White **Paper**

AMG
TRANSMISSION WITH INNOVATION
Proud to be a British Manufacturer

Introduction to VLAN

This document explains how Virtual LANs (VLANs) operate, when to use them and what features are required in the network.

AMG Systems Ltd. 3 The Omega Centre, Stratton Business Park, Biggleswade, Bedfordshire, SG18 8QB
T :: +44 (0) 1767 600 777 F :: +44 (0) 1767 600 077 E :: info@amgsystems.com
Company Registration Number 2838846. Registered Address: Brigham House, High Street, Biggleswade, Bedfordshire, SG18 0LD

AMG
www.amgsystems.com

Executive summary

VLANs offer a method of segregating a physical network into a logical network infrastructure.

By deploying VLANs, you can create multiple virtual LANs in your Ethernet infrastructure. VLANs help reduce traffic, decrease costs, improve performance, increase security, provide more connectivity options and reduce the size of fault domains, improving the diagnostic process.

As the use of VLAN technology has become more common, designing and maintaining networks must now involve being aware of the use of and presence of VLANs.

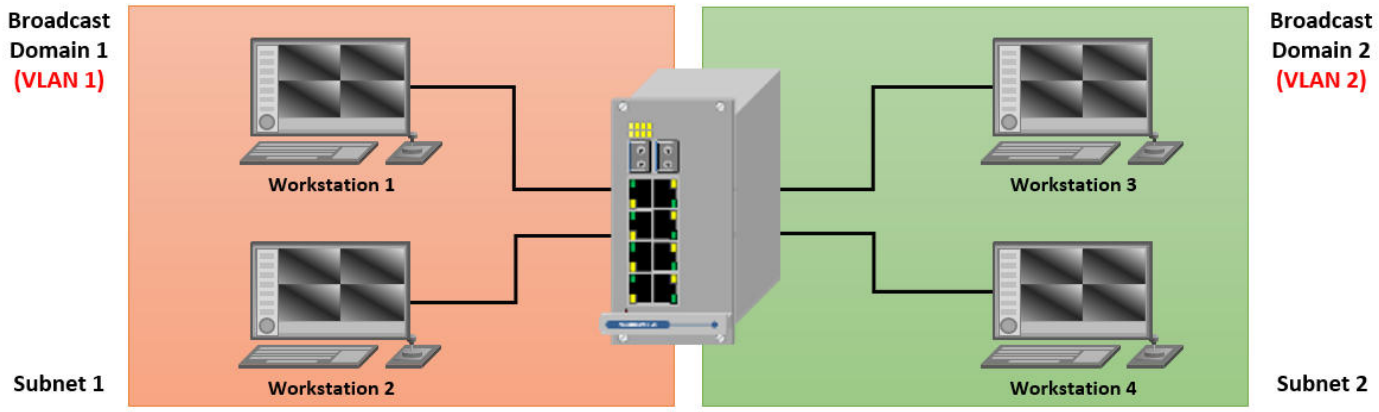
Virtual Local Area Network definition

Before understanding VLANs, you must first have an understanding of the definition of LANs. For example, from one perspective a LAN includes all the user devices, servers, switches, routers, cameras, cables and wireless access points in one locations. However, a more technical definition of LANs can help in understanding the concept of a virtual LAN:

A LAN includes all devices in the same **Broadcast domain**.

A broadcast domain includes the set of all LAN-connected devices, so that when any of the devices sends broadcast frames, all the other devices receive a copy of the frame. You can think of a LAN and a broadcast domain as being basically the same thing.

Without VLANs, a switch considers all its interfaces to be in the same broadcast domain. With support for VLANs, a single switch can configure some interfaces into one broadcast domain and some into another, creating multiple broadcast domains. These individual broadcast domains are called virtual LANs (VLANs).



LAN Segmentation

VLANs allow logical network topologies to overlay the physical switched infrastructure such that any arbitrary collection of LAN ports can be combined into an autonomous user group or community of interest. The technology logically segments the network into separate Layer-2 broadcast domains whereby packets are switched between ports designated to be within the same VLAN. Switched virtual networks avoid wasting bandwidth, a drawback inherent to traditional bridged and switched networks in which packets are often forwarded to LANs or devices with no need for them. Implementation of VLANs also improves scalability, particularly in LAN environments that support broadcast or multicast-intensive protocols and applications that flood packets throughout the network.

