HITACHI
Inspire the Next

Readme for Network OS v4.1.3b

Appendix for Administrator Guide

FASTFIND LINKS

Document Organization

Product Version

Getting Help

Contents

Hitachi Data Systems

MK-99COM156-00

Hitachi, Ltd., reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. This document contains the most current information available at the time of publication. When new or revised information becomes available, this entire document will be updated and distributed to all registered users.

Some of the features described in this document might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Data Systems Corporation at https://portal.hds.com.

Notice: Hitachi, Ltd., products and services can be ordered only under the terms and conditions of the applicable Hitachi Data Systems Corporation agreements. The use of Hitachi, Ltd., products is governed by the terms of your agreements with Hitachi Data Systems Corporation.

Contents

Preface

This document describes how to use the Network OS for Brocade 10Gbps DCB switch module.

This preface includes the following information:

- □ Intended Audience
- □ Product Version
- □ Release Notes
- □ Document Organization
- □ Document Conventions
- □ Getting Help
- □ Comments

Notice: The use of the Network OS for Brocade 10Gbps DCB switch module and all other Hitachi Data Systems products are governed by the terms of your agreement(s) with Hitachi Data Systems.

Intended Audience

This document is intended for the personnel who are involved in planning, managing, and performing the tasks to prepare your site for Compute Blade installation and to install the same.

This document assumes the following:

- The reader has a background in hardware installation of compute systems.
- The reader is familiar with the location where the Compute Blade will be installed, including knowledge of physical characteristics, power systems and specifications, and environmental specifications.

Product Version

This document revision applies to Network OS for Brocade 10Gbps DCB switch module version 4.1.3b.

Release Notes

Release notes contain requirements and more recent product information that may not be fully described in this manual. Be sure to review the release notes before installation.

Document Organization

The following table provides an overview of the contents and organization of this document. Click the chapter title in the left column to go to that chapter. The first page of each chapter provides links to the sections in that chapter.

Chapter	Description
Chapter 1. Network OS 4.1.3b overview	Describes the overview of Network OS 4.1.3b.
Chapter 2. Prerequisites of Network OS 4.1.3b	Describes the prerequisites of Network OS 4.1.3b.
Chapter 3. New/Enhanced Feature Description	Provides the information of New/Enhanced feature for Network OS 4.1.3b.
Chapter 4. Firmware Upgrade and Downgrades	Describes the procedure of upgrade and downgrades for Network OS 4.1.3b.
Appendix A. Modifications for Hitachi	Describes the customization feature of Network OS for Hitachi, Ltd.

Document Conventions

This document uses the following typographic conventions:

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, fields, and labels. Example: Click **OK**.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `copy` *`source-file target-file`* ***Note:*** Angled brackets (< >) are also used to indicate variables.
`screen/code`	Indicates text that is displayed on screen or entered by the user. Example: `# pairdisplay -g oradb`
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `# pairdisplay -g <group>` ***Note:*** Italic font is also used to indicate variables.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.
underline	Indicates the default value. Example: [a | b]

This document uses the following icons to draw attention to information:

Icon	Meaning	Description
⚠	WARNING	This indicates the presence of a potential risk that might cause death or severe injury.
⚠	CAUTION	This indicates the presence of a potential risk that might cause relatively mild or moderate injury.
NOTICE	NOTICE	This indicates the presence of a potential risk that might cause severe damage to the equipment and/or damage to surrounding properties.
! Note	Note	This indicates notes not directly related to injury or severe damage to equipment.
••• Tip	Tip	This indicates advice on how to make the best use of the equipment.

Getting Help

If you purchased this product from an authorized HDS reseller, contact that reseller for support. For the name of your nearest HDS authorized reseller, refer to the HDS support web site for locations and contact information. To contact the Hitachi Data Systems Support Center, please visit the HDS website for current telephone numbers and other contact information: http://support.hds.com.

Before calling the Hitachi Data Systems Support Center, please provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure.
- The exact content of any error message(s) displayed on the host system(s).

Comments

Please send us your comments on this document: doc.comments@hds.com. Include the document title, number, and revision, and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Data Systems Corporation. **Thank you!**

1

Network OS 4.1.3b overview

In this chapter, the overview of Network OS 4.1.3b is described.

Brocade Network Operating System (NOS) v4.1.3b is an update to NOS v4.1.3. All features supported in NOS v2.0.1 kat4, NOS v3.0.0_dcb3, NOS v4.1.2, NOS v4.1.2a, NOS v4.1.3 and NOS v4.1.3a are also supported in NOS v4.1.3b.

- □ New/Enhanced Feature Outline

New/Enhanced Feature Outline

Network OS v4.1.3b includes the following features for embedded DCB switch module.

- xSTP over VCS
- Private VLAN
- vLAG Default Up
- UDLD
- DHCP IP Helper
- DHCP Automatic Deployment (DAD)
- VRRP-E across VCS fabrics
- Packet capture utility
- CLI Port Range
- Mixed-version

In addition, Network OS v4.0.0 includes the following new enhancements and support:

- OSPF enhancements
- VRRP/VRRPe enhancements
- VCS Fabric Scale
- vCenter Scale
- Multiple sflow collectors and IPv6 based sflow
- SPAN support on ISL port
- Management Services enhancements

2

Prerequisites of Network OS 4.1.3b

In this chapter, the prerequisites for Network OS 4.1.3b are described.

This chapter provides fundamental information about Network OS 4.1.3b as exemplified by the optional license, the standard compliance, scalability and compatibility.

Additionally the important notes described about the features of Network OS 4.1.3b.

OPTIONAL LICENSED SOFTWARE

FCoE and VCS capabilities can be enabled on the base SKU by adding software licenses. NOS 4.1.3b now incorporates the Brocade VCS License as part of the base offering. Customers would have to no longer purchase a license to enable VCS fabric (for more than 2 nodes).

- **Brocade FCoE license** — Enables Fibre Channel over Ethernet (FCoE) supporting transport FC protocols and frames over Data Center Bridging (DCB) networks. DCB is an enhanced Ethernet network that enables convergence of several data center applications onto a single interconnect technology. FCoE provides a method of encapsulating the Fibre Channel (FC) traffic over a physical Ethernet link.

Software licenses are available in following formats.

Software License	SKU Description
GG-BE3LSL2X1-Y	FCoE license

Standards Compliance

This software generally conforms to Ethernet Standards in a manner consistent with accepted engineering practices and procedures. In certain cases, Brocade might add proprietary supplemental functions to those specified in the standards, or choose to implement modifications to the standards for performance or behavioral improvements.

The embedded DCB switch module conforms to the following Ethernet standards:

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree
- IEEE 802.1w Rapid reconfiguration of Spanning Tree Protocol
- IEEE 802.3ad Link Aggregation with LACP
- IEEE 802.3ae 10G Ethernet
- IEEE 802.1Q VLAN Tagging
- IEEE 802.1p Class of Service Prioritization and Tagging
- IEEE 802.1v VLAN Classification by Protocol and Port
- IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
- IEEE 802.3x Flow Control (Pause Frames)

The following draft versions of the Data Center Bridging (DCB) and Fibre Channel over Ethernet (FCoE) Standards are also supported on the embedded DCB switch module:

- IEEE 802.1Qbb Priority-based Flow Control
- IEEE 802.1Qaz Enhanced Transmission Selection
- IEEE 802.1 DCB Capability Exchange Protocol (Proposed under the DCB Task Group of IEEE 802.1 Working Group)
- FC-BB-5 FCoE (Rev 2.0)

""The embedded DCB switch module conforms to the following Internet IETF RFCs:

- RFC 2865 Remote Authentication Dial In User Service (RADIUS)
- RFC 1112 IGMP
- RFC 2236 IGMPv2
- RFC4601 PIM-SM
- RFC2131 DHCP
- RFC 2571 Architecture for Describing SNMP Framework
- RFC 3176 sFlow
- RFC 1157 SNMPv1/v2c
- RFC4510 Lightweight Directory Access Protocol (LDAP)
- RFC 3768 Virtual Router Redundancy Protocol (VRRP)
- RFC 2328 OSPF Version 2
- RFC 1587 OSPF NSSA Option
- RFC 3101 OSPF Not-So-Stubby-Area (NSSA) Option
- RFC 1765 OSPF Database Overflow
- RFC 2154 OSPF with Digital Signatures (MD-5 Support)
- RFC 3137 OSPF Stub Router advertisement

Scalability

All scalability limits are subject to change. Limits may be increased after further testing has been completed, even after the release of a particular NOS version.

