

Cisco MDS FC Bladeswitch for IBM BladeCenter Technical Overview

Extending Cisco MDS 9000 Family Intelligent Storage Area Network Services to the Server Edge

Cisco MDS FC Bladeswitch for IBM BladeCenter

The Cisco® MDS FC Bladeswitch for IBM BladeCenter delivers embedded 4-Gb Fibre Channel performance for IBM BladeCenter platforms, allowing customers to consolidate storage area network (SAN) environments with a Fibre Channel switch that delivers superior performance, lowers the cost of management, and improves use of existing storage and IBM BladeCenter resources. The integrated design frees rack space, reduces the number of components, and uses shared power and cooling within the enclosure.

Built for IBM BladeCenter environments, the Cisco MDS FC Bladeswitch for IBM BladeCenter allows a new level of deployment flexibility and network scalability. Based on the technology of the award-winning Cisco MDS 9000 Family SAN switching technology, the Cisco MDS FC Bladeswitch for IBM BladeCenter delivers an outstanding feature set coupled with 4-Gb Fibre Channel performance to blade-server switching. The Cisco MDS FC Bladeswitch for IBM BladeCenter provides network intelligence features such as virtual SANs (VSANs), quality of service (QoS), and N-port interface virtualization (NPV) plus nondisruptive software upgrades and on-demand port activation to offer the most complete embedded Fibre Channel switching available for the IBM BladeCenter, BladeCenter-T and BladeCenter-H platforms.

Figure 1. Cisco FC Bladeswitch for IBM BladeCenter



Nonblocking 4-Gb Performance

The Cisco MDS FC Bladeswitch for IBM BladeCenter delivers up to 20 nonblocking 1-, 2-, and 4-Gb Fibre Channel ports available in two configurations, determined by the Cisco On-Demand Port Activation License: 7 internal ports and 3 external ports, or 14 internal ports and 6 external ports. Each port offers line rate performance up to 4 Gb with no performance loss for integrated features such as VSANs, QoS, or Network Address Translation (NAT). Each external port on the Cisco MDS FC Bladeswitch for IBM BladeCenter also delivers line-rate performance up to 4 Gb for Inter-Switch Links (ISLs) or additional device connectivity such as storage or host bus adapters (HBAs).

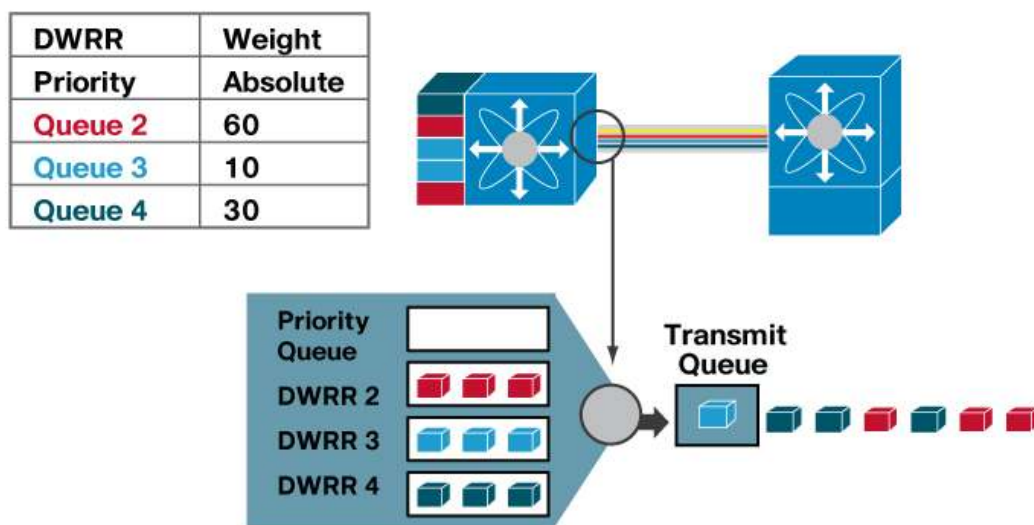
The performance of the Cisco MDS FC Bladeswitch for IBM BladeCenter is not just based on raw throughput; the switch also supports the unique Cisco Virtual Output Queue (VOQ) architecture, drastically reducing the head-of-line blocking problems found in other switching platforms that rely on a FIFO mechanism. VOQ helps ensure that each port maintains a separate set of internal buffers so that a frame that is traveling to a slow destination does not affect the performance of a frame traveling to another destination.

