Introduction ......................................................................................................................................... 2
VC networks ....................................................................................................................................... 2
vNets and VLANs ............................................................................................................................. 2
VC link configurations ...................................................................................................................... 4
VC domain network configurations ........................................................................................................ 7
VC domain active-standby configuration ............................................................................................. 7
VC domain active-active configuration ................................................................................................ 8
Configuring additional uplinks using LACP .......................................................................................... 8
Multi-enclosure stacking ..................................................................................................................... 9
VC converged network configuration .................................................................................................. 11
LAN and SAN operation in VC domains .............................................................................................. 12
VC with Fibre Channel networks ...................................................................................................... 13
Effect of VC converged networks on SAN traffic .............................................................................. 15
Optimizing networks in VC domains .................................................................................................... 16
VC fault tolerance and load balancing ............................................................................................... 16
Load balancing with the LACP (802.3ad) algorithm ............................................................................. 17
SmartLink ...................................................................................................................................... 18
Fast MAC Cache Failover ............................................................................................................... 18
Network loop protection ..................................................................................................................... 19
Summary .......................................................................................................................................... 19
Appendix: Standard networking terms and those associated with Virtual Connect ......................... 20
For more information .......................................................................................................................... 22
Introduction

When HP introduced Virtual Connect (VC) technology in 2007, it represented an entirely new way of connecting HP server blades to external networks. Since then, VC has become one of the most used technologies for server-to-server and server-to-network connections in an HP BladeSystem environment.

Server virtualization and migration tools create high-volume machine-to-machine traffic flows that affect administrator practices. Virtual networks blur traditional boundaries between network and server administration. Adopting more virtualized, dynamic application environments and new cloud-based delivery models drives a new set of technology requirements across servers, storage, and networking domains. As a result, network architects, designers, and all administrators should understand how VC integrates into their server networks and how data traffic flows from logical servers, through the VC domain, and out to external networks.

This paper examines VC networking technologies that we use to control data traffic flow within the VC domain. It explains how VC networking technologies interoperate with the core network infrastructure. The Appendix defines VC and standard networking terms used in this paper.

VC networks

VC hardware abstraction lets you configure and connect physical and virtual servers. You can use HP Virtual Connect Manager (VCM) to change, move, or redeploy any server within a single VC domain. VCM is embedded firmware on the HP Virtual Connect Ethernet Module and the HP FlexFabric Module. You access all VC management functions through the VCM GUI or CLI interface.

For large multi-domain environments, we developed HP Virtual Connect Enterprise Manager (VCEM), a stand-alone software application. You can use VCEM to change, move, or redeploy any server within the VC domains that VCEM controls.

VC Ethernet modules use standard Ethernet bridge circuitry with special firmware so that they function as a configurable Ethernet port aggregator. For a specific external data center connection, only the selected server NIC ports are visible on what appears to be an isolated, private, loop-free network. The VC Ethernet module uplinks do not participate in the data center Spanning Tree Protocol or other switch management protocols that could disrupt the data center network. The VC environment supports IEEE 802.1Q VLAN tagging, 802.3ad Link Aggregate Control Protocol (LACP), and 802.1ab Link Layer Discovery Protocol (LLDP). VLAN tagging allows a shared uplink set to carry traffic from multiple networks.

vNets and VLANs

“vNet” is the term we use for a VC internal network. VC allows vNets to carry tagged (VLAN) and untagged (non-VLAN) traffic through the VC domain. VC allows you to assign specific uplinks to the same Layer 2 Network (also referred to as a broadcast domain) by using VC dedicated networks (vNets) or Shared Uplink Sets (SUS). When a frame is broadcast within a vNet, only ports assigned to the vNet receive the broadcast frame, unless an external device bridges multiple vNets.

Within the VC domain, there are three types of ports:

- **VC downlinks** are non-visible ports that directly connect to server NIC ports through the enclosure midplane. Their only role is to provide connectivity to directly connected server blade NICs.

- **VC uplinks** are visible ports on the VC Ethernet module faceplate that provide external connectivity for the VC domain. Their roles include stacking link, network analyzer port, and normal mode (providing external connectivity).

- **Internal cross-connects** are ports that are not visible which interconnect two horizontally adjacent VC Ethernet modules. Their only role is to function as a stacking link.
Most often, you will assign VC uplinks to the vNets to provide network connectivity. In VC, you associate a vNet with a VC Ethernet module or modules and with one or more uplinks on those modules. Next, you associate physical NICs (pNICs) or virtual NICs (vNICs) on the server with one or more vNets. Assigning more than one VC uplink to the same vNet provides network redundancy, load balancing, or both for the servers (within an enclosure) assigned to that vNet. The VC uplinks then present one or more MAC addresses to the external network.

A vNet without uplink ports can provide server-to-server communication. Server NIC ports assigned to the same vNet can communicate directly with one another without exiting the enclosure. For example, in Figure 1, Server Blade 1 and Server Blade 2 can communicate with each other within the VC Domain. VC can also isolate server NIC ports in different vNets (at Layer 2). Server Blades 3 and 16 in Figure 1 are isolated.

**Figure 1:** Multiple vNets can provide server-to-server communication and VLAN isolation.

A vNet does not always represent a one-to-one correlation with a VLAN. VC network configurations such a VLAN tunnel or SUS pass multiple VLANs between an upstream switch and server downlinks.

When you move a server profile, the vNet assignments and any managed MAC addresses move with the profile. This means you can easily move a server’s Ethernet connectivity profile without help from the network administrator.