NOS v4.1.3b Scalability Limits	Standalone	VCS Fabric
Maximum # of VLANs	3,500	3,500
Maximum # of MAC addresses	30,000	30,000
Maximum # of port profiles(AMPP)	750	750
Maximum # of per priority pause levels	2	2
Maximum # of L2 multicast group	2,000	2,000
Maximum # of MSTP instance	32	N/A
Maximum # of LAG groups (Platform dependent)	60	60
Maximum # of members in a standard LAG	16	16
Maximum # of members in a Brocade LAG	8	8
Maximum # of switches in a Fabric cluster	N/A	32
Maximum # of switches in Logical cluster	N/A	24
Maximum # of Layer 2 ECMP Paths	N/A	8
Maximum # of VLAG groups	N/A	512
Maximum # of member ports in a VLAG	N/A	64
Maximum # of nodes in a VLAG	N/A	8
Maximum cable length for lossless connectivity	300m	300m
Maximum # of VLANS in port profiles	3,500	3,500
Maximum # of MAC Associations for AMPP	16,000	16,000
Maximum # of IGMP Snooping (*,G) forwarding entries	2,000	2,000
Maximum # of IGMP Snooping Interfaces supported	128	128
Maximum Group Learning Rate (in Frames Per Second)	128	256
Maximum Total # of L2 + L3 ACL rules	1,200	1,200
Maximum # VLAN per Edge Port in Trunk Mode Port	3,500	3,500
Maximum # of Enodes per Fabric	N/A	2,000
Maximum # of FCoE interfaces (Platform Dependent)	N/A	1,000
Maximum # of FCoE Devices per Fabric	N/A	2,000
Maximum # of FCoE Logins	N/A	1,000
Maximum # of member ports per VLAG per NODE	N/A	16
Maximum size of Zoning Database in bytes	N/A	150K
Maximum # of Management ACL	256	256
Maximum # of VMs supported in VM Aware Network Automation	8,000	8,000
Maximum # of ARP Entries	N/A	8,000
Maximum # of routes supported in OS	N/A	1,500

Maximum # of static routes	N/A	500
Maximum # of dynamic routes	N/A	1,500
Maximum # of VRRP instances per system	N/A	64
Maximum # of VRRP instances per interface	N/A	8
Maximum # of routers participating in a VRRP-E session	N/A	4
Maximum # of members per ECMP path (Layer 3)	N/A	8
Maximum # of routes with ECMP supported	N/A	1,500
Maximum # of IP interfaces per system	N/A	128
Maximum # of secondary IP address	N/A	255
Maximum # of MSTP instance	32	32
Maximum # of VLAN in PVST	128	128
Maximum # of Unicast IPv4 routes in the hardware	N/A	1,500
Maximum # of OSPF areas	N/A	16
Maximum # of OSPF routers in a single area	N/A	12
Maximum # of OSPF adjacencies	N/A	12
Maximum # of OSPF routes	N/A	1,500
# of OSPF Interfaces	N/A	64
# of OSPF enabled subnets	N/A	64
# of local subnets in a single area	N/A	64
Maximum # of I- BGP peers	N/A	20
Maximum # of E-BGP peers	N/A	20
Maximum # of BGP routes in HW	N/A	1,500
Maximum # of RIB IN Routes	N/A	2,000
Maximum # of RIB OUT Routes	N/A	10,000
Maximum # BGP Peer Group	N/A	10
Maximum # of UDLD enabled interfaces	60	60
Maximum # of PVLAN domain supported	N/A	31
Maximum # of Secondary vlans per PVLAN supported	N/A	24
Maximum # of primary vlans per PVLAN supported in promiscuous mode	N/A	24
DHCP IP Helper Addresses per interface	N/A	4
DHCP IP Helper Ve interfaces	N/A	128
DHCP IP Helper physical ports	N/A	60

Compatibility

In standalone mode, which means in traditional Ethernet network, 4.1.3b is interoperable at Layer 2 with standard Ethernet interfaces with not only all of Brocade NOS version but also other industry standard switches. But, Hitachi does not guarantee the interoperability with any other vender's network switch. Regarding to the interoperability, please refer to the Network OS Administrator Guide for details.

NOTE: Vlan 1002 is dedicated for FCoE. In standalone mode, FCoE is not available. However, Vlan 1002 is not available in even standalone mode in 4.1.2 or higher.

In VCS Fabric mode, 4.1.3b has the connectivity to only Brocade NOS 4.1.3b into same fabric. If 4.1.3b connects to other than Brocade NOS 4.1.3b, the VCS Fabric will be segmented. Regarding to the connectivity to standard Ethernet switch in VCS Fabric mode, please refer to the Network OS Administrator Guide.

Documentation Updates

When using the NOS 4.1.x documentation, the embedded DCB switch module is equivalent to the VDX 6720 except where noted in the release note document. The most recent NOS documentation manuals are available on MyBrocade: http://my.brocade.com/

Following three NOS 4.1.x documents are recommended references.

1. Network OS Administrator Guide Part # 53-1003225-06

2. Network OS MIB Reference Part # 53-1002560-01

3. Network OS Command Reference Part # 53-1003226-03

4. Network OS Message Reference Part # 53-1003227-01

The embedded DCB switch module uses additional commands to those listed in the Network OS Command Reference. Refer to Appendix A for additional commands.

IMPORTANT NOTES

This section contains information that you should consider before you use this NOS release.

Command Line Interface

- Some commands will not produce paginated output.

- Break command is not supported. Pl use ctrl-c as an alternative
- For certain commands (including no form with some commands), "?" will show unsupported additional options.
- Tab completion and <ctrl>-c (cancel) does not work for some commands.
- For some commands, "switchId" and "all" options are not applicable in this Brocade Network OS release but are still shown as options. These will be applicable and supported in future Brocade Network OS releases.
- Some CLI commands will generate an "Error:Access denied" message upon failure. This means the operation failed on the switch and may not be related to permissions.
- The "no" command always exists for all roles even if it is not required.
- Some no commands will execute without mandatory parameters that were originally used for configuration. Some needs mandatory parameters though help message does not suggest same
- Some no commands may produce an incorrect error message upon error.
- Incorrect range might be displayed in the help text for some of the show commands.
- Interface range command is not supported on breakout ports. Range command is not supported across multiple slots of the chassis
- System does not warn user on deleting the ip config when vrf is configured
- show interface stats brief does not distinguish loopback interfaces across rbridges
- Redistributed connected/static may be shown twice as part of config
- Some unsupported debug commands may be seen in NOS 4.1.0. Brocade recommends not to run them on switches:
    - Show confd-state -, for debugging purpose only.
    - Show parser dump -, for debugging purpose only
    - Show notification stream -, for debugging purpose only
    - Show features - no use
    - Show ssm -, for debugging purpose only.
    - Autoupgrade command in config mode

- 'snmp-server context CONTEXT_NAME vrf-name VRF-NAME command
- During "copy running-config startup-config" or "copy support" user might see occasional CPU spikes (to ~30-40%).
- While unconfiguring non-existent configs, for some features, "Error: Access Denied" may be displayed even though it is a no-op.
- Interface specific static arp entries are not shown when using show running command for an interface.
- show mac-address-table command on console with include option cannot be aborted with a break/ctl-C. Use a telnet session for the same.
- For ip access lists, display filtering based on sequence number alone does not work as expected.
- Security CLIs: In FC mode: the following are under rbridge-id context unlike earlier release
    - fcsp
    - secpolicy
    - system-monitor moves to rbridge context but system-monitor-mail is still in global mode
- DHCP/ipv6 autoconfig were moved from rbridge context in 3.x to mgmt. interface context in 4.x
- Though ICMPv6 RA guard CLI is available on all platforms , it is supported only for 6710/20/30
- "protocol vrrp-extended" is added to specifically enable VRRPE in 4.x which was implicitly enabled in 3.x using command 'protocol vrrp'
- TACACS/Radius local behavior is now changed and currently reflected using 'local backup'
- Do not use CLI 'no spanning-tree shutdown' from the vlan context from rspan-vlan
- Do not use lldp iscsi-priority' (and a couple of other similar CLIs from the same context) needs to be blocked on destination mirror port.
- "show chassis" output may show the PSU part number as "Unknown" after removal & re-insertion of the PSU
- Under certain scenarios, output of "show qos rcv-queue multicast ten <>" may not show accurate count of drops
- Certain oscmd commands may not work or give a different output under admin login

- Netconf commands 'debug internal rate-limit-delay' may fail
- debug ip bgp prefix-list <option> , debug ip bgp neighbor does not work
- 'no' command for 'qos map dscp-cos' does not work
- On rare scenario, configuration may not be applied to hardware on power-cycling the chassis
- Neighbor-discovery CLI ineffective after reload & needs a link-flap

Restrictions for Ports in 1G Mode

- RMON stats are calculated incorrectly for packet sizes 64-127 bytes.
- Brocade Trunks cannot be formed with 1G, as all Brocade Trunks should be 10G.
- A LAG cannot be created between 1G and 10G ports.
- FCoE configuration is NOT supported on 1G ports.
- DCBX configuration for FCoE is not supported on 1G ports.

Licensing

- DCB switches installed Network OS v3.0.0_dcb3 or earlier require a VCS License for each of the DCB switches to configure a VCS fabric with three or more DCB switches. DCB switches installed Network OS v4.1.1 or later require no VCS License to configure a VCS fabric with three or more DCB switches. To configure a VCS fabric with two or less DCB switches, DCB switches require no VCS License. To activate the FCoE function, FCoE license is required for each DCB switches.

Firmware Installation

In Standalone & Fabric Cluster

- Only standalone firmware download is supported. You need to log onto individual nodes and run firmware download there.
- Under certain stress conditions firmware download might time out on a node, e.g. due to excessive processing load on the processor, slow network, etc. The firmware download command will recover the system automatically. You need to wait for the completion of recovery before retrying the firmware download command.
- While upgrading firmware on the node, it is recommended not to make any configuration changes before firmware download has been completed successfully.

