

## CHAPTER 7: DEPLOYING VIRTUAL SYSTEMS IN A BRIDGED CONFIGURATION

---

A Virtual System in Bridge mode performs the same functions as a Virtual Switch, while supplying extra layers of security. Such Virtual Systems, operating at layer 2, are completely transparent and do not impact the existing IP structure, the different control protocols in use for VLAN management, or the protocols used for loop detection.

### Course Objectives

1. Identify the benefits of layer-2 bridging.
2. Diagram Bridge mode deployment scenarios.



## Key Terms

- Spanning tree protocol (STP)
- Multi protocol Label Switching (MPLS)
- Bridge protocol data unit (BPDU)

COPY



## VIRTUAL SYSTEM IN BRIDGE MODE

By having a Virtual System that implements native layer-2 bridging instead of IP routing, a VSX Gateway can provide transparent security inspection.

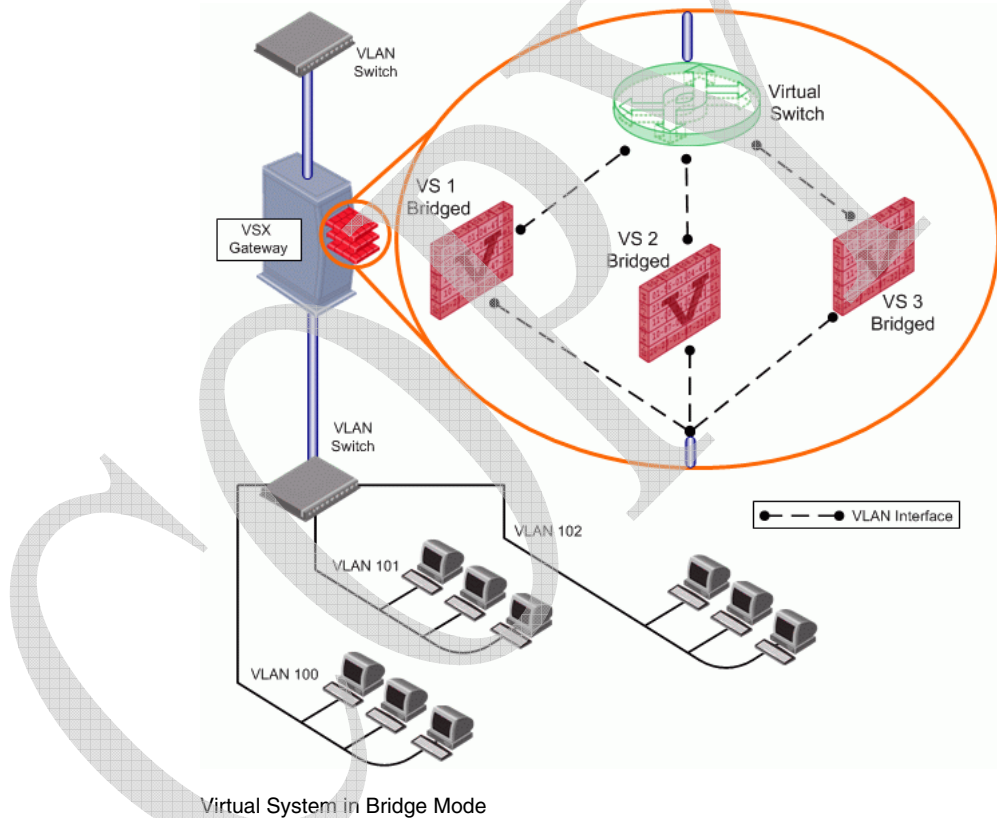
A typical network connection in such a scenario will involve a 802.1q VLAN switch on either side of the VSX Gateway. The interfaces of the bridge do not require IP addresses. The Virtual System in bridge mode remain, transparent to the existing IP network.

A Virtual System in Bridge mode:

- Has the same firewall-security capabilities of a Virtual System, except for VPN and NAT (NAT, modifies layer-3 information.)
- Enables easier configuration of Virtual Systems since no IP address or specific routing information is required.
- Does not segment an existing network.

## Security for Virtual Systems in Bridge Mode

A Virtual System in Bridge mode performs the same functions as a Virtual Switch while supplying extra layers of security, as shown in the following figure:



In the figure, each Virtual System in Bridge mode provides content inspection for each VLAN switched network without breaking the existing IP infrastructure. Thus **VS 1 Bridged** protects **VLAN 100**, **VS 2 Bridged** protects **VLAN 101**, and **VS 3 Bridged** protects **VLAN 102**.

## Core Side Security

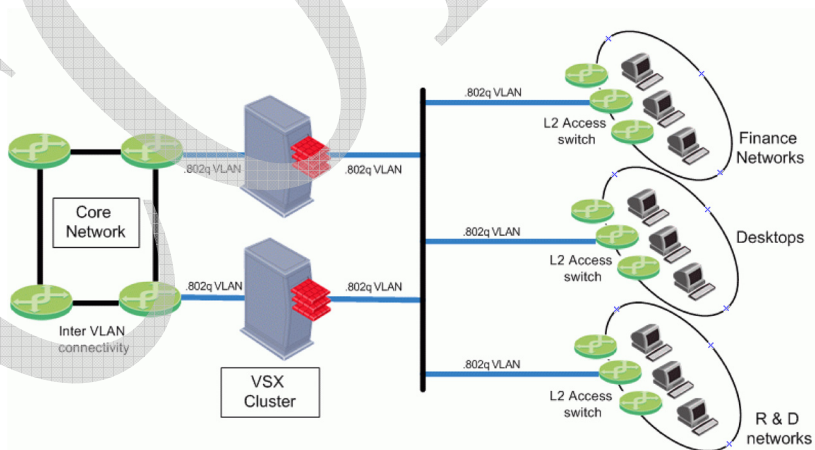
To provide a security layer for existing core networks, VSX offers Virtual Systems in Bridge mode. Such Virtual Systems, operating at layer 2, are completely transparent and do not impact the existing IP structure, the different control protocols in use for VLAN management, or the protocols used for loop detection. Assigning a Virtual System in Bridge mode to the different networks establishes security control points for the different segments.

Consider three common deployments:

- An enterprise deployment
- A service-provider deployment
- A data-center deployment

### ENTERPRISE DEPLOYMENT — INTERNAL SECURITY

Situated next to the core switches, VSX secures the internal network, adding a security layer at either level 2, level 3 or both, as shown in the following figure:



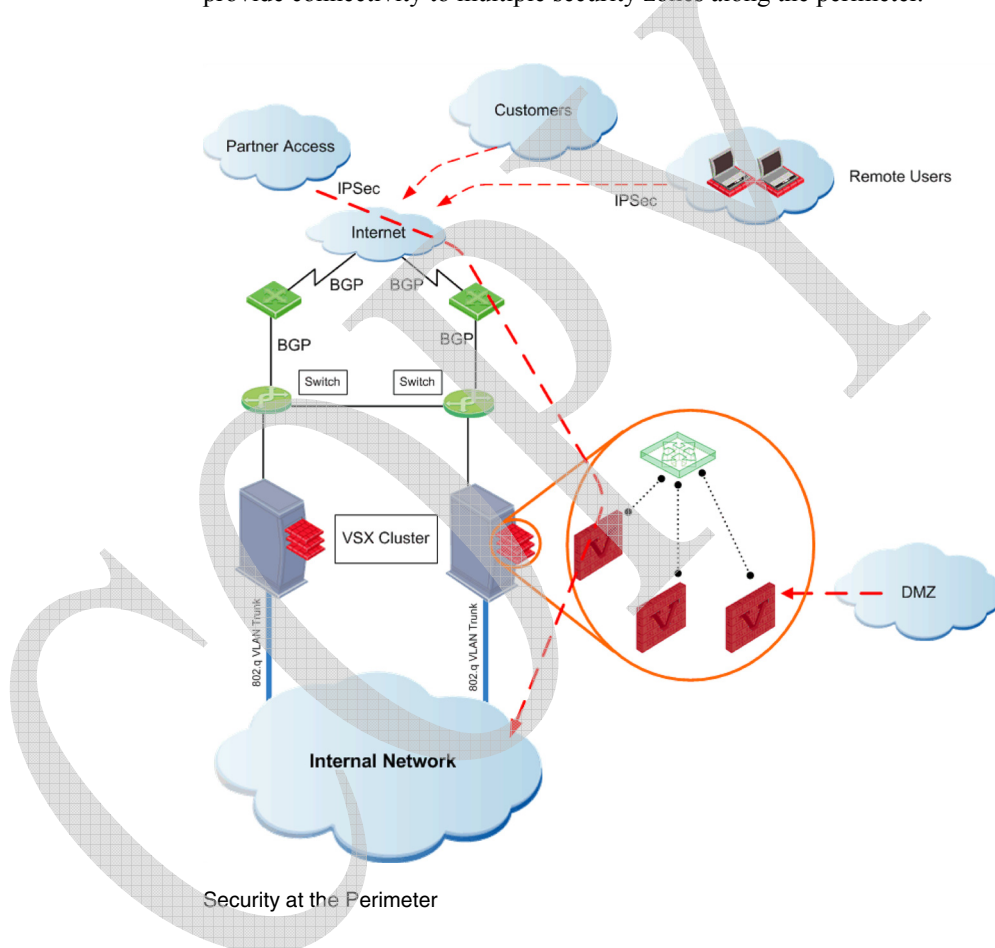
Internal Security

In the figure, the enterprise is composed of different types of networks with different security and access requirements for each department. VSX communicates with the routed core network using the existing infrastructure language, whichever dynamic and multicast protocols are active. Virtual Systems in Bridge mode provide layer-2 security for the various departmental networks, at the same time preventing network segmentation. Finance, Desktops, and R&D networks effectively terminate at the core. Layer-2 access switches are located at the entrance to each department's network. VSX provides connectivity between the core and the endpoint networks, placing the endpoint networks within a security envelope. Security is established per VLAN. Nothing changes in the layer 2 or layer 3 network structure except the addition of this security layer for different VLANs. By controlling traffic into and out of the core, VSX effectively secures the departmental VLANs.

In addition, for Virtual Systems in Bridge mode, VSX interoperates seamlessly with Spanning Tree Protocol (STP) and its variants. VSX does not disrupt layer-2 protocols such as VTP. This interoperability with layer-2 protocols enables load sharing and failovers between the members of the VSX cluster.

## ENTERPRISE DEPLOYMENT — PERIMETER SECURITY

Security is enforced per VLAN. Dynamic-routing protocols OSPF and BGP provide connectivity to multiple security zones along the perimeter.

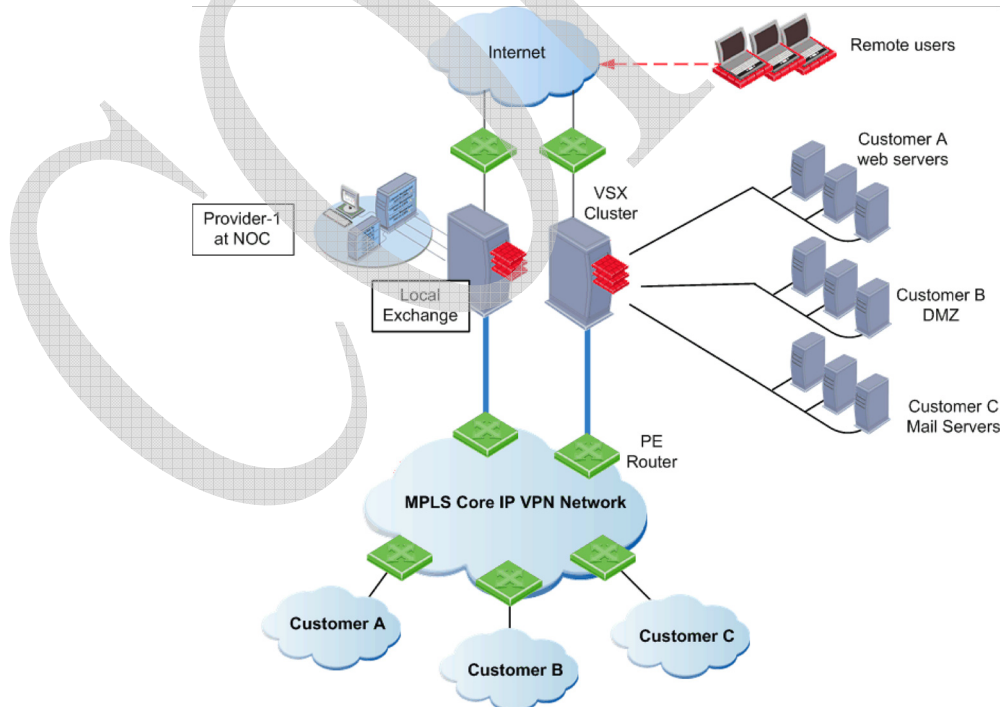


- Each partner has access to the enterprise through a dedicated Virtual System.
- Each partner has a private Security Policy based on need.
- Logs and audit information for each partner are collected separately, and saved to a private database.
- Applications and services are segregated by private Virtual Systems.
- Multiple Virtual Routers/Switches are used to control the access paths.

At the perimeter, VSX secures each DMZ service, VPN peer, customer and partner while providing complete integration with dynamic-routing protocols (OSPF/BGP).

### SERVICE PROVIDERS

In the following figure, a service provider supplies connectivity and security services to its customers, some of which have users that require remote access. In this service-oriented environment, VSX facilitates both connectivity and security without breaking the existing IP design of the Multi Protocol Label Switching (MPLS) network, for example. (The MPLS network provides a private WAN across a single core IP network.) While VSX does not support MPLS, VSX does seamlessly integrate into an MPLS environment. By configuring MPLS routers to map MPLS labels to VLAN tags, all tagged traffic is directed via the VSX gateway to appropriate Virtual Systems. Effectively, a VSX Security Policy is enforced on MPLS labeled packets.)



Service Provider Deployment



The VSX cluster resides in a point-of-Presence (POP) deployment of a service provider.

- The POP is monitored from the service provider's Network Operations Center (NOC) in a High Availability configuration.
- Each customer receives a private Security Policy, and secure VPN connectivity.
- Provider-1 supplies a centralized and granular provisioning system.
- Each customer's forensic information is collected separately, and logged to a private database on the Multi-Domain Logging Module (MLM).
- Applications and services are segregated by discrete Virtual Systems. Access to these services and applications is based on need.
- Multiple Virtual Routers/Switches are used to control the access paths.

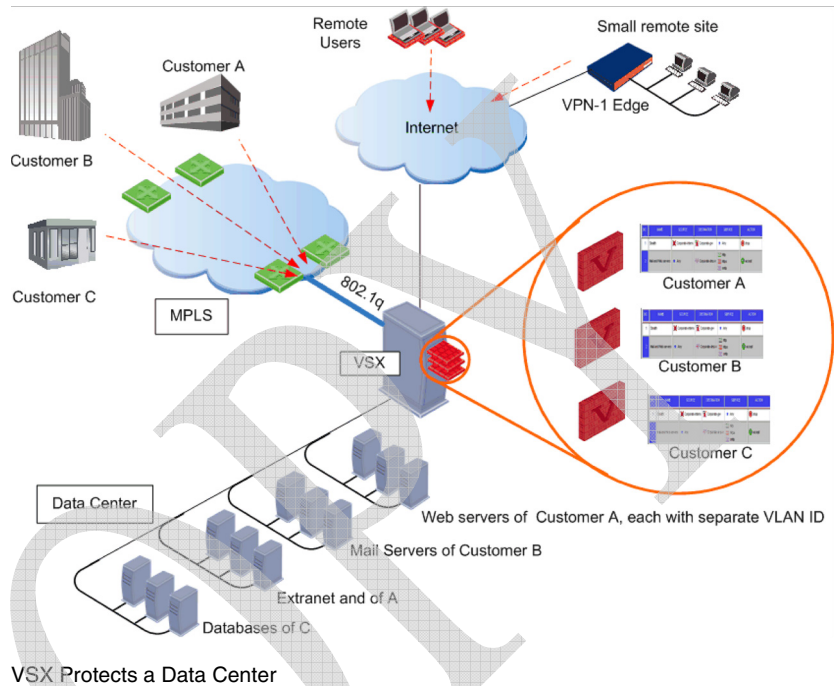
In the figure above, VSX consolidates hardware for the service provider, while ensuring privacy and secure connectivity solutions (VPN) for the service provider's customers. To deploy a new Security Policy, the service provider updates the VSX Gateway.

## DATA CENTERS

Consider the scenario of a service provider supplying infrastructure, connectivity, and security for three customers to the data center shown in the figure below.

In the figure, the MPLS backbone of a Managed Service Provider (MSP) maintains three separate networks over the same physical infrastructure, ensuring connectivity between these distinct customers and the data center. (The backbone does not have to be MPLS. The backbone could equally be Frame Relay or ATM.)

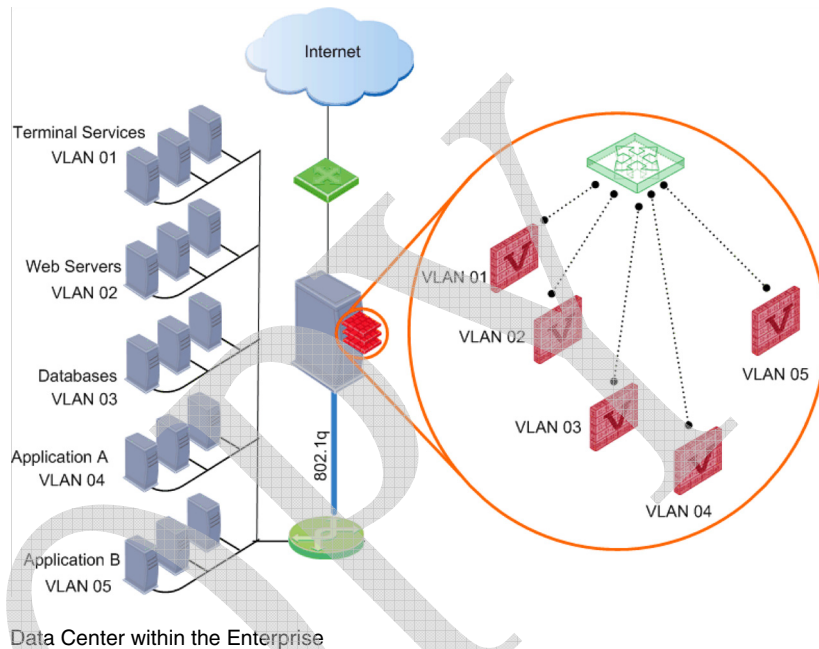
**Customer A** has connectivity with its Web hosting servers, **Customer B** with its mail servers, and **Customer C** with its database deployment. To enhance security and reduce the amount of hardware required, the MSP introduces a VSX cluster.



In the figure, an 802.1q VLAN connects a VSX cluster to the MPLS backbone. Traffic between the data center and Customers A, B, and C is via the VSX cluster. Each customer is associated with a distinct Virtual System. The advantage is scalability. If a remote site needs to be connected to the larger network, MPLS does not provide a cost effective solution. But a VPN connection between the relevant Virtual System and VPN-1 Edge appliance guarding the remote site integrates the remote site into the MPLS core. In the same way, the presence of a VSX cluster provides access for intermittent remote users.

### DATA CENTERS WITHIN THE ENTERPRISE

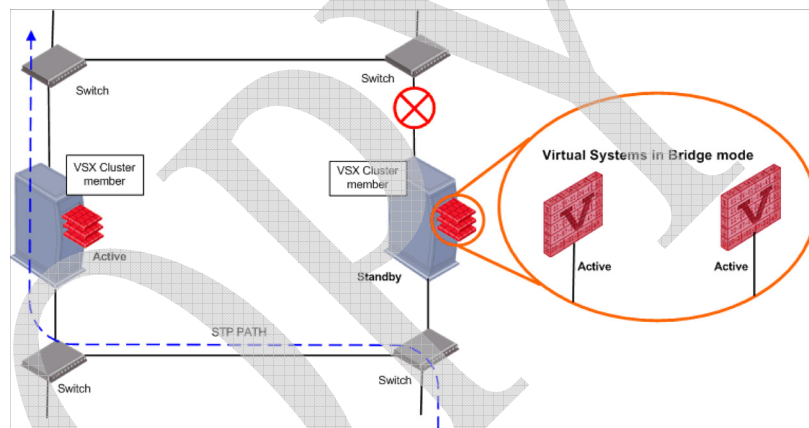
By assigning layer-2 connections to Virtual Systems, VSX reduces the number of physically managed devices within the data center while providing the same level of security. In the figure below, the VSX cluster provides users with protected access to the resources of the data center. The objective is to protect network applications (shared resources with differing access permissions), while increasing the modularity of the network.



For example, a Virtual System is created to protect the databases against SQL exploits and vulnerabilities. Another Virtual System is created to protect the Web Servers against known vulnerabilities, the appropriate protections in SmartDefense being enabled. When new applications and services are added to the enterprise data center, new Virtual Systems are easily created to secure them. In this way, the Virtual System provides a shim layer into which new applications and services can be plugged.

## Clustering Virtual Systems in Bridge Mode (ClusterXL only)

A Virtual System in Bridge mode transparently supports the Spanning Tree Protocol (STP), a link management protocol that provides path redundancy and prevents undesirable loops between switches. For a Virtual System in Bridge mode to support STP, the Virtual System must be connected directly to a physical interface, as shown in the figure below:



### STP Support

In the figure, the Virtual Systems in Bridge mode move traffic at layer 2 between the switches on either side of the VSX machine, and transparently support network-linking decisions forwarded by STP. Even though the members of the VSX cluster are in an active/standby configuration, the Virtual Systems (in Bridge mode) on each cluster member are defined as active/active.

Remember that:

- A Virtual System in Bridge mode forwards all traffic received from the switch.
- STP decides which Virtual System receives packets.
- STP detects a failure when it stops receiving Bridge Protocol Data Units (BPDU) (for example after a cable is disconnected), and immediately forwards traffic to the peer Virtual System in the cluster.



A Virtual System in Bridge mode is also capable of initiating a failover in the spanning tree by blocking BPDU packets. For example, if a critical firewall process fails in the Virtual System, the Virtual System initiates a failover to its peer in the VSX cluster by blocking BPDUs.

COPY

COPY