HITACHI
Inspire the Next

Readme for Network OS v.3.0.0_dcb3
Appendix for Administrator Guide

Hitachi Data Systems

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 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 v.3.0.0_dcb3.

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 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: [<u>a</u> | 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!**

Network OS 3.0.0_dcb overview

In this chapter, the overview of Network OS 3.0.0_dcb is described.

Brocade Network Operating System (NOS) v.3.0.0_dcb is a major release to support improved scalability numbers and several new features. All features supported in NOS v.2.0.1 kat4 are also supported in v.3.0.0_dcb.

NOS v.3.0.0_dcb includes support for new features such as FCoE feature, Layer 3 capabilities, Edge Loop Detection (ELD), BPDU Drop, Fabric Watch, Management PING/Traceroute, Management ACL, Virtual IP Management and others.

☐ New/Enhanced Feature Outline

New/Enhanced Feature Outline

In NOS 3.0.0_dcb, the following feature is supported newly or enhanced.

- Layer 2 enhancement

    - Edge Loop Detection (ELD)

    - BPDU Drop

    - BTRUNK Support in VCS mode

    - Configurable Load Balancing

    - Configurable Tail Drop Threshold

    - IGMP Dynamic m-router over VLAG

- Layer 3 feature support

    - IPv4 unicast routing /Static Routes in VCS

    - Layer 3 ACL's in VCS

    - Layer 3 QoS

    - VRRP and Brocade VRRP-E in VCS

- FCoE support

    - FCoE Over LAG

    - Zoning and Zone Alias Names

- AMPP enhancement

    - AMPP over VLAG

- vLAG enhancement

    - VLAG Minimum Links

    - VLAGs with 32 ports

- Management feature enhancement

    - DNS Configuration

    - DOT1X Readiness Check

    - Fabric Watch

- IP ACL for Management Interface

- IPv4 and IPv6 Management Services in VCS

- Management PING and Traceroute

- New MIBs for SNMP

- sFLOW Auto Adjust and Backoff

- Virtual IP Address

Prerequisites of Network OS 3.0.0_dcb

In this chapter, the prerequisites for Network OS 3.0.0_dcb are described.

This chapter provides fundamental information about Network OS 3.0.0_dcb as exemplified by the optional license, the standard compliance, scalability and compatibility.

Additionally the important notes described about the features of Network OS 3.0.0_dcb.

☐ OPTIONAL LICENSED SOFTWARE

☐ Standards Compliance

☐ Scalability

☐ Compatibility

☐ Documentation Updates

☐ IMPORTANT NOTES

☐ Unsupported feature for the embedded DCB switch module

OPTIONAL LICENSED SOFTWARE

FCoE and VCS capabilities can be enabled on the base SKU by adding software licenses.

- **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.

- **Brocade VCS license** — Allows formation of VCS fabrics with more than two switches, providing Virtual Cluster Switching for advanced virtualization and simplification of Ethernet fabrics. All switches participating in a VCS fabric with more than two switches must have the Brocade VCS license installed.

Software licenses are available in following formats.

Software License	SKU Description
GG-BE3LSL1X1-Y	VCS license
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 is interoperable at Layer 2 with standard Ethernet interfaces with other industry standard switches. The specifics of supported standards are listed in the release-notes under "Standards Compliance" topic. Please note that VDX switches in VCS mode do not participate in STP at this time.

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 v3.0.0 Scalability Limits	Standalone	VCS Fabric
Maximum # of VLANs	3,500[1]	3,500[1]
Maximum # of MAC addresses	30,000	30,000
Maximum # of port profiles(AMPP)	256	256
Maximum # of per priority pause levels	8	8
Maximum # of L2 multicast group	2,000	2,000
Maximum # of MSTP instance	32	N/A
Maximum # of LAG groups (Platform dependent)	60	As many ports as available
Maximum # of members in a standard LAG	16	16
Maximum # of members in a Brocade LAG	8	8
Maximum # of switches in a Fabric	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	32
Maximum # of nodes in a VLAG	N/A	4
Maximum cable length for lossless connectivity	300m	300m
Maximum # of VLANS in port profiles	3,500[1]	3,500[1]
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	128
Maximum Total # of L2 + L3 ACL rules	1,300	1,300
Maximum # VLAN per Edge Port in Trunk Mode Port	750	750
Maximum # of Enodes per Fabric	N/A	1,000
Maximum # of FCoE interfaces (Platform Dependent)	N/A	1,000
Maximum # of FCoE Devices per Fabric	N/A	1,000
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	100	100