Platform

- After "chassis disable" please wait for 60 seconds for VDX67xx before doing the next "chassis enable".
- Chassis-name is limited to 15 characters
- 1G links must have auto-negotiation enabled. 1G links without auto-negotiation are not supported.
- Current 1G copper SFP's do not support exchanging flow-control settings during the auto-negotiation process. It is recommended to configure static mode of configuration of flow-control on both the ends of the desired link.
- System verification/diagnostics performed on a switch will require a reboot.
- Configuration of more than one In-band management port on a single switch is not recommended.
- Under certain stress conditions 'copy support' command might time out for some modules. In such cases it is recommended to retry 'copy support' with higher timeout multiplier value.
- It is highly recommended to copy configuration file to running-config and then save the running-config to startup-config, instead of directly copying the external configuration file to startup-config, especially when using fabric distributed features such as Zoning, VM Aware Network Automation and Virtual IP.

Virtual IP Address Support

- A separate gateway cannot be configured for Virtual IP address. Default gateway will be the same as the gateway address for the management port of this switch.
- There is no Virtual MAC address associated with the Virtual IP address.
- For VCS Virtual IP address to work correctly, the management port's IPv4 address should be assigned, functional and both address should be in same subnet".

Security, ACLs, Authentication, Authorization

- Login authentication service (aaa authentication login cli):
    - With "local" option specified as secondary authentication service, local authentication will be tried only when the primary authentication service (TACACS+/Radius/LDAP) is either unreachable or not available.
    - Behavior of "local" option in pre-4.1.0 releases is changed to the "local-auth-fallback" option.

    - When login authentication configuration is modified, the user sessions are not logged out as in pre-4.1.0 releases. All connected user sessions can be explicitly logged out using "clear sessions" CLI.

- ACLs are not supported for egress traffic flows

- Configuring TACACS+ or RADIUS without a key is not supported. If no key is configured, the switch uses a default key of "sharedsecret".

- There is a possibility that locked user accounts will get unlocked after a reboot if the running-config (before reboot) is different from startup-config of user accounts.

- Encrypted text (taken from running-config of any user account password with encryption turned on) should not be used as input for clear-text password for the same user. This may result in login failure of the user subsequently.

- There is no upper limit for the number of rules that can be added to a management access-list. But when the ACL is applied to a management interface, only the top 256 rules will be applied if the ACL contains more than 256 rules.

- Access to ONLY the following Active Directory (AD) servers is supported by Brocade LDAP client:

    - Windows 2000

    - Windows 2003

    - Windows 2008 AD

- The DNS configuration is primarily used for LDAP. It should be noted that DNS look-up will not be used by PING, Traceroute or any other services. These services will still require specifying the actual IP address.

- When more than 250 rules ACL's are configured (over supported scale), they may be partially installed & effective

- A hard-drop ACL rule on VDX-6740 may not drop UDLD packets

- Counter for hard-drop ACL may not count accurately

- Even though IGMP snooping feature is supported over VLAG, all the multicast data traffic will be forwarded only over the primary.

- When a MAC ACL with several clauses is applied to a port-channel which is a member of 750 or more VLANS, the MAC ACL counters may take several minutes to be enabled due to processing load associated with such configurations.

- Deny / Harddrop ACL on VE does not work when pkt ingresses from TRILL port

Management Services

- During upgrade to 4.1.0, the existing users might lose access as password encryption is supported in Leo but not in pre-Leo releases. Same is applicable for V3 hosts where the particular user is mapped to.

- SNMP is not aware of cluster. Hence if we query 1 node through SNMP, we will get the info related to that particular node only

SPAN & RSPAN

- CPU-originated packets cannot be output spanned.

- SPAN is supported only within a port-group on the VDX 6720 and 6746.

- If SPAN has to be supported to multiple locations, please use RSPAN on VLAN.

- On VDX 6720 and 6746, only one port per port group can be configured as destination port for ingress spanning.

- On 6720 and 6746, only one port per port group can be configured as destination port for egress spanning.

- On 6720 and 6746, ISL port cannot be source or a destination SPAN port.

- On 6720, Inter-chip port spanning is not allowed.

- Spanning of LAG port is not supported. To span a LAG, user should individually enable spanning on all the member ports of the LAG.

- A profiled port cannot be a SPAN destination.

ICMPv6 RA Guard

- This feature is only supported by Brocade Fixed Port Switches VDX 6710, VDX 6720 and VDX 6730.

Trunking

- For the rest of the VDX platforms, Brocade trunk (BTRUNK) has a maximum throughput of 80G. Full link utilization of 8 ports in a trunk group is achievable with larger packet size (>128 Bytes).

VCS

- Loopback connection is not supported in VCS mode. If a loopback connection is done, those interfaces become ISL interfaces.

- Fabric Cluster Mode:

- When a new switch is added to an existing VCS fabric and if the new switch takes the role of principal node, the other switches in the fabric will receive the configuration of the distributed features such as Virtual IP and VM-Aware Network Automation from the newly added switch. This will cause the existing distributed configuration to be overwritten by the newly added switch in the principal role. This can be avoided by following the new switch addition procedures in the Admin Guide.

- After a cluster reboot, Brocade recommends to do both "show fabric all" and "show vcs" to ensure that cluster is entirely formed without any issue. User might see that 'show vcs' takes an additional 2-3 minutes to show all participating switches. This is an existing behavior and doesn't affect data path functionality in most cases.

- "show fabric isl" & "show fabric trunk" may show the interfaces in random order without sorting

VLAG

- LAGs are created with default speed of 10G. Therefore Brocade recommends end user to set required speed manually based on member speed using "speed" command.

- When configuring LACP LAG between VDX & non-Brocade switches it is highly recommended to enable the VLAG ignore-split on the VDX. Ignore split option is enabled by default in Brocade Network OS v4.1.0.

MAC Learning Considerations in VCS

- The CLI command "clear mac-address-table" has been enhanced to support clearing the mac-addresses associated with vLAG's. This command can be used to sync mac-address-tables of the VCS member switches.

- Post 3.x releases, FPMA mac addresses are not shown in "show mac-address-table dynamic". User can use 'show fcoe login' and ' show mac-address-table count' together to get this output

- Post 3.x releases, Internal Mac-addresses are shown in "show mac-address-table" output to support L3 use cases. The sync across the VCS has to be observed using "show mac-address-table dynamic".

- Under rare circumstances, end user might see mac address sync up issues on few nodes of a cluster (where 1 or more MAC addresses might be missing in some nodes). Brocade recommends to do "clear mac-address-table dynamic" in such cases.

- Static mac addresses will be displayed even when interfaces are down. This may cause blackholing of the traffic.

- There are 3 operational enhancements w.r.t VLAN Interfaces

- Removal of shutdown/ no shutdown at vlan interface level.

- Removal of vlans information entirely from 'show ip interface brief' cmd

- Output of 'show vlan brief' reflects the 'State' of VLAN as ACTIVE/INACTIVE (along with inactive reason . 'member port down') based on member ports' state.

- Under certain conditions, MAC addresses may not be learnt even though ARP's may be learnt for those same MAC addresses

PVLAN

- Following PVLAN features are not supported in this release:

  - IGMP on PVLANS but there is no error message displayed if operator configures IGMP snooping on PVLAN

  - ARP & Routing in PVLAN domain

  - Enabling Routing in Primary and Secondary Vlans

  - CLI to Enable Local Proxy ARP on primary vlan

  - IP Configuration on PVLANS

  - Ve Configuration on Secondary Vlans

  - AMPP on PVLANS

  - In case of MSTP if a primary VLAN is added to the instance automatically secondary VLAN also added to the instance.

  - When the operator wants to delete the host association on a host port recommended to use " no switchport" rather than "no switchport private-vlan host-association". This is applicable only when the host port is untagged. When the host port is tagged both the commands can be used.

  - Primary VLAN ID needs to be lower than the secondary VLAN IDs. If primary VLAN ID is greater than secondary there is an issue with config replay

UDLD

- The UDLD protocol is not supported on the members of a Brocade trunk.

- The UDLD protocol is not compatible with Cisco's proprietary UDLD protocol.

- UDLD needs to use the higher timer in Scale and Stress environment.

STP/DiST

- VDX does not support tunneling non-standard BPDUs and thus IEEE BPDUs (0180:C200:0000) generated as tagged packets in STP/RSTP/MSTP modes may not be tunneled successfully across VCS fabric. However, VDX supports tunneling standards' based BPDUs such as untagged IEEE BPDUs and tagged or untagged PVST BPDUs (0100:0CCC:CCCD). Post 3.0.1, the tagged IEEE BPDU can be tunneled across VCS fabric using command: "tunnel tagged-ieee-bpdu" under interface configuration.

- In Fabric Cluster mode, global spanning-tree configurations (STP enable, STP Vlan configurations, STP over vLAG configurations) have to be performed in all the switches in VCS at the same time. For example, to run spanning-tree, it has to be enabled on all the switches including switches that don't have any edge ports.

- By default global spanning-tree and interface level spanning-tree will be disabled, user has to explicitly enable on the desired ports. vlan spanning-tree state is default enabled

- BPDU tunnel configurations are permitted only when spanning-tree is disabled in VCS.

