Host location technology of campus network based on MAC address

Ding Ma¹, Xuelong Wang²

¹ Information Center, Xi’an Shiyou University, Xi’an, Shaanxi, 710065, China
² Information Center, Xi’an Shiyou University, Xi’an, Shaanxi, 710065, China
*Corresponding author’s e-mail: 58761926@qq.com

Abstract. With the increasingly strong nature of campus network teaching and service in the university, network management and security management are slowly catching up with the development of campus network construction. How to strengthen network security and public opinion supervision, how to locate the suspected computer location in the campus network has become an important problem. This paper proposes the campus network platform of colleges and universities as an example, expounds the process of computer physical location, analyzes the problems generated in the tracking process, and finally summarizes the application.

1. Introduction
As the campus network has become more and more powerful in the teaching and service of universities, the scale of network have also increased. In recent years, the performance of campus network decline, virus intrusion, network congestion and other issues are both plaguing and hindering the campus network management department. It’s important to locate the virus personal computer, abnormal host and small route interference host in the campus network. The campus network management department realize that it should strengthen the security management and effective control. At present, the campus network construction of each university is generally a three-layer design, the core layer, the aggregation layer, and the access layer. This article discusses how to locate and locate a target host in a campus network under a three-tier architecture.

2. Introduction to the three-tier architecture of the campus network
At present, the domestic campus network architecture is mainly a three-tier architecture[1]. From top to bottom, the core layer, the aggregation layer, and the access layer are respectively. The function of the core layer is to implement route transmission between the backbone areas, which is a convergence layer device. The key to inter-connection is generally designed for high availability and high redundancy. The core layer provides fast and large-scale data forwarding services to other lower layers.

The function of the aggregation layer is mainly connecting the core layer and the access layer. The aggregation layer usually has a large number of network segments. The communication between all gateways needs to be searched for by the core layer. This layer first aggregates the data from the access layer switch, transmits it to the core layer, and finally sends it to the final destination. The aggregation layer uses policies to control the traffic of the network and performs routing between the virtual VLAN defined by the access layer.

The access layer is responsible for connecting users, collecting user message information and communicating with hosts in other gateways through the gateway. This layer contains network devices
such as routers, switches, bridges, hubs, and AP. The access layer provides a protocol method for connecting devices to the network.

3. **MAC address positioning principle**

MAC (Media Access Control) address[2] used to indicate the identifier of each node on the Internet, a total of six bytes, 48 bits, of which the first three bytes are given by the IEEE registry Codes assigned by different manufacturers (the first 24 bits), also known as "the only identifier on the address", the last three bytes (the last 24 bits) are assigned by the many manufacturers to the network adapter interface of the production, called the extended identifier. Thus, such a 48-bit address constitutes the physical address of a unique node in the world. In the perspective of the MAC address we analyze the data transmitted in the three-tier architecture, and to find out the steps of host positioning.

3.1. **Establishment of access layer MAC address table**

There is a personal computer named host A, it sends a data frame to the switch. After the data frame enters the switch from Ethernet 1/0/1 of Switch A, the switch checks the source MAC address field in the data frame to set the field value (the MAC address of host A). Put it in the MAC address table of Switch A and associate it with Ethernet1/0/1 port, indicating that the host connected to the port is host A.

Similarly, when the switch receives the data of host B, host C, and host D, it will learn and store its address in the MAC address table, and finally generate a complete address table, as shown in Figure 1. At this time, if the data is only transmitted within the topology range of the switch connection, when the host host A sends a data frame to the host C, the MAC address table can be used to find the corresponding port, and the other ports are no longer affected, thereby establishing a relationship between the two hosts. Communication.

![Figure 1. MAC address table in Switch A](image)

3.2. **Three-layer exchange principle**

Each device connected to the access layer switch needs to be configured with an IP address, a sub-net mask, and a default gateway. These parameters are used for routing packets to be transmitted outside the aggregation layer (including the aggregation layer). First, the IP packet will be forwarded to the local default gateway. Second, the aggregation switch has integrated the routing function on its own backplane, the gateway data will be exchanged locally for Layer 3 routing[3]. The aggregation switch will look up the IP packet and find it in the routing table and finally appropriate next hop address and send it out.

3.3. **Routing table creation**

In the campus network, information exchange between sub-nets is performed by routing. The Layer 3 switch simply selects an appropriate routing path based on the destination address of the received data header and transmits the data packet to the next Layer 3 switch. The last three-layer switch in the path is responsible for sending the packet to the sub-net where the destination host is located. Layer 3
switches are characterized by forwarding one by one. Below we describe the establishment of the routing table.

The routing table[4] is the basis for the Layer 3 switch to forward packets. Each Layer 3 device maintains this routing table. Each routing information in the table indicates which of the Layer 3 switches the packet should pass through to a physical port transmission, this principle is the same as the MAC address table, because it effectively avoids the repeated and untargeted transmission of data packets, effectively improving the backplane bandwidth rate. The routing table contains the destination address, network mask, outbound interface, next hop address, metric, and other related parameters.

4. MAC address look-up in the campus network

We simulate a local area of the campus network. As shown in Figure 2, the aggregation equipment of the home area and the office area is connected to the core switch, and the access switch of the 1# building of the home area is connected to the aggregation switch of the home area, and the library access switch is connected to the office area aggregation switch.

![Figure 2. Local topological map of a university](image)

4.1. Network analysis with Wireshark capture tool

It is found that the Internet access speed of the library access switch is slow, and the CPU utilization of the switch is high. After the packet capture analysis by Wireshark[5], a large number of abnormal packets with the MAC address 2810-7b4f-e94c appear. As the Figure 3 shows that The MAC address is found to flow from the Ten-Gigabit port 1/0/54 in the MAC address table of the access switch.

![Figure 3. MAC address in the abnormal network](image)

4.2. Look-up from the aggregation layer to the core layer

The debug finds that the Ten-Gigabit port is connected to the aggregation switch of the office area, and then searches in the MAC address table of the aggregation switch, and finds that the MAC address
is forwarded from the core switch. Since the core switch is connected to each area of the campus network, the illegal MAC address can not be judged from so many access equipments.

4.3. Look-up from the aggregation layer to the access layer

Through data search, it is found that the MAC is forwarded from the family area aggregation switch, so that it can be roughly judged that the network interference of the library is caused by a device in the family area, and the MAC address is found in the routing table of the home area aggregation switch. It was found that it was forwarded from the access switch of Building 1# in the home area. Finally, we can lock the source of the illegal MAC address according to the port-room comparison table of Building 1# as shown in Figure 4.

![Port-room comparison table](image)

5. Conclusion

The process demonstrates the campus network location by the tool of the MAC address. The MAC address is globally unique, and all network devices in the world, including routers, switches, bridges, and wireless access devices have the MAC addresses. We can locate the network communication device in the world based on the MAC address accurately.

Acknowledgments

Thanks to the teachers in the Information Center of Xi’an Shiyou University for their help and support of this project.

References

[1] Guo C, Wu H, Tan K, et al. (2008) A scalable and fault-tolerant network. In: Proceedings of the Special Interest Group on Data Communication. Seattle. pp. 75-86.
[2] Xie X R. (2008) computer network. Electronic Industry Press, Beijing.
[3] Yao J, Tao J. (2005) Research and Implementation of Key Technologies of Route Switching Prototype System. Computer Engineering. 13: 109-111.
[4] DAH M C, RAM S, CHIU D M. (1992) Network Monitoring Explained: Design and Application. Prentice Hall Publishing, Massachusetts.
[5] Luo Q L, Xu K F, Zang W Y. (2011) Network protocol parsing and verification method in wireshark environment. Computer engineering and Design. 32: 770-773.