---

1 In 3.0.0_dcb, maximum # of VLAN is limited to 1024.

Maximum # of VMs supported in VM Aware Network Automation	8,000	8,000
Maximum # of ARP Entries	16,000	16,000
Maximum # of routes supported in OS	N/A	1,500
Maximum # of static routes	N/A	500
Maximum # of dynamic routes	N/A	1,000
Maximum # of VRRP instances per system	N/A	24
Maximum # of VRRP instances per interface	N/A	8
Maximum # of routers participating in a VRRP-E session	N/A	8
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 SVIs per system	N/A	128
Maximum # of secondary IP address	N/A	255

Compatibility

In standalone mode, which means in traditional ethernet network, 3.0.0_dcb 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.

In VCS Fabric mode, 3.0.0_dcb has the connectivity to only Brocade NOS 3.0.1 into same fabric. If 3.0.0_dcb connects to other than Brocade NOS 3.0.1, 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 3.0.0 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 3.0.0 documents are recommended references.

1. Network OS Administrator Guide Part # 53-1002561-02

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

3. Network OS Command Reference Part # 53-1002562-03

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.

VCS Fabric Support

- Switch, Domain, and RBridge ID all refer to the same node in the cluster.

- Frames with a hop count of zero (after decrementing) will be discarded instead of being forwarded.

- Changing the RBridge ID of a switch is disruptive. The system will be rebooted with the default configuration.

- Clearing dynamic MACs with live traffic may not clear all MACs across the cluster under some scenarios.

- When non-VCS switches are connected to a VCS fabric and STP is enabled on the Edge switches, the edge-ports of the Fabric connecting the STP-based switches should be configured with the 'switchport' command to allow BPDUs to tunnel through the fabric.

FCoE

- FCoE is only supported in VCS Fabric Mode.

- Boot over SAN/SAN Boot is not supported.

Command Line Interface

- Some commands will not produce paginated output.

- 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 NOS release, but are still shown as options. These will be applicable and supported in future NOS 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.

- Some CLI commands under RBAC were obsoleted and do not exist already.

- The 'no' command always exists for all roles even if it is not required.

- With respect to interface 'tengigabitethernet instance' sub mode:

    - "dot1x" option can be configured only if the role has "read-write" operation and "accept" action for both "dot1x" command interface te instances.

    - To perform 'no vlan', and 'no spanning-tree' on any instance, the user must have "read-write, accept" permission for 'vlan' and 'protocol spanning-tree' commands, "read-write, accept" permission for at least one interface tengigabitethernet instance, and "read-write/read-only, accept" permission for all other instances.

Non-Supported Functionality for Ports in 1G Mode

- FCoE

- Brocade LAG

- External loopback detection

- RMON stats are calculated incorrectly for packet sizes 64-127 bytes

- Brocade Trunks cannot be formed with 1G ISLs – all Brocade Trunks should be 10G ISLs

Trunking

- Brocade trunk has a maximum throughput of 80 Mbps. Full link utilization of 8 ports in a trunk group is achievable with larger packet size (>128 bytes).

Spanning

- To configure a span session, ensure that lldp is disabled from the desired destination port. The command to disable lldp under the desired interface is 'lldp disable'.

- CPU-originated packets cannot be output spanned on the embedded DCB switch module.

- SPAN is supported only within a port-group on the embedded DCB switch module.

    ''spanning-tree autoedge" option does not work after reload. If it is sure there is no loop in farther connection to a port, "spanning-tree edgeport" option should be configured to the prot.

AMPP and Port-Profiles

- Port-profile status does not reflect the remote interface information in Fabric mode.

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

- AMPP configuration works on physical interfaces (non-trunk ports) only.

