



Mercurion Systems, Inc.

Information Technology Consulting and Support Services

Phone: 919.266.5957

Fax: 919.217.5769

CASE STUDY: VLAN-BASED MULTILAYER NETWORK

Products: Cisco Catalyst 6509, Cisco Catalyst 3548, Cisco Catalyst 2948G, Cisco Secure PIX Firewall, Cisco VPN 3000 Series VPN Concentrator

Overview

This case study describes the implementation of a VLAN-based multilayer network. In this situation, the customer (a software development company) was growing very quickly and needed a scalable and flexible network infrastructure. To meet these needs, Mercurion Systems designed a network utilizing a Cisco Catalyst 6509 switch, Cisco Catalyst 2948G and 3548XL switches, Cisco PIX 520 firewalls, and Cisco VPN 3000 Series VPN concentrators.

More Information

An overview of the network architecture for this multilayer network is presented below in Figure 1.

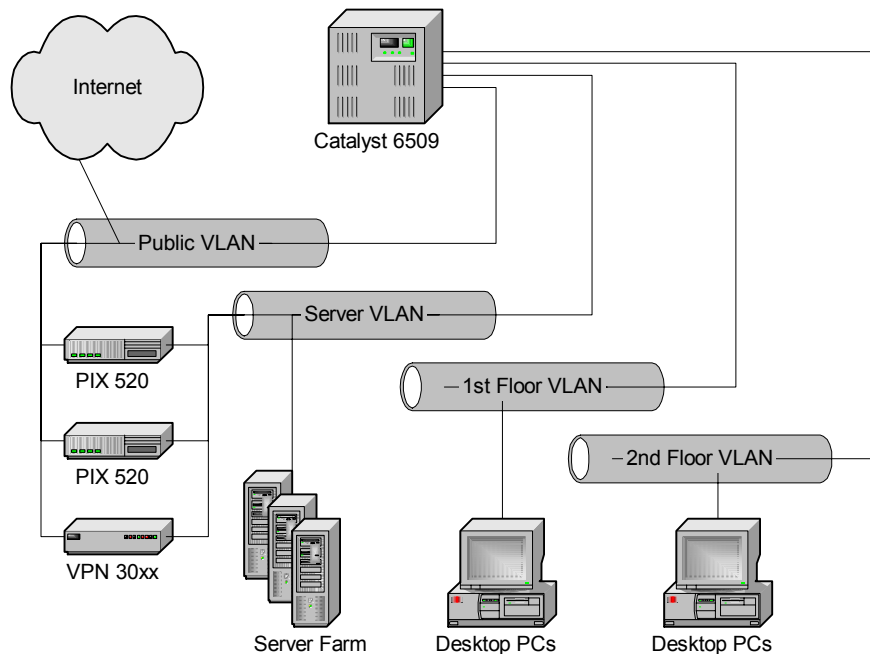


Figure 1. Overview of the multilayer network architecture

Figure 1 shows the core switch, some of the configured VLANs, and the PIX firewalls and VPN concentrators. Not displayed in this diagram are the distribution switches, which consisted of Cisco Catalyst 2948G and Catalyst 3548XL switches.

A number of key technologies were deployed in the implementation of this network. Some of these technologies and how they were used are described in more detail below.

Cisco IOS on Catalyst 6509 Supervisors

Instead of running a hybrid CatOS/IOS system on the redundant Supervisors in the Catalyst 6509, the Supervisors were upgraded to run native IOS. This provided greater redundancy (no need to configure HSRP for Layer 3 redundancy) and more consistent administration across the network. (The Catalyst 3548XL switches also ran Cisco IOS, so commands between those distribution switches were similar or identical to the commands on the core Catalyst 6509.)

Virtual LANs (VLANs)

VLANs formed the base of this network, providing a great deal of the functionality the customer needed. VLANs were created to separate the network into separate broadcast domains represented specific functions or physical locations within the organization—the offices on the 2nd floor, for example, had a VLAN specifically for the 2nd floor, and the Research & Development Group had a VLAN specifically for their department. In addition, VLANs were created for hardware management appliances, corporate servers, and the public segment (outside the firewalls) of the network. All of these VLANs were defined once on the core switch and propagated automatically to all connected distribution switches using VTP (see below for more information on VTP).

Gigabit Ethernet over Fiber

Each distribution switch was linked back to the core switch via a Gigabit Ethernet over fiber connection. This was a full-duplex fiber connection providing a theoretical maximum of 2Gbps of network throughput. Where necessary, Gigabit EtherChannel was employed to link multiple Gigabit Ethernet links together for increased aggregate bandwidth. In addition, Gigabit Ethernet was deployed to the servers in the customer's data center to provide increased performance for network applications such as e-mail, CRM, and database applications.

IEEE 802.1q Trunking

All connections from the distribution switches back to the core switch were configured as IEEE 802.1q trunks. The trunks were configured to allow traffic from all VLANs.

VTP (VLAN Trunking Protocol)

VTP (VLAN Trunking Protocol) was used to provide automatic distribution of VLAN definitions from the core switch to the distribution switches. This allowed the customer to define the VLANs once, on the core switch, and have that VLAN definition automatically propagate to all distribution switches on the network. Once the VLAN definition had propagated to the distribution switch, it was then possible to begin assigning ports to the VLAN.

PIX Firewall Stateful Failover

Dual PIX 520 firewalls were configured for stateful failover, providing a fault tolerant solution for outbound Internet traffic. This also provided a convenient mechanism for software upgrades as well, allowing the PIX firewall software to be easily upgraded with minimal downtime for the customer's users.

A few challenges were discovered during the implementation of this network. Some of these challenges and the corresponding resolutions are listed below.

- *VTP v2 incompatibility:* It was discovered that the specific version of IOS running on the Catalyst 6509 had a problem when a distribution switch connected via an 802.1q Gigabit Ethernet trunk joined the VTP domain without first being configured for VTP v2 mode. As a result, the core switch locked up and had to be cold-booted. A software upgrade to a newer version of IOS on the core Catalyst 6509 corrected the issue.
- *PIX routing limitations:* The Cisco PIX firewall, while able to perform some routing functions, was not able to route between subnets on a single interface. This forced the use of the core switch as the default gateway and caused problems with similar deployments of PIX firewalls and VPN concentrators (see the case study titled "Routing Issues in a Cisco PIX & VPN Concentrator Deployment").

Other Notes

Two other case studies also provide information related to the implementation described above. These case studies are:

- Routing Issues in a Cisco PIX & VPN Concentrator Deployment
- Exchange 2000 SMTP and Cisco PIX Firewalls

Legal Information

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification, in its entirety, and with this disclaimer and proof of authorship.