



**DATA CENTER**

# **Brocade VDX Deployment Guide Addendum for Edge Loop Detection**

**Brocade VCS Fabric Technology and Edge Loop Detection  
with Network OS 2.1.1**

**BROCADE**

## CONTENTS

<b>Introduction</b> .....	<b>3</b>
Purpose .....	3
Usage.....	4
Deployment.....	4
Representative VLAN .....	4
Redundancy .....	4
Topology.....	5
ELD Considerations .....	6
<b>Appendix A: Configurations</b> .....	<b>7</b>
Brocade VCS Fabric Configurations: ELD.....	7
Procedure to configure ELD global parameters:.....	7
Procedure to configure ELD on interfaces between VCS fabrics:.....	7
Procedure for checking ELD status on the configured interfaces:.....	9
Procedure to check ELD detected loop and shutdown redundant links:.....	10
Procedure to clear ELD on an RBridge:.....	11
Procedure to configure the ELD auto-enable function:.....	11
ELD Configuration for a VCS fabric to standalone node links: .....	11
<b>Glossary</b> .....	<b>12</b>
<b>Related Documents</b> .....	<b>12</b>
<b>About Brocade</b> .....	<b>13</b>

## INTRODUCTION

Edge Loop Detection (ELD) is a Brocade Layer 2 loop detection mechanism. It uses PDUs to detect loops in the network. This protocol is mainly intended for VCS to VCS loop prevention operation, but it can also be used in “VCS to standalone” mode.

Specifically, ELD can be used to prevent broadcast storms caused by loops in the following topologies:

- A Brocade VCS Fabric cluster connects to a standalone switch.
- A Brocade VCS Fabric cluster connects to a multiple node network.
- A Brocade VCS Fabric cluster connects to other Brocade VCS Fabric clusters.

The Brocade ELD feature is implemented to block redundant links between two VCS fabrics: When a device detects a loop by receiving packets originated from it, it should disable all redundant links in that network. This is to prevent packet storm creation due to loops caused by misconfiguration.

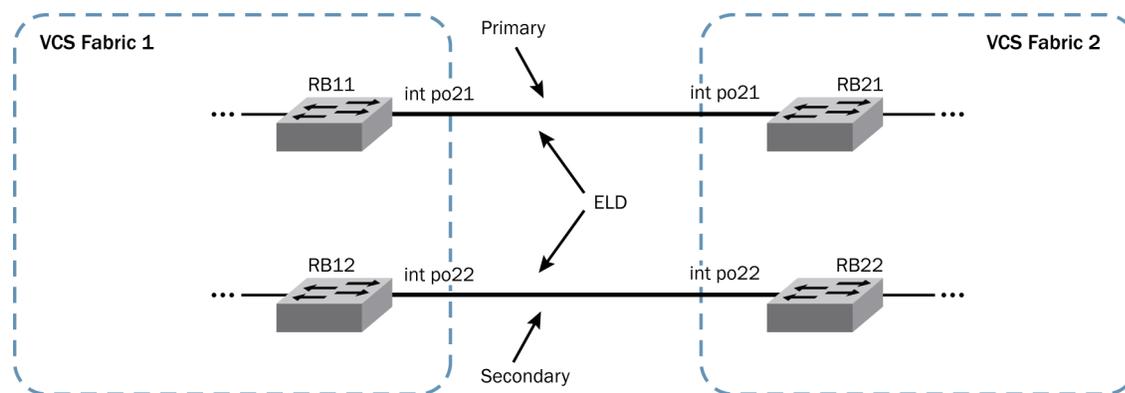
You should use ELD as a tool to detect any loop in the network, rather than using it to replace Layer 2 protocols such as xSTP, Metro Ring Protocol (MRP), and so forth.

