Virtual LAN

From Wikipedia, the free encyclopedia

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 an abbreviation of *local area network*.

To subdivide a network into virtual LANs, one configures a network switch or router. Simpler network devices can only partition per physical port (if at all), in which case each VLAN is connected with a dedicated network cable (and VLAN connectivity is limited by the number of hardware ports available). More sophisticated devices can mark packets through *tagging*, so that a single interconnect (*trunk*) may be used to transport data for multiple VLANs. Since VLANs share bandwidth, a VLAN trunk might use link aggregation and/or quality of service prioritization to route data efficiently.

VLANs allow network administrators to group hosts together even if the hosts are not on the same network switch. This can greatly simplify network design and deployment, because VLAN membership can be configured through software. Without VLANs, grouping hosts according to their resource needs necessitates the labor of relocating nodes or rewiring data links.

Contents

- 1 Uses
- 2 History
- 3 Implementation
- 4 Motivation
  - 4.1 Broadcast domains
- 5 Protocols and design
  - 5.1 IEEE 802.1Q
  - 5.2 Cisco VLAN Trunking Protocol (VTP)
  - 5.3 Multiple VLAN Registration Protocol
  - 5.4 Shortest Path Bridging
- 6 Establishing VLAN memberships
- 7 Protocol-based VLANs
- 8 VLAN Cross Connect

- 9 See also
- 10 References
- 11 Further reading
- 12 External links

Uses

Network architects set up VLANs to provide the network segmentation services traditionally provided only by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies filter broadcast traffic, enhance network security, perform address summarization, and mitigate network congestion. 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. For example, if a DHCP server is plugged into a switch it will serve any host on that switch that is configured for DHCP. By using VLANs, the network can be easily split up so some hosts will not use that DHCP server and will obtain link-local addresses, or obtain an address from a different DHCP server.

VLANs are data link layer (OSI layer 2) constructs, analogous to 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.

By using VLANs, one can control traffic patterns and react quickly to 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,[3] for example:

- Production
- Voice over IP
- Network management
- Storage area network (SAN)
- Guest network
- Demilitarized zone (DMZ)
- Client separation (ISP, in a large facility, or in a datacenter)

A common infrastructure shared across VLAN trunks can provide a very high level 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).

In cloud computing VLANs, IP addresses, and MAC addresses on them are resources which end users can manage. Placing cloud-based virtual machines on VLANs may be preferable to placing them directly on the Internet to avoid security issues.[4]

History

After successful experiments with Voice over Ethernet from 1981 to 1984, Dr. 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 any two nodes to a few hundred feet.

By contrast, although the existing telephone network's peak 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, capable of moving over a hundred thousand times more information in a given timescale.

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 the self-learning Ethernet switch.[5]

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, which limits scalability as more networks are interconnected.

To help alleviate this problem, Sincoskie invented VLANs by adding a tag to each Ethernet packet. These tags could be thought of as colors, say red, green, or blue. Then each switch could be assigned to handle packets 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 packet 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.[6] 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, using them for the original purpose would be rather unusual.

In 2012 the IEEE approved IEEE 802.1aq (shortest path bridging) to standardize load-balancing and shortest path forwarding of (multicast and unicast) traffic allowing larger networks with shortest path routes between devices. It was stated by David Allan and Nigel Bragg, in *802.1aq Shortest Path Bridging Design and Evolution: The Architect's Perspective* that shortest path bridging is one of the most significant enhancements in Ethernet's history.[7]

Implementation

A basic switch 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] 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 the devices to another, distinct switch of their own.

Configuration of the first *custom* VLAN port group usually involves removing ports from the default VLAN, such that the first custom group of VLAN ports is actually the second VLAN on the device, in addition to the default VLAN. The default VLAN typically has an ID of 1.

If a VLAN port group were to exist only on one device, no ports that are members of the VLAN group would need to be tagged. These ports would hence be considered "untagged". 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 these ports must be tagged. This also applies to the default VLAN.

Some switches either allow or require that a name be created for the VLAN, but only the VLAN group number is important from one switch to the next.

Where a VLAN group is to simply pass through an intermediate switch via two pass-through ports, only the two ports must be a member of the VLAN, and are tagged to pass both the required VLAN and the default VLAN on the intermediate switch.

Management of the switch requires that the administrative functions be associated with one of the configured VLANs. If the default VLAN were deleted or renumbered without first moving the management connection to a different VLAN, it is possible for the administrator to be locked out of the switch configuration, requiring a forced clearing of the device configuration (possibly to the factory default) to regain access or physical access to the switch if it has a console port or other means of direct management.

Switches typically have no built-in method to indicate VLAN port members 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. These charts must be manually updated by the technical staff whenever port membership changes are made to the VLANs.

Remote configuration of VLANs involves the risk for the administrator to cut off communications accidentally and lose connectivity to the devices they are attempting to configure. Actions such as subdividing the default VLAN by moving the switch uplink ports into a separate new VLAN can suddenly terminate all remote connectivity, requiring the device to be physically accessed at the distant location to continue the configuration process.

Generally, VLANs within the same organization will be assigned different non-overlapping network addresses. 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 / CIDR 16). However, it is generally not possible to route data between two networks with overlapping addresses, so if the goal of VLANs is segmentation of a larger overall organizational network, non-overlapping addresses must be used in each separate VLAN.

Motivation

In a legacy network, users were assigned to networks based on geography and were limited by physical topologies and distances. VLANs can logically group networks to decouple the users' network location from their physical location. Technologies that can implement VLANs are:

- Asynchronous Transfer Mode (ATM)
- Fiber Distributed Data Interface (FDDI)
- Ethernet
- HiperSockets

- InfiniBand

Broadcast domains

In a network based on broadcasts to all listeners to find peers, as the number of peers on a network grows, the frequency of broadcasts also increases, potentially to a point that much of the network time and capacity is occupied with only sending broadcasts between all members. VLANs can help reduce network traffic by forming multiple broadcast domains, to break up a large network into smaller independent segments with fewer broadcasts being sent to every device on the overall network.

Protocols and design

IEEE 802.1Q

The protocol most commonly used today to configure VLANs is IEEE 802.1Q. The IEEE committee 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's ISL (Inter-Switch Link) and 3Com's VLT (Virtual LAN Trunk). 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 existing Ethernet frame, while 802.1Q uses a frame-internal field for tagging, and therefore does modify the Ethernet frame. This internal tagging is what allows IEEE 802.1Q to work on both access and trunk links: frames are standard Ethernet, and so can be handled by commodity hardware.

Under IEEE 802.1Q, the maximum number of VLANs on a given Ethernet network is 4,094 (the 4,096 provided for by the 12-bit VID field minus reserved values 0x000 and 0xFFF). 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. The VLAN limit is expanded to 16 million with Shortest Path Bridging.

Inter-Switch Link (ISL) is a Cisco proprietary protocol used to interconnect multiple switches and maintain VLAN information as traffic travels between switches on trunk links. This technology provides one method for multiplexing bridge groups (VLANs) over a high-speed backbone. It is defined for Fast Ethernet and Gigabit Ethernet, as is IEEE 802.1Q. ISL has been available on Cisco routers since Cisco IOS Software Release 11.1.

With ISL, an Ethernet frame is encapsulated with a header that transports VLAN IDs between switches and routers. ISL does add overhead to the packet as a 26-byte header containing a 10-bit VLAN ID. In addition, a 4-byte CRC is appended to the end of each frame. This CRC is in addition to any frame checking that the Ethernet frame requires. The fields in an ISL header identify the frame as belonging to a particular VLAN.

A VLAN ID is added only if the frame is forwarded out a port configured as a trunk link. If the frame is to be forwarded out a port configured as an access link, the ISL encapsulation is removed.

