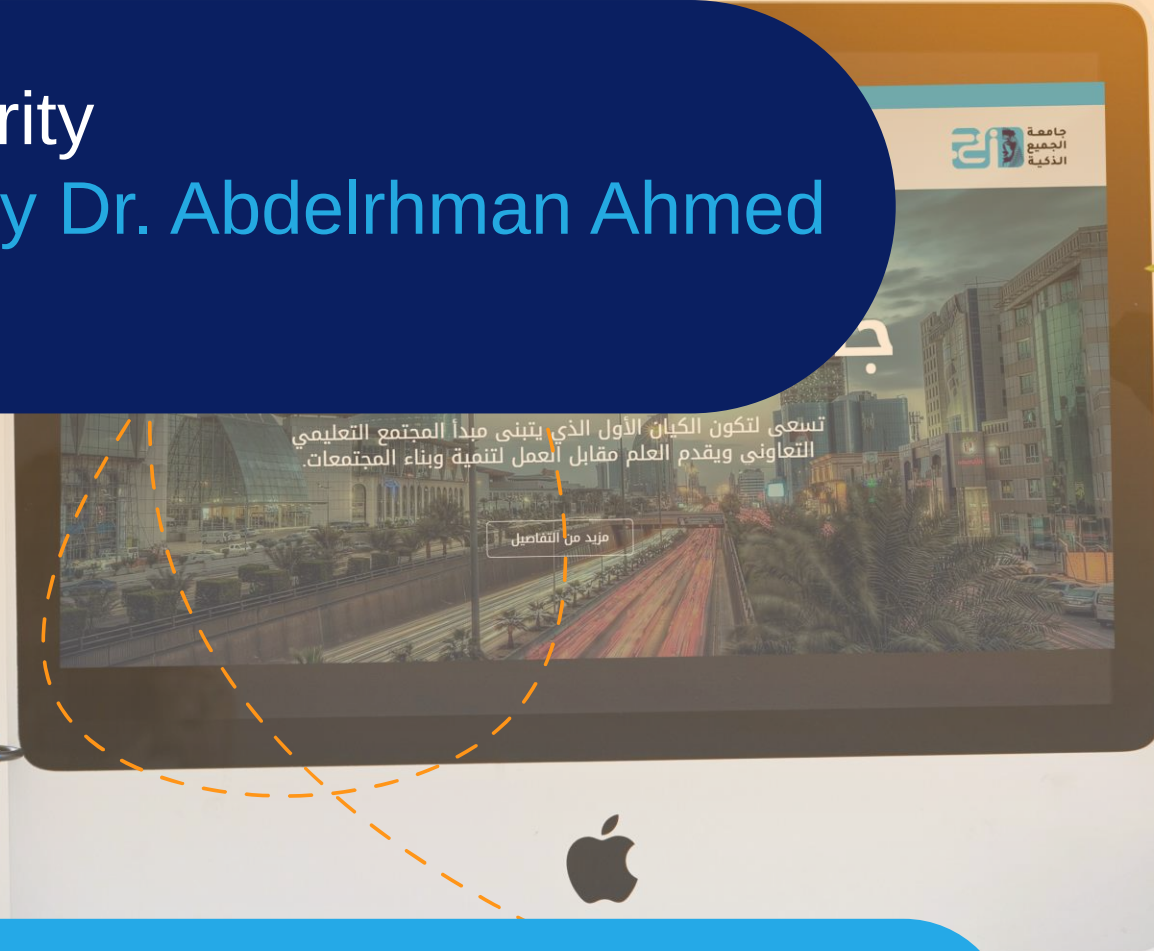


HCIA Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 3



جامعة الذكاء
EVERYONE'S SMART UNIVERSITY

Common Network Devices

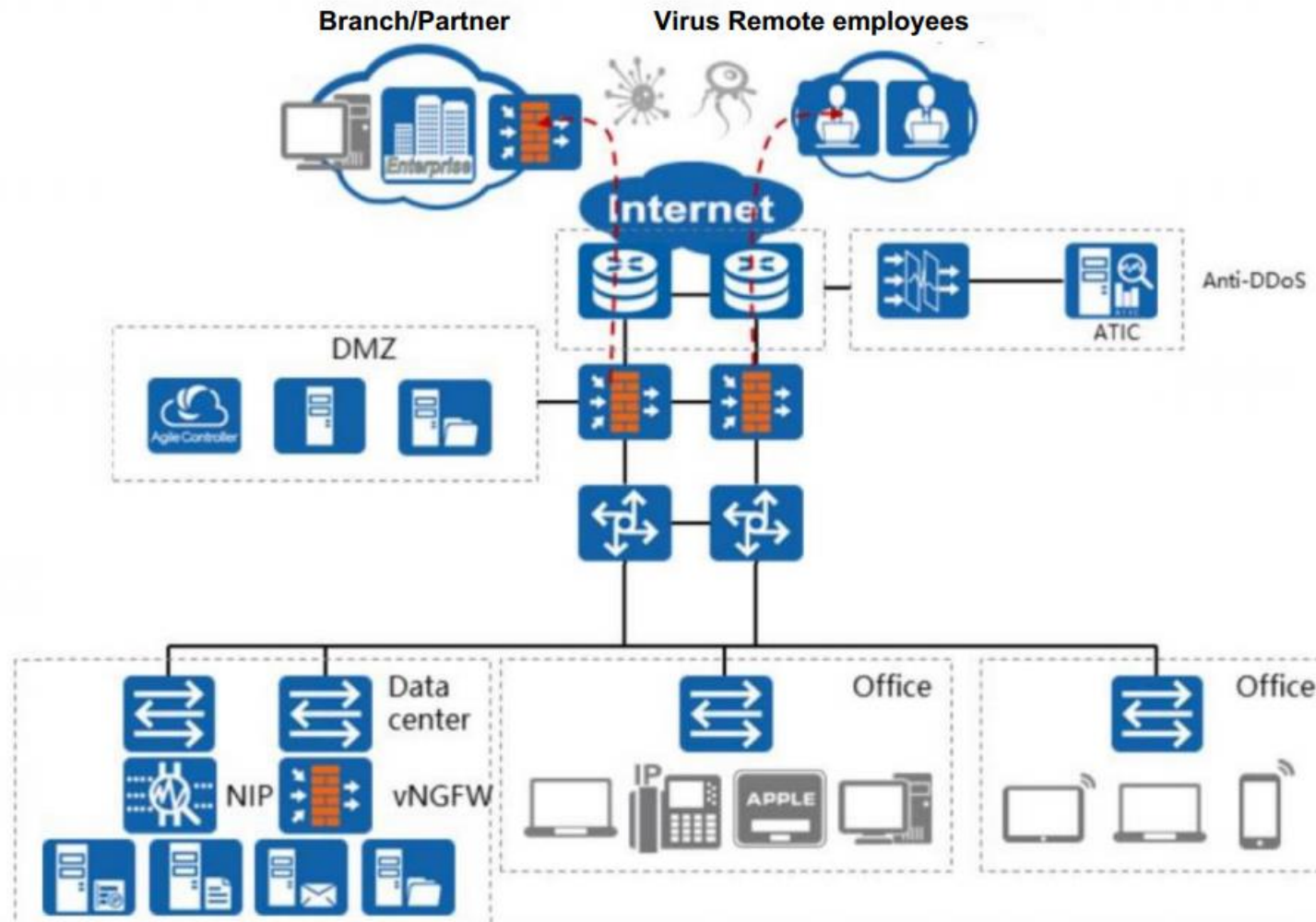
- Network devices are the basic components of a network. When planning and constructing a network, you need to deploy and configure the network devices to meet network connection or network security requirements.



