Cisco N-Port Virtualizer for Large-Scale Fibre Channel Blade Switch Deployments

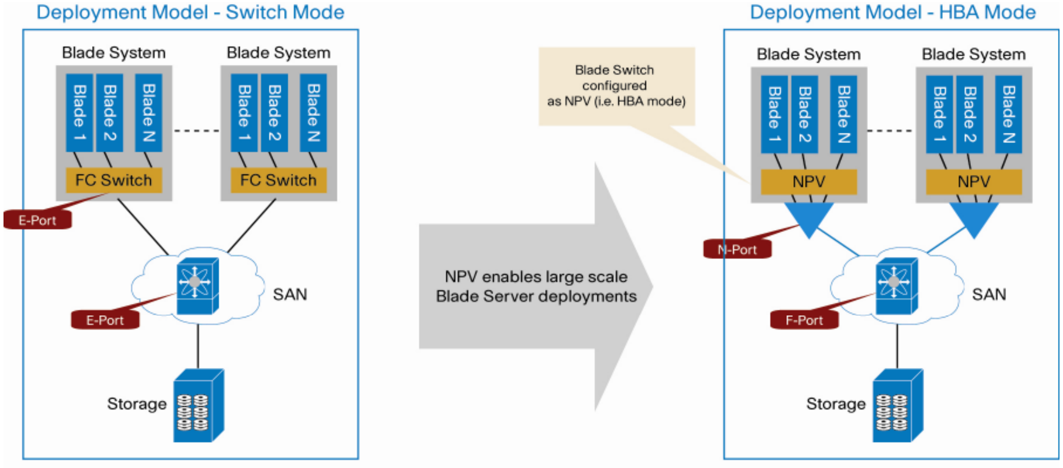
Blade switch depoyments are increasingly common among enterprise customers. Gartner claims that blade servers are the fastest growing segment of the server market. This trend means that Fibre Channel attach rates for blade server enclosures will also grow. As the scale of blade server deployment increases, however, it introduces some challenges, such as large increases in the number of domain IDs, increased server and network management complexity, and interoperability concerns in multivendor environments. The Cisco® N-Port Virtualizer (NPV) feature introduced in Cisco MDS 9000 SAN-OS Software Release 3.2(1) addresses these challenges, offering these features:

- Increased scalability by reducing the number of Fibre Channel domain IDs used
- Seamless interoperability between Fibre Channel blade switches and multivendor core storage area network (SAN) switches
- Enterprise-class high availability
- Virtual SANs (VSANs), for segmentation and fault isolation
- Advanced traffic management
- Increased operational flexibility for blade server additions, moves, and changes
- Simplified Fibre Channel blade switch management

Introduction

There are two architectural models for Fibre Channel blade switch deployment: switch and host bus adapter (HBA) models (Figure 1).

Figure 1. Fibre Channel Blade Switch Deployment Architectural Models



	Blade Switch Attribute	
Fibre Channel Switch Model (E-Port)	Deployment Model	HBA Model (N-Port)
One per Fibre Channel Blade Switch	Number of Domain IDs Used	None (Uses Domain ID of Core Switch)

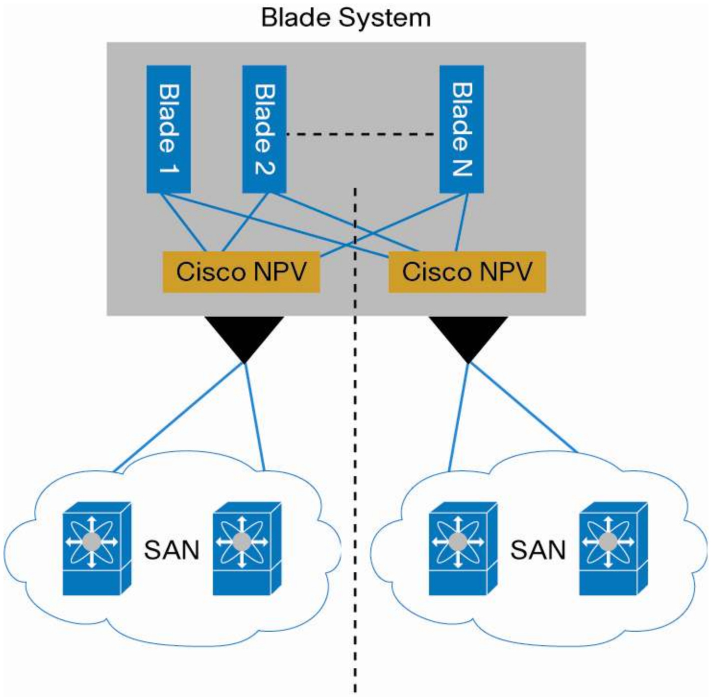
In the switch model, the Fibre Channel blade switch connects to the core SAN through an E port. In the HBA model, the Fibre Channel blade switch connects to the core SAN through an N port using N-port ID virtualization (NPIV) technology.

Key Features and Benefits of NPV

- Enhanced scalability with reduced domain ID use: One of the primary challenges in large-scale blade server deployments is the number of Fibre Channel domain IDs that are required. Each Fibre Channel blade switch in a blade server uses one Fibre Channel domain ID and provides Fibre Channel connectivity for up to 16 blade servers. For example, a 1000–blade server deployment will require up to 60 Fibre Channel blade switches, which translates to 60 Fibre Channel domain IDs. This number becomes a deployment challenge because storage OSMs(Original Storage Manufacturers) place an upper limit on the number of Fibre Channel domain IDs in a SAN. This number is typically less than 40 even though the theoretical limit is 239. Cisco NPV addresses this challenge. With Cisco NPV, the Fibre Channel blade switch behaves like an HBA, so it does not use a Fibre Channel domain ID. Instead, it gets a Fibre Channel ID (FC-ID) for the blade servers from the core SAN. Therefore, a 1000–blade server deployment will use only two or so Fibre Channel doman IDs.
- Seamless interoperability in multivendor environements: The existing switch-switch interoperability between multivendor SANs based on E-port connectivity requires configuration of special interopability modes and has to be managed carefully in an ongoing process. Cisco NPV addresses this challenge. With Cisco NPV, the Fibre Channel switch behaves like an HBA, so it provides transparent interoperability in multivendor environemnts. Thus, interoperability between Fibre Channel blade switches with Cisco NPV enabled and the core SAN is no different than interoperability today between a server connected to a SAN using N-port–to–F-port connectivity.
- Enterprise-class high availability: Cisco NPV in conjunction with inherent Cisco MDS 9000 SAN-OS Software capabilities offers enterprise-class high availability for blade server deployments. Cisco MDS 9000 SAN-OS Software supports Cisco In-Service Software Upgrade (ISSU), or nondisruptive software upgrade. With dual HBAs in the server, dual

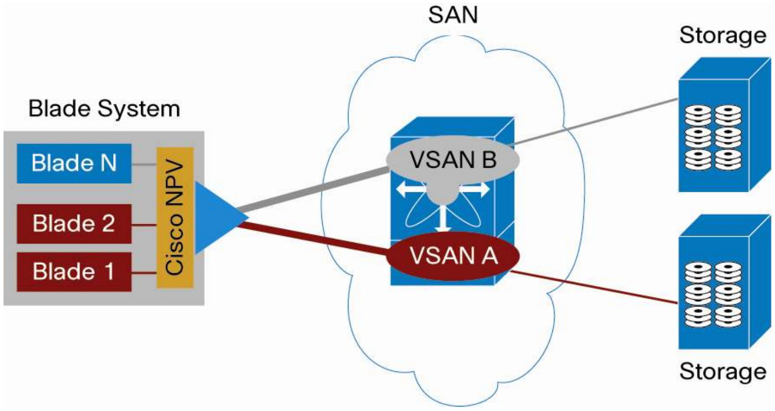
homing of servers to fabric switches and a two-core design eliminates any single point of failure. HBA failure, fabric switch failure, or link failure is handled without any loss of connectivity (Figure 2).

Figure 2. High Availability



- VSANs for segmentation and fault isolation: VSAN, an industry standard for fabric virtualization capabilities, allows more efficient storage network use through creation of hardware-based isolated environments within a single physical SAN fabric or switch. Up to 16 VSANs are supported per switch. Each VSAN supports role-based access control (RBAC), allows separate configuration and separate fabric services, and operates as a separate SAN. In the example in Figure 3, two VSANs are created and traffic is segregated. Each blade server can have an independent VSAN or a group of servers can be on one VSAN, offering maximum flexibility and resiliency. Faults or outages in one VSAN do not affect other VSANs.

Figure 3. VSANs for Segmentation and Fault Isolation

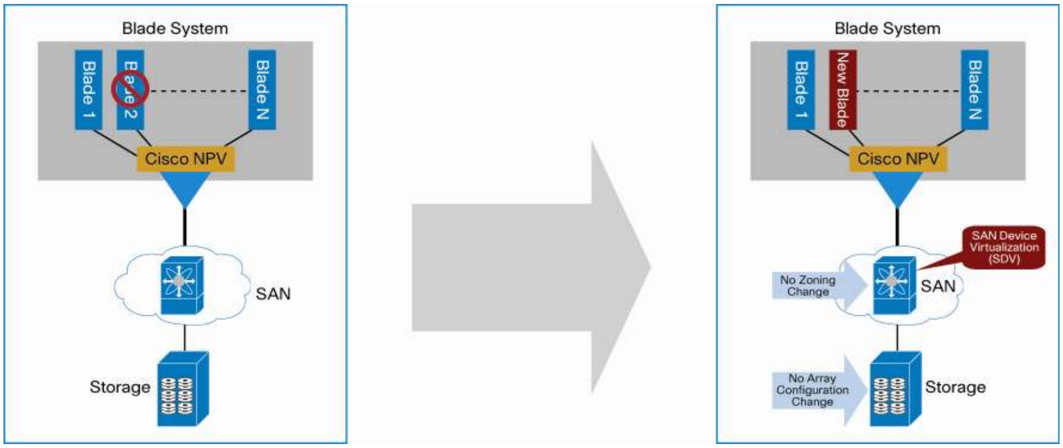


Advanced traffic management: If one or more fabric connection to the core fails, the software will automatically login the servers from the failed link to other links, helping ensure continuity in connection even during link failures. Advanced traffic management capabilities integrated into the Cisco Fibre Channel blade switches optimizes deployment as follows:

  - ◦ Virtual output queuing helps ensure line-rate performance on each port, independent of traffic pattern, by eliminating head-of-line blocking.
  - ◦ VSAN-based partitioning increases fabric efficiency and availability by sectionalizing the fabric.
  - ◦ Comprehensive port and flow statistics facilitate sophisticated performance analysis and service-level agreements (SLAs).
  - ◦ Dynamic load balancing across multiple links equalizes the number of FC-IDs per link.

- Increased operational flexibility for blade server additions, moves, and changes: The Cisco SAN Device Virtualization (SDV) feature makes it easy to add, remove, or modify blade servers without reconfiguration of the SAN and storage arrays. Without Cisco SDV, when a server fails, considerable downtime is required to bring the secondary server online because of the need for zoning changes and reconfiguration of storage arrays. Cisco SDV presents the virtual address for provisioning. When a physical device is changed, no reconfiguration is required because the virtual address remains the same and the new physical address is automatically mapped to the virtual address (Figure 4).

Figure 4. Cisco NPV Flexibility for Additions, Moves, and Changes



- Simplified Fibre Channel blade switch management: Cisco Fabric Manager is a responsive, easy-to-use, Web-based application that simplifies the management of Cisco blade switches. 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. The following feaures help simplify management:

  - End-to-end Cisco switches, so that Cisco MDS 9000 SAN-OS Software is common to all devices, thereby helping ensure a consistent feature set
  - Centralized authentication, authorization, and accounting (AAA) server for authentication
  - RBAC on a per-VSAN basis
  - Switch handled as an HBA and so requires minimal configuration and management

Specifications

Minimum Software Requirements

- Cisco MDS 9000 SAN-OS Software Release 3.2(1)

Cisco NPV Support

- IBM and HP blade switches
- Cisco MDS 9124 Multilayer Fabric Switch
- Cisco MDS 9134 34-Port Multilayer Fabric Switch

Scalability

- Up to 70 switches connected to a single external switch
- Core can have two switches to enhance resiliency (high availability), with logins load balanced across both the cores (active-active)

Cisco MDS 9000 SAN-OS Software Features

- Cisco Fabric Manager
- Port security
- Cisco Fabric Device Management Interface (FDMI)
- VSAN
- Simple Network Management Protocol Version 3 (SNMPv3) and Secure Shell (SSH)
- Cisco ISSU
- AAA and TACACS
- Cisco SDV
- Fibre Channel traceroute and ping
- Fibre Channel Security Protocol (FC-SP) for host-to-switch and switch-to-switch authentication

For More Information

For more information, visit http://www.cisco.com/en/US/products/hw/ps4159/index.html or contact your local account representative.

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.**

Printed in USA C78-421188-00 07/07