Network OS v4.1.1 for Brocade VDX
Release Notes

Document History

<table>
<thead>
<tr>
<th>Version of Document</th>
<th>Summary of Changes</th>
<th>Publication Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial Release</td>
<td>March 19, 2014</td>
</tr>
</tbody>
</table>
Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government. Notice: The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit http://www.brocade.com/support/oscd
Contents

Overview ............................................................................................................................................. 7
  Summary of Features and Enhancements .......................................................................................... 8

Deprecation of old Features .................................................................................................................. 8

Descriptions of New Features .............................................................................................................. 8
  Virtual Fabric ...................................................................................................................................... 8
  Policy-based Routing .......................................................................................................................... 9
  Inter-VRF Leaking .............................................................................................................................. 9
  DHCP IP Helper .................................................................................................................................. 9
  DHCP Automatic Deployment (DAD) .................................................................................................... 9
  Logical Chassis HA ............................................................................................................................. 9
  Access Gateway (VDX 6730) .............................................................................................................. 10
  Auto QoS for NAS .............................................................................................................................. 10
  Brocade Trunking on 40Gbe ............................................................................................................... 10
  ISL on Breakout .................................................................................................................................. 10
  VRRP-E Across VCS fabric ................................................................................................................. 10
  VCS VXLAN Gateway for VMWare NSX ............................................................................................ 10

Supported hardware ............................................................................................................................. 11
  Supported devices .............................................................................................................................. 11
  Supported blades for VDX 8770: ....................................................................................................... 14
  Supported power supplies .................................................................................................................. 14
  Supported Optics ............................................................................................................................... 15

Standards Compliance .......................................................................................................................... 17

Software or Image filenames ................................................................................................................. 18

Licensing information ........................................................................................................................... 18
  Temporary License Support ............................................................................................................... 19
  Brocade Network OS Compatibility .................................................................................................. 19
  Fabric OS Compatibility .................................................................................................................... 19

Limitations and Restrictions ................................................................................................................. 20
  Command Line Interface ................................................................................................................... 20

Network OS v4.1.1 Release Notes v1.0
VRF ............................................................................................................................... 34
Interoperability ............................................................................................................. 34
Miscellaneous ............................................................................................................... 35
Virtual Fabric ................................................................................................................ 35
Policy-based Routing (PBR) .......................................................................................... 36
Inter-VRF Leaking (Static) ............................................................................................ 36
DHCP IP Helper ............................................................................................................. 36
DHCP-based Firmware download (DAD – DHCP Automatic Deployment) ...................... 36
Logical Chassis HA ........................................................................................................ 37
Access Gateway (6730) ................................................................................................. 37
Auto QOS for NAS ......................................................................................................... 37
Brocade ISL trunking on 40Gb ports .............................................................................. 37
VCS VXLAN Gateway for VMWare NSX ........................................................................ 38
Upgrade and migration considerations ........................................................................ 38
Recommended Migration Paths for Brocade Network OS v4.1.x ..................................... 39
Considerations and Limitations: .................................................................................... 39
Upgrading from Brocade Network OS v3.x ..................................................................... 39
Upgrading from Brocade Network OS 2.x ....................................................................... 40
Switch additions to cluster scenarios: ............................................................................. 40
Adding a switch running Brocade Network OS v4.0.x to Brocade Network OS v4.1.x cluster 40
Adding a switch running Brocade Network OS v4.1.x to Brocade Network OS v4.0.x cluster 40
Adding a switch running Brocade Network OS 2.X to Brocade Network OS v4.1.x cluster 40
Adding a switch running Brocade Network OS v3.0.x to Brocade Network OS 4.1.x cluster 40
Upgrading to this release ............................................................................................... 41
Downgrading to a previous release ................................................................................ 42
Upgrade / Downgrade Considerations for FCoE .......................................................... 42
Upgrade / Downgrade Considerations for vLAG .......................................................... 43
Scalability ..................................................................................................................... 46
Scalability ..................................................................................................................... 46
SNMP support documentation changes ....................................................................... 55
Obtaining the MIBs ....................................................................................................... 55

Network OS v4.1.1 Release Notes v1.0 5
Changes in MIBs and objects ................................................................. 55

User guides ............................................................................................. 56
  List of Documents ................................................................................. 56
  Reporting errors in the guides ............................................................. 57

Contacting Brocade .............................................................................. 57
  Support .................................................................................................. 57

Defects .................................................................................................... 58
  TSBs - Critical Issues to Consider Prior to Installing This NOS Release ............................................. 58

Software Fixes .......................................................................................... 60
  Closed with Code Change in Network OS v4.1.1 .................................. 60

Known issues ............................................................................................. 67
  Newly Open defects in Network OS v4.1.1 ........................................... 67
Overview

Brocade Network Operating System (NOS) v4.1.1 is an update to NOS 4.1.0 (and NOS 4.1.0a). The details for NOS 4.1.0 are retained here as customers can upgrade to this release from a NOS 4.0.x base. All the features described for NOS 4.1.0 are applicable to NOS 4.1.1 with appropriate differences called out.

NOS 4.1.x is a new release to support new platforms, new features, and improved scalability on all VDX platforms. Accompanying NOS 4.1.0 is NOS 4.1.0a for the VDX6740T-1G. These releases are identical other than a change made to NOS 4.1.0a to fix a manufacturing related problem with flash partitioning. The change made to NOS 4.1.0a does not affect functionality in any way and is only applicable to the VDX6740T-1G. Throughout, this document references v4.1.0 however all references are also applicable to NOS v4.1.0a.

Network OS v4.1.0 introduces new features such as Virtual Fabric that enables customers to design multi-tenant data centers. This feature uses TRILL Fine-grained-label based extensions to deliver a user-friendly fabric-native functionality that overcomes restrictions on VLAN scale. Virtual Fabric also delivers functionality unique to multi-tenant data center designs – Overlapping VLANs, VLAN translation and Transparent VLAN services. NOS 4.1.1 enhances the Virtual Fabric feature by adding support for classifying untagged traffic into Native VLAN.

NOS 4.1.0 builds upon L3 functionality in NOS 4.0 by delivering features such as Policy-based Routing, Inter-VRF Route leaking and DHCP IP Helper.

Additionally, NOS 4.1.0 continues to enhance the VCS Fabric-based automation by incorporating features (such as DAD) that enable customers to reduce operational costs incurred for upgrading and maintaining the NOS firmware installed on the VDX switches.

NOS 4.1.0 enhances our HA functionality to work within the context of a Logical chassis.

Finally, NOS 4.1.0 delivers Access gateway functionality to enable NPIV devices to connect to a FC fabric in an efficient manner.

NOS 4.1.1 delivers the Brocade VCS VXLAN Gateway for VMWare NSX (on the VDX 6740 and 6740-T). This enables a network virtualization solution for customers who have a combination of physical and virtual data center infrastructure and need a high-performing and resilient gateway to bridge between the physical and virtual assets.

Brocade Network v4.1.0 also introduces further new features and enhancements. The following is a complete list of all new features and enhancements that will be part of the NOS 4.1.0 release.

This release also delivers a new 1G (upgradable to 10G via a license) platform the Brocade VDX 6740T-1G.
Summary of Features and Enhancements

Network OS v4.1.1 includes the following features for Brocade VDX products:

- Virtual Fabric
- Policy-based Routing (PBR)
- Inter-VRF Leaking (Static)
- DHCP IP Helper
- DHCP-based Firmware download (DAD – DHCP Automatic Deployment)
- Logical Chassis HA
- Access Gateway (6730)
- VRRP-E across VCS fabrics
- Auto QOS for NAS
- Brocade trunking on 40Gbe
- ISL on Breakout
- VCS VXLAN Gateway for VMWare NSX.

Deprecation of old Features

- None

Descriptions of New Features

Virtual Fabric

The Virtual Fabric feature of Brocade VCS Fabric technology is designed to address the scalability restrictions of traditional VLANs used for multi-tenant segmentation. It provides native secure multi-tenant support for both physical and virtual application deployments. Managed centrally through Brocade VCS Logical Chassis, the Virtual Fabric feature simplifies and accelerates application deployment, and ensures policy consistency for each tenant regardless of how application components are distributed across the data center.

The VCS Virtual Fabric feature is designed to address the scalability restrictions of traditional VLANs that are used for multitenant segmentation. Using the 24-bit TRILL FGL header, a VCS Virtual Fabric provides expanded VLAN space. This allows for overlapping VLANs and MAC addresses, while maintaining tenant isolation. The VCS Virtual Fabric capability requires no modifications to existing VLAN configurations, which simplifies implementation as well as communication with vSwitches. The VCS Virtual Fabric ID is assigned at the edge port and is carried transparently on transit nodes to the destination node, where it is matched with the corresponding tenant VLAN. You can implement Layer 3 VE interfaces for inter-Virtual Fabric routing. In summary, the VCS Virtual Fabric feature functions much like a traditional VLAN, but without its limitations. NOS 4.1.1 adds support for processing and classifying untagged frames into Native VLANs for both Transport as well as Service Virtual Fabric.
**Policy-based Routing**

Policy-based Routing (or PBR) is a technique to make routing decisions based on policies configured by a network administrator. PBR configuration is done by using a combination of IP ACLs and route maps. The VDX platform programs the ACLs on the interfaces and routes traffic that matches the ACLs according to instructions in the route map entry.

PBR can be configured based on Layer 3 and Layer 4 information and the VDX platform can be instructed to forward packets to a pre-determined next-hop gateway or drop the packet.

PBR is supported on VDX 8770 and VDX 6740x.

**Inter-VRF Leaking**

Virtual Routing and Forwarding (VRF) is a technology that provides you with the ability to have multiple virtual routers on a single physical router or switch. VRFs operate without knowledge of one another unless they are imported or exported into one another using Inter-VRF Route Leaking. Inter-VRF route leaking allows leaking of specific route prefixes from one VRF instance to another VRF instance on the same physical router, which eliminates the need for external routing. This is useful in cases where multiple VRFs share the same path to reach an external domain, while maintaining their internal routing information limited to their own VRF. This feature enables a data center to consolidate multiple VRF services onto a single server.

**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 a VDX device 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.

**Logical Chassis HA**

NOS 4.1.0 builds upon the HA functionality in NOS 4.0 and delivers HA support in Logical Chassis mode. This includes system-wide HA sync and warm recovery both for ISSU as well as non-ISSU scenarios.
**Access Gateway (VDX 6730)**

The Access Gateway functionality simplifies server and storage connectivity by enabling the connection of servers to any SAN fabric. It also enhances scalability by eliminating the switch domain identity from the VCS fabric and simplifies local switch device management. This feature provides significant improvements in the connectivity options to a Fibre Channel SAN over the previous method, by sending device logins directly to the FC SAN. Hence, the scalability and management of these devices are now properties of the FC SAN, with the VCS fabric simply providing access. This feature is supported only on the VDX 6730.

**Auto QoS for NAS**

NOS 4.1.0 extends storage functionality by introducing Auto QoS for NAS. This allows customers to prioritize delay-sensitive IP Storage traffic within the VCS Fabric and help ensure consistent performance. Auto QoS automatically classifies and prioritizes traffic based on source or destination IPv4 address. It does so by assigning the identified traffic to separate priority queues. This allows a minimum bandwidth guarantee to be provided to the queue.

This functionality is available on the 6740x and the 8770 platforms. Other platforms do not support this functionality but can act as a transit switch for the prioritized traffic.

**Brocade Trunking on 40Gbe**

40GbE Brocade Trunking will be available on the VDX 8770 12 x 40GbE blade starting with the NOS 4.1 release. In order to achieve 2 x 40GbE brocade trunking on the 12 x 40GbE blade the user has to configure 40GbE ports in breakout mode and must use breakout optics (40GbE-SR4-INT) with a single QSFP optical cable.

**ISL on Breakout**

ISL on breakout capability is enabled on all 40GbE capable device including the VDX6740, VDX 6740T, VDX6740T-1G and VDX 8770 in this release. Now the user can use ISL on breakout to form a fabric with 10GbE capable VDX products using 40GbE ports on VDX6740, VDX 6740T, VDX6740T-1G and VDX 8770. This capability is useful when a user wants to form a single fabric between VDX6740/VDX 6740T/VDX6740T-1G /VDX 8770 and VDX 6710/20/30 (Note: VDX 6710/20/30 does not have native 40GbE ports).

**VRRP-E Across VCS fabric**

NOS4.1.0 and later versions support VRRP-E across the VCS to VCS.

**VCS VXLAN Gateway for VMWare NSX**

NOS 4.1.1 delivers the VCS VXLAN Gateway for VMWare NSX functionality that enables a network virtualization solution. This feature enables customers to combine the virtual and physical architecture within their data centers to allow for a seamless migration to a cloud-based architecture. NOS 4.1.1 accomplishes this by implementing a VTEP (VXLAN Tunnel Endpoint) on the VDX 6740x. This enables VMWare NSX to provision and configure the VTEPs on the
VDX H/W similar to a S/W VTEP (in the hypervisor). The VXLAN gateway is based on a VDX 6740-based VCS fabric and is able to take advantage of:

1. Performance – As the VXLAN to VLAN (and vice-versa) translation is done on custom ASIC, the VCS VXLAN gateway is able to deliver line-rate performance for the VXLAN/VLAN traffic.
2. Resilience - The resiliency within VCS fabric allows for instantaneous failover between the VDX switches
3. Logical chassis functionality, where the VXLAN gateway is presented to VMWare NSX as a single logical gateway reducing the number of VTEPs that need to be configured.

**Supported hardware**

*Supported devices*

Brocade Network OS v4.1.0 and NOS 4.1.1 support the following VDX Switches:

- Brocade VDX 6710-54
- Brocade VDX 6720-24
- Brocade VDX 6720-60
- Brocade VDX 6730-32
- Brocade VDX 6730-76
- Brocade VDX 6740
- Brocade VDX 6740T
- Brocade VDX6740T-1G (newly supported platform)
- Brocade VDX 8770-4
- Brocade VDX 8770-8

Brocade VDX 6720-24 and VDX 6720-60 supports the following:

- VDX 6720-24 offers a base configuration with 16 ports and can be upgraded via Brocade’s Ports on Demand license to a full 24 10GbE ports.
- VDX 6720-60 offers a base configuration with 40 ports and can be upgraded via Brocade’s Ports on Demand license to either 50 ports or a full 60 10GbE ports.
- Extremely low latency for classic Ethernet networks or for scale-out of layer2 fabrics for virtual data centers.
- Enables end-to-end convergence of Fibre Channel over Ethernet (FCoE) and iSCSI storage traffic along with IP LAN data traffic.
- Can be deployed as a traditional stand-alone ToR (Top of Rack) switch or in an Ethernet fabric with VCS technology.

Brocade VDX 6710-54 supports the following:

- VDX 6710-54 provides 48x1GbE ports and 6x10GbE ports.
• 1 GbE ports are intended for extending VCS technology to the access layer which provides the benefits of both Top of the Rack (ToR) and End of the Row (EoR) architectures.
• 6 x 10GE SFP+ ports can be used as uplink to VDX 6720/VDX 6730 switches to form a VCS fabric or to connect to 10G servers at the access layer.
• VDX 6710-54 offers extremely low latency for classic Ethernet networks or for scale-out of layer-2 fabrics for virtual data centers.

Brocade VDX 6730-32 and VDX 6730-76 supports the following:
• VDX 6730-32 offers a base configuration with 16 ports and can be upgraded via Brocade’s Ports on Demand license to a full 24 10GbE ports.
• VDX 6730-76 offers a base configuration with 40 ports and can be upgraded via Brocade’s Ports on Demand license to either 50 ports or a full 60 10GbE ports.
• VDX 6730-32 supports 24 10GbE ports and 8 8G Fibre Channel Ports. VDX 6730-76 supports 60 10GbE ports and 16 8G Fibre Channel Ports. VDX 6730 facilitates VCS fabric to Fibre Channel SAN Connectivity.
• Enables end-to-end convergence of Fibre Channel (FC), Fibre Channel over Ethernet (FCoE) and iSCSI storage traffic along with IP LAN data traffic.