You cannot use a vNet to bridge multiple VC uplinks for connectivity between two external devices or to connect two external networks. VC is not a transit device, and you cannot configure it as one.
VC link configurations

As of VC 3.30, you can have both mapped and tunneled networks within the same domain. VC now controls VLAN tunneling support on a per-network basis instead of by domain. You can enable or disable VLAN tunneling when adding or modifying a network with a dedicated uplink. You cannot tunnel networks associated with a SUS because they’re already mapped.

Dedicated links don’t have to be tunneled; they can handle multiple VLANs. You can use both dedicated and SUS links for aggregation, load balancing, and failover. You can use SUS to provide server access to a shared pool of networks consisting of up to 1,000 VLANs per SUS within a VC domain.

When you select the “Enable VLAN Tunneling” checkbox in VCM, packets on that network—tagged and untagged—pass through the dedicated uplink with no changes. If you don’t select the Enable VLAN Tunneling checkbox, the dedicated uplink ports in that network will only pass untagged packets.

Figure 2 shows how FlexNIC connections of Flex-10 and FlexFabric adapters and modules handle VLANs as they travel through the VC domain. SUS supports both tagged and untagged VLANs, while dedicated links support untagged VLANs. Tunneling supports tagged and untagged VLANs on dedicated links.

---

**Figure 2:** Data travels through SUS, dedicated, and tunneled links (left to right) simultaneously.

<table>
<thead>
<tr>
<th>Server NIC</th>
<th>FlexNic transmits Packet</th>
<th>Packet Enters VC module</th>
<th>Packet Exits VC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shared Uplink Set (SUS)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS sends untagged packet</td>
<td>FlexNIC adds tag</td>
<td>VC replaces FlexNIC tag with vNet tag</td>
<td>VC translates vNet tag upon uplink egress</td>
</tr>
<tr>
<td>OS sends tagged packet</td>
<td>FlexNIC adds tag</td>
<td>VC replaces FlexNIC and OS tag with vNet tag</td>
<td>VC translates vNet tag upon uplink egress</td>
</tr>
</tbody>
</table>

| **Dedicated Uplink** | | | |
| OS sends untagged packet | FlexNIC adds tag | VC replaces FlexNIC tag with vNet tag | VC removes tag upon egress |
| OS sends tagged packet | FlexNIC adds tag | VC drops packet | Nothing is transmitted |

| **VLAN Tunneling - Dedicated Uplink Only** | | | |
| OS sends untagged packet | FlexNIC does not add tag | VC does not add tag | VC passes packet unchanged |
| OS sends tagged packet | FlexNIC does not alter or add tag | VC does not alter or add tag | VC passes packet unchanged |
**SUS and mapping**

A SUS is a VC-specific term equivalent to a “trunk” or “VLAN trunk.” A SUS can carry multiple vNets over the same physical link. Each vNet uses a specific VLAN tag to identify it on that SUS, as shown in Figure 3 (VC Uplink 2). The SUS forwards VLAN traffic based on the VLAN tags and vNet’s rules.

![Figure 3: This VC domain displays various uses of vNets.](image)

When you configure VC support for VLAN tagging on a vNet, VC maps the VLAN. Mapping means that VC interprets the VLAN tag that the server operating system assigns to frames. Based on that tag information, VC classifies each frame’s VLAN membership by inserting and removing tags as VLANs enter and exit the VC domain.

SUS allows you to configure an uplink from the server NIC to the VC module with multiple vNets for mapped VLANs. The VLANs can be from any uplinks within the VC domain. To use a SUS and mapping, you must configure the server OS to handle tagged traffic.

The vNets use IEEE 802.1Q-in-Q VLAN tagging by default. In this mode, the vNet keeps all frames within the same Layer 2 domain (vNet). VC, however, allows the frames to carry different VLAN tags from the external network all the way to and from the server NIC ports. See VC Uplink 2 in Figure 3.

SUS manages uplink redundancy in the same way as individual vNets. When you assign multiple uplinks to a SUS, the uplinks can operate in failover-only mode or as link aggregation groups (LAGs). Also, all VLANs and associated vNets within a single SUS use the same active uplink or the same active LAG.

**SUS compared to dedicated links and tunneling**

We designed SUS to allow for intuitive server-to-VLAN connectivity management and environments where aggregation provides access to multiple-link configurations. Multiple links allow redundancy, failover, and load balancing.
Tunneling is simply a pass-thru for VLANs. You can create vNets that support both mapped and tunneled VLANs at the same time. Tunneled and mapped vNets cannot share the same VC module uplink port(s).

Dedicated links and tunneling are most appropriate if you have not adopted VLAN architecture in your network or if you want to segment traffic by using a different vNet. Tunneling uses a single dedicated vNet to pass many VLANs with no changes to the VLAN tags. In effect, tunneling uses the VC Ethernet module as a transparent VLAN pass-through module.

Tunneled and mapped vNet connections can coexist in the same server profile. They can even coexist on the same physical port, but on different FlexNICs. In such a configuration, the “Multiple Networks” VC server profile feature only works with mapped vNets. This feature allows sharing server links among multiple networks.

**SUS connection modes and link aggregation**

VCM supports two different mechanisms for specifying a SUS connection: Auto mode (the default) and Failover mode.

When you choose Auto mode, VCM uses the uplinks in an attempt to form aggregation groups using LACP, and to select the active path to external networks. The active path selection in the link aggregation process also determines fault tolerance. You can read more about active path selection and fault tolerance in the “Optimizing networks in VC domains” section of this paper.