Objectives

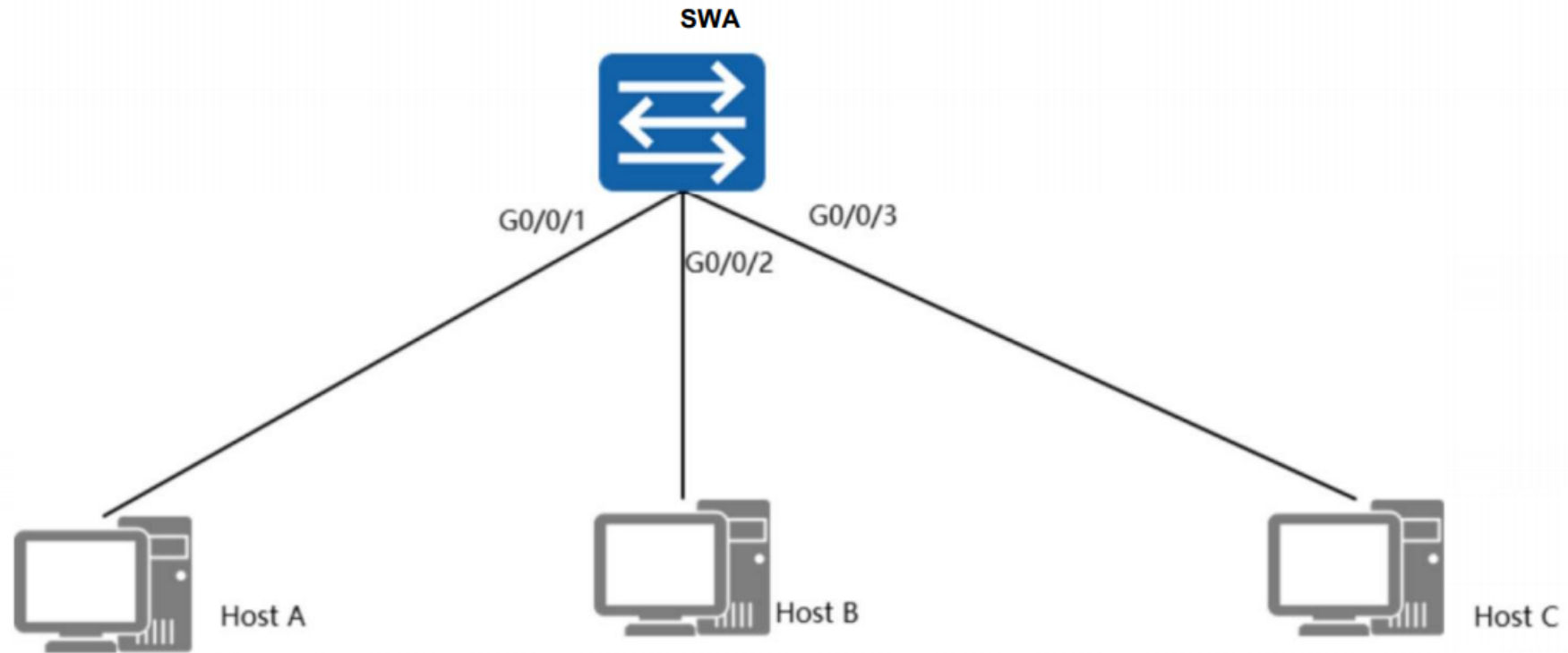
- Upon completion of this course, you will be able to:
 - Describe Huawei common network devices.
 - Describe the functions of network devices.
 - Log in to network devices and perform basic configurations.





- **Router:** device for communications across network segments
- **Switch:** device for communications on the same network segment or across network segments
- **Anti-DDoS:** The anti-distributed denial of service (DDoS) system is deployed at the network egress in bypass mode. It is upstream of the firewall to reduce the firewall's packet processing load.
- **NGFW:** The next-generation firewall (NGFW) can be deployed at the network egress to provide preliminary protection or to protect the data center from attack.
- **vNGFW:** The virtual NGFW (vNGFW) is deployed on virtual machines (VMs) and has similar functions to a hardware firewall.
- **NIP:** The next-generation intrusion prevention (NIP) system is a Huawei-developed intrusion detection and prevention device that can be deployed in a data center to provide protection against intrusion.
- **Agile-Controller:** The agile controller is an automated network resource control system used for access control. It is based on users and applications and is deployed in the DMZ.

A switch works at the data link layer and forwards data frames.

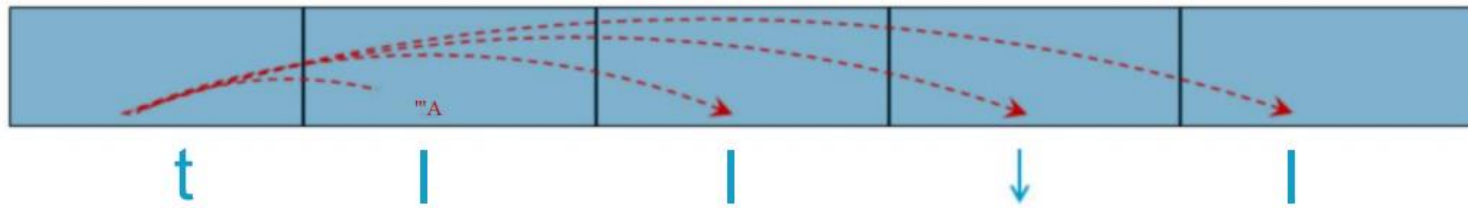


IPaddress: 10.1.1.1/24
MAC address: 00-01-02-03-04-AA

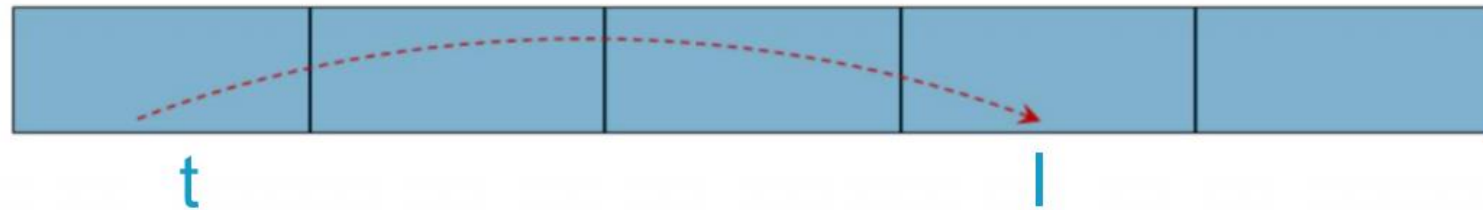
IPaddress: 10.1.1.2/24
MAC address: 00-01-02-03-04-BB