- For cisco proprietary Per Vlan Spanning Tree protocols (PVST and RPVST) user needs to configure Brocade switch to send BPDU on Cisco multicast destination mac address "0100.0ccc.cccd" for non-native vlans. By default, NOS 4.1.0 software use's brocade "0304.0800.0700" multicast mac to send BPDU's on non-native vlans.

  Since NI/FI/Cisco boxes use Cisco multicast mac address to send spanning tree BPDU on non-native vlans, this configuration is needed in VDX switches to interoperate. This is an interface specific configuration

  Below is the example to configure Cisco BPDU mac for PVST and RPVST under interface mode,

```
VDX 6740-VCS1# conf t
VDX 6740-VCS1(config)# protocol spanning-tree rpvst
VDX 6740-VCS1(config-rpvst)# exit
VDX 6740-VCS1(config)# interface Port-channel 100
VDX 6740-VCS1(config-Port-channel-100)# spanning-tree bpdu-mac ?
Possible completions:
 0100.0ccc.cccd Cisco Control Mac
 0304.0800.0700 Brocade Control Mac
VDX 6740-VCS1(config-Port-channel-100)# spanning-tree bpdu-mac
0100.0ccc.cccd
VDX 6740-VCS1(config-Port-channel-100)# exit
VDX 6740-VCS1(config)#
```

Edge Loop Detection (ELD)

- ELD is supported on the edge ports that are connected either by end-hosts OR another switch OR another VCS.

- Maximum of 256 instances are supported in a fabric. Instance is counted per interface per vlan.

- To limit the number of instances utilized, it is recommended to enable ELD on only 1 vlan per interface.

- ELD is supported for edge interfaces connected to hosts too.

- . For 4.1.0 release, ELD can't be enabled for multiple vlans for an interface

- ELD may not be enabled after line card power cycle

AMPP and Port-Profiles

- Port-profile status does not reflect the remote interface info in VCS fabric mode.

- Native VLAN support inside AMPP does not honor the global enable/disable flag.

- SPAN destination port cannot be a profiled port.

- All AMPP features that were supported only on a physical interface on Brocade Network OS v2.0 are now supported on a VLAG in Brocade Network OS v2.1 and higher. However, only FCoE sub-profile is not supported in VLAG mode still.

  Brocade recommends deleting all manually created port-profiles when migrating from a legacy AMPP environment to VM Aware Network Automation.

- Vmkernel related port-profiles may unapply/reapply during HA resulting in vmotion failures.

- Default port-profile configuration is not the same as prior version. The "switch port trunk allow vlan all" that was present in prior version is removed. Other configuration stays the same.

- User defined port-profile-domain is introduced to control the VM mobility. Port-profile created must be explicitly associated with a profile domain.

- After upgrade, a new port-profile named UpgradedVlanProfile is auto-created. This profile has the single vlan profile that contains the "switch port trunk allow vlan all". This is the configuration that is present in the default port-profile of prior version

- After upgrade, a default port-profile-domain is created. This default domain contains all the existing user created port-profile and vCenter created auto-profiles prior to the upgrade plus the UpgradedVlanProfile

- Mac-based classification allowed only on access port-profile and C-tag classification allowed only on trunk port-profile

- When a port becomes a profiled-port, all SERVICE VFs in that domain are provisioned on this port.

- "Switch trunk allow vlan all" can only be present in one domain, It cannot co-exist with other c-tag based classifications in that domain.

- user is not allowed to edit/delete the default-profile-domain when Service VF is disabled

- New port-profile is not auto added to the default domain when Service VF is enabled. It can only be explicitly added to or removed from the default profile-domain.

- On disabling Service VF UpgradedVlanProfile should be re-configured with "switchport trunk allowed vlan all" in Default-profile-domain if it is removed /modified

- Newly created port-profiles which is not part of any domain should be added to the default-profile-domain explicitly while disabling the Service VF

- SERVICE VF classification cannot overlap across port-profiles in the same domain, but it can overlap across PP in different domains

vCenter

- VM-Aware Network Automation will work only with VMware vSphere version 4.0, 4.1, 5.0, 5.1 and 5.5.

- Receiving more than five vCenter events within a span of 30 seconds, results in asset discovery getting initiated. Post discovery cluster configuration will be in sync with vCenter.

- vCenter auto-profile is automatically added/deleted to the default profile-domain in Service VF enabled/disabled mode

- Modifying/editing the auto port-profiles in the default-domain is not recommended, which may cause auto-pp application failure during vcenter operation and end up in traffic failure

- Adding/removing the auto-port-profile to the user-created domain when Service VF is enabled is not recommended which may cause auto-pp application failure during vcenter operation and end up in traffic failure

- In Network OS v4.1.0, vCenter auto-profile does not support SERVICE VF classification.

QoS

- It is recommended to use the same CoS Tail drop threshold on all members of a port-channel to avoid unpredictable behavior.

- Asymmetric pause is supported on 1G port interfaces

- Flow control is disabled by default on all interfaces.

- Trust- support is available only standalone mode, no VCS mode
- DSCP to CoS Mutation- all platforms
- DSCP to Traffic Class Mutation -all platforms
- Priority 7 is reserved for control traffic on VDX switches. User data traffic should use priorities 0 through 6.
- Brocade VDX architecture prioritizes Unicast traffic over Broadcast or Multicast traffic under port congestion.

FCoE

- Brocade recommends that for all LAGs with FSB, the fcoeport config must be applied on the LAG itself and for all LAGs with directly attached CNAs, the fcoeport config must be applied on the member ports.
- If FCoE priority is changed from default to non-default, user might see that FCoE login may not happen. Please toggle the interface using "shutdown" followed by "no shutdown" to work this around.
- Binding an enode mac to FCoE interface is not allowed in range context, as only one enode mac can be bound to one FCoE interface
- While providing range for FCoE interfaces, it is recommended to provide the range only in ascending order. For example: interface fcoe 1/48/11-38 is recommended, interface fcoe 1/48/38-11 is not recommended
- FCoE traffic may not be mirrored using RSPAN. Workaround is to use SPAN
- In use cases with FSB, it is noticed that after converting dynamic port-channel to static, hosts and targets don't see each other.
- Some FCoE related commands take longer than 5 seconds to respond.
- "show fcoe fab default" takes 11 seconds
- "bind TenGigabitEthernet 3/0/42" takes 60 seconds

VRRP

- VRRP-E global sessions may get disabled after firmware upgrade
- Large VRRP config may increase config download time

OSPF

- Graceful restart is not supported

BGP

- Following BGP features are not supported in this release:
  - Graceful Restart
  - AS Confederation
  - Outbound Route Filtering capability
  - Extended Community Filter support
- BGP Aggregate route is preferred over direct network
- Standard and Extended community may be allowed to be configured on same interface

L2/L3 Multicast

- The following PIM features are not supported in this release:
  - Non-Stop Routing (NSR)
  - IP version 6
  - Prefix list
  - Configuring the switch as the BSR (Bootstrap Router) candidate.
  - Configuring the switch as the Rendezvous Point or Rendezvous Point candidate
- The Rendezvous Point (RP) must be configured outside the VCS cluster.
- All PIM enabled routers should be directly connected to RP
- IGMP Snooping must be enabled in all the switches in the VCS cluster.
- IGMP timers configured on PIM enabled L3 interface are not considered over the timers on VLAN
- CLI incorrectly allows same interface to be selected as incoming and outgoing interface for PIM-DR
- IGMP leave from one receiver will affect other receivers if connected through a vLAG
- IGMP join does not get forwarded via vLAG on shutting the primary port until general query is received
- PIM OIF list may not be updated when static IGMP group from VE is removed

Interoperability

- In a VPC environment where the Brocade VDX side has the active LACP settings and the Cisco side has the passive settings on the vLAG, the port-channel takes over 30 seconds to come up. Workaround: Reverse the settings and have the Brocade VDX LACP settings passive and the Cisco side set as active. The port channel will then restore after about 10 seconds.

- There is a compatibility issue between Brocade and Cisco chassis that can cause an LACP protocol timeout. If you have a Brocade VDX 6710 and a C24 VDX cluster and two Cisco Nexus 5k chassis configured in a VPC cluster using a combination of 1G fiber copper links, after shutting down links on the Cisco side, about 10 seconds of traffic loss can occur. The shutdown operation of the Nexus 1G port does not shut down the transmitter, so the Brocade VDX 6710 port is not able to detect link down. This leads to LACP protocol timeout.

- When interoperating with Brocade 8000, it is recommended to set the mac-aging time to 0 on the VDX switch to prevent any adverse impact caused by certain errors generated by the Brocade 8000.

- PVST-RPVST interop may not work between VDX and FCX/ICX

Miscellaneous

- Brocade VDX switches load balance internal and external traffic based on hash functions using standard network headers as keys. Due to this implementation, users may experience traffic imbalance depending upon application flow definition.

- Packet drops will be seen for a short duration due to routing changes with link flaps and/or node failovers.

- On both ISL and Edge ports, sFlow sampling is supported only in inbound direction.

- SFlow collectors are not queried in snmp v1, v2 & v3 versions

- If multiple VLANs are configured on a switch, then in order to enable certain features such as IGMP or PVST it is recommended that specific features be enabled on a per-VLAN basis instead of enabling them globally.

- "clear ip route all" need to be issued once the maximum number of routes supported by a router is exceeded.

