

Release Notes

Virtual Switch Extension for IBM BladeCenter,
SmartConnect Version 41.1

Part Number: BMD00086, March 2009

BLADE
NETWORK TECHNOLOGIES

2350 Mission College Blvd.
Suite 600
Santa Clara, CA 95054
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: BMD00086.

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

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

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

Originated in the USA.

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

Release Notes

These *Release Notes* provide the latest information regarding Virtual Switch Extension (VSE) for IBM BladeCenter, SmartConnect, for the BNT 1/10Gb Uplink Ethernet Switch Module. This document supplements information found in the complete documentation:

User's Guide—

Virtual Switch Extension for IBM BladeCenter,
SmartConnect Version 41.1
(Part Number BMD00082, February 2009)

The publication listed above is available from the following support web site:

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

Please keep these *Release Notes* with your product documentation.

Overview

The Virtual Switch Extension (VSE) for IBM BladeCenter, SmartConnect, provides a simple Ethernet interface option for connecting a blade server chassis to the network infrastructure. The number and type of configuration options on the VSE SmartConnect software are restricted to reduce the initial setup complexity and to minimize the impact on upstream networking devices.

VSE SmartConnect software provides a graphical user interface that lets you remotely configure and manage switches through a Web browser. Using the VSE 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.
- View a variety of switch information and statistics.

VSE SmartConnect software includes the following features for use in virtual networking environments:

- 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 VSE 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.
- *Trunking* multiple switch ports into a single, high-bandwidth link to other large 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. VSE SmartConnect software supports one stack with up to eight switches. Stacking also permits the use of up to 56 internal port trunks.

- Virtual segregation

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 you to assign server IP addresses 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, VSE SmartConnect software provides a highly-flexible framework for allocating and managing switch resources.

Software Update Procedure

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 your network, or onto your 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

You can 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 you require a software update, the latest version of the VSE SmartConnect software is available from the support website. Download the switch image and place it on a FTP or TFTP server, or on your 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 you load new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot`.

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

Note – The switch image type is checked during the software download, to validate that the image is compatible. If the image is incompatible, an error message is displayed.

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

- FTP server
- TFTP server
- Local computer

Perform the following steps to transfer a software image:

1. **On the BBI, choose menu `System Settings > Boot Management > General`.**
2. **In the Boot Management window, 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.**
 - 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 your 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 the Image to Run

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

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

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

- VSE SmartConnect software image
- BNT 1/10Gb Uplink Ethernet Switch Module image

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

3. **If necessary, select an option from the `Next Boot Config Block` drop-down list.**

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

4. **Click `Apply` to submit the image and configuration changes to the switch.**

Resetting the Switch

Reset the switch to make your software image file and configuration block changes active:

1. **On the BBI, choose menu System Settings > Boot Management > General.**
2. **On the Boot Management window, click Reboot the Module.**

Supplemental Information

This section provides additional information about configuring and operating the BNT 1/10Gb Uplink Ethernet Switch Module and VSE SmartConnect software, Version 41.1.

SFP+ Copper Direct Attach Cables (DAC)

The switch will not disable the SFP+ ports when using any MSA-compliant DAC cables. For best results, the following cables have been qualified to work with the switch:

Model Number	Description
BN-SP-CBL-1M	SFP+ Copper Direct Attach Cable - 1 meter
BN-SP-CBL-3M	SFP+ Copper Direct Attach Cable - 3 meters
BN-SP-CBL-7M	SFP+ Copper Direct Attach Cable - 7 meters
BN-SP-CBL-10M	SFP+ Copper Direct Attach Cable - 10 meters

Multiple Management Sessions

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.

Virtual Machines

The switch will normally accept a maximum of 1024 Virtual Machines (VMs). Once this limit is reached, the switch will reject additional VMs.

However, in some rare situations, the switch may reject the addition of new VMs prior to reaching the 1024 VM maximum. 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.

Statistics on Discarded Packets

Under specific circumstances, packets may be counted as discarded in some Layer 3 statistics, even though they are actually forwarded.

This can occur for some Layer 3 statistics, such as RIPD4, which is incremented when a packet has an IPv4 multicast Ether type, but no corresponding Layer 3 interface. Although the packet continues through Layer 2, it is considered discarded by the Layer 3 counters.

