DEDICATED NETWORKS FOR IP STORAGE
VDX-6740B

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 mission-critical IP storage applications.

Connectrix VCS® Fabric technology and the Connectrix VDX-6740B switch provide a robust network infrastructure ideally suited for dedicated IP storage environments.

Hallmarks of the Connectrix VDX switch include unsurpassed automation, a load-balanced, multipath architecture for maximum link efficiency and resiliency, and deep buffers to handle bursty storage traffic.

DEDICATED IP STORAGE NETWORKING EXAMPLES
The modern medium to large-scale data center typically has many separate IP storage networks, including:

- **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**: To isolate node-to-node communications within a storage cluster.

- **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**: To provide dedicated IP storage for Virtual Machines (VMs) and their associated data—a common scale-out 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. These SLA’s can be for specific performance objectives without fear of impact from other network traffic and for ease of management or troubleshooting by the storage solution providers.

![Figure 1.](image)

A physically separate IP storage network delivers predictable performance, low latency, and high availability.

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 NFS for their boot drives, application drives, data, and more. As such, a network outage could be catastrophic to all business logic/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. The VDX-6740B and their ability to self-form into fabrics that can be managed in a similar manner to traditional SANs allows the entire NAS storage solution to be delivered and managed similar to the SLAs that the storage teams require.

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

**EMC DATA DOMAIN NETBACKUP 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 and recovery time objectives. 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.²

**EMC NETWORK ATTACHED STORAGE**

EMC Unified VNX® storage systems and Isilon® scale-out NAS systems as well as the new VMAX™eNAS NAS solution greatly benefit from a dedicated IP segment. It provides predictability, low latency, traffic isolation, and performance. It can also help maintain service-level guarantees, contain failure domains, while also providing security, or isolated change and span of control.

IP networking is becoming more and more mission critical for organizations and the Connectrix VDX solution adds flexibility, performance, and ease of use to these requirements. EMC Unified VNX, VMAX3 eNAS and Isilon systems offer enterprise class IP storage for customers requiring all of the services listed above. Connectrix VDX switches with VCS fabric technology enhances the dedicated IP storage network making it a best in class solution for IP networking products.


**CONNECTRIX VCS FABRICS FOR DEDICATED IP STORAGE NETWORKING**

Connectrix VCS Fabric technology eliminates 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.

To meet the challenges of dedicated IP storage networks, Connectrix VDX switches powered by Connectrix VCS Fabric technology provide the following benefits:

- **A highly automated and simple-to-deploy solution**: VCS Fabric technology and Connectrix VDX data center switches are self-provisioning and self-healing, delivering a 50 percent reduction in operational costs.

- **Predictable performance**: Non-blocking, multipathing at network Layers 1–3 provides the industry’s best and most predictable network utilization.

- **Deep buffers**: Connectrix VDX switches offer the industry’s deepest buffers to handle bursty storage traffic and minimize latency and packet drops.

- **A solution purpose-built for next-generation data centers**: Chassis-based HA, ISSU, and fixed-configuration redundant power supplies and fans provide high availability.

Connectrix VDX provides Ethernet storage connectivity for 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 Connectrix VDX 6730 Switch.

**Figure 2.**
EMC Connectrix VDX-6740B.

**SUMMARY**

Dedicated, private networks for IP storage have become a commonly accepted best practice in many enterprises. While the 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—whether it be improved management, performance, contained failure domain, security, or span of control.

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller, visit [www.emc.com](http://www.emc.com), or explore and compare products in the EMC Store.