Why use VLANs?

There are several reasons a network administrator may want to create one or more logical groupings of devices. In most cases, these reasons are broadcast control, security and Layer-3 address management.

Broadcast Control

As the number of devices within a broadcast domain increases, so does the broadcast rate within that broadcast domain. The broadcast rate is significant, since each device must process each broadcast to determine whether the contents of the broadcast should be pushed up the protocol stack.

For each broadcast that is received, the receiving device must interrupt the CPU to evaluate the contents of the broadcast frame. These interruptions take processing time away from other tasks running on the CPU and can increase the amount of time it takes for those tasks to complete. An example being the introduction of video latency or loss in CCTV networks.

An important aspect of VLANs is that broadcasts transmitted in one VLAN are not propagated to other VLANs. By limiting the number of devices in each VLAN, the broadcast rate within that VLAN can also be limited.

Security

There are times when an organization needs to limit access to a specific device or devices on the local area network. If all of the devices within that organization are within the same broadcast domain, it becomes very difficult to limit this access. By placing devices in different broadcast domains, it is possible to limit access through the use of address filters and access lists. For traffic to pass from one VLAN to another, the traffic must pass through a Layer-3 routing device. These routing devices allow you to specify which devices may access other devices. The use of this access control capability allows access to sensitive devices to be controlled and monitored.

Layer-3 Address Management

Creating IP subnets based on device type is a common design in local area networks. Cameras may be assigned to one IP subnet, while workstations and servers are assigned to another subnet or subnets. While logically this makes sense, deploying this architecture across a large local area network can prove to be impractical without the use of VLANs.

Types of VLAN

Port Based VLAN

For port based VLANs, a switch port is manually configured to be a member of a specific VLAN. Any device connected to this port will belong to the same broadcast domain as all other ports configured with the same VLAN number.

The challenge of port based VLANs becomes documenting which ports belong to each VLAN. The VLAN membership information is not displayed on the front of the switch. The VLAN membership cannot be determined just by looking at the physical switch port. Only by looking at the configuration information can the membership be determined.

Protocol Based VLAN

With Protocol based VLANs, the Layer-3 protocol being carried by the frame is used to determine VLAN membership. While this may work in multi-protocol environments, in a predominately IP based network, this method is not practical.

MAC Based VLAN

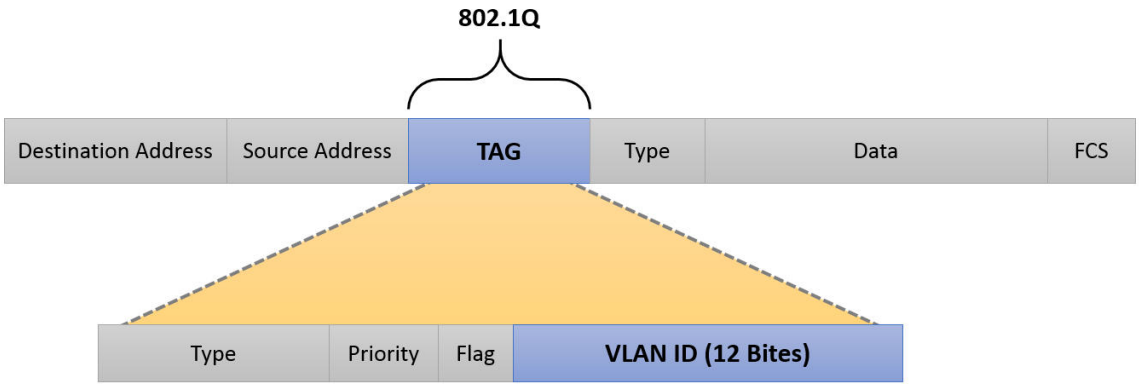
One problem with port based VLANs is that if the original device is removed from the port and another device is connected, the new device will be in the same VLAN as the original. Let's say a camera was removed from a switch port and a laptop was connected to the empty port - The laptop would now be in the camera VLAN. This may limit the access the laptop has to resources on the network but it also presents a potential security risk as the laptop now has access to the network and its introduction may go unnoticed.

