Virtual LAN

A **virtual LAN** (**VLAN**) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).[1][2] *LAN* is the abbreviation for *local area network* and in this context *virtual* refers to a physical object recreated and altered by additional logic. VLANs work by applying tags to network frames and handling these tags in networking systems – creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks. In this way, VLANs can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.

VLANs allow network administrators to group hosts together even if the hosts are not directly connected to the same network switch. Because VLAN membership can be configured through software, this can greatly simplify network design and deployment. Without VLANs, grouping hosts according to their resource needs the labor of relocating nodes or rewiring data links. VLANs allow devices that must be kept separate to share the cabling of a physical network and yet be prevented from directly interacting with one another. This managed sharing yields gains in simplicity, security, traffic management, and economy. For example, a VLAN can be used to separate traffic within a business based on individual users or groups of users or their roles (e.g. network administrators), or based on traffic characteristics (e.g. low-priority traffic prevented from impinging on the rest of the network's functioning). Many Internet hosting services use VLANs to separate customers' private zones from one other, allowing each customer's servers to be grouped in a single network segment no matter where the individual servers are located in the data center. Some precautions are needed to prevent traffic "escaping" from a given VLAN, an exploit known as VLAN hopping.

To subdivide a network into VLANs, one configures network equipment. Simpler equipment might partition only each physical port (if even that), in which case each VLAN runs over a dedicated network cable. More sophisticated devices can mark frames through VLAN tagging, so that a single interconnect (*trunk*) may be used to transport data for multiple VLANs. Since VLANs share bandwidth, a VLAN trunk can use link aggregation, quality-of-service prioritization, or both to route data efficiently.

Contents

Uses

VLANs address issues such as scalability, security, and network management. Network architects set up VLANs to provide network segmentation. Routers between VLANs filter broadcast traffic, enhance network security, perform address summarization, and mitigate network congestion.

In a network utilizing broadcasts for service discovery, address assignment and resolution and other services, as the number of peers on a network grows, the frequency of broadcasts also increases. VLANs can help manage broadcast traffic by forming multiple broadcast domains. Breaking up a large network into smaller independent segments reduces the amount of broadcast traffic each network device and network segment has to bear. Switches may not bridge network traffic between VLANs, as doing so would violate the integrity of the VLAN broadcast domain.

VLANs can also help create multiple layer 3 networks on a single physical infrastructure. VLANs are data link layer (OSI layer 2) constructs, analogous to Internet Protocol (IP) subnets, which are network layer (OSI layer 3) constructs. In an environment employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, although it is possible to have multiple subnets on one VLAN.

Without VLAN capability, users are assigned to networks based on geography and are limited by physical topologies and distances. VLANs can logically group networks to decouple the users' network location from their physical location. By using VLANs, one can control traffic patterns and react quickly to employee or equipment relocations. VLANs provide the flexibility to adapt to changes in network requirements and allow for simplified administration.[2]

VLANs can be used to partition a local network into several distinctive segments, for instance:[3]

- Production
- Voice over IP
- Network management
- Storage area network (SAN)
- Guest Internet access
- Demilitarized zone (DMZ)

A common infrastructure shared across VLAN trunks can provide a measure of security with great flexibility for a comparatively low cost. Quality of service schemes can optimize traffic on trunk links for real-time (e.g. VoIP) or low-latency requirements (e.g. SAN). However, VLANs as a security solution should be implemented with great care as they can be defeated unless implemented carefully.[4]

In cloud computing VLANs, IP addresses, and MAC addresses in the cloud are resources that end users can manage. To help mitigate security issues, placing cloud-based virtual machines on VLANs may be preferable to placing them directly on the Internet.[5]

Network technologies with VLAN capabilities include:

- Asynchronous Transfer Mode (ATM)

- Fiber Distributed Data Interface (FDDI)
- Ethernet
- HiperSockets
- InfiniBand

History

After successful experiments with voice over Ethernet from 1981 to 1984, W. David Sincoskie joined Bellcore and began addressing the problem of scaling up Ethernet networks. At 10 Mbit/s, Ethernet was faster than most alternatives at the time. However, Ethernet was a broadcast network and there was no good way of connecting multiple Ethernet networks together. This limited the total bandwidth of an Ethernet network to 10 Mbit/s and the maximum distance between nodes to a few hundred feet.

By contrast, although the existing telephone network's speed for individual connections was limited to 56 kbit/s (less than one hundredth of Ethernet's speed), the total bandwidth of that network was estimated at 1 Tbit/s (100,000 times greater than Ethernet).

Although it was possible to use IP routing to connect multiple Ethernet networks together, it was expensive and relatively slow. Sincoskie started looking for alternatives that required less processing per packet. In the process, he independently reinvented transparent bridging, the technique used in modern Ethernet switches.[6] However, using switches to connect multiple Ethernet networks in a fault-tolerant fashion requires redundant paths through that network, which in turn requires a spanning tree configuration. This ensures that there is only one *active* path from any source node to any destination on the network. This causes centrally located switches to become bottlenecks, limiting scalability as more networks are interconnected.