Brocade VDX 6740
The Brocade VDX 6740 offers 48 10GbE SFP+ ports and 4 ports of 40 Gigabit quad small form-factor pluggable plus (QSFP+), each can be broken out into four independent 10 GbE SFP+ ports, providing an additional 16 10 GbE SFP+ ports.
• It is available in as 24, 48 and 64 port SKU
• 850ns microsecond latency for any port to port to assure rapid response for latency-sensitive applications.
• The base SKU is available with 24 ports and can be upgraded up to 48 ports via 10Gbe DPOD license of 8 ports
• It has 4 X 40Gbe QSFP ports which can be used for the uplink and VCS fabric formation with VDX8770 /VDX6740/VDX6740T
• Each 40GbE port is capable of doing a breakout of 4 X 10GbE ports

Brocade VDX 6740T
The VDX 6740T offers 48 10GbE Base-T ports and 4 ports of 40 Gigabit quad small form-factor pluggable plus (QSFP+), each can be broken out into four independent 10GbE SFP+ ports, providing an additional 16 10 GbE SFP+ ports.
• It is available in as 24, 48 and 64 port SKU
• 3 microsecond latency for any port to port to assure rapid response for latency-sensitive applications.
• The base SKU is available with 24 ports and can be upgraded up to 48 ports via 10Gbe DPOD license of 8 ports
- It has 4 X 40Gbe QSFP ports which can be used for the uplink and VCS fabric formation with VDX8770/VDX6740/VDX6740T
- Each 40Gbe port is capable of doing a breakout of 4 X 10Gbe ports. This also helps to form fabric with VDX 6710/20/30

Brocade VDX 6740T-1G

The Brocade VDX 6740T-1G offers 48 1000BASE-T ports and two 40 GbE QSFP+ ports in base version. Each 40 GbE port can be broken out into four independent 10 GbE SFP+ ports, providing an additional eight 10 GbE SFP+ ports for uplink. All 48 1000BASE-T ports can be upgraded to 48 10GBase-T ports via a Capacity on Demand (CoD) software license. Two 40 GbE ports are enabled as part of the base license. The additional two 40 GbE ports can be upgraded via the Ports on Demand (PoD) software license.

- Base version is available with 48 1000BASE-T ports and two 40 GbE QSFP+ ports
- 3 microsecond latency for any port to port to assure rapid response for latency-sensitive applications.
- All 48 48 1000BASE-T ports can be upgraded to 10Gbase-T port with capacity on demand license.
- Additional 2X40Gbe port can be added to base version with 2X40Gbe POD license.
- It has 4 X 40Gbe QSFP ports which can be used for the uplink and VCS fabric formation with VDX8770/VDX6740/VDX6740T
- Each 40GbE port is capable of doing a breakout of 4 X 10GbE ports. This also helps to form fabric with VDX 6710/20/30
- 100 Mbit support for point to point Management server connection on VDX6740T-1G
  - Full duplex speed support on Base-T ports for management server P2P connection.
  - Limited L2 configuration supported. For e.g. Switchport, LLDP, **MTU size, L2 ACL** and **L3 ACL**
  - L3 configuration, FCoE, Trill, VLAG configuration, Nhalf duplex speed support, PFC configuration are NOT supported on 100Mbits
  - No support for adding a 100Mbit shared media/ hub.

Example for 100Mbit usage are as follows.
- 100MB Host Device Requirement with Ipv4 Connectivity, PING, ICMP Traffic over V4, V4 Neighbor Discovery
- Server with HTTP/HTTPS/FTP/SSH/TELNET Server, Filesharing and RDP Services and application testing over the V4 connectivity

Brocade VDX 8770-4 and VDX 8770-8

The Brocade VDX 8770 is available in two form factors; a 4-I/O slot system and an 8 I/O slot system with linecard support for 1-Gbe, 10-Gbe and 40GbE ports. The Brocade VDX 8770 delivers a high-performance switch to support the most demanding data center networking needs, capable of supporting:
- 1, 10, and 40 GbE to satisfy current needs, with 100 GbE readiness to support future bandwidth requirements and technology.
- 4 Tbps per slot line-rate design for substantial capacity and headroom.
- ~4-microsecond latency to assure rapid response for latency-sensitive applications.
- Up to 384,000 MAC addresses per fabric for extensive virtualization scalability.
- More than 8000 ports in a single VCS fabric with Brocade Fabric Multipathing technology, enabling the switch to serve extremely large-scale deployments with the best-possible network utilization.

**Supported blades for VDX 8770:**
The flexible, modular switch design offers interconnection with other Brocade VDX 8770 switches, Brocade VDX 6710, 6720, and 6730 fabric switches, traditional Ethernet switch infrastructures, and direct server connections. Modular 4-slot and 8-slot chassis options are available to match the switch to the needs of the organization. These include:

- **Brocade VDX 8770-4**: Supports up to 192 1/10 GbE ports, or 48 40 GbE ports, or a combination.
- **Brocade VDX 8770-8**: Supports up to 384 1/10 GbE ports, or 96 40 GbE ports, or a combination.

The switches support two Management Modules in an active standby configuration. The 4 slot chassis can hold up to 3 Switch Fabric Modules (SFM) and 4 Power supply Units (PSU) while the 8 slot chassis can hold 6 SFMs and 8 PSUs. The switch supports a variety of wire-speed line cards to offer maximum flexibility in terms of port bandwidth as well as cable and connector technology:

- 1 GbE: LC48×1G line card provides up to 48 SFP/SFP-copper ports.
- 10 GbE: LC48×10G line card provides up to 48 SFP+ ports.
- 40 GbE: LC12×40G line card provides up to 12 40 GbE QSFP ports.
- Each 40GbE port is capable of doing a breakout of 4 X 10GbE ports

**Supported power supplies**
The VDX-6710-54 switch ships with two internal, redundant, field-replaceable, load-sharing AC power supplies.

The VDX-6720-24 and VDX-6720-60 switches both ship with two internal, redundant, field-replaceable, load-sharing AC power supplies. The VDX-6730-32 and VDX-6730-76 switches both ship with two internal, redundant, field-replaceable, load-sharing AC power supplies.

The VDX 8770 switches ship with multiple, field replaceable, load-sharing AC or DC power supplies based on the configuration selected. The PSUs are shared by both 4- and 8-slot systems. The VDX8770-4 ships with a minimum of 2 AC or DC PSU. Additional 2 PSU can be
ordered for redundancy. The VDX8770-8 system ships with a minimum of 3 PSU and additional PSU may be ordered for redundancy:

- XBR-ACPWR-3000 - 3000 W power supply unit AC
- XBR-DCPWR-3000 - 3000 W power supply unit DC

The VDX-6740 switches both ship with two internal, redundant, field-replaceable, load-sharing AC power supplies.

- XBR-250WPSAC-F - FRU 250 W AC power supply/fan, non-port-side exhaust airflow
- XBR-250WPSAC-R - FRU 250 W AC power supply/fan, port-side exhaust airflow

The VDX-6740T switches ship with two internal, redundant, field-replaceable, load-sharing AC power supplies.

- XBR-500WPSAC-01-F -FRU 500 W AC power supply/fan, non-port-side exhaust airflow
- XBR-500WPSAC-01-R - FRU 500 W AC power supply/fan, port-side exhaust airflow

**Supported Optics**

The VDX switches support following optics types listed below. The 8G FC optics are only supported on the VDX-6730 switches. Breakout optics are supported only for 8770 (40G Linecard) and 6740/T

<table>
<thead>
<tr>
<th>FRU and Optics SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1GbE</td>
<td></td>
</tr>
<tr>
<td>XBR-000190 (1-pack)</td>
<td>1 GbE copper</td>
</tr>
<tr>
<td>E1MG-SX-OM (1-pack)*</td>
<td>1000Base-SX</td>
</tr>
<tr>
<td>E1MG-SX-OM-8 (8-pack)*</td>
<td>1000Base-LX</td>
</tr>
<tr>
<td>E1MG-LX-OM (1-pack)*</td>
<td></td>
</tr>
<tr>
<td>E1MG-LX-OM-8 (8-pack)*</td>
<td></td>
</tr>
<tr>
<td>10G-SFPP-SR (1-pack)</td>
<td>10 Gbps SR</td>
</tr>
<tr>
<td>10G-SFPP-SR-8 (8-pack)</td>
<td>10 Gbps LR</td>
</tr>
<tr>
<td>10G-SFPP-LR (1-pack)</td>
<td>10 Gbps ER</td>
</tr>
<tr>
<td>10G-SFPP-LR-8 (8-pack)</td>
<td></td>
</tr>
<tr>
<td>10G-SFPP-ER (1-pack)</td>
<td></td>
</tr>
<tr>
<td>10G-SFPP-ER-8 (8-pack)</td>
<td></td>
</tr>
<tr>
<td>10G-SFPP-TWX-0101 (1-pack)</td>
<td>1 m Twinax copper cable</td>
</tr>
<tr>
<td>10G-SFPP-TWX-0108 (8-pack)</td>
<td>3 m Twinax copper cable</td>
</tr>
<tr>
<td>10G-SFPP-TWX-0301 (1-pack)</td>
<td></td>
</tr>
<tr>
<td>10G-SFPP-TWX-0308 (8-pack)</td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>10G-SFPP-TWX-0501 (1-pack)</td>
<td>5 m Twinax copper cable</td>
</tr>
<tr>
<td>10G-SFPP-TWX-0508 (8-pack)</td>
<td></td>
</tr>
<tr>
<td>10Ge-SFPP-AOC-0701</td>
<td>10Gbe SFP+ Direct Attached Active Optical Cable, 7m, 1-pack</td>
</tr>
<tr>
<td>10Ge-SFPP-AOC-1001</td>
<td>10Gbe SFP+ Direct Attached Active Optical Cable, 10m, 1-pack</td>
</tr>
<tr>
<td>40G-QSFP-QSFP-C-0101</td>
<td>40GbE Direct Attached QSFP+ to QSFP+ Active Copper cable, 1m, 1-pack</td>
</tr>
<tr>
<td>40G-QSFP-QSFP-C-0301</td>
<td>40GbE Direct Attached QSFP+ to QSFP+ Active Copper cable, 3m, 1-pack</td>
</tr>
<tr>
<td>40G-QSFP-QSFP-C-0501</td>
<td>40GbE Direct Attached QSFP+ to QSFP+ Active Copper cable, 5m, 1-pack</td>
</tr>
<tr>
<td>40G-QSFP-4SFP-C-0101</td>
<td>4x10Gbe Direct Attached QSFP+ to 4 SFP+ Copper Breakout Cable, 1m, 1-pack</td>
</tr>
<tr>
<td>40G-QSFP-4SFP-C-0301</td>
<td>4x10Gbe Direct Attached QSFP+ to 4 SFP+ Copper Breakout Cable, 3m, 1-pack</td>
</tr>
<tr>
<td>40G-QSFP-4SFP-C-0501</td>
<td>4x10Gbe Direct Attached QSFP+ to 4 SFP+ Copper Breakout Cable, 5m, 1-pack</td>
</tr>
<tr>
<td>40G-QSFP-SR4</td>
<td>40 GbE SR4 optic</td>
</tr>
<tr>
<td>40G-QSFP-SR4-INT</td>
<td>40 GbESR4 (4×10 Gbe SFP+ break-out capable) . Breakout Optical cable is not included with this optics</td>
</tr>
<tr>
<td>XBR-000163 (1-pack)</td>
<td>8G FC SWL</td>
</tr>
<tr>
<td>XBR-000164 (8-pack)</td>
<td></td>
</tr>
<tr>
<td>XBR-000153 (1-pack)</td>
<td>8G FC LWL – 10km</td>
</tr>
<tr>
<td>XBR-000172 (8-pack)</td>
<td></td>
</tr>
<tr>
<td>XBR-000174 (1-pack)</td>
<td>8G FC ELWL – 25km</td>
</tr>
</tbody>
</table>
*Note: Legacy Foundry Networks branded optics are not supported

**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 VDX products conform 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 VDX products:

- 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 VDX products conform 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
Software or Image filenames

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network OS v4.1.1.tar.gz</td>
<td>Network OS v4.1.1 for Unix</td>
</tr>
<tr>
<td>Network OS v4.1.1.zip</td>
<td>Network OS v4.1.1 for Windows</td>
</tr>
<tr>
<td>Network OS v4.1.1_all_mibs.tar.gz</td>
<td>Network OS v4.1.1 MIBs</td>
</tr>
<tr>
<td>Network OS v4.1.1.md5</td>
<td>Network OS v4.1.1 md5 Checksum</td>
</tr>
</tbody>
</table>

Licensing information

Brocade Network OS v4.1.1 supports the following licensed features. NOS 4.1.0 and above incorporates the Brocade VCS License as part of the base offering. This would mean customers would have to no longer purchase a license to enable VCS fabric (for more than 2 nodes).

- **Brocade Ports on Demand (POD) license** — Allows customers to instantly scale the fabric by provisioning additional ports via license key upgrade. (Applies to select models of switches).

- **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 Layer 3 License**: Enables support for Layer 3 features like OSPF, VRRPe and PIM. This license is required on the VDX8770 only. The VDX6710, VDX6720, VDX6730, 6740/T switches include these features in the default license.

- **Brocade Advanced Services license**: - Provides a single upgrade option to enable Virtual Cluster Switching (VCS), Fibre Channel over Ethernet (FCoE) and Layer 3 features on a VDX8770 switch with default license.

- **Brocade Upgrade License**: Provides a single license option to upgrade from either FCoE license or Layer 3 license to the advanced service license bundle.

- **Brocade 10G Port Upgrade License**: Allows customers to instantly scale the fabric by provisioning additional 10G ports via license key upgrade. (Does not apply to Modular Switches).

- **Brocade 10G Capacity on Demand License (for 6740T-1G)**: Allows customers to upgrade ports from 1G speed to 10G speed. With a license instance, customer can upgrade any 16 ports of the VDX 6740T-1G. To upgrade all the 48 ports, the customer will have to purchase
and install 3 license instances.

- **Brocade 40G Port Upgrade License**: Allows customers to instantly scale the fabric by provisioning additional 40G ports via license key upgrade. (Applies to VDX6740 and VDX6740-T only).

- **NOTE**: Layer 3 license is included in the default license on VDX67XX switches.

Some models may offer optional feature bundles that include two or more optionally licensed features. Refer to specific product model offerings for additional details on bundled options.

**Temporary License Support**
Temporary Licenses are available for all of the features listed above.

**Brocade Network OS Compatibility**
The VDX platforms with Brocade NOS v4.1.0 have been qualified for Ethernet or FC connectivity with the following Brocade platforms at the minimum firmware level noted for each:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Firmware Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCX/ICX</td>
<td>8.0.0a</td>
</tr>
<tr>
<td>BNA</td>
<td>12.2.0</td>
</tr>
<tr>
<td>vCenter</td>
<td>4.0,4.1,5.0,5.1,5.5</td>
</tr>
<tr>
<td>Brocade 8000</td>
<td>Fabric OS (FOS) v6.4.0b and up to v7.1.0</td>
</tr>
<tr>
<td>Brocade 8470 Switch Module (for IBM BladeCenter)</td>
<td>FOS v6.3.1_cee</td>
</tr>
<tr>
<td>Brocade 6520</td>
<td>FOS v7.1.0 or later</td>
</tr>
<tr>
<td>Brocade 5100/VA-40FC/5300/DCX/DCX-4S, 6510, DCX8510-8/ DCX8510-4</td>
<td>FOS v7.0.1 and later versions</td>
</tr>
</tbody>
</table>

**Fabric OS Compatibility**
A VDX 6730 running Brocade Network OS v2.1.1 or higher can form an Inter Fabric Link (IFL) by connecting to an EX-port on most Brocade 8Gbps or 16Gbps FC platforms operate with FOS v7.0.1 or later. In most common deployment scenarios, a VDX 6730/VCS fabric connects as an edge fabric to an FCR “backbone” fabric (an FC fabric with a switch acting as a Fibre Channel Router, or FCR). FCoE CNAs attached to the VCS fabric are then able to communicate with FC devices in an FC fabric, either connected directly to the FC backbone or to another FC edge fabric connected through the FC backbone fabric. The following table provides interoperability information and minimum firmware versions required for Brocade Network OS and FOS platforms.
<table>
<thead>
<tr>
<th>VDX Platforms/Brocade Network OS Firmware Versions</th>
<th>FCPlatforms/FOS Firmware Versions</th>
<th>FOS Firmware Version on Switches in FC Backbone or Edge Fabrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDX 6710/Brocade Network OS v2.1.1 or later</td>
<td>Brocade DCX/DCX-4S/DCX8510-8/DCX8510-4/6510/5300/5100/VA-40FC support forming an IFL connection to a VCS fabric with FOS v7.0.1 or later.</td>
<td>Please refer to FOS v7.1.0 release notes for complete interoperability matrix.</td>
</tr>
<tr>
<td>VDX 6720/Brocade Network OS v2.1.1 or later</td>
<td>Brocade 6520 support forming an IFL connection to a VCS fabric with FOS v7.1.0 or later.</td>
<td></td>
</tr>
<tr>
<td>VDX 6730/Brocade Network OS v2.1.1 or later 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VDX 8770/Brocade Network OS v3.0.0a or later</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VDX 6740, 6740-T/Brocade Network OS v4.1.0 or later</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table Notes:

1 The VDX 6730 is the only VDX platform that supports the FC ports necessary to form an IFL connection to an FC SAN. Other VDX platforms may participate in the VCS fabric, but cannot form the connection to the SAN.
2 There are other Brocade FC platforms that support FOS v7.0.1 and FCR/Integrated Routing functionality; however, those platforms are not supported for interoperability with VDX platforms when using FOS v7.0.1.