MAC based VLANs are intended to resolve this problem. In a MAC based VLAN, the VLAN membership is based on the MAC address of the device, not the physical switch port. If a device is moved from one switch port to another, the VLAN membership will follow the device.

Unfortunately, the correlation of MAC address to VLAN is a very time consuming process and this type of VLAN is rarely used.

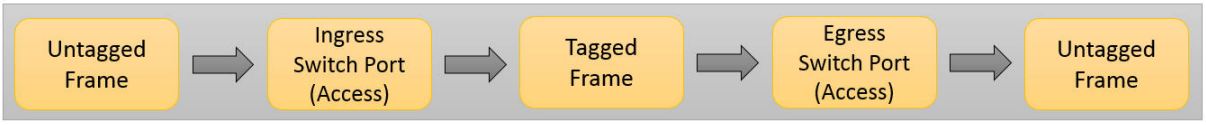
VLAN Tagging

VLAN tagging is usually done based on the standard IEEE 802.1Q. The tags are used to indicate VLAN membership within a frame going across the network. These tags are attached to the frame as it enters a switch port belonging to a VLAN and the tags are removed when the frame leaves a port belonging to the VLAN. The type of port within the VLAN will determine whether the VLAN tag is stripped from the frame or whether it remains attached to the frame. The two port types within a VLAN environment are known as access ports and trunk ports.



Access Ports

Access ports are used where a frame enters or exits the VLAN. When an access port receives a frame, the frame does not contain a VLAN tag. As the frame enters the access port, the VLAN tag is attached to the frame.



While the frame is within the switch, it carries the VLAN tag that was attached when it entered through the access port. As the frame leaves the switch through the destination access port, the VLAN tag is removed. The transmitting device and the receiving device are not aware that the VLAN tag was ever attached.

Trunk Ports

In networks containing more than one switch, it becomes necessary to be able to send VLAN tagged frames from one switch to another. The difference between trunk ports and access ports is that trunk ports do not strip off the VLAN tag before sending the frame. With the VLAN tag preserved, the receiving switch will know the membership of the transmitted frame. This frame can then be sent out of the appropriate ports on the receiving switch.