To help alleviate this problem, Sincoskie invented VLANs by adding a tag to each Ethernet frame. These tags could be thought of as colors, say red, green, or blue. In this scheme, each switch could be assigned to handle frames of a single color, and ignore the rest. The networks could be interconnected with three spanning trees, one for each color. By sending a mix of different frame colors, the aggregate bandwidth could be improved. Sincoskie referred to this as a *multitree bridge*. He and Chase Cotton created and refined the algorithms necessary to make the system feasible.[7] This *color* is what is now known in the Ethernet frame as the IEEE 802.1Q header, or the VLAN tag. While VLANs are commonly used in modern Ethernet networks, they are not used in the manner first envisioned here.

In 1998, Ethernet VLANs were described in the first edition of the IEEE 802.1Q-1998 standard.[8] This was extended with IEEE 802.1ad to allow nested VLAN tags in service of provider bridging. This mechanism was improved with IEEE 802.1ah-2008.

Configuration and design considerations

Early network designers often segmented physical LANs with the aim of reducing the size of the Ethernet collision domain—thus improving performance. When Ethernet switches made this a non-issue (because each switch port is a collision domain), attention turned to reducing the size of the data link layer broadcast domain. VLANs were first employed to separate several broadcast domains across one physical medium. A VLAN can also serve to restrict access to network resources without regard to physical topology of the network.[a]

VLANs operate at the data link layer of the OSI model. Administrators often configure a VLAN to map directly to an IP network, or subnet, which gives the appearance of involving the network layer. Generally, VLANs within the same organization will be assigned different non-overlapping network address ranges.

This is not a requirement of VLANs. There is no issue with separate VLANs using identical overlapping address ranges (e.g. two VLANs each use the private network *192.168.0.0/16*). However, it is not possible to route data between two networks with overlapping addresses without delicate IP remapping, so if the goal of VLANs is segmentation of a larger overall organizational network, non-overlapping addresses must be used in each separate VLAN.

A basic switch that is not configured for VLANs has VLAN functionality disabled or permanently enabled with a *default VLAN* that contains all ports on the device as members.[2] The default VLAN typically uses VLAN identifier 1. Every device connected to one of its ports can send packets to any of the others. Separating ports by VLAN groups separates their traffic very much like connecting each group using a distinct switch for each group.

Remote management of the switch requires that the administrative functions be associated with one or more of the configured VLANs.

In the context of VLANs, the term *trunk* denotes a network link carrying multiple VLANs, which are identified by labels (or *tags*) inserted into their packets. Such trunks must run between *tagged ports* of VLAN-aware devices, so they are often switch-to-switch or switch-to-router links rather than links to hosts. (Note that the term 'trunk' is also used for what Cisco calls "channels" : Link Aggregation or Port Trunking). A router (Layer 3 device) serves as the backbone for network traffic going across different VLANs. It is only when the VLAN port group is to extend to another device that tagging is used. Since communications between ports on two different switches travel via the uplink ports of each switch involved, every VLAN containing such ports must also contain the uplink port of each switch involved, and traffic through these ports must be tagged.

Switches typically have no built-in method to indicate VLAN to port associations to someone working in a wiring closet. It is necessary for a technician to either have administrative access to the device to view its configuration, or for VLAN port assignment charts or diagrams to be kept next to the switches in each wiring closet.

Protocols and design

The protocol most commonly used today to support VLANs is IEEE 802.1Q. The IEEE 802.1 working group defined this method of multiplexing VLANs in an effort to provide multivendor VLAN support. Prior to the introduction of the 802.1Q standard, several proprietary protocols existed, such as Cisco Inter-Switch Link (ISL) and 3Com's Virtual LAN Trunk (VLT). Cisco also implemented VLANs over FDDI by carrying VLAN information in an IEEE 802.10 frame header, contrary to the purpose of the IEEE 802.10 standard.

Both ISL and IEEE 802.1Q tagging perform *explicit tagging* – the frame itself is tagged with VLAN information. ISL uses an external tagging process that does not modify the Ethernet frame, while 802.1Q uses a frame-internal field for tagging, and therefore does modify the basic Ethernet frame structure. This internal tagging allows IEEE 802.1Q to work on both access and trunk links using standard Ethernet hardware.

IEEE 802.1Q

Under IEEE 802.1Q, the maximum number of VLANs on a given Ethernet network is 4,094 (4,096 values provided by the 12-bit VID field minus reserved values at each end of the range, 0 and 4,095). This does not impose the same limit on the number of IP subnets in such a network since a single VLAN can contain

multiple IP subnets. IEEE 802.1ad extends the number of VLANs supported by adding support for multiple, nested VLAN tags. IEEE 802.1aq (Shortest Path Bridging) expands the VLAN limit to 16 million. Both improvements have been incorporated into the IEEE 802.1Q standard.

Cisco Inter-Switch Link

Inter-Switch Link (ISL) is a Cisco proprietary protocol used to interconnect switches and maintain VLAN information as traffic travels between switches on trunk links. ISL is provided as an alternative to IEEE 802.1Q. ISL is available only on some Cisco equipment and has been deprecated.[10]

Cisco VLAN Trunking Protocol

VLAN Trunking Protocol (VTP) is a Cisco proprietary protocol that propagates the definition of VLANs on the whole local area network. VTP is available on most of the Cisco Catalyst Family products. The comparable IEEE standard in use by other manufacturers is GARP VLAN Registration Protocol (GVRP) or the more recent Multiple VLAN Registration Protocol (MVRP).

Multiple VLAN Registration Protocol

Multiple VLAN Registration Protocol is an application of Multiple Registration Protocol that allows automatic configuration of VLAN information on network switches. Specifically, it provides a method to dynamically share VLAN information and configure the needed VLANs.

Membership

VLAN membership can be established either statically or dynamically.

Static VLANs are also referred to as port-based VLANs. Static VLAN assignments are created by assigning ports to a VLAN. As a device enters the network, the device automatically assumes the VLAN of the port. If the user changes ports and needs access to the same VLAN, the network administrator must manually make a port-to-VLAN assignment for the new connection.

Dynamic VLANs are created using software or by protocol. With a VLAN Management Policy Server (VMPS), an administrator can assign switch ports to VLANs dynamically based on information such as the source MAC address of the device connected to the port or the username used to log onto that device. As a device enters the network, the switch queries a database for the VLAN membership of the port that device is connected to. Protocol methods include Multiple VLAN Registration Protocol (MVRP) and the somewhat obsolete GARP VLAN Registration Protocol (GVRP).

Protocol-based VLANs

In a switch that supports protocol-based VLANs, traffic may be handled on the basis of its protocol. Essentially, this segregates or forwards traffic from a port depending on the particular protocol of that traffic; traffic of any other protocol is not forwarded on the port. This allows, for example, IP and IPX traffic to be automatically segregated by the network.

VLAN cross connect

VLAN cross connect (CC or VLAN-XC) is a mechanism used to create Switched VLANs, VLAN CC uses IEEE 802.1ad frames where the S Tag is used as a Label as in MPLS. IEEE approves the use of such a mechanism in part 6.11 of IEEE 802.1ad-2005.

See also

- HVLAN, hierarchical VLAN
- Multiple VLAN Registration Protocol, GARP VLAN Registration Protocol
- Network virtualization
- Private VLAN
- Software-defined networking
- Switch virtual interface
- Virtual Extensible LAN (VXLAN)
- Virtual Private LAN Service
- Virtual private network
- VLAN access control list
- Wide area network

Notes

a. The strength of VLAN security can be compromised by VLAN hopping. VLAN hopping can be mitigated with proper switchport configuration.[9]

References

1. IEEE 802.1Q-2011, *1. Overview*
2. IEEE 802.1Q-2011, *1.4 VLAN aims and benefits*
3. "VLAN & Its Implementation over ATM by using IP: a communication" (https://web.archive.org/web/20150618172303/http://www.discovery.org.in/discoveryengineering/current_issue/v2/n8/A11.pdf) (PDF). Discovery Institute. Archived from the original (http://www.discovery.org.in/discoveryengineering/current_issue/v2/n8/A11.pdf) (PDF) on 2015-06-18.
4. "Virtual LAN Security: weaknesses and countermeasures" (https://www.sans.org/reading-room/whitepapers/networkdevs/virtual-lan-security-weaknesses-countermeasures-1090), *SANS Institute InfoSec Reading Room*, SANS Institute, retrieved 2018-05-18
5. Amies A; Wu C F; Wang G C; Criveti M (21 June 2012), "Networking on the cloud" (https://web.archive.org/web/20131101082835/http://www.ibm.com/developerworks/cloud/library/cl-networkingtools/cl-networkingtools-pdf.pdf) (PDF), *IBM developerWorks*, archived from the original (http://www.ibm.com/developerworks/cloud/library/cl-networkingtools/cl-networkingtools-pdf.pdf) (PDF) on 2013-11-01
6. Sincoskie, WD (2002) "Broadband packet switching: a personal perspective." (http://ieeexplore.ieee.org/iel5/35/21910/01018008.pdf?arnumber=1018008) IEEE Commun 40: 54-66
7. W. D. Sincoskie and C. J. Cotton, "Extended Bridge Algorithms for Large Networks" (http://ieeexplore.ieee.org/iel3/65/185/00003233.pdf) IEEE Network, Jan. 1988.
8. *IEEE Std. 802.1Q-1998, Virtual Bridged Local Area Networks* (https://standards.ieee.org/standard/802_1Q-1998.html). 1998.
9. Rik Farrow. "VLAN Insecurity" (https://web.archive.org/web/20140421082757/http://rikfarrow.com/Network/net0103.html). Archived from the original (http://rikfarrow.com/Network/net0103.html) on 2014-04-21.

Further reading

- Andrew S. Tanenbaum, 2003, "Computer Networks", Pearson Education International, New Jersey.