- SNMPset operation is not fully supported

- Under rare conditions, the switch may bootup with default configuration on power-cycling the switch

- Firmware downgrade is not blocked if the scale configured would not be supported in the downgraded release

- Under rare conditions, after disabling keep alive timeout followed by shut & no shut of the port-channel link may prevent FCoE logins through that port-channel
- Please make sure to not have large no of unreachable TACACS+ accounting server configured, else it might cause unit to reboot. This issue is hit only with large config (4K vlan etc and 20K lines or config)
- The access-lists on Mgmt interfaces may not be effective during the bootup after the upgrade
- On CB500 system, "Restart BMC" function is available for the trouble shooting. The function is described as "Action" to BMC in "Hitachi Compute Blade 500 Series Web Console User’s Guide". If the function is performed, the link status between the mezzanine card and the DCB switch may stay down. In that case, please perform 'shutdown' and 'no shutdown' to the target port for the recovery.
- When the backuped configuration is restored on NOS 4.1.2, the management IP address in the management module must be set again. If the IP address is already set, it must be overwrite by the CLI or Web UI of the management module.

DHCP IP Helper

- When the DHCP relay configuration is also enabled on another VE interface on another RBridge the DHCP OFFER from the Server will get trapped and hence get dropped
- DHCP Relay Agent Information Option (option-82) is not supported in this Release

DHCP-based Firmware download (DAD. DHCP Automatic Deployment)

- DAD is dependent on DHCP, if DHCP is not enabled on management interface, DAD cannot function.
- In order for successful version upgrade using DAD method, switch should undergo 2 reloads.
- Config only download is not supported using DAD
- In FIPS mode, DAD is not supported.

3

New/Enhanced Feature Description

In this chapter, the New/Enhanced feature of the Network OS is described.

Network OS v4.1.3b includes support for new features such as DiST (STPoVCS), PVLAN, Uni-directional Link Detection (UDLD), Flow-based QOS, Flow-based sflow, RSPAN, Border Gateway Protocol (BGP), Inbuilt packet capture utility (PCAP), Management Services enhancements, DHCP IP Helper, DHCP-based Firmware download (DAD . DHCP Automatic Deployment), VRRP-E across VCS fabrics for embedded DCB switch module.

And, Network OS v4.1.3b deprecates 'ip gateway-address' CLI and replaces it by 'ip route' CLI

Descriptions of New Features

Distributed Spanning Tree Protocol (DiST/STPoVCS)

Network OS v4.1.2 and later supports any version of STP to run in VCS mode and function correctly between interconnecting VCSs, or between VCS and other vendor's switches. This feature is called Distributed Spanning Tree Protocol (DiST).

The purpose of DiST is:

- To support VCS to VCS connectivity and automatic loop detection and prevention.

- To assist deployment plans for integrating with the legacy xSTP enabled switches in the network, for eventual replacement of such switches with fabrics.

- Support following flavors of spanning-tree protocol: STP, RSTP, MSTP, PVST+, and RPVST+

Private VLAN (PVLAN)

A private VLAN divides the Layer 2 broadcast domain of a VLAN into subdomains, allowing you to isolate the ports on the switch from each other. A subdomain consists of a primary VLAN and one or more secondary VLANs. All VLANs in a private VLAN domain share the same primary VLAN. A private VLAN (PVLAN) domain is built with at least one pair of VLAN IDs; one (and only one) primary VLAN ID plus one or more secondary VLAN IDs. A primary VLAN is the unique and common VLAN identifier of the whole private VLAN domain and of all its VLAN ID pairs.

Secondary VLANs can be configured as one of two types; either isolated VLANs or community VLANs. Only one isolated VLAN can be part of one PVLAN domain.

A PVLAN is often used to isolate networks from security attacks, or to simplify IP address assignments.

UDLD (UniDirectional Link Detection)

UniDirectional Link Detection (UDLD) protocol is a nonstandard Layer 2 protocol that detects when a physical link becomes unidirectional by means of the exchange of UDLD protocol data units (PDUs). A unidirectional loop can lead to the creation of a loop in a network, which the Spanning Tree Protocol (STP) could inadvertently allow to occur.

This proprietary UDLD protocol is compatible only with the Brocade IP product line UDLD protocol. It can be configured on all physical ports in Standalone mode and on all physical edge ports in a Virtual Cluster Switching (VCS) environment. When a physical link is detected as unidirectional, traffic is blocked on the physical link. When a unidirectional link is detected as bidirectional, traffic is automatically unblocked on the physical link.

Flow based features (sFlow/QoS)

Flow-based sFlow is used to analyze a specific type of traffic (flow based on access control lists, or ACLs). This involves configuring an sFlow policy map and binding it to an interface.

RSPAN

RSPAN extends SPAN by enabling remote monitoring of multiple switches across your network.

The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The SPAN traffic from the sources is copied onto the RSPAN VLAN and then forwarded over trunk ports that are carrying the RSPAN VLAN to any RSPAN destination sessions monitoring the RSPAN VLAN.

Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) is an exterior gateway protocol that performs inter-autonomous system (AS) or inter-domain routing. It peers to other BGP-speaking systems over TCP to exchange network reachability and routing information.

Support for BGP on NOS platforms is for BGP4 (compliant with RFC 1771 and 4271), and provides the following:

- Connectivity from the VCS to a core/external network or cloud

Administrative distance for BGP routes cannot be changed using route-map configuration

Inbuilt packet capture utility (PCAP)

The packet capture utility, executed by means of the "capture packet interface" command, enables capturing packets from an interface that are to / from CPU, as well as transit packets if a trap is enabled by means of ACL logging. This command can provide significant help in debugging, especially for capturing & viewing Layer 2 TRILL and Layer 3 packets using "show capture packet". Moreover, the packets captured can be saved & exported in the PCAP format for enabling to be viewed offline using commonly used tools like WireShark.

Management Services

Brocade Network OS v4.1.3b supports various enhancements to existing management services, including TACACS+ and SNMP. SNMP supports v1/v2c/v3. SNMP is not cluster-aware. New supports added for 4.1.3b are:

- UDLD Traps
- Community MIB
- Password encryption for SNMPv3

Netconf Bulk config support is available for limited yang calls.

DHCP IP Helper

DHCP IP Helper (also known as DHCP Relay) allows DHCP Clients and DHCP servers on different subnets to communicate with each other. This is particularly important in large networks. The DHCP Relay can be configured on any L3 interface. An L3 interface can be a VE port or a physical port.

This feature helps consolidate the number of DHCP servers that need to be configured for a network.

DHCP Automatic Deployment (DAD)

DHCP Automatic Deployment (DAD) is a method used to download, install and bring up an embedded DCB switch module with new firmware or preset configuration automatically.

This method uses DHCP (option 66/67) to retrieve parameters such as firmware-path, VCS ID, RBridge-ID and the preset configuration file. These parameters are used to perform the firmware and configuration downloads.

This feature needs to be enabled via CLI. After the DAD process is completed, it is automatically disabled.

VRRP-E Across VCS fabric

NOS4.1.2 and later versions support VRRP-E across the VCS to VCS.

Mixed-version

A mixed-version Fabric Cluster is a group of fabric cluster nodes running Network OS v4.1.3b and Network OS v5.0.x. This allows legacy hardware to continue to function running 4.1.3b image along and co-exist with newer hardware running Network OS v5.0.x in the same cluster.

When a fabric cluster is loaded with mixed-versions, the cluster only works with the older feature set. Any cluster-wide features that were introduced in Network OS v5.0.0 are not supported in the mixed-version fabric cluster. Most fabric cluster features work properly in a mixed-version cluster. You can perform cluster management normally, as in a normal fabric cluster with all nodes running the same Network OS releases.

Mixed version between 4.1.3b & 5.0.x releases are supported only in "Fabric-Cluster" mode & not Logical-Chassis mode.

For complete information on mixed-version support, refer to the Network OS Administrator's Guide.

4

Firmware Upgrade and Downgrades

In this chapter, the procedure of upgrade and downgrades for Network OS is described.

Upgrade considerations

Upgrade from NOS 2.0.1_katx and NOS 3.0.0_dcbx to NOS 4.1.3b is supported for the embedded DCB switch module. Due to potential compatibility issues, Brocade does not recommend downgrading from NOS 4.1.3b to NOS 2.0.1_katx and NOS 3.0.0_dcbx.

Please refer to the NOS 4.1.x Administrator Guide for details regarding firmware upgrade and downgrade.

Note: Installing Brocade Network OS is service disruptive and any un-saved running configuration will be lost during the installation.

Switches operating with earlier versions of Brocade Network OS, including Brocade Network OS v2.0.1_katx, should first be upgraded to Brocade Network OS v3.0.0_dcb4, then to Brocade Network OS v4.1.3b.

Upgrading Equipment parameter is necessary before upgrading Network OS to v4.1.3b.

Incompatibility between NOS 3.0.0_dcbx and NOS 4.1.3b

The followings show the consideration for upgrading to NOS 4.1.3b on the incompatibility point of view between NOS 3.0.0_dcbx and NOS 4.1.3b.

DHCP setting, which is enabled in default startup-config, will disruptive management access from the management module. DHCP setting has to disable using 'no dhcp' before upgrading.