IPaddress: 10.1.1.3/24
MAC address: 00-01-02-03-04-CC

- As the number of users on an enterprise network increases, a switch can be deployed to provide a sufficient number of access interfaces. In addition, a switch completely solves the conflict issue of the Ethernet, greatly improving the performance and security of the Ethernet.
- A switch works at the data link layer and forwards data frames. After receiving the data frame, a switch forwards a data frame according to the header information.
- Next, let's take a small switch network as an example to explain the basic working principles of a switch.



Flooding



Forwarding



Discarding

- A switch has a MAC address table that stores the mapping between MAC addresses and switch interfaces. A MAC address table is also called a Content Addressable Memory (CAM) table.
- As shown in the figure, a switch can perform three types of frame operations: flooding, forwarding, and discarding.
 - **Flooding:** The switch forwards the frames received on an interface through all other interfaces. (It does not forward frames through the interface that receives them).
 - **Forwarding:** The switch forwards the frames received on an interface through another interface (it does not forward frames through the interface that receives them).
 - **Discarding:** The switch discards the frames received on an interface.

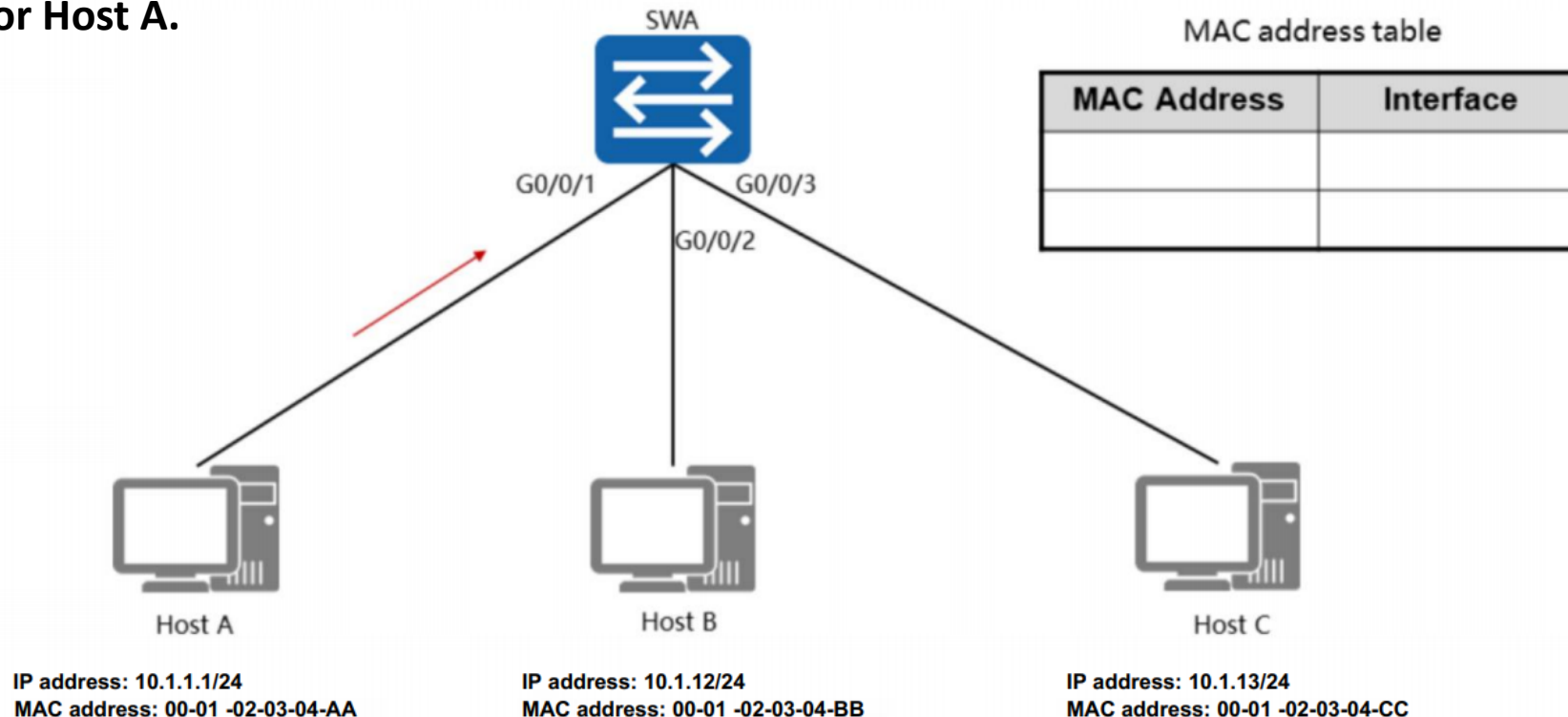
The basic working principles of a switch are as follows:

- Upon receipt of a unicast frame, the switch searches the MAC address table for the destination MAC address of the frame.
 - If the MAC address cannot be found, the switch floods the frame.
 - If the MAC address is found, the switch forwards the frame if the MAC address is not that of the interface on which the frame was received. Otherwise, the switch discards the frame.

If a switch receives a broadcast frame, the switch does not check the MAC address table but directly performs the flooding operation.

