Making the Most of VLANs

Take a look under the hood of this powerful networking tool so that your agency can reap the benefits of bandwidth, availability and security.

By Chris Partsenidis

▷ Networking

It's easy to see why virtual LANs have become popular on networks of all sizes. Imagine having multiple separate physical networks within a single organization — without the headache of managing multiple cable plants and switches.

Because VLANs segment a network, creating multiple broadcast domains, they effectively allow traffic from those domains to remain isolated while increasing the network's bandwidth, availability and security.

Most managed switches are VLAN-capable, but they don't perform equally well. The market has been flooded by thousands of switches that seem to do the job, but special consideration must be taken before making a purchase.

A switch in a VLAN-enabled network needs to do a lot more than just switch packets between its ports.

TOM GRILL/GETTY IMAGES

Core backbone switches undertake the hefty task of managing the network's VLANs to ensure everything runs smoothly. These switches prioritize network packets based on their source and destination, ensure all edge switches are aware of the VLANs configured in the network, continuously monitor for possible network loops on every VLAN, switch packets between VLANs as required and ensure network security according to their configuration.

Edge (or access) switches are dedicated to end devices: users' systems, network peripherals and, sometimes, servers. They must be compatible with the VLAN features that the core backbone switches support. This is a reason why many organizations standardize network equipment from companies such as Cisco Systems, HP and Juniper Networks.

When deploying VLANs, here are five key considerations to address:

1: Links on VLAN Switches

VLAN switches have two main types of links: access links and trunk links.

Access links are the most common. All network hosts connect to the switch's access links to gain access to the local network. These links are the ordinary ports found on every switch, but configured to access a particular VLAN.

Trunk links connect two VLAN-capable switches. While an access link is configured to access a specific VLAN, a trunk link is almost always configured to carry data from all available VLANs.

2: Native VLAN, ISL and 802.1Q

When a port on a switch is configured as an access link, it has access to one specific VLAN. Any network device connecting to it will become part of that VLAN.

Ethernet frames entering or exiting the port are standard Ethernet II type frames, which are understood by the network device connected to the port. Because these frames belong to one network, they are said to be "untagged" — meaning that they lack information as to which VLAN they are assigned.

Trunk links, on the other hand, are more complicated. Because they carry frames from all VLANs, it's necessary to identify the frames as they traverse switches. This is called VLAN tagging.

Two methods known for this job are ISL (Inter-Switch Link, a proprietary Cisco protocol) and IEEE 802.1Q. Of the two, 802.1Q is the most popular method and is compatible among all vendors supporting VLAN trunking.

But a trunk link can also be configured to act as an access link when a device that does not support VLAN trunking connects to it.

If you have a trunk link on a switch and connect a computer, the port will automatically provide access to a specific VLAN. The VLAN in this case is known as the "native VLAN," a common term referring to the untagged VLAN that a trunk port is configured for when acting as an access link.

3: Virtual Trunk Protocol

VTP is a proprietary Cisco protocol that ensures all VLAN information held by the VTP server is propagated to all network switches within the VTP domain.

During initial network configuration, all switches are configured members of the same VTP domain. With VTP, an IT administrator can create, delete or rename VLANs on the core switch. All information is then sent to all members of the VTP domain.

The VTP equivalent for other manufacturers is the GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol (GVRP), which includes many features implemented previously only in Cisco System's VTP protocol.

VTP pruning, an extension to VTP's functionality, ensures that unnecessary network traffic is not sent over trunk links. This is done by forwarding broadcasts and unknown unicast frames on a VLAN over trunk links only if the receiving end of the trunk has ports assigned to that VLAN.

If a network broadcast occurred on VLAN5, for instance, and a particular switch did not have any ports assigned to VLAN5, it would never receive the broadcast traffic through its trunk link. This translates to a major discount in broadcast or multicast traffic received by end switches in a VLAN network.

ELIZABETH HINSHAW

"The market has been flooded by thousands of switches that seem to do the job, but special consideration must be taken before making a purchase."

— Chris Partsenidis

4: Inter-VLAN Routing

Inter-VLAN routing routes packets between VLANs — one of the most important features found on advanced switches. Because inter-VLAN routing directs packets based on their Layer-3 information (the IP address), switches that perform this function are known as Layer-3 switches and are the most expensive.

The core switch is often a Layer-3 switch. When a Layer-3 switch is not available, this function can also be performed by a server with two or more network cards or a router, a method often referred to as "router on a stick."

Because this is one of the most important aspects of a VLAN network, the Layer-3 switch must have fast switching fabric (measured in Gbps) and provide advanced capabilities such as support for routing protocols, advanced access lists and firewalls. The Layer-3 switch offers outstanding protection for a VLAN network *if* it's properly configured.

5: Securing VLAN Devices

The first principle of securing a VLAN network is physical security. If an organization does not want its devices tampered with, physical access must be strictly controlled. Core switches are usually safely located in a data center with restricted access, but edge switches are often located in exposed areas.

Just as physical security guidelines require equipment to be in a controlled space, VLAN-based security requires using special tools and best practices to achieve the desired result.

To learn hands-on details about these security best practices, go to *fedtechmagazine.com/0211VLANsec.*

Raising the Throttle

VLAN technology enhances the network and provides paths to run multiple services in isolated environments without sacrificing speed, quality and availability. If basic security guidelines are followed during implementation and in ongoing administration, a VLAN can dramatically reduce administrative overhead.

Perhaps the most serious mistake that can be made is to underestimate the importance of the data link layer and of VLANs in particular in the architecture of switched networks.

It should not be forgotten that any network is only as robust as its weakest link. An equal amount of attention needs to be given to every layer to ensure the soundness of the entire structure.

Chris Partsenidis is a senior network engineer for Datavision in Greece. He is also the founder and senior editor of *Firewall.cx*, a globally recognized site dedicated to analysis, implementation and security of networking technologies.