The basic ELD functionality is as follows: ELD is enabled on a specific port and VLAN combination. Each ELD-enabled interface on an RBridge sends an ELD PDU. This PDU contains information about the VCS ID and RBridge ID of the node it is sending from, the VLAN associated with the interface on which ELD is enabled, ELD port priority parameters, and so on. ELD can be configured on access mode ports and trunk mode ports, and PDUs follow port configuration for tagging. The port priority parameter decides which port is shut down if ELD detects a loop. These PDUs are transmitted from every ELD-enabled interface at the configured “hello interval” rate. When these PDUs are received back at the originating VCS fabric, ELD detects a loop; this results in the shutdown of redundant interfaces based on the port priority parameter of the redundant links. If the port priority value is the same, then the decision is based on the port number.

ELD uses the system MAC address of the primary RBridge of the VCS fabric with the multicast (bit 8) and local (bit 7) on. For example, if the base MAC address of the primary RBridge of VCS is 00e0.5200.1800, then the destination MAC address will be 03e0.5200.1800.

### Purpose

You can connect several VCS fabrics and Layer 2 switches together using multiple links to provide redundancy. These redundant links create loops in the network. In a traditional Layer 2 network, spanning tree can be used to eliminate loops. However, spanning tree cannot eliminate loops between VCS fabrics. So ELD is introduced to eliminate the loops between the VCS fabrics. See Figure 1.



**Figure 1.** Using ELD to deploy redundant links between two VCS fabrics.

**NOTE:** For ELD to block redundant links, it should be enabled on all VCS-to-VCS links.

## Usage

The following are necessary considerations when you deploy ELD.

**Table 1.** ELD usage recommendations

Considerations	Recommended	Not recommended
Deployment	Configure on VCS-to-VCS links only	Enable on all links, including server-facing links
Redundancy	Primary/secondary	VLAN load balancing
Topology	Core-edge	Mesh

## Deployment

As shown in Figure 1, you should enable ELD only on links between Layer 2 switches (that is, VCS fabrics). Links that are not connected to another Layer 2 switch should not have ELD enabled.

Interfaces connected to hosts should not be enabled with ELD. ELD needs to be enabled on all interfaces before a loop forms and causes broadcast storms.

ELD functionality is supported only in VCS mode. It is disabled in standalone mode. If the connecting links are vLAGs, ELD should be enabled on the vLAG interface in all participating nodes.

ELD prevents loops between Brocade VDX switches within a VCS Fabric and non-VDX switches, for example, with Brocade VCS Fabric as an aggregation to core Cat 6K, Nexus, or Brocade MLX® routers.

**NOTE:** At any time ELD can be enabled on only one VLAN. In the case of trunk mode VLANs, only one tagged PDU is sent out for loop detection. If a loop exists in a trunk port with a different VLAN-ID, it *might not* be detected. This limitation is not applicable to native mode VLAN, where the loop is detected by enabling ELD on one VLAN only.

### Representative VLAN

The trunk ports connecting Layer 2 switches can carry many VLANs. It is recommended that all trunk ports that connect Layer 2 switches should allow all VLANs. ELD needs to be enabled on just one VLAN to represent all the VLANs that are being carried on the link. This is because ELD works at the VLAN level and takes action at the link level. Thus, on detecting a loop for a VLAN, ELD shuts down the whole interface.

**NOTE:** The number of ELD instances is defined by the number of VLANs times the number of ports that have ELD enabled. The maximum number of ELD instances for Network OS 2.1.1 is 256. ELD can be enabled on native VLAN, as well, and it functions in a similar way to normal VLAN.

### Redundancy

ELD provides redundancy when connecting several VCS fabrics and Layer 2 switches together using multiple links. This is accomplished by disabling redundant links that form one or more loops. For example, one link is active, while all other redundant links are in a shutdown state. In this scenario, all trunk ports that form these links should allow all VLANs.