Aggregation groups require one of these alternatives:

- Multiple ports from a single VC-Ethernet module connected to a single external switch that supports automatic formation of LACP aggregation groups
- Multiple external switches that use distributed link aggregation

When you select Failover mode, you must set the port to Primary or Secondary. A single link becomes the active link to the external networks while the other ports act as standby connections.

**VLAN capacity modes**

VC limits the number of VLANs in a domain and the number of server connections carrying multiple VLANs. When VCM detects 1/10 Gb (legacy) VC Ethernet modules in a VC domain, it enables legacy VLAN capacity mode. That mode has these limitations:

- 320 VLANs per Ethernet module
- 128 VLANs per shared uplink set
- 28 VLANs per server connection

Every VLAN on every uplink counts towards the 320 VLAN limit. If a shared uplink includes multiple uplinks, each VLAN on that shared uplink adds to the total uplink count. If a server connection has fewer than 28 VLANs, the remaining capacity is not available to other server connections on the same physical server port.

In a VC domain that does not contain legacy VC Ethernet modules, VCM can relax these restrictions to support more VLANs and provide more flexibility of mapping VLANs to server connections. When VCM detects no legacy modules in the domain, it lets you select a new domain mode called Expanded VLAN Capacity mode. The ability to add VLANs per domain and to allocate VLANs among the server connections for a physical port give you more options when configuring a VC environment.

Expanded VLAN capacity mode raises support limits:

- Up to 1000 VLANs per domain
- Up to 1000 VLANs per shared uplink set
• Up to 162 VLANs per physical server port, with no restriction on how those VLANs are distributed among the server connections mapped to the same physical server port
• Up to 162 VLANs per server connection

VC domain network configurations

A VC domain network includes the VC BladeSystem adapters (or FlexFabric Adapters), the VC interconnect modules, and all the network links between these two devices, up to the server-network edge. The VC network handles LAN and SAN traffic as separate or as converged network streams, depending on the VC network configuration and VC hardware used. You must use at least one VC Ethernet or FlexFabric module in any VC configuration, because the HP Virtual Connect Manager (VCM) resides on these modules. Non-converged VC infrastructures use both VC Ethernet and VC Fibre Channel modules to handle LAN and SAN traffic.

VC domain active-standby configuration

The VC domain active-standby configuration defines a single vNet to connect a server to a network. The upstream network switch connects a network to a single port on each VC module. Figure 4 shows basic network architecture for a single-enclosure VC domain in a redundant, active-standby configuration.

Figure 4: This active-standby configuration uses a single Ethernet uplink from Port 1 on Module 1 in Bay 1 on the first network switch and a single uplink from Port 1 on Module 2 in Bay 2 to Port 1 on the second network switch.

In the configuration illustrated in Figure 3, the upstream network switch connects a network to a single port on each VC module. VC requires no special upstream switch configuration because the switch is in the factory default configuration, typically as an access port. The hardware configuration requires an HP BladeSystem c7000 enclosure with one or more server blades and two VC Ethernet modules installed in bays 1 and 2. The configuration also requires one or two external network switches.
Because VC does not appear to the network as a switch and is transparent to the network, any standards-based, managed switch will work with VC.

VC domain active-active configuration

You can configure VC domains in an active-active configuration like the example in Figure 5. It is a single-enclosure VC domain configured with two VC modules. Active-active configurations make more uplink bandwidth available to the servers and reduce the oversubscription rates for server-to-core network traffic.

**Figure 5:** This is an example of multiple, simple networks configured with active-active uplinks and optional link aggregation 802.3ad (LACP) in a Microsoft Windows environment.

This active-active configuration has two separate vNets. Each vNet has a single uplink to a VC module. The upstream network switch connects a network to a single port on each VC module. The hardware configuration requirements are the same as those for the active-standby scenario.

Configuring additional uplinks using LACP

If you need more uplink bandwidth or redundancy, you can configure additional uplinks for an existing vNet. There are two options for configuring additional uplinks, the Auto and Failover connection modes discussed earlier in this paper.

In the first option, you can configure all uplinks within a vNet to connect a single VC module to a single upstream switch, making all links active. LACP requires you to configure the upstream switch for link aggregation on these ports and to include the switch in the same link aggregation group. That makes all active links within the vNet available for additional bandwidth.

The second option lets you configure some of the uplinks within a vNet to connect a VC module to different upstream switches or to connect multiple VC modules to a single or multiple switches. As a result, some links are active and the others are on standby.

Figure 6 shows the first option where all uplinks connect to a single external switch in an active-active configuration.
Multi-enclosure stacking

Single VC domains can occupy up to four physically linked enclosures in a configuration called multi-enclosure stacking. You can implement multi-enclosure stacking with module-to-module links. Multi-enclosure stacking gives you additional configuration flexibility:

- It provides connectivity for any blade server to any uplink port in the VC domain
- It reduces expensive upstream switch port utilization requiring fewer required cables for uplink connectivity
- It supplies a 10GbE+ backbone with multi-enclosure failover
- It gives the ability to move a profile between enclosures
- Reduces data center core switch traffic because internal communication between enclosures remains inside the VC domain (for example, cluster server heartbeats or VMotion traffic)
- It weathers a failure or outage of a sustained chassis, module, uplink or upstream switch while maintaining network connectivity
- It needs fewer management touch points because multi-enclosure stacking consolidates VCM interfaces

With multi-enclosure stacking, any VC uplink on any VC Ethernet module within the VC domain can provide external connectivity for any server downlink. You can also configure VC for connectivity between any set of server downlinks on any VC Ethernet module. VC provides this flexible connectivity by stacking links between VC Ethernet modules. Stacking links let you configure and operate all VC Ethernet modules in the VC domain as a single device.