- While attempting VDX6730’s bridging ability to FC SAN, please use FOS version 7.0.1 at least on SAN side.

Limitations and Restrictions

Command Line Interface

- Some commands will not produce paginated output.
- Break command is not supported. Please 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 can not 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 & MC mode: the following are under rbridge-id context unlike earlier release
  ▪ fcsp
  ▪ secpolicy
  ▪ system-monitor is move 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

**VDX 6740/6740T**
- VDX 6740/6740T Platforms do not support IP fragmentation. MTU errors are reported in “show interface” as “Errors” under the “Transmit Statistics”

**Breakout functionality on 40Gb ports**
- Breakout functionality is supported on 40G ports on VDX 6740, VDX 6740T, VDX6740T-1G, and VDX 8770 only.
- Brocade Trunking is supported on Breakout Ports.
- Going to and from Breakout mode requires reload for VDX 6740, VDX6740T, and VDX6740T-1G. It requires reload of the LC with the affected 40G ports for VDX 8770.
- For VDX 6740, 6740T, and 6740T-1G platforms, the LED state for a breakout interface is deterministic. For all other supported platforms, the LED state for a breakout interface is not deterministic.
- In breakout mode, there is only SFP and no per-breakout media information. The show media command will display the same media information for all breakout interfaces. The TX Power Field in the show media command is not supported by the 40G optics.
- 1G speed cannot be configured on QSFP or breakout ports.
- Since ISL on breakout interface is not supported in prior releases, please note that this configuration may be lost if downgraded.

**Restrictions for Ports in 1G Mode and 1G Ports on VDX 6710**
- ELD not supported for 6710
- RMON stats are calculated incorrectly for packet sizes 64-127 bytes.
- 1G port in VDX 6710 cannot form ISL links. Only 10G ports in VDX 6710 can be used to form ISL links.
- 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.
- 1G portchannel between VDX 6740-T and MLX may not form

**Licensing**
- In Brocade Network OS v2.1.0 or later, VCS mode is no longer dependent on a full POD license being installed on the switch. In Brocade Network OS v2.0.0, a full POD (one POD license installed on VDX 6720-24, two POD licenses installed on VDX 6720-60) license was required in order to enable VCS mode. This restriction no longer applies in Brocade Network OS v2.1.0 or later, thus VCS mode can be enabled without installing POD licenses.
- POD and FCoE licenses are not used on the VDX 6710 platform. No POD license is required to enable any of the 48x1G ports or 6x10G CEE uplink ports on the VDX 6710.
For VDX 6730 platforms, enabling FC ports requires only the FCoE license and is not POD license controlled.

An Integrated Routing license is NOT required on FOS-based SAN platforms running FOS 7.0.1 or above for FCR interoperability connectivity with VCS fabrics and the VDX 6730. Please refer to FOS v7.0.1 Admin Guide documentation on configuring FOS platforms for connectivity to VDX 6730 switches and VCS fabrics.

The Layer 3 license is required on VDX 8770 switches to enable Layer 3 feature set including OSPF, VRRP, BGP, VRF etc. A separate Layer 3 license is not required on VDX 67XX switches as Layer 3 features are included in the default license.

After releasing a DPOD reserved interface, ‘show running-config’ may incorrectly show the interface as reserved. Please keep the unreserved interface in ‘shutdown’ to avoid undesirable behavior.

The Advanced Services License provides a single upgrade option to enable Virtual Cluster Switching (VCS), Fibre Channel over Ethernet (FCoE) and Layer 3 features on VDX 8770 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.

**In Logical Chassis**

- Standalone firmware download is supported. You can log onto individual nodes and run firmware download there. In such a case, please follow the notes above.
- You can run the logical-chassis firmware download command to upgrade one or more nodes from the principal node.
  - It is recommend to keep auto-activate mode off (which is the default) when running the logical-chassis firmware download command. After you download the new firmware to all of the nodes in the cluster, you can run “firmware activate rbridge-id <rbridge-ids>” to activate the nodes in the desired order.
  - Under certain stress conditions firmware download might time out on some nodes, e.g. due to excessive processing load on the processor, slow network, etc. It is recommended to re-run the logical-chassis firmware download command to upgrade these failed nodes and bring their firmware level to be the same as the rest of nodes first before activating any of them.
- While upgrading the cluster, it is recommended not to make any configuration changes in the cluster until all of the nodes have been upgraded to the same firmware. Otherwise, it may cause cluster segmentation.

**Logical Chassis**

- Number of nodes are limited to 24.
- Number of nodes can be 32 for VDX 8770 and VDX 6740/T cluster.
- Configurations are not auto preserved on mode transitions (between Fabric Cluster and Logical Chassis mode). Please follow the mode transition procedure as outlined. Non-default User id/password will be lost when migrating from FC to LC
- “show vcs” output displaying “Co-ordinator” OR “Coordinator” indicates “Principal” node role.
- “show vcs” output may not display expected output when management IP is removed & primary node is removed from the cluster
- Principal priority value ranges from 1 to 128, 1 being the highest. Recommend to set higher principle priority to VDX8770 & VDX6730 than VDX6720 & VDX 6710
- Shall not make configuration change during Logical Chassis firmware upgrade or ISL toggling to prevent the switch node segmenting from the cluster due to configuration mis-match
- Upon Node segmentation from the cluster, user shall run “copy default start” on the segmented switch node to bring it back to the cluster.
- Number of config snapshots saved on switch is limited to 4 per rbridge ID. So on 24 node cluster, a max of 24 * 4 = 96 snapshots are possible.
- For netconf and snmp, user has to poll using individual node Management IP
- Creating a snapshot with “\“ in snapshot-id creates the snapshot file with incorrect name
- There will not be any raslog to the user when replacement of a node fails
- With large configs, while a switch is rejoining a fabric with default config, “%Error:Could not find Interface” may be printed temporarily. The switch will recover and join the fabric.
- Under rare conditions, copy default to startup command may fail and restart VDX6740
- Config changes during principle switch-overs are not supported and may segment the cluster.

**HA**

- Full HA support is for L2, FCoE data and control protocols on VDX8770 in Fabric Cluster mode
- No HA support for IP data/control planes.
- After a recent failover, “show ha” may display HA state as ‘in sync’ even though it is not complete. Any attempt to failover at this stage may result in cold boot.
- RMON HA not supported.
- vMotion during HA failover is not supported
- UDLD HA is supported with higher range of udld timers ( >1 sec timer)
- HA failover is not supported for L3 features. However, L3 configuration is retained across failover
Platform

- After “chassis disable” please wait for 60 seconds for VDX67xx and for 300 seconds for VDX87xx before doing the next “chassis enable”.
- Chassis-name is limited to 15 characters.
- Under certain scenario, chassis airflow direction may not change for VDX-6730 even after configuring & rebooting the switch.
- 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.
- VDX-6740-T may display amber colored LED for the 40G interfaces that are up/up.
- Under certain conditions, the interface using 1G LX optics on VDX-6740 may show green LED even though the link is down. Occasionally, 1GE optics may display down state on one end whereas up state on the VDX-6740 end.
- 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.
- After “power-off linecard <x>” please wait for 120 seconds before doing the next “power-on linecard <x>” to avoid hitting a known defect where some interfaces might remain in administratively shut state.
- The speed on the management interface for VDX-8770 can be hardset to desired speed after configuring speed as auto. The speed on VDX-6740 is supported only in auto mode.
- Multiple OIR(Online insertion and removal) of 40G LR optics interop with ICX/FCX may cause link to remain down. Workaround is to flap the link.

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”.
- Chassis Virtual-IP is only supported on 8770.
**Security, ACLs, Authentication, Authorization**

- Netconf session may get closed for get-vlan-brief
- Slot-eth-port-cnt may not be reflected for 87xx line cards
- 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 (Tac+/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.
- If SPAN has to be supported to multiple locations, please use RSPAN on vlan.
- On VDX 6720, only one port per port group can be configured as destination port for ingress spanning.
- On 6720, only one port per port group can be configured as destination port for egress spanning.
- On 6720, ISL port cannot be source or a destination SPAN port. On 8770 and SPAN in VCS feature, ISL can be source port, but the destination has to be on the same rbridge.
- 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. RSPAN may not mirror traffic from VDX 6740-T to the port on VDX-6740.

**ICMPv6 RA Guard**

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

**Trunking**

- For the VDX 6740 and VDX 6740T Brocade trunk (BTRUNK) has a maximum throughput of 160G using 16 10G ports in the same trunk group. On these platforms traffic may not be distributed evenly across all member of a trunk at lower traffic rates.
- 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).
- 40G BTRUNK is supported between VDX 6740/VDX 6740-T (2-port trunk).

**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 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 envrioment. UDLD may flap during HA failover and ISSU

**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 uses 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 linecard powercycle

**Long Distance ISL Ports**
- Standard ISL is supported on 10G/40G interfaces up to a distance of 1000m without any special commands. "long-distance-isl" command is not required and should not be used to form an ISL up to a distance of 1000m.
- Long distance ISL is only supported on 10G interfaces.
- Long distance ISL configuration is not allowed if CEE Map/fcoeport is configured on any edge ports in the same port group.
- CEE Map modification is not allowed when long distance ISL is configured.
- A maximum of three PFCs can be supported on a long distance ISL configured platform.
- When long distance ISL is configured on the switches, all ports in the port group will be bounced.
- Both side of long distance link should have long-distance-isl configuration. Otherwise end to end PFC might not work appropriately.
- For 10Km/Extended Range long distance configuration, all other ISLs in the port group will be disabled.
- For 2Km/5 Km long distance configuration, one other ISL will be allowed to come online in the port group.
• For 2 km, 5 km and 10 km long-distance, use Brocade supported Long Range (LR) optics for direct connectivity.
• For 30 km long-distance, use Brocade-supported Extended Range (ER) optics for direct connectivity.

**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 with an exception of FCoE sub-profile which is not supported in VLAG mode.

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 VF s 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 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 is supported 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.x, 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.
- In a hybrid logical-chassis, if a user configures a platform specific feature, it will be configured only on the rbridges which support that feature.
- Asymmetric pause is supported on 1G ports on 6710 and other 1G port interfaces.
- VDX 6740 supports 3 PFC queues.
- Flow control is disabled by default on all interfaces.
- Trust- support only standalone mode, no VCS mode.
- DSCP to CoS Mutation- all platforms (VDX8770, VDX 67xx).
- DSCP to Traffic Class Mutation - all platforms (VDX8770, VDX 67xx).
- DSCP to DSCP Mutation (VDX 8770 and 6740/T only).
- Random Early Discard (RED) (VDX 8770 and 6740/T only).
- 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 not having FCoE ports and Long Distance ISL ports in the same port-groups. This configuration will NOT be prevented by the CLI; however it can result in unpredictable behavior for FCoE traffic.
- 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’s recommended to provide the range only in ascending order. For ex: 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.
• After non ISSU upgrade from NOS4.0.1 to NOS 4.1.0 sometimes plogi failures are observed. Work around is unknown.
• 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

**FC/Fport**
• F port can support only 63 NPIV devices
• Loop devices are not supported.
• No long distance support for F-Ports.
• Proprietary features such as trunking, QOS, D-Port, FAPWWN, Credit Recovery and FEC are not supported on FC F-Ports.

**VRRP**
• VRRP and VRRP-E cannot be enabled together on VDX 6740 and 6740T platforms. Command “protocol vrrp-extended” is added to specifically enable VRRPE.
• VRRP/VRRPE undergoes disruption during ISSU or HA failover.
• VRRP-E global sessions may get disabled after firmware upgrade
• Large VRRP config may increase config download time
• ‘no preempt-mode’ is not honored on physical interfaces of 87xx

**OSPF**
• Graceful restart is not supported

**BGP**
• Following BGP features are not supported in this release:
  - VRF-Lite support
  - 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
- VRF
- 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

**VRF**

- Management VRF is not supported
- VRF lite supports OSPF and static routing but not BGP
- On configure VRF on an interfaces, all previous IP config would be lost
- IP Services like telnet are not supported on non-default VRF
- User will not be able to access VDX switches through interfaces belonging to non-default VRF
- Static route leak is supported across VRFs
- Modifying VRF address family will lose all IPv4 configuration related to that VRF including router ospf instance on that VRF
- User should delete all route leak configuration on a VRF before deleting that VRF

**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
- L2 packets may not be sampled on linecard power OFF & ON
- 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 keepalive timeout followed by shut & no shut of the port-channel link may prevent FCoE logins through that port-channel
- On rare instances of HA failover, SFM may turn faulty. Workaround is to manually reseat the card
- On rare instances of ISSU, HA failover, linecard may turn faulty. Workaround is to reset the linecard
- PCAP utility may not work correctly after HA failover operation. Workaround is to reload the chassis system.
- 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)

**Virtual Fabric**
- This feature is NOT supported on eAnvil based platforms.
- PIM-SM is not supported on Virtual Fabric.
- Virtual Fabric & Transport Fabrics do not support Native VLAN configuration. While the CLI does not restrict, we strongly recommend not using this feature.
- For frames forward on a transport fabric, ingress CTAG tagging is preserved at the egress port regardless of the egress tagging classification. Default-vlan can only be configured using TRANSPORT VF IDs
**Policy-based Routing (PBR)**

- This feature is NOT supported on eAnvil based platforms.
- If a PBR route-map is applied to an interface that is actively participating in a control protocol and the ACL specified in the route-map also matches the control protocol traffic the control protocol traffic will be trapped to the local processor and not be forwarded according to the route-map.

**Inter-VRF Leaking (Static)**

- S+ symbol routes indicated leaked routes
- There is no CLI check for Route leak configuration in source VRF colliding with route/interface configuration in target VRF – User has to take care of this
- VRF route leak cascading is not supported
- User should avoid making Static, dynamic and connected route conflict with routes in target VRF when configuring route leak
- Static route leak with interface as next hop is not supported
- Before deleting a VRF, user should delete all route leaks configured under that VRF
- For bidirectional traffic with router leak, user needs to configure route leak in both direction separately
- Route leak configuration to next hop IP on the same box on different is not a valid configuration, but CLI will be accepted
- Ongoing Switch generated traffic like ping through leaked routes will continue flow even after deleting VRF route leak
- Precaution needs to be taken when leaking default routes - this can result in routing loops
- Switch management from non-default VRF by leaking route from non-default VRF to default VRF is not supported

**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
- There is no HA support for dhcp relay statistics. When a switchover happens, the statistics will not be replicated to the new active MM.

**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
- For dual MM chassis, dual MM must be in sync for DAD to function
- DAD is a disruptive. ISSU is not supported
- In FIPS mode, DAD is not supported.
**Logical Chassis HA**

- Logical Chassis HA is supported only on VDX8770 with dual Management Modules (MM).
- Full HA sync is supported.
- As long as the system has HA “In-Sync” state, warm recovery is supported for both planned as well as unplanned MM failover.
- There will be no overall configuration replay after warm recovery, except for Layer 3 protocol configurations which do not support HA. If the switch undergoing MM failover is the VCS cluster principal switch, it will continue to remain as the principal switch after the MM failover. All the secondary nodes will first disconnect from it when the MM failover starts and then rejoin as the VCS cluster is reformed. The Fabric Cluster will remain intact and there will be no traffic disruption.
- If the switch undergoing MM failover is a secondary switch, the switch will disconnect and rejoin the VCS cluster after reestablishing connection with the principal switch and the rest of the cluster will stay intact. The Fabric Cluster will remain intact and there will be no traffic disruption.