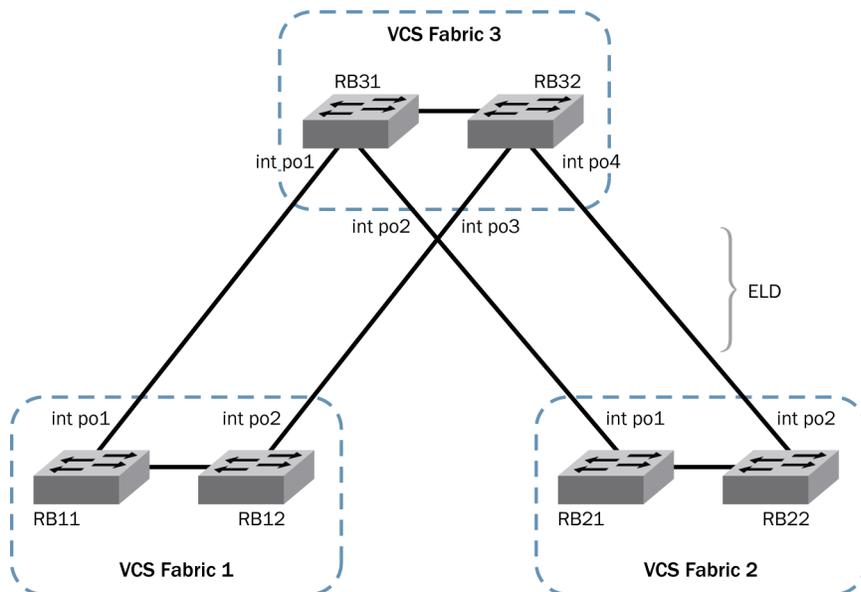
However, it is not recommended to have multiple links between switches while allowing only a subset of VLANs on each link to provide VLAN load balancing. ELD operates by disabling an entire port and/or a set of ports, which may or may not cause connectivity in some VLANs to break.

The ELD auto-enable feature—when used in conjunction with the ELD shutdown timer—can be set to allow failover to a redundant link when the primary link fails. The possible timer range is from 10 minutes to 1440 minutes (24

hours). The default value of the timer is 0, a value that indicates that ELD does not bring back the redundant link, even if the primary link fails.

### Topology

The recommended topology for using ELD is a core-edge topology. When using a partial-mesh or full-mesh topology, the ports that ELD might shut down are more unpredictable, and this might cause traffic disruption. When ELD is used in conjunction with spanning tree, a partial-mesh or full-mesh topology might cause issues with spanning tree operation. Use core-edge topology to avoid these issues. See Figure 2.



**Figure 2.** Using ELD in a core-edge topology with three VCS fabrics.

## ELD Considerations

**Table 2.** ELD Considerations

Considerations	Recommendation
ELD supports only up to 256 instances (as defined earlier in this document).	Brocade recommends staying within the 256 instance limit.
ELD is not able to block redundant links, if it is configured after a loop is created and there is a network storm by broadcast/multicast/unknown unicast frames.	Configure ELD before deployment. Before connecting two VCS fabrics, ELD needs to be enabled on interconnected links.
ELD does not block redundant links, if there is a unidirectional loop. This means that ELD PDUs are received in one direction but not in the other direction; for instance, this can be due to PDU discard in one direction.	Troubleshoot why ELD PDUs are not forwarded in both directions on the peer network.
ELD may block all interfaces from a VCS fabric, thus isolating the VCS fabric from the rest of the network, if there are loops somewhere in the upstream network.	Make sure that there are no other loops in the network at the location where the fabric under consideration is connecting.
There may be implications if an Access Control List (ACL) is applied at the receiving side to block packets coming from a particular MAC address. For example, if an ACL is matching with the ELD source MAC address, or there is a “deny all” rule, then these frames will be dropped as per the ACL rules.	Remove any ACL deny rules that match the source MAC address of an ELD-enabled interface, or deny any rule that is configured and applied at the interface.
When ELD is enabled on an interface on one side, its peer node learns the MAC address associated with that interface at the opposite side. For the peer node, these ELD PDUs are data packets, hence the MAC address learns from these packets. The MAC address table shows these MACs against the VLAN on which the ELD is enabled.	Note the MAC address of all ELD-enabled interfaces and associated RBridges.
After ELD shuts down redundant links, then when an active link goes down, ELD does not automatically enable one of the shut down links. The user has to issue a “clear edge-loop-detection” command to bring all the interfaces back to the active state and restart the ELD process.	Either enable ELD with the auto-enable feature, or watch for the active link failure and issue a “clear edge-loop-detection” command when the active link fails, so that it brings one of the interfaces online.
Using the ELD auto-enable feature or issuing the “clear edge-loop-detection” command creates a temporary loop in the network.	To solve the issue of the MAC address being out of sync, execute the “clear mac-address table” command. To clear a multicast issue, execute the “clear ip igmp groups” command.
The user should be familiar with all of the interfaces that connect the two VCS fabrics. There is no global command for enabling ELD on all interfaces.	Note all of the interfaces connecting the two VCS fabrics, and enable ELD on all these interfaces from one VCS fabric.
Temporary loops in the fabric may cause ELD PDUs to storm and have an impact on other network devices, such as Brocade MLX Series routers and FCX Series switches, and others.	Use the “clear edge-loop-detection” command in a maintenance time frame, and disable the ELD auto-enable feature.