Firmware Installation

- An extended timeout period may be experienced when attempting to download firmware to a switch from a network server that becomes unreachable.

- Start-up SNMP notifications (traps and informs), coldStart, linkup, linkDown may be seen after a firmware download.

Security, ACLs, Authentication, Authorization

- ACLs are not supported for egress traffic flows.

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

- To perform some of the 'clear' and 'show' operations for interface 10GbE instances, users must have at least "read-only, accept" permission for the related instances.

- There is a possibility that locked user accounts will get unlocked after a reboot if the running-config (before reboot) is different from the 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 the clear-text password for the same user. This may result in login failure of the user subsequently.

Miscellaneous

- Dynamic VLAG to Nexus 5020 causes repeated link flaps after interface bounces. Disabling 'err-disable' mode on the Nexus switch will allow the link to go into an up state.

- On 1G Copper PHY, only auto-negotiation is supported. (No support for fixed 1G.)

- The embedded DCB switch module load balances internal and external traffic based on hash functions using standard network headers as keys. Due to this implementation, the customer may experience traffic imbalance depending upon the application flow definition.

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

- Priority 7 is reserved for control traffic on the embedded DCB switch module. User data traffic should use priorities 0 through 6.

- Dynamic mrouter ports are unsupported over trunk interfaces. As a workaround, a static mrouter port should be statically configured on the primary link interface of the trunk.

- SPAN and sFlow are supported only on physical ports and are not supported on ISL/LAG ports.

- The embedded DCB switch module architecture prioritizes Unicast traffic over Broadcast or Multicast traffic under port congestion.

- System verification/diagnostics performed on a switch will require a reboot.

- Configuration of more than one inband management port on a single switch is not recommended.

- By default, flow-control is disabled for all interfaces. To confirm the flow-control state for an interface, do not use the 'show interface' command, but instead use the 'show qos flowcontrol interface' command as follows:

-
```
sw0# show qos flowcontrol interface tengigabitethernet 0/1
Interface TenGigabitEthernet TenGigabitEthernet 0/1
Mode Off
```

Unsupported feature for the embedded DCB switch module

The following features against the original Brocade NOS version are unsupported in 3.0.0_dcb, because Hitachi does not complete to verify yet. Hitachi will support them after further verification.

- NETCONF

- LDAP

- VM Aware Network Automation

- Open Shortest Path First (OSPF)

- Offline diagnostics and db packet capture

- Federal Information Processing Standards (FIPS)

  The following problems had closed between Network OS v3.0.0_dcb and v3.0.0_dcb3.

- DCB Switches using NOS version 3.0.0_dcb may exhibit login failures if non-management ports are used. (DEFECT000464306)

- DCB Switchs may not link-up with server blades. (DEFECT000470049)

  For the details, please refer to the Release Notes of Network OS v3.0.0a and v3.0.0_dcb3 for Brocade VDX at http://my.brocade.com.

3

New/Enhanced Feature Description

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

NOS v.3.0.0_dcb includes support for new features such as FCoE feature, Layer 3 capabilities, Edge Loop Detection (ELD), BPDU Drop, Fabric Watch, Management PING/Traceroute, Management ACL, Virtual IP Management and others.

And, NOS v.3.0.0_dcb includes enhancement such as Layer 2 capabilities, AMPP, vLAG, Management feature and others.

- □ Layer 2 enhancement
- □ Layer 3 feature support
- □ FCoE support
- □ AMPP enhancement
- □ vLAG enhancement
- □ Management feature enhancement

Layer 2 enhancement

Edge Loop Detection (ELD)

NOS v3.0.0_dcb supports Edge Loop Detection (ELD) - a protocol that detects loop by shutting down ports when it receives its own PDU. ELD is primarily used to detect Layer-2 loops due to bad configuration, malformed physical connections and other user errors. ELD is supported only in VCS mode. ELD should NOT be treated as a substitute for Layer-2 loop prevention protocols such as STP, MSTP, and RSTP etc.