**Access Gateway (6730)**

- Access Gateway (AG) functionality can be enabled only on VDX6730.
- Enabling AG requires FCoE license.
- In Logical Chassis mode, AG is enabled on the local node and AG configurations will not be distributed.
- The switch will be reloaded on enabling Access Gateway.
- AG does not bridge the VCS and SAN fabrics because hosts connected to the AG switch are registered in the SAN name-server only. Therefore, all zoning operations for AG are done on the SAN fabric.
- At least one N-port must be up in order for FCoE devices to log in.
- In FC mode, if user enables Access Gateway mode, changes configuration, commits it to the startup config and disables Access Gateway mode, the user will need to perform a copy running to start-up once before enabling again Access Gateway mode if he wishes to get default Access Gateway configuration. Please note that otherwise, user will get the previous Access Gateway configuration which was present the last time when he performed running to start-up with Access Gateway enabled.

**Auto QOS for NAS**

- All auto-nas config should be removed before downgrading board from NOS4.1.0 to prior releases.
  Downgrade without first removing the related autonas configs will result in running-config still displaying the configs.

**Brocade ISL trunking on 40Gb ports**

- Brocade trunking is supported on 40G ports of VDX6740, VDX6740T, VDX6740T-1G and VDX8770
- 40G ports can form a Brocade trunk only if they are from same port-group.
In order that the 40G ports on VDX8770 form Brocade trunk, it is required that the ports be in breakout mode. There is no such requirement for VDX6740, VDX6740T and VDX6740T-1G.

Two 40G breakout ports in the same port-group of VDX8770 can form 80G trunk consisting of 8 10G ISL ports. Breakout optics with a single QSFP optical cable must be used.

Prior to NOSv4.1.0, “fabric trunk enable” configuration on the 40G interfaces on VDX8770 is allowed, however it does not provide non-breakout mode trunk capability to the ISLs.

Upgrading from any previous version to NOS4.1.x will change the default configuration on 40G interfaces on VDX8770 from “fabric trunk enable” to “no fabric trunk enable” to accurately indicate the capability. Configuring “fabric trunk enable” directly on the 40G interfaces is accordingly blocked.

**VCS VXLAN Gateway for VMWare NSX**

- VCS VXLAN Gateway for NSX is supported only on VDX6740, VDX6740T and VDX6740T-1G.
- VCS VXLAN Gateway for NSX is supported only in the VCS Logical Chassis mode.
- A maximum of 2 RBridges are supported in a VXLAN enabled VCS Cluster.
- Only 1 VTEP Gateway is supported in a VXLAN enabled VCS Cluster.
- VMware NSX vSwitch with vSphere version 5.5 (ESXi 5.5) and KVM on Ubuntu 12.04 are supported as hypervisors.
- Only one-to-one VLAN to VNI mapping is supported.
- Only Default VRF is supported for VCS VXLAN Gateway configuration.
- Tunnel interfaces cannot be used as SPAN (Switch port Analyzer) destination.
- Ingress/Egress ACLs cannot be applied to tunnels
- Ingress/Egress QoS policies cannot be applied to tunnels
- Unicast/Multicast routing between VXLAN and VLAN/VXLAN is not supported.
- After removing the transport node from the NSX, the switch is disconnected from the NSX controller. After multiple retries to reconnect, the switch eventually declares the connection as dead. The connection status can be checked using “show nsx-controller brief”. If the connection status is declared dead before the transport node is added back, the commands “nsx-controller name <name> reconnect” or “nsx-controller <name> no activate/activate” need to be performed on the switch to reconnect to the NSX controller.
- When using the command “show overlay-gateway name <name> vlan statistics” for debugging overlay-gateway VLANs, it should be noted that the statistics information is limited to 256 VLANs for RX and 116 VLANs for TX.

**Upgrade and migration considerations**

General information on installing Brocade Network OS can be found in the Brocade Network OS Admin Guide. This section includes special considerations and caveats to be aware of when upgrading to or from this version of Brocade Network OS, as well as recommended migration paths to use to reach this version of Brocade Network OS.

**Note:** Installing Brocade Network OS is service disruptive and any un-saving running configuration will be lost during the installation.
This table summarizes the upgrade/downgrade scenarios between NOS 4.0.x and NOS 4.1.x. Details for the scenarios and other versions are provided after the table.

The following table applies to both Fabric Cluster and Logical Chassis modes.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>NOS 4.0.x patch (4.0.1x)</th>
<th>NOS 4.1.0</th>
<th>NOS 4.1.x</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.x GA (4.0.0a, 4.0.0b)</td>
<td>NA</td>
<td>ISSU Upgrade (Config Preserved)</td>
<td>Non-ISSU Upgrade (Config Preserved)</td>
<td>Non-ISSU Upgrade (Config Preserved)</td>
</tr>
<tr>
<td>NOS 4.0.x patch (4.0.1)</td>
<td>ISSU Downgrade (Config preserved)</td>
<td>NA</td>
<td>Non-ISSU Upgrade (Config Preserved)</td>
<td>Non-ISSU Upgrade (Config Preserved)</td>
</tr>
<tr>
<td>NOS 4.1.0</td>
<td>Non-ISSU Downgrade (Config Loss, switch goes to default-config)</td>
<td>Non-ISSU Downgrade Config Preserved (without new feature enabled/configured)</td>
<td>NA</td>
<td>ISSU Upgrade (Config Preserved)</td>
</tr>
<tr>
<td>NOS 4.1.x</td>
<td>Non-ISSU Downgrade (Config Loss, switch goes to default-config)</td>
<td>Non-ISSU Downgrade Config Preserved (without new feature enabled/configured)</td>
<td>ISSU Downgrade (Config preserved)</td>
<td>NA</td>
</tr>
</tbody>
</table>

**Recommended Migration Paths for Brocade Network OS v4.1.x**

Switches operating with earlier versions of Brocade Network OS, including Brocade Network OS v2.1.X, should first be upgraded to Brocade Network OS v3.0.1b, then to 4.0.1 and then to Brocade Network OS v4.1.x.

**Considerations and Limitations:**

**Upgrading from Brocade Network OS v3.x**

- Firmware upgrade is supported for all VDX6730/VDX6720/VDX6710 TOR and VDX8770 chassis platforms.
- Switches operating with earlier versions of Brocade Network OS, including Brocade Network OS v3.X, should first be upgraded to 4.0.1 and then to Brocade Network OS v4.1.0.
- This upgrade doesn’t apply to VDX6740 TOR based platform, as by default it comes with Brocade Network OS 4.0.0.
**Upgrading from Brocade Network OS 2.x**

- Switches operating with earlier versions of Brocade Network OS, including Brocade Network OS v2.1.1, should first be upgraded to Brocade Network OS v3.0.1b, then to 4.0.1 and then to Brocade Network OS v4.1.0. If the switches are running a NOS version prior to 2.1.1, then the switches need to be upgraded to NOS 2.1.1.
- Firmware upgrade is only supported on all VDX67XX platforms.
- This upgrade doesn’t apply to VDX87XX chassis based platform, as by default it comes with Brocade Network OS 3.0.1x.

**Switch additions to cluster scenarios:**

**Adding a switch running Brocade Network OS v4.0.x to Brocade Network OS v4.1.x cluster**

- When a switch with Brocade Network OS v4.0.x is added to Brocade Network OS v4.1.x it will form a mixed cluster and Fabric distribution service will be disabled. Some of the services that will not be supported and utilizes “FDS cluster” are 1) Zoning 2) vCenter 3) “show vcs” CLI 4) Virtual IP. Limited support for all other services is available in mixed image environment.

**Adding a switch running Brocade Network OS v4.1.x to Brocade Network OS v4.0.x cluster**

- When a switch with Brocade Network OS v4.1.x is added to Brocade Network OS v4.0.x it will form a mixed cluster and Fabric distribution service will be disabled. Some of the services that will not be supported and utilizes “FDS cluster” are 1) Zoning 2) vCenter 3) “show vcs” CLI 4) Virtual IP. Limited support for all other services is available in mixed image environment.

**Adding a switch running Brocade Network OS 2.X to Brocade Network OS v4.1.x cluster**

- Brocade Network OS 2.x switch would not interoperate with Brocade Network OS 4.1.x.
- ISLs will be segmented with a reason of FDS mode mismatch.

**Adding a switch running Brocade Network OS v3.0.x to Brocade Network OS 4.1.x cluster**

- Brocade Network OS 3.0.x switch would not interoperate with Brocade Network OS 4.1.x.
- ISLs will be segmented with a reason of FDS mode mismatch.
Upgrading to this release
Upgrading Best Practices (Applies for all VDX Platforms)

In Logical Chassis mode it is required to upgrade Principal switch at the end if Option (B) or (C) is opted.

A. Upgrade all nodes in the cluster at same time -- Service Disruptive Cluster Wide
   - Download the firmware (Brocade Network OS v4.1.x) in all the switch nodes running Brocade Network OS v3.x without reboot. In case of VDX8770 chassis systems with dual MM, user needs to individually download the firmware (Brocade Network OS v4.1.x) to both the MMs without reboot.
   - After all switches complete the firmware download, reboot all nodes at the same time.
   - After all switches boot-up, they shall form one Brocade Network OS v4.1.x cluster.
   - This is Service Disruptive Cluster Wide regardless of Cluster topology.
   - Brocade Network OS 2.x.x cannot be directly upgraded to Brocade Network OS 4.1.x.

B. Upgrade Odd/Even Nodes (one segment at a time)—Lossless Upgrade: (Mixed version fabric is supported during upgrade maintenance window)
   - This is the most recommended procedure for lossless upgrade. This requires servers to be dual homed.
   - Download the firmware (Brocade Network OS v4.1.x) in all the switch nodes running Brocade Network OS v4.0.x without reboot. In case of VDX8770 chassis systems with dual MM, user needs to individually download the firmware (Brocade Network OS v4.1.x) to both the MMs without reboot.
   - After all switches complete the firmware download, reboot all the odd nodes. Half of the cluster is now on the latest version. Traffic resumes and passes through other half of the cluster.
   - Now reboot all even nodes. At this point, entire cluster is loaded with latest image and up and running.

C. Upgrade one node at a time -- Service Disruptive at Node level in the Cluster
   - Download the firmware Brocade Network OS v4.1.x on a one node at a time in cluster running Brocade Network OS v3.x and reboot. Principal node in a cluster should be last to be upgraded.
   - After a node is upgrade to Brocade Network OS v4.1.x, it will join the existing NOS v3.x Cluster but with no FDS services. Eventually, when all the nodes are upgraded, they will form one NOS v4.1.x VCS Cluster. [Note no configuration changes are allowed at this time.]
Downgrading to a previous release
Downgrading Best Practices for VDX 67XX and VDX 87XX

- The downgrade process is service disruptive.
- Before downgrading to NOS 4.0.x, **backup** the running configuration of NOS v4.1.x
  - To external FTP server as well as
  - To startup-config.
- In-Service Software Upgrade (ISSU) is not supported while downgrading from NOS4.1.x to 4.0.x and prior versions on VDX8770.
- In-Service Software Upgrade (ISSU) is supported while downgrading to/from NOS4.1.x for different versions of “x” on VDX8770.
- When downgrading to 4.0.1 please use ‘coldboot’ option along with ‘firmware download’ command. Configuration will be preserved in this process.
- When downgrading to 4.0.0, the configuration will not be preserved and hence we recommend to use the ‘default-config’ and ‘manual, noreboot’ options. Please ensure that both management modules are reloaded at the same time.
- If there are new features or new scale enhancements specific to NOS v4.1.x, we recommend to remove them before downgrade. As an alternative, user may use ‘default-config’ option and use the backed up configuration to restore after downgrade.
- If a certificate was generated on the switch for NSX-controller (show nsx-controller client-cert), it is required to delete the certificate before downgrading below NOS v4.1.1. Use command “nsx-controller client-cert delete” to delete the certificate before downgrading.
- Before downgrading to NOS4.0.1b or lower with vCenter enabled on the switch, ensure that there are no ESXi5.5 hosts with "NSX vSwitch" configuration attached to the vCenter server. Downgrading with ESXi5.5 hosts with vSwitch and dvSwitch configuration has no such restrictions.

Upgrade / Downgrade Considerations for FCoE

The default number of FCoE interfaces has been reduced from 256 (NOS4.0.x) to 64 (NOS4.1.x) in order to optimize running-configuration size. Two new CLIs have been introduced to support back-ward compatibility; “fcoe-enodes” and “enode-config” under “rbridge-id fabric-map”. Please note the following.

**Upgrade from NOS4.0.x to NOS4.1.1 on nodes with FCoE License**

- If number of static FCoE bindings is between 0 to 64
  - The parameter “fcoe-enodes” will be defaulted to 64.
  - Any extra fcoe interfaces (“max-enodes – fcoe-enodes”) will be deleted
- If number of static FCoE bindings is more than 64
  - The parameter “fcoe-enodes” will be set to the same value as number of static bindings.
Upgrade from NOS4.0.x to NOS4.1.1 on nodes without FCoE license

- The parameter “fcoe-enodes” will be set to 0
- All fcoe interfaces will be deleted

Downgrade from NOS4.1.1 to NOS4.0.x

The parameter “enode-config” under fabric-map is newly added in NOS4.1.0 and will be set to value “local” after upgrade from NOS4.0.x to NOS4.1.x. Before downgrade from NOS4.1.0 to NOS4.0.x the “enode-config” needs to be set to “global”. This will ensure that at least 256 interfaces are present.

Upgrade / Downgrade Considerations for vLAG

Upgrade Scenario for vLAG (Not applicable for VDX87XX)

VLAG supports Firmware Upgrade from NOS v4.0.x to Network OS v4.1.x on VDX67XX platforms. VLAG Feature doesn’t have any restriction or add new limitation for the Firmware Upgrade scenario from NOS v4.0.x to Network OS v4.1.x

In all there are 2 approaches with which vLAG nodes can be upgrade to NOSv4.1.x from NOS v4.0.x

Please refer to above topology for below 2 approaches.

Approach 1 - Involves graceful shutdown of vLAG ports on one of the nodes at a given time:

Below are the steps to upgrade nodes running NOS v4.0.x to Network OS v4.1.x in a VCS cluster. Say there are 2 nodes R1 and R2 with are part of one vLAG

- Pick a node (say R1) with vLAG ports, Admin shut all the vLAGs (shut under int port-channel x) on the node. Save running configuration to startup-configuration. This should basically reduce the vLAG into a single node vLAG/port-channel.
- If the vLAG is in static mode, all members of the port-channel should be shutdown. This is due to Static LAG behavior where it may bring UP the member link even if the port-channel is admin shut.
- Upgrade R1 with Network OS v4.x and reboot R1.
- After R1 is operational up running Network OS v4.1.x software, perform admin shut of local vLAGs (shut under int port-channel x) on the other NOS v4.0.x node (R2). There will be a complete data path impact on the vLAG at this given time.
- Immediately perform admin no shut on the vLAG on R1 running Network OS v4.0.x. This will help you to avoid a longer delay here, so please perform this step efficiently and optimally.
- Upgrade/Reboot R2 with Network OS v4.1.x. This time no need to save running configuration to startup on the second node (R2).
- After R2 reboots and operationally up, it will re-join the vLAG and we should now have the vLAG spanning two nodes running Network OS v software.
- After all vLAG nodes are upgraded, save running configuration back to startup on R1.
Advantages

- Clean upgrade
- No duplicate primary port issues
- Works well for both Static and Dynamic vLAGs

Disadvantages

- Involves some work for the administrator to perform shut/no-shut on vLAGs, particularly when in large numbers.
- Need precise and efficient execution of the plan.
- There will be a data-path impact for a very small period (when vLAG is shut on the second node, until a no shut is executed on the first node).

Approach 2 - Applicable for Static vLAGs and Dynamic vLAGs without configuration changes

Below are the steps to upgrade nodes running NOS v4.0.x to Network OS v4.1.x in a VCS cluster. For example there are 2 nodes R1 and R2 with are part of one vLAG.

Step 1: Pick a node (say R1) with vLAG ports, Upgrade with Network OS v4.1.x and Reboot R1. There are 2 possibilities as follows:

- **Possibility 1**: No impact/reconvergence to Static or Dynamic (with Ignore-Split ON) vLAGs. Minimal data path impact observed.
- **Possibility 2**: For Dynamic vLAGs with ignore-split OFF (Applies if someone has explicitly made ignore-split OFF).
  - If R1 was a lower rbridge-id, there will be minimal data path impact but no vLAG reconvergence.
  - If R1 was a higher rbridge-id, you’ll notice vLAG flap and observe few seconds of data path impact.

Step 2: After R1 is operational up running Network OS v4.1.x software, it will re-join the vLAG. There will be 3 possibilities.

- **Possibility 1**: For Static vLAG, the new node will not pick itself as primary RBridge. The NOS v3.x node will retain the Primary role.
- **Possibility 2**: For Dynamic vLAG, with ignore-split ON, will result in the NOS v4.1.x node retaining the primary role
- **Possibility 3**: For Dynamic vLAGs with ignore-split OFF (Applies if someone has explicitly made ignore-split OFF)
  - If R1 was a lower Rbridge-id, it will not pick itself as primary. The NOS 3.X node will retain the Primary role.
  - If R1 was a higher Rbridge-id, due a LACP SID mismatch the local ports will be logically offline.
**Step 3:** Upgrade R2 to Network OS v4.1.x and reboot it. After this there are 3 possibilities

- **Possibility 1:** No impact to Static vLAGs. The Minimal data path impact is less than 1 Sec.
- **Possibility 2:** No impact to Dynamic vLAGs with *ignore-split ON*. The Minimal impact to data path is less than 1 Sec.
- **Possibility 3:** For Dynamic vLAGs with *ignore-split OFF*, If R1 was higher rbridge-id, LACP will re-converge on R1 and vLAG will be re-formed. This will result in a data path loss for few seconds.

**Step 4:** After R2 boots up, it’ll re-join the vLAG and we’ll now have vLAG spanning two nodes and actively running Network OS v4.1.x firmware.

**Advantages:**

1. No additional administration or configuration changes.
2. It is a straightforward upgrade process, no special handling for vLAGs.

**Disadvantages:**

1. There will be a data-path impact as detailed above.

**Downgrade Consideration for vLAG**

There is no downgrade consideration for vLAG. First the rbridge has to be downgraded like a normal downgrade procedure mentioned below. Once it is successfully downgraded to NOS 4.0.x, vLAG should function normally.

- Copy the running configuration of NOS 4.0.x to FTP before you upgrade it to Network OS v4.1.x.
- Copy the default configuration to the startup configuration.
- Reboot the Rbridge.
- Downgrade the Rbridge to NOS 4.0.x.
- Copy the default configuration to the startup configuration.
- Reboot the Rbridge. It will have the 4.0.x configuration as default.
- Copy the configuration file of NOS 4.0.x from FTP server to the running configuration.
- Save the configuration.

**Changing Management Gateway IP for Network OS 4.0.1 and above**

**VDX67xx**

In Network OS 4.0.1 and above, VDX67xx (Standalone, VCS fabric cluster mode and VCS logical chassis mode) admin has to use "ip route 0.0.0.0/0 <gateway ip>" command to configure the gateway.

Prior to 4.0.0, 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 and LC mode this command is available under RB context, whereas in SA mode the same is available in configuration mode.

Please note the following:
- L3 license is enabled by default on VDX67xx.
- After upgrading to NOS 4.0 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.

**VDX8770 (No L3 license/with L3 license)**

In Network OS 4.0.1 and above, VDX87xx (VCS fabric cluster mode and VCS logical chassis mode) admin has to use “ip route 0.0.0.0/0 <gateway ip>” command to configure the gateway.

Prior to 4.0.0, there were two ways to configure the gateway based on the availability of L3 license in the device
- L3 license available: admin has to use the command "ip route 0.0.0.0/0 <gateway ip>". Other command "ip gateway-address" under the management interface used to display an error.
- L3 license not available: admin has to use the "ip gateway-address" under the management interface.

In 4.0 there is only one option to configure the gateway that is "ip route 0.0.0.0/0 <gateway ip>".

Please note the following:
- After upgrading to NOS 4.0.1 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.
- In 3.x without L3 License the user had the option to configure gateway in both the MMs, which is not the case in 4.x

**Scalability**

Scalability

All scalability limits are subject to change. Limits may be increased once further testing has been completed, even after the release of a particular Brocade Network OS version. The limits noted in this table apply to all the VDX platforms unless otherwise specified.

<table>
<thead>
<tr>
<th>Network OS v4.1.1 Scallability Numbers</th>
<th>VDX 6710/20/30 Standalone Mode</th>
<th>VDX 6710/20/30 VCS Mode</th>
<th>VDX 6740 VCS Mode</th>
<th>VDX 8770 VCS Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum # of VLANs</td>
<td>3,500</td>
<td>3,500</td>
<td>3,500</td>
<td>4,000</td>
</tr>
<tr>
<td>Maximum # of MAC addresses</td>
<td>30,000</td>
<td>30,000</td>
<td>120,000</td>
<td>128,000</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------</td>
<td>--------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Maximum # of port profiles(AMPP)</td>
<td>750</td>
<td>750</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Maximum # of VLANs in port profiles</td>
<td>3,500</td>
<td>3,500</td>
<td>3,500</td>
<td>4,000</td>
</tr>
<tr>
<td>Maximum # of MAC Associations for AMPP</td>
<td>16,000</td>
<td>16,000</td>
<td>16,000</td>
<td>24,000</td>
</tr>
<tr>
<td>Maximum # of per priority pause levels</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>Maximum # of IGMP Snooping Interfaces supported</td>
<td>NA</td>
<td>128</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>Learning rate for IGMP snooping (groups/second)</td>
<td>NA</td>
<td>256</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>Maximum # of L2 (IGMP Snooping) multicast groups</td>
<td>NA</td>
<td>2,000</td>
<td>6,000</td>
<td>6,000</td>
</tr>
<tr>
<td># of L3 (S,G) forwarding Entries</td>
<td>NA</td>
<td>NA</td>
<td>2,000</td>
<td>2,000</td>
</tr>
<tr>
<td># of L3 (*,G) forwarding Entries</td>
<td>NA</td>
<td>NA</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td># of L2/L3 Multicast Flows</td>
<td>NA</td>
<td>NA</td>
<td>10,000</td>
<td>10,000</td>
</tr>
<tr>
<td>PIM Interfaces Supported</td>
<td>NA</td>
<td>NA</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>Feature</td>
<td>4.1.1</td>
<td>N/A</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>IGMP interfaces supported</td>
<td>NA</td>
<td>NA</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>Learning Rate for PIM-SM (flows/second)</td>
<td>N/A</td>
<td>N/A</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>Maximum Total # of L2 + L3 ACL rules</td>
<td>12,000</td>
<td>12,000</td>
<td>12,000</td>
<td>12,000</td>
</tr>
<tr>
<td>Maximum # VLAN per Edge Port in Trunk Mode</td>
<td>3,500</td>
<td>3,500</td>
<td>4,000</td>
<td>4,000</td>
</tr>
<tr>
<td>Maximum # of VF Ports (Per switch)</td>
<td>NA</td>
<td>1,000</td>
<td>1,000</td>
<td>1,000</td>
</tr>
<tr>
<td>Maximum # of NPIV per Port</td>
<td>NA</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>Maximum # of Enodes per Fabric</td>
<td>NA</td>
<td>2,000</td>
<td>2,000</td>
<td>2,000</td>
</tr>
<tr>
<td>Maximum # of FCoE interfaces (Per switch)</td>
<td>NA</td>
<td>1,000</td>
<td>1,000</td>
<td>1,000</td>
</tr>
<tr>
<td>Maximum # of FCoE Devices per Fabric</td>
<td>N/A</td>
<td>2,000</td>
<td>2,000</td>
<td>2,000</td>
</tr>
<tr>
<td>Maximum # of SAN Devices (FC + FCoE) per Fabric</td>
<td>N/A</td>
<td>3,000</td>
<td>3,000</td>
<td>3,000</td>
</tr>
<tr>
<td>Maximum # of FCoE Logins (Per switch)</td>
<td>N/A</td>
<td>1,000</td>
<td>1,000</td>
<td>1,000</td>
</tr>
<tr>
<td>Number of active STP nodes (Per cluster)</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>60</td>
<td>60</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------</td>
<td>-------------------------</td>
<td>-------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>No. of ports per node (phy) participating in xSTP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No. of ports per Cluster in xSTP</td>
<td>480</td>
<td>480</td>
<td>480</td>
<td>480</td>
</tr>
<tr>
<td>No. of vlags assuming 2-4 nodes in vlag</td>
<td>64(512* if bpdu guard enabled)</td>
<td>64(512* if bpdu guard enabled)</td>
<td>64(512* if bpdu guard enabled)</td>
<td>64(512* if bpdu guard enabled)</td>
</tr>
<tr>
<td>No. of vlags (participating xSTP) assuming 2-4 nodes in vlag</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>No. of vlags (participating xSTP) assuming 8 nodes in vlag</td>
<td>32</td>
<td>32</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>No. of PVST instances</td>
<td>128</td>
<td>128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>No. of RPVST instances</td>
<td>128</td>
<td>128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Maximum # of MSTP instance</td>
<td>32</td>
<td>32</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>Maximum # of VLAN in PVST</td>
<td>128</td>
<td>128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Maximum # of LAG groups</td>
<td>60</td>
<td>60</td>
<td>60</td>
<td>384</td>
</tr>
<tr>
<td>Maximum # of members in a standard LAG</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Maximum # of</td>
<td>8</td>
<td>8</td>
<td>16</td>
<td>8</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>members in a</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brocade LAG</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum # of</td>
<td>NA</td>
<td>32</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>switches in a Fabric</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum # of</td>
<td>NA</td>
<td>24</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>switches in Logical</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum # of</td>
<td>NA</td>
<td>8</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>ECMP Paths</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum # of</td>
<td>NA</td>
<td>8</td>
<td>16</td>
<td>8</td>
</tr>
<tr>
<td>trunk members for</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fabric ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum # of</td>
<td>NA</td>
<td>512</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>VLAG groups</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum # of</td>
<td>NA</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>member ports in a</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAG</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum # of</td>
<td>NA</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>nodes in a VLAG</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum # of</td>
<td>NA</td>
<td>16</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>member ports per</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAG per Node</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum # of</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>Management ACL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum # of</td>
<td>8,000</td>
<td>8,000</td>
<td>8,000</td>
<td>8,000</td>
</tr>
<tr>
<td>VMs supported in VM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aware Network Automation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum # of</td>
<td>NA</td>
<td>8,000</td>
<td>12,000</td>
<td>50,000</td>
</tr>
<tr>
<td>ARP Entries</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum # of</td>
<td>N/A</td>
<td>1,500</td>
<td>4,000</td>
<td>32,000</td>
</tr>
<tr>
<td>----------------</td>
<td>-----</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>Unicast IPv4 routes in the hardware</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum # of OSPF areas</td>
<td>N/A</td>
<td>16</td>
<td>20</td>
<td>64</td>
</tr>
<tr>
<td>Maximum # of OSPF routers in a single area</td>
<td>NA</td>
<td>12</td>
<td>64</td>
<td>200</td>
</tr>
<tr>
<td>Maximum # of OSPF adjacencies</td>
<td>NA</td>
<td>12</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>Maximum # of OSPF routes</td>
<td>NA</td>
<td>1,500</td>
<td>4,000</td>
<td>32,000</td>
</tr>
<tr>
<td># of OSPF Interfaces</td>
<td>NA</td>
<td>64</td>
<td>100</td>
<td>1,000</td>
</tr>
<tr>
<td># of OSPF enabled subnets</td>
<td>NA</td>
<td>64</td>
<td>100</td>
<td>600</td>
</tr>
<tr>
<td># of local subnets in a single area</td>
<td>NA</td>
<td>64</td>
<td>100</td>
<td>600</td>
</tr>
<tr>
<td>Maximum # of routes in SW</td>
<td>NA</td>
<td>1,500</td>
<td>4,000</td>
<td>32,000</td>
</tr>
<tr>
<td>Maximum # of static routes</td>
<td>NA</td>
<td>500</td>
<td>1,000</td>
<td>5,000</td>
</tr>
<tr>
<td>Maximum # of dynamic routes</td>
<td>NA</td>
<td>1,500</td>
<td>4,000</td>
<td>32,000</td>
</tr>
<tr>
<td>Maximum # of VRRP instances per system</td>
<td>N/A</td>
<td>64</td>
<td>256</td>
<td>1,024</td>
</tr>
<tr>
<td>Maximum # of VRRP instances per interface</td>
<td>N/A</td>
<td>8</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>Maximum # of routers participating in a VRRP-E session</td>
<td>N/A</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Maximum # of routes with ECMP supported</td>
<td>NA</td>
<td>1500</td>
<td>4,000</td>
<td>32,000</td>
</tr>
<tr>
<td>Maximum # of IP interfaces per system</td>
<td>NA</td>
<td>128</td>
<td>256</td>
<td>1,000</td>
</tr>
<tr>
<td>Maximum # of VRF per node</td>
<td>NA</td>
<td>NA</td>
<td>32</td>
<td>128</td>
</tr>
<tr>
<td>Maximum # of I-BGP peers</td>
<td>NA</td>
<td>20</td>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td>Maximum # of E-BGP peers</td>
<td>NA</td>
<td>20</td>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td>Maximum # of BGP routes in HW</td>
<td>NA</td>
<td>1,500</td>
<td>4,000</td>
<td>32,000</td>
</tr>
<tr>
<td>Maximum # of RIB IN Routes</td>
<td>NA</td>
<td>2,000</td>
<td>50,000</td>
<td>100,000</td>
</tr>
<tr>
<td>Maximum # of RIB OUT Routes</td>
<td>NA</td>
<td>10,000</td>
<td>100,000</td>
<td>250,000</td>
</tr>
<tr>
<td>Maximum # of BGP Peer Group</td>
<td>NA</td>
<td>10</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Maximum # of UDLD enabled interfaces</td>
<td>60</td>
<td>60</td>
<td>64</td>
<td>384</td>
</tr>
<tr>
<td>Maximum # of PVLAN domain supported</td>
<td>NA</td>
<td>31</td>
<td>1,000</td>
<td>1,000</td>
</tr>
<tr>
<td></td>
<td>System A</td>
<td>System B</td>
<td>System C</td>
<td>System D</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>Maximum # of Secondary vlans per PVLAN supported</td>
<td>NA</td>
<td>24</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>Maximum # of primary vlans per PVLAN supported in promiscuous mode</td>
<td>NA</td>
<td>24</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>Sum total of all the rules across L2 Ingress ACLs</td>
<td>1300/2048 *</td>
<td>1300/2044*</td>
<td>508</td>
<td>16380</td>
</tr>
<tr>
<td>Sum total of all the rules across L2 Egress ACLs</td>
<td>NA</td>
<td>NA</td>
<td>124</td>
<td>6144</td>
</tr>
<tr>
<td>Sum total of all the rules across L3 Ingress ACLs</td>
<td>768</td>
<td>744</td>
<td>508</td>
<td>16352</td>
</tr>
<tr>
<td>Sum total of all the rules across L3 Egress ACLs</td>
<td>NA</td>
<td>NA</td>
<td>511</td>
<td>8190</td>
</tr>
<tr>
<td>Maximum # of primary vlans per PVLAN supported in promiscuous mode</td>
<td>NA</td>
<td>24</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>DHCP IP Helper Addresses per interface</td>
<td>NA</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>DHCP IP Helper Ve interfaces</td>
<td>NA</td>
<td>128</td>
<td>256</td>
<td>1,000</td>
</tr>
<tr>
<td>DHCP IP Helper physical ports</td>
<td>NA</td>
<td>60</td>
<td>60</td>
<td>384</td>
</tr>
</tbody>
</table>
*** Enabling 3500 VLANs in trunk mode on all the ports of the system might lead to system instability. Brocade recommends that “trunk mode VLAN all” should be restricted to a handful uplink ports or a set of selected ports where it is desirable to carry all the VLAN trunks.

- In Hybrid cluster environment (a cluster involving VDX87xx and VDX67xx), the scalability limits of the cluster is determined by the scalability limits of VDX6710/20/30. For instance, in such a fabric, the MAC scalability limit will be 30,000 in spite of VDX87xx’s capability to do 128,000 MAC addresses.

### VDX 6710/6720/6730 ACL Limitations:
- If mac-addresses are unique, 1300 L2 ACL rules can be applied, else 2048/2044 L2 ACL rules can be applied.
Only 54 AppType L2/L3 ACL rules (Ether-type, TCP/UDP Port numbers) can be applied at any instance.

These numbers are the aggregate count across the entire switch. The table assumes no other configurations, AMPP ACLs, L2 macs (for VDX 6710/6720/6730).

The numbers are quoted for best case scenarios. Actual number of ACL rules may vary depending upon the complexity of the ACL rules & number of forwarding ASICs in the platform.

SNMP support documentation changes
Starting with the NOS 4.0.0 release, the Network OS MIB Reference document is not updated. You can obtain the latest MIBs from the downloads area of MyBrocade site after logging in.

For information about SNMP support in Network Operating System (NOS) and how to use MIBs, refer to the Network OS Administrator’s Guide.

Obtaining the MIBs
You can download the Brocade-specific MIB files required for this release from the Downloads area of the MyBrocade site. To download the Brocade-specific MIBs from the Brocade Technical Support website, you must have a user name and password.

2. Login with your user name and password.
3. Click the downloads tab.
4. On the downloads tab, under Product Downloads, select All Operating Systems from the Download by list.
5. Select Network Operating System (NOS), and then navigate to the release.
6. Navigate to the link for the MIBs package and either open the file or save it to disk.

NOTE: Distribution of standard MIBs has been stopped. Download the required standard MIBs from the http://www.oidview.com or http://www.ietf.org websites.

Changes in MIBs and objects
This release introduces the following changes in MIBs and objects:

New MIBs

- SNMP-MPD-MIB: This standard MIB defines the objects for message processing and dispatching.
- SNMP-TARGET-MIB: This standard MIB defines MIB objects which provide mechanisms to remotely configure the parameters used by an SNMP entity for the generation of SNMP messages.
- SNMP-VIEW-BASED-ACM-MIB: This standard MIB defines the management information definitions for the View-based access control model for SNMP.

Updated MIBs

- Updated the BROCADE-PRODUCTS-MIB.mib with the following object identifier for vdx6740 switches.
New Traps

- **connUnitPortStatusChange**
  The SNMP trap that is generated when the GBIC is pulled in/out from the FC port slot in vdx6730 switches.

**SERVICE VF support for SNMP**

- SNMP does not support VLAN ID greater than 4K.
- For VLAN ID less than 4k, only the provisioned VLANs will be displayed

**User guides**

*List of Documents*

Refer to [www.brocade.com](http://www.brocade.com) or my.brocade.com for the latest versions of the

<table>
<thead>
<tr>
<th>Document Description</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brocade VDX 8770-8 Four-Post Flush and Recessed Mount Rack Kit Installation Procedure</td>
<td>VDX8770_8_FourPostFlushRecessRailKit.pdf</td>
</tr>
<tr>
<td>Brocade VDX 8770-8 Two-Post Flush and Mid-Mount Rack Kit Installation Procedure</td>
<td>VDX8770_8_TwoPostMidMountRackKit.pdf</td>
</tr>
<tr>
<td>Brocade VDX 8770-4 Four-Post Flush Mount Rack Kit Installation Procedure</td>
<td>VDX8770_4_FourPostFlushMountRackKit.pdf</td>
</tr>
<tr>
<td>Brocade VDX 8770-4 Two-Post Flush and Mid-Mount Rack Kit Installation Procedure</td>
<td>VDX8770_4_TwoPostMidMountRackKit.pdf</td>
</tr>
<tr>
<td>Brocade VDX 8770-4 Four-Post Flush and Recessed Mount Intake Air Duct Rack Kit</td>
<td>VDX8770_4_IntakeDuctRackKit.pdf</td>
</tr>
<tr>
<td>Installation Procedure</td>
<td></td>
</tr>
<tr>
<td>Network OS YANG Reference Manual, 4.1.1</td>
<td>NOS_YangRef_v411.pdf</td>
</tr>
<tr>
<td>Network OS Administrator's Guide 4.1.1</td>
<td>NOS_AdminGuide_v411.pdf</td>
</tr>
</tbody>
</table>
**Reporting errors in the guides**

Send an email to documentation@brocade.com to report errors in the user guides.

**Contacting Brocade**

**Support**

Contact your switch supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information immediately available:

- Technical Support contract number, if applicable
- Switch model
- Switch operating system version
- Error numbers and messages received
- Detailed description of the problem, including the switch or network behavior immediately following the problem, and specific questions
- Description of any troubleshooting steps already performed and the results
- Switch Serial Number

To contact Brocade, go to http://www.brocade.com/services-support/index.page for the latest e-mail and telephone contact information.

1. **General Information**

- Switch model
- Switch operating system version
- Error numbers and messages received
- Provide support data collection output with the ‘copy support’ command
- Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
- Description of any troubleshooting steps already performed and the results
- Serial console and Telnet session logs
- Syslog message logs

2. **Switch Serial Number**

   The switch serial number and corresponding bar code are provided on the serial number label as illustrated below:

   ![Serial Number Label](image)

   The serial number and barcode label is located on the switch ID pull-out tab located on the bottom of the port side of the switch.

3. **License Identifier (License ID)**

   There is only one License Identifier associated with a physical switch. This License Identifier is required as part of the ordering process for new NOS licenses.

   Use the `show license id` command to display the License Identifier.

   If you cannot use the `show license id` command because the switch is inoperable, you can get the WWN from the same place as the serial number.

**Defects**

**TSBs - Critical Issues to Consider Prior to Installing This NOS Release**

Technical Support Bulletins (TSBs) are produced to provide detailed information about high priority defects or issues present in NOS releases. The following sections specify all current TSBs that have been identified as being a risk to or resolved with this specific version of Brocade Network OS. Please review carefully and refer to the complete TSB for relevant issues prior to migrating to this version of code. TSBs can be found at [http://my.brocade.com](http://my.brocade.com) under the “Technical Documentation” section of the “documentation” tab (note that TSBs are generated for all Brocade platforms and products, so not all TSBs apply to NOS-based platforms).
**TSB Issues Outstanding in Network OS v4.1.1**

Issues in the following list of TSBs are known to be potential risks to using Network OS v4.1.0 and v4.1.1 and should be considered carefully prior to using this release of code:

None

**TSB Issues Outstanding in Network OS v4.1.0**

Issues in the following list of TSBs are known to be potential risks to using Network OS v4.0.1 and v4.1.0 and should be considered carefully prior to using this release of code:

None
## Software Fixes

### Closed with Code Change in Network OS v4.1.1

This section lists the defects with Critical, High, and Medium Technical Severity closed with a code change as of March 17, 2014 in Network OS v4.1.1.

<table>
<thead>
<tr>
<th>Defect ID</th>
<th>Technical Severity</th>
<th>Probability</th>
<th>Product</th>
<th>Technology</th>
<th>Reported In Release</th>
<th>Technology Area</th>
<th>Closed In Release(s)</th>
<th>Symptom</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFECT000476976</td>
<td>Medium</td>
<td>Medium</td>
<td>NOS</td>
<td>Monitoring/RAS</td>
<td>NOS4.0.0</td>
<td>Syslog</td>
<td>NOS4.1.1(Fixed)</td>
<td>In logical chassis cluster mode, a VDX8770 will sometimes send syslog messages from its management interface address and sometimes from its chassis virtual-ip address.</td>
<td>Observed after doing HA failover.</td>
</tr>
<tr>
<td>DEFECT000477018</td>
<td>Medium</td>
<td>Medium</td>
<td>NOS</td>
<td>Layer 2</td>
<td>NOS4.0.0</td>
<td>VLAG</td>
<td>NOS4.1.1(Fixed)</td>
<td>If LAG between the 2 VDXs is shutdown, &quot;show span brief&quot; command will show path cost of Infinity (20,000,000), which is normal. However, occasionally, when LAG is re-enabled, the path-cost may stay at Infinity, instead of going back to actual value.</td>
<td>LAG is toggled and 'show span brief' used to check path cost.</td>
</tr>
<tr>
<td>DEFECT000477723</td>
<td>High</td>
<td></td>
<td>NOS</td>
<td>Layer 2</td>
<td>NOS3.0.1</td>
<td>Edge Loop Detection</td>
<td>NOS4.1.1(Fixed)</td>
<td>Unexpected reboot on one of the Layer 2 protocol modules.</td>
<td>Unexpected reload is due to exceeding the limit of ELD instances. Workaround: Avoid enabling the ELD instances on more than the max. limit.</td>
</tr>
<tr>
<td>DEFECT000481666</td>
<td>Medium</td>
<td></td>
<td>NOS</td>
<td>Other</td>
<td>NOS4.0.1</td>
<td>Other</td>
<td>NOS4.1.1(Fixed)</td>
<td>Ping &quot;timeout&quot; option in the ping command sets the timeout after a set amount of time regardless of conditions. It needs to specify timeout of pings between transmissions.</td>
<td>When ping issues with &quot;timeout&quot; option.</td>
</tr>
</tbody>
</table>
**Defect ID:** DEFECT000481813  
**Technical Severity:** High  
**Product:** NOS  
**Reported In Release:** NOS4.1.0  
**Closed In Release(s):** NOS4.1.1(Fixed)  
**Symptom:** Under certain conditions, GVLAN creation and CTAG classification addition on a port on VDX-6740 may fail.  
**Condition:** Occurs on VDX-6740, under high scale conditions, when VPN TCAM table is full.  
**Workaround:** Avoid a high scale configuration with GVLAN.  
**Recovery:** Once the VPN TCAM table is full, no more GVLAN CTAG classification rules can be added. To add new classification rules, user has to remove existing configuration and apply the new configuration. User has to explicitly delete the provisioned VLANs.

**Defect ID:** DEFECT000481879  
**Technical Severity:** High  
**Product:** NOS  
**Reported In Release:** NOS4.1.0  
**Closed In Release(s):** NOS4.1.1(Fixed)  
**Symptom:** Profiled port will not become part of newly created vlan though it has 'switchport trunk allowed vlan all' in the default domain.  
**Condition:** Profiled port is part of default domain and domain has 'switchport trunk allowed vlan all' and a new VLAN is created.  
**Workaround:** Create the VLANs beforehand and then configure 'switchport trunk allowed vlan all' in the default domain.

**Defect ID:** DEFECT000482159  
**Technical Severity:** High  
**Product:** NOS  
**Reported In Release:** NOS4.1.0  
**Closed In Release(s):** NOS4.1.1(Fixed)  
**Symptom:** Device logins will be lost when the keepalive timeout is disabled and hafailover is done on VDX8770.  
**Condition:** If user disable FIP Keep Alive timeout and then perform a hafailover operation on VDX8770, then all FCoE login will be lost.  
**Workaround:** Enable the Keepalive timeout using the following command:  
VDX8770(config)# fcoe  
VDX8770(config-fcoe)# fabric-map default  
VDX8770(config-fcoe-fabric-map)# keep-alive timeout  
**Recovery:** The following is the recovery steps:  
1. Enable the Keepalive timeout using the following command:  
VDX8770(config)# fcoe  
VDX8770(config-fcoe)# fabric-map default  
VDX8770(config-fcoe-fabric-map)# keep-alive timeout  
2. shut/no shut on the interfaces where the FCOE devices are connected
<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000483636</th>
<th>Technical Severity:</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product:</td>
<td>NOS</td>
<td>Technology:</td>
<td>Layer 2</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.0.0</td>
<td>Technology Area:</td>
<td>FCoE</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
<td>Symptom:</td>
<td>Under certain conditions, the FCoE login though a LAG from a third party device may fail, when one of the LAG member interfaces fails DCBX negotiation.</td>
</tr>
<tr>
<td>Condition:</td>
<td>When one of the LAG member interfaces fail the DCBX negotiation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workarounds:</td>
<td>Configure FCoE on the LAG with the third party device only after confirming all LAG members are capable of completing DCBX negotiation successfully.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery:</td>
<td>Delete the FCoE configuration on the LAG at the third party device, wait for the LAG (all members) to come up, and then configure FCoE on the LAG at the third party device.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000486127</th>
<th>Technical Severity:</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product:</td>
<td>NOS</td>
<td>Technology:</td>
<td>Other</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.0.0</td>
<td>Technology Area:</td>
<td>Other</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
<td>Symptom:</td>
<td>Under certain conditions, the switch may exhibit a slow unexpected growth of memory.</td>
</tr>
<tr>
<td>Condition:</td>
<td>When interfaces are in disabled state.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workarounds:</td>
<td>Keep the interfaces in enabled state.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery:</td>
<td>To recover the lost memory, power-off the linecard &amp; then do a no shut &amp; shut for the disabled interfaces.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000486540</th>
<th>Technical Severity:</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product:</td>
<td>NOS</td>
<td>Probability:</td>
<td>Low</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.1.0</td>
<td>Technology:</td>
<td>Layer 2</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
<td>Symptom:</td>
<td>Provisioning of GVLAN or 801.q VLANs can fail if the forwarding entries are used up in ASIC. On the other hand, if the mac-address-table is full, new MAC addresses may not be learnt.</td>
</tr>
<tr>
<td>Condition:</td>
<td>More probable when Virtual Fabric (GVLAN or TVLAN) is configured on the switch.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workarounds:</td>
<td>User can check if there are enough resources available by issuing the following CLI command:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```plaintext
do show overlapping-vlan-resource usage

e.g.

sw0(conf-if-te-10/0/11)# do show overlapping-vlan-resource usage

Number of table entries used:0.02%(max 4028, used 1)
```

<p>| Recovery: | Re-configure a lower scale. |</p>
<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000487137</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>High</td>
</tr>
<tr>
<td>Probability:</td>
<td>Medium</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Technology:</td>
<td>Layer 2</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.1.0</td>
</tr>
<tr>
<td>Technology Area:</td>
<td>VLAG</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
</tr>
<tr>
<td>Symptom:</td>
<td>Under rare conditions, vLAG member interfaces may take around 4 minutes to come online after &quot;no shutdown&quot; of Port Channel.</td>
</tr>
<tr>
<td>Condition:</td>
<td>When VDX switch is connected to a third party switch, which reacts adversely to the Link Reset message sent on the link-up</td>
</tr>
<tr>
<td>Workaround:</td>
<td>The following hidden command should be executed in VDX switches on all member ports of the vLAG connected to the Third Party switches using &quot;unhide neighbor-discovery&quot; command:</td>
</tr>
<tr>
<td></td>
<td>&quot;fabric neighbor-discovery disable&quot;</td>
</tr>
<tr>
<td>Recovery:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000487365</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>Medium</td>
</tr>
<tr>
<td>Probability:</td>
<td>Low</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Technology:</td>
<td>Layer 3</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.1.0</td>
</tr>
<tr>
<td>Technology Area:</td>
<td>IP Route Management</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
</tr>
<tr>
<td>Symptom:</td>
<td>Non-user friendly error message logged when trying to configure an ip address to an fcoe port</td>
</tr>
<tr>
<td>Condition:</td>
<td>When configuring an invalid condition.</td>
</tr>
<tr>
<td>Recovery:</td>
<td>no change occurs, so no recovery needed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000487375</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>High</td>
</tr>
<tr>
<td>Probability:</td>
<td>Low</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Technology:</td>
<td>Security</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.0.1</td>
</tr>
<tr>
<td>Technology Area:</td>
<td>Port Security</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
</tr>
<tr>
<td>Symptom:</td>
<td>this is a new CLI. without this, customer cannot enable/disable the HTTP(s) service.</td>
</tr>
<tr>
<td>Condition:</td>
<td>this is a new JITC requirement</td>
</tr>
<tr>
<td>Recovery:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000487804</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>High</td>
</tr>
<tr>
<td>Probability:</td>
<td>Low</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Technology:</td>
<td>Layer 2</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.1.0</td>
</tr>
<tr>
<td>Technology Area:</td>
<td>MAC ACLs</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
</tr>
<tr>
<td>Symptom:</td>
<td>Under rare conditions, the MAC Address count among the VCS nodes in the fabric may remain inconsistent causing forwarding or flooding issues.</td>
</tr>
<tr>
<td>Condition:</td>
<td>When spanning-tree protocol (variant flavors) mode is changed or topology changes are introduced in the VCS fabric causing transitional loops.</td>
</tr>
<tr>
<td>Recovery:</td>
<td>Perform &quot;clear mac-address dynamic&quot; from NOSCLI to recover from the condition.</td>
</tr>
</tbody>
</table>
**Defect ID:** DEFECT000488008  
**Technical Severity:** High  
**Probability:** Medium  
**Product:** NOS  
**Technology:** Layer 2  
**Reported In Release:** NOS4.1.0  
**Technology Area:** VLAN  
**Closed In Release(s):** NOS4.1.1(Fixed)  
**Symptom:** Under certain rare scenarios, Primary link for a port-channel may not be selected with three 40G member ports in a VCS on VDX-6740. This would result in multicast traffic / unknown unicast / broadcast traffic to be dropped.  
**Condition:** Rarely, when all nodes are reloaded at the same time  
**Recovery:** Flap all the member links of the port-channel.

**Defect ID:** DEFECT000488040  
**Technical Severity:** High  
**Probability:** Low  
**Product:** NOS  
**Technology:** Monitoring/RAS  
**Reported In Release:** NOS4.1.0  
**Technology Area:** Copy Support  
**Closed In Release(s):** NOS4.1.1(Fixed)  
**Symptom:** Under high scale setup, the copy-support on 8770 may not complete when principal node of a logical chassis.  
**Condition:** Fully populated linecards on 8770 when acting as principal node.

**Defect ID:** DEFECT000489113  
**Technical Severity:** High  
**Probability:** Low  
**Product:** NOS  
**Technology:** Traffic Management  
**Reported In Release:** NOS4.1.0  
**Technology Area:** QoS - Quality of Service  
**Closed In Release(s):** NOS4.1.1(Fixed)  
**Symptom:** `show interface <int>` not showing the RED discard statistics in Tx direction. Also, "show qos red statistics interface <if>" is not showing RED stats for default RED profile.  
**Condition:** Traffic over subscription for egress interface.  
**Recovery:** Functionality is not impacted. Over subscribed packets are dropped on the egress interface as RED discards.

**Defect ID:** DEFECT000489118  
**Technical Severity:** High  
**Probability:** Low  
**Product:** NOS  
**Technology:** Other  
**Reported In Release:** NOS4.1.0  
**Technology Area:** Other  
**Closed In Release(s):** NOS4.1.1(Fixed)  
**Symptom:** After performing chassis disable/enable with breakout ports link toggles may be observed for a while.  
**Condition:** Configure breakout port and perform chassis disable, chassis enable.

**Defect ID:** DEFECT000489224  
**Technical Severity:** High  
**Probability:** Low  
**Product:** NOS  
**Technology:** Layer 2  
**Reported In Release:** NOS4.1.0  
**Technology Area:** VLAN  
**Closed In Release(s):** NOS4.1.1(Fixed)  
**Symptom:** Unexpected reload after executing "show overlapping-vlan-resource usage" on VDX8770  
**Condition:** Executing "show overlapping-vlan-resource usage" command repeatedly on VDX 8770 series switches.  
**Workaround:** Avoid using the CLI command "show overlapping-vlan-resource usage" on VDX 8770 series switches, where it is not applicable.
<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000489773</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>High</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.1.0</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
</tr>
<tr>
<td>Symptom:</td>
<td>User may experience traffic loss on a VE interface when PIM is disabled on that VE interface.</td>
</tr>
<tr>
<td>Condition:</td>
<td>When PIM is disabled on a VE interface</td>
</tr>
</tbody>
</table>
| Recovery: | Following options:  
- Shut/no shut on that VE interface.  
- Disable/Enable PIM on that VE interface.  
- User can delete the VE interface and configure again. |

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000490016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>High</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.1.0</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td></td>
</tr>
<tr>
<td>Symptom:</td>
<td>After shut/no shut of an ISL port &amp; when the other end is a VDX6740, the port may not join the Brocade Trunk</td>
</tr>
<tr>
<td>Condition:</td>
<td>When a VDX switch is connected to a VDX6740 and shut/no shut of the ISL link is issued</td>
</tr>
<tr>
<td>Recovery:</td>
<td>Re-try the command after a minute</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000490397</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>High</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.1.0</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td></td>
</tr>
<tr>
<td>Symptom:</td>
<td>Under certain rare conditions, when the switch undergoes reload after VCS ID is changed using the CLI, the NOS CLI may fail to instantiate.</td>
</tr>
<tr>
<td>Condition:</td>
<td>Can occur if switch goes for an unexpected reboot during VCS ID change instead of graceful reboot.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000490908</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>High</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.0.1</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
</tr>
<tr>
<td>Symptom:</td>
<td>Static MAC's for multicast mac addresses are not allowed, including L2 &amp; L3 Multicast Mac. Need to allow L2 multicast mac to be configured to interoperate with certain 3rd party devices using L2 multicast MAC for communications.</td>
</tr>
<tr>
<td>Condition:</td>
<td>Under all conditions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000491294</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>High</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.1.0</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
</tr>
<tr>
<td>Symptom:</td>
<td>If one side of a link is shutdown, &quot;show media interface&quot; command at the other side shows the error &quot;Pluggable Media not present&quot;.</td>
</tr>
<tr>
<td>Condition:</td>
<td>Happens only when one side of the link is shutdown.</td>
</tr>
<tr>
<td>Defect ID:</td>
<td>DEFECT000491327</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Technical Severity:</td>
<td>High</td>
</tr>
<tr>
<td>Probability:</td>
<td>Low</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Technology:</td>
<td>Traffic Management</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.1.0</td>
</tr>
<tr>
<td>Technology Area:</td>
<td>QoS - Quality of Service</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
</tr>
<tr>
<td>Symptom:</td>
<td>When QoS strict priority is enabled for multiple COS values, the priority for the COS values is not correctly followed. (eg. COS 4 traffic is given higher priority than COS 6).</td>
</tr>
<tr>
<td>Condition:</td>
<td>When strict priority queuing is enabled for multiple COS values.</td>
</tr>
<tr>
<td>Workaround:</td>
<td>Instead of per-port scheduler, configure the same on CEE map.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000493558</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>Medium</td>
</tr>
<tr>
<td>Probability:</td>
<td>Low</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Technology:</td>
<td>Layer 2</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS3.0.1</td>
</tr>
<tr>
<td>Technology Area:</td>
<td>VLAN</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
</tr>
<tr>
<td>Symptom:</td>
<td>Under certain conditions, a long vlan string in &quot;switchport trunk allowed vlan add&quot; command may fail to apply.</td>
</tr>
<tr>
<td>Condition:</td>
<td>When ASCII config is replayed during upgrade failure OR when startup-config is modified with an external copy command.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000493800</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>High</td>
</tr>
<tr>
<td>Probability:</td>
<td>Medium</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Technology:</td>
<td>Traffic Management</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.0.1</td>
</tr>
<tr>
<td>Technology Area:</td>
<td>Buffer Queue Management</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
</tr>
<tr>
<td>Symptom:</td>
<td>Enhancement to introduce Dynamic Buffering mechanism for VDX-6740.</td>
</tr>
<tr>
<td>Condition:</td>
<td>The buffering will be more useful during congestion scenarios.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000494429</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>High</td>
</tr>
<tr>
<td>Probability:</td>
<td>High</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Technology:</td>
<td>Layer 2</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.0.1</td>
</tr>
<tr>
<td>Technology Area:</td>
<td>IEEE 801.2w RSTP</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
</tr>
<tr>
<td>Symptom:</td>
<td>Under rare conditions of rapid link flapping of a vLAG member, the STP state may not converge correctly after the link state stabilizes, thus causing traffic-drops.</td>
</tr>
<tr>
<td>Condition:</td>
<td>When link members of vLAG are flapped alternately / rapidly.</td>
</tr>
<tr>
<td>Recovery:</td>
<td>Flapping the link again would re-initiate the STP convergence &amp; converge correctly.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000494729</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>Medium</td>
</tr>
<tr>
<td>Probability:</td>
<td>Low</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Technology:</td>
<td>Layer 2</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.0.0</td>
</tr>
<tr>
<td>Technology Area:</td>
<td>IEEE 802.1d STP</td>
</tr>
<tr>
<td>Closed In Release(s):</td>
<td>NOS4.1.1(Fixed)</td>
</tr>
<tr>
<td>Symptom:</td>
<td>Under rare conditions, during topology change, the spanning-tree may not converge for the native-vlan &amp; may continue to flap.</td>
</tr>
<tr>
<td>Condition:</td>
<td>While removing the member from a static LAG.</td>
</tr>
</tbody>
</table>
Known issues

Newly Open defects in Network OS v4.1.1

This section lists known defects newly found in NOS 4.1.1 with Critical, High, and Medium Technical Severity as of March 17, 2014.

**Defect ID:** DEFECT000474393  
**Technical Severity:** High  
**Product:** NOS  
**Reported In Release:** NOS4.1.0  
**Symptom:** In a PBR configuration with 900 ARP traffic flows in a VDX6740, some of the traffic flows are not recovered after the reboot of the box.  
**Condition:** The problem happens when there are many ARP configurations along with PBR configurations.  
**Workaround:** clear arp no-refresh

**Technical Severity:** Low  
**Technology:** Layer 3  
**Technology Area:** IP Route Management

**Defect ID:** DEFECT000479287  
**Technical Severity:** High  
**Product:** NOS  
**Reported In Release:** NOS4.1.0  
**Symptom:** Under certain rare conditions, the pings to VRRP gateway from one of the nodes fail in the logical-chassis mode  
**Condition:** In logical chassis mode, when pinged from one of the TOR switches in the cluster  
**Recovery:** Clearing ARP with no-refresh should recover from the condition

**Technical Severity:** Low  
**Technology:** Layer 3  
**Technology Area:** VRRP & VRRP-E (IPv4)

**Defect ID:** DEFECT000481607  
**Technical Severity:** High  
**Product:** NOS  
**Reported In Release:** NOS4.1.0  
**Symptom:** ECMP does not utilize all equal cost links although 10G, 40G, 100G links have equal cost.  
**Condition:** Mixed bandwidth connections to another Rbridge, like 100G and 10G in parallel

**Technical Severity:** Low  
**Technology:** VCS  
**Technology Area:** TRILL

**Defect ID:** DEFECT000481972  
**Technical Severity:** High  
**Product:** NOS  
**Reported In Release:** NOS4.1.0  
**Symptom:** Metric and distance not set on OSPF routes installed in IP routing-table even though OSPF distribute-list route-map configuration has set-metric or set-distance clause.  
**Condition:** Metric and/or Distance set in Route-map and the Route-map is applied on OSPF distribute-list.  
**Workaround:** Configure desired cost on OSPF area-range or on OSPF interface

**Technical Severity:** Low  
**Technology:** Layer 3  
**Technology Area:** OSPF (IPv4)

**Defect ID:** DEFECT000486496  
**Technical Severity:** High  
**Product:** NOS  
**Reported In Release:** NOS4.1.0  
**Symptom:** Junk values for the vLAG counters could be observed if counters are cleaned followed by fail-over.  
**Condition:** After establishing vLAGs, clear all the counters and do fail-over.  
**Workaround:** Do not clean the counters before fail-over or else clear all counters after the fail-over.  
**Recovery:** Clear the counters, if junk values are seen.
<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000486748</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>High</td>
</tr>
<tr>
<td>Probability:</td>
<td>Medium</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Technology:</td>
<td>Management</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.1.0</td>
</tr>
<tr>
<td>Technology Area:</td>
<td>DHCP (IPv4)</td>
</tr>
<tr>
<td>Symptom:</td>
<td>Changing IP from DHCP to static gets gateway-ip from old and not existing default route</td>
</tr>
<tr>
<td>Condition:</td>
<td>Changing IP from DHCP to static</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000487152</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>High</td>
</tr>
<tr>
<td>Probability:</td>
<td>Low</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Technology:</td>
<td>Layer 2</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.1.0</td>
</tr>
<tr>
<td>Technology Area:</td>
<td>VLAN</td>
</tr>
<tr>
<td>Symptom:</td>
<td>Spanning-tree related information of a GVLAN is not getting removed from the interface even after unconfiguring the GVLAN from that interface.</td>
</tr>
<tr>
<td>Condition:</td>
<td>Configuring spanning-tree edge port with GVLAN configured followed by unconfiguring the GVLAN.</td>
</tr>
<tr>
<td>Recovery:</td>
<td>Use “no spanning-tree vlan xx” command for unconfiguring the spanning-tree related features enabled for a GVLAN after unconfiguring GVLAN from the interface.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000487654</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>Medium</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Technology:</td>
<td>Management</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.0.1</td>
</tr>
<tr>
<td>Technology Area:</td>
<td>VMWare</td>
</tr>
<tr>
<td>Symptom:</td>
<td>Port-profiles configured prior to upgrade to 4.x.x will not be present after the upgrade. Connection to vCenter might get lost. Additionally if manual discovery is triggered, automated discovery may not initiate at set interval.</td>
</tr>
<tr>
<td>Condition:</td>
<td>Upgrade from 3.0.1b to 4.0.1 with vCenter config present.</td>
</tr>
<tr>
<td>Workaround:</td>
<td>Its advisable to remove vCenter config in 3.0.1b prior to an upgrade to 4.x.x. If this is not followed and this issue is encountered then remove the vCenter config and re-configure.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000489103</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>High</td>
</tr>
<tr>
<td>Probability:</td>
<td>Low</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Technology:</td>
<td>Layer 2</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.1.0</td>
</tr>
<tr>
<td>Technology Area:</td>
<td>FCoE</td>
</tr>
</tbody>
</table>
| Symptom: | Message on console:  
  “Standby, CRITICAL, VDX8770-4, FSS Error on service component [ethsw1:fcoek]: sync-failure: -999” may be seen |
| Condition: | 1. Change FKA timer from 8 sec to 250 ms  
2. Immediately do "no fcoeport" and "fcoeport default" on the lag |
<p>| Workaround: | Customer should not change any fcoe provisioning on any interface, during the transition duration of FKA timer. Transition duration is 5 times the bigger FKA timer starting immediately after changing the FKA timer in VCS. |
| Recovery: | Oce the issue is seen, do ha synctop, ha synccstart. |</p>
<table>
<thead>
<tr>
<th>Defect ID: DEFECT000490150</th>
<th>Technical Severity: High</th>
<th>Probability: Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product: NOS</td>
<td>Technology: Management</td>
<td></td>
</tr>
<tr>
<td>Reported In Release: NOS4.1.0</td>
<td>Technology Area: Switch Management</td>
<td></td>
</tr>
<tr>
<td>Symptom:</td>
<td>Under certain scaled conditions, switch may become less responsive to user initiated commands, even when CPU utilization is not above 50%.</td>
<td></td>
</tr>
<tr>
<td>Condition:</td>
<td>Heavy BNA polling will cause switch to be less responsive to CLI commands</td>
<td></td>
</tr>
<tr>
<td>Recovery:</td>
<td>Reduce BNA polling rate.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID: DEFECT000491296</th>
<th>Technical Severity: High</th>
<th>Probability: Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product: NOS</td>
<td>Technology: Layer 2</td>
<td></td>
</tr>
<tr>
<td>Reported In Release: NOS4.1.0</td>
<td>Technology Area: FCoE</td>
<td></td>
</tr>
<tr>
<td>Symptom:</td>
<td>Under rare conditions, powering OFF &amp; ON the faulty linecard may result into an unexpected system reboot.</td>
<td></td>
</tr>
<tr>
<td>Condition:</td>
<td>Power cycling faulted linecard.</td>
<td></td>
</tr>
<tr>
<td>Recovery:</td>
<td>Power cycle switch to recover faulty line cards.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID: DEFECT000491426</th>
<th>Technical Severity: High</th>
<th>Probability: Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product: NOS</td>
<td>Technology: Layer 2</td>
<td></td>
</tr>
<tr>
<td>Reported In Release: NOS4.1.0</td>
<td>Technology Area: FCoE</td>
<td></td>
</tr>
<tr>
<td>Symptom:</td>
<td>FSB's from certain vendors may not be able to login into VDX 8770. Error message would be reported on console.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This issue is not seen on VDX 67XX platform.</td>
<td></td>
</tr>
<tr>
<td>Condition:</td>
<td>When using FSB from certain vendors</td>
<td></td>
</tr>
<tr>
<td>Workaround:</td>
<td>The issue can be avoided by enforcing dot1q tagging for frames from those FSB's. The native VLAN on both the FSB interface and the VDX 8770 interface would need to be set to anything other than 1.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID: DEFECT000492785</th>
<th>Technical Severity: High</th>
<th>Probability: Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product: NOS</td>
<td>Technology: Layer 2</td>
<td></td>
</tr>
<tr>
<td>Reported In Release: NOS4.1.0</td>
<td>Technology Area: IEEE 802.1d STP</td>
<td></td>
</tr>
<tr>
<td>Symptom:</td>
<td>Occasionally, spanning shutdown on VLAN mode may fail internally, when <code>spanning-tree shutdown</code> command is done inside VLAN range command mode.</td>
<td></td>
</tr>
<tr>
<td>Condition:</td>
<td>This issue can happen, when spanning-tree shutdown command is done immediately after entering the range mode.</td>
<td></td>
</tr>
<tr>
<td>Workaround:</td>
<td>Have a minor delay in the spanning-tree shutdown/no shutdown after entering the range command mode</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID: DEFECT000493432</th>
<th>Technical Severity: High</th>
<th>Probability: Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product: NOS</td>
<td>Technology: Management</td>
<td></td>
</tr>
<tr>
<td>Reported In Release: NOS4.1.1</td>
<td>Technology Area: Managing User Accounts</td>
<td></td>
</tr>
<tr>
<td>Symptom:</td>
<td>Accounts may not expire.</td>
<td></td>
</tr>
<tr>
<td>Condition:</td>
<td>Issue occurs when configuration of expiration of user account (&quot;expire&quot; attribute of username CLI) is preceded by &quot;password-attributes&quot; CLI.</td>
<td></td>
</tr>
<tr>
<td>Workaround:</td>
<td>1. &quot;no password-attribute&quot; CLI to reset configured parameters to default values.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Configure expire with &quot;username&quot; CLI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Revert step 1 using &quot;password-attribute&quot; CLI.</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Reported In Release: NOS4.1.0</td>
<td>Technology Area: VLAN</td>
<td>Symptom: When certain Third Party storage arrays are connected to a VDX switch, the iSCSI ports are not working and login fails.</td>
</tr>
<tr>
<td>Condition: Interoperating with certain Third Party storage devices with VDX switches using iSCSI protocol.</td>
<td>Workaround: Configure “cee default” on the switch ports connected to the Third Party storage device iSCSI ports.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported In Release: NOS4.0.1</td>
<td>Technology Area: VLAG</td>
<td>Symptom: Traffic will flood for a moment when it is flowing on primary link only and it is shut. There will be momentary flooding before another link becomes primary.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condition: Traffic is flowing on primary link only and it is shut.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported In Release: NOS4.1.1</td>
<td>Technology Area: TRILL</td>
<td>Symptom: Switch in cluster shows online locally but offline in all other switches of the cluster</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condition: This issue happens only when the cluster is upgraded from 4.0.1b to 4.1.1 with logical chassis configured.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported In Release: NOS4.1.1</td>
<td>Technology Area: VLAN</td>
<td>Symptom: On toggling the global knob 'vlan dot1q tag native' the native gvlans are also taking the effect and their tagging properties are also changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condition: global - no vlan dot1 tag native local - sw trunk tag native</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All the native gvlans on all ports accept untagged and native-tagged and send out tagged packets now.

**Workaround:**
1) Keeping the global knob '[no] vlan dot1 tag native' and local interface knob '[no] sw trunk tag native' same should solve the issue for gvlans.
2) Keep the global knob as 'vlan dot1q tag native' and toggle the interface knob alone '[no] sw trunk tag native' as desired should also solve the issue.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported In Release: NOS4.1.1</td>
<td>Technology Area: VLAN</td>
<td>Symptom: Adding/deleting ctag on a port repeatedly may result in the configuration failure.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condition: Repeated add/delete command for ctag.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defect ID</td>
<td>DEFECT000495151</td>
<td>Technical Severity: Medium</td>
<td>Probability: Medium</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>----------------------------</td>
<td>-------------------</td>
<td></td>
</tr>
<tr>
<td>Product</td>
<td>NOS</td>
<td></td>
<td>Technology: Traffic Management</td>
<td></td>
</tr>
<tr>
<td>Reported In Release</td>
<td>NOS4.0.1</td>
<td></td>
<td>Technology Area: Buffer Queue Management</td>
<td></td>
</tr>
<tr>
<td>Symptom</td>
<td>Under certain conditions, VDX 6740 may send FFC pause frames on a wrong COS value.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condition</td>
<td>When PFC is enabled.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID</th>
<th>DEFECT000495266</th>
<th>Technical Severity: High</th>
<th>Probability: Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>NOS</td>
<td></td>
<td>Technology: Management</td>
</tr>
<tr>
<td>Reported In Release</td>
<td>NOS4.1.1</td>
<td></td>
<td>Technology Area: NetCONF</td>
</tr>
<tr>
<td>Symptom</td>
<td>Netconf session is not logged out when the user account is disabled in the same session.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condition</td>
<td>Issue seen only with netconf interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery</td>
<td>Disconnect existing netconf session. Subsequent login attempt (via netconf) will fail.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID</th>
<th>DEFECT000495727</th>
<th>Technical Severity: High</th>
<th>Probability: Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>NOS</td>
<td></td>
<td>Technology: Layer 2</td>
</tr>
<tr>
<td>Reported In Release</td>
<td>NOS4.1.1</td>
<td></td>
<td>Technology Area: VLAN</td>
</tr>
<tr>
<td>Symptom</td>
<td>When attempting ISSU between NOS4.1.0 release to NOS4.1.1 release with large number of AMPP Profiles and VLANs (256 profiles and 3k VLANs), switch will run out of memory and will crash.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condition</td>
<td>ISSU is attempted with large number of AMPP Profiles and VLANs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workaround</td>
<td>Scale limit AMPP profiles and number of VLANs.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID</th>
<th>DEFECT000495842</th>
<th>Technical Severity: High</th>
<th>Probability: Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>NOS</td>
<td></td>
<td>Technology: Monitoring/RAS</td>
</tr>
<tr>
<td>Reported In Release</td>
<td>NOS4.1.1</td>
<td></td>
<td>Technology Area: Copy Support</td>
</tr>
<tr>
<td>Symptom</td>
<td>In some instances, copy support may timeout and fail to collect the supportsave.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condition</td>
<td>When switch is fairly busy servicing several Northbound requests, triggering supportsave can fail with timeout error.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workaround</td>
<td>Check if BNA is polling the cluster/switch disable it and retry.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defect ID</th>
<th>DEFECT000495886</th>
<th>Technical Severity: High</th>
<th>Probability: Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>NOS</td>
<td></td>
<td>Technology: Other</td>
</tr>
<tr>
<td>Reported In Release</td>
<td>NOS4.1.1</td>
<td></td>
<td>Technology Area: Other</td>
</tr>
<tr>
<td>Symptom</td>
<td>Number of fcoe interfaces in plugin do not match the fcoe-enodes config and number of interfaces in fcoe backend</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condition</td>
<td>This is seen in a specific scenario</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. In MC mode, fcoe-enodes is configured to a non-default higher value</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. A node is segmented and joins back with default config</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. The mismatch is seen only on the node which joined back</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery</td>
<td>Configure fcoe-enodes to 1000 and then back to 64. This resolves the issue.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Defect ID:** DEFECT000495988  
**Technical Severity:** High  
**Product:** NOS  
**Reported In Release:** NOS4.1.1  
**Technology Area:** VLAN  
**Symptom:** Failure to handle large VLAN ranges during VLAN delete operations results in the following possible errors:  
1. "application communication failure"  
2. "internal error"  
3. "time-out" errors  
**Condition:** As the VLAN delete operation is involved in cleaning up other related configurations as well, it takes lot of time in completing the delete operation. When this is performed for a large range of VLANs, the operation times out and results in errors like "application communication failure" or "internal error".  
**Workaround:** Delete the VLANs in smaller chunks of 500 or less instead of deleting all the VLANs in the system at one time.

**Defect ID:** DEFECT000496616  
**Technical Severity:** High  
**Product:** NOS  
**Reported In Release:** NOS4.1.1  
**Technology Area:** Firmware Upgrade/ Downgrade  
**Symptom:** Occasional Software Verify error during firmware upgrade.  
VERIFY - Failed: 0 && "ble_store_copy_upd can't find obj",  
file = chassis_ha.c, line = 1099, kernel mode  
args = 2073381592  
**Condition:** Firmware upgrade to 4.1.1 release.

**Defect ID:** DEFECT000496692  
**Technical Severity:** High  
**Product:** NOS  
**Reported In Release:** NOS4.1.1  
**Technology Area:** VLAN  
**Symptom:** Configuring Private VLAN for 8191 may erroneously apply to VLAN 4096 as well.  
**Condition:** Enabling Virtual Fabric and configuring Private VLAN for VLAN tag 8191.  
**Workaround:** Avoid using VLAN 8191 for configuring Private VLAN.

**Defect ID:** DEFECT000496727  
**Technical Severity:** High  
**Product:** NOS  
**Reported In Release:** NOS4.1.1  
**Technology Area:** VLAN  
**Symptom:** Secondary vlans may not associate with primary vlan.  
**Condition:** In some scenarios, secondary vlans are allowed to associate with Isolated VLANs which is not desirable behavior  
**Workaround:** Ensure that type of vlan being associated to Secondary vlans is indeed the primary vlan.

**Defect ID:** DEFECT000496945  
**Technical Severity:** High  
**Product:** NOS  
**Reported In Release:** NOS4.1.1  
**Technology Area:** Fabric Build  
**Symptom:** When switch configurations are restored to default configuration by executing "copy default to start", 40G port breakout settings are lost. Breakout settings have to be applied again which requires one more switch reboot.  
**Condition:** Default configurations are applied using copy default to start CLI.  
**Recovery:** Reapply the breakout configuration.
**Defect ID:** DEFECT000497104  
**Technical Severity:** High  
**Probability:** Medium  
**Product:** NOS  
**Technology:** Management  
**Reported In Release:** NOS4.1.1  
**Technology Area:** Firmware Upgrade/ Downgrade  
**Symptom:** The below errors are introduced during firmware downgrade from nos4.1.1 to nos4.1.0:

1. port-profiles which do not belong to "default" port-profile-domain, will get added to the "default" port-profile-domain.

2. If the "UpgradedVlanProfile" has "switchport trunk allowed vlan all" config, the same will be lost.

**Condition:** During firmware upgrade from nos4.0.1 to nos4.1.0, as per the design, all the port-profiles get added to the "default" port-profile-domain.

During firmware downgrade from nos4.1.1 to nos4.1.0 also, all the port-profiles get added to the "default" port-profile-domain incorrectly.

**Recovery:** After firmware downgrade from nos4.1.1 to nos4.1.0:

1. Please remove all the un-necessary port-profiles which got added to the "default" port-profile-domain, during firmware downgrade.

2. Configure "switchport trunk allowed vlan all" under "UpgradedVlanProfile", if the same is lost during firmware downgrade.

---

**Defect ID:** DEFECT000497360  
**Technical Severity:** High  
**Probability:** Medium  
**Product:** NOS  
**Technology:** Management  
**Reported In Release:** NOS4.1.1  
**Technology Area:** Switch Management  
**Symptom:** Even though "show virtual fabric status" shows fabric as virtual fabric capable, user may not be able to enable virtual fabric by executing "vcs virtual-fabric enable" CLI.

**Condition:** virtual fabric non capable nodes such as VDX 6720 are in offline state and are still part of the cluster.

**Workaround:** remove virtual fabric non capable nodes from the cluster by executing "no vcs enable rbridge-id <id>" command.

---

**Defect ID:** DEFECT000497425  
**Technical Severity:** High  
**Probability:** Medium  
**Product:** NOS  
**Technology:** Layer 2  
**Reported In Release:** NOS4.1.1  
**Technology Area:** VLAN  
**Symptom:** On a Virtual fabric enabled switch, VLAN Tagged IGMP membership reports will be learnt on port configured as untagged.

**Condition:**
1) Enabling Virtual Fabric
2) Enabling IGMP Snooping
3) Configuring port as untagged using "switchport mode trunk-no-default-native" and "native-vlan-untagged" CLI.
Defect ID: DEFECT000497649
Technical Severity: High
Product: NOS
Technology: Layer 2
Reported In Release: NOS4.1.1
Technology Area: VLAN
Symptom: LC cluster disturbance when configuring transparent VLAN
Condition: This will be observed only when VDX 6740 and VDX 8770-4 are present in LC cluster and VDX 6740 port 0/25 is configured for TVLAN.
Workaround: Use any other port in VDX6740.
Recovery: Reboot the LC cluster.

Defect ID: DEFECT000498001
Technical Severity: High
Product: NOS
Technology: Layer 2
Reported In Release: NOS4.1.1
Technology Area: VLAN
Symptom: With Virtual Fabric enabled mode, if ctag list is greater than 1023, then the configuration is not applied, but it can be seen in "show running config" command.
Condition: If the user tries to configure ctag list greater than 1023 on Virtual Fabric enabled switch.

Defect ID: DEFECT000498238
Technical Severity: Medium
Product: NOS
Technology: Other
Reported In Release: NOS4.1.1
Technology Area: Other
Symptom: When using the command "show overlay-gateway name <name> vlan statistics" for debugging overlay-gateway VLANs, VLANs may be displayed as “Err” for TX instead of "-".
Condition: When VLANs exceed 256 for RX or 116 for TX.

Defect ID: DEFECT000498331
Technical Severity: High
Product: NOS
Technology: Traffic Management
Reported In Release: NOS4.1.1
Technology Area: QoS - Quality of Service
Symptom: Cli command: "show qos tx-queue int te 500/15"
Field "MaxBytes" shows as ",-"
Condition: During of testing of Lossless traffic drops, cli show command displays a problem.

Defect ID: DEFECT000498510
Technical Severity: High
Product: NOS
Technology: Layer 2
Reported In Release: NOS4.1.1
Technology Area: VLAN
Symptom: In rare circumstances, when a dvSwitch is created along with dvPg on the vCenter, in addition to the proper auto-port-profiles created on the switch, some incorrect auto port-profile names (excludes datacenter name in the auto port-profile) may also get created.
Condition: The issue was observed while creating a dvSwitch along with dvPg using a automated script.
Workaroud: Create dvSwitch first and then create dvPg.
Recovery: After this dvswitch with dvpGs add event, when incorrect port-profiles are created perform the following:
1) Run manual discovery (vnetwork vcenter <vCenter-name> discovery) or wait for next discovery run.
2) Run “vnetwork reconcile vcenter <vCenter-name>” command.
This will remove all incorrect additional auto-port-profiles from the switch.
<table>
<thead>
<tr>
<th>Defect ID:</th>
<th>DEFECT000496011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Severity:</td>
<td>Medium</td>
</tr>
<tr>
<td>Probability:</td>
<td>Medium</td>
</tr>
<tr>
<td>Product:</td>
<td>NOS</td>
</tr>
<tr>
<td>Technology:</td>
<td>Layer 2</td>
</tr>
<tr>
<td>Reported In Release:</td>
<td>NOS4.1.1</td>
</tr>
<tr>
<td>Technology Area:</td>
<td>Edge Loop Detection</td>
</tr>
</tbody>
</table>

**Symptom:** Detection of a loop will result in inconsistency of MAC in the system. Presence and detection of other loops may aggravate the problem substantially.

Command to remove MAC(s) at the fabric-level exists, but it needs to be issued by system administrator. That is, fabric-wise flushing of MAC(s) does not happen automatically for relevant interfaces.

(no) mac-refresh <60...300> <allports> is non-operational

**Condition:** If two interfaces are present in a layer-2 loop, same set of MACs are learnt on both of them. When ELD detects the layer-2 loop, it puts the participating interface into operationally down state. Consequently, MACs learnt on that particular interface gets flushed. However, the same MACs will be present at the interface at the other end of the (already detected) loop. MAC(s) learnt on one interface will be learnt on the other since they are in the same VLAN. ELD, if enabled at both the ends of the loop, will detect and break the loop. L2sys will subsequently issue a flush command to remove MAC(s) learnt on that interface which was just brought down by ELD. However, L2sys will not remove MAC(s) learnt on the same VLAN at the other end of the erstwhile loop.

Presence and detection of other loops may aggravate the problem substantially.

**Recovery:** "clear mac-address-table dynamic" and can bring the system to a clean state