In Network OS 4.1.3b, admin in Standalone (SA) mode and VCS fabric cluster (FC) mode has to use "ip route 0.0.0.0/0 <gateway ip>" command to configure the gateway.

Prior to 3.0.0_dcb3, there was an option to configure the gateway under the interface management. However this would error out on configuration. In 4.0 this option itself is not supported.

In FC mode this command is available under RB context, whereas in SA mode the same is available in configuration mode

After upgrading to NOS 4.1.3b remove the old gateway using "no ip route" command and configure the new route with high metric, otherwise both of the gateways (old and new) will form ECMP.

Incompatibility between NOS 2.0.1_katx and NOS 4.1.3b

The followings show the consideration for upgrading to NOS 4.1.3b on the incompatibility point of view between NOS 2.0.1_katx and NOS 4.1.3b.

If the following settings are included in startup-config, they are ignored and deleted at bootup.

- **Inband management IP address** – As VE interface is supported in NOS 4.1.3b newly, an inband management IP address is assigned to the VE interface instead of VLAN interface. The management IP address has to be assigned to VE interface after upgrading.
- **MAC ACL** – The necessary operand for MAC ACL configuration is added. MAC ACL configuration has to be re-configured according to new CLI format after upgrading.
- **SNMP v3 user with passwords** – The configured user with password will not be persistent across firmware upgrade/downgrade. Please re-configure the new user after the firmware downgrade / upgrade.

Adding a switch running Brocade Network OS 2.0.1_katx to Brocade Network OS v4.1.3b cluster

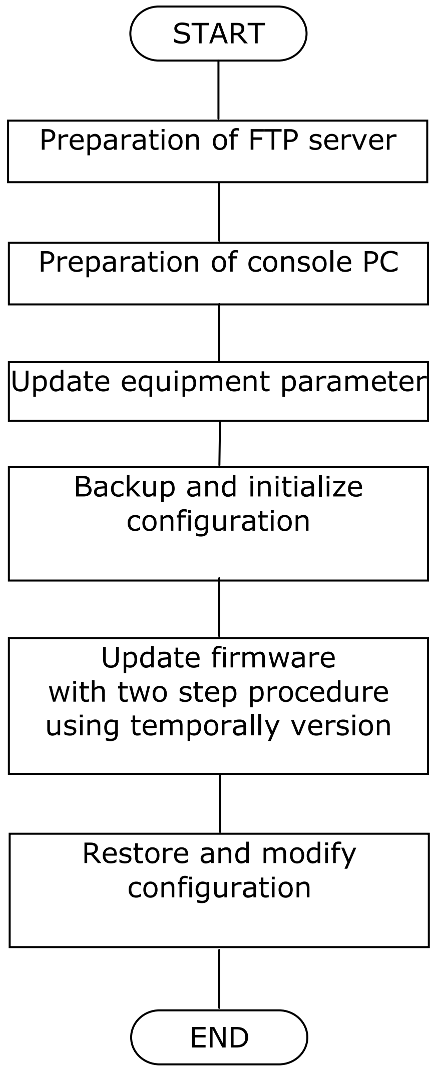
- Brocade Network OS 2.0.1_katx switch would not interoperate with Brocade Network OS 4.1.3b.
- ISLs will be segmented with a reason of FDS mode mismatch.

Adding a switch running Brocade Network OS v3.0.0_dcbx to Brocade Network OS 4.1.3b cluster

- Brocade Network OS 3.0.0_dcbx switch would not interoperate with Brocade Network OS 4.1.3b.
- ISLs will be segmented with a reason of FDS mode mismatch.

Procedure summary

The following shows work flow of the update procedure.


START
Preparation of FTP server
Preparation of console PC
Update equipment parameter
Backup and initialize configuration
Update firmware with two step procedure using temporally version
Restore and modify configuration
END

Target product

Target product of this guide is

Product name	Product code	Available NOS version
Brocade 10Gbps DCB switch module	GG-BE3LSW3X1-Y GV-BE2LSW3X1-Y	4.1.3b

Notice for update work

i. Please refer to the following guides before NOS update work.

- Brocade Network OS Network OS Update Guide for 4.1.0
- Brocade Network OS Command Reference
- Hitachi Compute Blade 500 Series Startup guide
- Hitachi Compute Blade 500 Series Management Module Setup Guide
- Hitachi Compute Blade 2000 USER'S GUIDE

ii. FTP server is needed for NOS update work. Please confirm an available FTP server in customer's network.

iii. In this guide, the external LAN port of the management module is used in the update procedure of NOS. Before update work, please setup the external LAN port (MGMT0 or MGMT1) to be communicated with the DCB switch module and assign an IP address to the management port of DCB switch module.

[How to setup the external LAN port]

At the CB500 system, set "Connect through management LAN port " to Connect Type of IP address tab in Management LAN section through the Web console of the management module, or set "mgmt" to Connection type of the switch module with 'set sw-module mgmt-lan' command of the management module.

At CB2000 system, set "Ext" to Ext setting for the switch module in 'LC' command menu of the management module.

iv. Please assign the same IP segment of the management module to both the management IP address of DCB switch module and FTP server. This guide describes the procedure with the following IP address settings.

The management module:	192.168.0.1
The DCB switch module:	192.168.0.7x (x: the slot number of the switch module)
PC (FTP server):	192.168.0.100

v. Hitachi recommends that NOS update should be executed at out of business time or under closing (shutdown) all ports of DCB switch module, because NOS update corrupts network communication through the DCB switch module.

vi. Please execute update work by the user account with administrator role.

vii. When downgrading from Network OS v4.1.x to Network OS v3.0.0_dcb3, please downgrade to Network OS v3.0.0_dcb4 at first. Then downgrade to Network OS v3.0.0_dcb3.

viii. During the downgrade from Network OS v4.1.x to Network OS v3.0.0_dcb4

- If the DCB switch is in Logical Chassis mode, it must be converted to Fabric Cluster mode before starting the downgrade.

- Please use “default-config” option along with “firmware download” command. “interactive” option cannot use for downgrading to Network OS v3.0.0_dcb4.

Preparation

Preparation of FTP server

FTP server is needed for update work. This guide described the update procedure as the premise that FTP server perform on the console PC.

Connecting the console PC to Compute Blade

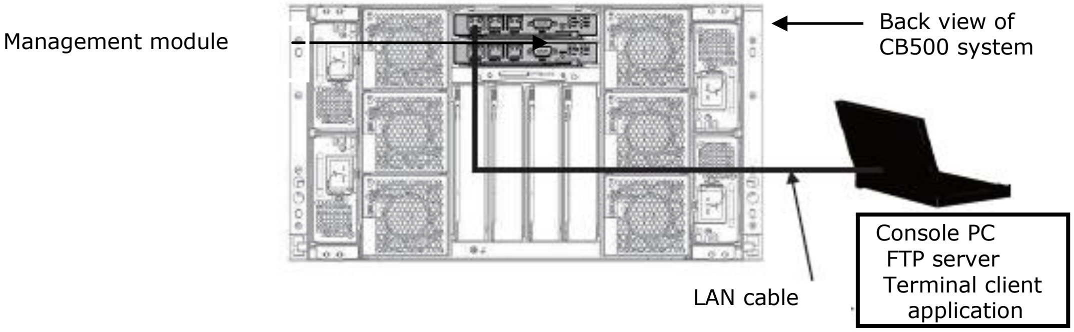
As the all embedded modules by an internal network on the management module, the management port of DCB switch module is accessible with the connection to the LAN port (MGMT0 or MGMT1) of the management module. Please refer to "Connecting management module" of "Hitachi Compute Blade 500 Series Management Module Setup Guide" or "Cable Connection for the System Console" of "Hitachi Compute Blade 2000 USER'S GUIDE" for the connection to the management module.

NOTE

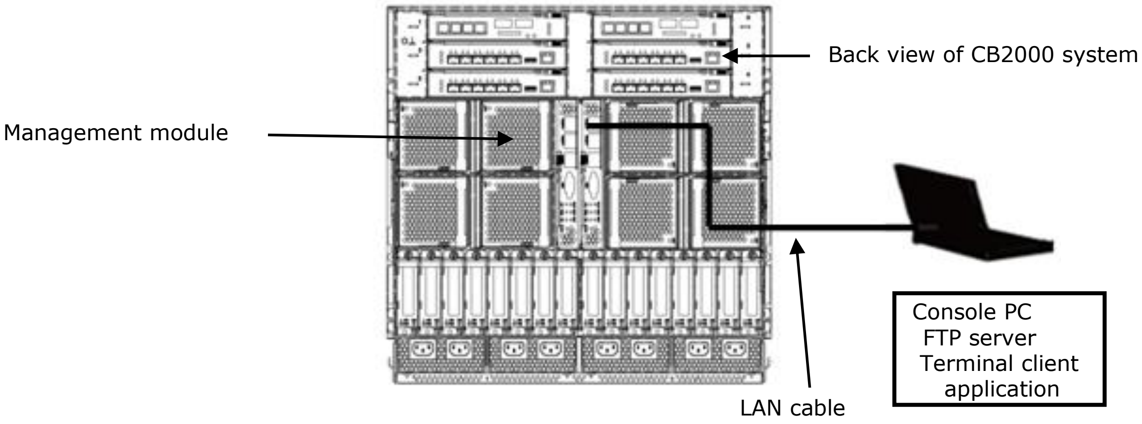
If the factory default setting is maintained, please use LAN port (MGMT0).