Stacking

Stack Links

The cables used for connecting the switches in a stack carry low-level, inter-switch communications critical to shared switching functions. If the stack is physically connected in a bidirectional ring topology as recommended, stack operation should recover in the event of any single loss of link. Always maintain the stability of stack links in order to avoid internal stack reconfiguration.

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.

Factory Defaults

Under the factory default configuration, stacking mode is disabled on the switch. However, once stacking is enabled, the stacking mode will be retained upon reboot, even after reverting the switch back to its factory default configuration. This allows switches to rejoin their stack in instances where the administrator has purged their configuration.

To reset all configuration values, including stacking mode, disable stacking prior to resetting the switch to its factory default configuration.

Resetting a Stack

When using some versions of Mozilla Firefox to access the BBI and reset a switch stack, the BBI is temporarily disconnected from the switch, causing a **Try Again** button to appear on the browser interface. The **Try Again** button reissues last command issued before the BBI was disconnected (the stack reboot), and should not be interpreted as a command for reconnecting to the BBI.

If the **Try Again** button is clicked, the user will be asked to log in, at which time the interface will execute its prior command, resetting the stack a second time.

Using SNMP to Download Images

When stacking is enabled, using SNMP to download boot images or software images can result in the image being loaded multiple times. This occurs when the download time (which is larger for the stacking images) exceeds the normal timeout value configured for the SNMP connection. The SNMP agent then restarts the download multiple times, as governed by the configured SNMP retry value.

When switches are stacked, it is recommended to increase the SNMP timeout value to allow for a single, complete software and boot image download.

IBM Advanced Management Module

Protected Mode Ports

When using Microsoft Internet Explorer 6 (Service Pack 1) or Internet Explorer 7, the IBM Advanced Management Module (AMM) software interface does not disable the external (EXT) ports list as expected when the switch Protected Mode (PRM) is enabled. This is only a display problem: the interface does not allow configuration changes to the protected ports.

Stack Management

The AMM can be used for many stack management operations.

To display various information about managed switches, including their IP addresses and stacking mode, use one of the following AMM pages:

- Monitors > System Status > I/O Modules
- I/O Module Tasks > Admin/Power/Restart

For example:

IBM BladeCenter - Advanced Management Module

Welcome USER

About | Help | Logout

Bay 1: Blade-Marketing

- Monitors
- Blade Tasks
- I/O Module Tasks
 - Admin/Power/Restart
 - Configuration
 - Firmware Update
- MM Control
- Service Tools

I/O Module Power/Restart ?

Select one or more module(s) using the checkboxes in the first column, select the desired action below the table, and then click Perform action

<input type="checkbox"/>	Bay	Type	Manufacturer	MAC Address	IP Address	Pwr	Unique ID Type	ID	Stacking Mode	Protected Mode
<input type="checkbox"/>	1	Ethernet SM	BNT (BNT)	00:18:B1:31:X0:00	192.168.12.13	On	n/a	n/a	n/a	Disabled
<input type="checkbox"/>	2	Ethernet SM	BNT (BNT)	00:18:B1:31:X9:00	192.168.12.14	On	n/a	n/a	Standby	Disabled
<input type="checkbox"/>	3	Ethernet SM	BNT (BNT)	00:18:B1:31:XA:00	192.168.12.15	On	n/a	n/a	Master	Active
<input type="checkbox"/>	4	Ethernet SM	BNT (BNT)	00:18:B1:31:X4:00	192.168.12.16	On	n/a	n/a	Member	Active

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

Available actions

Power On Module(s)

The following Stacking Modes are used with SmartConnect switches:

- **Master**

The switch is currently participating in an active stack as the Master. The Master controls stack operation and provides a single point to manage the stack. A stack must have one and only one Master. Firmware image, configuration information, and run-time data are kept by the Master and pushed to each Member switch in the stack.

You can use the IP address of the switch identified as the *Master* in the *Stacking* column to manage the stack.

- **Member**

The switch is currently participating in an active stack as a Member. 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. A Member can also be configured to act as a Backup to the Master, in case the Master switch fails or is disconnected from the stack.

- **Standby**

The switch is configured to operate in stacking mode, but is currently isolated from an active stack. A switch may be isolated due to unconnected ports, or when no Master or Backup is present.

Note – Protected Mode is enabled for all SmartConnect Master and Member switches. Protected mode is also enforced by switches in Standby mode. Restricted activities, such as resetting the switch to its factory default configuration, are not permitted on standby switches even though the AMM Protected Mode is displayed as disabled.