Stacking links are to a group of VC Ethernet modules what the PCI bus is for a team of server NICs—a common communication path allowing all devices to work together as one. Making an uplink into a stacking link requires no manual configuration. Simply connect two VC uplinks. When
you directly connect any two VC Ethernet modules from the same VC domain using 1 Gb or 10 Gb ports, the two modules automatically negotiate the link as a stacking link using LLDP.

Figure 7 shows two multi-enclosure stacking configurations. Enclosure 1 includes two Ethernet uplinks from ports 1 and 2 on module 1 to ports 1 and 2 on the first network switch. Enclosure 2 includes two uplinks from ports 1 and 2 on module 2 in enclosure 2 to ports 1 and 2 on the second network switch.

**Figure 7:** This multi-enclosure stacking configuration includes redundant FlexFabric modules and stacking links between the modules.

VC multi-enclosure stacking allows you to consolidate infrastructure resources further by stacking up to four c-Class 7000 enclosures together to form a VC domain. This allows you to reduce upstream switch and port utilization. It is ideal for Windows, Linux, VMware clusters, and tiered environments. Stack VC FlexFabric modules or mix them with any other VC Ethernet modules (Ethernet traffic only).

**Stacking link identification**

VC only allows stacking link connections between VC modules in enclosures to be imported into the same VC domain. VC automatically detects and enables stacking links on uplink ports not configured as uplinks of a vNet or SUS. VC then defines a number of HP specific and standard LLDP-type link value pairs that include VC module names. The links attached to the faceplate ports advertise these LLDP-type link value pairs and ensure that the modules activate a stacking link only if both modules exist on the same VC domain (Table 1). A VC module uplink attached to a non-VC module can serve as an uplink. If modules do not belong to the same VC domain, VCM blocks the stacking link. VCM blocks a VC module port configured as an uplink and then connected as a stacking link. VCM blocks the VC module port because it assumes that the network administrator wants that port to be an uplink and will not reconfigure it as a stacking link.
### Table 1: VC support for stacking links

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Stacking link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both modules on same VC domain</td>
<td>Activated</td>
</tr>
<tr>
<td>Modules not on same domain</td>
<td>Blocked</td>
</tr>
<tr>
<td>VC module uplink attached to non-VC module</td>
<td>Activated</td>
</tr>
<tr>
<td>VC module port configured as uplink, then connected as a stacking link</td>
<td>Blocked</td>
</tr>
</tbody>
</table>

For more detailed information on these and other VC configurations, see the “HP Virtual Connect Ethernet Cookbook: Single and Multi Enclosure Domain (Stacked) Scenarios”. Find it at [http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01990371/c01990371.pdf](http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01990371/c01990371.pdf)

### VC converged network configuration

When you use HP VC Flex-10 adapters and interconnect modules, VC converges the LAN traffic into 10 Gb Ethernet streams on each of the adapter’s dual ports. VC dynamically partitions the network traffic between the adapters and Flex-10 module. Dynamic partitioning allows you to adjust the partition bandwidth for each FlexNIC.

HP FlexFabric adapters and VC FlexFabric interconnect modules extend Flex-10 attributes to include Fibre Channel over Ethernet (FCoE) and iSCSI as part of the network convergence. When you use FlexFabric, storage traffic can be part of the 10 Gb link between the FlexFabric adapter and the interconnect module.

VC Flex-10 technology with FlexFabric enhances VC virtualization capabilities with dynamically partitioned 10Gb network links. FlexFabric converges LAN-SAN fabric networks within the VC domain network fabric to deliver high-performance connectivity to storage and server resources. FlexFabric networks combine three solutions:

- Network architecture that’s optimized for virtualization and high speed
- Direct-flight server-to-server connectivity with advanced security and management tools for virtualization-aware threat management
- Dynamic, virtualization-integrated network provisioning
Figure 8 shows a basic network architecture for a single-enclosure VC domain using a FlexFabric converged network in an active-standby, redundant configuration.

**Figure 8**: This VC converged network configuration includes redundant FlexFabric modules and internal links between the modules.


**LAN and SAN operation in VC domains**

Before the introduction of VC FlexFabric modules, VC required both VC Fibre Channel modules and VC Ethernet modules to handle LAN and SAN traffic within the VC domain. Even in storage-only VC Fibre Channel networks, VC required both VC Fibre Channel modules and VC Ethernet modules. This is because the VC Ethernet module contains the processor on which the VCM firmware runs. A single instance of VCM manages all network traffic within the VC domain. Now with HP FlexFabric adapters and VC FlexFabric interconnect modules, you can use both converged and uncovered LAN and SAN traffic at the same time in a single VC domain.
VC with Fibre Channel networks

A SAN fabric can consist of a single SAN switch or multiple switches. Each switch or a subset of a switch, within a SAN fabric is a single Fibre Channel (SAN) domain with a unique domain ID. All SAN fabrics can support a limited number of Fibre Channel Domain IDs. The maximum number they can support varies by vendor.

VC Fibre Channel does not consume a Domain ID. Each port of a VC Fibre Channel module is a simple Node Port (N_Port) within the fabric using N_Port ID Virtualization (NPIV) on the SAN switch port. The VC Fibre Channel modules can aggregate connectivity for a maximum of 255 physical or virtual server HBA ports through each of the module’s uplink ports. The ability to aggregate connectivity on the downlink ports varies between 128 and 256, depending on the VC Fibre Channel or FlexFabric module. This aggregation method is especially important to SAN administrators who struggle with SAN fabric segmentation and Fibre Channel Domain ID consumption. The VC Fibre Channel technology provides flexibility for server connectivity. It supports reduced and shared cabling, high-performance, and auto-negotiation of external SFP ports. VC Fibre Channel technology cleanly separates SAN and server management domains and ensures that server connectivity within each module is fault tolerant.

FlexFabric addressing

You can use either VC-assigned or factory default MAC addresses for FlexFabric adapters. A FlexFabric adapter has up to four Physical Functions per port for LAN/IP traffic. You can configure one function on each FlexFabric adapter port for storage traffic (FlexHBA). When using factory default MAC addresses, FlexHBAs also have unique MAC addresses.

For FCoE FlexHBAs, you can assign and manage MAC addresses. You can also assign World Wide Names (WWNs) from pools of managed addresses. This capability makes managing WWNs consistent for both native Fibre Channel environments and FCoE-enabled converged-network environments within the VC domains. VC FlexFabric lets you manage converged and non-converged data center infrastructure components with common management procedures. It simplifies transitioning from non-converged to converged technology.

Mapping FlexHBAs to VC SAN Fabrics

VC storage administrators define VC SAN Fabrics. A VC SAN Fabric is an object within a VC environment that represents a unique SAN. VC SAN Fabrics do not span multiple VC modules. As a result, VC SAN Fabric traffic cannot travel across stacking links from one module to another. Fibre Channel traffic that travels to or from servers attached to a VC module must be forwarded to or from the Fibre Channel uplinks on that module.

You can assign each FlexHBA on a physical port to a different vNet or VC SAN Fabric, depending on the personality of the FlexHBA function. "Personality" refers to the Fibre Channel or iSCSI function assigned to a FlexFabric FlexNIC. Because iSCSI traffic uses regular Ethernet protocols, you can assign iSCSI traffic to a vNet.

You can assign one or more Fibre Channel uplinks on a module to the same VC SAN Fabric. The VC module checks the fabric login information to make sure that all the Fibre Channel uplink ports connect to the same external SAN Fabric.

You can assign server Fibre Channel or FCoE ports to only one VC SAN Fabric, so the ports can connect to only one external SAN fabric. VC modules use Fibre Channel N_Port mode operation on the Fibre Channel uplink ports. This will load-balance each server’s connection to a VC SAN Fabric as an N_Port ID Virtualization (NPIV) login across all VC SAN Fabric uplinks attached to the same external SAN fabric.
You can assign an FCoE FlexHBA function on a physical port to any VC SAN Fabric on the module connected to that FlexHBA. If you don’t assign the FlexHBA function to a VC SAN Fabric, the FCoE FlexHBA function reports a logical “link down” condition.

You can assign an iSCSI FlexHBA function on a physical port to any vNet. You can assign an iSCSI FlexHBA either to a vNet dedicated for iSCSI storage traffic, or to a vNet shared with NIC/IP FlexNIC traffic. The iSCSI FlexHBA function reports a logical link down condition if it is unassigned.

In typical environments, you will connect the FCoE (or iSCSI) FlexHBA functions to different VC SAN Fabrics (or vNets) for redundant storage connections.

**NPIV support**

For Fibre Channel connections on VC Fibre Channel and FlexFabric modules, you must use Fibre Channel switch ports compliant with N_port_ID virtualization (NPIV). It allows connecting the VC Fibre Channel modules to any switch supporting the NPIV protocol, such as data center Brocade, McData, Cisco, and Qlogic Fibre Channel switches. But you cannot connect VC Fabric uplink ports directly to a storage array because the array has no NPIV support.

Fiber Channel Standards are the basis for VC Fibre Channel and VC FlexFabric modules. The modules are compatible with all other switch products compliant with the NPIV standard. Because these modules use NPIV, they do not support special features that are available in standard Fibre Channel switches, such as ISL Trunking, QoS, and extended distances. The exception is for VC 8 Gb 24-port modules that support up to 10 km with long wave SFPs.

**VC Fibre Channel multiple-fabric support**

VC Fibre Channel supports multiple SAN fabrics. That allows you to assign any available VC Fibre Channel Module uplinks to a different SAN fabric and dynamically assign server HBAs to the desired SAN fabric (Figure 9).
The VC 8Gb 20-Port Fibre Channel modules support up to four SAN fabrics. Each FlexFabric module also supports up to four SAN fabrics and is typically connected to Fibre Channel switches configured to run in NPIV mode. You can set the speed of the four FC configurable uplink ports for 2 Gb/s, 4 Gb/s, or 8 Gb/s.

**Effect of VC converged networks on SAN traffic**

When VC converts between FCoE and Fibre Channel at the VC domain boundary, the traffic model works just like native Fibre Channel. This traffic model prohibits using Fibre Channel stacking links between VC Ethernet modules. Where the HBAs connect to the VC Fibre Channel module, the Fibre Channel module aggregates the traffic and sends it over the uplinks to the SAN. In the VC FlexFabric traffic flow, we’re doing only one more thing to native Fibre Channel. We’re converting it to FCoE, but the traffic routing rules work the same. VC doesn’t move FCoE over stacking links. Fibre Channel traffic has the same entry and exit points on the VC module. This feature maintains side A /side B fabric separation of storage traffic. The separation is crucial for SAN storage design.

**FCoE and Enhanced Transmission Selection**
Converged traffic in the VC domain affects LAN traffic, but it does so using methods based on the Enhanced Transmission Selection (ETS) standard. The ETS standard defines the logic an Ethernet port uses to select the next frame sent from multiple traffic class queues. Traffic Class Groups is the term for the ETS priority mechanism. Using Traffic Class Groups, you can combine one or more traffic classes (priorities) into a group and allocate a minimum guaranteed bandwidth to that group. ETS formalizes
the scheduling behavior of multiple traffic classes, including strict priority and minimum guaranteed bandwidth capabilities. ETS enables fair sharing of the link, better performance, and metering.

VC lets you configure FCoE bandwidth as part of VC server profiles and automatically applies that bandwidth allocation. VC FlexFabric FCoE bandwidth allocation works just like unconverged VC Flex-10 applications, but FlexFabric combines the LAN and SAN bandwidth allocations in the FCoE stream. VC automatically applies ETS management to the FlexFabric bandwidth allocation set in the server profile. ETS management then provides central control of all traffic classes without user intervention.

In a non-VC environment, you must typically configure converged LAN and SAN bandwidth manually on a server-by-server basis.

**FCoE traffic conversion**

When a FlexFabric module receives converged traffic from a downlink port, VC converts it to Fibre Channel as the uplink passes through the FlexFabric module. At the same time, the FlexFabric module manages VC LAN traffic. This feature includes server-to-core traffic exiting the module uplinks and server-to-server traffic moving through stacking links.

**Traffic flow differences for FCoE and iSCSI**

Significant differences exist in the way that VC manages FCoE and iSCSI. Just as in external networks, VC iSCSI traffic follows standard LAN traffic rules, and FCoE follows Fibre Channel traffic rules. iSCSI follows LAN routing rules and can co-exist with LAN traffic on stacking links. You can share iSCSI on the same vNet as LAN traffic, or you can create separate vNets for iSCSI traffic.

**Optimizing networks in VC domains**

Without the proper safeguards, VC domains would have the same issues with fault tolerance, load balancing, failover, congestion, and loop avoidance as external networks. VC employs many of the industry standard methods used to manage these issues in conventional networks.

**VC fault tolerance and load balancing**

You can configure VC to provide both fault tolerance and load balancing for VC networks and the associated server NIC ports. You can set the vNet’s connection mode to “Failover” for fault tolerance operation, or to the default Auto mode for fault tolerance plus load balancing. Auto mode assigns multiple VC uplinks to the same vNet and uses the Link Aggregate Control Protocol (LACP) to negotiate a LAG (or SUS). If LACP negotiation fails, the vNet operates in fault tolerance mode only. VC uses one VC uplink port as the active port while all other VC uplink ports remain in standby (blocking) mode (Figure 10).
In selecting active uplinks, VC calculates path cost. Path cost considerations include selecting the optimal root bridge path and the point where the active uplinks terminate. Active path selection is also part of the VC loop prevention mechanism.

A vNet will failover from one uplink to another whenever the active uplink loses connectivity. As soon as VC detects link loss on the active uplink, VC chooses a new active uplink from the available standby uplinks assigned to the same vNet. This process of choosing a new active uplink typically occurs in less than 5 seconds. If the previous active uplink is restored and if it is the preferred uplink, VC automatically fails back to it. An uplink is preferred if it has more bandwidth or if more server NICs are connected to the VC module where it resides.

Load balancing with the LACP (802.3ad) algorithm

The VC implementation of the LACP protocol uses a load-balancing algorithm to distribute frames across the physical ports within the LAG. The biggest concern in distributing frames across multiple physical ports is frame ordering. Optimally, for any communication between two network devices (for example, FTP transfer or telnet session), the network infrastructure delivers the frames in the order that the transmitter sent them. This structure minimizes frame reordering on the receiver end. TCP provides header information for putting frames back into the correct order, but other protocols, such as UDP, do not. This means that any load-balancing algorithm used by the LACP protocol must load balance frames and maintain frame ordering.

VC uses one of these three algorithms based on the type of frame being load balanced:

- **Source and Destination MAC addresses.** The algorithm identifies —all conversations between two MAC addresses and load-balances them all down a single link in the LAG
• **Source and Destination IP addresses.** The algorithm identifies—all conversations between two IP addresses and load-balances them all down a single link in the LAG

• **Source and Destination IP address plus TCP or UDP ports (socket).** The algorithm identifies — specific transmissions between two IP addresses and may load balance them down different links in the LAG

VC load-balances unicast frames in these ways:

- Using the socket (best method above) if it has a TCP or UDP header
- Using the source and destination IP address if it is an IP frame without a TCP or UDP header
- Using the source and destination MAC address if it is not an IP frame

VC handles broadcast, multicast, and unknown unicast (destination lookup failure) frames differently. They are load-balanced, so VC doesn’t always send these frames down the first port in the channel. The algorithm used to determine the port in the LAG is based on the source and destination MAC addresses, the source LAG number (if the source is a LAG), and module ID plus port number (if the source is a regular port and not a LAG).

VC automatically load balances traffic across the ports in a LAG. There is no user configurable setting for this function. Also, VC can use one balancing algorithm while the upstream network switch uses a different algorithm. Each side can implement its own algorithm without affecting connectivity.

**SmartLink**

SmartLink disables VC downlink physical ports (if connected to non Flex-10 ports) or individual FlexNIC ports when all VC uplinks for the associated vNet fail. SmartLink communicates via the Device Control Channel (DCC) to the FlexNICs that a link down event has occurred on a vNet’s uplinks. This feature enhances link status-based NIC teaming failover policies by detecting not only server and VC connection failures but also failures between VC and external switch connections.

Each FlexNIC tracks its individual link state, and SmartLink preserves each FlexNIC link state. If SmartLink disables a single FlexNIC, it does not force link state change even to Sibling FlexNICs, which share the same physical port.

It only takes the loss of uplink connectivity on one vNet to disable a FlexNIC. As a result, one vNet failure will disable a FlexNIC carrying multiple vNets.

**Fast MAC Cache Failover**

When a VC Ethernet uplink that was previously in standby mode becomes active, several minutes can elapse before external Ethernet switches automatically identify the connection to the c-Class server blades. Enabling Fast MAC Cache Failover causes VC to transmit Ethernet frames on newly active links. That lets the external Ethernet switches identify the new connection and update their MAC caches. This transmission sequence repeats a few times at the MAC refresh interval (we recommend 5 seconds) and completes in about 1 minute.

VC only transmits MAC Cache update frames on VLANs that you configure in the VC domain. This means the update frames are VLAN tagged appropriately for networks defined on SUS. For dedicated networks, only untagged update frames are generated, regardless of whether you enable VLAN tunneling. In a VLAN tunnel, all operating system VLAN tags pass through VC transparently. VC does not examine or record VLAN tag information in tunneled networks, and as a result, cannot generate tagged update frames.
Network loop protection

Depending on the role of the VC Ethernet port, VC can use several loop avoidance mechanisms. A VC Ethernet port can be an uplink, a downlink, or a stacking link. VC Ethernet uplink ports connect to external LAN switches. VC Ethernet downlink ports connect to server NIC ports. VC Ethernet stacking link ports connect to other VC Ethernet modules.

Loop avoidance in VC uplinks

VC Ethernet uplink ports avoid network loops with external switches. When you choose uplink ports to a vNet, the uplink ports can belong to only one vNet topology, either to a SUS or to a dedicated network. But a vNet can have zero, one, or more uplink ports.

VC server profiles establish server network connectivity by associating downlink ports to a vNET. A dedicated network consists of a single vNet (tagged or untagged packets), but a SUS contains one or more vNets (tagged packets). A vNet topology can span multiple VC Ethernet modules using stacking links. No matter how many uplinks a vNet has, only one path to the external network switch is possible. VC either combines multiple uplink ports into a single logical port (LAG or LACP), or ensures that a single physical port actively forwards traffic while the remaining uplink ports remain on standby. By ensuring there is only one network path from VC to the external switch, VC avoids a network loop between VC uplink ports and the external switch ports.

Loop avoidance in VC downlinks

VC Ethernet downlink ports are edge devices that inherently avoid network loops, if no bridging exists between server NIC ports. If you mistakenly bridge NIC ports, a network loop may occur. The VC Network Loop Prevention feature detects bridged NIC ports and disables the offending port. The loop prevention feature activates when a downlink port receives inappropriate multicast packets, such as Per-VLAN Spanning Tree + Bridge Protocol Data Unit (PVST+ BPDU) packets from a server NIC.

Loop avoidance in stacked VC modules

VC stacking links form only when VC modules automatically discover other VC modules that are part of the same VC domain. VC stacking links allow a network topology to span multiple VC Ethernet modules. VC stacking links between a pair of VC modules consist of one or more cables. Multiple stacking links between the same pair of VC modules automatically form a link aggregation group or LAG. Within the VC domain, LAGs are also known as SUS.

VC stacking links avoid network loops by using an internal Layer 2 loop avoidance protocol. When you stack multiple VC modules together, the internal Layer 2 protocol calculates the optimal path to the root bridge, which is always the module with the active uplink port(s). Each stacked module seeks a single, optimal network path to the root bridge. Any alternate paths block network traffic, preventing network loops within the VC domain. Each network topology has only one root bridge at a time. Network topologies without uplinks usually assign the VC module with the lowest MAC address as the root bridge. The VC stacking link’s loop avoidance protocol only transmits from stacking link ports, and never from downlink or uplink ports.

Summary

VC provides a Layer 2 network domain for uplink-downlink communication to external networks. The same Layer 2 domain accommodates server-to-server traffic within the enclosure and between connected enclosures by using stacking links. VC network mechanisms are based on accepted network standards and implementations such as VLAN tagging, LLDP, and LACP. VC uses fault tolerance and load balancing mechanisms in conjunction with tools such as SmartLink and Fast MAC Cache Failover to ensure optimal network performance and stability. All of these VC network capabilities are available and configurable through a single VCM GUI interface, VCM CLI, or remote console.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated link</td>
<td>Operates as a simple vNet passing untagged frames, or as a vNet tunnel passing tagged frames for one or many VLANs</td>
</tr>
<tr>
<td>Downlink</td>
<td>An internal port (enclosure midplane) on an Interconnect Module (blade switch or Virtual Connect) that directly connects to a server blade’s NIC port.</td>
</tr>
<tr>
<td>External Network</td>
<td>The network and associated network devices external to the VC domain</td>
</tr>
<tr>
<td>Flex-10</td>
<td>Technology that provides the ability to divide a 10 Gb NIC port into four Flex NIC connections with configurable bandwidth. Each FlexNIC appears to the operating system as a separate physical device with its own driver. This functionality requires a Flex-10 capable NIC and a Flex-10 capable VC module.</td>
</tr>
<tr>
<td>FlexFabric module</td>
<td>Similar to Flex-10 module except it provides the ability to divide a 10 Gb NIC into four FlexNICs or three FlexNICs and one FlexHBA. The FlexHBA can support FCoE or iSCSI.</td>
</tr>
<tr>
<td>FlexHBA</td>
<td>See FlexFabric module above</td>
</tr>
<tr>
<td>Flex-NIC</td>
<td>See Flex-10 above</td>
</tr>
<tr>
<td>IEEE 802.1Q-in-Q</td>
<td>This IEEE standard is also called 802.1ad Q-in-Q and is commonly referred to as &quot;Q-in-Q&quot; tag stacking. Q-in-Q is an amendment to IEEE’s 802.1Q (Virtual LANs) standard enabling stacked VLANs. Q-in-Q is intended to support bridge protocols and separate instances of the MAC services for functions such as tunneling and VLAN mapping.</td>
</tr>
<tr>
<td>Internal cross-connect</td>
<td>A non-visible port that interconnects two horizontally adjacent VC-Enet modules</td>
</tr>
<tr>
<td>ISL Trunking</td>
<td>Inter-Switch Link (ISL) is a Cisco-specific implementation of trunking multiple VLANs between two Cisco switches where a single interface will carry traffic for more than one VLAN. ISL was designed to work with Ethernet, FDDI, Token Ring, and ATM.</td>
</tr>
<tr>
<td>LACP</td>
<td>Link Aggregation Control Protocol: An 802.3ad Link Aggregation configuration frame exchanged between two devices that form a port trunk\channel between them</td>
</tr>
<tr>
<td>LAG</td>
<td>Link Aggregation Group. 802.3ad terminology for a port trunk\channel group</td>
</tr>
<tr>
<td>LLDP</td>
<td>Link Layer Discovery Protocol. An IEEE protocol that provides CDP-like functionality</td>
</tr>
<tr>
<td>Logical Path</td>
<td>A single physical port or a single port channel. Both represent a single communication path.</td>
</tr>
<tr>
<td>LOM</td>
<td>LAN on Motherboard. A NIC embedded on the system board of a server.</td>
</tr>
<tr>
<td>Native VLAN</td>
<td>A network to which VC assigns all untagged incoming Ethernet</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>frames. Only one network per SUS can be designated as the native network. You can use VCM to select whether native VLAN is enabled (checked) or disabled (unchecked).</td>
<td></td>
</tr>
<tr>
<td>Port Trunk (channel group)</td>
<td>A group of two or more ports that operate as a single logical port and single logical path for the purposes of load balancing. 802.3ad and Ether Channel are both port trunking technologies.</td>
</tr>
<tr>
<td>Quality of Service (QoS)</td>
<td>A very broad term associated with network traffic classification, prioritization, queuing, marking, etc.</td>
</tr>
<tr>
<td>Server Profile</td>
<td>An object within the Virtual Connect domain that is assigned to a server bay and contains the server’s LAN and SAN connectivity settings (vNet assignments, managed MAC addresses &amp; WWNs, server boot parameters, PXE configuration, and fiber channel boot parameters).</td>
</tr>
<tr>
<td>Shared Uplink Set (SUS)</td>
<td>The VC term for configuring one or more VC uplinks as a VLAN trunk connected to a switch that uses IEEE 802.1Q VLAN trunking.</td>
</tr>
<tr>
<td>Stacking Link</td>
<td>A link that directly connects two VC ports from the same VC domain.</td>
</tr>
<tr>
<td>VC VLAN tunnel</td>
<td>When you select the Enable VLAN Tunneling checkbox in VCM, both tagged and untagged packets on that network pass through the dedicated uplink with no changes.</td>
</tr>
<tr>
<td>VC Uplink</td>
<td>An external faceplate port on an Interconnect Module (blade switch or Virtual Connect module) that directly connects to an external, upstream network device.</td>
</tr>
<tr>
<td>VC</td>
<td>Virtual Connect: Broad term used to reference all the Virtual Connect components as a whole – Converged Networking modules, Ethernet modules, Fiber Channel modules, and Virtual Connect management</td>
</tr>
<tr>
<td>VCM</td>
<td>Virtual Connect Manager: The user interface, web or CLI, used to manage a Virtual Connect domain.</td>
</tr>
<tr>
<td>VC domain</td>
<td>All VC Fiber Channel modules and all stacked VC-Enet modules within the same enclosure and under the control of the same Virtual Connect Manager.</td>
</tr>
<tr>
<td>VC downlink</td>
<td>Non-visible ports that are directly connected to server NIC ports through the enclosure midplane.</td>
</tr>
<tr>
<td>VCEM</td>
<td>Virtual Connect Enterprise Manager: An HP software product that extends management to as many as 250 VC domains from a single console.</td>
</tr>
<tr>
<td>Virtual Connect Network (vNet)</td>
<td>A logical grouping of VC ports (downlinks or downlinks and uplinks) that comprise a single layer 2 network or broadcast domain as defined within a Virtual Connect domain.</td>
</tr>
<tr>
<td>VC uplink</td>
<td>Visible ports on the VC-Enet module faceplate that provides external connectivity for the enclosure.</td>
</tr>
<tr>
<td>VLAN Trunk</td>
<td>A single physical port with VLAN tagging enabled, used to provide connectivity to one or more VLANs over the same logical path.</td>
</tr>
</tbody>
</table>
For more information

Visit the URLs listed below if you need additional information.

<table>
<thead>
<tr>
<th>Resource description</th>
<th>Web address</th>
</tr>
</thead>
</table>

Send comments about this paper to TechCom@HP.com.

Follow us on Twitter: http://twitter.com/ISSGeekatHP.