Early network designers often configured VLANs with the aim of reducing the size of the collision domain in a large single Ethernet segment and 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

broadcast domain at the MAC layer. A VLAN can also serve to restrict access to network resources without regard to physical topology of the network, although the strength of this method remains debatable as VLAN hopping[8] is a means of bypassing such security measures. VLAN hopping can be mitigated with proper switchport configuration.

VLANs operate at Layer 2 (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 Layer 3 (the network layer). 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.

Cisco VLAN Trunking Protocol (VTP)

Multiple VLAN Registration Protocol

Shortest Path Bridging

IEEE 802.1aq (Shortest Path Bridging SPB) allows all paths to be active with multiple equal cost paths, provides much larger layer 2 topologies (up to 16 million compared to the 4096 VLANs limit), faster convergence times, and improves the use of the mesh topologies through increased bandwidth and redundancy between all devices by allowing traffic to load share across all paths of a mesh network.

Establishing VLAN memberships

The two common approaches to assigning VLAN membership are as follows:

- Static VLANs
- Dynamic VLANs

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. 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-based VLANs

In a switch that supports protocol-based VLANs, traffic is 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.

For example, it is possible to connect the following to a given switch:

- A host generating ARP traffic to port 10
- A network with IPX traffic to port 20
- A router forwarding IP traffic to port 30

If a protocol-based VLAN is created that supports IP and contains all three ports, this prevents IPX traffic from being forwarded to ports 10 and 30, and ARP traffic from being forwarded to ports 20 and 30, while still allowing IP traffic to be forwarded on all three ports.

VLAN Cross Connect

VLAN Cross Connect (CC) 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
- Multiple VLAN Registration Protocol
- GARP VLAN Registration Protocol
- Private VLAN
- Virtual network
- VLAN access control list
- VoIP recording
- Virtual Private LAN Service
- Virtual private network
- Switch virtual interface
- Wide Area Network
- Software-defined networking

References

1. IEEE 802.1Q-2011, *1. Overview*
2. IEEE 802.1Q-2011, *1.4 VLAN aims and benefits*
3. "Engineering - Discovery Publication" (PDF). Discovery Institute. Retrieved 18 June 2015.
4. Amies A, Wu C F, Wang G C, Criveti M (2012). Networking on the cloud (http://www.ibm.com/developerworks/cloud/library/cl-networkingtools/index.html) *IBM developerWorks*, June 21.
5. 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
6. 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.
7. Allan, David; Bragg, Nigel (2012). *802.1aq Shortest Path Bridging Design and Evolution : The Architects' Perspective*. New York: Wiley. ISBN 978-1-118-14866-2.

8. Rik Farrow. "VLAN Insecurity". Archived from the original on 2014-04-21.

Further reading

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

External links

- IEEE's 802.1Q standard 1998 version (http://standards.ieee.org/getieee802/download/802.1Q-1998.pdf) (2003 version (http://standards.ieee.org/getieee802/download/802.1Q-2003.pdf))(2005 version (http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf))
- Cisco home page for Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) (http://www.cisco.com/en/US/tech/tk389/tk689/tsd_technology_support_protocol_home.html) (discusses DSL, DTP, GVRP, ISL, VTP, 802.1Q)
- Cisco's Overview of Routing between VLANs (http://www.cisco.com/en/US/docs/ios/12_2/switch/configuration/guide/xcfvl.html)
- University of California's VLAN Information (https://web.archive.org/web/20140312173147/http://net21.ucdavis.edu/newvlan.htm)
- OpenWRT guide to VLANs (http://wiki.openwrt.org/doc/networking/network.interfaces): Provides a beginners' guide to VLANs
- Study of VLAN usage in Purdue University's Campus Network (http://docs.lib.purdue.edu/ecetr/362/)
- Towards Systematic Design of Enterprise Networks (http://docs.lib.purdue.edu/ecetr/375/): Demonstrates how to systematically produce a VLAN design
- VLAN And Benefits (http://www.networkel.com/2015/10/virtual-local-area-network-vlan-and.html): Provides basic VLAN information and configuration steps.