

HCIA Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 2

جامعة الجميع الذكية

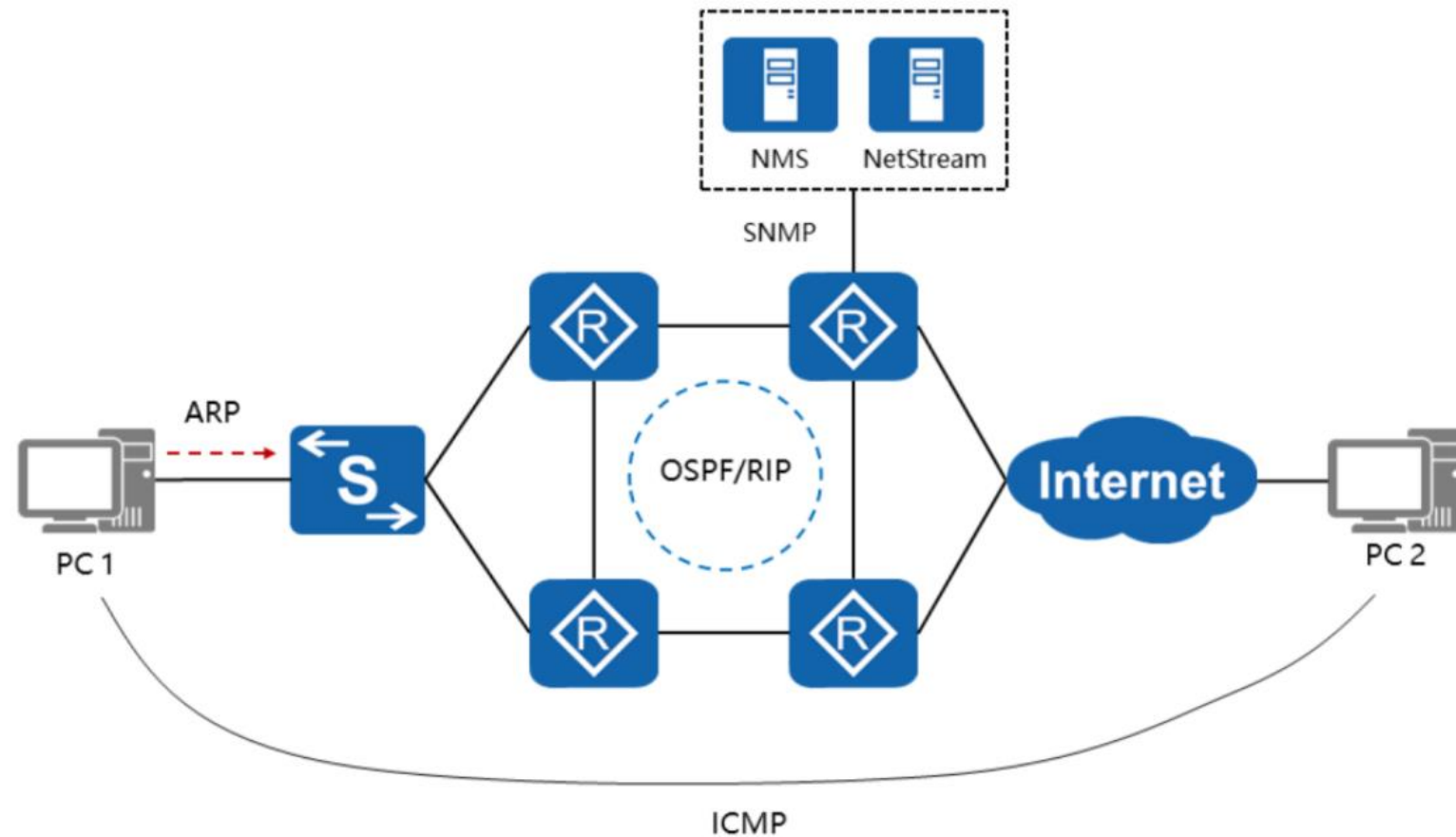
تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Common Network Protocols



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Common Network Protocols

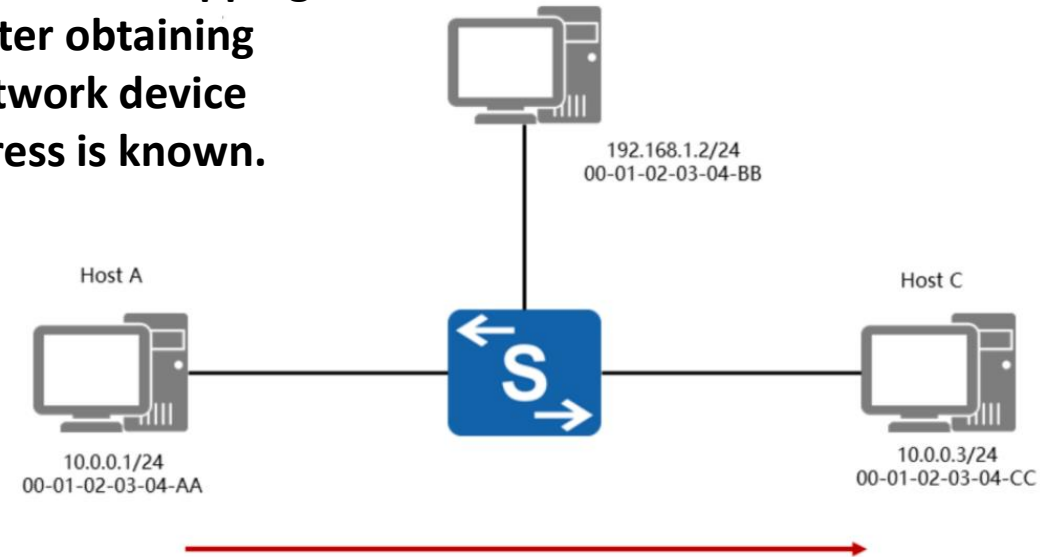


Common Network Protocols

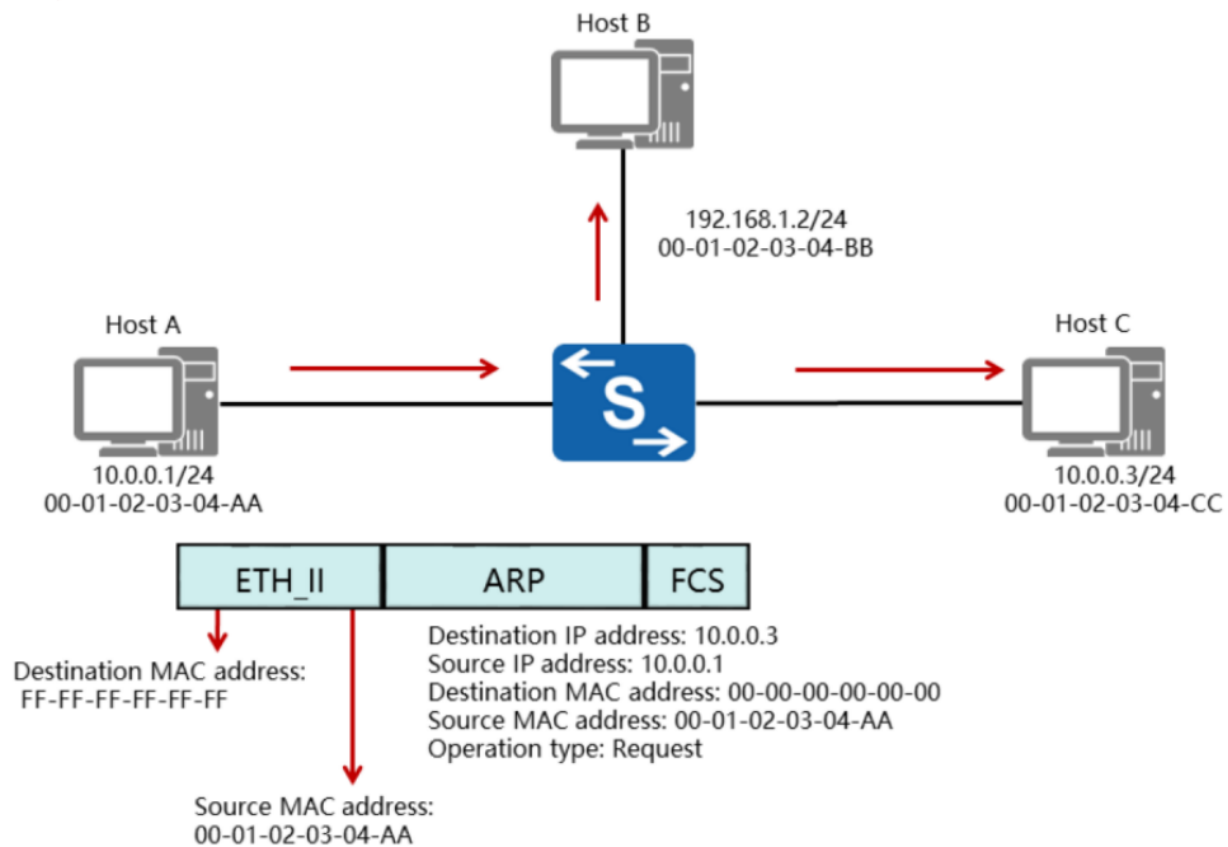
- **ARP:** When a packet is forwarded to a host or gateway in the same network segment, the destination address is known and the MAC address corresponding to the destination address is obtained. In the same network segment, the MAC address is used for communications.
- **ICMP:** ICMP is used to test network connectivity. Typical applications are Ping and Tracert.
- **Routing protocol:** Used for communications between users in different network segments.
- **SNMP:** a network device management protocol
- **NetStream:** an information sampling protocol. It is usually associated with other devices, such as AntiDDoS.

Overview of ARP

- ❖ Before sending a data packet to Host C, Host A needs to obtain the MAC of Host c
- By using the ARP protocol, a network device can establish a mapping between a destination IP address and MAC address. After obtaining the destination IP address at the network layer, the network device needs to determine whether the destination MAC address is known.

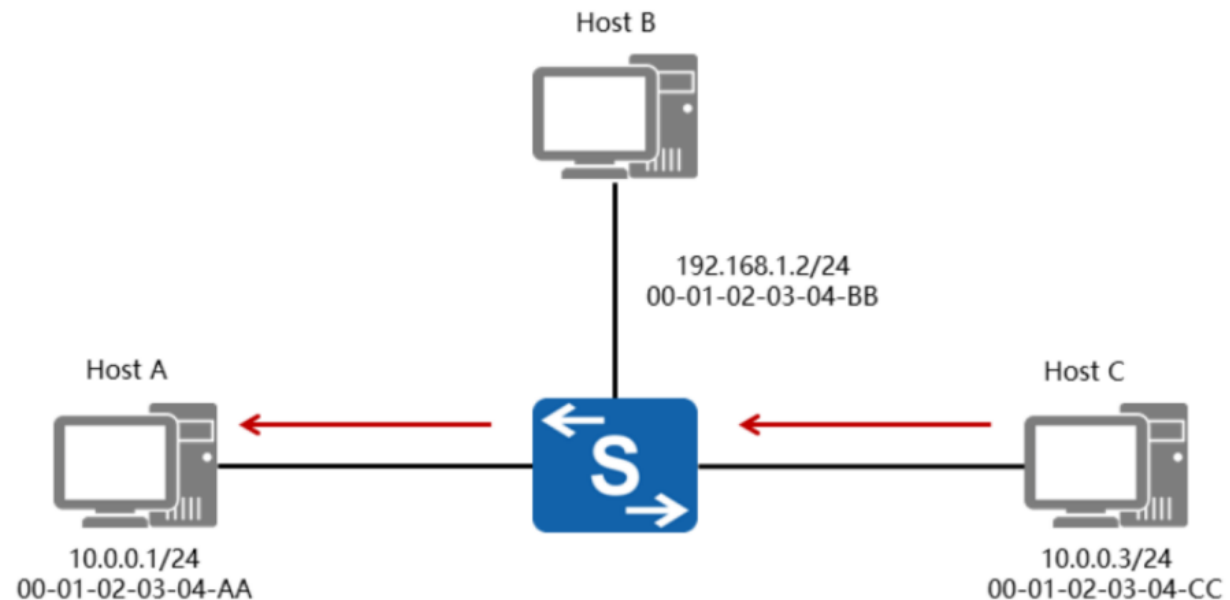


ARP Request



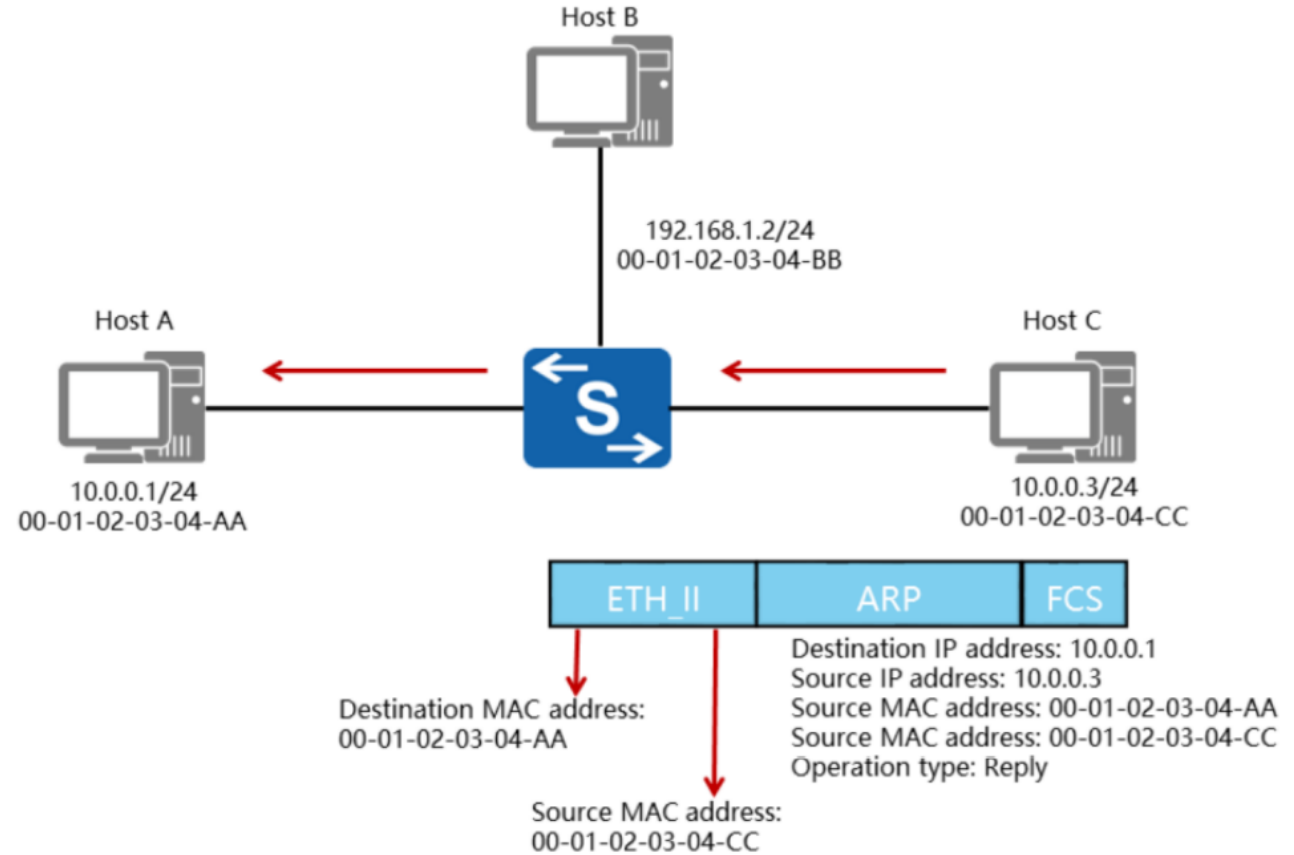
- ❖ In this example, the ARP cache table of Host A does not contain the MAC address of Host C. Therefore, Host A sends an ARP request packet to obtain the destination MAC address. ARP request packets are encapsulated in Ethernet frames. In the frame header, the source MAC address is the MAC address of Host A. In addition, because Host A does not know the MAC address of Host C, the destination MAC address is the broadcast address FF-FF-FF-FF-FF-FF.
- ❖ The ARP request packet contains the source IP address, destination IP address, source MAC address, and destination MAC address. The destination MAC address in the packet is all zeros. ARP request packets are broadcast to all hosts, including gateways, on the network. The gateway will prevent the packet from being sent to other networks.

- After receiving the ARP request packet, each host checks whether the target protocol address matches its IP address. If the addresses do not match, the host ignores the ARP request packet. If the addresses match, the host creates an entry in its ARP cache table, recording the source MAC address and source IP address in the ARP request packet. The host then replies with an ARP reply packet.



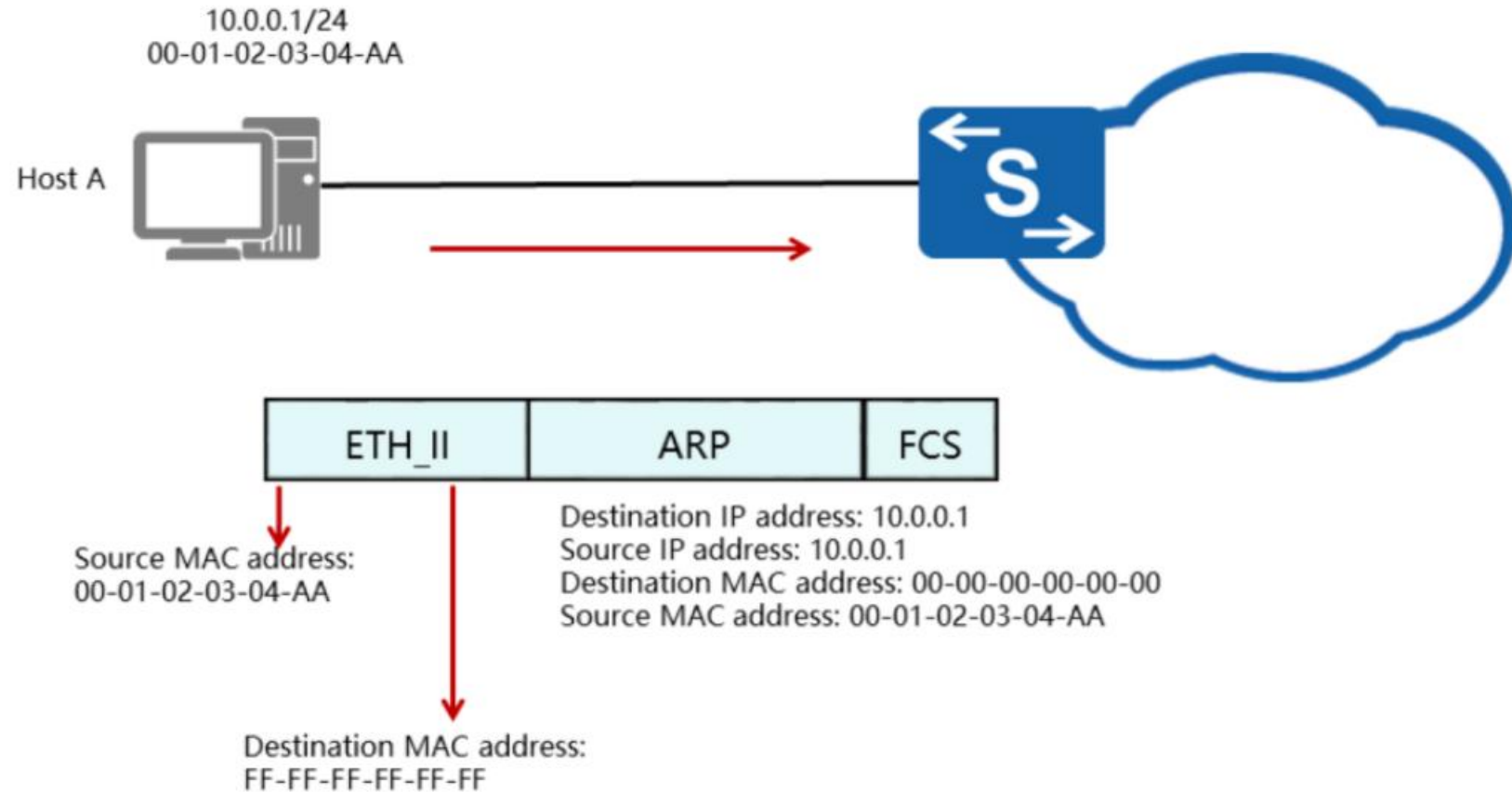
```
Host C>arp -a
Internet address Physical address Type
10.0.0.1         00-01-02-03-04-AA Dynamic
```

- Host C unicasts an ARP reply packet to Host A. In the ARP reply packet, the sender protocol address is the IP address of Host C, and the target protocol address is the IP address of Host A. In the Ethernet frame header, the destination address is the MAC address of Host A, and the source MAC address is the MAC address of Host C. The operation code is set to Reply. ARP does not provide any security protection measures and therefore, authentication cannot be performed. Malicious users may exploit this weakness to launch attacks, such as MAC address spoofing. For details, see the following sections.



Gratuitous ARP

- Gratuitous ARP can be used to detect whether IP addresses conflict.

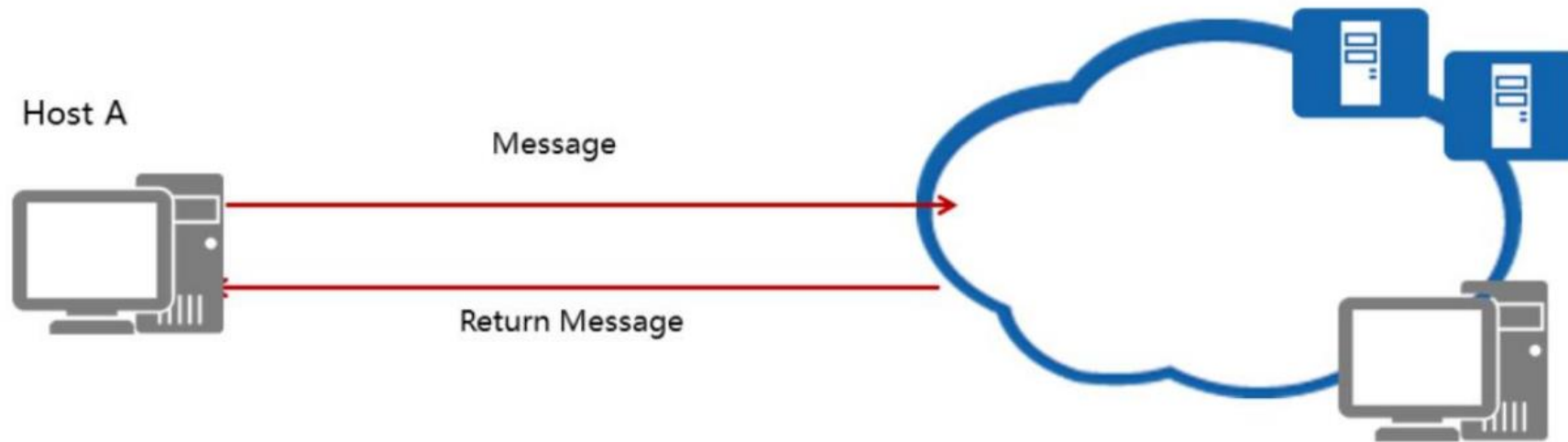


Gratuitous ARP

- After an IP address is encompassed to the host, the IP address must be checked to ensure that it is unique on the network and does not conflict with another address. The host sends ARP request packets to detect address conflicts.
- Host A sets the destination IP address in the ARP request packet to its own IP address and broadcasts the packet on the network. If Host A receives an ARP reply, it knows that the IP address is in use and can detect IP address conflict.

Introduction to ICMP

- ICMP is used to transmit error, control, and query messages.



- ICMP is one of the core protocols in the TCP/IP protocol stack. ICMP is used to send control packets between IP network devices to transmit error, control, and query messages.

ICMP Application: Ping (1)



```
<Router A>ping ?
STRING<1-255> IP address or hostname of a remote system
-a           Select source IP address, the default is the IP address of the
            output interface
-c           Specify the number of echo requests to be sent, the default is
            5
-d           Specify the SO_DEBUG option on the socket being used
-f           Set Don't Fragment flag in packet (IPv4-only)
-h           Specify TTL value for echo requests to be sent, the default is
            255
-i           Select the interface sending packets
...
```

ICMP Application: Ping (1)

- A typical ICMP application is the ping command. Ping is a common tool for checking network connectivity and collecting related information. In the ping command, users can assign different parameters, such as the length and number of ICMP packets, and the timeout period for waiting for a reply. Devices construct ICMP packets based on the parameters to perform ping tests.
- Common Ping parameters:
 - ❑ -a source-ip-address: Specifies the source IP address for sending ICMP Echo Request packets. If the source IP address is not specified, the IP address of the outbound interface is used by default.
 - ❑ -c count: Specifies the number of times that ICMP Echo Request packets are sent. The default value is 5.
 - ❑ -h ttl-value: Specifies the Time To Live (TTL) for ICMP Echo Request packets. The default value is 255.
 - ❑ -t timeout: Specifies the timeout period of waiting for an ICMP Echo Reply packet after an ICMP Echo Request packet is sent.



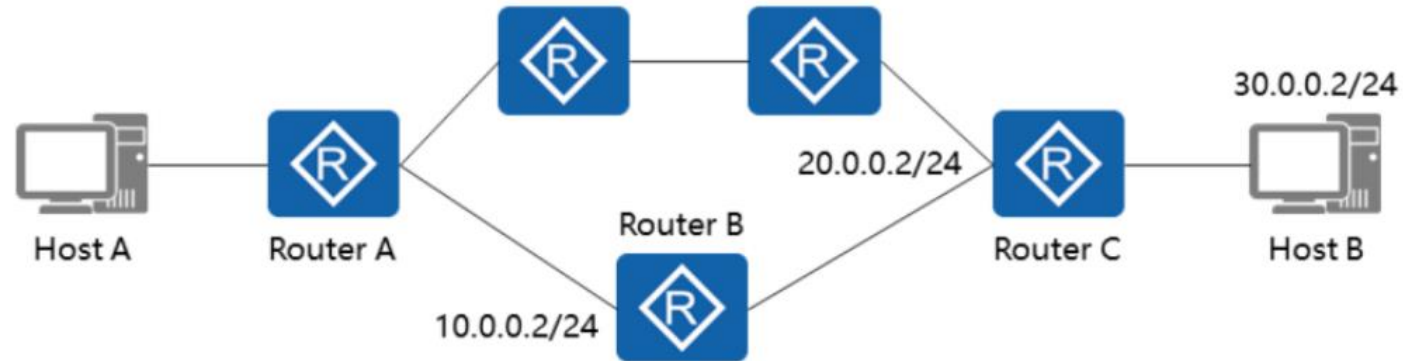
ICMP Application: Ping (2)

```
[Router A]ping 192.168.1.2
PING 192.168.1.2 : 56 data bytes, press CTRL_C to break
  Reply from 192.168.1.2 : bytes=56 Sequence=1 ttl=255 time=340 ms
  Reply from 192.168.1.2 : bytes=56 Sequence=2 ttl=255 time=10 ms
  Reply from 192.168.1.2 : bytes=56 Sequence=3 ttl=255 time=30 ms
  Reply from 192.168.1.2 : bytes=56 Sequence=4 ttl=255 time=30 ms
  Reply from 192.168.1.2 : bytes=56 Sequence=5 ttl=255 time=30 ms

--- 192.168.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 10/88/340 ms
```

- The ping command output contains the destination address, ICMP packet length, packet number, TTL value, and round-trip time. The packet number is a variable parameter field contained in an Echo Reply message (Type=0). The TTL and round-trip time are included in the IP header of the message.

ICMP Application: Tracert (1)



```
<Router A>tracert ?
STRING<1-255> IP address or hostname of a remote system
-a           Set source IP address, the default is the IP address of the
             output interface
-f           First time to live, the default is 1
-m           Max time to live, the default is 30
-name        Display the host name of the router on each hop
-p           Destination UDP port number, the default is 33434
-q           Number of probe packets, the default is 3
-s           Specify the length of the packets to be sent. The default
             length is 12 bytes
...
```



ICMP Application: Tracert (1)

Tracert is another typical application of ICMP. Tracert traces the forwarding path of packets hop by hop based on the TTL value in the packet header. To trace the path to a specific destination address, the source end first sets the TTL value of the packet to 1.

After the packet reaches the first node, the TTL times out. Therefore, this node sends a TTL timeout message carrying the timestamp to the source end. Then, the source end sets the TTL value of the packet to 2. After the packet reaches the second node, the TTL times out.

This node also returns a TTL timeout message. The process repeats until the packet reaches the destination. In this way, the source end can trace each node through which the packet passes according to the information in the returned packet. This allows the source end to calculate the round-trip time according to the timestamp information.

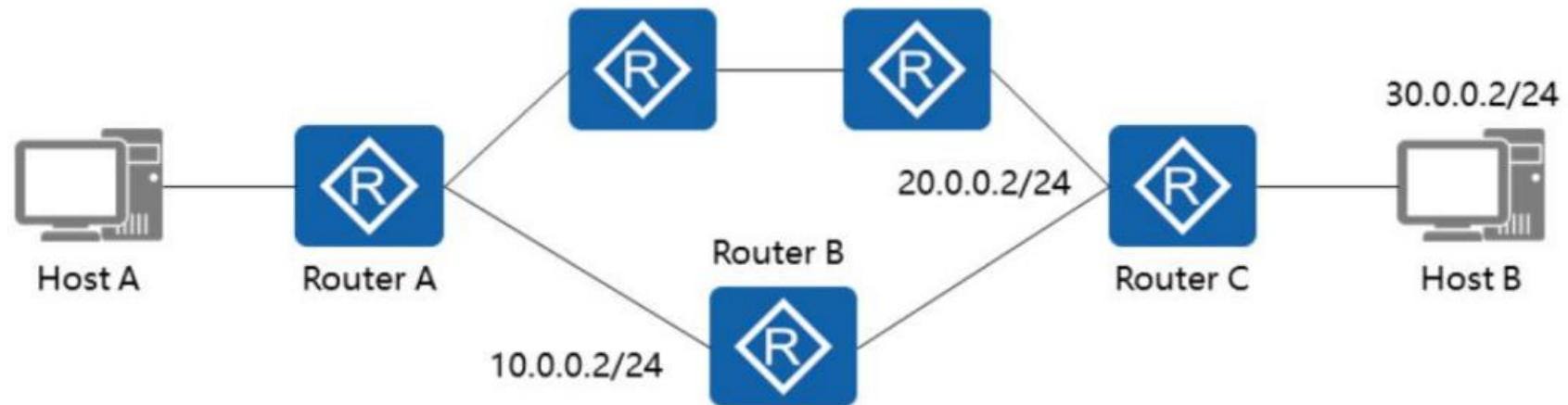
Tracert is an effective method to detect packet loss and delay, and helps administrators discover routing loops on the network

ICMP Application: Tracert (1)

- **Common Tracert parameters:**
 - ❑ **-a source-ip-address:** Specifies the source address of a tracert packet.
 - ❑ **-f first-ttl:** Indicates the initial TTL. The default value is 1.
 - ❑ **-m max-ttl:** Indicates the maximum TTL. The default value is 30.
 - ❑ **-name:** Displays the host name on each hop.
 - ❑ **-p port:** Specifies the UDP port number of the destination host.

ICMP Application: Tracert (2)

- The Tracert command displays each hop that packets pass through during network transmission.



```
<Router A>tracert 30.0.0.2
Tracert to 30.0.0.2(30.0.0.2), max hops:30, packet length:40, press CTRL_C to
break
 1 10.0.0.2 130 ms  50 ms  40 ms
 2 20.0.0.2  80 ms  60 ms  80 ms
 3 30.0.0.2  80 ms  60 ms  70 ms
```

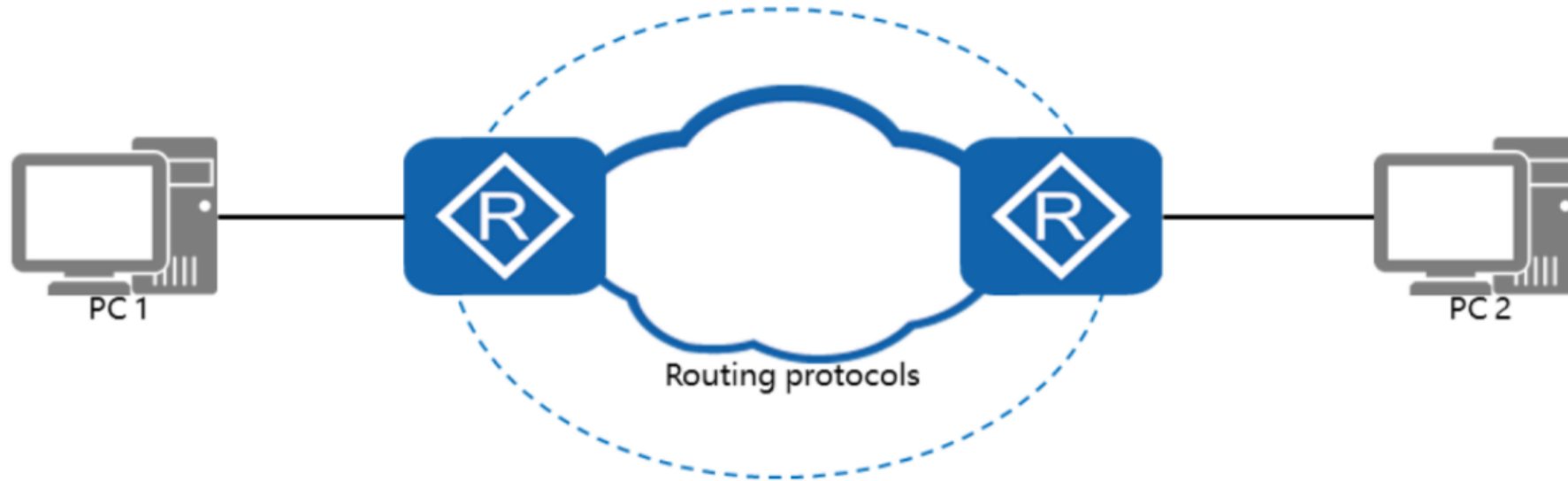
ICMP Application: Tracert (2)

- The source end (Router A) sends a UDP packet whose TTL value is 1 and destination UDP port number is larger than 30000 to the destination end (Host B). A UDP port number larger than 30000 is not commonly used by any program.
- After receiving the UDP packet, the first-hop host (Router B) determines that the destination IP address of the packet is not its own IP address and decreases the TTL value by one. The TTL value is now 0. Therefore, Router B discards the UDP packet, and sends an ICMP Time Exceeded packet containing its IP address 10.1.1.2 to Router A. In this way, Router A obtains the IP address of Router B.
- Upon receiving the ICMP Time Exceeded packet from Router B, Router A sends a UDP packet with a TTL value of 2.
- Upon receiving the UDP packet, the second-hop host (Router C) returns an ICMP Time Exceeded packet containing its IP address 10.1.2.2 to Router A.

- The preceding steps are repeated until the destination end determines that the destination IP address of the UDP packet is its IP address and processes the packet. The destination end searches for the upper-layer protocol that occupies the UDP port number based on the destination UDP port number in the packet. If the destination end does not use the UDP port number, the destination end returns an ICMP Destination Unreachable packet to the source end.
- Upon receiving the ICMP Destination Unreachable packet, the source end determines that the UDP packet has reached the destination end. It then stops running tracert and generates the path of the UDP packet (10.1.1.2; 10.1.2.2; 10.1.3.2).

Routing Protocol Overview

- Routing is the most basic element in a data communications network. It is the process of selecting paths on a network through which packets are sent from a source to a destination.



- Routes are classified into the following types based on the destination address:
 - Network segment routes: The destination is a network segment. The subnet mask of an IPv4 destination address is less than 32 bits or the prefix length of an IPv6 destination address is less than 128 bits.
 - Host routes: The destination is a host. The subnet mask of an IPv4 destination address is 32 bits or the prefix length of an IPv6 destination address is 128 bits.

Routing Protocol Overview

- **Routes are classified into the following types based on whether the destination is directly connected to a router:**
 - ❑ **Direct routes:** A router is directly connected to the network where the destination is located.
 - ❑ **Indirect routes:** A router is indirectly connected to the network where the destination is located.
- **Routes are classified into the following types based on the destination address type:**
 - ❑ **Unicast routes:** The destination address is a unicast address.
 - ❑ **Multicast routes:** The destination address is a multicast address.

- **Differences between static routes and dynamic routes**
 - ❑ **Static routes are easy to configure, have low requirements on the system, and apply to small, simple, and stable networks. However, static routes cannot automatically adapt to network topology changes and manual intervention is required.**
 - ❑ **Dynamic routing protocols have their own routing algorithms. Dynamic routes can automatically adapt to network topology changes and apply to networks with a large number of Layer 3 devices. The configurations of dynamic routes are complex. Dynamic routes have higher requirements on the system than static routes do and consume both network and system resources.**

Routing Protocol Overview

- **Classifications of dynamic routing protocols**

- **According to the application range, dynamic routing protocols are classified into the following types:**

- **Interior Gateway Protocols (IGP):** running in an AS. Common IGPs include the RIP, OSPF, and IS-IS.

- **Exterior Gateway Protocols (EGP):** running in different ASs. BGP is the most frequently used EGP protocol.

- **According to the used algorithms, dynamic routing protocols are classified into the following types:**

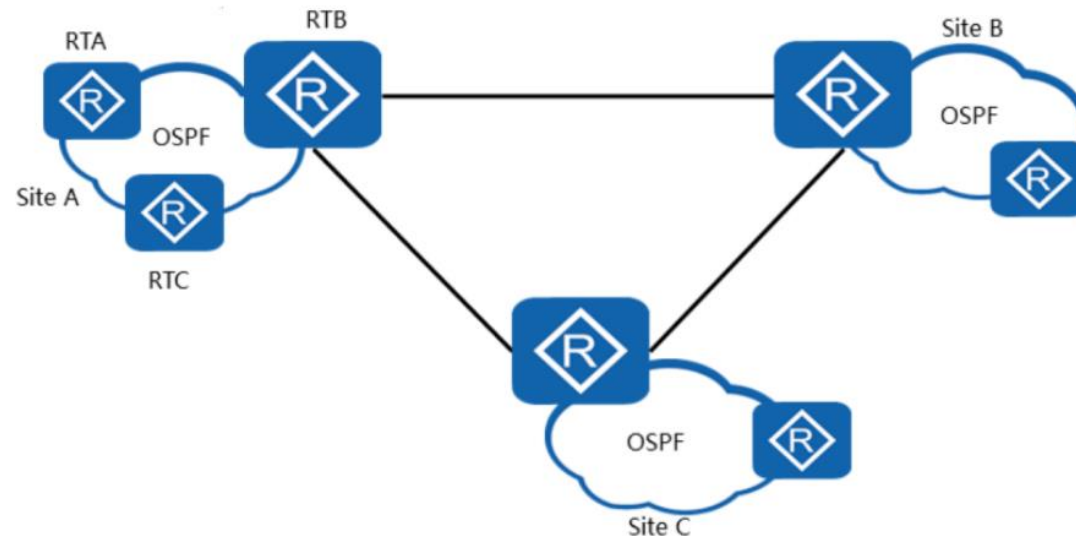
- **Distance-vector protocol:** includes RIP and BGP. BGP is also called a path vector protocol.

- **Link-state protocol:** includes OSPF and IS-IS.

Introduction to OSPF

- OSPF is a routing protocol based on link status and ensures that the network topology is loop-free. OSPF supports area division. Routers in an area use the shortest path first (SPF) algorithm to ensure that no loop exists in the area. OSPF also uses inter-area connection rules to ensure that no routing loop exists between areas.
- OSPF can trigger an update to rapidly detect and advertise topology changes within an AS.
- OSPF can solve common issues caused by network expansion. For example, if additional routers are deployed and the volume of routing information exchanged between them increases, OSPF can divide each AS into multiple areas and limit the range of each area. OSPF is suitable for large and medium-sized networks. In addition, OSPF supports authentication: packets between OSPF routers can be exchanged only after being authenticated.

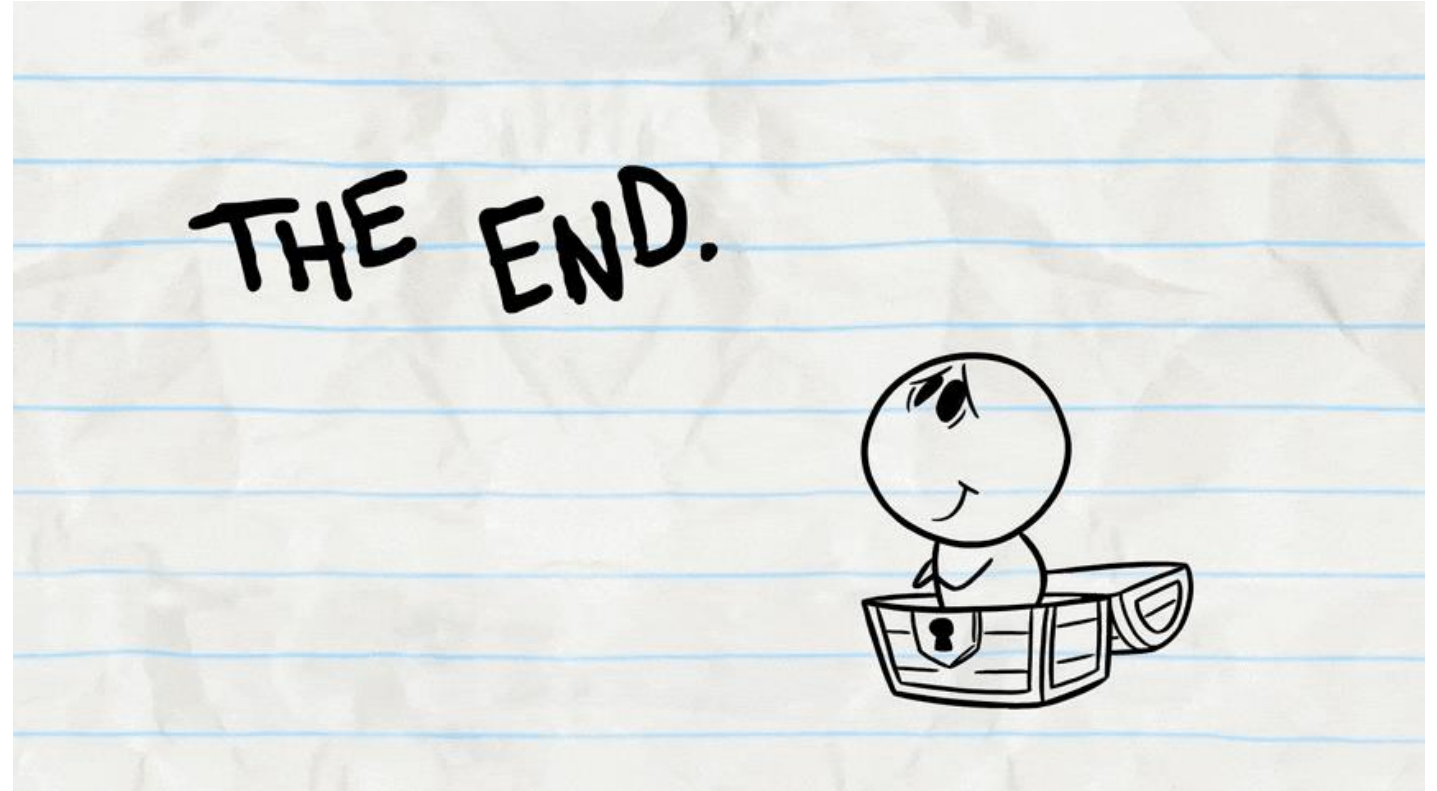
- No loop
- Fast convergence
- Good scalability
- support authentication



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