The related terms of switch

Switch

Switches are devices used to implement switched networks. In ISO's OSI model, it is located on the second layer-data link layer, which can operate on frames and is a smart device.

IEEE 802.3

The standard for Ethernet .

IEEE 802.3u

The standard for Fast Ethernet.

IEEE 802.3ab

The standard for Gegabyte Ethernet (UTP).

IEEE 802.3z

The standard for Gegabyte Ethernet(fiber or copper).

IEEE 802.3x

The standard for Access control.

IEEE 802.1X

The standard for access control on port.

IEEE 802.1q

The standard for VLAN.

IEEE 802.1p

The standard for traffic priority control.

IEEE 802.1d

The spanning tree protocol.

DLL(data link layer)

It is located on the second floor the ISO/OSI model and are responsible for a series of methods such as testing, flow control and resend error-free data transmit a frame for the unit on the line node to node, make the upper layer (network layer) seems to be an error-free links.

Full duplex and half-duplex

In the network, full duplex is receiving and sending data via two different channels, which can be carried out simultaneously without any interference. And half duplex is receiving and sending data via the same channel, which can only be sent or received at the same moment, so half duplex may has the conflication.The switch is a full-duplex device.

MAC address

The MAC address is the address used in the media access layer, which is the physical address of the network card (LAN node). In the physical transmission, the mainframe (LAN node) is identified by physical address, and it is generally the only one in the world.The current MAC address generally use the 6 bytes and 48 bits.

IP address

An IP address is a 32bit address assigned to each mainframe access to the Internet. Each mainframe can be accessed through an IP address.

Auto-Negotiation

The auto-negotiation standard enables the switch to adapt to the working rate and working mode refer to the following order: 100M full duplex, 100M and half duplex, 10M full duplex, 10M and half duplex.

The traffic control of full duplex

Following the IEEE 802.3x standard, when network congestion, network devices use predefined Pause frames to control the traffic.

The traffic control of half duplex

Based on the IEEE802.3x standard, when the processor finds that the buffer is about to fill, it sends a false conflicting signal to the originator, delays a moment, and then continues to send.Can alleviate and eliminate congestion.

Line speed

The theoretical maximum value of switch data transmission.

Broadcast storm control

Broadcast on the network frame (forward) by number increase sharply and affects network communication of the abnormal phenomenon, broadcast storm will quite objective of network bandwidth, cause the entire network cannot work normally.Broadcast storm control is to allow ports to filter broadcast storms that appear on the network.When the broadcast storm control is enabled, the port will automatically discard the broadcast frame received when the broadcast frame received by the port accumulates to the predetermined threshold value.When this feature is not enabled or the broadcast frame is not accumulated to the threshold, the broadcast frame is normally broadcast to other ports on the switch.

Trunk

It is often used to aggregate multiple ports to form a high-bandwidth data transmission channel.Switches treat all ports that are clustered together as a logical port.

VLAN(Virtual Local Area Network

It is composed of a set of workstations broadcast domain, the mainframes (switch ports) which are in the same VLAN to communicate with each other, it can build logic working group without consider the specific wiring structure. It is flexible configured and increase the security of the system.

Port VLAN

On the unmanaged switch, there's a VLAN mode. Each POE port is isolated to inhibit the broadcast storm and enhance the stability of the switch.

Tag VLAN

Based on IEEE 802.1q, different VLAN are divided by VID.

VID（VLAN ID）

A VLAN identifier used to represent a Tag VLAN.

The digestion time of MAC address

Each port on the switch has the function of automatic learning address, and the source address (source MAC address, switch port number) of the frame sent and received via port will be stored in the address table. Digestion time is a parameter that affects the learning process of switches. From one address records join the table to chronography, if the port in digestion time have not received the source address to the MAC address of the frame, so the address will be delete from dynamic forwarding address table (the source MAC address, the destination MAC address and their corresponding switch port number). Static MAC address table is not affected by address digestion time.

Static address table

Static MAC address is different from dynamic MAC addresses. Once the static address item is added, the address will remain valid until it is removed, it will not effected by the digestion time .The static address table records the static address. one of the MAC address in a static address table corresponds to a port, and if do certain setting, all data sent to this address will only be forwarded to that port. It also a MAC address binding.

MAC address filtering

MAC address filtering is by configuring the filter address to allow the switch to filter the data frames that are not expected to be forwarded. When the restricted MAC address is connected to the switch, the switch automatically filters the destination address to the

frame of the address for security purposes.The address in the filter address table takes effect on all switch ports.The addresses that have been added to the filter address table cannot be added to the static address table and cannot be dynamically bound by the port.

Dynamic MAC address binding

Dynamic address binding means that the port of the switch can dynamically learn MAC address in dynamic address binding state, but the number of learning addresses is limited. When the port learns a MAC address, it is immediately bound and then the next address.The bound address do not be effected by the digestion time and will remain valid. After learning a certain number of addresses, ports are no longer learning and binding.The MAC address bound by the port will not be released until the port address binding is disabled.

Port security

When port security is enabled on a port, the port will not learn the new MAC address, and only forward the data frame of the MAC address which has been learned, and the other data frames will be discarded. If the source address is a member of the MAC address table of that port, then it is allowed to forward, otherwise it will be discarded. When the port security option is disabled, the port will resume automatically learning the new MAC address and forward the received frame.

Cable testing

When the switch port is connected with the appropriate twisted pair, the state of the twisted pair can be tested by the switch to confirm whether there is any problem and where the problem occurs.

SNMP

Simple Network Management Protocol (SNMP) is the Protocol of the OSI layer 7 (application layer) for remote monitoring and configuration of Network devices. SNMP enables the network management workstation to read and modify the setting values of gateways, routers, switches, and other network devices.

IGMP（Internet Group Management Protocol）

IP manages multicast communication by using switches, multicast routers, and mainfame that support IGMP. A group of mainframes, routers (or switches) and members of the same multicast group communicate multicast data streams. And all devices in this group use the same multicast group address. IGMP Snooping technology has been applied to

video, which greatly improves network utilization. In the network, when IP multicast communication is performed for various multimedia applications, you can reduce unnecessary bandwidth usage by setting IGMP on each port of the switch.

IEEE 802.1D/STP

The IEEE 802.1d spanning Tree Protocol automatically disconnects the loop when it detects there's a loop on the network. When there are multiple connections between the switches, the primary one is only started, and the other connections are blocked and the connections are turned into alternate connections. When a problem occurs in the main connection, the spanning tree protocol automatically takes the backup connection to replace the main connection, without any human intervention.

IEEE 802.1X Authentication protocl

Port Base Network Access Control Protocol. The protocol architecture is divided into three parts: client, authentication system and authentication server. Our company has built-in 802.1x authentication system to provide advanced charging solution for users.