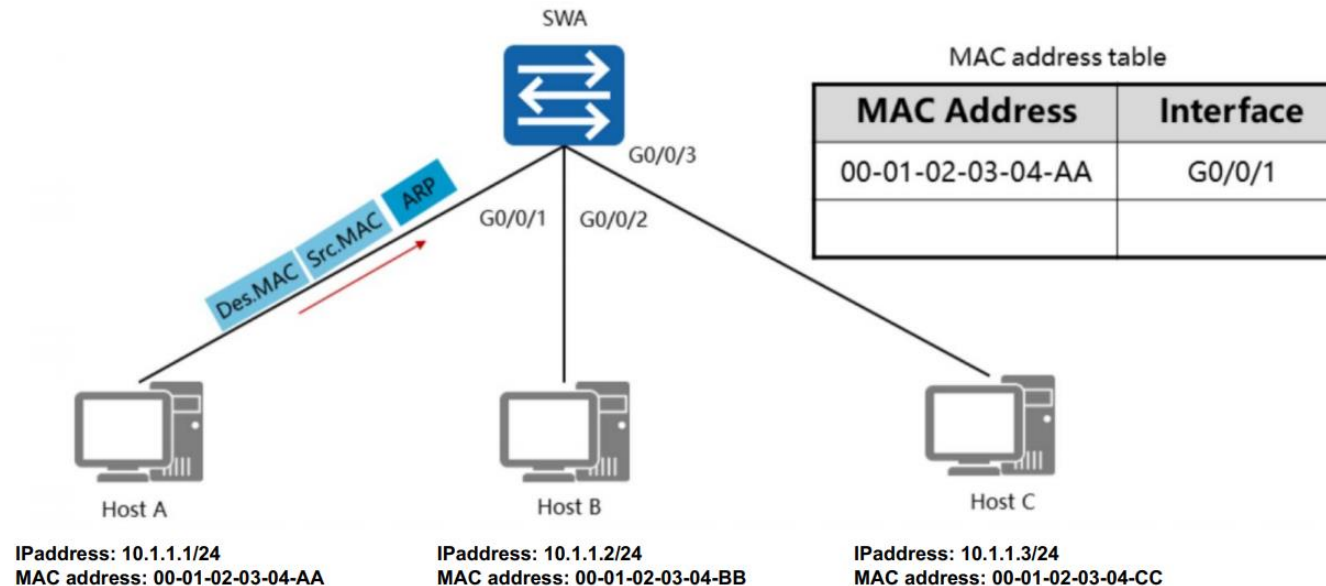
Upon receipt of a broadcast frame, the switch directly floods the frame without checking the MAC address table. For a multicast frame, the switch performs complex processing that is beyond the scope of this course. In addition, a switch has the capability to learn information from received frames. Upon receipt of a frame, a switch checks the source MAC address of the frame, maps this address to the interface that receives the frame, and saves the mapping to the MAC address table.

- In the initial state, the MAC address table of a switch is empty.
- In the initial state, a switch does not know any MAC addresses of the connected hosts. Therefore, the MAC address table is empty. In this example, SWA is in the initial state. Before receiving a data frame from Host A, SWA's MAC address table contains no entry for Host A.

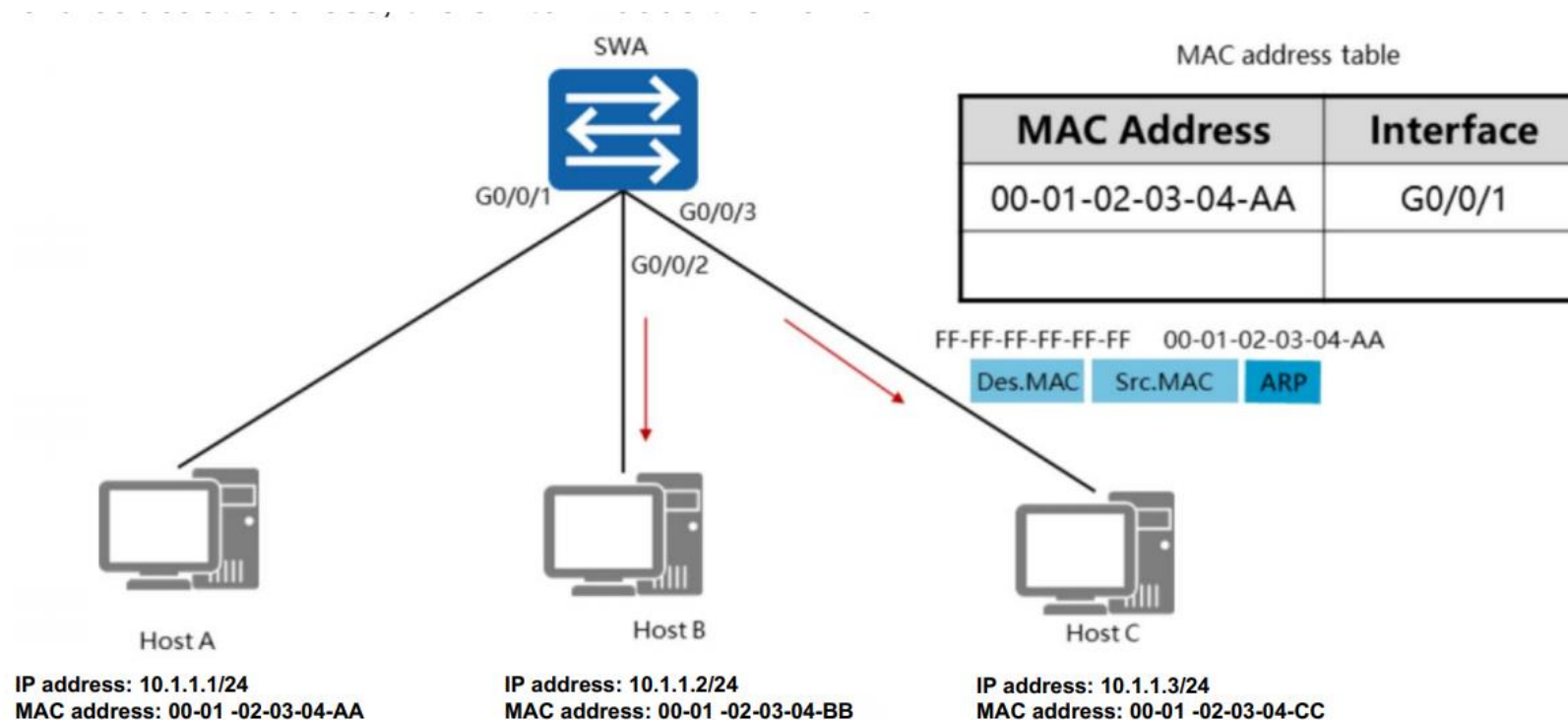


The switch records the source MAC address and corresponding interface of the received data frame in the MAC address table.

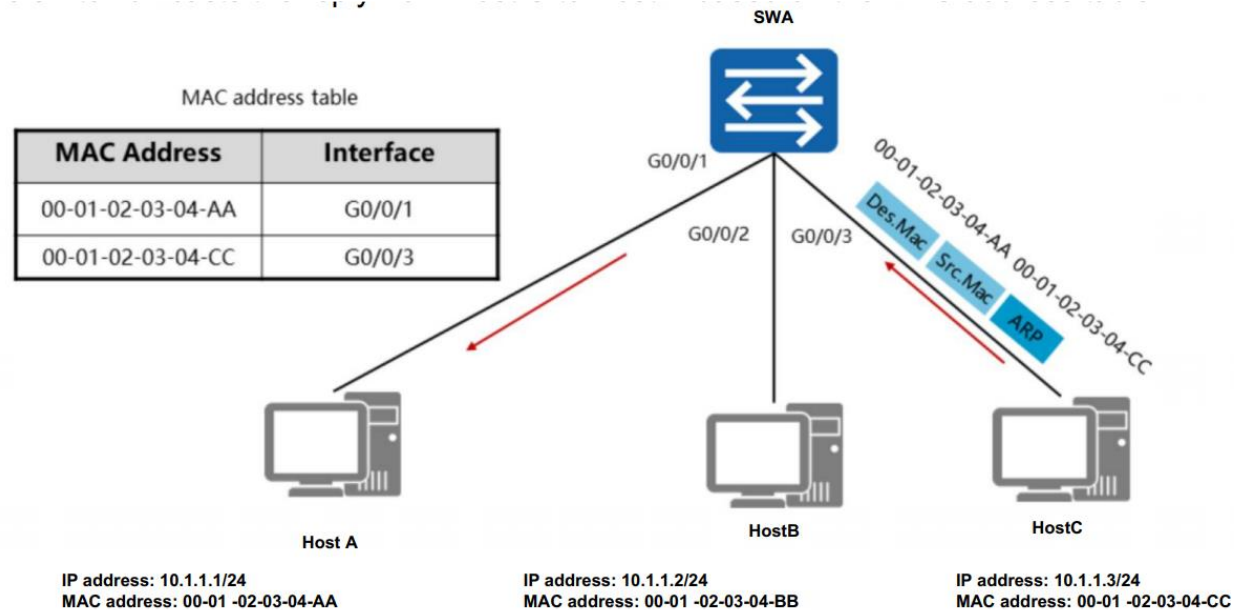
- When Host A sends data to Host C, it sends an ARP request to obtain the MAC address of Host C. In the ARP request, the destination MAC address is the broadcast address, and the source MAC address is the MAC address of Host A. After receiving the ARP request, SWA adds the mapping between the source MAC address and the receiving interface to the MAC address table. The aging time of MAC address entries learned by X7 series switches is 300 seconds by default. If SWA receives a data frame from host A again within the aging time, SWA updates the aging time of the mapping between Host A's MAC address and G0/0/1. After receiving a data frame whose destination MAC address is 00-01-02-03-04-AA, SWA forwards the frame through interface G0/0/1.



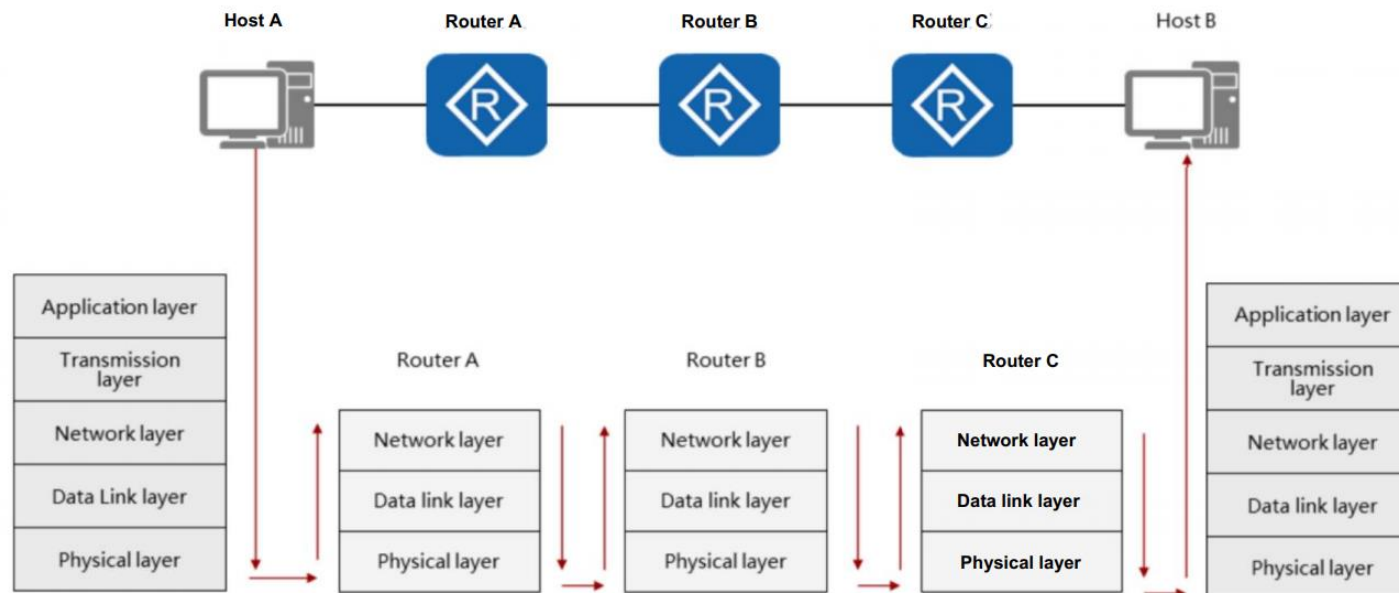
- When the destination MAC address of a data frame is not in the MAC address table or it is a broadcast address, the switch floods the frame.
- In this example, the destination MAC address of the ARP request sent by Host A is a broadcast address. Therefore, the switch broadcasts the ARP request to Host B and Host C through interfaces G0/0/2 and G0/0/3.



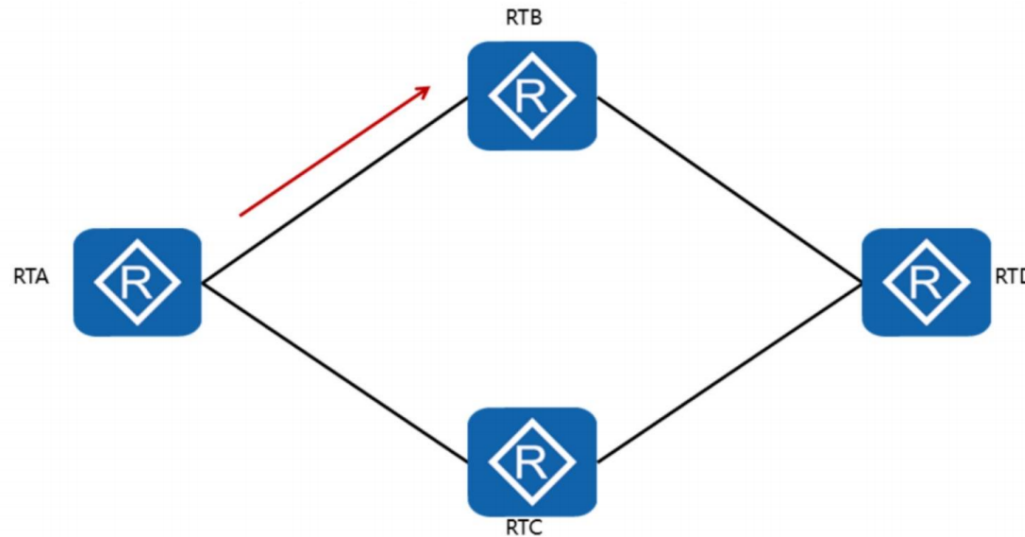
- The switch unicasts the reply from Host C to Host A based on the MAC address table.
- After receiving the ARP request, Host B and Host C query the ARP packet. Host C processes the ARP request and sends an ARP reply. However, Host B does not reply. The destination MAC address of the ARP reply is the MAC address of Host A and the source MAC address is the MAC address of Host C. After receiving the ARP reply, SWA adds the mapping between the source MAC address and the receiving interface to the MAC address table. If the mapping exists in the MAC address table, the mapping is updated. Then SWA queries the MAC address table, finds the corresponding forwarding interface according to the destination MAC address of the frame, and forwards the ARP reply through G0/0/1.



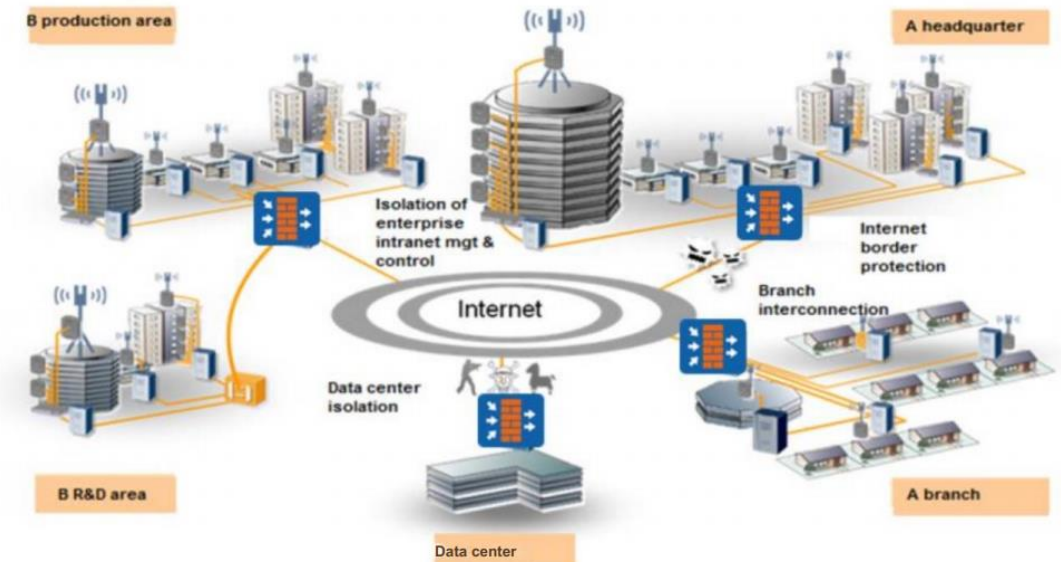
- **Function: forwards data packets between different networks**
- **A router is a network layer device that forwards packets between different networks. As shown in the figure, host A and host B reside on different networks. When host A wants to communicate with host B, host A sends a frame to host B. Upon receipt of this frame, the router that resides on the same network as host A analyzes the frame. At the data link layer, the router analyzes the frame header and determines that the frame is sent to itself. It then sends the frame to the network layer. At the network layer, the router determines to which network segment the destination address belongs based on the network layer packet header of the frame. It then searches the table and forwards the frame through the corresponding interface to the next hop destined to host B.**



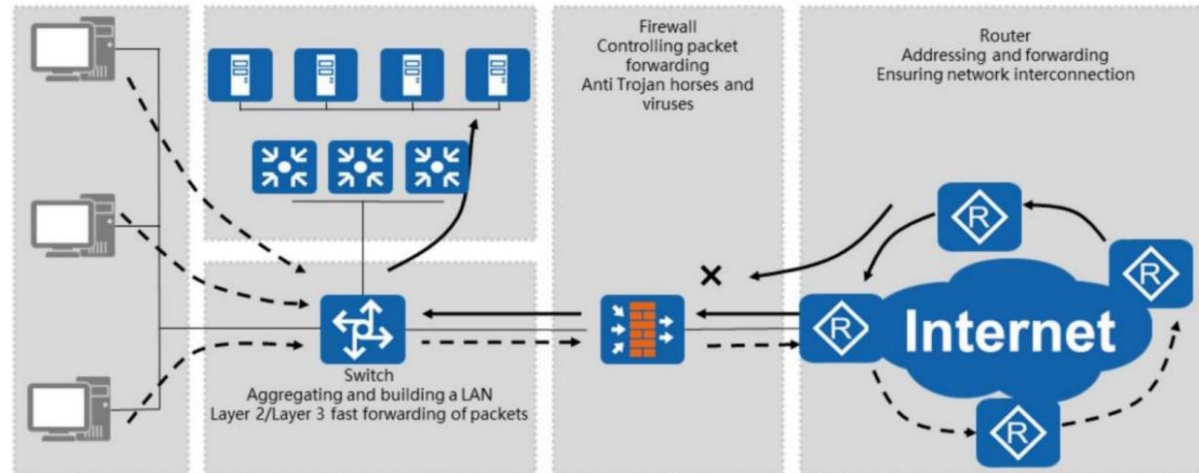
- A router selects an optimal path for data packets and forwards the packets.
- After receiving a packet, a router selects an optimal path according to the destination IP address of the packet. It then forwards the packet to the next router. The last router on the path forwards the packet to the destination host. The transmission of data packets on the network is similar to a relay race. Each router forwards data packets to the next hop router according to the optimal path, and the packets are forwarded to the destination through the optimal path. In some cases, because certain routing policies are implemented, the path through which the data packets pass may not be optimal.
- A router can determine the forwarding path of data packets. If multiple paths exist to the destination, the router determines the optimal next hop according to calculations specific to the routing protocol in use.