## APPENDIX A: CONFIGURATIONS

### Brocade VCS Fabric Configurations: ELD

#### Procedure to configure ELD global parameters:

There are three ELD parameters that have global impact on the VCS node. They are called hello timer, shutdown timer, and pdu receive limit. The ELD hello timer is the frequency at which ELD PDUs are transmitted from an interface. Its value ranges from 100 msec to 5 sec, with a default value of 1 sec. The ELD shutdown timer is used for the auto-enable feature. Using the auto-enable feature, the earlier shutdown link can be brought online after the “shutdown time” minutes have elapsed, and the ELD process has restarted. In the presence of a loop, on receiving the pdu-rx-limit, ELD shuts down redundant links. The range for this parameter is from 1 to 5. The default value is 1.

These parameters are configured at the protocol edge-loop-detection configuration level. ELD global parameters can be retrieved using the Command Line Interface (CLI) command: **show edge-loop-detection globals**.

```
RB1#
RB1# conf
Entering configuration mode terminal
RB1(config)# protocol edge-loop-detection
RB1(config-eld)# hello-interval ?
Possible completions:
  <100-5000> Millisecond[1000]
RB1(config-eld)# shutdown-time ?
Possible completions:
  <0, 10-1440> Minute[0]
RB1(config-eld)# pdu-rx-limit ?
Possible completions:
  <1-5> Number[1]
RB1(config-eld)#
RB1(config-eld)# do show edge-loop-detection globals
```

Edge-loop-detection global configuration values are as below:

```
PDU receive limit (packets):    1
Shutdown-time (minutes):       0
Hello-time (msec):             1000
RB1(config-eld)#
```

#### Procedure to configure ELD on interfaces between VCS fabrics:

1. Identify all switchport interfaces connecting two VCS fabrics.
2. Enable ELD on the interfaces from one VCS fabric for a particular VLAN. There is no need to enable ELD on both of the VCS fabrics. The VLAN should be a common VLAN among all the links between these two VCS fabrics.
3. Retrieve and verify that the ELD parameters have default values.

```
RB1(config-Port-channel-21)# do show running-config interface Port-channel 21
interface Port-channel 21
  vlag ignore-split
  description 21
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
```

```
    switchport trunk tag native-vlan
    no shutdown
!
RB1(config-Port-channel-21)# do show running-config interface Port-channel 22
interface Port-channel 22
    vlag ignore-split
    description 22
    switchport
    switchport mode trunk
    switchport trunk allowed vlan all
    switchport trunk tag native-vlan
    no shutdown
!
RB1(config-Port-channel-21)# edge-loop-detection vlan 2000
RB1(config-Port-channel-21)# do show running-config interface Port-channel 21
interface Port-channel 21
    vlag ignore-split
    description 21
    switchport
    switchport mode trunk
    switchport trunk allowed vlan all
    switchport trunk tag native-vlan
    edge-loop-detection vlan 2000
    no shutdown
!
RB1(config-Port-channel-21)#int po 22
RB1(config-Port-channel-22) # edge-loop-detection vlan 2000
RB1(config-Port-channel-22)# do show running-config interface Port-channel 22
interface Port-channel 22
    vlag ignore-split
    description 22
    switchport
    switchport mode trunk
    switchport trunk allowed vlan all
    switchport trunk tag native-vlan
    edge-loop-detection vlan 2000
    no shutdown
```

Identify interfaces that should be shut down in case ELD detects a loop. ELD port priority decides which interface to shut down when it detects redundant links. Links with highest priority values are shut down, and links with lowest priority value remain active. If the priority values are the same for multiple interfaces, the decision is based on the interface number. The highest numbered interfaces are shut down, and the interfaces with the lowest number remain active. So you should configure ELD port priority based on which interfaces should be shut down or kept active.

**NOTE:** A port with priority 0 means that shutdown for this port is disabled. The default port priority value is 128.

Assume that there are two port-channel interfaces connecting two VCS fabrics: port-channel 21 and port-channel 22. To configure ELD, go to the individual interfaces and enable ELD for any one of the common VLANs.

If port-channels 21 and 22 are vLAGs, then the above steps should be repeated for these port-channels on all RBridges that are participating in those vLAGs.

Now both of these interfaces are configured for ELD to detect loops. This initiates ELD PDUs from interface port-channel 21 and interface port-channel 22 over VLAN 2000 and sends ELD PDUs at the “hello interval” time intervals. When ELD PDUs are sent from port-channel 21 and are received at interface port-channel 22, and vice versa, a loop is detected. ELD shuts down one of the interfaces based on priority or port number, when receiving the pdu-rx-limit number of the PDUs associated with the other interface/s. Here, since the port priority values are the same, shutdown is based on the port number.

4. The ELD port priority value can vary from 0 to 256, with 128 being the default value. Configure ELD port priority for an interface before configuring ELD on that interface.

```
RB1(config-Port-channel-21)# edge-loop-detection port-priority ?
Possible completions:
  <NUMBER:0-256>   Priority value
RB1(config-Port-channel-21)#
```

5. ELD can be enabled on Ten Gigabit Ethernet interfaces, Gigabit Ethernet interfaces, and port-channel interfaces.

### Procedure for checking ELD status on the configured interfaces:

To check whether ELD is enabled and is sending ELD PDUs, follow this procedure:

1. Retrieve the running configuration of the interfaces linking two VCS fabrics, and make sure that ELD provisioning is done on these interfaces.

```
RB1(conf-eld)# do show running-config interface Port-channel 21
interface Port-channel 21
  vlag ignore-split
  description 21
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
  switchport trunk tag native-vlan
  edge-loop-detection vlan 2000
  no shutdown
!
```

2. All online interfaces (state “up”) should be sending ELD PDUs periodically at the hello interval time. This can be verified by retrieving ELD status at the interface level, as shown here:

```
RB1(config-Port-channel-21)# do show edge-loop-detection interface port-channel 21
Number of eld instances: 1
Enabled on VLANs:      2000
Priority:              128
Interface status:     DOWN (due to eld on vlan 2000)
Auto enable in:      Never
Packet Statistics:
vlan      sent      rcvd
2000      1              1
RB1(config-Port-channel-21)#
```

**NOTE:** In the case of a LAG or vLAG, ELD PDUs are sent out on the active primary port of the LAG. The ELD protocol shuts down all the member ports of the LAG on the RBridge receiving the PDU. So, for a vLAG, the ELD PDU statistics are shown only on the RBridge that has the primary link for that port-channel.

- For all ELD-enabled interfaces, execute the command shown in step 2 above, ***show edge-loop-detection interface port-channel 21*** and ensure that the interfaces are able to send and receive ELD PDUs.

**NOTE:** In the above example, which is based on Figure 1, ELD is enabled on VCS cluster 1 on interfaces port-channels 21 and 22 on VLAN 2000. In this case, ELD PDUs use the interface MAC for VLAN 2000 as the source MAC address. These PDUs are treated as data packets at VCS 2, so these MAC addresses are learned at VCS 2 against these interfaces for VLAN 2000.

Example: if “***show interface port-channel 21***” on VCS 1 shows the current MAC address as 0005.1ecd.4b30, then “***show mac-address-table***” on VCS 2 shows this MAC address against this interface for the ELD-enabled VLAN 2000.

### Procedure to check ELD detected loop and shutdown redundant links:

Once ELD configuration is complete, and the interfaces are online, they start sending ELD PDUs. Upon reception of these PDUs back at the originating VCS fabric, some of the links will be shut down based on port priority value or the interface number. ELD operation can be verified to confirm that ELD has shutdown some of the interfaces using the “***show stats edge-loop-detection***” command at the Network OS command prompt, as shown below:

```
RB1# show edge-loop-detection rbridge-id 155
Number of edge-loop-detection instances enabled: 2
Interface: po21
-----
      Enabled on VLANs: 2000
      Priority:          128
      Interface status: UP
      Auto enable in: Never
Interface: po22
-----
      Enabled on VLANs: 2000
      Priority:          128
      Interface status: DOWN (due to eld on vlan 2000)
Auto enable in: Never
```

In this example, when comparing interface port-channels 21 and 22, one of them is redundant and needs to be shut down. Upon enabling ELD on these interfaces, ELD has shut down interface port-channel 22. Given that ELD port priority for interface port-channels 21 and 22 is the same, the interface with the higher interface number—in this case, port-channel 22—has been shut down.

The above command lists all ELD-enabled interfaces on the RBridge that the command is executed on—in this case, RB1. The command shows ELD link status for those interfaces, whether or not the interface status is UP or DOWN.

An ELD interface state of DOWN indicates that ELD detected a loop through this interface for VLAN 2000 and shut down the interface.

Upon detecting a loop in the network, ELD will place all redundant interfaces in a ‘line protocol down’ state, and will not modify the interface’s administrative state.

**Procedure to clear ELD on an RBridge:**

In case the active link fails, the earlier shutdown redundant link can be brought online by executing a “*clear edge-loop-detection*” command at the Network OS prompt. This command can also be used to restart the ELD process. ELD enables previously shut down links online and starts sending PDUs to detect loops.

```
RB1#
RB1# clear edge-loop-detection
RB1#
```

**NOTE:** When the “clear edge-loop-command” is executed, it brings back all links that were shut down by ELD on that RBridge. This creates a temporary loop in the network before ELD again detects loop and shutdown redundant links. This process may cause the MAC address table and the multicast forwarding table to become out of sync. One way to resolve this issue is by using “*clear mac-address dynamic*” and “*clear ip igmp groups*”.

**Procedure to configure the ELD auto-enable function:**

Please note that when using default ELD global parameters, once ELD shuts down redundant links they are shut down permanently. However, with the ELD auto-enable feature, you can bring shutdown links back online on elapsing the configured shutdown timer minutes. When the ELD shutdown timer is configured as 10, then ELD re-enables all the shutdown links once 10 minutes has elapsed after the shutdown time. ELD then restarts the loop detection process and shutdown redundant links on detection of loop.

```
RB1(config)# protocol edge-loop-detection
RB1(conf-eld)# shutdown-time ?
Possible completions:
  <0, 10-1440> Minute[0]
RB1(conf-eld)# shutdown-time 10
RB1(conf-eld)#
RB1(conf-eld)# do clear edge-loop-detection
RB1(conf-eld)#
RB1(conf-eld)# do show edge-loop-detection rbridge-id 155
Number of edge-loop-detection instances enabled: 2
Interface: po21
-----
      Enabled on VLANs: 2000
      Priority:         128
      Interface status: UP
      Auto enable in:  Never
Interface: po22
-----
      Enabled on VLANs: 2000
      Priority:         128
      Interface status: DOWN (due to eld on vlan 2000)
Auto enable in:      10 minutes to go
RB1(conf-eld)#
```

**ELD Configuration for a VCS fabric to standalone node links:**

ELD is mainly used for loop detection in a VCS fabric to VCS fabric links. However, ELD can also be used for loop detection between a VCS fabric and a standalone node. Usually xSTP is configured on the standalone node to detect any Layer 2 loops and block redundant links. ELD can be enabled on an xSTP enabled network. This procedure is not recommended, because there is little predictability in knowing whether ELD or xSTP will block redundant links in certain scenarios, such as after rebooting, switching the power cycle, and so forth.