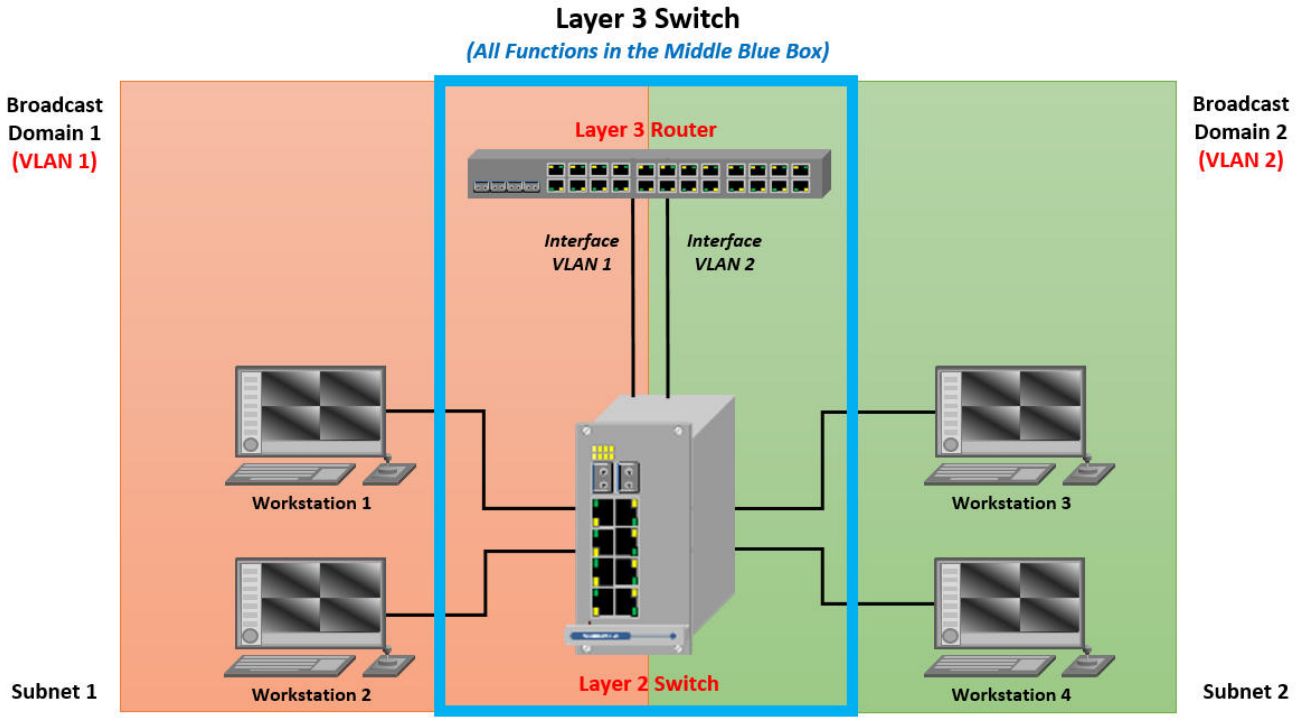
VLAN Routing

Communication between VLANs is accomplished through routing. When a host in one VLAN must communicate with a host in another VLAN, the traffic must be routed between them. This type of routing is called **VLAN routing**.

Routing is a **Layer 3 feature** and it could be provided by any Layer 3 device.

Standard Managed switches forward data based on Layer 2 logic (MAC address) and usually are called **Layer 2 switches**. However, some other switches include some functions like a router, using additional logic defined by Layer 3 protocols. These switches go by the name **multilayer switch**, or **Layer 3 switch**.

The Layer 3 switch or router uses IP subnets to move traffic between VLANs. Each VLAN has a different IP subnet, and there is a one-to-one correspondence of VLAN and IP subnet boundaries. If a host is in a given IP subnet, it is also assigned to a VLAN, and vice-versa.



Summary

A VLAN segregates local area networks (LAN) by providing data link connectivity for a subnet. One or more network switches may support multiple, independent VLANs, creating Layer-2 (data link) implementation of a subnet. A VLAN is associated with a broadcast domain.

VLANs make it easy for network administrators to partition a single switched network to match the functional and security requirement of their systems without having to run new cables or make major changes to their current network infrastructure. Ports (interfaces) on switches can be assigned to one or more VLANs, enabling systems to be divided into logical groups and establish rules about how systems in the separate groups are allowed to communicate with each other.

Each VLAN provides data link access to all hosts connected to switch ports configured with the same VLAN ID. The VLAN tag is a 12-bit field in the Ethernet header that provides support for up to 4,096 VLANs per switching domain. VLAN tagging is standardised in IEEE 802.1Q standard.

When an untagged frame is received from an attached host, the VLAN ID tag configured on that interface is added to the data link frame header, using the 802.1Q format. The 802.1Q frame is then forwarded toward the destination. Each switch uses the tag to keep each VLAN's traffic separate from other VLANs, forwarding it only where the VLAN is configured.

Multiple VLANs can be configured on a single port using a trunk configuration in which each frame sent via the port is tagged with the VLAN ID. The neighboring device's interface, which may be on another switch or on a host that supports 802.1Q tagging, will need to support trunk mode configuration in order to transmit and receive tagged frames.

By establishing VLANs, broadcast traffic can be reduced considerably within backbones and individual subnetworks. In a virtual LAN:

- Each packet sent from any workstation can be associated with one VLAN.
- A workstation receives all multicast and broadcast packets within its associated VLAN.
- A workstation can receive unicast packets (packets addressed to an individual receiver) transmitted within its VLAN, if those packets are addressed to it.

In some networks, communications between individual workstations need to be prohibited at a relatively low level. Without VLANs all workstations belong to a single broadcast domain, so by assigning the workstations to different VLANs access can be denied or explicitly admitted by controlling devices such as routers. In general, this is referred to as First Level security.