configuration files will be used.
- [Chapter 12, “Switch Information,”](#) described how to view and interpret detailed configuration and status information regarding a variety of switch features.
- [Chapter 13, “Switch Statistics,”](#) described how to view and interpret operational information regarding port and network activity and switch operational characteristics.

For initial setup of the BBI and access, see [Chapter 2, “Getting Started with the Browser-Based Interface.”](#)

## CHAPTER 7

# Understanding the Browser-Based Interface

---

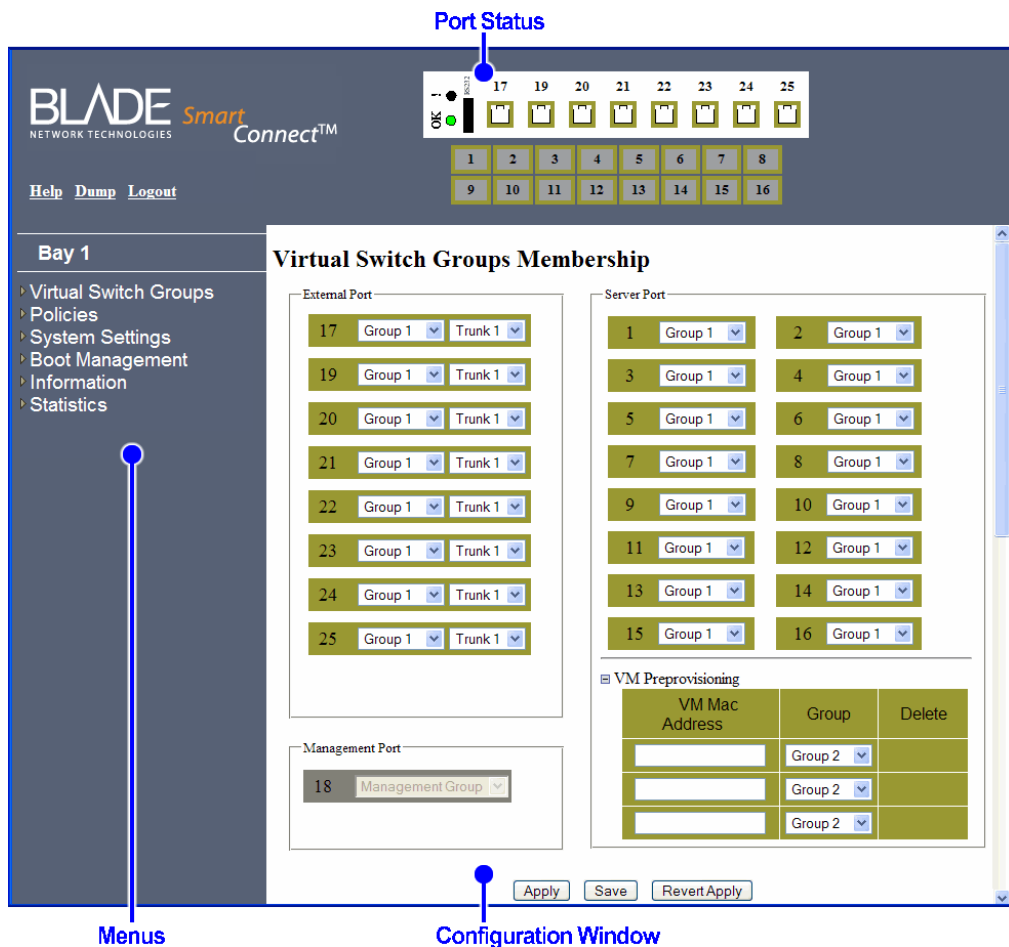
The SmartConnect software offers two user interfaces: a browser-based interface (BBI) and a command-line interface (CLI). The BBI allows you to perform basic switch configuration tasks quickly and easily using a standard Web browser. The CLI provides more detailed configuration options for SmartConnect software.

This *User's Guide* covers primarily the usage of the SmartConnect software BBI. For details on the initial setup and access to the BBI, see [Chapter 2, “Getting Started with the Browser-Based Interface.”](#) For information about using the CLI, see [Chapter 5, “Command Reference.”](#)

### *The SmartConnect BBI Screen*

The SmartConnect software BBI has three major areas, as shown below and described in the following sections:

Figure 7-A Main SmartConnect Software Screen



## Port Status Area

The port status area displays port icons representing each port in the switch. The border color of each icon indicates the Virtual Switch Group (VSG) to which the port belongs.

Each port's operational status is also displayed, as indicated by the port icon's interior color:

**Table 7-1** Port Status Colors

Color	Description
Grey	Disabled
Green	Active link
White	No link

Click on a port icon to display statistics for the port (see [“Switch Ports Statistics Summary”](#) on page 170).

Click on the background area outside a port to display IGMP statistics for the switch.

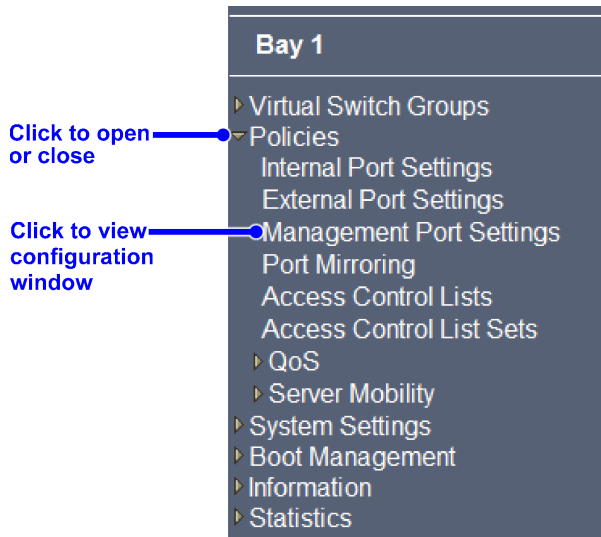
---

**Note** – The format used for depicting the port number depends on whether the switch is part of a multi-switch stack. If stacked, the Configured Switch number (c<sub>s</sub>num) is placed in front of the port number. For example, 1:3 indicates c<sub>s</sub>num 1, port 3. See [“Stacking Port Numbers”](#) on page 60 for more information.

---

### Menu Area

The menu area displays the switch type and the bay number where the switch resides. It also displays a list of menu items, arranged in a tree of feature folders (indicated with a small triangle) and feature names:



**Figure 7-B** SmartConnect Software Menu Area

Click on a closed feature folder to open it and reveal its contents. Click on it again to close it. When a feature folder is open, click on any feature name display the corresponding information in the configuration area.

## Configuration Window

When you choose a feature name from the menu area, the corresponding configuration controls are displayed in the configuration window. Depending on the selected feature, the configuration window provides switch information or allows you to view and change the settings of the SmartConnect software features.

If you use the configuration area to change the switch configuration, click on one of the buttons at the bottom of the window, as follows:

**Table 7-2** Configuration Buttons

Button	Description
Apply	When altering fields in the configuration area, your changes are “pending” and do not take effect until you click the <b>Apply</b> button. Once applied, all configuration changes take effect on the switch immediately. However, if you do not also save the changes, they will be lost the next time the switch is rebooted or whenever the <b>Revert Apply</b> command is given.
Save	Writes the applied configuration changes to non-volatile flash memory on the switch so that the configuration is retained beyond reboot or power cycles.
Revert Apply	Clears any unsaved configuration changes, whether applied or not. Use this command to return all configuration fields to their last saved state.

Some configuration screens have other buttons (such as **Delete**, **Clear**, or **Search**). The functions of these controls are described in the sections detailing each configuration page.

---

**Note** – In some instances where multiple BBI and/or CLI sessions are simultaneously applying and reverting configuration changes, the next use of the **Apply**, **Save**, or **Revert Apply** command may not function as expected unless another configuration item is updated.

---



## CHAPTER 8

# Virtual Switch Groups

---

Switch resources can be pooled or divided into logical units known as Virtual Switch Groups (VSGs). Up to 32 VSGs are available.

Two different types of resources can be assigned to VSGs:

- Ports (internal and external)
- Virtual Machines (VMs)

### *Port Groups*

Each internal and external port can be independently assigned to one of the 32 available VSGs. Each VSG can contain multiple ports, but each port can belong to only one VSG.

VSGs for port groups must have the following characteristics:

- It is recommended that each VSG contain at internal server ports *and* external ports for proper network operation.
- By default, all external ports in the same VSG are placed into one trunk to aggregate their bandwidth.

For VSG port group and trunk configuration, see [“Virtual Switch Groups Membership” on page 103](#).

---

**Note** – The port references that appear in this *User’s Guide* might differ from your system. The number of ports is based on the type of blade server chassis, and the firmware versions and options installed.

---

## Virtual Machine Groups

The switch automatically discovers VMs that reside in the hypervisor directly connected to the switch. As with ports, VMs can be independently assigned to VSGs in order to group or separate them. Optionally, uplink ports can also be assigned to VSGs that include VMs.

The switch will accept a maximum of 1024 VMs. Once this limit is reached, the switch will reject additional VMs.

---

**Note** – In some rare situations, the switch may reject the addition of new VMs prior to reaching the 1024 VM limit. This can occur when the hash bucket corresponding to the new VM is already full. If this occurs, change the virtual machine's MAC address and retry the operation. The MAC address can usually be changed from the virtualization platform's management console (such as the VMware Virtual Center). This limitation is independent of whether switches are acting alone or as part of a stack.

---

VSGs containing VMs have the following characteristics:

- The VSG may consist of VMs and (optionally) external port.
- Internal ports cannot be added to VSGs which contain VMs, and VMs cannot be added to VSGs which contain internal ports.
- The switch allows communication between VMs in the same group.
- The switch does not allow communication between VMs which are not in the same group. However, VMs which are in the same hypervisor may still communicate with each other even if they are not assigned to the same VSG on the switch.

For information on configuration, see [“Assigning Virtual Machines to VSGs” on page 103](#).

## Link Aggregation

The default network configuration of the SmartConnect software places all ports into a single VSG, and aggregates all external ports together into a static Link Aggregation Group (LAG, or trunk).

This configuration eliminates the need for Spanning Tree Protocol to prevent network loops, since the uplink ports act as a single link. Also, since all of the uplink ports in each VSG participate in a static LAG, if a link fails, the existing traffic is redirected to the other links.

To override default VSG assignments and trunk settings, see [“Assigning Ports to VSGs” on page 103](#).

## Virtual Switch Groups Membership

---

Use this window to group ports or virtual machines into VSGs.