If the connection procedure is modified to LAN port (MGMT1), please use LAN port (MGMT1).

[connecting at CB500]



[connecting at CB2000]



Starting FTP server and confirmation

Please start FTP server on the console PC and confirm the settings to FTP server, which are user name, password and the folder to be unarchived NOS image files to, by login to FTP server from the console PC. The following shows the sample setting of FTP server in this guide.

user name: upload

password: password

folder: C\inetpub\ftproot

Preparation of NOS image files on FTP server

For updating to NOS 4.1.3b, the archived file named 'nos4.1.3b.tar.gz' and 'nos3.0.0_dcb4.tar.gz' are needed. Please consult with OEM partner and get the archived file.

The archived file:'nos4.1.3b.tar.gz' and 'nos3.0.0_dcb4.tar.gz' should be stored in the ftp root folder of FTP server, and please unarchive it to the folder named 'nos4.1.3b' and 'nos3.0.0'. These 'nos4.1.3b' and 'nos3.0.0' will be used in section "Apply updated firmware".

Update the equipment parameter

Please login to the management module of CB500/CB2000 and apply the equipment parameter with the following version.

CB500: 1014 or higher

CB2000: A012 or higher

Regarding how to login to the management module and how to apply the equipment parameter, please refer to the Hitachi Compute Blade USER'S GUIDE of each system. And, the all DCBSW module must be performed power cycle once after updating the new equipment parameter to make it effective.

Backup configuration

Login to the DCB switch module

Please login to the DCB switch module according to the following procedure.

Login to the DCB switch module at the case of CB500

i. Start a terminal emulation application, and telnet to the management module with the management IP address.

```
telnet "IP address of the management module"[Enter]
```

ii. Login to the management module by entering user name and password. If login successfully, the prompt of (0)$ is appeared. In the following sample, 'administrator' as user name and 'password' as password, which are factory default setting, are used.

```
login: administrator [Enter]
Password: password [Enter]   <-- ‘password’is not shown
Last login: Mon Jun  3 02:46:28 from 192.168.0.100
BladeSymphony BS500 Management Module
ALL RIGHTS RESERVED, COPYRIGHT (C), 2011, 2014, HITACHI, LTD.
Chassis ID        :
Firmware Revision : A0145-G-7300
(0)$
```

iii. Change the internal LAN connection to DCB switch module with 'change console' command. If success to connect to the DCB switch module, the prompt '#' of the DCB switch module is appeared. The following shows the sample of the connection to the DCB switch module mounted on switch slot #2.

```
(0)$ change console -s 2 -F [Enter]
Welcome to the Brocade Network Operating System Software
ssouser$ connected from 192.168.0.1 using console on switch
sw0#
```

Login to the DCB switch module at the case of CB2000

i. Start a terminal emulation application, and telnet to the management module with the management IP address.

```
telnet "IP address of the management module"[Enter]
```

ii. Login to the management module by entering user name and password. If success to login to the management module, the main menu of system console is appeared. In the following sample, 'administrator' as user name and 'password' as password, which are factory default setting, are used.

```
login: administrator [Enter]
Password: password [Enter]   <-- 'password'is not shown
BladeSymphony BS2000 Management Module
ALL RIGHTS RESERVED, COPYRIGHT (C), 2008, 2014, HITACHI, LTD.
Chassis ID        :  XXXXXXXXXX
Firmware Revision : XXXXXXXXXXX

<< System Console Main Menu >>

    P. Start OS console session.
   SW. Start switch module console session.
    S. System command mode.
    X. Exit.
(P,SW,S,X) :
```

iii. Enter 'sw' to the prompt of the system console main menu, and select a target DCB switch module. If success to connect the DCB switch module, the login prompt of DCB switch module is appeared.

```
(P,SW,S,X) : SW [Enter]
Select switch module (0-5,[Q=Quit]) : 2 [Enter]
Confirm? (Y,[N]) : Y [Enter]
nos2.0.1_katX
sw0 login:
```

iv. Login to the DCB switch module using the user name and the password of DCB switch module. If success to login to DCB switch module, the prompt '#' of the DCB switch module is appeared. In the following sample, 'admin' as user name and 'password' as password, which are factory default setting, are used.

```
sw0 login: admin [Enter]
Password: password [Enter]   <-- 'password'is not shown
WARNING: The default password of 'admin' and 'user' accounts have not been changed.
Welcome to the Brocade Network Operating System Software
admin connected from 192.168.253.33 using console on switch
sw0#
```

Backup of the configuration file

Before NOS update work, please get the backup of DCB switch configuration as the following steps. The backup in the steps will be used for being applied to 'startup-config' in the section "Download and apply the backuped configuration file".

i. Upload the configuration file of DCB switch module

Please upload the configuration file of DCB switch module using 'copy' command. In the following sample, upload the 'startup-config' to FTP server as the name of "Config_SW1_mmdd".

```
sw0# copy startup-config
ftp://upload:password@192.168.0.100/Config_SW1_mmdd[Enter]
sw0#

upload:  the user name of FTP server
password:  the password of FTP server
```

(*): The IP address of FTP server is the IP address of the console PC which FTP server running on.

Apply the default configuration of the DCB switch module

In the case of an update from NOS v2.0.1 kat4 and NOS v3.0.0_dcb3, for shortening the time of reboot in NOS update work, first, please apply the default configuration to DCB switch module.

i. Confirm the operational mode of DCB switch module using 'show vcs' command

After entering 'show vcs' command, please write down 'vcsid' and 'rbridgeid' in the output of 'show vcs' command for recovering vcs mode. If the DCB switch module does not running in VCS mode, please ignore this step and execute step (5).

```
sw0# show vcs [Enter]

[example in VCS mode]
state       : Enabled
vcsid       : 1          }  Write down 'vcsid' and 'rbridgeid'
rbridgeid   : 16         }

[Example in standalone mode(non VCS mode)]
state       : Disabled
```

ii. Change VCS mode to standalone mode using 'no vcs enable' command

```
sw0# no vcs enable [Enter]
This operation will change the configuration to default and reboot the switch. Do
you want to continue? [y/n]:y [Enter]

Broadcast message from root Tue Jul  9 11:31:19 2013...

The system is going down for reboot NOW !!
```

iii. Re-login to the DCB switch module

Please login to the DCB switch module again according to the procedure in "Login to the DCB switch module" about 5 minutes later from appearing the message of "`The system is going down for reboot NOW !!`".

iv. Confirm that the operational mode is standalone mode using 'show vcs' command

```
sw0# show vcs [Enter]
state      : Disabled
```

v. Apply the default configuration to the DCB switch module

```
 sw0# copy default-config startup-config [Enter]
 This operation will modify your startup configuration. Do you want to continue?
[y/n]:y [Enter]
 sw0#
```

Apply updated firmware

As described in the section "Upgrade considerations", Network OS v3.0.0_dcb4 should be applied before v4.1.x. In this section, update procedure using Network OS v4.1.x is described. Please apply Network OS v3.0.0_dcb4 according to the procedure in this section by reading in the v3.0.0_dcb4 version before applying v4.1.x.

Execute NOS update

NOS update is downloading NOS image files to the DCB switch and applying those files using '`firmware download`' command. Never turn off the DCB switch module or unplug the LAN cable.

i. Execute 'firmware download' with entering 'n' for the message of "Do Auto-Commit after Reboot?" as the following sample.

```
sw0# firmware download interactive [Enter]
Server name or IP address: 192.168.0.100  [Enter]  <-- the IP address of FTP server(*)
File name: nos4.1.3a [Enter]    <-- the folder name unarchived in section 4 (3)
Protocol (ftp, scp): ftp [Enter]
User: upload [Enter]                        <-- the user name of FTP server
Password: password [Enter]                  <-- the password of FTP server
Reboot system after download? [y/n]:y [Enter]
Do Auto-Commit after Reboot? [y/n]:n [Enter]
Checking conditions for downloading to 3.0.x

System sanity check passed.

Do you want to continue? [y/n]:y [Enter]

   <<< snip >>>

dir-1.0.5-5
############################### [ 100% ]
ldconfig-2.16.2-4
############################### [ 100% ]
glibc-te500v2-2.8.74-7
############################### [ 100% ]
bash-2.05-9
############################### [ 100% ]

   <<< snip >>>

Start to install packages...
All packages have been downloaded successfully.
Firmware has been downloaded to the secondary partition of the switch.

Broadcast message from root ddd MMM DD hh:mm:ss YYYY...

The system is going down for reboot NOW !!
```

(*): The IP address of FTP server is the IP address of the console PC which FTP server running on.

It will take about 20 minutes for downloading NOS image files.

If downloading is success, the DCB switch will reboot automatically and the communication of telnet will be terminated.

If downloading NOS fails to start, please check the following points and retry to download.

- Is FTP server running?
- Is the setting of FTP server, the account information and folder of the FTP server, correct?
- Is the NOS image file unarchived correctly?