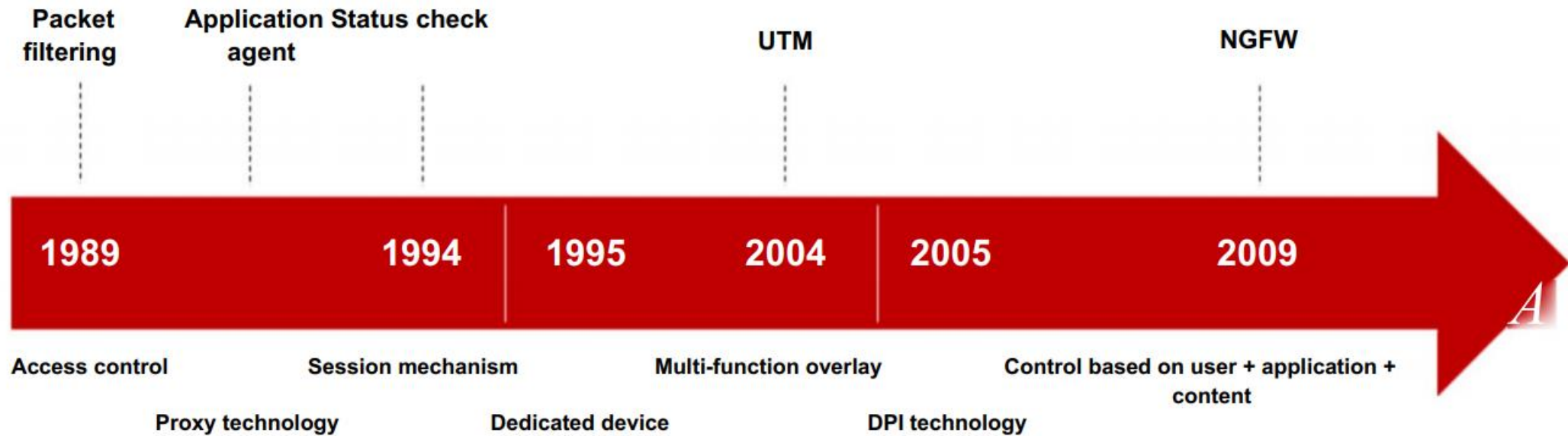


- A firewall is mainly used to protect one network area against network attacks and intrusions from another network area.
- The word "firewall" was first used in the construction field, where a firewall's primary function is to isolate and prevent a fire from spreading. In the communications field, a firewall device is usually deployed to meet certain requirements by logically isolating networks. It blocks various attacks on networks and allows normal communication packets to pass through.
- In communications, a firewall is mainly used to protect one network area against network attacks and intrusions from another network area. Because of its isolation and defense capabilities, it can be flexibly applied to network borders and subnet isolation, for example, enterprise network egress, internal subnet isolation, and data center border.



- The primary function of routers and switches is forwarding, whereas that of firewalls is controlling.
- Firewalls are different from routers and switches. A router is used to connect different networks and ensure interconnection through routing protocols so that packets can be forwarded to the destination. A switch is usually deployed to set up a local area network (LAN) and serve as an intermediate hub for LAN communications. A switch forwards packets through Layer 2/Layer 3 switching. A firewall is deployed at the network border to control access to and from the network. Security protection is the core feature of a firewall. The primary function of routers and switches is forwarding, whereas that of firewalls is controlling.
- It is common for mid-range and low-end devices to integrate router and firewall functionality. Huawei has released a series of such all-in-one devices. Currently, there is a trend for mid-range and low-end routers and firewalls to integrate for function complementary. Huawei has released a series of such all-in-one devices.





- The earliest firewall can be traced back to the late 1980s. Broadly speaking, firewall development can be divided into the following phases:

□ 1989-1994:

- Packet filtering firewalls were developed in 1989 for simple access control. This type of firewall is called the first-generation firewall.
- Proxy firewalls were developed soon after and acted as a proxy for communications between an intranet and an extranet at the application layer. This type of firewall is referred to as the second-generation firewall. Proxy firewalls have high security but low processing. In addition, developing a proxy service for each type of application can be difficult. Therefore, a proxy is provided for only a few applications.
- In 1994, the industry released the first stateful inspection firewall, which determined what action should be performed by dynamically analyzing packet status. Because it does not need to proxy each application, a stateful inspection firewall provides faster processing and higher security. This type of firewall is called the third-generation firewall.

□ 1995-2004:

- During this period, stateful inspection firewalls had gained popularity. In addition to access control, firewalls also provided other functions, such as VPN
- At the same time, specific devices started to appear, for example, Web Application Firewalls (WAFs) that protect web servers.
- In 2004, the industry proposed the concept of United Threat Management (UTM). This concept integrates the conventional firewall, intrusion detection, antivirus, URL filtering, application control, and mail control into one firewall for all-round security protection.

□ From 2005 to now:

- After 2004, the UTM market developed rapidly, and the UTM products mushroomed, but new problems arose. First, the detection degree of the application layer information was limited, and a more advanced detection method is required, which makes the Deep Packet Inspection (DPI) technology widely applied. Next was performance issues. When multiple functions are running at the same time, the processing performance of the UTM deteriorated greatly.
- In 2008, the industry released the next-generation firewall to solve the performance deterioration issue when multiple functions were running at the same time. In addition, management and control can be performed based on users, applications, and content.
- In 2009, the industry defined the next-generation firewall to specify its functions and features. Subsequently, security vendors launched their next generation firewall products, and firewalls entered a new era.

- Security zone (or zone):

- ☐ A local logical security zone
- ☐ A network connected to one or more interfaces

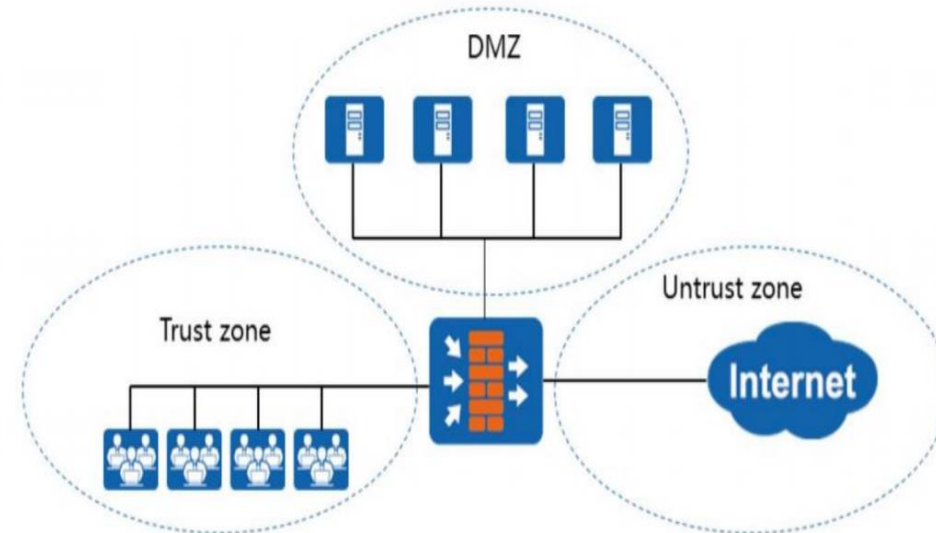
- Zone functions:

n Security policies are implemented based on security zones.

- ☐ Data flows in the same security zone bring no security risks and therefore require no security policies.
- ☐ The firewall performs security checks and implements security policies only when data flows between security zones.
- ☐ All devices on the networks connected to the same interface must reside in the same security zone, and one security zone may contain the networks connected to multiple interfaces.

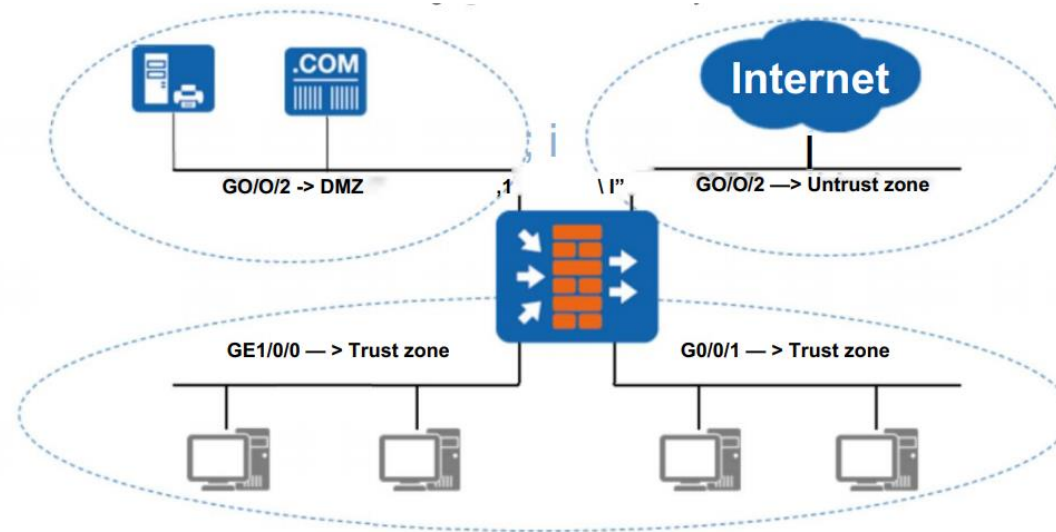
- Default security zones

- ☐ Untrust zone
- ☐ DMZ
- ☐ Trust zone
- ☐ Local zone



Relationship Between Firewall Security Zones and Interfaces

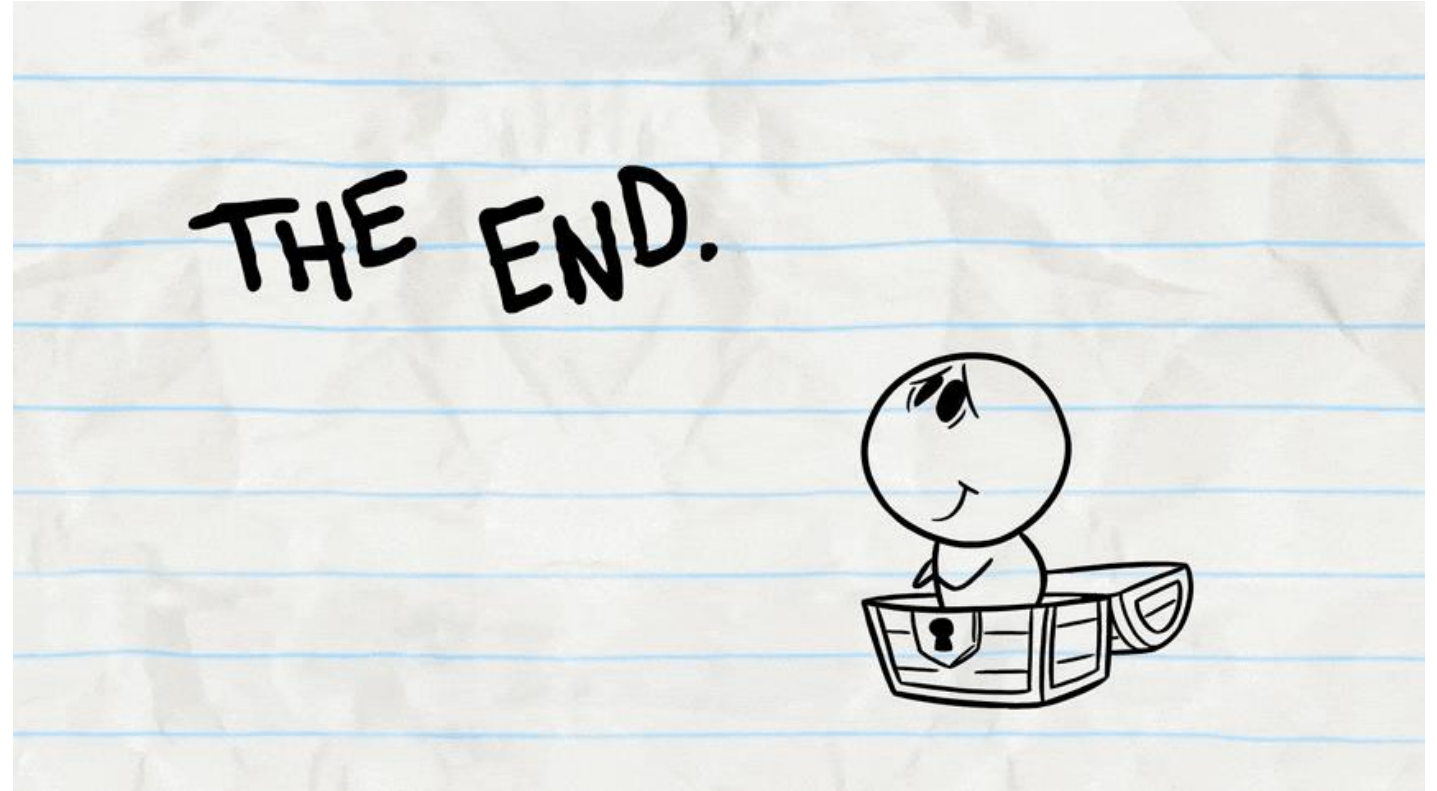
- Does the firewall have two security zones with the same security level?
 - Does the firewall allow the same physical interface to belong to two different security zones?
 - Can different interfaces on a firewall belong to the same security zone?
-
- All devices on the networks connected to the same interface must reside in the same security zone. Each security zone may contain networks connected to multiple interfaces. The interfaces can be physical or logical interfaces. Users on different network segments connected to the same physical interface can be added to different security zones by using logical interfaces such as sub interfaces or VLANIF interfaces.
 - Question: If different interfaces belong to the same security zone, does the inter-zone security forwarding policy take effect?



The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY