Objective: The BCEFE Nutshell guide is designed to help you prepare for the BCEFE Certification, exam number 150-610.

Audience: The BCEFE Nutshell self-study guide is intended for those who have successfully completed the CEF 200 Certified Ethernet Fabric Engineer Training course, and who wish to undertake self-study or review activities before taking the actual BCEFE exam. The BCEFE guide is not intended as a substitute for classroom training or hands-on time with Brocade products.

How to make the most of the BCEFE guide: The BCEFE guide summarizes the key topics on the BCEFE exam for you in an easy to use format. It is organized closely around the exam objectives. We suggest this guide be used in conjunction with our free online knowledge assessment test. To benefit from the BCLP guide, we strongly recommend you have successfully completed the CEF 200 Certified Ethernet Fabric Engineer Training course.

We hope you find this useful in your journey towards BCEFE Certification, and we welcome your feedback by sending an email to jcannata@brocade.com.

Joe Cannata
Certification Manager
# Table of Contents

1 — Theory and Concepts
   - VCS™ Terminology .................................................. 1
   - TRILL ................................................................. 2
   - Ethernet Fabric Formation ......................................... 4
   - Layer2 Forwarding .................................................... 7
   - Distributed MAC Learning ........................................ 10
   - Data Path ............................................................. 13
   - Data Center Bridging (DCB) ...................................... 20
   - Enhanced Transmission Selection (ETS) ....................... 22
   - vLAGs ................................................................. 25
   - AMPP ................................................................. 28

2 — Hardware and Product Features
   - Hardware ............................................................. 32
   - Product Features .................................................... 36

3 — Installation, Configuration, and Management
   - Installation ........................................................... 42
   - Configuration ......................................................... 45
   - Management .......................................................... 49

4 — Troubleshooting
   - Collecting Support Data ........................................... 52
   - Ethernet Fabric Troubleshooting Overview .................... 53
   - Verifying the Ethernet Fabric .................................... 54
   - Rules for Trunk Formation ....................................... 54
   - Verifying Fabric ISL Formation .................................. 55
   - Troubleshooting the Fabric ...................................... 55
   - Device Connectivity Verification — The name-server command .................................................. 56
   - VLAN Interfaces ....................................................... 57
   - Default VLAN Values ............................................... 57

Taking the Test ................................................................ 58
List of Figures

<table>
<thead>
<tr>
<th>Ethernet fabric using VCS terminology</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRILL Frame</td>
<td>3</td>
</tr>
<tr>
<td>VCS Auto-neighbor Dis coo very</td>
<td>5</td>
</tr>
<tr>
<td>VCS-formed Adjacencies</td>
<td>6</td>
</tr>
<tr>
<td>FSPF for ECMP</td>
<td>7</td>
</tr>
<tr>
<td>ECMP Paths</td>
<td>8</td>
</tr>
<tr>
<td>FSPF Link Cost Example</td>
<td>9</td>
</tr>
<tr>
<td>Multicast Root Election</td>
<td>9</td>
</tr>
<tr>
<td>Distributed MAC Learning</td>
<td>10</td>
</tr>
<tr>
<td>eNS Distribution</td>
<td>11</td>
</tr>
<tr>
<td>MAC Aging</td>
<td>11</td>
</tr>
<tr>
<td>eNS MAC Aging</td>
<td>12</td>
</tr>
<tr>
<td>MAC Moving</td>
<td>12</td>
</tr>
<tr>
<td>Updated MAC Moving</td>
<td>13</td>
</tr>
<tr>
<td>Unicast Ethernet Frame Example</td>
<td>14</td>
</tr>
<tr>
<td>Unicast Ethernet Frame with TRILL Header Added</td>
<td>15</td>
</tr>
<tr>
<td>TRILL Ethernet Frame: Link Transport Header Added</td>
<td>16</td>
</tr>
<tr>
<td>TRILL Ethernet Frame: Data Path</td>
<td>17</td>
</tr>
<tr>
<td>Ethernet Frame: End of Data Path</td>
<td>18</td>
</tr>
<tr>
<td>Example of multicast TRILL to Ethernet frame</td>
<td>19</td>
</tr>
<tr>
<td>ETS Priority Group ID</td>
<td>24</td>
</tr>
<tr>
<td>vLAGs</td>
<td>25</td>
</tr>
<tr>
<td>vLAGs with MCTs</td>
<td>26</td>
</tr>
<tr>
<td>VDX 6720-24 Port Groups</td>
<td>27</td>
</tr>
<tr>
<td>VDX 6720-60 Port Groups</td>
<td>27</td>
</tr>
<tr>
<td>VM Migration Challenges</td>
<td>28</td>
</tr>
<tr>
<td>VM Migration</td>
<td>29</td>
</tr>
<tr>
<td>VM Migration</td>
<td>30</td>
</tr>
<tr>
<td>Brocade’s VDX 6720</td>
<td>32</td>
</tr>
<tr>
<td>Airflow Labels</td>
<td>33</td>
</tr>
<tr>
<td>Active-active Multihomed ToR Topology</td>
<td>39</td>
</tr>
<tr>
<td>ToR Blade Servers Topology</td>
<td>41</td>
</tr>
<tr>
<td>Principal RBridge Election</td>
<td>44</td>
</tr>
<tr>
<td>Spanning Tree on VCS</td>
<td>45</td>
</tr>
<tr>
<td>Static vLAGs</td>
<td>46</td>
</tr>
<tr>
<td>ECMP Path Decision</td>
<td>47</td>
</tr>
<tr>
<td>AMPP Port-profile</td>
<td>48</td>
</tr>
</tbody>
</table>
List of Tables

<table>
<thead>
<tr>
<th>Table Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key to Figure 5</td>
<td>7</td>
</tr>
<tr>
<td>AMPP States</td>
<td>31</td>
</tr>
<tr>
<td>AMPP Behavior</td>
<td>31</td>
</tr>
<tr>
<td>Scalability Notes</td>
<td>34</td>
</tr>
<tr>
<td>Brocade VDX 6720 10 GbE Connector Comparison</td>
<td>35</td>
</tr>
<tr>
<td>One Virtual LAG per VCS</td>
<td>40</td>
</tr>
<tr>
<td>Default VLAN Values</td>
<td>57</td>
</tr>
</tbody>
</table>
1 — Theory and Concepts

VCS™ Terminology

Routing Bridge (RBridge): A switch that is part of the Ethernet fabric. Each switch in an Ethernet fabric is assigned a unique RBridge ID.

ISL or fabric port: Ports connected between VCS-enabled switches.

VCS edge ports: Switch ports used to connect to external devices including end-stations or non-VCS switches and routers.

World Wide Name (WWN): A unique ID associated with all switches. This is assigned by IEEE similar to the MAC OUI by IEEE.

VCS ID: Identifies fabric membership. Every RBridge that participates in a fabric must share the same VCS ID.

1. For SAN experienced students, an RBridge ID is equivalent to a domain ID and the VCS ID is equivalent to a Fabric ID (FID).
TRILL

TRILL Defined
Transparent Interconnection of Lots of Links (TRILL) provides a solution for shortest path frame routing for multihop Layer 2 Ethernet that:

- Supports arbitrary topologies (ring, mesh, star)
- Uses link-state routing protocols²
  - Brocade uses Fabric Shortest Path First (FSPF) as the routing protocol

TRILL is currently a proposed Internet Engineering Task Force (IETF) standard³ and is an Equal-Cost Multi-Path (ECMP)-capable protocol⁴. It uses a link state-based control plane to form loop-free optimized paths between a source and destination. TRILL provides the following features:

- Minimal configuration required
- Load balancing among multiple paths
- Forwarding loop mitigation without the need for STP
- Support of multiple points of attachment to the TRILL network¹
- Support for broadcast and multicast
- No significant service delay after attachment
- No less secure than existing bridged solutions
- Behaves as a normal bridge to devices outside the TRILL network

TRILL Frames
Ingress RBridge prepends frames with a TRILL header and an outer MAC header. Outer MAC header is modified hop-by-hop as with routing. The TRILL header contains ingress and egress RBridge nicknames. Egress RBridge decapsulates the frame and learns the association of the Inner MAC Source Address with the source RBridge nickname.

---
² The link-state protocol is performed by every switching node in the network. The basic concept of link-state routing is that every node constructs a map of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical path from it to every possible destination in the network. The collection of best paths will then form the node's routing table.

³ More information about the TRILL standard can be found by visiting the IETF web site: http://datatracker.ietf.org/wg/trill/

⁴ Equal-cost multi-path routing (ECMP) is a routing strategy where next-hop packet forwarding to a single destination can occur over multiple "best paths" which tie for top place in routing metric calculations. Multipath routing can be used in conjunction with most routing protocols, since it is a per-hop decision that is limited to a single router. It potentially offers substantial increases in bandwidth by load-balancing traffic over multiple paths
**TRILL Frame Example**

Figure 2 details a TRILL data frame with an outer VLAN tag traveling on an Ethernet link between transit RBridges RB3 and RB4. The native frame originated at end station ES_A, was encapsulated by ingress RBridge RB1 and will ultimately be decapsulated by egress RBridge RB2 and delivered to destination end station ES_B.

### Hop Count

The Hop Count field is a 6-bit unsigned integer. An RBridge drops frames received with a hop count of zero, otherwise it decrements the hop count. (This behavior is different from IPv4 and IPv6 in order to support the later addition of a trace route-like facility that would be able to get a hop count exceeded from an egress RBridge.)

For known unicast frames, the ingress RBridge should set the hop count in excess of the number of RBridge hops it expects to the egress RBridge to allow for alternate routing later in the path. For multi-destination frames, the hop count should be set by the ingress RBridge to at least the expected number of hops to the most distant RBridge.

To accomplish this, RBridge RBn calculates, for each branch from RBn of the specified distribution tree rooted at RBI, the maximum number of hops in that branch. Multi-destination frames are of particular danger because a loop involving one or more distribution tree forks could result in the rapid generation of multiple copies of the frame, even with the normal TTL mechanism. It is for this reason that multi-destination frames are subject to a stringent Reverse Path Forwarding Check and other checks. As an optional additional traffic...
control measure, when forwarding a multi-destination frame onto a distribution tree branch, transit RBridge RBm may decrease the hop count by more than 1, unless decreasing the hop count by more than 1 would result in a hop count insufficient to reach all destinations in that branch of the tree rooted at RBI. Using a hop count close or equal to the minimum needed on multi-destination frames provides additional protection against problems with temporary loops when forwarding. Although the RBridge MAY decrease the hop count of multi-destination frames by more than 1, under the circumstances described above, the RBridge forwarding a frame must decrease the hop count by at least 1, and discards the frame if it cannot do so because the hop count is 0. The option to decrease the hop count by more than 1 under the circumstances described above applies only to multi-destination frames, not to known unicast frames.

**Ethernet Fabric Formation**

VCS leverages proven Fibre Channel fabric protocols to build a TRILL-based fabric. The main functions of the fabric formation protocols are:

- Confirming that each switch in the Ethernet fabric is assigned the same VCS ID
- Confirming that each switch in the Ethernet fabric is assigned a unique RBridge ID
- Create a network topology database using a link state routing protocol (FSPF)
- Compute a broadcast tree to distribute fabric broadcast and multicast traffic

Before connecting VDX switches, the following should be configured:

- Enable or disable VCS mode

If VCS is enabled, configure the following:

- VCS ID
- RBridge ID

**Fabric ISL Configuration**

Limited configuration is allowed on ISL interfaces. No configuration needed for normal ISL operation. ISLs can be shutdown and have ISL and trunk functionality turned on or off. Below are examples of enabling ISL and trunk functionality:

```
RB1(config-TenGigabitEthernet-1/0/1)# [no] shutdown
RB1(config-TenGigabitEthernet-1/0/1)# [no] fabric isl enable
RB1(config-TenGigabitEthernet-1/0/1)# [no] fabric trunk enable
```

No edge port configuration is allowed on an ISL. Below is an example of enabling the physical interface of a switch port:

```
switch1(config-TenGigabitEthernet-1/0/1)# switchport
% Interface Port Role is ISL, nothing to be done
```

The fabric ISL configuration attribute controls whether an ISL is formed between two cluster members. With the default setting of ISL discovery mode set to auto, and ISL administrative mode set to enable, an ISL automatically forms between two fabric switches.
Performing the `fabric isl enable` command on an operational ISL has no effect. However, performing the `no fabric isl enable` command on an interface toggles its link status, and subsequently disables ISL formation. In addition, the `no fabric isl enable` command triggers the switch to inform its neighbor that the local interface is ISL disabled. Upon receiving such information, a neighbor switch stops its ISL formation activity regardless of its current interface state.

**Note:** A shutdown on an operating ISL interface not only brings down the physical link but also its FSPF adjacency. The main difference between a shutdown and using the `no fabric ISL enable` command is that the link stays up after the `no fabric isl enable` command has been issued, whereas the link stays down after a shutdown. It is recommended that users use the `no fabric isl enable` command to expedite ISL state transition as its link state stays up.

**VCS Auto-neighbor Discovery**

When two VDX switches are connected, Brocade proprietary hardware primitives are sent to detect a Brocade neighbor. Provided the neighbor is a VDX Switch, a proprietary protocol called Fabric Link Discovery Protocol (FLDP) is used to discover if the neighbor is a VCS-capable switch. Figure 3 displays the following attribute validation during this stage:

- Is the neighbor VCS-enabled (VCS Mode)?
- Do the VCS IDs match on both sides?
- Default settings for NOS 2.0:
  - VCS Mode = 1
  - VCS-ID = 1

![Figure 3: VCS Auto-neighbor Discovery](image)

**Note:** A new role is discovered only when the link toggles from offline to online forcing the control protocol to run again.
**Automatic Layer 2 Adjacency Formation**

VCS forms adjacencies with its directly connected VCS-enabled neighboring switches. These adjacencies are called Inter Switch Links (ISLs). The ISLs can be separate ports or Brocade proprietary hardware-based trunks.

![Figure 4: VCS-formed Adjacencies](image)

**Registered State Change Notification**

Registered State Change Notification (RSCN) events generated in the Ethernet fabric are forwarded to other devices in the following cases:

- When an Ethernet device logs in or out of an Ethernet fabric through any means
- VF_port goes online or offline
- When two VDX switches merge or segment, causing switches to be added or removed

**Note:** DCB is not aware of RSCN events.
Layer2 Forwarding

**FSPF Protocol for Equal Cost Multiple Path (ECMP)**

VCS uses the Fabric Shortest Path First (FSPF) routing protocol to distribute link-state information of all ISLs. FSPF is a Link State Path Selection protocol, similar to OSPF, which is an Interior Gateway Protocol (IGP) widely used in IP networks.

FSPF protocol keeps track of the state of the links on all switches in the Ethernet fabric. It also associates a cost with each link. The protocol computes paths from a switch to all the other switches in the fabric, by adding the cost of all the links traversed by the path, and choosing the path that minimizes the cost.

FSPF is similar to Layer 3 routing protocols like OSPF. Although it has roots from OSPF, FSPF only defines and implements point-to-point links. In other words, there is no concept of a designated router (DR) and a backup designated router (BDR), areas or summarization, or anything similar like that being managed in FSPF.

FSPF forms a single adjacency per fabric trunk.

![Figure 5: FSPF for ECMP](image)

<table>
<thead>
<tr>
<th>Table 1: Key to Figure 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>From RB3</td>
</tr>
<tr>
<td><strong>Destination RB</strong></td>
</tr>
<tr>
<td>RB1</td>
</tr>
<tr>
<td>RB2</td>
</tr>
<tr>
<td>RB4</td>
</tr>
<tr>
<td>RB5</td>
</tr>
<tr>
<td>RB6</td>
</tr>
</tbody>
</table>
**VCS Layer 2 ECMP**

With NOS v2.0.0a, up to 8 ECMP paths are supported per switch. When multiple ECMP paths exist, the traffic is load balanced across all available equal cost paths based on a hash from fields in the frames.

- IP: MAC DA, MAC SA, VLAN, IP DA, IP SA, TCP/UDP ports
- FCoE: Input port, MAC DA, MAC SA, VLAN, D_ID, S_ID, OX_ID
- Other: MAC DA, MAC SA, VLAN

![ECMP Paths](image)

**FSPF Link Cost**

ECMP in an Ethernet fabric behaves slightly differently from the traditional L3 ECMP. Link cost is a metric value assigned to the transmit (Tx) side of each ISL port. The link cost (metric) value for all interfaces is 500, regardless of bandwidth. A 10 Gbps interface has the same link cost as an 80 Gbps fabric trunk. If a neighbor switch is reachable through several interfaces of various link speeds, all of them are treated as ECMP routes.

**FSPF Link Cost Example**

- From RB1 to RB3:
  - Ports 2 and 5 have a cost of 500
  - Port 6 has a cost of 1000 from RB1 to RB3
  - 500 (RB1 to RB2) + 500 (RB2 to RB3)
  - Lowest cost paths are ports 2 and 5
• FSPF configures the routing table on RB1 to only use the routes on ports 2 and 5 for frames with a destination of RB3

In Figure 7, there are three paths: port 2 and port 5, each with a cost of 500, and port 6 with a cost of 1000 between RB1 and RB3. Only the lowest cost routes are in the routing table. Therefore, RB1 ports 2 and 5 are in the routing table and port 6 is not.

**VCS L2 Multicast Tree**

- VCS uses FSPF to calculate and elect a loop-free multicast tree root switch
- The multicast tree is calculated after the unicast routes are computed
- The following rules determine the multicast root election:
  - RBridge ID with the highest priority°
  - If priority is same, lowest RBridge ID is the multicast root
- Of all links that are shortest path towards the root only one is chosen as a primary link°
  - Primary links can be ISL trunks

---

5. The default multicast RBridge priority is zero. The default can be changed using CLI using the `fabric route mcast RBridgeId <RB-ID> priority <priority>` command. The priority range is 0 through 255.
6. Also known as designated ports.
Distributed MAC Learning

Ethernet Name Server (eNS Lookup Table) — MAC Addresses

When the destination MAC address is not in the lookup table the frame is flooded on all ports in the same VLAN, except the ingress port. When the destination MAC address is present in the lookup table the frame is switched only to the correct egress port. If the egress port is the same as the ingress port, the frame is dropped. MAC addresses in the eNS lookup table are removed when one of the following occur:

- The MAC address times out
- A device is moved to a new location
  When a device is moved, the ingress frame from the new port causes the old lookup table entry to be discarded and the new entry to be inserted into the lookup table. Frame forwarding remains unicast to the new port.
- The lookup table is full
  When the lookup table is full, new entries replace the oldest MAC addresses after the oldest MAC addresses reach a certain age and time out. MAC addresses that still have traffic running are not timed out. New entries start replacing older entries when the lookup table reaches 90 percent of its 32K capacity.

Example Learning Process

- The frame is forwarded into the fabric with TRILL encapsulation based on whether the Destination Address (DA) in the frame is known or unknown.
  - If the DA is known to exist on a specific RBridge, then it is sent to that specific destination RBridge.
  - If the DA is unknown, then the frames go out on the multicast tree that covers all RBridges in the fabric.

Note: RB1 is the multicast root bridge.
The first time an unknown DA is encountered, flooding occurs.

When the MAC address is learned anywhere in the Ethernet fabric, the eNS MAC distribution service distributes the learned MAC, interface, VLAN and RBridge entry using the control plane.

The entry is distributed to every VCS member switch to complete the missing information that is not provided by TRILL.

This method minimizes flooding.

**VCS MAC Aging**

- MAC address aging logic on each switch is identical to how aging is performed on a standard IEEE 802.1Q switch.
- Addresses that are learned on local edge port interfaces are aged by the aging function local to the switch.
- In VCS mode, the local aging function informs eNS of an entry that is aged out after it ages it out locally.
- Similarly, addresses are aged out using eNS.
• eNS then informs all the other switches in the fabric to have the forwarding entry removed
• The default aging time is 300 seconds
• Only the physical switch that the MAC resides on can age a MAC

VCS MAC Moving
• When MAC A starts sending frames on RB3, RB3 learns about MAC A locally and immediately sees a conflict
• RB3 updates its local table
• MAC A now resides on RB3, so RB3 has the responsibility for updating the fabric
• RB3 then sends the update to eNS and eNS distributes the change to the other VCS member switches

Figure 14: Updated MAC Moving

Data Path

Traffic Types
The data path through the fabric changes depending on the type of traffic. Traffic is classified into two distinct types:

• Known unicast (destination MAC is known)
• Broadcast, unknown unicast, or multicast

VCS Known Unicast Data Path
For a known unicast frame, no flooding occurs when the one of the following occurs:

• MAC has been previously learned
• RBridges know the RB that is hosting the MAC
• FSPF knows the shortest path to get to the destination RBridge because the routing topology has already been created
Learning of a source MAC to an ingress RBridge is done through the data plane. The ingress RBridge encapsulates the native Ethernet frame with TRILL headers until the frame reaches the destination RBridge. The outer MAC header is changed at every hop. The frame enters the fabric through the ingress RB (RB1). The source MAC (ES_A) is learned by RB1.

![Diagram of Unicast Ethernet Frame Example](image)

**Figure 15: Unicast Ethernet Frame Example**
The ES_B is a known MAC and RB1 knows that MAC ES_B is hosted by RB2
RB1 adds a TRILL header with an egress RB nickname of RB2
• RB1 uses the FSPF routing table to determine the path to RB2
• RB1 adds the link transport header which specifies:
  - The next hop RB for the path (RB3)
  - Itself as the Outer MAC SA

Figure 17: TRILL Ethernet Frame: Link Transport Header Added
As a transit switch, RB3 removes the previous link transport header and replaces it with one that specifies the next hop RB

Figure 18: TRILL Ethernet Frame: Data Path
• The frame arrives at the egress RB, RB2
• RB2 removes the TRILL header and delivers the frame to the end station

Figure 19: Ethernet Frame: End of Data Path
**VCS Multicast Data Path**

- Unknown MAC, broadcast, or multicast traffic enters the fabric
- Traffic is flooded and sent to multicast root

---

**Figure 20: Example of multicast TRILL to Ethernet frame**
**Data Center Bridging (DCB)**

Traditional Ethernet is not suitable for protocols that require or could benefit from a lossless, low latency and low congestion medium such as Fibre Channel or iSCSI. DCB is an umbrella term for an Ethernet technology enhanced by additional standards to meet these requirements. Also referred to as Converged Enhanced Ethernet (CEE).

Key features of DCB include:

- A lossless, full-duplex Ethernet environment which provides in-order delivery and supports a minimum of 2.5 KB mini-jumbo frames
- Convergence of multiple protocols with different requirements over the same Ethernet network
- High speed transport of Ethernet traffic

Enhanced Ethernet—also called Converged Enhanced Ethernet (CEE), Data Center Ethernet or Data Center Bridging (DCB)—eliminates Layer 3 TCP/IP protocols in favor of native Layer 2 Ethernet. Traditional Ethernet commonly experiences network congestion, latency and dropped frames, which renders it unreliable for Fibre Channel traffic. However, 10 GbE Enhanced Ethernet changes this by dispensing with TCP/IP in favor of a “lossless” Ethernet fabric. The lossless environment’s basic requirements are Priority Flow Control (priority pause), ETS (scheduler), and the discovery protocol. (Congestion management is attractive but optional.) These capabilities allow the Fibre Channel frames to run directly over 10Gbps Ethernet segments with no performance degradation.

In order to make Ethernet as reliable as Fibre Channel at the lower layers, it is necessary to add several enhancements to Ethernet to mimic the behavior at the lower layers of Fiber Channel.

For example, the **PAUSE** command is necessary to avoid congestion and frame drop, as is the case with a “best-effort” network such as Ethernet. There have to be logical channels on the Ethernet link, just as virtual channels exist in our Fibre Channel technology. This allows storage traffic to move reliably through the network, while IP traffic is handled on a best-effort basis.

Fibre Channel FSPF allows multiple paths to be used between switches if their path cost is the same, but Ethernet with its Spanning Tree (and variations) routing model does not.

Other enhancements allow for the detection and communication of congestion in the network, to avoid hot spots and throttle back inbound traffic.

**DCB Enhancements to Ethernet**

Data Center Bridging eXchange (DCBX) is based on IEEE 802.1Qaz and leverages functionality provided by IEEE 802.1AB (Link Layer Discovery Protocol - LLDP). It is used for conveying capabilities and configuration features between single-hop neighbors.

Priority Flow Control (PFC) based on IEEE 802.1Qbb provide the following:

- Link level flow control mechanism
- Controlled independently for each Class of Service (CoS). The Ethernet CoS is different from the Fibre Channel CoS. It is defined as the priority level in DCB.
- Goal of this mechanism is to ensure zero loss under congestion in DCB networks

Enhanced Transmission Selection (ETS) is based on IEEE 802.1Qaz and enables bandwidth management by assigning bandwidth segments to different traffic flows.
**DCBX**

The Data Center Bridging Capability Exchange Protocol (DCBX) is used to exchange DCB-related parameters with neighbors including ETS and PFC configuration information. It is based on IEEE 802.1AB which defines a set of DCBX specific TLVs. DCBX capabilities include:

- DCB peer discovery
- Mismatched configuration detection
- DCB-link peer configuration

DCBX uses LLDP to exchange parameters between two link peers. The DCBX TLVs are added to the LLDP frame. There are two types of LLDP TLVs, as specified in the IEEE 802.3AB standard:

- **Basic management TLVs** consist of both optional general system information TLVs as well as mandatory TLVs. Mandatory TLVs cannot be manually configured. They are always the first three TLVs in the LLDPDU, and are part of the packet header. General system information TLVs are optional in LLDP implementations and are defined by the Network Administrator. Common Basic Management TLVs include:
  - Chassis ID (mandatory)
  - Port ID (mandatory)
  - Time to Live (mandatory)
  - DCBX
  - DCBX Control Sub-TLV
  - Priority group sub-TLV
  - Priority flow control sub-TLV
  - Logical link down feature sub-TLV
  - Port description
  - System name
  - System description
  - System capabilities
  - Management address
  - End of LLDPDU

- **Organizationally-specific TLVs** are optional in LLDP implementations and are defined and encoded by individual organizations or vendors. These TLVs include support for, but are not limited to, the IEEE 802.1 and 802.3 standards and the TIA-1057 standard. Examples of Organizationally-specific TLVs include:
  - 802.1 organizationally-specific TLVs: 1) Port VLAN ID; and 2) VLAN name TLV
  - 802.3 organizationally-specific TLVs: 1) MAC/PHY configuration/status; 2) Power through MDI; 3) Link aggregation; 4) Maximum frame size
Enhanced Transmission Selection (ETS)

ETS Overview
Enhanced Transmission Selection (ETS) allocates bandwidth between different traffic classes such as LAN, FCoE, and iSCSI. When the offered load in a traffic class does not use its allocated bandwidth, ETS allows other traffic classes to use the available bandwidth. ETS uses QoS to distinguish between traffic classes and provide different service characteristics to different traffic classes. This allows bandwidth-allocated priorities to coexist with strict priorities through the use of a hybrid scheduler. The hybrid scheduler allows bandwidth sharing between traffic classes while allowing strict priority for time-sensitive and management traffic requiring minimum latency.

QoS Overview
Quality of Service (QoS) provides the capability to control how traffic is moved from switch-to-switch. In a network with different types of traffic with different needs, the goal of QoS is to provide each traffic class with a virtual pipe. QoS is only enforced when congestion is detected. All traffic classes have access to the full bandwidth until congestion is detected. When congestion is detected, each traffic class virtual pipe is restricted to the bandwidth assigned to it. DCB uses traffic class mapping, scheduling, and flow control to provide Quality of Service. Traffic moving through the switches can be classified as follows:

- Multicast traffic has a single source but multiple destinations
- Unicast traffic has a single source with a single destination

QoS Features
Scheduling algorithms include Strict Priority (SP) and Deficit Weighted Round Robin (DWRR) queuing. The hybrid policy combines SP and DWRR servicing. The highest priority queues are serviced by SP while lower priority queues share the remaining bandwidth using the DWRR service. The Brocade VDX™ platform uses the hybrid scheduling policy.

In Strict Priority (SP) scheduling, each CoS queue associated with the egress port is serviced in priority order from highest 7 to lowest 0. All traffic for a given CoS is transmitted before the scheduler proceeds to the next highest priority queue. The purpose of strict priority scheduling is to ensure lower latency and priority transmission of critical traffic by always transmitting higher priority traffic before lower priority traffic.

---

7. Traffic types and Classes of Service (CoS) are interchangeable terms and are a 3-bit field within a Layer 2 Ethernet frame header when using IEEE 802.1Q. It specifies a priority value of between 0 (signifying best-effort) and 7 (signifying priority real-time data) that can be used by Quality of Service disciplines to differentiate traffic. Class of Service (CoS) is a way of managing traffic in a network by grouping similar types of traffic (for example, e-mail, streaming video, voice, large document file transfer) together and treating each type as a class with its own level of service priority. Unlike Quality of Service (QoS) traffic management, Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a best-effort. On the other hand, CoS technology is simpler to manage and more scalable as a network grows in structure and traffic volume. One can think of CoS as coarsely-grained traffic control and QoS as finely-grained traffic control.
Weighted Round Robin (WRR) scheduling services each CoS queue associated with the egress port in round-robin order from highest priority to lowest priority. WRR provides a weighted access to the egress port bandwidth at the frame level. If there are less frames in the CoS queue than the weight assigned to the queue, the scheduler sends all frames in the queue and then begins servicing the next CoS queue. WRR provides sharing of the egress port bandwidth across multiple CoS queues.

Deficit Weighted Round Robin (DWRR) is a weighted round-robin (WRR) method that uses a deficit counter. A maximum frame size number is subtracted from the frame length, and frames that exceed that number are held back until the next visit of the scheduler.

The hybrid policy combines SP and DWRR servicing. The highest priority queues are serviced by SP while lower priority queues share the remaining bandwidth using the DWRR service. The Brocade VDX™ platform uses the hybrid scheduling policy.

CoS Overview

Only a single Class of Service (CoS) can be mapped to a PFC-enabled priority queue. The CoS number must be identical to the PFC-enabled priority queue number. If your configuration violates this restriction an error message displays and the Priority Group Table is set back to the default values. Multiple priority groups may be PFC-enabled. When the CEE map is applied only one strict priority PGID is allowed, PGID 15.0 to PGID 15.7.
**ETS Priority Group ID (PGID)**

PGID enables the mapping of like-priority traffic into Priority Groups (PG) and scheduling operations take place across the priority groups. PGID 0-7 have user assignable weights, in the form of bandwidth allocations and uses DWRR scheduling. PGID 15 is strict priority.

---

8. PGID 8 through 14 are reserved.
9. IPC is normally server-to-server control traffic and therefore has a very high priority.
vLAGs

vLAG Introduction
A vLAG is a fabric service that allows LAGs to originate from multiple Brocade VDX™ switches acting as a single logical switch to an external switch or server. It acts the same way as a standard LAG using the Link Aggregation Control Protocol (LACP), a method to control the bundling of several physical ports together to form a single logical link or trunk.

vLAG Features
- Provisioning and management is consistent with a standard LAG implementation
- Interoperable with servers and third-party switches
  - Standard LACP (IEEE 802.3ad)-based interoperable solution
- Support vLAG links across more than one VDX switch and they do not need to be directly connected (limit of 2 VDX switches with NOS v2.0.0a release)
- From a user perspective, features running on top of the vLAG are configured and operate similarly to features running over a standard LAG (i.e. ACL, QoS)
- FCoE is not supported over a vLAG
**vLAG Example Topology**

Connection between the core Multi-Chassis Trunking (MCT) chassis and Ethernet fabric forms a single vLAG\(^{10}\). Figure 23 displays the following:

- MCT chassis’ form a single logical device
- VDX switches form a single logical fabric
- Eliminates need to run STP between tiers (from access to core)
- Active-active redundant paths between the network tiers

Server connectivity into the fabric gain active-active link utilization. Brocade ISLs or trunks are formed within the Ethernet fabric.

---

10. Multi-Chassis Trunking (MCT), currently available in Brocade MLX routers, is a Brocade technology that allows multiple switches (2) to act as a single logical switch connected to another switch using a standard LAG. MCT at the core with vLAG in the edge fabric enables a single LAG between the two logical elements — which results in a fully active-active network.
**VDX 6720 Port Groups**

Port groups are divided as follows:

- VDX 6720-24: 1-12; 13-24

![Figure 24: VDX 6720-24 Port Groups](image)

- VDX 6720-60: 1-10; 11-20; 21-30; 31-40; 41-50; 51-60

![Figure 25: VDX 6720-60 Port Groups](image)
AMPP

Virtual machine mobility (migration) challenge is when server managers, like VMware’s vCenter, control the migration of server side profiles to ensure the server-side consistency.

In traditional networks, post-migration tasks often require manual configuration changes. VM migration across physical server and switches can result in non-symmetrical network policies. Port setting information must be identical at destination switch/port.

Figure 26: VM Migration Challenges
Virtual Machine Networking Overview

1. vMotion\(^{11}\) is VMware’s technology that allows migration of live virtual machines from one physical server to another without losing VM state, its data or its LAN or SAN sessions.

2. With a Distributed vSwitch implementation server side network policies within the Virtual machine’s soft switch are maintained across different Virtual servers.

3. Network side policies need to be re-created on Layer 2 switch as they may not match between physical Ethernet switches.

Figure 27: VM Migration

4. Figure 28 on page 30 shows the purpose of AMPP is to allow for the creation of common port profiles which are created based on the MAC address of virtual machine (instance). Network settings are distributed across physical switches within the VCS Fabric.

5. Figure 28 on page 30 shows that because of the distributed nature of the port profiles this provides for seamless migration of virtual machine (instances) across physical VCS fabric switches. No post-migration network configuration changes are required to maintain existing policies within the VCS Fabric.\(^{12}\)

\(^{11}\) vMotion is VMware’s technology that allows migration of live virtual machines from one physical server to another without losing VM state, its data or its LAN or SAN sessions.

\(^{12}\) A virtual machine instance post-migration maintains its pre-migration MAC and IP address.
AMPP Hypervisor Agnostic — Underlying Ethernet Fabric Mechanics

AMPP is designed to be hypervisor agnostic. After a migration has occurred the VCS switch uses MAC address learning as the trigger to apply policies (profile). It views a MAC address move within a switch or across switches through the eNS (Ethernet Name Server) to detect a VM migration. Each VM maintains its administratively assigned (within the VM server manager application) IP and MAC address post-migration. All hypervisors send a gratuitous ARP to the connected Layer 2 switch before resuming the application data of a VM. This allows VCS to learn the new location of the VM and apply the relevant policies before the application data traffic resumes.

Port Profile Configuration Overview

1. Create a port profile
2. Define policies within the port profile (e.g. VLAN)
3. Activate the port profile
4. Associate VM-MACs to the port profile
   - One port profile can be associated with multiple VM-MACs
5. Enable the port profile mode on all VDX edge ports across the Ethernet fabric to which VMs may be moved
   - Created port profiles are not activated on an interface
   - AMPP is not supported on LAG or vLAG ports with NOS v2.0.0a
6. Repeat steps 1-5 on each switch in the fabric
**AMPP States and Behavior**

**Table 2: AMPP States**

<table>
<thead>
<tr>
<th>State</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>This state specifies that a port-profile is created but may not be complete. Occurs when the port-profile is created or modified.</td>
</tr>
<tr>
<td>Activated</td>
<td>This state specifies that a port-profile is activated and is available for MAC &gt; port-profile association. If the port-profile created is not complete then the activation fails. Upon failure, you must resolve any conflicts or dependencies and reactivate the port-profile.</td>
</tr>
<tr>
<td>Associated</td>
<td>This state specifies that one or more MAC addresses have been associated to this port-profile within the fabric.</td>
</tr>
<tr>
<td>Applied</td>
<td>This state indicates that the port-profile is applied on the profiled port where the associated MAC address appears. In the absence of any signaling protocol, the system snoops the packet to detect if the associated MAC address has appeared on the profiled port. Configuration of two different port-profiles can coexist on a profiled port, but if there is a conflict then the application of the secondary port-profile fails.</td>
</tr>
</tbody>
</table>

**Table 3: AMPP Behavior**

<table>
<thead>
<tr>
<th>Event</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>• If the port-profile does not exist, then it is created. If it exists, then it is available for modification (if it is not yet activated)</td>
</tr>
<tr>
<td>Activated</td>
<td>• Unless the port-profile is activated, it is not applied on any switch port. • If all the dependency validations succeed, the port-profile is in the ACTIVE state and is ready for association.</td>
</tr>
<tr>
<td>De-activate</td>
<td>• Removes the applied port-profile configuration from all the profiled-ports • De-activation is allowed even if there are MAC addresses associated with the port-profile.</td>
</tr>
<tr>
<td>Modify</td>
<td>• Can be edited only in the pre-activation stage. • Set to the INACTIVE state if any conflicting attributes are configured, or some dependent configuration is not completed • Set as INACTIVE and any attempt to associate the port-profile to a MAC address may not be allowed</td>
</tr>
</tbody>
</table>
2 – Hardware and Product Features

Hardware

Brocade VDX 6720 Data Center Switches Overview

- Built for the Virtual Data Center
  - Uses Brocade fabric switching eAnvil2 ASIC
  - Supports Brocade Network Operating System (NOS) including VCS™ technology
- Performance and Density
  - 24- and 60-port models (VDX 6720-24 and VDX 6720-60)
  - Ports on Demand (POD) enables 24 to 60 port configurations
  - 600 ns port-to-port latency
- Configuration Flexibility
  - 1 Gbps or 10 Gbps supported on every port
  - Twinax, direct-attached optical, and SFP optical connectivity options
  - Front-to-back or back-to-front airflow
- Enables Network Convergence
  - Complete FCoE support including multi-hop (license required)
  - iSCSI Data Center Bridging support (DCB)

Figure 29: Brocade’s VDX 6720
**Airflow Options**

Some high-density server racks have specific cooling requirements. The Brocade VDX 6720 Data Center switches support the following configurations:

- Front-to-back or back-to-front airflow
- Airflow direction determined by integrated power/fan unit, power supply, or fan installed

**Note:** Must order the FRU with correct airflow direction\(^{13}\).

---

\(^{13}\) When ordering FRUs, verify that the part number supports the correct airflow. You must replace a failed unit with the same type of unit. This applies to both power supplies and fan assemblies. A new FRU must have the same part number (P/N) as the FRU being replaced. The manufacturing P/N is located on the top of the FRU. The P/N ends in either -F (front-to-back airflow) or -R (back/rear-to-front airflow). You must use a replacement FRU that has the same airflow designator with the part number. Additionally, you can use external labels as a guide. Some FRUs are labeled with an airflow symbol on the faceplate to indicate whether the assembly takes in or exhausts air. The symbol also appears on the top of the assembly.
Brocade VDX 6720-60 Fan Assembly Replacement

Tools required:
- Phillips-head screwdriver #1

To remove a fan assembly:
1. Unscrew the captive screw on the fan assembly to be replaced.
2. Pull the handle on the fan assembly out and away from the chassis.

To replace a fan assembly:
1. Verify the replacement fan matches the airflow direction of the failed fan assembly.
   - If the airflow does not match, a warning message is generated. Below are examples of warning messages:
     WARNING, Brocade6720, MISMATCH in PSU-FAN FRUS Air Flow direction. Replace PSU with fan air flows in same direction.
     WARNING, Brocade6720, MISMATCH in FAN Air Flow direction. Replace FRU with fan air flows in same direction.
2. Orient the new fan assembly with the captive screw on the left.
3. Carefully insert the fan assembly into the chassis until firmly seated.
4. Tighten the captive screw.
5. Verify that the fan status LED is lit steady green to indicate normal operation.

Table 4: Scalability Notes

<table>
<thead>
<tr>
<th>Type</th>
<th>Mode</th>
<th>Standalone</th>
<th>Both VCS and Standalone</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCB Priority Flow Control (PFC) classes</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISL Trunking: Maximum ports per trunk</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum jumbo frame size</td>
<td>9600 bytes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum multicast group</td>
<td>256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link aggregation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum port per group</td>
<td>64</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>Maximum groups</td>
<td>16</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>MAC addresses</td>
<td>32,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per priority pause levels</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port profiles (AMPP)</td>
<td>256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Queues per port</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum STP (Spanning Tree instances)</td>
<td>16</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Maximum VLANs</td>
<td>4096</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Brocade VDX 6720 Main CPU:
- 1.3GHz PowerPC CPU
- 4 MB on-board boot flash
- 1 GB on-board compact flash for OS and application files storage
- Real-time clock (RTC) with battery
- SEEPROM for switch identification
- Voltage monitoring
- Fan monitoring
- Three digital temperature sensors

Table 5: Brocade VDX 6720 10 GbE Connector Comparison

<table>
<thead>
<tr>
<th>Type</th>
<th>Connector</th>
<th>Cable</th>
<th>Distance</th>
<th>Power (each side)</th>
<th>Transceiver Latency (link)</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive Copper</td>
<td>SFP+ copper</td>
<td>Twinax</td>
<td>&lt; 10 m</td>
<td>~ 0.1 W</td>
<td>~ 0.1 µs</td>
<td>SFF 8431</td>
</tr>
<tr>
<td>Active Copper</td>
<td>SFP+ copper</td>
<td>Twinax</td>
<td>Up to 20 m (up to 5m supported)</td>
<td>~ 0.25 W</td>
<td>~ 0.1 µs</td>
<td>IEEE 802.3ae</td>
</tr>
<tr>
<td>Active Optical cable</td>
<td>SFP+ copper</td>
<td>Plastic optical fiber</td>
<td>Up to 30 m (10m, 20m supported)</td>
<td>~ 0.5 W</td>
<td>~ 0.1 µs</td>
<td>SFF 8431</td>
</tr>
<tr>
<td>10GbE-SR SFP+</td>
<td>SFP+ MMF, SR</td>
<td>MM OM2</td>
<td>82 m</td>
<td>~ 0.65 W</td>
<td>~ 0.1 µs</td>
<td>IEEE 802.3ae</td>
</tr>
<tr>
<td></td>
<td>MM OM3</td>
<td>300 m</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10GbE-LR SFP+</td>
<td>SFP+ SMF, SR</td>
<td>SM</td>
<td>10,000 m</td>
<td>~ 1.0 W</td>
<td>~ 0.1 µs</td>
<td>IEEE 802.3ae</td>
</tr>
<tr>
<td>10GBase-T</td>
<td>RJ-45</td>
<td>Cat 6a</td>
<td>Up to 100 m</td>
<td>~ 4.5-7 W</td>
<td>~ 2.5 µs</td>
<td>IEEE 802.3ae</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cat 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Each VDX product interoperates with the following:
- BR 1010
- BR 1020
- VDX 6720-24
- VDX6720-60
Product Features

**Brocade Network OS**

Brocade’s Network Operating System (NOS) represents an evolution of:

- Fabric OS used with Storage Area Network (SAN) products
- CMSH used with the Brocade FCoE products
- NOS CLI is an industry standard Ethernet CLI

NOS has been built specifically to run the new product family and will be used on all future VCS products. It combines the best of our hardened Fabric OS—which is known industry-wide for its stability, non-stop operation, and advanced diagnostic capabilities—with the hardened routing stack and operational interfaces from our product portfolios including the CMSH used with the Brocade 8000 product.

Every device running Brocade Network OS has a full Fibre Channel services stack and a full Ethernet stack. This means that every device is inherently designed to support any type of traffic: “traditional” IP, iSCSI, CIFS, NFS, and FCoE.

Merging these services stacks gives us a unique ability to support the requirements of virtualized infrastructure while also reliably interfacing with and preserving your investment in existing products.

**RBridge Overview**

Routing Bridges (RBridges) combine the advantages of bridges and routers and are interoperable with industry standard Layer 2 and 3 devices. Though RBridges are Layer 2 devices, they are similar to routers as they:

- Include an additional outer Layer 2 frame header that includes hop count and is replaced at each hop
- Use optimal paths
- Have fast convergence

RBridges are similar to bridges as they:

- Connect devices together to form a single Layer 2 broadcast domain
- Are plug-and-play (to an extent)

**RBridge Physical Port Numbers**

Ports on an RBridge are referenced as follows:

```
Switch(config)# interface TenGigabitEthernet 9/0/1
Switch(config)# int te 9/0/1
```

In the examples above:

- Nine represents the RBridge ID of the physical switch
- Zero represents the slot number, which for non-chassis-based systems is always zero
- One represents the physical port number
**VDX Platform Modes**

Brocade NOS supports two modes of operation for VDX platforms:

- VCS mode
- Standalone mode
  - Default state (By default, all interfaces are in “shutdown” state when a switch is in standalone mode.)
  - A switch goes into a standalone mode and operates like a regular 802.1Q switch if the VCS Enable attribute is turned off
  - DCB-capable, but no support for FCoE

**iSCSI Support**

Provides deterministic delivery of iSCSI traffic which maximizes iSCSI throughput. The intent is to minimize TCP retransmissions by eliminating congestive packet loss. To accomplish deterministic delivery DCB Ethernet enhancements are utilized, such as per-Priority Flow Control (PFC) and Enhanced Transmission Selection (ETS). It uses DCB Capability eXchange Protocol (DCBX) to distribute DCB configuration to iSCSI devices. To help avoid manual configuration of the iSCSI Priority a new TLV is required. The iSCSI TLV is currently only supported in standalone mode (v2.0.0a).

**Spanning Tree Configuration Overview**

Available Spanning-Tree configuration options (standalone mode only):

- 802.1D Spanning Tree Protocol (STP) — STP is required to create a loop-free topology in the LAN
- Rapid Spanning Tree Protocol (RSTP) — RSTP evolved from the 802.1D STP standard. RSTP provides for a faster spanning tree convergence after a topology change
- Multiple Spanning Tree Protocol (MSTP) — With per-VLAN MSTP, you can configure a separate spanning tree for each VLAN group. The protocol automatically blocks the links that are redundant in each spanning tree

**sFlow — Overview**

sFlow is an Industry standard for monitoring high-speed, multilayer switched networks and complies with RFC 3176. It monitors traffic flow for all network ports or specific ports by using a sampling technology to collect statistics. It is effective at gigabit speeds and does not impact network performance. sFlow is protocol independent to ensure that all the traffic is seen and is supported on physical interfaces only.

---

14. Within data communication protocols, optional information may be encoded as a type-length-value or TLV element inside of the protocol.
- Benefits of sFlow:
  - Minimizes network downtime
  - Rapidly pin-points congestion problems
  - Troubleshoots network problems quickly
  - Detailed data capture enables rapid problem resolution, minimizing costly network
  - Protect the assets with Security and Surveillance
  - Identify access policy violations and intrusions
  - Distributed Denial of Service Detection and diagnosis

**sFlow Components**

sFlow uses two types of sampling:
  - Statistical packet based sampling of packet flows (this release samples packet headers only)
  - Time based sampling of interface counters (this release samples generic and Ethernet counters)

**FCoE Feature Set: Supported**

- FIP version 1\(^1\)\(^5\) (FC-BB-5 rev 2.00)
- FC Fabric Services for FCoE VN_Port devices
- Multipathing with in the Ethernet fabric for FCoE traffic
- Up to 255 logins per logical port
  - 1 FLOGI
  - 254 NPIV FDISCs
- Up to 4096 VN ports per switch
- FCoE devices must be directly connected to a Ethernet fabric switch

---

**FCoE Feature Set: Not Supported**

- FCoE device drivers that only support
  - Pre-FIP
  - FIP version 0
- FCoE to FC bridging
- Virtual Fabrics, only single Virtual Fabric supported
- Zoning\(^\text{16}\)
  - All devices are in a default zone, allowing any-to-any communication
- Stand-alone mode (VCS disabled)
- FCoE over LAG (vLAG)
- Use of CoS 0 or 7 for FCoE traffic

**VCS Use Case #1: 1/10 Gbps Top-of-Rack Access — Topology**

- Active-active multi-homed server connections
  - Servers only see one ToR switch
  - Half the server connections

---

16. The fabric device limitation is set to 256 FCoE devices in a Ethernet fabric since open zoning floods all the SCNs to every FCoE device without any zoning.
• Reduced switch management
  - Half the number of logical switches to manage
• Unified uplinks
  - One virtual LAG per VCS

Table 6: One Virtual LAG per VCS

<table>
<thead>
<tr>
<th>Utilization</th>
<th>Classic TOR</th>
<th>VCS ToR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connections per Server</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Logical Switches per Rack</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>LAG per Rack</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
VCS Use Case #2: 10 Gbps Top-of-Rack Access for Blade Servers — Topology

- 1st stage network aggregation
  - 2-switch pair at ToR
  - Aggregates 4 blade server chassis per rack (8 access switches)
- Reduced switch management
  - Half the number of logical ToR switches to manage
- Unified uplinks
  - One virtual LAG per VCS

Figure 32: ToR Blade Servers Topology
3 – Installation, Configuration, and Management

Installation

Brocade VDX 6720 Licenses and Ports On Demand

- VDX 6720-24
  - VCS license is needed for an Ethernet fabric containing three or more VCS-enabled switches\(^\text{17}\)
  - FCOE_BASE license
  - Ports on Demand (POD) license: 8-port POD license can be added to create a 24 port model\(^\text{18}\)
- VDX 6720-60
  - VCS license is needed for an Ethernet fabric containing three or more VCS-enabled switches\(^\text{17}\)
  - FCOE_BASE license
  - Pod license: Two 10-port POD licenses can be added to create a 50 and 60 port model

Note: No ISL Trunking license is required

Temporary Licenses

There are three types of temporary licenses:

- Individual time-based licenses
  - Locked to a single switch
  - Fixed expiration date
  - Cannot install this license on multiple switches
- Universal time-based licenses
  - Use a specified feature for a limited trial period specified in days
  - Can be used on any product that supports the feature
  - Cannot install a license with an expired shelf life
- License expiration
  - The expiration date is based on the system time at the installation of the license plus the number of days that the universal time-based license is valid
  - The feature continues to work while generating warning messages until the switch reboots

---

\(^\text{17}\) Only a two-switch VCS license is built-in. If your Ethernet fabric contains three or more VCS-enabled switches, then you need to purchase a VCS license.

\(^\text{18}\) Ports on Demand (POD) license enables inactive ports, ships with switches.
**FCoE License Requirements**

- Required licenses:
  - **VCS**
    - License is built-in
    - VCS mode must be enabled
  - **FCOE_BASE**
    - If no FCoE base license is installed:
      - Configuration commands fail
      - Show commands work

**Addition of a Switch to VCS**

- The new switch joining should have the same VCS ID or else it will not be allowed to join the fabric
- If the joining switch has a conflicting RBridge ID configured, it is not allowed to join the fabric
- If a newly joined switch is the lowest WWN, it becomes the new principal switch
- If the newly joined switch is the lowest RBridge ID then it becomes the multicast root\(^{19}\)
- The multicast and unicast paths can change
- eNS proactively sync’s the MAC database to the new switch. This avoids flooding in the fabric due to a new switch

**RBridge ID Conflicts**

- If there is a conflict for a RBridge ID, one of the offending switches must have their RBridge ID changed
- Valid RBridge IDs are 1-239
- An RBridge ID change requires a reboot of the switch
  - The RBridge ID is set in all configuration databases (DBs) and these DBs must be modified when an RBridge ID is changed. It is this change to the DBs which require the reboot

---

\(^{19}\) This is based on that the multicast root priority has not been set.
RBridge ID and VCS ID Assignment

- In NOS v2.0.0a, a unique RBridge ID is assigned manually by the administrator, along with the fabric VCS ID
  
  ```
  VDX6720# vcs rbridgeid 3 vcsid 1
  ```

- Enabling VCS requires a VCS license and it requires the switch to be rebooted

- The RBridge ID can also be explicitly set using
  
  ```
  VDX6720# vcs rbridgeid <value>
  ```

- The RBridge ID assigned to a switch is persisted across reboots

- All interface configurations use the RBridge ID as the first number in the interface number
  
  ```
  VDX6720(config)# interface tengigabitethernet3/0/1
  ```

Principal RBridge Election

The principal switch decides whether a new RBridge joining the fabric conflicts with any existing RBridge IDs. If there is a conflict, the principal switch keeps the joining switch segmented. Every VCS-enabled switch assumes itself as a principal switch after boot-up. All VCS-enabled switches elect the switch with the lowest WWN as the principal. Unlike STP root bridge elections, the principal RBridge does not dictate data path forwarding and has no effect on the data plane.

![Figure 33: Principal RBridge Election](image)

---

20. Value range is 1-239.
Configuration

Spanning Tree on VCS
VCS can coexist with legacy STP deployments. In tunneling mode STP BPDUs are tunneled across the multicast tree. All edge switches see each others BPDUs and VCS acts as a wire.

![Spanning Tree on VCS Diagram](image)

Figure 34: Spanning Tree on VCS

FCoE Port Numbering

- **Physical** port mapping notation:
  - `<Switch_RBID>/<Slot_Number>/<Physical_Port>`
    - VDX 6720-24 and VDX 6720-60 switches the slot number will always be 0
    - Example: 2/0/10 would be switch RBID 2, slot 0, and port 10
  - VDX 6720-24 and VDX 6720-60 switches the slot number will always be 0
  - Example: 2/0/10 would be switch RBID 2, slot 0, and port 10

- **FCoE** port format:
  - `<Mapped-VN-Number>^21/<Switch_RBID>/<Logical_Port>`
    - Switch RBID: Switch-ID in the VCS
    - Port: Logical port number
    - Example: Interface FCoE 1/4/5 would be VN 1, switch RBID 4 and port 5
  - 1:1 Mapping of physical port to FCoE logical port
    - Example: TenGigabitEthernet 5/0/1 changes to FCoE 1/5/1

Configuring FCoE interfaces

An FCoE map is a placeholder for an FCoE VLAN and a CEE map. Assign FCoE maps on to physical interfaces using the `fcoeport` command. Once the FCoE map is assigned onto an interface the following applies:

- The corresponding FCoE VLAN 1002 is applied to the interface
- The corresponding CEE map is applied to the interface
- The FCoE/FIP vlan classifiers are applied to the interface

---

^21. The `<Mapped-VN-Number>` is a virtual network number which gets mapped to a VLAN (used for FCoE traffic).
   In NOS v2.0.0a, the `<Mapped-VN-Number>` is fixed to 1 and the default VLAN used for FCoE traffic is 1002, which can be changed.
Switchport Modes
The `switchport` command is used on the switch port interfaces to make them functional for L2 traffic. You enable L2 on edge ports with devices attached using the following command:

```
switch(conf-if-te-0/1)# switchport
```

Switchport modes are used to control the flow of traffic in the Brocade Ethernet fabric. There are three switchport modes:

- **Access mode** is used for untagged traffic
  
  ```
  switch(conf-if-te-1/0/1)# switchport mode access
  ```

- **Trunk mode** is used for VLAN tagged traffic
  
  ```
  switch(conf-if-te-1/0/1)# switchport mode trunk
  ```

- **Converged mode** is used for tagged and untagged traffic
  
  ```
  switch(conf-if-te-1/0/1)# switchport mode converged
  ```

Virtual LAG Overview
Ports must be at the same speed to be aggregated into a vLAG. Consistently configure all nodes in the vLAG. Brocade proprietary LAGs are not available to be a part of a vLAGs. A port-channel interface is created on all the vLAG members. vLAGs are not able to detect configuration errors. A zero port vLAG is allowed. The primary link of a vLAG is used to carry multicast traffic. Interface statistics are collected and shown per vLAG member per switch. The statistics are not aggregated across switches participating in a vLAG. LACP automatically negotiates and forms the vLAG. The VCS fabric supports static vLAGs which can be configured when servers do not support or implement LACP.

Static vLAG
Current hypervisors do not support LACP-based dynamic LAGs. In order to provide link and node level redundancy, VCS supports static vLAGs. Similar to static LAGs, a statically configured vLAG cannot detect configuration errors.

![Figure 35: Static vLAGs](image)
Example of Static LAG configuration:

```bash
RB1(config)# interface te 1/0/13
RB1(conf-if-te-1/0/13)# channel-group 4 mode on
RB1(config-if-te-1/0/13)# interface te 1/0/14
RB1(config-if-te-1/0/14)# channel-group 4 mode on
```

**vLAG Optimized Multi-pathing**

The ECMP based multi-pathing requires that all the member RBridges in a vLAG are equal cost from a given ingress, otherwise ECMP may not be exercised. VCS delivers an “Optimized Multi-Pathing” by implementing the following:

- Load balance across RBs based on the DST MAC addresses
- The decision is made at the entry point of the VCS

For example, if vLAG connection for Virtual Machine Server C was between RB2 and RB4 traffic destined to a different Virtual Machine (MAC1 and MAC2) deployed on Server C would be load balanced on alternate paths.

![Figure 36: ECMP Path Decision](image)

**vLAG versus LAG Provisioning**

Once VCS detects that the LAG configuration spans multiple VDX switches, the LAG automatically becomes a vLAG. The standard “Admin Key” (Channel #) provisioning needs to be the same for ports that belong to the same vLAG. Only ports with same speed are aggregated. Brocade proprietary LAGs are not allowed or applicable for vLAGs. Brocade-proprietary aggregation is similar to standards-based link aggregation but differs in how the traffic is distributed.
AMPP Port-Profiles — Basic guidelines

The default port-profile contains the entire configuration needed for a VM to get access to the LAN and SAN. A port-profile operates as a self-contained configuration container. Editing of the port-profile is not allowed once the port-profile is activated. De-activate, modify, then re-activate the port profile. Figure 37 displays the parts of a port profile.

![Figure 37: AMPP Port-profile](image)

Configuring Security Profiles

A security profile defines all the security rules needed for the server port. A typical security profile contains attributes for MAC-based standard and extended ACLs. To configure the security profile, perform the following steps in global configuration mode:

1. AMPP profiles cannot be modified while active. De-activate the port-profile before modifying the security profile

   ```
   switch(config)# no port-profile vml-port-profile activate
   ```

2. Enter security profile configuration mode

   ```
   switch(config)# port-profile vml-port-profile
   switch(conf-pp)# security-profile
   ```

3. Modify the ACL security attributes

4. Apply the ACL to the security profile

   ```
   switch(conf-pp-security)# mac access-group vml-acl in
   ```

5. Exit security profile configuration mode

   ```
   switch(conf-pp-security)# exit
   ```

6. Activate the profile

   ```
   switch(config)# port-profile vml-port-profile activate
   ```

7. Associate the profile to the MAC address for each host

   ```
   switch(config)# port-profile vml-port-profile static 0050.56bf.0001
   switch(config)# port-profile vml-port-profile static 0050.56bf.0002
   switch(config)# port-profile vml-port-profile static 0050.56bf.0003
   switch(config)# port-profile vml-port-profile static 0050.56bf.0004
   switch(config)# port-profile vml-port-profile static 0050.56bf.0005
   ```
Management

sFlow Protocol Overview
sFlow monitors high-speed switched networks. The sFlow agent collects statistics from the switch and forwards the data to the sFlow collector. The sFlow collector stores the sFlow datagrams from all agents on the network for processing at a later time. The sFlow agent uses two forms of operation:

- Time-based sampling of interface counters
- Statistical sampling of switched packets

SPAN Overview
Switched Port Analyzer (SPAN) is used for network monitoring. Sends a copy of packets from one switch port to a monitoring connection on another switch port. Allows bidirectional traffic monitoring on the source port. A port can not be mirrored to multiple locations in the same direction. A monitor session can have only one source port. For additional ports you must create additional monitor sessions. The mirror port should not be configured to carry normal traffic. On the Brocade VDX 6720-24 the following applies:

- The mirror port can be any port in the switch
- Only one port per switch can be configured as a destination port for ingress mirroring
- Only one port per switch can be configured as a destination port for egress mirroring

On the Brocade VDX 6720-60 the following applies:

- The mirror port should be in the same port-group as the source port
- Only one port per port-group can be configured as a destination port for ingress mirroring
- Only one port per port-group can be configured as a destination port for egress mirroring

TACACS+ Overview
The Terminal Access Controller Access-Control System Plus (TACACS+) is a protocol used in AAA server environments. It is used only for authentication. A maximum of five TACACS+ servers can be configured per switch. A role should be assigned to a user configured on the TACACS+ server and configured on the switch. The user role is assigned by default when the following occur:

- If the switch fails to get the user’s role from the TACACS+ server after successful authentication
- If the role does not match any of the roles present on the switch

RBAC Overview
Role-based access control (RBAC) is used as an authorization mechanism. Roles can be created dynamically. Roles are associated with rules to define permissions (i.e. read-only, read-write). User accounts must be associated with only one role. Permissions cannot be assigned directly to the user accounts. Permissions can only be acquired through the associated role. RBAC is the function of specifying access rights to resources for roles. When a user executes a command, privileges are evaluated to determine access to the command based on the role of the user.
Firmware Management Overview
Firmware is installed on the switch by executing the firmware download command. You can download the firmware from a remote server or from an attached Brocade-branded USB device. The VDX 6720 switches maintain two partitions of nonvolatile storage areas, a primary and a secondary partition, to store two firmware images. This enables you to download a version of firmware for testing and then if necessary, restore the switch to the previous firmware version.

Firmware Management Commands — The firmware download command
Downloads firmware onto a switch and starts the installation process. Supports command line and interactive CLI. Firmware can be downloaded using FTP, SCP, or USB drive. Requires you to accept the download during installation.

Syntax:
```
firmware download ftp|scp [nocommit] [noreboot] host <host_ip> user <username> password <password> directory <directory> [file <file name>]
firmware download usb directory <directory>
firmware download interactive
```

NOS Configuration Management
It is recommended to create a backup copy of the running configuration. To create a backup copy of the running configuration, use one of these methods:

- Copy the running-config to the switch’s startup-config
- Copy the startup-config or running-config files to the switches “flash://” directory

The copy command copies the file to another location.

Syntax: copy <source-file-url> <destination-file-url>

Operands: <source-file-url> — Specifies location of the source file to be copied using one of the following formats:
- FLASH copies from URL [flash://]filename
- FTP copies from URL ftp://[username[:password]@server/path]
- SCP copies from URL scp://[username[:password]@server/path]
- <destination-file-url> — Specifies the destination file using one of the following formats:
- FLASH copies to URL [flash://]filename
- FTP copies to URL ftp://[username[:password]@server/path]
- SCP copies to URL scp://[username[:password]@server/path]
- running-config: Copies to the current running configuration
- Startup-config: Copies to the current running configuration file
Upload the startup-config or running-config files to a remote location by FTP or SCP. Upload any configuration files to a remote location directly from the running-config, startup-config or flash. Following is an example to copy the source file to a remote machine using FTP:

```
VDX6720# copy running-config ftp://user:password@10.10.10.10/path/file1
Building configuration...
```

**Configuration Files on a USB device—Backing up**

The destination file is the file URL on the USB device. You do not need to specify the target directory. The file is automatically recognized as a configuration file and stored in the default configuration directory

1. Enable the USB device
   ```
   switch#usb on
   USB storage enabled
   ```

2. Enter the `copy startup-config <destination_file>` command
   ```
   switch#copy startup-config usb://startup-config_vdx24-08_20101010
   ```

**Configuration Files on a USB device—Restoring the default configuration**

1. Download an archived backup copy from an external host or from an attached USB device.

2. Enter the `copy <source_file> <destination_file>` command to overwrite the startup configuration with the default configuration.
   ```
   switch# copy flash://defaultconfig.novcs startup-config
   This operation will modify your startup configuration. Do you want to continue? [Y/N]: y
   ```

**Note:** There are different default configs based on whether the switch is in VCS or standalone mode.
4 — Troubleshooting

Collecting Support Data

Two ways to get the support data:

- Command line mode
  
  RB1# `copy support ftp all directory /vdxsupport`
  
  host 10.255.252.50 password pswd user guest

- Interactive mode
  
  RB1# `copy support-interactive`
  
  Server Name or IP Address: 10.255.252.50
  
  Protocol (ftp, scp): ftp
  
  User: guest
  
  Password: ******
  
  Directory: /vdxsupport
  
  VCS support [y/n]? (y): y
  
  copy support start
  
  Saving support information for chassis:BROCADE-VDX6720, module:RAS...
  
  Saving support information for chassis:BROCADE-VDX6720, module:CTRACE_OLD...
  
  Saving support information for chassis:BROCADE-VDX6720, module:CTRACE_NEW...
  
  Saving support information for chassis:BROCADE-VDX6720, module:INFRA...
  
  Saving support information for chassis:BROCADE-VDX6720, module:INFRA_USER...
  
  Saving support information for chassis:BROCADE-VDX6720, module:ASICDB...
  
  Saving support information for chassis:BROCADE-VDX6720, module:DCEHSL...
  
  Saving support information for chassis:BROCADE-VDX6720, module:CEEDEBUG...
  
  Saving support information for chassis:BROCADE-VDX6720, module:MAPS...
  
  Saving support information for chassis:BROCADE-VDX6720, module:RAS_POST...
  
  copy support completed
  
  copy support complete

The file name format is as follows:

- SWITCH_NAME+slot#+CPUPType+YYYYMMDDHHMM.MODULE_NAME.txt.gz
- Example: BROCADE-VDX6720-S0cp-201010290121.DCMD_LOGS.txt.gz

All files are zipped. Files that have an “ss” extension are encrypted and require a decoder to view them.

- Example: BROCADE-VDX6720-S0cp-201010290121.INFRA.txt.ss.gz
Below is a complete list of the files created:

- BROCADE-VDX6720-S0cp-201010290121.CTRACE_NEW.dmp.gz
- BROCADE-VDX6720-S0cp-201010290121.CTRACE_OLD.dmp.gz
- BROCADE-VDX6720-S0cp-201010290121.DCMD_LOGS.txt.gz
- BROCADE-VDX6720-S0cp-201010290121.INFRA.txt.ss.gz
- BROCADE-VDX6720-S0cp-201010290121.INFRA_USER.txt.gz
- BROCADE-VDX6720-S0cp-201010290121.RAS.txt.ss.gz
- BROCADE-VDX6720-S0cp-201010290122.ASICDB.txt.gz
- BROCADE-VDX6720-S0cp-201010290122.CEEDEBUG.txt.ss.gz
- BROCADE-VDX6720-S0cp-201010290122.DCEHSL.txt.gz
- BROCADE-VDX6720-S0cp-201010290122.FC_SERVICE.txt.ss.gz
- BROCADE-VDX6720-S0cp-201010290122.FC_SERVICE_USER.txt.gz
- BROCADE-VDX6720-S0cp-201010290122.MAPS.txt.gz
- BROCADE-VDX6720-S0cp-201010290122.OS.txt.ss.gz
- BROCADE-VDX6720-S0cp-201010290122.RAS_POST.txt.gz
- BROCADE-VDX6720-S0cp-201010290122.SSHOW_SEC.txt.gz
- BROCADE-VDX6720_FILE-S0cp-201010290121.Dcmdlogs.tar.gz
- BROCADE-VDX6720_FILE-S0cp-201010290122.regdump.tar.gz

**Ethernet Fabric Troubleshooting Overview**

Troubleshooting an Ethernet fabric can involves verifying parameters and device connectivity, and reviewing rules. Use the following commands to verify the output you see is what you expect for your fabric:

- show mac-address-table
- show fabric trunk
- show vcs
- name-server
Verifying the Ethernet Fabric

VDX6720# show mac-address-table
VlanId  Mac-address       Type     State      Ports
VlanId  Mac-address       Type     State      Ports
1  0005.1ed9.f024    Dynamic  Active     Te 1/0/16
1  0005.3326.574b    Dynamic  Active     Te 1/0/6
1  0005.3326.57e2    Static   Active     Te 2/0/9
1  0015.5d51.6404    Static   InActive   Te 1/0/16
1  0050.56bf.0000    Dynamic  Active     Te 2/0/6
1  0050.56bf.0005    Dynamic  Active     Te 1/0/4
1  0050.56bf.0006    Dynamic  Active     Te 2/0/6
1  0100.1111.2222    Static   InActive   Te 1/0/6
1  0010.9400.0005    Dynamic  Active     Po 10
100 0010.9400.0006    Dynamic  Active     Te 2/0/6
100 0efc.0001.1e00    FPMA    Active     Te 1/0/6
100 0efc.0001.2900    FPMA    Active     Te 1/0/17
Total MAC addresses : 12

Rules for Trunk Formation

All ISLs in the trunk need to be part of the same port group and configured for the same speed. Following are the port groups for each VDX model (refer to Figure 24, “VDX 6720-24 Port Groups,” on page 27 for a visual aid):

- VDX 6720-24: 1-12; 13-24
- VDX 6720-60: 1-10; 11-20; 21-30; 31-40; 41-50; 51-60
Verifying Fabric ISL Formation

The first two show that an ISL formed properly because they fit the criteria: same port group, same speed.

RB12# show fabric trunk

RBridge-ID: 12

<table>
<thead>
<tr>
<th>Group</th>
<th>Src-Port</th>
<th>Nbr-Port</th>
<th>Nbr-WWN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>te12/0/1</td>
<td>te3/0/13</td>
<td>10:00:00:05:1E:CD:55:6A</td>
</tr>
<tr>
<td>1</td>
<td>te12/0/2</td>
<td>te3/0/14</td>
<td>10:00:00:05:1E:CD:55:6A</td>
</tr>
</tbody>
</table>

Troubleshooting the Fabric

The VCS ID determines the fabric ID and which fabric the switch belongs to. In this example the two switches will not merge because they are in different fabrics. If the VCS ID is the same the switches would merge.

- Check the VCS settings (example 1):

  RB1# show vcs
  state : Enabled
  vcsid : 1
  rbridgeid : 1

  RB2# show vcs
  state : Enabled
  vcsid : 2
  rbridgeid : 2

  **VCS IDs must match**
  **RBridge IDs must be unique**

  In this example, the VCS IDs are not the same so the switches would not attempt to merge
Example VCS settings (example 2):

```bash
RB1# show vcs
state : Enabled
vcsid : 1
rbridgeid : 1

RB2# show vcs
state : Enabled
vcsid : 1
rbridgeid : 1
```

The RBridge ID is like the Domain ID in the SAN world, every switch must have a unique RBridge ID. The example above would result in the following error message and the fabric would not merge:

```
2010/11/03-13:39:14, [FABR-1001], 903,, WARNING, RB1, port 4, domain IDs overlap
```

**Device Connectivity Verification — The name-server command**

Below shows the output from the two `name-server` commands:

```bash
RB2# show name-server brief
{ 021e00
1 entries }

RB2# show name-server detail
{ 021e00; 3;10:00:00:05:33:26:57:49;20:00:00:05:33:26:57:49
SCR: 3
FC4s: FCP
IP address: PortSymb: [77] "Brocade-1020 | 2.2.0.0 | DL380-113107 | Windows Server 2008 R2 Standard | N/A"
NodeSymb: NULL
Fabric Port Name: 20:1E:00:05:1E:CD:42:6A
Permanent Port Name: 10:00:00:05:33:26:57:49
Device type: Physical Initiator
Port Index: 30
Share Area: No
Redirect: No
total number of 1 entries }
```
VLAN Interfaces

VLANs allow you to isolate network traffic between virtual networks thus reducing the size of administrative and broadcast domains. By default, all the DCB ports are assigned to VLAN 1 (VLAN ID equals 1). The `vlan_ID` value can be 1 through 3583. VLAN IDs 3584 through 4094 are internally-reserved VLAN IDs. Traffic between VLANs must be routed. VLAN membership is configurable on a per interface basis.

Default VLAN Values

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>1</td>
</tr>
<tr>
<td>FCoE VLAN</td>
<td>1002</td>
</tr>
<tr>
<td>Edge control VLAN</td>
<td>4095</td>
</tr>
<tr>
<td>Fabric control VLAN</td>
<td>4093</td>
</tr>
</tbody>
</table>
Taking the Test

After the Introduction Screen, once you click on **Next**, you will see the following non-disclosure agreement:

**IMPORTANT: PLEASE READ THE FOLLOWING BROCADE NON-DISCLOSURE CONFIDENTIALITY AGREEMENT CAREFULLY BEFORE TAKING THIS EXAM.**

The following Non-Disclosure Confidentiality Agreement (the “Agreement”) sets forth the terms and conditions of your use of the exam materials as defined below.

The Disclosure to you of this Exam and any questions, answers, worksheets, computations, drawings, diagrams, or any communications, including verbal communication by any party, regarding or related to the Exam and such Exam Materials and any derivatives thereof is subject to the Terms and Conditions of this Agreement.

You understand, acknowledge and agree:

- That the questions and answers of the Exam are the exclusive and confidential property of Brocade and are protected by Brocade intellectual property rights;
- That you may not disclose the Exam questions or answers or discuss any of the content of the Exam Materials with any person, without prior approval from Brocade;
- Not to copy or attempt to make copies (written, photocopied, or otherwise) of any Exam Material, including, without limitation, any Exam questions or answers;
- Not to sell, license, distribute, or give away the Exam Materials, questions, or answers;
- You have not purchased, solicited or used unauthorized (non-Brocade sanctioned) Exam Materials, questions, or answers in preparation for this exam;
- That your obligations under this Agreement shall continue in effect after the Exam and, if applicable, after termination of your credential, regardless of the reason or reasons for terminations, and whether such termination is voluntary or involuntary.

Brocade reserves the right to take all appropriate actions to remedy or prevent disclosure or misuse, including, without limitation, obtaining an immediate injunction. Brocade reserves the right to validate all results and take any appropriate actions as needed. Brocade also reserves the right to use any technologies and methods for verifying the identity of candidates. Such technology may include, without limitation, personally identifiable information, challenge questions, identification numbers, photographic information, and other measures to protect against fraud and abuse.

Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable by you.

By clicking on the "A" button (“YES, I AGREE”), you are consenting to be bound by the terms and conditions of this agreement and state that you have read this agreement carefully and you understand and accept the obligations which it imposes without reservation. You further state that no promises or representations have been made to induce agreement and that you accept this agreement voluntarily and freely.

A.  YES, I AGREE
B.  NO, I DO NOT AGREE