

What is VLAN? How to configure a VLAN on Cisco Switch?

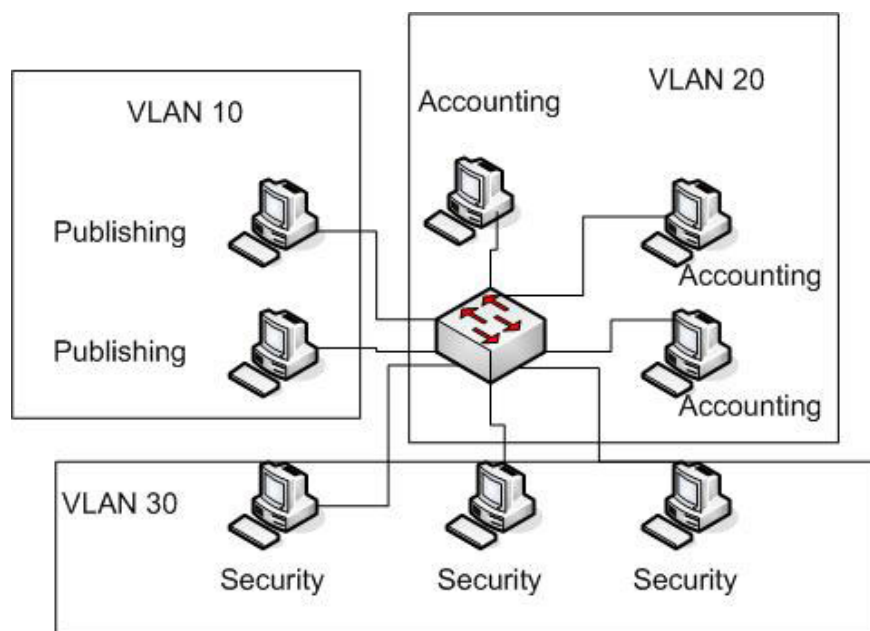
Have you ever asked yourself questions like virtual LAN or VLAN? When and why do you need a VLAN?

TipsMake.com - *Have you ever asked yourself questions like: virtual LAN (or VLAN)? When and why do you need a VLAN? The following article will share with you the basics of VLAN, giving you a sense of VLAN and its usefulness.*

What is VLAN?

Most of you understand what a LAN is. However, we should repeat a bit, because if you don't know what a LAN is, you won't be able to have a VLAN concept. A LAN is a local area network (short for Local Area Network), which is defined as all computers in the same broadcast domain. Keep in mind that routers block routers, while switches only forward them.

VLAN stands for Virtual Local Area Network or virtual LAN. A VLAN is defined as a logical group of network devices and is set up based on factors such as functions, parts, applications . of the company. Technically, VLANs are a broadcast domain created by switches. Normally, the router plays the role of creating the broadcast domain. For VLANs, switches can create broadcast domains.



This is done when you - the administrator - set some switch ports in the VLAN except VLAN 1 - the default VLAN. All ports in a single VLAN are in a single broadcast domain.

Since switches can communicate with each other, some ports on switch A may be in VLAN 10 and some ports on switch B may also be in VLAN 10. The broadcast messages between these computers will not be exposed. on ports belonging to any VLAN except VLAN 10. However, all of these computers can communicate with each other because they belong to the same VLAN. Without additional configuration, they will not be able to communicate with other computers outside this VLAN.

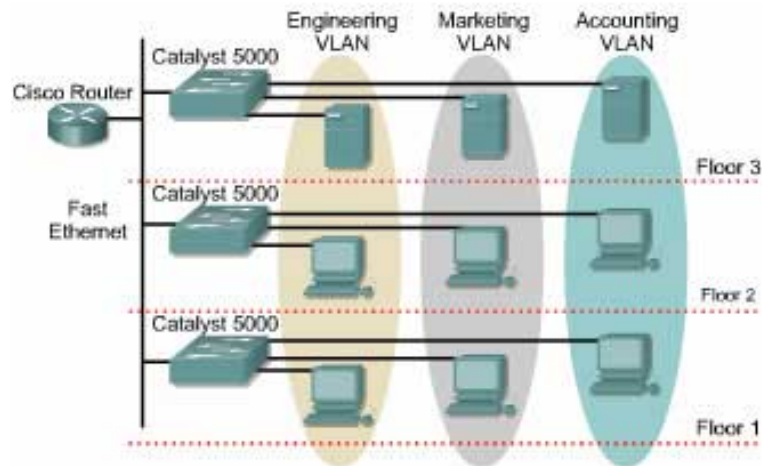
VLAN classification

1. **Port - based VLAN:** is a simple and popular VLAN configuration. Each switch port is attached to a specific VLAN (default is VLAN 1), so any host device attached to that port belongs to a certain VLAN.
2. **MAC address based VLAN:** This configuration is rarely used because of the inconvenience in management. Each MAC address is marked with a specific VLAN.
3. **Protocol - based VLAN:** This configuration is similar to MAC Address based, but uses a logical address or IP address to replace the MAC address. The configuration is no longer common using the DHCP protocol.

Is VLAN necessary?

Currently, VLAN plays a very important role in LAN technology. To see clearly the benefits of VLANs, let us consider the following case:

Suppose a company has 3 divisions: Engineering, Marketing, Accounting, each of which is spread out over 3 floors. To connect computers in one part together, we can install each switch on each floor. That means that each floor must use 3 switches for 3 parts, so to connect 3 floors in the company need to use 9 switches. Obviously, this method is very expensive and cannot take full advantage of the inherent port numbers of a switch. Therefore, VLAN solution was born to solve the problem in a simple way but still save resources.



As shown in the figure above, each layer of the company needs only one switch, and this switch is divided into VLANs. The computers in the engineering department will be assigned to VLAN Engineering, the PCs in other parts will also be assigned to the corresponding VLANs, Marketing and Accounting. This way of making it possible to save the maximum number of switches must be used and make the most of the available ports.

Benefits of VLANs

1. **Saving bandwidth of the network system:** VLAN divides the LAN into several small segments, each of which is a broadcast domain. When there is a broadcast, it is transmitted only in the corresponding VLAN. Therefore, dividing VLANs saves network bandwidth.
2. **Increased security:** Because devices on different VLANs cannot access each other (unless you use a router that connects VLANs). As in the above example, computers in VLAN accounting can only communicate with each other. The machine in VLAN accounting cannot be connected to the computer at VLAN engineer (Engineering).
3. **Easily add or remove computers to VLANs:** Adding a computer to the VLAN is simple, just configure the port for that machine to the desired VLAN.
4. **High network flexibility:** VLANs can easily move devices. Suppose in the above example, after a period of use the company decided to leave each part on a separate floor. With VLANs, you only need to reconfigure switch ports and place them on the required VLANs. VLANs can be configured static or dynamic. In a static configuration, the network administrator must configure each port of each switch. Then, assign it to a VLAN. In the dynamic configuration, each switch port can configure its VLAN based on the MAC address of the connected device.

One important thing I need to emphasize is that you don't need to configure a virtual LAN unless your computer network is too big and has too much traffic. Many times people use VLAN simply because the computer network they are working on already uses them.

Another important issue is that on Cisco switches, VLANs are enabled by default and all computers are in a VLAN. That VLAN is VLAN 1. So by default, you can use all ports on the switch and all computers are able to communicate with each other.

When do you need a VLAN?

You need to consider using VLAN in the following cases:

1. You have more than 200 computers in the LAN
2. Broadcast traffic in your LAN is too large
3. Workgroups need to increase security or be slowed because of too many advertisements.
4. Workgroups need to be on the same broadcast domain because they are sharing applications. For example, a company uses VoIP phones. Some people who want to use the phone may belong to another VLAN, not with regular users.
5. Or just to convert a single switch into multiple virtual switches.

Why not subnet?

One common question is why not subnet (instead of using VLAN)? Each VLAN should be in its own subnet. VLANs have advantages over subnets in that computers in different physical locations (not returning to the same router) can be in the same network. The drawback of dividing subnets with a router is that all computers on that subnet must be connected to the same switch and that switch must be connected to a port on the router.

With VLANs, a computer can be connected to this switch while another computer can connect to the other switch, all computers are still on the same VLAN (broadcast domain).

How can computers on different VLANs communicate with each other?

Computers on different VLANs can communicate with a router or a Layer 3 switch. Since each VLAN is its own subnet, a Layer 3 switch or router must be used to route between subnets.

What is trunk port?

When a link between two switches or between a router and a switch carries the traffic of multiple VLANs, that port is called trunk port.

Trunk port must run special communication protocol. The protocol used may be Cisco's proprietary ISL protocol or IEEE 802.1q standard.

How to create VLANs?

How to configure a VLAN network can vary depending on different Cisco switch models. Your goal is:

1. Create a new VLAN
2. Set each port to the appropriate VLAN

Suppose we want to create VLAN 5 and 10. We want to put port 2 and 3 into VLAN 5 (Marketing) and port 4 and 5 into VLAN 10 (HR). Here's how to do it on the Cisco 2950 switch:

```
COM1 (1) - SecureCRT
File Edit View Options Transfer Script Window Help
CAT1#
09:59:20: %SYS-5-CONFIG_I: Configured from console by console
CAT1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CAT1(config)#da?
% Unrecognized command
CAT1(config)#vlan 5
CAT1(config-vlan)#name marketing
CAT1(config-vlan)#exit
CAT1(config)#vlan 10
CAT1(config-vlan)#name humanresources
CAT1(config-vlan)#exit
CAT1(config)#interface fast
CAT1(config)#interface fastEthernet 0/2
CAT1(config-if)#switchport mode access
CAT1(config-if)#switchport access vlan 5
CAT1(config-if)#exit
CAT1(config)#interface fastEthernet 0/3
CAT1(config-if)#switchport mode access
CAT1(config-if)#switchport access vlan 5
CAT1(config-if)#exit
CAT1(config)#interface fastEthernet 0/4
CAT1(config-if)#switchport mode access
CAT1(config-if)#switchport access vlan 10
CAT1(config-if)#exit
CAT1(config)#interface fastEthernet 0/5
CAT1(config-if)#switchport mode access
CAT1(config-if)#switchport access vlan 10
CAT1(config-if)#exit
CAT1(config)#
```

At this point, only ports 2 and 3 can communicate with each other as only ports 4 and 5 can communicate with each other. The reason is because they are on the same VLAN. In order for the computer on port 2 to communicate with the computer on port 4, you need to configure the trunk port to the router so that it can disassemble the VLAN information, route the packet and replenish the VLAN information.

What does VLAN provide?

VLANs increase the performance of medium and large LANs because they restrict broadcast messages. As the number of computers and the traffic flow increases, the number of broadcast packets also increases. By using VLANs, you will limit the advertisement.

VLANs also enhance security because you essentially put a group of computers in a VLAN on their own network.

summary

Below is a summary of the main ideas in the lesson:

1. VLAN is a broadcast domain created by switches.
2. The administrator must create a VLAN and then specify which port to VLAN manually.
3. VLANs increase performance for medium and large LANs.
4. All computers are in VLAN 1 by default.
5. The trunk port is a special port that uses the ISL or 802.1q protocol, so that it can transmit traffic of multiple VLANs.
6. For computers of different VLANs to communicate with each other, you need to use a router or Layer 3 switch.

You finished reading the article "**What is VLAN? How to configure a VLAN on Cisco Switch?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