### *Viewing Ports*

If stacking is enabled, the View Ports control is added to the top of the configuration window. Use this drop-down list to specify whether to display all ports for all switches, all present switches, all defined switches, or a specific Configured Switch number.

### *Assigning Ports to VSGs*

Choose menu **Virtual Switch Groups > Membership** to select the VSG in the Group drop-down list for each of the external ports and internal server blade ports. Also in this configuration window, external ports can be assigned to a VSG trunk. Click **Apply** to make your changes active, and **Save** to retain changes beyond reboot.

To enable Layer 2 Failover, Link Aggregation Control Protocol (LACP), or IGMP Snooping for the VSG, choose menu **Virtual Switch Groups > Settings**.

### *Assigning Virtual Machines to VSGs*

Choose menu **Virtual Switch Groups > Membership**. Ports with VMs attached to them are noted with a plus (+) or minus (-) in front of the port designation. Click on the plus icon to reveal the list of VMs attached to the port, or on the minus icon to hide them.

When VMs are revealed, the VM Group field shows the VSG to which the VMs are assigned. To put a VM into a specific VSG, choose the desired group number from the list of available group numbers. To put a VM in a different VSG, choose the new group number. By default, all VMs are unassigned.

It is important to assign at least one uplink port to the VM group if the VMs in the group need to communicate with other servers connected to the network. It is not necessary to assign an uplink port to a VSG if the VMs in the group only communicate with each other.

---

**Note** – VMs may belong to the same or different group as the port to which they are attached. The regular (non-VM) port traffic always uses the VSG specified for the port, and the VM traffic always uses the VSG specified for the VM. If the two are different, their traffic is internally separated, as if occurring on individual switches with independent ports.

---

### *VM Pre-provisioning*

Use the VM Pre-Provision menu to add a VM in advance (prior to automatic discovery) into a group. Enter the MAC address of the VM and select the VSG to which it will be added. When the VM becomes active, it will be added to the selected group automatically.

### *Switch Management Ports*

This part of the window lists the ports that are reserved for switch management access. Listed ports are shown as part of the “Management” group.

# Virtual Switch Groups Settings

---

Use this window to configure the following features for VSGs:

- Delete the settings VSGs
- Switch Failover
- Link Aggregation Control Protocol (LACP)
- IGMP Snooping
- BPDU policy

## *Delete Virtual Switch Group Settings*

Use the Delete drop-down list to remove all settings for a specific VSG or all VSGs. This resets all configured settings for selected VSGs to their factory default values, including all VSG-related settings made in other windows throughout the BBI. Ports assigned to the VSG will be reassigned to default VSG 1. VMs and ACLs assigned to the VSG will be de-assigned.

## *Switch Failover*

The primary application for Layer 2 failover is to support Network Adapter Teaming. With Network Adapter Teaming, all the NICs on each server share the same IP address, and are configured into a team. One NIC is the primary link, and the other is a standby link.

You can configure VSGs as failover trigger groups such that if some (or all) of the links fail in a group, the SmartConnect software 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 SmartConnect software enables the internal ports. 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 switch processes traffic until the primary switch's internal links come up, which takes up to five seconds.

To configure Switch Failover (Layer 2 Failover) on a VSG:

1. **In the Switch Failover drop-down list, select *enable*.**
2. **In the Number of Links to Trigger Failover drop-down list, select the trigger value.**
3. **Click *Apply* at the bottom of the window to make the changes active, and *Save* to retain them beyond reboot and power cycles.**

### *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). If a link in a LACP trunk group fails, traffic is reassigned dynamically to the remaining link or links of the dynamic trunk.

To configure Link Aggregation Control Protocol on a VSG, select **enable** in the drop-down list. When disabled (as by default), external ports in the VSG's external trunk act as a static trunk. Click **Apply** to make the changes active, and **Save** to retain them beyond reboot.

### *IGMP Snooping*

To configure IGMP Snooping on a VSG, select **enable** in the drop-down list.

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.

### *BPDU Policy*

To configure the Spanning Tree BPDU policy for a VSG, select the desired policy, as follows:

- **drop**: If BPDUs are received on ports belonging to this group, the BPDUs are dropped.
- **guard**: If BPDUs are received on a port belonging to this group, the port is disabled.
- **flood**: If BPDUs are received on ports belonging to this group, the BPDUs are flooded on all ports in the group. Use this setting if the Switch Group's external ports are connected to upstream switches that have Spanning Tree enabled.

### *Reset to Default*

To reset items in this window for a specific VSG, select **Reset to default all group's settings**, and click **Apply**.

---

**Note** – This action will also de-assign any ACLs configured for the VSG.

---

**See also:**

- [“External Port Settings” on page 111](#)

## Virtual Switch Groups ACL QoS

---

Use this window to assign Access Control Lists (ACLs) or ACL Sets (group of ACLs) to a VSGs.

Assigning ACLs has the following prerequisites:

- A valid VSG must be configured (see [“Virtual Switch Groups Membership” on page 103](#)).
- A valid ACL or ACL set must be configured ([“ACL Configuration Table” on page 114](#) and [“Access Control List Sets” on page 119](#)).

Once prerequisites are met, an ACL or ACL Set can be applied to different port group combinations within a VSG, as follows:

- All Internal Ports
- All External Ports
- All ports in the Group

To add an ACL or ACL Set:

1. **Select the VSG from the ACL Config drop-down list.**
2. **Choose a port option in the Option drop-down list.**
3. **Click **Edit ACLs** to add an ACL to the VSG, or click **Edit ACL Sets** to add an ACL Set to the VSG.**

The ACLs Applied or ACL Sets Applied window will appear.

4. **Add or remove ACLs or ACL sets for the specified VSG ports.**
  - To add an ACL or ACL Set, select an item in the Available column and click Add.
  - To remove an ACL or ACL Set, select an item in the Group column and click Remove.
5. **Click **Apply** at the bottom of the window to make the changes active, and **Save** to retain them beyond reboot and power cycles.**



## CHAPTER 9

# Switch Policies

---

Switch Policies include configuration windows for the following port and access related features:

- “Internal Port Settings” on page 110
- “External Port Settings” on page 111
- “Management Port Settings” on page 112
- “Port Mirroring” on page 113
- “Access Control Lists” on page 114
- “Access Control List Sets” on page 119
- “Quality of Service” on page 120
- “ServerMobility” on page 122™

## Internal Port Settings

Use this window to configure internal port settings.

**Table 9-1** Internal Port Settings Fields

Field	Description
Port	Displays the port number. This field is non-configurable. <b>Note:</b> If the switch is part of a multi-switch stack, the displayed number indicates the Configured Switch number ( <i>csnum</i> ) followed by the port number. See <a href="#">“Stacking Port Numbers” on page 60</a> for more information.
Group	Displays the current VSG for the port. To configure the VSG, see <a href="#">“Virtual Switch Groups Membership” on page 103</a> .
Enable	Set the operational status of the port: enable or disable.
Name	Set the port name which appears on information and statistics displays.
Flow Control	Select the flow control setting (rx, tx, both, none).
PVID	Select the Port VLAN Identifier (PVID). If a PVID is configured, when untagged traffic ingresses on the port, the configured VLAN tag will be automatically added. Upon egress, if the PVID of the egress port matches the packets's tag, the tag will be stripped from the packet.
Internal Trunk ID	Configures the trunk ID for internal ports. Ports in the same VSG that have the same internal trunk ID form a trunk. Specify a value between 1 and 56, or 0 (zero) for none. <b>Note:</b> This field is available only when stacking is enabled.
DSCP Remarking	Enable or disable DiffServ Code Point (DSCP) remarking for the port (see <a href="#">“DiffServ Code Point QoS” on page 121</a> ).

If stacking is enabled, the View Ports drop-down list allows you to display all internal ports for all switches, all present switches, all defined switches, or a specific Configured Switch number.

### See also:

- [“Virtual Switch Groups Membership” on page 103](#)
- [“External Port Settings” on page 111](#)
- [“Port-Based VLAN Tagging” on page 30](#)
- [“Stacking” on page 45](#)
- [“DiffServ Code Point QoS” on page 121](#)

## External Port Settings

Use this window to configure external port settings.

**Table 9-2** External Port Settings Fields

Field	Description
Port	Displays the port number. This field is non-configurable. <b>Note:</b> If the switch is part of a multi-switch stack, the displayed number indicates the Configured Switch number (CSnum) followed by the port number. See <a href="#">“Stacking Port Numbers” on page 60</a> for details.
Group	Displays the current VSG for the port. To configure the VSG, see <a href="#">“Virtual Switch Groups Membership” on page 103</a> .
Name	Set the port name which appears on information and statistics displays.
Status	Set the operational status of the port: enable or disable.
Speed	Select the proper speed setting for the port. All external ports in the same VSG must have the same setting.
Duplex	Select the proper duplex setting for the port. All external ports in the same VSG must have the same setting.
Auto Negotiation	Select the proper auto-negotiation setting for the port. All external ports in the same VSG must have the same setting.
Flow Control	Select the flow control setting (rx, tx, both, none).
PVID	Select the Port VLAN Identifier (PVID). If a PVID is configured, when untagged traffic ingresses on the port, the configured VLAN tag will be automatically added. Upon egress, if the PVID of the egress port matches the packets's tag, the tag will be stripped from the packet.
ErrDisable Recovery	Enables or disables automatic recovery for the port when it becomes error-disabled. An error-disabled port is re-enabled by the switch only if this port setting is enabled and the global ErrDisable Recovery setting is also enabled (see <a href="#">“ErrDisable System Settings” on page 133</a> ).
DSCP Remarking	Enable or disable DiffServ Code Point (DSCP) remarking for the port (see <a href="#">“Diff-Serv Code Point QoS” on page 121</a> ).

**Note** – Some types of ports are pre-set for speed, duplex, and auto-negotiation. For these ports, settings are displayed but cannot be configured on this window.

If stacking is enabled, the View Ports drop-down list allows you to display all external ports for all switches, all present switches, all defined switches, or a specific Configured Switch number.

**See also:**

- [“Virtual Switch Groups Membership” on page 103](#)
- [“Internal Port Settings” on page 110](#)
- [“Stacking” on page 45](#)

## Management Port Settings

---

Use this window to configure management port settings.

**Table 9-3** Management Port Settings Fields

Field	Description
Port	Displays the port number. This field is non-configurable. <b>Note:</b> If the switch is part of a multi-switch stack, the displayed number indicates the Configured Switch number ( <i>csnum</i> ) followed by the port number. See <a href="#">“Stacking Port Numbers” on page 60</a> for more information.
Group	Displays the VSG for the port. as “Management.”
Port Name	Set the port name which appears on information and statistics displays.
Status	Set the operational status of the port: enable or disable.
Speed and Duplex	Select the proper speed and duplex setting for the port.
Flow Control	Select the flow control setting (rx, tx, both, none).

If stacking is enabled, the View Ports drop-down list allows you to display all management ports for all switches, all present switches, all defined switches, or a specific Configured Switch number.

**See also:**

- [“Virtual Switch Groups Membership” on page 103](#)
- [“Stacking” on page 45](#)

## Port Mirroring

---

Port mirroring allows you to attach a sniffer to a monitoring port that is configured to receive a copy of all packets forwarded from the mirrored port. SmartConnect enables you to mirror port traffic for all Layer 2 and Layer 3 traffic, including ports involved in VSG and stacking. Port mirroring can be used as a troubleshooting tool or to enhance the security of your network. For example, you can connect an IDS server to the monitor port to detect intruders attacking the network.

Consider the following guidelines while configuring port mirroring:

- SmartConnect does not support a single port being monitored by multiple ports.
- SmartConnect cannot mirror LACPDU and self-generated flow control packets.
- Ingress and egress traffic is duplicated and sent to the monitor port after processing.

---

**Note** – Among the egress ports, only one copy of broadcast and unknown unicast packets will go to the monitor port.

---

If stacking is enabled, the View Ports drop-down list allows you to display all ports for all switches, all present switches, all defined switches, or a specific Configured Switch number.

To configure port mirroring:

1. **At the top of the window, select a Monitor Port from the drop-down list.**
2. **For each port you wish to mirror:**
  - Select **Enabled** in the Mirrored drop-down list.
  - Select the port mirror Direction in the drop-down list.
    - In: Mirror only packets entering the target port.
    - Out: Mirror only packets exiting the target port.
    - Both: Mirror all packets entering or existing the target port.
3. **At the top of the window, select **Enabled** in the drop-down list.**
4. **Click **Apply** at the bottom of the window to make the changes active, and **Save** to retain them beyond reboot and power cycles.**

## Access Control Lists

---

Access Control Lists (ACLs) are used for limiting or permitting network traffic based on a variety of port, network, and traffic characteristics.

Use the [ACL Configuration Table](#) window to select or search for existing ACLs to view or edit, or to launch the window for configuring a new ACL.

Once ACLs or ACL sets are defined, see [“Virtual Switch Groups ACL QoS” on page 107](#) for assigning them to VSGs.

Also see [“Access Control List Sets” on page 119](#) for information on grouping ACLs together for quicker application.

### ACL Configuration Table

Existing ACLs are listed below the search fields on this window. The search fields can be used to narrow the displayed ACLs to those that match specified parameters.

#### *Searching for an Existing ACL*

**1. Enter the parameters (optional) of the ACL or ACLs you wish to locate:**

- Range of ACL IDs
- Set ID
- Switch Egress Unit
- Switch Egress Port
- Source MAC address
- Destination MAC address
- VLAN ID
- Protocol type
- Source IP address
- Destination IP address
- TCP/UDP source port
- TCP/UDP destination port
- Filter action
- Statistics

Fields that have a value of “any” are ignored during the search.

**2. Choose a search operation:**

- **or**  
Search for ACLs specified in the search range that meet any of the criteria entered.
- **and**  
Search for ACLs specified in the search range that meet all of the criteria entered.

**3. Click **Search** to display ACLs that fit the range and meet the criteria entered.**

Search results are displayed below the search criteria controls. Select any displayed ACL to view or edit its configuration using the [Access Control List](#) configuration window.

*Adding a New ACL*

Click Add New ACL to display the [Access Control List](#) configuration window.

**See also:**

- [“Virtual Switch Groups Membership”](#) on page 103
- [“Access Control List Sets”](#) on page 119

## Add or Edit ACLs

This configuration window is used for modifying existing ACLs or defining new ACLs. This window is reached from the [ACL Configuration Table](#) window.

### Access Control List

Use these fields to configure basic ACL parameters

**Table 9-4** ACL Configuration Fields

Field	Description
ACL ID	Configures the ACL number.
Filter Action	Defines the filter action, as follows: <ul style="list-style-type: none"> <li>■ Permit</li> <li>■ Deny</li> <li>■ None</li> </ul>
Ethernet Packet Format	Defines the Ethernet format for the ACL.
Tagging Packet Format	Defines the tagging format for the ACL.
IP Packet Format	Defines the IP addressing format for the ACL.
Source MAC Address	Defines the source MAC address for this ACL.
Destination MAC address	Defines the destination MAC address for this ACL.
Ethernet Type	Defines the Ethernet type and value for this ACL.
VLAN ID	Defines a VLAN number and mask for this ACL. <b>Note:</b> When this field is set, the ACL will match incoming packets only when they are tagged. Untagged packets will not be matched.
802.1p Priority	Defines the 802.1p priority for the ACL. <b>Note:</b> When this field is set, the ACL will match incoming packets only when they are tagged. Untagged packets will not be matched.
Type of Service	Defines a Type of Service value for the ACL. For more information on ToS, see RFC 1340 and 1349.
Protocol	Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Some of the well-known protocols include: <ul style="list-style-type: none"> <li>■ 1: ICMP</li> <li>■ 2: IGMP</li> <li>■ 6: TCP</li> <li>■ 17: UDP</li> <li>■ 89: OSPF</li> <li>■ 112: VRRP</li> </ul>

**Table 9-4** ACL Configuration Fields (continued)

Field	Description
Source IP Address	Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation.
Destination IP Address	Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.
TCP/UDP Src Port	Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Some of the well known ports include: <ul style="list-style-type: none"> <li>■ 20: ftp-data</li> <li>■ 21: ftp</li> <li>■ 22: ssh</li> <li>■ 23: telnet</li> <li>■ 25: smtp</li> <li>■ 37: time</li> <li>■ 42: name</li> <li>■ 43: whois</li> <li>■ 53: domain</li> <li>■ 69: tftp</li> </ul>
TCP/UDP Dst Port	Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with sport above.
TCP Flags	Defines a TCP flag for the ACL.
Statistics	Enables or disables the statistics collection for the ACL.
Egress Port	Selects an egress port to add to the ACL. <b>Note:</b> The egress port ACL will not match a Layer 2 broadcast/Multi-cast or Destination Lookup Failure (DLF) packet. Also, if the egress port is a member of a trunk, the ACL will be applied for all ports in that trunk.

### ACL Metering Settings

The following table describes the ACL metering configuration controls:

**Table 9-5** ACL Metering Configuration Fields

Field	Description
Committed rate	Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64.
Maximum burst size	Configures the maximum burst size, in Kilobits. Enter one of the following values for mbsize: 32, 64, 128, 256, 512, 1024, 2048, 4096
Set out-of-profile Drop or Pass	Configures the ACL Meter to either drop or pass out-of-profile traffic.
Enable	Enables or disables the ACL meter.

### ACL Remark Control

The following table describes the ACL remarking configuration controls:

**Table 9-6** ACL Remarking Configuration Fields

Field	Description
Set in-profile update DSCP enable	Enables or disables DiffServ Code Point (DSCP) updates for In-Profile packets.
Set in-profile update DSCP	Sets the DSCP of In-Profile packets to the selected value.
Set out-of-profile update DSCP enable	Enables or disables DSCP updates for Out-of-Profile packets.
Set out-of-profile update DSCP	Sets the DSCP of Out-of-Profile packets to the selected value.

#### See also:

- [“Virtual Switch Groups Membership” on page 103](#)
- [“Access Control List Sets” on page 119](#)

## Access Control List Sets

---

Use this window to assign ACLs to a set for quicker application.

To search for an ACL Set, enter a range of ACL Set numbers in the From and To fields. Click **Search** to display ACL Sets that fit the range.

The following table describes the ACL Sets configuration controls:

**Table 9-7** ACL Sets Configuration Fields

Field	Description
Set ID	Assigns a numeric identifier to the ACL Set.
ACLs Available	Lists the ACLs that you can add to the ACL Set. Select an ACL number in the ACLs Available list, and click <b>Add</b> to add the ACL to the ACL Set.
ACLs in Set	Lists the ACLs that belong to the ACL Set. Select an ACL number in the ACLs in Set list, and click <b>Remove</b> to remove the ACL from the ACL Set.

**See also:**

- [“Virtual Switch Groups Membership” on page 103](#)
- [“Access Control Lists” on page 114](#)

## Quality of Service

---

SmartConnect software supports two types of Quality of Service (QoS) classifications:

- “IEEE 802.1p for MAC-Level QoS” on page 120
- “DiffServ Code Point QoS” on page 121

### IEEE 802.1p for MAC-Level QoS

SmartConnect software supports the following configuration windows for IEEE 802.1p QoS classifications:

- “Priority CoS Configuration Table” on page 120
- “CoS Weight Configuration Table” on page 120
- “Port Priority Configuration” on page 120
- “Number of Cos Configuration” on page 120

#### Priority CoS Configuration Table

Use this window to map 802.1 priority to Class of Service queues (CoSq). For each 802.1p priority value (0-7), select a corresponding CoSq number.

#### CoS Weight Configuration Table

Use this window to configure the scheduling weight for each CoSq.

#### Port Priority Configuration

Use this window to configure the 802.1 priority for each switch port.

#### Number of Cos Configuration

Use this window to configure the number of Class of Service (CoS) queues available for use.

---

**Note** – If you change the number of CoS queues, you must **Save** the configuration and reset the switch for the change to take affect.

---

## DiffServ Code Point QoS

Use this configuration window to re-map DiffServ Code Point (DSCP) values.

**Table 9-8** DSCP Configuration Fields

Field	Description
DSCP	Lists the initial DSCP values.
New Mapped DSCP	Enter the new DSCP value to which the initial DSCP value will be mapped.

**See also:**

- [“Internal Port Settings” on page 110](#)
- [“External Port Settings” on page 111](#)
- [“IEEE 802.1p for MAC-Level QoS” on page 120](#)

## ServerMobility

---

The ServerMobility feature uses the DHCP Relay Agent information option (option 82) to support fixed server address allocation, based on host location. The Relay Agent information option allows the switch to append location information to packets sent to a DHCP server, as follows:

- Agent circuit ID sub-option encodes the chassis ID, in hexadecimal format. In the advanced management system, the chassis ID is displayed in the UUID field on the System Vital Product Data window (**Monitors > Hardware VPD**). The following example shows how the chassis ID is configured in the Agent circuit ID sub-option:  
4F:B2:F3:A8:6E:34:35:54:8B:0B:D8:2D:F2:B7:E9:49
- Agent remote ID sub-option encodes the switch slot number and the port ID that corresponds to the blade server, in hexadecimal. The following example shows how Slot ID 1 and Port Number 2 is configured in the Agent remote ID sub-option:  
01:0:0:0:02

SmartConnect software provides the following ServerMobility configuration windows:

- [“ServerMobility General Configuration” on page 123](#)
- [“ServerMobility Port Configuration” on page 124](#)

## ServerMobility General Configuration

Use this window to configure global settings for the ServerMobility feature.

**Table 9-9** ServerMobility - General Configuration Fields

Field	Description
Server Mobility State	Enables or disables the ServerMobility feature on the SmartConnect software.
Relay on Non-Server-Mobility Ports	Enables or disables BOOTP Relay for all ports that have ServerMobility disabled.
Auto-Recovery State	Enables or disables DHCP failover for the ServerMobility ports. When enabled, a backup blade server will get the same IP address as the active blade server if and when the active blade server goes down.
Auto_Recovery Failover Time	Sets the lease time for the temporary IP address assigned by the switch to a backup (standby) blade server while the active blade server is up.
Set Server Mobility configuration to factory default	Resets ServerMobility feature parameters to factory default values.

## ServerMobility Port Configuration

Use this window to configure ServerMobility feature settings for each port on the SmartConnect.

**Table 9-10** ServerMobility - Port Configuration Fields

Field	Description
Port	Identifies each port in the switch. <b>Note:</b> If the switch is part of a multi-switch stack, the displayed number indicates the Configured Switch number ( <i>csnum</i> ) followed by the port number. See “ <a href="#">Stacking Port Numbers</a> ” on page 60 for more information.
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.

If stacking is enabled, the View Ports drop-down list allows you to display all ports for all switches, all present switches, all defined switches, or a specific Configured Switch number.

## CHAPTER 10

# System Settings

---

The SmartConnect software provides configuration windows for the following system settings:

- “Management Settings” on page 126 for SNMP and Syslog settings
- “General Settings” on page 127 for system idle and watchdog timer settings
- “Local User Administration” on page 128 for defining switch user accounts
- “Remote User Administration” on page 130 for defining switch access using RADIUS or TACACS+.
- “Time Services Settings” on page 132 for local time and time zones, and configuring NTP.
- “ErrDisable System Settings” on page 133
- “Management Network Settings” on page 133 for defining the network through which switch management access is allowed.
- “Bootstrap Protocol Settings” on page 134 for BOOTP settings.
- “SSH/Telnet Settings” on page 135 for configuring Secure Shell and Telnet access settings
- “Virtual Machine Group Settings” on page 136 for enabling or disabling VM Groups, and for setting the VMware ESX heartbeat port.
- “Syslog Settings” on page 137 for setting the types of messages sent to the system log.
- “Stacking Configuration” on page 138 for binding individual switches to a stack, and for configuring the stack interface.

## Management Settings

---

Use this window to configure SNMP and System Log (syslog) settings.

### SNMP

SmartConnect supports SNMP-based network management. If you are running a SNMP network management station on your network, you can manage the SmartConnect using standard SNMP MIBs.

**Table 10-1** SNMP Management Fields

Field	Description
System Name	Defines the name for the system, up to 64 characters.
System Contact	Defines the name of the system contact, up to 64 characters.
System Location	Defines the name of the system location, up to 64 characters.
Read Community String	Defines the SNMP read community string, up to 32 characters. The read community string controls SNMP “get” access to the switch. The default read community string is <i>public</i> .
Write Community String	Defines the SNMP write community string, up to 32 characters. The write community string controls SNMP “set” and “get” access to the switch. The default write community string is <i>private</i> .

### System Log

SmartConnect software uses system log files to transmit event messages and alerts to a management host. A primary and secondary host may be defined.

**Table 10-2** Management Fields

Field	Description
IP Address	Configures the IP address of the syslog host.
Severity	Configures the severity level of the syslog host. The default is 7, which means log all severity levels.
Facility	Configures the facility level of the first syslog host displayed. The default value is 0.

# General Settings

---

Use this window to configure general switch settings.

**Table 10-3** General Configuration Fields

Field	Description
Idle Timeout	Sets the idle timeout for CLI sessions.
Enable/Disable Watchdog	Enables or disables the system watchdog. The system watchdog monitors system activity, and resets the switch if it becomes unresponsive.
Watchdog Timeout	Configures the watchdog reset interval, in seconds. A lower value means the switch resets after a shorter period of unresponsiveness.

## Local User Administration

---

SmartConnect software provides three built-in (static) user accounts, and up to ten end-user accounts. The Local User Administration window allow user accounts, passwords, and access levels to be defined, and allows the administrator to disconnect users from current switch access.

### *Built-In Users*

The following types of user accounts are always available:

- **User**  
The User has no direct responsibility for switch management. He or she can view all status information and statistics but cannot make any configuration changes to the switch.
- **Operator**  
The Operator manages various functions of the switch. The operator can view all information and statistics and can reset ports.
- **Administrator**  
The super-user 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.

**Table 10-4** Built-In User Administration Fields

Field	Description
Username	Displays the username for this user type.
Password	Sets the password for this user type, up to 15 characters.
User Type	Displays the authority level for the user type. SmartConnect defines these levels as: User, Operator, and Administrator, with User being the most restricted level.
Enabled	Enables or disables the user type.

## User Configuration

The administrator can define and manage up to ten end-user accounts. Depending on the user type specified for each account, the user can perform various operation tasks via the CLI commands. Once end-user accounts are configured and enabled, the SmartConnect software requires username/password authentication.

**Table 10-5** Local User Administration Fields

Field	Description
Username	Defines the user name, up to eight characters.
Password	Sets the user password of up to 15 characters maximum.
User Type	Configures the user's authority level. SmartConnect defines these levels as: User, Operator, and Administrator, with User being the most restricted level.
Enabled	Enables or disables the user.

## Ejecting Users

To disconnect a user from a current connection to the switch management interface, specify the username in the Eject field and click **Eject user**.

## Remote User Administration

---

Use this window to manage remote user authorization for RADIUS or TACACS+.

### RADIUS

SmartConnect software supports the RADIUS (Remote Authentication Dial-in User Service) method to authenticate and authorize remote administrators for managing the switch. The SmartConnect software acts as a RADIUS client and communicates to the RADIUS server which authenticates and authorizes a remote administrator.

**Table 10-6** RADIUS Fields

Field	Description
Radius	Enables or disables the RADIUS server.
Port	Displays the number of the User Datagram Protocol (UDP) port for RADIUS.
Radius Primary Server	Defines the primary RADIUS server IP address.
Radius Secondary Server	Defines the secondary RADIUS server IP address.
Radius Secret	Sets the shared secret between the switch and the RADIUS server(s).
Radius timeout	Displays the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed.
Radius retries	Displays the number of failed authentication requests before switching to a different RADIUS server.
Radius Backdoor for telnet/ssh/http/https	Displays the status of the RADIUS back door for Telnet/SSH/ HTTP/HTTPS.
Radius Secure Backdoor for telnet/ssh/http/https	Displays the status of the RADIUS back door using secure password for Telnet/SSH/ HTTP/HTTPS.

## TACACS+

SmartConnect software supports authentication and authorization using the Cisco Systems TACACS+ protocol.

**Table 10-7** TACACS+ Fields

Field	Description
TACACS+	Enables or disables the TACACS+ server.
Port	Displays the number of the TCP port for TACACS+.
TACACS+ Primary Server	Defines the primary TACACS+ server IP address.
TACACS+ Secondary Server	Defines the secondary TACACS+ server IP address.
TACACS+ Secret	Sets the shared secret between the switch and the TACACS+ server(s).
TACACS+ timeout	Displays the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed.
TACACS+ retries	Displays the number of failed authentication requests before switching to a different TACACS+ server.
TACACS+ Backdoor for telnet/ssh/http/https	Displays the status of the TACACS+ back door for Telnet. This command does not apply when secure backdoor is enabled.
TACACS+ Secure Backdoor for telnet/ssh/http/https	Displays the status of the TACACS+ back door using secure password for Telnet/SSH/ HTTP/HTTPS. This command does not apply when backdoor is enabled.
TACACS+ password change	Enables or disables TACACS+ password change.
TACACS+ command authorization	Displays the status of TACACS+ command authorization.
TACACS+ command logging	Displays the status of TACACS+ command logging.
TACACS+ new privilege level mapping	Displays the status of the TACACS+ new privilege-level mapping feature.

## Time Services Settings

Use this window to synchronize the SmartConnect's system clock to a Network Time Protocol (NTP) server.

### General Settings

**Table 10-8** Time Services General Settings Fields

Field	Description
Current Date	Configures the system date. The date reverts to its default value when the switch is reset.
Current Time	Configures the system time using a 24-hour clock format. The time reverts to its default value when the switch is reset.
Timezone Location	Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the time zone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Savings Time, etc.
DST for US	Enables or disables system Daylight Savings Time for USA prior to 2007.
Daylight Savings	Disables or enables daylight savings time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock.

### NTP Settings

**Table 10-9** Time Services NTP Fields

Field	Description
Time Services	Enables or disables the NTP synchronization service.
Update Interval	Specifies the time interval the switch waits re-synchronize the switch clock with the NTP server.
Primary Server	Configures the IP addresses of the primary NTP server to which you want to synchronize the switch clock.
Secondary Server	Configures the IP addresses of the secondary NTP server to which you want to synchronize the switch clock.

## ErrDisable System Settings

---

Use this window to configure the global ErrDisable settings.

**Table 10-10** ErrDisable Configuration Fields

Field	Description
Global ErrDisable Recovery	Enables or disables automatic recovery of error-disabled ports.
Global ErrDisable Timeout	Sets the time, in seconds, that the system waits before it automatically re-enables an error-disabled port.

## Management Network Settings

---

Use this window to add a defined network through which switch access is allowed through Telnet, SNMP, SSH, or the SmartConnect browser-based interface (BBI). A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation.

**Note:** If you configure the management network without including the switch interfaces, it will cause the Firewall Load Balancing health checks to fail and will create a “Network Down” state on the network.

**Table 10-11** Management Network Configuration Fields

Field	Description
Index	Displays the numeric ID of each management network entry.
Management Network Address	Configures the IP address of the management network.
Management Network Sub-net Mask	Configures the subnet mask of the management network.

## Bootstrap Protocol Settings

---

Use this window to configure BOOTP settings.

**Table 10-12** BOOTP Configuration Fields

Field	Description
BOOTP State	Globally enable or disable BOOTP relay on the switch.
BOOTP Server IP Address	Sets the IP address of the BOOTP server.
Secondary BOOTP Server IP Address	Sets the IP address of the second BOOTP server (optional).

## SSH/Telnet Settings

---

**Note** – For security purposes, the ability to change SSH and Telnet settings through the BBI is disabled by default and the fields in this window are subdued. To allow the BBI to make Telnet and SSH changes, use the following CLI command: `/cfg/sys/access/tsbbi enable`.

---

### Switch SSH Settings

Use these fields to configure Secure Shell (SSH) settings.

**Table 10-13** SSH Configuration Fields

Field	Description
SSH Time Interval	Set the interval for auto-generation of the RSA server key.
SSH Port	Sets the SSH server TCP port number.
SSH Generate Host Key	Generates the RSA host key.
SSH Generate Server Key	Generates the RSA server key.
SSH Server State	Enables or disables the SSH server.
SCP Admin Password	Set the administration password for SCP access.
SCP Apply and Save	Enables or disables SCP apply and save.

### Switch Telnet Settings

Use these fields to configure Telnet settings.

**Table 10-14** DSCP Configuration Fields

Field	Description
Telnet Access	Enables or disables Telnet access.
Telnet Port	Sets an optional telnet server TCP port number for cases where the server listens for telnet sessions on a non-standard port.

## Virtual Machine Group Settings

---

Use this window to configure VM Group settings.

**Table 10-15** VM Group Configuration Fields

Field	Description
Virtual Machine Groups	Enable or disable Virtual Machine Groups.
VMware ESX Service Console Heartbeat Port Number	The port number that the VMWare ESX server and VMware Virtual Console use to exchange heartbeat messages.

SmartConnect software VMready can identify ESX Service Console interfaces connected to internal ports. The Virtual Switch Group Information window displays an asterisk ( \* ) in the IP Address field for ESX Service Console entries.

VMready identifies Service Consoles by listening to heartbeat communication packets periodically transmitted by the Service Consoles to the VMware Virtual Center. If the default values used for the heartbeat communication are changed in the VMware environment of a data center, use this window to set a new heartbeat port.

### *See also:*

- [“Virtual Switch Groups Membership” on page 103](#)

## Syslog Settings

---

Use this screen to control the types of activity messages logged by the system, and whether or not they are sent to the system console in addition to being appended to the system log file.

Available activity message types are as follows:

- Syslog of Console messages
- Syslog of System messages
- Syslog of Management messages
- Syslog of CLI messages
- Syslog of VLAN messages
- Syslog of SSH messages
- Syslog of NTP messages
- Syslog of IP messages
- Syslog of WEB messages
- Syslog of CFG messages
- Syslog of Stacking messages
- Syslog of TFTP messages
- Syslog of Virtual Machine (VM) messages

Each message type can be independently enabled or disabled.

## Stacking Configuration

Stacking allows up to eight switches to act as a single logical unit for aggregating bandwidth. Initial configuration of stacking is performed using a combination of CLI and BBI commands (see “Stacking” on page 45). The BBI provides the following stacking configuration options.

- “Stack Switch Configuration” on page 138
- “Stack IP Interfaces” on page 139
- “Managing a Stack” on page 59

### Stack Switch Configuration

The following settings are available for the overall stack:

**Table 10-16** Stack Switch Configuration Fields

Field	Description
Stack Name	Set a name for the stacked switch (optional).
Master Switch	Information showing the Master switch Configured Switch number ( <i>csnum</i> ). This field is non-configurable.
Backup Switch	The Backup takes over control of the stack if the Master fails. Configuration information and run-time data are synchronized with the Master.

For each configured switch in the stack, the following fields are available:

**Table 10-17** Stack Switch Configuration Fields

Field	Description
Bind asnum	Select an attached switch number ( <i>asnum</i> ) from the drop-down menu to bind it the configured switch number ( <i>csnum</i> , shown in the title for each set of switch parameters).
UUID	This is the Unit ID number of the blade server chassis where the switch resides. This field is non-configurable.
Bay number	This is the bay number of the blade server chassis where the switch resides. This field is non-configurable.
Delete	To remove the target switch from the stack, check this box and click <b>Apply</b> .

**See also:**

- “Stack IP Interfaces” on page 139
- “Managing a Stack” on page 59

## Stack IP Interfaces

Use the Stack IP Interfaces window to configure a single IP interface for the stack. This interface is known at the master interface and is shared by all switches in the stack.

Enter the following information for the master and backup stacking IP interfaces:

**Table 10-18** Master Switch Interface Fields

Field	Description
IP Address	Define the IP address used for the stack entity.
Subnet Mask	Use the mask to define an IP address range for the interface.
Group	Assign the interface to a Virtual Switch Group (VSG).
Smvlan	Assign the interface to specific VLAN.
Default Gateway Address	Define a default IP gateway for the interface.
Delete	To remove the interface settings from the stack, check this box and click <b>Apply</b> .

Click **Apply** to make your changes active, and **Save** to retain changes beyond reboot cycles.

To delete an interface, check the appropriate **Delete** box and click **Apply**.

---

**Note** – If no Backup Switch Interface is configured, the Master Switch Interface is used if the Backup switch takes over operation of the stack. Gratuitous ARP for the backup IP address is sent out to the network when a failover to the Backup switch occurs.

---

This screen also displays information about the management IP interface:

- IP address and subnet mask
- Default gateway IP address
- Default VLAN number

### *See also:*

- [“Stack Switch Configuration” on page 138](#)
- [“Managing a Stack” on page 59](#)



## CHAPTER 11

# Boot Management

---

Use the Boot Management window to manage SmartConnect software. The Boot Management window allows you to perform the following tasks:

- **General Boot Settings:**
  - Reboot the switch, or if stacking is enabled, reboot the entire stack, the Master switch, or individual member switches.
  - View information about the currently installed software and configuration images.
  - Select a configuration block and software image to be used when the switch is next reset.
  - Load a new software image on the SmartConnect switch via FTP, TFTP, or HTTP.
  - Obtain a dump of switch information needed during technical support.
- **Boot Schedule:** Set a time when the switch will next reset.

## General Boot Settings

---

Use the General Boot Settings configuration window to reboot switches, update switch software, and to select software and configuration images.

### *Rebooting Switches*

The following table describes the reboot buttons on the Boot Management window.

**Table 11-1** Boot Management Reboot buttons

Field	Description
Reboot the Module	Performs a software reboot/reset. This button appears only on switches where the stacking features is disabled (as by default).
Reboot Stack	Available only when stacking is enabled. This performs a software reboot/reset for all switches in the stack.
Reboot Master	Available only when stacking is enabled. This performs a software reboot/reset for the active Master switch in the stack. If a Backup is configured and available, the Backup will assume control of the stack.
Reboot Switches	Available only when stacking is enabled. This performs a software reboot/reset for any stack switches selected in the accompanying switch list.

### *Viewing Current Software Information*

The Current Image Information contains the current version number, download date, and name of each software image loaded into the switch.

### *Selecting Configuration and Software Images*

When the system restarts, the software image specified in the “Image to boot” drop-down list becomes the active image, and the configuration block specified in the “Next config boot block” becomes the active configuration.

If stacking is enabled, the Master switch will synchronize the selected software image and configuration with all Member switches in the stack when it starts.

### *Downloading or Uploading Software Images and Configuration Files*

Perform the following steps to load a software image to the SmartConnect switch:

- 1. In the “Image to transfer” drop-down list, select the software image you wish to replace.**

## 2. In the Update Image/Cfg section, perform the following steps:

- Select the method to use for transfer from the drop-down list.  
Choices are TFTP or FTP for transferring files from a remote server, or HTML for using the browser to transfer files from the local computer and attached file systems.
- Enter the appropriate information to use for the file transfer, such as the file location and any login information, if necessary.

## 3. Click Get Image.

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

## 4. Activate the new software.

In the “Image to boot” field, select the newly loaded image. Restart the switch using one of the following methods, depending on your switch configuration:

- If the switch is operating independantly (stacking disabled), click **Reboot** to restart the switch.
- If stacking is enabled, click **Reboot Stack**. When the stack restarts, the Master switch will synchronize the updated software with all Member switches in the stack.

Software images and configuration files can be tranfered to or from remote servers. The following table describes the image and configuration buttons on the Boot Management window.

**Table 11-2** Boot Management Image and Configuration buttons

Field	Description
Get Image	Loads the software image specified in the Remote File Name field to the switch. Places the software in the block specified in the Image to transfer drop-down list.
Put Image	Loads the software image specified in the Image to transfer drop-down list to the remote server. Places the software in the file name specified in the Remote File Name field.
Get Cfg	Loads a configuration file specified in the Remote File Name field from the remote server to the switch. Places the configuration file into the active configuration block.
Put Cfg	Loads the active configuration file to the remote server. Places the configuration into the file name specified in the Remote File Name field.

## Obtaining Support Dumps

Support dumps contain detailed diagnostic information about the state of the switch software. When working with BLADE customer support, the administrator may be asked to provide dump files. The following table describes the support dump buttons.

**Table 11-3** Boot Management Support Dump buttons

Field	Description
Put TS Dump	Loads the technical support dump file to the remote Server Address specified in the Update Image/Cfg section of the page. Places the dump into the file specified in the Remote File Name field.
Put Crash Dump	Loads the switch system crash dump file to the remote Server Address specified in the Update Image/Cfg section of the page. Places the dump into the file specified in the Remote File Name field.
Clear Crash Dump	Clears the switch system crash dump.

### See also:

- [“Boot Schedule” on page 144](#)

## Boot Schedule

Use this window to schedule a specific time for a system reboot.

**Table 11-4** Boot Schedule Fields

Field	Description
Enter day of the week for reboot	Configures the day of the week of the scheduled reboot.
Enter hour in 24-hour format (0...23)	Configures the hour of the scheduled reboot.
Enter minutes (0...59)	Configures the minute of the scheduled reboot.
Cancel scheduled reboot?	Select “cancel” if you want to cancel a scheduled reboot.
Currently scheduled reboot time	Displays the current scheduled time and date.

### See also:

- [“General Boot Settings” on page 142](#)

## CHAPTER 12

# Switch Information

---

The following windows display information about switch settings and operational status:

- “Access Control List Information” on page 146
- “Access Control List Sets Information” on page 146
- “ARP Cache Information” on page 147
- “Bootstrap Protocol Relay Information” on page 148
- “Forwarding Database Information” on page 148
- “Virtual Switch Group Information” on page 150
- “IGMP Information” on page 151
- “IP Information” on page 152
- “Link Status Information” on page 153
- “ServerMobility” on page 154
- “SNMPv3 Information” on page 156
- “Syslog Messages” on page 158
- “Port Transceiver Status” on page 159
- “Trunk Groups Information” on page 159
- “User Information” on page 160
- “Virtual Machine Group Information” on page 160

## Access Control List Information

---

Use this screen to view information about existing Access Control Lists (ACLs).

Initially, all ACLs configured on the switch are displayed. Use the optional search fields to narrow the list to show only those ACLs that match specific parameters. To reset the search to include all ACLs, click **Reset**.

To view the configuration details of a listed ACL, click the ACL number.

### *See also:*

- [“Access Control Lists” on page 114](#)
- [“Access Control List Sets” on page 119](#)
- [“Virtual Switch Groups ACL QoS” on page 107](#)

## Access Control List Sets Information

---

Use this window to display ACL Set information.

Initially, this window displays a list of all ACL Sets configured on the switch. Use the optional “From” and “To” fields to list only ACLs within the specified set range. To reset the search to include all ACL Sets, click **Reset**.

To view the configuration details of a listed ACL Set, click the Set number.

### *See also:*

- [“Access Control Lists” on page 114](#)
- [“Access Control List Sets” on page 119](#)
- [“Virtual Switch Groups ACL QoS” on page 107](#)

## ARP Cache Information

This window displays ARP cache information.

Initially, this window displays a list of all ARP cache entries on the switch. To narrow the list to specific parameters, use the optional search fields and click **Submit**. The following search fields are available:

**Table 12-1** ARP Cache Information Search Fields

Field	Description
Show Entries of a Specific Port	View only the ARP entries associated with a specific switch port. Select <b>any</b> to remove the search restriction.
Show Entries of a Specific Group	View only the ARP entries associated with a specific Virtual Switch Group (VSG). Enter <b>0</b> to remove the search restriction.
Show Entries of a Specific VLAN	View only the ARP entries associated with a specific VLAN. Enter <b>0</b> to remove the search restriction.
Show Entries of a Specific IP Address	View only the ARP entries associated with a specific IP Address. Enter <b>0 . 0 . 0 . 0</b> to remove the search restriction.

The following table describes the information fields for listed ARP cache entries.

**Table 12-2** ARP Cache Information Fields

Field	Description
Entry #	Displays the numeric identifier of the ARP entry.
IP Address	Displays the IP address of the ARP entry.
Flags	Displays the address status flag for the ARP entry.
MAC Address	Displays the MAC address of the ARP entry.
Group	Displays the VSG of the ARP entry.
Vlan	Displays the VLAN number of the packet where the ARP entry request is received.
Port	Displays the source port number of the ARP entry. <b>Note:</b> If the switch is part of a multi-switch stack, the displayed number indicates the Configured Switch number ( <i>csnum</i> ) followed by the port number. See “ <a href="#">Stacking Port Numbers</a> ” on page 60 for more information.
Age	Displays the number of seconds before the ARP entry expires.

To clear the ARP cache, click **Clear ARP Cache**.

## Bootstrap Protocol Relay Information

---

The following table describes the BOOTP Relay information fields.

**Table 12-3** BOOTP Relay Information Fields

Field	Description
BOOTP State	Displays the BOOTP status (enabled or disabled).
BOOTP Server IP Address	Displays the IP address of the BOOTP server.
Secondary BOOTP Server IP Address	Displays the IP address of the secondary BOOTP server.

This window displays information about the blade chassis in which the switch resides.

## Forwarding Database Information

---

This window displays Forwarding Database (FDB) information.

Initially, this window displays a list of all FDB entries on the switch. To narrow the list to specific parameters, use the optional search fields and click **Submit**. The following search fields are available:

**Table 12-4** FDB Information Search Fields

Field	Description
Show Entries of a Specific Port	View only the FDB entries associated with a specific switch port. Select <b>any</b> to remove the search restriction.
Show Entries of a Specific State	View only the FDB entries associated with a specific state (unknown, forward, or trunk). Select <b>any</b> to remove the search restriction.
Show Entries of a Specific Group	View only the FDB entries associated with a specific VSG. Enter <b>0</b> to remove the search restriction.
Show Entries of a Specific Trunk	View only the FDB entries associated with a specific trunk. Enter <b>0</b> to remove the search restriction.
Show Entries of a Specific MAC Address	View only the FDB entries associated with a specific MAC Address. Enter <b>00:00:00:00:00:00</b> to remove the search restriction.

The following table describes the information fields for the listed FDB entries.

**Table 12-5** FDB Information Fields

Field	Description
Entry #	Displays the numeric identifier of the FDB entry.
MAC Address	Displays the MAC address of the FDB entry.
Group	Displays the VSG number on which the MAC was learned. If the entry was learned on a management port, the field displays Mgmt.
Port	Displays the VLAN number of the FDB entry.
Trunk	Displays the trunk number of the FDB entry, if applicable.
State	Displays the port state of the FDB entry.
Delete	Clear the specific FDB entry.

To clear all displayed FDB entries, click **Clear**. If the FDB list is narrowed using the search parameters, only those FDB entries in the resulting list are cleared.

## Virtual Switch Group Information

---

This window displays information about VSGs.

Initially, all VGSs are displayed. Use the View drop-down list to view information for a specific VSG, or for all “non-empty” VSGs (those with ports assigned).

The following table describes the VSG information fields.

**Table 12-6** Virtual Switch Group Information Fields

Field	Description
VM MAC Address	Displays a list of the MAC addresses of Virtual Servers that are members of the VSG. Optional.
Internal Ports	Displays a list of the internal port members in the VSG. Optional.
Ports in External Trunk 1	Displays a list of external ports that are members of the first external trunk of the VSG.
Ports in External Trunk 2	Displays a list of external ports that are members of the second external trunk of the VSG.
Oper Disabled External Ports	Displays a list of ports that were disabled due to trunk policy because of different type ports member in same external trunk or too many ports of same type member in same external trunk.
External Trunk 1	Displays the trunk group number and status (enabled or disabled) of the first external trunk of the VSG.
External Trunk 2	Displays the trunk group number and status (enabled or disabled) of the second external trunk of the VSG.
LACP	Displays the LACP status of the VSG (enabled or disabled).
IGMP	Displays the status of IGMP Snooping for the VSG (enabled or disabled).
Failover	Displays the Failover status of the VSG (enabled or disabled)
Failover Limit	Displays the number of ports in the VSG that must fail before Failover occurs.
BPDU Policy	Displays the BPDU Policy setting (drop, guard, or flood).
ACL SCM Group config	Displays the ACLs configured for the group.

---

**Note** – For port numbers, if a switch is part of a multi-switch stack, the displayed number indicates the Configured Switch number (*csnum*) followed by the port number. See “[Stacking Port Numbers](#)” on page 60 for more information.

---

## IGMP Information

### IGMP Multicast Groups

The following table describes the IGMP Multicast Groups information fields.

**Table 12-7** IGMP Multicast Groups information

Field	Description
MCGroup	Displays the IP address of the IGMP Multicast Group.
Group	Displays the VSG number.
Vlan	Displays the VLAN number of the IGMP Multicast Group.
Port	Displays the port numbers of ports that carry IGMP Multicast traffic for the group. <b>Note:</b> If a switch is part of a multi-switch stack, the displayed number indicates the Configured Switch number ( <i>csnum</i> ) followed by the port number. See <a href="#">“Stacking Port Numbers” on page 60</a> for more information.
Version	Displays the IGMP version.
Expires	Displays the time remaining until a Mrouter port is deleted from the Multicast IGMP table.

### IGMP Snooping Multicast Router Ports

The following table describes the IGMP Multicast Router Ports information fields.

**Table 12-8** Mrouter Ports information

Field	Description
Group	Displays the VSG number.
VLAN	Displays the VLAN number of the IGMP Multicast Group.
Port	Displays the port numbers of ports that carry IGMP Multicast traffic for the group. <b>Note:</b> If a switch is part of a multi-switch stack, the displayed number indicates the Configured Switch number ( <i>csnum</i> ) followed by the port number. See <a href="#">“Stacking Port Numbers” on page 60</a> for more information.
Version	Displays the IGMP version.
Expires	Displays the time remaining until a Mrouter port is deleted from the Multicast IGMP table.
Max Query Resp. Time	Displays the snooped value of the Maximum Response Time in IGMP query packet.

## IP Information

---

### *IP Interfaces*

The following table describes the IP information fields.

**Table 12-9** Interface information

Field	Description
Status	Shows the IP Interface status: enabled, disabled, or enabled but down.
IP Interface ID	Displays the numeric identifier of the IP Interface.
IP Address	Displays the IP address of the IP Interface.
Subnet Mask	Displays the Subnet Mask of the IP Interface.
Broadcast Address	Displays the IP Broadcast address for this IP Interface.
Group	Displays the VSG of the interface.
SMVLAN	Displays the VLAN number for this interface. Each interface can belong to one VLAN, although any VLAN can have multiple IP interfaces in it.

### *Default Gateways*

The following table describes the Default Gateway information fields.

**Table 12-10** Default Gateway information

Field	Description
Default Gateway ID	Displays the ID number of the default gateway.
IP Address	Displays the gateway IP address.
Status	Displays the operational status of the gateway (enabled or disabled).

## Link Status Information

---

The following table describes the Link Status information fields.

**Table 12-11** Link Status information

Field	Description
Port	Displays the port name and number. <b>Note:</b> If a switch is part of a multi-switch stack, the displayed number indicates the Configured Switch number ( <i>csnum</i> ) followed by the port number. See <a href="#">“Stacking Port Numbers” on page 60</a> for more information.
Speed	Displays the port speed.
Duplex	Displays the port duplex mode (half, full, or any)
Flow Control	Displays the port's flow control setting (yes or no)
Link	Displays the port's link status (up, down, disabled)

## ServerMobility

---

These windows display information about the ServerMobility feature:

- [“ServerMobility General Information” on page 154](#)
- [“ServerMobility Port Information” on page 155](#)

### ServerMobility General Information

The following table describes the general ServerMobility information fields.

**Table 12-12** ServerMobility General information

Field	Description
ServerMobility settings	Displays the current ServerMobility status (enabled or disabled).
ServerMobility Encoding Scheme	Displays the current scheme used for encoding the Client Identifier (option 61) and Relay Agent Information (option 82) in DHCP request packets.
ServerMobility ports	Displays the ports that have ServerMobility enabled.
DHCP request filtering enabled ports	Displays the ports on which filtering of DHCP request information is enabled.
Relay on non-ServerMobility ports	Displays the current BOOTP relay status (enabled or disabled) for all ports that have ServerMobility disabled.
Active-Backup ports	Displays the active ServerMobility ports and their backup ports.
Auto-Recovery	Displays the current DHCP failover status (enabled or disabled) of ServerMobility ports.
Auto-Recovery Time	Displays the current lease time of the temporary IP addresses that are assigned by the switch to blade servers connected to a backup (standby) ServerMobility ports.

---

**Note** – For port numbers, if a switch is part of a multi-switch stack, the displayed number indicates the Configured Switch number (*csnum*) followed by the port number. See [“Stacking Port Numbers” on page 60](#) for more information.

---

#### See also:

- [“ServerMobility General Configuration” on page 123](#)
- [“ServerMobility Port Information” on page 155](#)

## ServerMobility Port Information

The following table describes the ServerMobility Port information fields.

**Table 12-13** Server Mobility Port information

Field	Description
client-id	Displays the client identifier value (option 61) that will be encoded by the switch in the DHCP request packets received on the port.
agent.circuit-id	Displays the relay agent circuit ID sub-option value that will be encoded in the DHCP request packets received on the port.
agent.remote-id	Displays the relay agent remote ID sub-option value that will be encoded in the DHCP request packets received on the port.
Server Mobility	Displays the current ServerMobility status of the port (enabled or disabled).
Filtering	Displays the current DHCP filtering status of the port (enabled or disabled).
Failover Port	Displays the backup port or the active port associated with the port.
Failover State	<p>Displays the current failover status of the port, as follows:</p> <ul style="list-style-type: none"> <li>■ active</li> <li>■ standby</li> <li>■ fail</li> </ul> <p>If the failover state of the port is <i>active</i>, DHCP requests received on the port will be relayed by the switch.</p> <p>If the failover state is <i>standby</i> or <i>fail</i>, the DHCP requests will not be relayed. The switch will respond to DHCP requests received on standby ports with a temporary IP address.</p>

### See also:

- [“ServerMobility General Configuration” on page 123](#)
- [“ServerMobility Port Information” on page 155](#)

## SNMPv3 Information

The following table describes the SNMPv3 information fields.

**Table 12-14** SNMPv3 information

Field	Description
Engine ID	Displays the unique identifier for the SNMP engine.
<b>usmUser Table</b>	
User Name	This text string represents the name of the user that you can use to access the switch.
Authentication Protocol	This indicates whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol which is used. SmartConnect software supports two authentication algorithms: MD5 and HMAC-SHA.
Privacy Protocol	This indicates whether messages sent on behalf of this user are protected from disclosure, and if so, the type of privacy protocol which is used. SmartConnect software supports DES algorithm for privacy.
<b>vacmAccess Table</b>	
Group Name	Displays the name of group.
Prefix	Displays the prefix that is configured to match the values.
Model	Displays the security model used, for example, SNMPv1, or SNMPv2 or USM.
Level	Displays the minimum level of security required to gain rights of access. For example, <i>noAuthNoPriv</i> , <i>authNoPriv</i> , or <i>authPriv</i> .
Match	Displays the match for the <i>contextName</i> . The options are: <i>exact</i> and <i>prefix</i> .
ReadV	Displays the MIB view to which this entry authorizes the read access.
WriteV	Displays the MIB view to which this entry authorizes the write access.
NotifyV	Displays the Notify view to which this entry authorizes the notify access.
<b>vacmViewTreeFamily Table</b>	
View Name	Displays the name of the view.
Subtree	Displays the MIB subtree as an OID string. A view subtree is the set of all MIB object instances which have a common Object Identifier prefix to their names.
Mask	Displays the bit mask.

Table 12-14 SNMPv3 information (continued)

Field	Description
Type	Displays whether a family of <i>view subtrees</i> is included or excluded from the MIB view.
<b>vacmSecurityToGroup Table</b>	
Sec Model	Displays the security model used, which is any one of: <i>USM</i> , <i>SNMPv1</i> , <i>SNMPv2</i> , and <i>SNMPv3</i> .
User Name	Displays the name for the group.
Group Name	Displays the access name of the group.
<b>snmpCommunity Table</b>	
Index	Displays the unique index value of a row in this table.
Name	Displays the community string, for which a row in this table represents the configuration.
User Name	Displays the User Security Model (USM) user name.
Group Name	To be added
<b>snmpCommunity Table</b>	
Index	Displays the unique index value of a row in this table
Name	Displays the community string, which represents the configuration.
User Name	Displays the User Security Model (USM) user name.
Tag	Displays the community tag. This tag specifies a set of transport end-points from which a command responder application accepts management requests and to which a command responder application sends a SNMP trap.
<b>snmpNotify Table</b>	
Name	The locally arbitrary, but unique identifier associated with this <i>snmpNotifyEntry</i> .
Tag	This represents a single tag value which is used to select entries in the <i>snmpTargetAddrTable</i> . Any entry in the <i>snmpTargetAddrTable</i> that contains a tag value equal to the value of this entry, is selected. If this entry contains a value of zero length, no entries are selected.
<b>snmpTargetAddr Table</b>	
Name	Displays the locally arbitrary, but unique identifier associated with this <i>snmpTargetAddrEntry</i> .
Transport Addr	Displays the transport addresses.
Port	Displays the SNMP UDP port number.

**Table 12-14** SNMPv3 information (continued)

Field	Description
Taglist	This column contains a list of tag values which are used to select target addresses for a particular SNMP message.
Params	The value of this object identifies an entry in the <i>snmpTargetParamsTable</i> . The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address.
<b>snmpTargetParams Table</b>	
Name	Displays the locally arbitrary, but unique identifier associated with this <i>snmpTargetParamsEntry</i> .
MP Model	Displays the Message Processing Model used when generating SNMP messages using this entry.
User Name	Displays the <i>securityName</i> , which identifies the entry on whose behalf SNMP messages will be generated using this entry.
Sec Model	Displays the security model used when generating SNMP messages using this entry. The system may choose to return an <i>inconsistentValue</i> error if an attempt is made to set this variable to a value for a security model which the system does not support.
Sec Level	Displays the level of security used when generating SNMP messages using this entry.

## Syslog Messages

This window lists the most recently logged system messages.

**See also:**

- [“Syslog Settings” on page 137](#)

## Port Transceiver Status

The following table describes the Transceiver information fields.

**Table 12-15** Transceiver information

Field	Description
Port	Displays the port number and SFP/XFP number.
Device	Displays the transmission media and device type for the port, as follows: <ul style="list-style-type: none"> <li>■ Media:               <ul style="list-style-type: none"> <li><input type="checkbox"/> CU (Copper SFP)</li> <li><input type="checkbox"/> FI (Fiber SFP)</li> <li><input type="checkbox"/> SR (Short Range XFP)</li> <li><input type="checkbox"/> LR (Long Range XFP)</li> </ul> </li> <li>■ Device: SFP or XFP module</li> </ul>
TX-Enable	Displays the transmission status of the module (enabled or disabled).
RX-Signal	Displays the link state of the module port (OK or LOST).
TX-Fault	Displays the fault status of the module (none or FAULT).

## Trunk Groups Information

The following table describes the Trunk Group (Portchannel) information fields.

**Table 12-16** Trunk Group information

Field	Description
Trunk Group	Displays the Trunk number.
Protocol	Displays the protocol used by the trunk (static or LACP)
Virtual Switch Group	Displays the VSG supported by the trunk.
Switch Port	Lists the port members of the trunk. <b>Note:</b> If a switch is part of a multi-switch stack, the displayed number indicates the Configured Switch number ( <i>csnum</i> ) followed by the port number. See <a href="#">“Stacking Port Numbers” on page 60</a> for more information.
Status	Displays the status of the trunk.

## User Information

---

The following table describes the User information fields.

**Table 12-17** User Access information

Field	Description
User ID	Displays the numeric identifier for the user.
User Name	Displays the name of the user.
COS	Displays the Class of Service level for the user.
Password	Indicates whether a valid password is defined for the user.
Status	Displays whether the user is enabled or disabled.
Login	Displays the login status of the user (online or offline).

Built-in user accounts are always available. This page lists the built-in accounts, and displays the status (enabled or disabled) and whether a user is online or offline.

## Virtual Machine Group Information

---

The following table describes the VM Group information fields.

**Table 12-18** VM Group information

Field	Description
IP Address	Displays the IP address of the Virtual Machine.
MAC Address	Displays the MAC address of the Virtual Machine.
Port	Displays the switch port where the Virtual Machine is connected.
VLAN	Displays the VLAN of the Virtual Machine.
Group	Displays the VSG to which the Virtual Machine belongs.

### *See also:*

- [“Assigning Virtual Machines to VSGs” on page 103](#)
- [“VM Pre-provisioning” on page 104](#)

## CHAPTER 13

# Switch Statistics

---

These windows provide collective packet and event counters for a variety of switch transactions:

- “Access Control List Statistics” on page 161
- “FDB Statistics” on page 162
- “Layer 3 Statistics” on page 162
- “IGMP Group Snooping Statistics Summary” on page 166
- “IP Statistics” on page 167
- “MP-Specific Information” on page 168
- “Network Time Protocol Statistics” on page 170
- “Port Statistics” on page 170

## Access Control List Statistics

---

The following table describes the ACL statistics fields.

**Table 13-1** ACL Statistics

Field	Description
ACL	Numeric identifier of each ACL.
Hits	Number of times the ACL was activated.
Clear	To be added

## FDB Statistics

---

The following table describes the Forwarding Database statistics fields.

**Table 13-2** FDB Statistics

Field	Description
current	Current number of entries in the Forwarding Database.
hiwat	Highest number of entries recorded at any given time in the Forwarding Database.

To clear FDB statistics, select **Clear** in the Clear FDB Statistics field and click **Submit**.

## Layer 3 Statistics

---

### *Address Resolution Protocol Statistics*

The following table describes the Address Resolution Protocol statistics fields.

**Table 13-3** ARP Statistics

Field	Description
Current Entries	The total number of outstanding ARP entries in the ARP table.
High Water Mark	The highest number of ARP entries ever recorded in the ARP table.
Maximum Entries	The maximum number of ARP entries that are supported.

To clear ARP statistics, select **clear** in the Clear ARP Statistics field and click **Submit**.

## ICMP Statistics

The following table describes the ICMP statistics fields.

**Table 13-4** ICMP Statistics

Field	Description
icmpInMsgs	The total number of ICMP messages which the entity (the switch) received. Note that this counter includes all those counted by <code>icmpInErrors</code> .
icmpInErrors	The number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so forth).
icmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
icmpInTimeExcds	The number of ICMP Time Exceeded messages received.
icmpInParmProbs	The number of ICMP Parameter Problem messages received.
icmpInSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages received.
icmpInRedirects	The number of ICMP Redirect messages received.
icmpInEchos	The number of ICMP Echo (request) messages received.
icmpInEchoReps	The number of ICMP Echo Reply messages received.
icmpInTimestamps	The number of ICMP Timestamp (request) messages received.
icmpInTimestampReps	The number of ICMP Timestamp Reply messages received.
icmpInAddrMasks	The number of ICMP Address Mask Request messages received.
icmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
icmpOutMsgs	The total number of ICMP messages which this entity (the switch) attempted to send. Note that this counter includes all those counted by <code>icmpOutErrors</code> .
icmpOutErrors	The number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
icmpOutSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages sent.

**Table 13-4** ICMP Statistics (continued)

Field	Description
icmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
icmpOutEchos	The number of ICMP Echo (request) messages sent.
icmpOutEchoReps	The number of ICMP Echo Reply messages sent.
icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

To clear ICMP statistics, select **clear** in the Clear ICMP Statistics field and click **Submit**.

### TCP Statistics

The following table describes the TCP statistics fields.

**Table 13-5** TCP Statistics

Field	Description
tcpRtoAlgorithm	The algorithm used to determine the <code>timeout</code> value used for retransmitting unacknowledged octets.
tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission <code>timeout</code> , measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission <code>timeout</code> . In particular, when the <code>timeout</code> algorithm is <code>rsre(3)</code> , an object of this type has the semantics of the LBOUND quantity described in RFC 793.
tcpRtoMax	The maximum value permitted by a TCP implementation for the retransmission <code>timeout</code> , measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission <code>timeout</code> . In particular, when the <code>timeout</code> algorithm is <code>rsre(3)</code> , an object of this type has the semantics of the UBOUND quantity described in RFC 793.
tcpMaxConn	The limit on the total number of TCP connections the entity (the switch) can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
tcpActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

**Table 13-5** TCP Statistics (continued)

Field	Description
tcpAttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
tcpEstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
tcpInSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	The total number of segments received in error (for example, bad TCP checksums).
tcpCurBuff	The total number of outstanding memory allocations from heap by TCP protocol stack.
tcpCurConn	The total number of outstanding TCP sessions that are currently opened.
tcpOutRsts	The number of TCP segments sent containing the RST flag.

To clear TCP statistics, select **clear** in the Clear TCP Statistics field and click **Submit**.

### UDP Statistics

The following table describes the UDP statistics fields.

**Table 13-6** UDP Statistics

Field	Description
udpInDatagrams	The total number of UDP datagrams delivered to the switch.
udpOutDatagrams	The total number of UDP datagrams sent from this entity (the switch).
udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.

To clear UDP statistics, select **clear** in the Clear UDP Statistics field and click **Submit**.

## IGMP Group Snooping Statistics Summary

---

The following table describes the IGMP Snooping statistics fields.

**Table 13-7** IGMP Snooping Statistics

Field	Description
Group #	Displays the Switch Group number.
rxIgmpValidPkts	Total number of valid IGMP packets received
rxIgmpInvalidPkts	Total number of invalid packets received
rxIgmpGenQueries	Total number of General Membership Query packets received
rxIgmpReports	Total number of Membership Reports received

To clear IGMP statistics, select **clear** in the Clear IGMP Statistics field and click **Submit**.

## IP Statistics

The following table describes the Internet Protocol statistics fields.

**Table 13-8** IP Statistics

Field	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ipForwDatagrams	The number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source-Route option processing was successful.
ipInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in <code>ipForwDatagrams</code> .
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in <code>ipForwDatagrams</code> if any such packets met this (discretionary) discard criterion.

**Table 13-8** IP Statistics (continued)

Field	Description
ipOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in <code>ipForwDatagrams</code> , which meet this <i>no-route</i> criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ipReasmReqds	The number of IP fragments received which needed to be reassembled at this entity (the switch).
ipReasmOKs	The number of IP datagrams successfully re- assembled.
ipReasmFails	The number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
ipFragOKs	The number of IP datagrams that have been successfully fragmented at this entity (the switch).
ipFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their <code>Don't Fragment</code> flag was set.
ipFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).
ipRoutingDiscards	The number of routing entries, which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
ipDefaultTTL	The default value inserted into the <code>Time-To-Live</code> (TTL) field of the IP header of datagrams originated at this entity (the switch), whenever a TTL value is not supplied by the transport layer protocol.
ipReasmTimeout	The maximum number of seconds, which received fragments are held while they are awaiting reassembly at this entity (the switch).

To clear IP statistics, select **clear** in the Clear IP Statistics field and click **Submit**.

## MP-Specific Information

These windows provide information about the switch's internal processors:

- [“CPU Utilization” on page 169](#)
- [“MP Packet Statistics” on page 169](#)

## CPU Utilization

The following table describes the CPU Utilization fields.

**Table 13-9** CPU Utilization

Field	Description
CpuUtil1Second	The utilization of MP CPU over 1 second. It shows the percentage.
CpuUtil4Seconds	The utilization of MP CPU over 4 seconds. It shows the percentage.
CpuUtil64Seconds	The utilization of MP CPU over 64 seconds. It shows the percentage.

## MP Packet Statistics

The following table describes the MP Packet statistics fields.

**Table 13-10** MP Packet Statistics

Field	Description
allocs	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
frees	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
mediums	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
mediums hi-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
jumbos	Total number of packet allocation with size more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
jumbos hi-watermark	The highest number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
smalls	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
smalls hi-watermark	The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
pkt_hdrs	Total number of packet headers from the packet buffer pool by the TCP/IP protocol stack.
pkt_hdr hi-watermark	The highest number of packet headers from the packet buffer pool by the TCP/IP protocol stack.
failures	Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack.

## Network Time Protocol Statistics

---

The following table describes the NTP statistics fields.

**Table 13-11** NTP Statistics

Field	Description
Request Sent	The total number of NTP requests the switch sent to the primary NTP server to synchronize time.
Response Received	The total number of NTP responses received from the primary NTP server.
Updates	The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.
Last update time	The time stamp showing the time when the switch was last updated.
Current system time	The current switch system time.

To clear these statistics, select **clear** in the Clear NTP Statistics field and click **Submit**.

## Port Statistics

---

### *Switch Ports Statistics Summary*

The following table describes the switch port statistics fields.

**Table 13-12** Port Statistics

Field	Description
Switch Port	Port identifier. <b>Note:</b> If a switch is part of a multi-switch stack, the displayed number indicates the Configured Switch number ( <i>csnum</i> ) followed by the port number. See <a href="#">“Stacking Port Numbers”</a> on page 60 for more information.
InOctets	The total number of octets received on the interface, including framing characters.
OutOctets	The total number of octets transmitted out of the interface, including framing characters.
Total Errors	The number of packets that could not be transmitted because of errors.

To clear port statistics, click **Clear all ports statistics**.

# Index

---

## Symbols

[ ]..... 11

## A

accessing the switch  
    defining source IP addresses..... 78  
    RADIUS authentication..... 79, 130  
    security..... 77  
    using the Browser-based Interface..... 75  
active configuration block ..... 25, 72  
administrator account..... 79  
apply (global command)..... 71  
applying configuration changes..... 71

## B

backup configuration block ..... 25, 72  
broadcast domains ..... 30

## C

Cisco EtherChannel ..... 33  
command conventions ..... 11  
configuration  
    apply changes..... 71  
    save changes ..... 72  
    view changes..... 71  
configuration block  
    active ..... 25  
    backup..... 25  
    factory..... 25  
    selection ..... 25  
configuration rules  
    port mirroring..... 33  
    spanning tree..... 33  
    Trunking..... 33

## D

daylight savings time ..... 132  
default password..... 79  
diff (global) command, viewing changes..... 71  
downloading software ..... 22

## E

EtherChannel ..... 32, 33  
    as used with port trunking ..... 33

## F

factory configuration block ..... 25  
FailoverLayer 2 Failover ..... 35, 105  
fault tolerance  
    port trunking..... 34

## I

IGMP Snooping..... 38, 106  
image  
    downloading ..... 22  
    software, selecting..... 24  
IP subnets  
    VLANs..... 30  
ISL Trunking..... 33

## L

LACP ..... 34, 106  
Link Aggregation Control Protocol..... 34, 106  
logical segment. *See* IP subnets.

**M**

Main Menu	
summary .....	68
Management Processor (MP)	
use in switch security .....	78
manual style conventions .....	11
mirroring ports .....	113
monitoring ports .....	113
multi-links between switches	
using port trunking .....	32

**N**

NTP synchronization .....	132
---------------------------	-----

**P**

password	
administrator account .....	79
default .....	79
user account .....	79
port mirroring .....	113
configuration rules .....	33
port trunking .....	34
EtherChannel .....	32, 33
fault tolerance .....	34
ports	
monitoring .....	113

**Q**

Quick Start .....	17
-------------------	----

**R**

RADIUS	
authentication .....	79, 130
SSH/SCP .....	90
read community string (SNMP option) .....	126
routers	
port trunking .....	33
RSA keys .....	89

**S**

save (global command) .....	72
noback option .....	72
save command .....	25
SecurID .....	90

security	
allowable SIP addresses .....	78
port mirroring .....	113
RADIUS authentication .....	79, 130
switch management .....	78
VLANs .....	30
segmentation. <i>See</i> IP subnets.	
segments. <i>See</i> IP subnets.	
SNMP	
set and get access .....	126
software	
image .....	22
spanning tree	
configuration rules .....	33
spoofing, prevention of .....	78
SSH	
RSA host and server keys .....	89
SSH/SCP	
configuring .....	85
stacking .....	45
statistical load distribution .....	34
switch	
resetting .....	26
switch management	
security .....	78

**T**

TACACS+ .....	81, 131
text conventions .....	11
Trunking	
configuration rules .....	33
typographic conventions .....	11

**U**

user account .....	79
--------------------	----

**V**

VLANs	
broadcast domains .....	30
security .....	30