BPDU Drop

BPDU Drop is introduced in NOS v3.0.0_dcb to suppress unwanted BPDUs on edge ports. When configured on an edge port of a cluster, this feature will cause the all received BPDUs (STP, MSTP, RSTP and PVST BPDUs) to be dropped on the ports. BPDU Drop can be configured on Ports and VLAGs but not on profiled ports. Functionally, BPDU Drop prevents excessive broadcasts in the VCS fabric and thus improves utilization.

BTRUNK Support in VCS mode

In NOS v3.0.0_dcb, Brocade-Proprietary Aggregation or Brocade LAGs (commonly known as BTRUNK) are supported in VCS mode along with standalone mode. In previous NOS releases the support for Brocade LAG was provided only in standalone mode. Basic behaviors remain unchanged – the member ports must belong to the same port-group. Brocade LAGs can only work with another Brocade device supporting this feature. Brocade LAG cannot be a part of a VLAG.

Configurable Load Balancing

Sometimes traffic patterns fail to distribute evenly, leading to only one ECMP path for all traffic. This causes underutilization of ECMP paths resulting in a loss of data traffic even though one or more ECMP paths may be available to offload the traffic. Configurable load balancing on VDX switches allow traffic distribution based on user configured parameters. In NOS v3.0.0_dcb a new command is introduced to configure ECMP load balancing parameters.

Configurable Tail Drop Threshold

User configurable CoS tail drop thresholds are supported in NOS v3.0.0_dcb. This feature allows users to configure tail drop threshold on a physical interface. When the configurable threshold levels for a given traffic class (CoS) are exceeded, the packets for that traffic class get tail dropped. Allowing user configurable thresholds provides the flexibility to assign more buffers to some traffic classes over others. A traffic class with deep buffers will encounter fewer tail drops.

IGMP Dynamic m-router over VLAG

In NOS v3.0.0_dcb, m-router ports can be learned dynamically via queries received on VLAG member ports. This dynamic learning of m-router ports is enabled by default so a query received on a VLAG member port will automatically cause the port to be marked as an m-router port. No special configuration is required for dynamic m-router over VLAG.

1G connectivity with 1Gb LAN mezzanine

In NOS v3.0.0_dcb, new option for the 1G connectivity with 1Gb LAN mezzanine is supported. If embedded DCB switch connects to the 1G LAN mezzanine on a server blade, the option should be set to the interface of the embedded DCB switch. For the details, please refer to Appendix A.2.

Layer 3 feature support

IPv4 unicast routing /Static Routes in VCS

Brocade VCS Fabric technology brings intelligent, efficient routing to VCS fabrics. It enables highly elastic Layer 2 and Layer 3 domains with extremely efficient load balancing and multiple active Layer 3 gateways, partnered with L2 ECMP and Brocade ISL Trunking. The result is more effective link utilization that reduces overall cost, increases network resiliency resulting in greater application uptime, and a more flexible and agile network that helps organizations rapidly adapt to changing business conditions. The addition of Layer 3 routing to VCS technology is the next logical step in the evolution of VCS fabrics. The addition of routing capabilities has effectively flattened the traditional access and aggregation layers into a single layer. In other words, the traditional three tier architecture is now flattened into two layers.

Layer 3 in VCS is supported by both the fixed configuration and modular VDX platforms.

Layer 3 support in the Brocade VCS Fabric includes the following:

- Inter-VLAN routing in the VCS Fabric

- Router port to VE (Virtual Ethernet) routing capabilities in the VCS Fabric

- Router port to Router port routing within the VCS Fabric.

Layer 3 ACL's in VCS

In NOS v3.0.0_dcb, both Ingress Layer 2 MAC access control lists (ACLs) and Layer 3 IP access control lists are supported. NOS v3.0.0_dcb also supports standard and extended ACLs.

MAC ACLs are supported on the following interface types:

- Physical interfaces

- Logical interfaces (LAGs)

- VLANs

IP ACLs are supported on the following interface types:

- Logical interfaces (LAGs)

- Management interfaces

- VLANs

Layer 3 QoS

The following QoS features are supported in NOS v3.0.0_dcb.

- Layer2 and Layer3 QoS

- Traffic Policing

- Control Traffic Prioritization

- BUM Traffic Control

- Enhanced Transmission Selection (ETS) and Priority Flow Control (PFC)

The NOS v3.0.0_dcb QoS features that are supported by the embedded DCB switch module are.

- DSCP Trust

- DSCP to CoS Mutation

- DSCP to Traffic Class Mutation

VRRP and Brocade VRRP-E in VCS

In NOS v3.0.0_dcb, VRRP is available on the embedded DCB switch module and supports two versions of VRRP protocol for IPv4:

- Standard VRRP—the standard router redundancy protocol, VRRP v2 supports the IPv4 environment. Also, the Brocade version of standard VRRP is compliant with RFC 3768.

- VRRP-E (Extended)—A Brocade proprietary protocol similar to standard VRRP. It does not interoperate with VRRP.

    The VRRP and VRRP-E protocol supports:

- VRRP — TenGigabitEthernet, Gigabitethernet, and VE.

- For VRRP-E — VE ports only.

FCoE support

Hitachi supports FCoE in NOS 3.0.0_dcb officially.

FCoE Over LAG

In NOS v3.0.0_dcb, FCoE over LAG is only supported on links between two switches, and FCoE traffic can be configured and load balanced across the entire LAG.

FCoE is not supported on LAG interfaces between a VDX switch and host CNA.

Zoning and Zone Alias Names

Zoning support allows user to create LSAN Zones when connecting via FCR to communicate with Fibre Channel (FC) fabrics. WWN zoning is used for both regular VCS zoning (for zoning devices within VCS) and LSAN zoning (for zoning devices in VCS and FC-SAN). Zoning also provides RSCN storm suppression for native FCoE devices within Ethernet fabrics. New CLIs are added to support zone DB, zone transaction display, zone entry management (create, add, delete, remove, save, disable and enable), default zone access mode and ability to abort transactions. Zoning is not supported in standalone mode.

In NOS v3.0.0_dcb, Zone Alias Names also are supported. Zone Aliases make a zone database more organized, readable and interchangeable.

AMPP enhancement

AMPP over VLAG

In NOS v3.0.0_dcb, Automatic Migration of Port Profile (AMPP) is now supported on VLAGs. All other AMPP features that were supported only on a physical interface are now supported on a VLAG. This enhancement allows a profiled port to be a part of VLAG. In NOS v3.0.0_dcb, AMPP is also supported on a SPAN allowing a span port to be a profiled port. However, a SPAN destination port cannot be a profiled port. This feature in NOS v3.0.0_dcb will allow customers to monitor traffic on a profiled port.

vLAG enhancement

VLAG Minimum Links

The ability to specify minimum number of links that must be active on a VLAG before it can form aggregation is now supported in VCS mode. This was earlier supported only in standalone mode. The existing —minimum-links CLI under port-channel will now be available in VCS mode.

VLAGs with 32 ports

In NOS v3.0.0_dcb, VLAGs are enhanced to support up to 32 port members. The 32 member ports are supported on both dynamic and static VLAGs. There is no change in the maximum number of R-Bridges that a given VLAG can support – it is limited to 4 R-Bridges per VLAG. It should be noted that each individual R-Bridge can only support a maximum of 16 member ports.

Management feature enhancement

DNS Configuration

In NOS v3.0.0_dcb, the domain name service (DNS) parameters can be set using CLI. The DNS parameters are the domain name and the name server IP address for primary and secondary name servers. Only two name server IP addresses can be entered and only IPv4 is supported in the current release. This DNS configuration is primarily used for LDAP.

DOT1X Readiness Check

In NOS v3.0.0_dcb, 802.1X readiness check is added, which monitors 802.1x activities on all the switch ports and displays information about the devices connected to the ports. This feature can be used to determine if the devices connected to the switch ports are 802.1x-capable. When DOT1x readiness is enabled on the port it queries the connected client about its 802.1x capability when the link comes up.

Fabric Watch

Fabric health refers to the capability of the fabric to route data. A healthy fabric enables effective data transmission between networked devices. One of the more obvious criteria for fabric health is the condition of the network hardware. A switch or port failure can prevent data packets from reaching their destination. Network traffic can also influence fabric health. Fabric Watch functionality introduced in NOS v3.0.0_dcb allows monitoring of two aspects of Fabric– Fabric Health and Field Replacement Unit (FRU) monitoring. Fabric Watch monitors fabric health and sends an alert when a predefined threshold limit is reached. FRU monitoring feature in NOS v3.0.0_dcb monitors the insertion and removal of the field replaceable components (FRUs). Fabric Watch monitors each of the FRUs of the switch and sends an alert when a FRU gets removed, inserted or goes into faulty state.

IP ACL for Management Interface

IP Access List (both IPv4, IPv6) support in NOS v3.0.0_dcb helps the user control ingress traffic. Management traffic such as Telnet, SSH, HTTP, HTTPS, SNMP etc can be filtered to deny access to unauthorized hosts or allow access to only authorized hosts. Brocade NOS v3.0.0_dcb supports both the standard and extended ACLs. Standard rules allow filtering based on IP Address and Subnets, while extended rules allow filtering based on source and destination IP Addresses, IP Protocol and TCP Ports.

IPv4 and IPv6 Management Services in VCS

NOS v3.0.0_dcb supports various IPv4 and IPv6 Management Services, including Inband Management using IPv4 addressing, Secure Syslog and IP Static Routes in VCS.

The services are:

- Inband Management is available on the embedded DCB switch module. Inband Management can be used for switch management and SNMP functions such as sourcing SNMP traps.

- IPv6 addressing is available on the embedded DCB switch module for the management interfaces. The embedded DCB switch module can be managed through IPv6 management network and IPv6 services such as ping, traceroute, and DNS DHCPv6 are supported.

- DNS Server configuration allows either ipv4 or ipv6 dns server addresses to be configured on the switch.

- Static Routing is available on the embedded DCB switch module in the VCS fabric. Static routes can be used to avoid overhead of running dynamic protocols in simple networks, overwrite the routes calculated by routing protocols, inject networks that don't have routing protocol enabled and keep default back up paths when routing protocol instabilities affect the network.

Management PING and Traceroute

NOS v3.0.0_dcb supports PING and Traceroute on management interfaces. Only IPv4 PING and Traceroute are supported. The management interface itself can be either IPv4 or IPv6.

New MIBs for SNMP

NOS v3.0.0_dcb continues to support SNMPv3 originally introduced in NOS v2.0.1. System and Resource MIBs are now also supported in NOS v3.0.0_dcb. System MIB provides general switch related information and resource MIB provides CPU and memory utilization of the switch. A new SNMP option is added in NOS v3.0.0_dcb to allow setting up severity in the host command. This command allows throttling the number of traps received by the host based on severity level.

sFLOW Auto Adjust and Backoff

Enhancements to SFLOW behavior in NOS v3.0.0_dcb protect against poorly chosen Sampling Rates or unexpected changes in peak traffic rates, but still allow low Sampling Rates to be safely selected where appropriate. Setting a low value for sampling rate to avoid overload under high traffic conditions is not advisable since such a conservative setting doesn't reflect true network condition. To avoid this, NOS v3.0.0_dcb supports auto adjust of sampling rate, which ramps up the sampling rate whenever a threshold is exceeded, eventually reaching a sustainable value. Similarly, to avoid switch overload with packet flow samples under worst case traffic load, an automated one way back-off mechanism is also added in NOS v3.0.0_dcb. This auto back-off is triggered whenever an excessive number of samples per second are generated.

Virtual IP Address

Virtual IP address cannot be configured on a standalone node in VCS mode. 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 Virtual IP address to work correctly, the management port's IPv4 address should be assigned and functional.

Firmware Upgrade and Downgrades

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

- ☐ [Summary](#)
- ☐ [Procedure summary](#)
- ☐ [Target product](#)
- ☐ [Notice for update work](#)
- ☐ [Preparation](#)
- ☐ [Backup configuration](#)
- ☐ [Apply updated firmware](#)
- ☐ [Restore configuration](#)

Summary

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

Please refer to the NOS 3.0.0 Administrator Guide for details regarding firmware upgrade and downgrade.

The followings show the consideration for upgrading to NOS 3.0.0_dcb on the incompatibility point of view between NOS 2.0.1_katx and NOS 3.0.0_dcb.

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 3.0.0_dcb 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.

Procedure summary

The following shows work flow of the update procedure.

```
                    ( START )
                        |
            +-----------------------+
            | Preparation of FTP server |
            +-----------------------+
                        |
            +-----------------------+
            | Preparation of console PC |
            +-----------------------+
                        |
            +-----------------------+
            |   Backup and initialize   |
            |      configuration        |
            +-----------------------+
                        |
            +-----------------------+
            |     Update firmware       |
            +-----------------------+
                        |
            +-----------------------+
            |   Restore and modify      |
            |      configuration        |
            +-----------------------+
                        |
                    ( END )
```
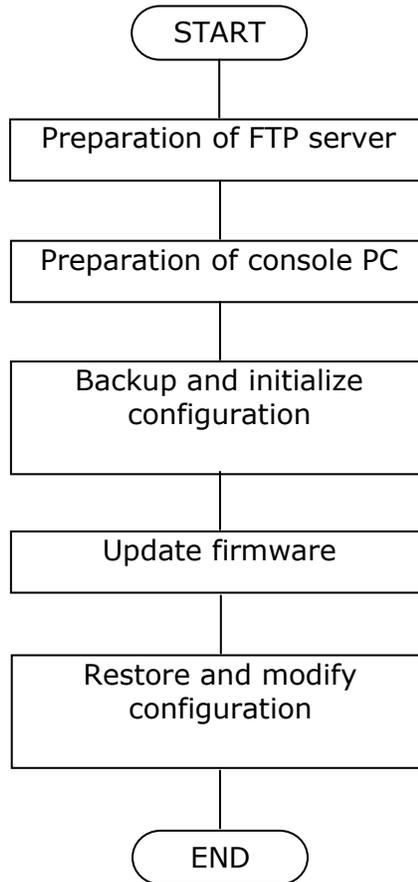
Target product

Target product of this guide is

Product name	Produce code	Available NOS version
Brocade 10Gbps DCB switch module	GG-BE3LSW3X1-Y GV-BE2LSW3X1-Y	3.0.0_dcb3

Notice for update work

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

- Brocade Network OS Network OS Update Guide for 3.0.0_dcb3

- 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): 192.168.0.1

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. There are incompatibilities between NOS 2.0.1_katx and NOS 3.0.0_dcb3 on the configuration of the following features. If customer uses the following feature, please change your configuration according to the following table.

No.	feature	Modification at NOS 3.0	Influence	Measure
1	Management IP address	As the 'interface VE' is supported newly, assign method of inband management IP address is changed to 'interface VE' from 'interface Vlan'.	After update to NOS 3.0, assigned IP address to 'interface Vlan' will be removed.	Please create 'interface VE' newly, and re-assign IP address to created 'interface VE'.
2	MAC ACL (standard)	The option of MAC ACL (standard), which masks MAC address for 'deny', 'permit' and 'seq' command, is added.	After update to NOS 3.0, defined MAC ACL will be removed.	Please re-define 'deny', 'permit' and 'seq' command with added mask option which is fixed value (ffff.ffff.ffff).
3	MAC ACL (extended)	The option of MAC ACL (extended), which masks MAC address for 'deny', 'permit' and 'seq', is added.	After update to NOS 3.0, defined MAC ACL will be removed.	Please re-define 'deny', 'permit' and 'seq' command with added mask option which is fixed value (ffff.ffff.ffff).

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]

Management module

Back view of CB500 system

Console PC
FTP server
Terminal client
application

LAN cable

[connecting at CB2000]

Back view of CB2000 system

Management module

Console PC
FTP server
Terminal client
application

LAN cable
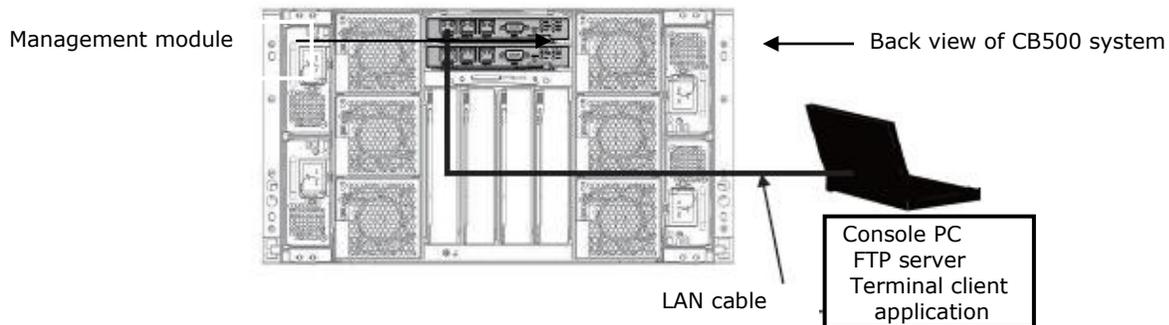
Starting FTP server and confirmation

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 3.0.0_dcb3, the archived file named 'nos3.0.0_dcb3.tar.gz' is needed. Please consult with OEM partner and get the archived file.

The archived file:'nos3.0.0_dcb3.tar.gz'should be stored in the ftp root folder of FTP server, and please unarchive it to the folder named 'nos3.0.0_dcb3'. This 'nos3.0.0_dcb3' will be used in section "0Execute NOS update".
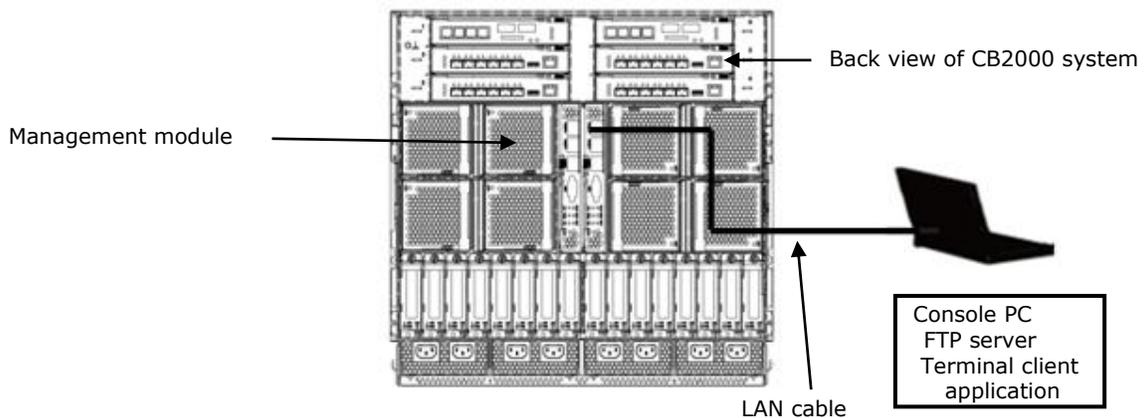
Backup configuration

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, 2013, 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, 2013, HITACHI, LTD.
Chassis ID        : XXXXXXXXXX
Firmware Revision : XXXXXXXXXX


<< 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

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

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: nos3.0.0_dcb3 [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

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 "3.0.0_dcb3" using 'show version' command.

```
sw0# show version [Enter]


Network Operating System Software
Network Operating System Version: 3.0.0
Copyright (c) 1995-2012 Brocade Communications Systems, Inc.
Firmware name:      3.0.0_dcb3
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      3.0.0_dcb3
         3.0.0_dcb3
```

Restore configuration

Recover to VCS mode

If the operational mode before this work is VCS mode, 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

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 !!".

Modification of startup-configuration caused by NOS version up

If the original configuration included the setting in vii of "Notice for update
work", the modification to the startup-configuration is needed. Please modify
the configuration according to the vii of "Notice for update work". If the
configuration is modified, please save the configuration to 'startup-config'
using 'copy' command.

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

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.

A. Modifications for Hitachi

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

□ Port Association Feature (track command)

□ 802.3 Clause 37 1Gbls AN support

□ Show Enclosure Command

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

MK-99COM110-00