BROCADE

AT-A-GLANCE

Dedicated Networks for IP Storage

HIGHLIGHTS

- Dedicated networks for IP storage provide predictable performance, ensure proper levels of security, contain failure domains, and maximize uptime—all critical attributes for today's business-critical IP storage applications.
- Brocade® VDX® switches enable plug-and-play deployment and provide Logical Chassis management to minimize the learning curve and ongoing operational expense for storage administrators. Brocade VCS® Fabric technology and Brocade VDX switches, which are purpose-built for storage performance and resiliency, provide a robust network infrastructure ideally suited for dedicated IP storage environments.
- Brocade VDX switches deliver unsurpassed automation and a load-balanced, multipath architecture for maximum link efficiency and resiliency, and they are optimized for bursty storage traffic with deep buffers.
- Brocade VCS fabrics mirror the properties of scale-out storage with a scale-out network architecture.
- Unified storage networking management delivers unprecedented network visibility and insight across all storage networks, with Brocade Network Advisor, Fabric Vision and support for VMware vRealize.

Dedicated Networks for High-Performance, Predictable, and Resilient IP Storage

People often think of the IP/Ethernet network as one large, integrated network for all end hosts, appliances, servers, and IP storage. This is likely because over the past two decades network developers have managed to converge various disparate networks into a common IP/Ethernet network. This process began with voice convergence and continued with similar work in video and storage.

The business drivers behind the push toward a converged IP/Ethernet infrastructure are straightforward. After all, why would an organization not want a single IP/Ethernet network interconnecting everything? The economies of scale should reduce capital costs, and having fewer networks to manage should minimize complexity and reduce operational costs. And if organizations need to segment the IP network, they can do so with Virtual Local Area Networks (VLANs), Virtual Routing and Forwarding instances (VRFs), or overlays on the single shared IP/Ethernet network, right? While the theoretical benefits sound compelling, in practice organizations seldom take this approach, for numerous business and technical reasons. This also is the case with IP storage.

Dedicated IP Storage Networking Examples

The modern medium- to large-scale data center typically has many separate IP storage networks, including these:

- **Backup network:** For example, an IP-based tape/virtual tape/deduplication network driven by the need to minimize RPO/RTO thresholds.
- **IP storage back-end network:** Used to isolate node-to-node communications within a storage cluster.
- **Internet Small Computer System Interface (iSCSI) block storage network:** Segregated primarily for storage performance reasons. According to Gartner, 30 to 50 percent of iSCSI deployments use a separate dedicated network for performance.
- **vMotion network:** VMware's best-practices guide recommends a separate network for vMotion (including Storage vMotion).

- **Object store:** For data centers in which capacity is measured in petabytes or larger units, content is unstructured or semi-structured, and the need is for scale out with eventual consistency. The object store is optimized for cost and scale, as opposed to performance and transactional consistency, and is often deployed and managed separately as part of an analytics project.
- **Virtual infrastructure storage:** Provides dedicated IP storage for Virtual Machines (VMs) and their associated data—a common scale-out Network-Attached Storage (NAS) use case.
- **Replication network:** For example, distributed storage technologies in which replication is critical for redundancy and failure handling.

A dedicated network can be deployed as either a physically separate network or as a separately managed network. The need for dedication varies and can include performance and service-level guarantees, contained failure domains, security, or isolated change control and span of control.

For example, if virtual infrastructure storage is deployed to provide VM images and their associated data for a server farm, the best practice is to have a physically separate network (see Figure 1) for management, performance, security, and failure domain reasons. Using this model, end hosts or other appliances do not need to have network access, and Internet connectivity is not needed. A physically separate network also provides a separate change control domain and allows for Service Level Agreements (SLAs) specific to the virtual infrastructure storage use case.

Conversely, a new analytics pod introduced into an existing shared network can be deployed as a separate pod, with different compute, storage, and networking hardware. The pod also can be deployed and managed by a separate team and requires connectivity only into the spine of the existing data center network. In this scenario, the deployment decision is often driven by the Line of Business that owns the application or workload, not just the IT infrastructure owner.

Deployment Strategies and Best Practices

The following examples illustrate ways to deploy dedicated IP storage networks using industry best practices.

Virtual Infrastructure Storage

Consider a server farm that needs access to a large library of VMs. In this case, all virtual servers in a data center might rely on Network File System (NFS) for their boot drives, application drives, data, and more. As such, a network outage could be catastrophic to all business logic and applications simultaneously. This is in stark contrast to traditional, classic NAS deployments as a simple file share, in which outages are far less impactful.

The most recent best-practices document from VMware states:

> Private Network: vSphere implementation of NFS supports NFS version 3 in TCP. Storage traffic is transmitted in an unencrypted format across the LAN. Therefore, it is considered best practice to use NFS storage on trusted networks only and to isolate the traffic on separate physical switches or to leverage a private VLAN. All NAS-array vendors agree that it is good practice to isolate NFS traffic for security reasons.[1]

In this deployment, the NFS environment is analogous to a Storage Area Network (SAN). It should be modified only when absolutely necessary and should have a separate change-control decision-making process.

Traditionally, networks experience problems for many reasons, including misconfiguration, software defects, and human error. Physically isolating

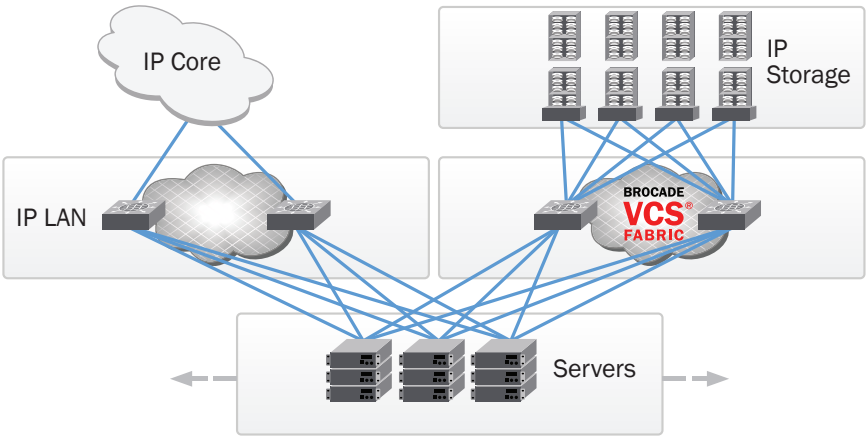

Figure 1: A physically separate IP storage network delivers predictable performance, low latency, and high availability

[1] VMware, Inc., *Best Practices for Running VMware vSphere® on Network-Attached Storage (NAS)*, Technical Marketing Documentation V 2 .0, January 2013.

the environment ensures that these disruptions are minimized to the highest degree possible, thus ensuring maximum application uptime.

This protection cannot be provided simply by isolating this traffic to specific VLANs on a shared infrastructure. Separate physical switches are the best practice.

In summary, this use case is best served by a separate physical network for security, span of control, and uptime.

iSCSI Block Storage Networking

The next example is the iSCSI SAN. Unlike NAS, these deployments often use separate dedicated network switches, as noted in the *Dell EqualLogic Configuration Guide*:

> Note: It is recommended to use a physically separated network dedicated to iSCSI traffic that is not shared with other traffic. If sharing the same physical networking infrastructure is required, then use Data Center Bridging (DCB) for EqualLogic SAN.[2]

The same guide also states:

> Several switch vendors may provide additional link aggregation options that are completely proprietary or may be extensions to one of the two previously mentioned solutions. In most cases, this type of link aggregation solution is designed to reduce or eliminate the need—and the overhead—of the Spanning Tree Protocol that must be used in the two previous options. If available, these proprietary options should be considered. They may be very useful in allowing the network administrator to create a more efficient multi-switch Layer 2 network infrastructure for a SAN.[3]

Backup Network

Dedicated backup networks are generally considered a best practice. Although the value proposition of 10 Gigabit Ethernet (GbE)—network consolidation—includes collapsing the general-purpose LAN with the backup network in the data center, many organizations have found that this adversely impacts Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO). Thus, they maintain separate backup networks to ensure optimal RPO/RTO.

The EMC Data Domain/NetBackup best-practices guide states:

> By segregating NetBackup media server and storage unit traffic from other network traffic, potential contention issues are limited to backup and recovery jobs. Known available bandwidth can be managed to achieve aggressive data protection and recovery service levels.
>
> A scalable infrastructure has been established in case data protection network bandwidth requirements change over time.
>
> While not always possible based on customer requirements and pre-existing NetBackup media server and network infrastructure deployments, the use of a dedicated backup network is preferred when compared to mixed-use network configurations.[4]

Brocade VCS Fabrics for Dedicated IP Storage Networking

To address these various use cases, Brocade is redefining networking for IP storage with connectivity solutions optimized for business-critical storage environments. Brocade VDX switches powered by Brocade VCS Fabric technology deliver performance, availability, and management similar to Fibre Channel. Brocade VCS fabric solutions eliminate Spanning Tree Protocol (STP) to deliver active-active links, doubling network efficiency and improving resilience. This flat, multipath, deterministic mesh network is ideal for IP storage environments. Storage administrators can efficiently address business-critical SLAs with resilient, high-performance fabric network architectures and can manage the network and storage holistically to significantly improve IT agility. Brocade VDX switches powered by Brocade VCS Fabric technology provide the following benefits:

- **Highly automated:** Brocade VCS Fabric technology and Brocade VDX Data Center switches are self-provisioning and self-healing and offer zero-touch scale out, delivering a 50 percent reduction in operational costs.
- **Simple to deploy and manage:** The Brocade VCS Logical Chassis feature enables an entire fabric to be treated as a single logical switch, greatly simplifying management, configuration, maintenance, and troubleshooting. It also provides a single logical interface to orchestration tools.
- **Predictable performance:** Brocade VCS Fabric technology and Brocade VDX switches are optimized for storage performance with the patented Brocade Layer 1 load balancing leveraged from Fibre Channel and Layer 2 multipathing.
- **Deep buffers:** Brocade VDX switches offer the industry's deepest buffers to handle bursty storage traffic and minimize latency and packet drops.

[2] Dell, *Dell EqualLogic Configuration Guide*, Version 14.3, October 2013.

[3] Ibid.

[4] EMC Corporation, *EMC Data Domain Boost for Symantec NetBackup Open Storage Best Practices Planning*, 2011.

- **A solution purpose-built for next-generation data centers:** High Availability (HA), In-Service Software Upgrade (ISSU), and fixed-configuration redundant power supplies and fans provide a resilient network for business-critical applications.
- **Visibility and insight across storage networks:** Brocade Fabric Vision technology, Brocade Network Advisor and support for VMware vRealize deliver visibility, management and analysis across the entire storage network environment.

The portfolio of Brocade VDX switches provides Ethernet storage connectivity for Fibre Channel over Ethernet (FCoE), iSCSI, and NAS storage solutions within a single product family (see Figure 2). IT organizations can protect their Fibre Channel investment by connecting Fibre Channel SANs to Ethernet fabrics with the Brocade VDX 6740 Switch and the Brocade VDX 6940 Switch.

For additional information about VCS Fabric technology, read the white paper *An Introduction to Brocade VCS Fabric Technology*. For more information on the Brocade VDX 6740 Switch, read the Datasheet. For details on the Brocade VDX 6940 Switch, read the Datasheet.

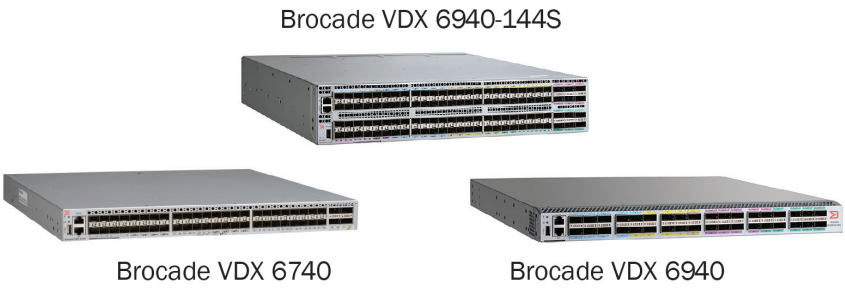

Figure 2: Brocade VDX switches designed for dedicated IP storage networks

Summary

Dedicated, private networks for IP storage have become a commonly accepted best practice in many enterprises. While applications and business reasons may vary, a common thread is the need to support the application or workload in the most effective and reliable manner possible. The goal is to ensure autonomous administrative control and operation, as well as a tight coupling of the application, compute, storage, and network, in order to achieve the objective—improved management, performance, contained failure domain, security, span of control, or IT agility.

About Brocade

Brocade networking solutions help organizations achieve their critical business initiatives as they transition to a world where applications and information reside anywhere. Today, Brocade is extending its proven data center expertise across the entire network with open, virtual, and efficient solutions built for consolidation, virtualization, and cloud computing. Learn more at www.brocade.com.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

BROCADE