## GLOSSARY

<b>BPDU</b>	Bridge Protocol Datagram Unit
<b>ELD</b>	Edge Loop Detection protocol. Used on the edge ports of a VCS fabric to detect and remove loops.
<b>MAC</b>	Media Access Control. In Ethernet, it refers to the 48-bit hardware address.
<b>PDU</b>	Protocol Datagram Unit
<b>RBridge</b>	Routing Bridge. A switch that runs the TRILL (Transparent Interconnection of Lots of Links) protocol.
<b>RSTP</b>	Rapid Spanning Tree Protocol. An IEEE standard for building a loop-free LAN (Local-Area Network), which allows ports to rapidly transition to forwarding state.
<b>VCS</b>	Virtual Cluster Switching. Brocade® VCS® Fabric technology is a method of grouping a fabric of switches together to form a single virtual switch that can provide a transparent bridging function.
<b>vLAG</b>	Virtual Logical Aggregation Group. You can create a LAG using multiple switches in a VCS fabric. vLAG provides better high availability and faster protection switching than a normal LAG.
<b>VLAN</b>	Virtual LAN. Subdividing a LAN into logical VLANs allows separation of traffic from different sources within the LAN.
<b>xSTP</b>	An abbreviation used in this document to indicate all types of Spanning Tree Protocol, for instance, STP, RSTP, MSTP (Multiple STP), PVST+ (Per VLAN Spanning Tree Plus), and RPVST+ (Rapid PVST+).

## RELATED DOCUMENTS

For more information about Brocade VCS Fabric technology, please see the Brocade VCS Fabric Technical Architecture:

[http://www.brocade.com/downloads/documents/technical\\_briefs/vcs-technical-architecture-tb.pdf](http://www.brocade.com/downloads/documents/technical_briefs/vcs-technical-architecture-tb.pdf)

For the Brocade Network Operating System Admin Guide and Network OS Command Reference:

[http://www.brocade.com/downloads/documents/product\\_manuals/B\\_VDX/NOS\\_AdminGuide\\_v211.pdf](http://www.brocade.com/downloads/documents/product_manuals/B_VDX/NOS_AdminGuide_v211.pdf)

[http://www.brocade.com/downloads/documents/product\\_manuals/B\\_VDX/NOS\\_CommandRef\\_v211.pdf](http://www.brocade.com/downloads/documents/product_manuals/B_VDX/NOS_CommandRef_v211.pdf)

The Network OS Release notes can be found at <http://my.brocade.com>

For more information about the Brocade VDX® Series of switches, please see the product Data sheets:

Brocade VDX 6710 Data Center Switch:

<http://www.brocade.com/products/all/switches/product-details/vdx-6710-dc-switches/index.page>

Brocade VDX 6720 Data Center Switch:

<http://www.brocade.com/products/all/switches/product-details/vdx-6720-dc-switches/index.page>

Brocade VDX 6730 Data Center Switch:

<http://www.brocade.com/products/all/switches/product-details/vdx-6730-dc-switches/index.page>

## ABOUT BROCADE

As information becomes increasingly mobile and distributed across the enterprise, organizations today are transitioning to a highly virtualized infrastructure, which often increases overall IT complexity. To simplify this process, organizations must have reliable, flexible network solutions that utilize IT resources whenever and wherever needed—enabling the full advantages of virtualization and cloud computing.

As a global provider of comprehensive networking solutions, Brocade has more than 15 years of experience in delivering Ethernet, storage, and converged networking technologies that are used in the world's most mission-critical environments. Based on the Brocade One™ strategy, this unique approach reduces complexity and disruption by removing network layers, simplifying management, and protecting existing technology investments. As a result, organizations can utilize cloud-optimized networks to achieve their goals of non-stop operations in highly virtualized infrastructures where information and applications are available anywhere.

For more information, visit [www.brocade.com](http://www.brocade.com).

© 2012 Brocade Communications Systems, Inc. All Rights Reserved. 03/12 GA-DG-437-00

Brocade, Brocade Assurance, the B-wing symbol, DCX, Fabric OS, MLX, SAN Health, VCS, and VDX are registered trademarks, and AnyIO, Brocade One, CloudPlex, Effortless Networking, ICX, NET Health, OpenScript, and The Effortless Network are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of their respective owners.

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.