Another important performance feature of the Cisco MDS FC Bladeswitch for IBM BladeCenter is its capability to support QoS. The flexibility of QoS on the Cisco MDS FC Bladeswitch for IBM BladeCenter provides a simple mechanism to prioritize applications both within a switch and across the entire network. Using the proven mechanism of Deficit Weighted Round Robin (DWRR), users can determine application priority and also the weight of that priority. The Cisco MDS FC Bladeswitch for IBM BladeCenter supports four QoS queues, the first of which is absolute priority. The remaining three queues are user-definable.

Each of the three user-definable queues maintains a separate weight, with the total weight of the three queues equaling 100 percent. Although the fourth queue (absolute priority) is used for network control traffic such as Fabric Shortest Path First (FSPF) updates or zoning changes, the three user-definable queues are used for end devices. To facilitate simple management and easy operation, QoS can be activated on a per-zone basis. This simple method allows easy QoS configuration either when a zone is created or when QoS is activated.

Figure 2 shows a typical scenario in which QoS is applied within a switch and across ISLs, helping ensure performance of crucial applications during network congestion. Several devices share the same ISL for communication across the network. If the ISL becomes congested, QoS begins to prioritize traffic. Whether servers are talking to the same storage or different subsystems, QoS prioritizes output order, thereby (in this case) helping ensure that the traffic for queue 2 and queue 3 receives preferential treatment to bandwidth compared to queue 4.

Figure 2. QoS Applied on the Egress in the Switch and Across ISLs



QoS is useful in many scenarios. For example, a failure may occur as a result of a network outage or simply a storage subsystem interface failure that forces failover traffic to another interface. In both situations, bandwidth in the network can become constrained at crucial points. Activating QoS prior to a failure allows users to determine which applications should have priority.

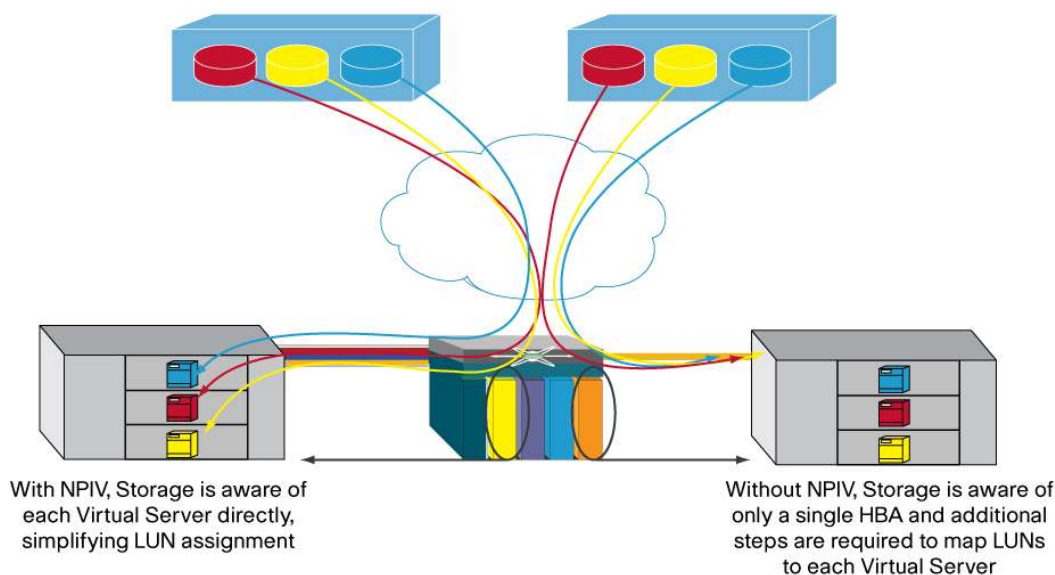
Integrated Network, Port, and Device Virtualization

Fibre Channel switches have evolved tremendously over the past several years. Intelligent network features such as VSANs, user-definable traffic management, and enhanced network security have allowed options in the SAN typically formerly seen only in Ethernet-based networks. VSANs in particular have allowed a fundamental shift in the way SANs are now designed and deployed. VSAN, an industry standard for fabric virtualization capabilities, allows more efficient storage network use by creating hardware-based logically isolated environments within a single physical SAN fabric or switch. The Cisco MDS FC Bladeswitch for IBM BladeCenter supports up to 16 VSANs per blade switch. Another major benefit of the VSAN feature is its contribution to high availability. VSANs provide not only hardware-based isolation, but also a full replicated set of Fibre Channel services for each VSAN. Therefore, when a VSAN is created, a completely separate set of fabric services, configuration management capabilities, and policies are created within the new VSAN. Examples of fabric services that are created include name server, zone server, domain

controller, alias server, and login server. This replication of services provides the capability to build the isolated environments needed to address high-availability concerns on top of the same physical infrastructure. For example, an installment of an active zone set within VSAN 1 does not affect the fabric in any way within VSAN 2.

In addition to the capability of the Cisco embedded Fibre Channel switch to virtualize the network, the switch can virtualize individual ports with support for NPIV, a technology that facilitates simplified management within virtual server environments by allowing a single host bus adapter (HBA) to be virtualized into multiple HBAs (Figure 3).

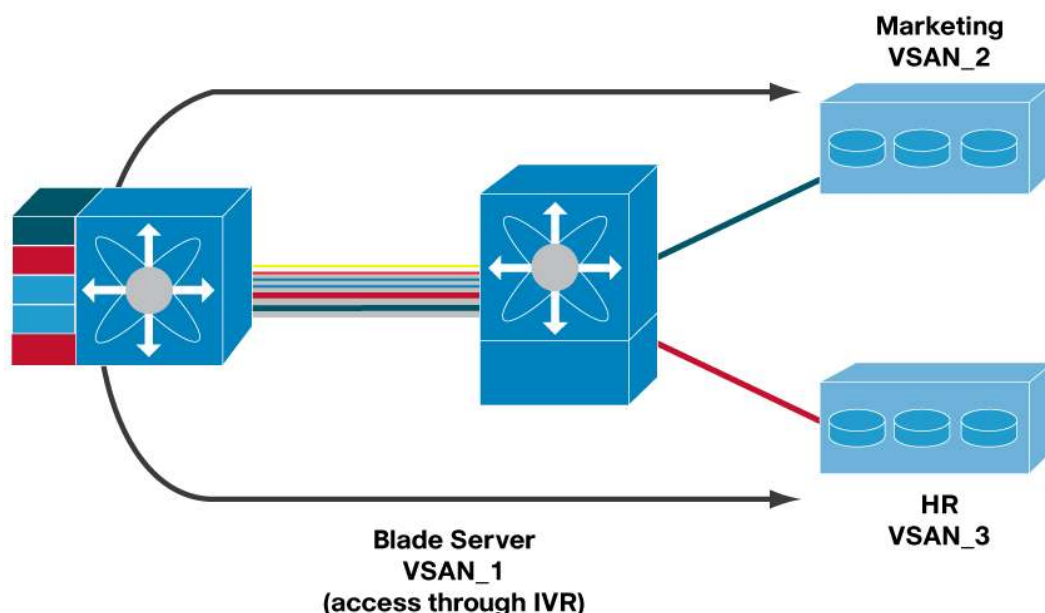
Figure 3. Example of Virtual Server Management With and Without NPIV



Activating NPIV on the switch allows a single F-port to communicate with multiple virtual HBAs represented by virtual World Wide Names (WWNs) on the physical HBA of the server. Without NPIV, all fabric functions would require an extra step to determine which virtual server was the intended resource for that WWN. With a virtual HBA assigned to each virtual server instance, logical unit number (LUN) assignment, zoning, and QoS can all be managed as they would be with separate physical servers while still maintaining the cost advantages of virtual server technology.

Increased Blade-Server Scalability

A common limitation in blade-server environments is the scalability of the domain ID addressing space defined by Fibre Channel. A domain ID is a unique address, ranging from 1 to 239, that is assigned to each switch in the network. Each blade-server chassis contains a Fibre Channel switch, so large swaths of addressing space may be consumed in large-scale blade deployments. The Cisco combination of VSANs and interactive voice response (IVR) extends the scalability of the network by creating separate addressing space for each VSAN, allowing administrators to widely deploy blade servers without affecting the scalability of the overall network (Figure 4).

Figure 4. IVR Allows Communication with Between Blade Servers and Other VSANs

Coupling VSAN technology with IVR allows blade servers to be extended throughout the entire storage network without affecting scalability and while maintaining the separation of services that VSANs provide.

Unparalleled Availability

Every IT operation is concerned about availability of the SAN environment. Connectivity between the Cisco MDS FC Bladeswitch for IBM BladeCenter and the rest of the SAN infrastructure is a crucial component of maintaining the level of availability expected in a blade environment.

Cisco PortChannels aggregate multiple physical ISLs into one logical link with higher bandwidth and port resiliency for Fibre Channel traffic. With this feature, up to 6 expansion ports (E_Ports) or trunking E_Ports (TE_Ports) can be bundled into a PortChannel to achieve a maximum of 24 Gbps of aggregate bandwidth. ISL ports can reside on any external port within the switching module, and they do not need a designated master port. Thus, if any external port fails, the PortChannel, containing the remaining ISLs, continues to function properly without requiring a fabric reconfiguration.

The Cisco SAN-OS Software uses a protocol to exchange PortChannel configuration information between adjacent switches to simplify PortChannel management, including misconfiguration detection and autocreation of PortChannels among compatible ISLs. In the autoconfigure mode, ISLs with compatible parameters automatically form channel groups; no manual intervention is required.

Cisco SAN-OS provides resilient software architecture for mission-critical deployments. A critical component of the software architecture is the ability to provide nondisruptive software upgrades for both director-class products and blade switches. In addition, the SAN-OS architecture was designed with self-healing capabilities. The SAN-OS automatically restarts failed software processes, helping ensure that any hardware or software failures on the control plane do not disrupt traffic flow in the fabric.

Network Interoperability

To ensure the easiest possible integration into an existing network, the Cisco MDS FC Bladeswitch for IBM BladeCenter supports interoperability with connectivity options for Brocade, McData, and Qlogic. The Cisco MDS FC Bladeswitch for IBM BladeCenter includes four interoperability modes to help ensure the most flexible interoperability in the industry.

- Interop Mode 1—The standards based interoperability mode, this mode interoperates with Brocade and McData switches that have been configured for their own interoperability modes.
- Interop Mode 2—This mode, also known as traditional switch interop mode 2, allows transparent integration with specific Brocade switches running in their own native mode of operation. Brocade switches must be configured with core pid = 0 to work with this mode.
- Interop Mode 3—Similar to interop mode 2, interoperability mode 3 was introduced for Brocade switches that contained more than 16 ports. With this interop mode, Brocade switches do not have to be altered from their native mode (core pid = 1).
- Interop Mode 4—This mode, also known as legacy switch interop mode 4, provides transparent integration with McData switches running in McData Fabric 1.0 interop mode.

Robust Network Security

Cisco takes a comprehensive approach to network security with the Cisco SAN-OS Software. In addition to VSANs, which provide true isolation of SAN-attached devices, Cisco SAN-OS Software offers numerous security features. The Fibre Channel Security Protocol (FC-SP) capabilities in the Cisco SAN-OS Software provide switch-to-switch and host-to-switch authentication for enterprise wide fabrics. Diffie-Hellman extensions with Challenge Handshake Authentication Protocol (DH-CHAP) are used to perform authentication locally in the Cisco FC Bladeswitch for IBM BladeCenter or remotely through RADIUS or TACACS+. If authentication fails, a switch or host cannot join the fabric.

The Cisco SAN-OS Software also provides role-based access control (RBAC) for management access of the Cisco FC Bladeswitch for IBM BladeCenter command-line interface (CLI) and Simple Network Management Protocol (SNMP). In addition to the two default roles in the switch, up to 64 user-defined roles can be configured. Applications using SNMP Version 3 (SNMPv3), such as Cisco Fabric Manager, have full RBAC for switch features managed using this protocol. The roles describe the access-control policies for various feature-specific commands on one or more VSANs. CLI and SNMP users and passwords also are shared; only a single administrative account is required for each user.

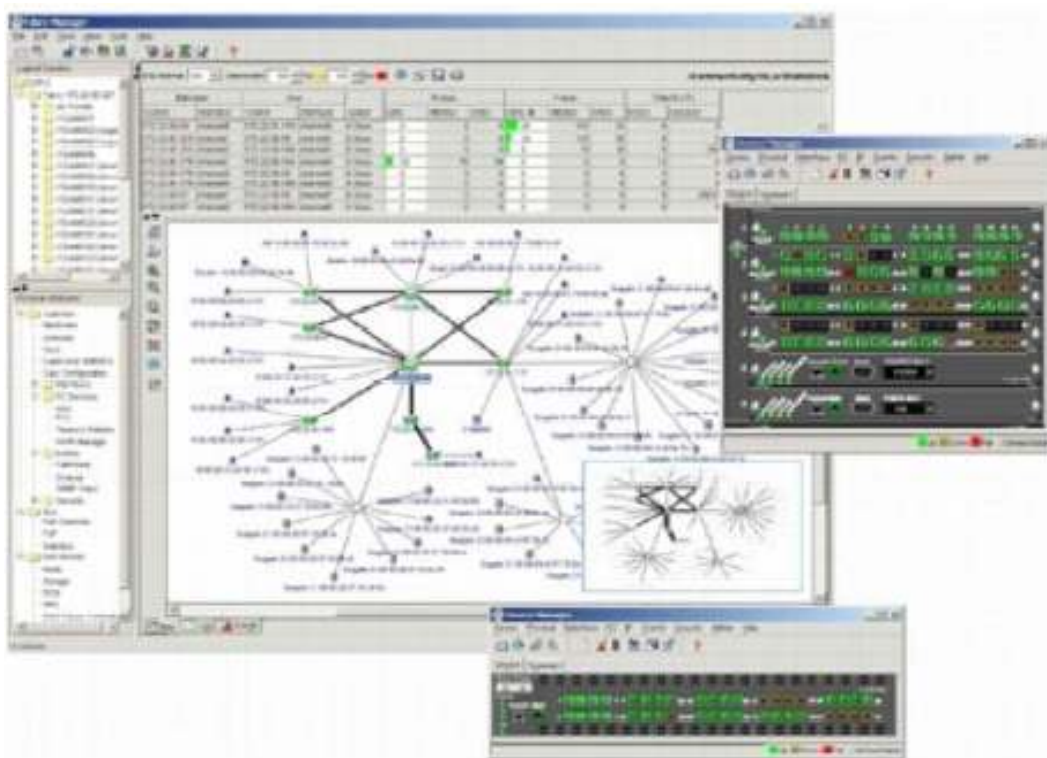
Port security locks down the mapping of an entity to a switch port. The entities can be hosts, targets, or switches that are identified through WWN. This locking helps ensure that unauthorized devices connecting to the switch port do not disrupt the SAN fabric. Fabric binding extends port security to allow ISLs between only specified switches.

Simplified Network Management

Today, large enterprise end users require management tools that are centralized and easy to use, that provide significant troubleshooting capabilities that help to resolve potential problems very quickly, and that are standards-based in an effort to integrate transparently with other management tools. Today's users are also looking for more in their management tools as they make new choices for growing their enterprise SANs, using differing protocols to create efficient business-continuance solutions, and cost-effective solutions built to withstand SAN changes.

Cisco Fabric Manager (Figure 5) is a responsive, easy-to-use, Web-based application that simplifies the management of Cisco MDS 9000 Family switches in SANs through an integrated approach to switch and fabric administration. Cisco Fabric Manager offers storage administrators fabricwide management capabilities, including discovery, multiple-switch configuration, continuous network monitoring, and troubleshooting. This powerful approach greatly reduces switch setup times, increases overall fabric reliability, and provides robust diagnostics for resolving network problems and configuration inconsistencies.

Figure 5. Cisco Fabric Manager



With the Cisco Fabric Manager intuitive GUI, storage administrators can compare switch configurations side by side, perform configuration policy checks across Cisco MDS 9000 Family switches, set alarm thresholds to report to third-party fault-management applications, view individual device and aggregate statistics in real time, and analyze historical performance statistics. All these capabilities are available through a secure interface that facilitates remote management from almost any location.

A problem common to many blade-server customers is the overhead of managing a large number of switches. Whereas a traditional server environment may have one Fibre Channel switch for as many as 400 servers, blade-server architecture may demand one Fibre Channel switch for as few

as 14 servers. With the possibility of such a large number of switches, management of the network can become difficult. Cisco SAN-OS uses the Cisco Fabric Services to simplify SAN provisioning by automatically distributing configuration information to all Cisco MDS switches in a fabric. Cisco Fabric Services enables administrators to configure features for an entire fabric from a single switch. From mundane tasks such as configuring Network Time Protocol (NTP) or advanced configuration of Inter-VSAN Routing, Cisco Fabric Services provides a simple and efficient mechanism to manage a large number of Fibre Channel switches.

Conclusion

The Cisco MDS MDS FC Bladeswitch for IBM BladeCenter is the most advanced Fibre Channel blade-switching platform available today. By integrating the technology of the award-winning Cisco MDS 9000 Family of switches and directors into a blade-switch architecture, Cisco allows SAN architects to now integrate advanced technology across the entire SAN. The advanced architecture of the Cisco MDS MDS FC Bladeswitch for IBM BladeCenter coupled with 4-Gb technology provides outstanding performance between blades and the rest of the Fibre Channel infrastructure. With its advanced virtualization capabilities and on-port activation, the Cisco MDS MDS FC Bladeswitch for IBM BladeCenter also provides cost efficiencies regardless of the deployment size.



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0701R)