Re-connect the DCB switch module and commit of NOS update

Before login to the DCB switch module, please set the IP address from the management module console again to restore the IP address of DCB switch management port

And, please login to the DCB switch module again for the commit of NOS update.

i. Re-login to the DCB switch module

Please login to the DCB switch module again according to the procedure in "Login to the DCB switch module" about 10 minutes later from appearing the message of "`The system is going down for reboot NOW !!`".

ii. Commit of NOS update

Please commit the NOS update using '`firmware commit`' command. Please wait for the message "`The command has completed successfully.`"

```
sw0# firmware commit [Enter]


The command has completed successfully.
sw0#
```

Check the status of NOS update

To check the completion of NOS update to expected version, please execute the following steps.

i. Please check that the version of both "Primary" and "Secondary" are "4.1.3b" using 'show version' command.

```
sw0# show version [Enter]

Network Operating System Software
Network Operating System Version: 4.1.3b
Copyright (c) 1995-2012 Brocade Communications Systems, Inc.
Firmware name:      4.1.3b
Build Time:         hh:mm:ss MMM DD, YYYY
Install Time:       hh:mm:ss MMM DD, YYYY
Kernel:             2.6.34.6
BootProm:           2.2.0
Control Processor:  e500v2 with 2048 MB of memory

Appl     Primary/Secondary Versions
------------------------------------------
NOS      4.1.3b
         4.1.3b
```

Restore configuration

Recover to VCS mode

If the operational mode before this work is VCS mode or applied the default configuration in the previous work, please recover to VCS mode. If the operational mode is standalone, please skip this section and continue from "Download and apply the backuped configuration file".

i. Please enter 'vcs enable' command with 'vcsid' and 'rbridgeid' written down in "Apply the default configuration of the DCB switch module".

```
sw0# vcs vcsid 1 rbridge-id 16 enable [Enter]
This operation will change the configuration to default and reboot the switch. If
this switch is being added to an existing vcs-cluster, the vCenter and Virtual IP
configurations of the cluster might be lost. Please follow the procedure outlined
in the release notes to add a node to an existing cluster. Do you want to
continue? [y/n]:y [Enter]
```

Re-connect the DCB switch module and check VCS mode

To confirm that the operational mode is VCS mode, please login to the DCB switch module.

i. Please login to the DCB switch module again according to the procedure in "Login to the DCB switch module" about 5 minutes later from "Re-connect the DCB switch module and check VCS mode"

ii. Confirm that the operational mode is VCS mode using 'show vcs' command.

```
sw0# show vcs [Enter]
Config Mode     : Local-Only
VCS ID          : 1
Total Number of Nodes           : 1
Rbridge-Id       WWN                            Management IP   Status
HostName
--------------------------------------------------------------------------------
-------
16              >XX:XX:XX:XX:XX:XX:XX:XX*       XXX.XXX.XXX.XXX    Online
sw0
```

Download and apply the backuped configuration file

Please download the backuped configuration file in "Backup configuration" to the startup-file. And restart the DCB switch module to enable the setting of the configuration file.

i. Download the backuped configuration file

Please download the backuped configuration file to the DCB switch module using 'copy' command. In the following sample, the configuration file named as "Config_SW1_mmdd" on the FTP server is downloaded to the startup-config.

```
sw0# copy ftp://upload:password@192.168.0.100/Config_SW1_mmdd startup-config
[Enter]
This operation will modify your startup configuration. Do you want to continue?
[y/n]: y [Enter]
Startup configuration file was copied successfully.

upload: the user name of FTP server
password: the password of FTP server
192.168.0.100: the IP address of FTP server(*)
```

(*): The IP address of FTP server is the IP address of the console PC which FTP server running on.

ii. To enable over written startup-config, please restart the DCB switch module using 'reload' command.

```
sw0# reload [Enter]

Warning: Unsaved configuration will be lost. Please run `copy running-config
startup-config` to save the current configuration if not done already.

Are you sure you want to reload the switch? [y/n]:y [Enter]
The system is going down for reload NOW !!
```

Re-connect to the DCB switch module

Before login to the DCB switch module, please set the IP address from the management module console again to restore the IP address of DCB switch management port.

For the following procedure, please connect and login to the DCB switch module again.

i. Re-login to the DCB switch module

Please login to the DCB switch module again according to the procedure in "Login to the DCB switch module" about 10 minutes later from appearing the message of "`The system is going down for reboot NOW !!`".

Backup the latest configuration

Please backup the latest configuration for the latest NOS version according to the procedure in "Backup configuration" again for the accident.

The backuped configuration should be stored in safety location.

5

Software Fixes

In this chapter, the defects closed with a code change in Network OS v4.1.3b are described.

Closed with Code Change in Network OS v4.1.3b

The following defects as critical issues had closed between Network OS v4.1.3a and v4.1.3b.

For the details and another defect, please refer to the Release Notes of Network OS v4.1.3b for Brocade VDX at http://my.brocade.com/.

- Ping to VRRP virtual-IP address fails and traffic loss occurs. (DEFECT000540588)
- During an extended power cycle test overnight, one of the ports would stay admin down. (DEFECT000542160)
- Unexpected reload can happen with CLI “no interface vlan”. (DEFECT000510350)
- Applying access lists causing rules to fail after a few successful passthroughs. (DEFECT000523004)
- ISL between ports may not come online. (DEFECT000533780)
- Switch is not using the configured DHCP Gateway IP Address. (DEFECT000537283)
- Multicast packets with source IP as 0.0.0.0 is not forwarded by VDX. (DEFECT000541649)
- Switch may become unresponsive during heavy CPU usage. (DEFECT000544753)
- Switch might experience an unexpected reload during boot process, if inband virtual-ip is configured. (DEFECT000550010)

A. Modifications for Hitachi

In this chapter, the customization feature of Network OS for Hitachi, Ltd. is described.

Port Association Feature (track command)

Overview

The port association feature facilitates the automatic shutdown of the internal (downlink) ports on external (up link) ports or LAG failure. It automatically brings up the associated internal ports when external ports or LAGs come online.

Each internal port is optionally configured to follow an external port or LAG/trunk. On external link failure (or LAG failure), corresponding internal ports are shutdown. When the link comes up (LAGs come up), it causes the corresponding internal ports to be brought up.

In case of LAGs, the user can define the threshold limit of minimum operational links to declare LAG state as up or not. When the number of links that are up is below this limit, LAG is considered as down and doesn't come up until the limit is reached.

CLI

```
[no] track interface ethernet <rbridge_id>/slot/port
[no] track interface port-channel <port_channel_number>
```

This command is allowed under internal port interface sub-mode. Using this command, the user can track one or more external ports. Only external physical interfaces and port-channel interfaces are allowed to be tracked.

The show output for internal interfaces will include the information of which external interfaces are being tracked.

```
[no] track enable
```

This command is used to enable/disable tracking under internal interface sub-mode. External interfaces are started to be tracked only if tracking is enabled by means of this command.

Examples

```
kat2360# configure
Entering configuration mode terminal
kat2360(config)# interface TenGigabitEthernet 0/24
kat2360(conf-if-te-0/24)# track enable
kat2360(conf-if-te-0/24)# track interface ethernet 0/1
kat2360(conf-if-te-0/24)# track interface ethernet 0/2
```

In the above example, on the internal interface 0/24, tracking has been enabled and external interfaces 0/1 and 0/2 are tracked.

Command Semantics

The semantics of the above commands are as follows:

- One internal interface can track one or more external interfaces.
- When the external interface goes down, the admin and operational status (line protocol) of the internal interface which is tracking the external interface, also goes down.
- Multiple internal interfaces can track the same external interface.
- If multiple external interfaces are being tracked by one internal interface, the internal interface should go down only if all of them go down.
- Only the operational status of the external interface is tracked – not the admin state. This means that if the admin state of the external interface goes down and the line protocol (i.e. operational state) of the external interface is still up, then the internal interface should not go down. However, when operational status of the external interface goes down, the admin and operational status of the internal interface goes down.
- If multiple internal interfaces are tracking a single external interface and if the external interface goes down, all of the internal interfaces should go down.
- A maximum of 8 external interfaces can be tracked from an internal interface.
- Forward referenced port-channels (non-existing port-channel) should be allowed to be tracked.
- The two functionalities ([no] Track interface ethernet slot/port and [no] Track enable) are independent of each other. Executing 'no track enable' does not remove the tracked interfaces list from the internal interface, and executing 'track enable' on the internal interface again will resume tracking of the external interfaces.

Caution

If you configure 1 internal port to track by 3 external ports, disabling the tracked external port causes to go all internal ports down as design. But, after the following operations, all internal ports become enabled. In this case, please unplug all cables connected external port before reload and plug again after reload.

```
copy running-config startup-config
reload
```

802.3 Clause 37 1 Gbps AN support

Overview

A new CLI option '1000-auto' has been added to the 'speed' CLI to support '802.3 Clause 37' 1 Gbps Auto Negotiation. This CLI is only supported on internal ports.

```
sw0(conf-if-te-65/0/10)# speed ?
Possible completions:
[auto]
1000             1Gbps
1000-auto        1Gbps AN (802.3 Clause 37 Auto-Negotiation)
10000            10Gbps
auto             Auto negotiation (default)
```

Show Enclosure Command

Overview

Shows the chassis model name and bay ID in which the switch is inserted.

```
#Show enclosure
Possible completions:
modelname       Provides Chassis model name
slotid          Provides Present Slot Id of switch
```

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0) 1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems