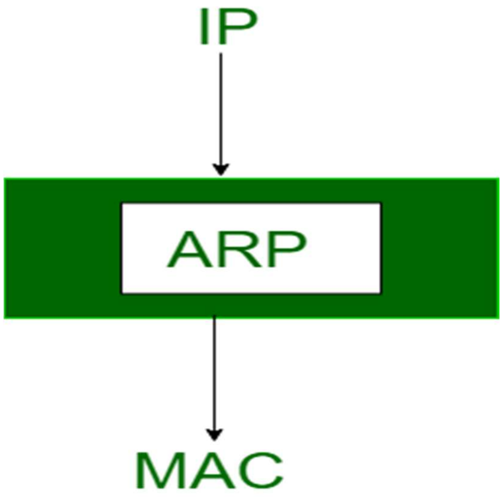
ADDRESS RESOLUTION PROTOCOL (ARP)

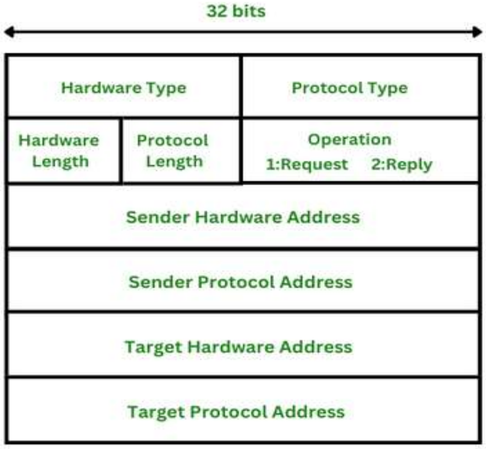
Prepared by	Nagendra Babu Kothapalli
Reviewed by	Kumar, Aamod

ARP is a communication protocol used to find the MAC (Physical) address of a device from its IP address. This protocol is used when a device wants to communicate with another device on a LAN or Ethernet. When the device wants to communicate across the network then Router will initiate a new ARP request for that network.



ARP Header

An ARP packet’s format, also known as an ARP packet header, has numerous fields required to describe the type of ARP message, the addresses being resolved, and other communication-related information.



Hardware type: This is 16 bits field defining the type of the network on which ARP is running. Ethernet is given type 1.

Here values of the Hardware type

Hardware type	Value
Ethernet	1
IEEE 802.11 Networks	6
ARCNET	7
Frame Relay	15
Fibre Channel	18

Remaining are reserved.

Protocol type: This is 16 bits field defining the protocol. The value of this field for the IPv4 protocol is 0*800H.

In Internet Protocol Version 6 (IPv6) networks, the functionality of ARP is provided by the Neighbour Discovery Protocol (NDP).

Hardware length: This is an 8 bits field defining the length of the physical address in bytes. Ethernet is the value 6.

Protocol length: This is an 8 bits field defining the length of the logical address in bytes. For the IPv4 protocol, the value is 4.

Operation (**request or reply):** This is a 16 bits field defining the type of packet. Packet types are ARP request (1), and ARP reply (2).

ARP Message Type	**OPCODE**
ARP Request	1
ARP Reply	2
RARP Request	3
RARP Reply	4
DRARP Request	5
DRARP Reply	6
DRARP Error	7
InARP Request	8
InARP Reply	9

DRARP is used to acquire (or allocate) a protocol level address given the fixed hardware address for a host.

Sender hardware address: This field defining the physical address of the sender. For example, for Ethernet, this field is 6 bytes long.

Sender protocol address: This field defining the logical address of the sender For the IP protocol, this field is 4 bytes long.

Target hardware address: This field defining the physical address of the target. For Ethernet, this field is 6 bytes long. For the ARP request messages, this field is all O's because the sender does not know the physical address of the target. **Target hardware address: 00:00:00: 00:00:00**

Target protocol address: This field defining the logical address of the target. For the IPv4 protocol, this field is 4 bytes long.

Ethernet Frame:

Source MAC	Destination MAC	Type	Data	FCS
Sender MAC	Broadcast	O*0806	ARP Packet	Checksum value

Important Points:

1. ARP Request is Broadcast while ARP Reply is Unicast.
2. ARP operates with in the Subnets.
3. The target IP address is necessary in the request packet.
4. The sender MAC address and sender IP address are mandatory fields because they are going to be updates on ARP Table.

ARP Table:

ARP table is used to keep the record of the IP address and MAC of the devices. For communication between two devices, it is necessary that IP and MAC of the source and destination addresses of device should be stored on an ARP table. If there is no record in the ARP table, an ARP broadcast is sent by the source to all the devices in the network.

When IP address of the device matches with each other, that device sent the response which is updated in ARP table.

Each host that connected to the network should have to maintain an ARP table on its own.

Operations in an ARP Table:

We can perform many operations in an ARP table such as to display, add and remove ARP entries in the ARP table (ARP cache).

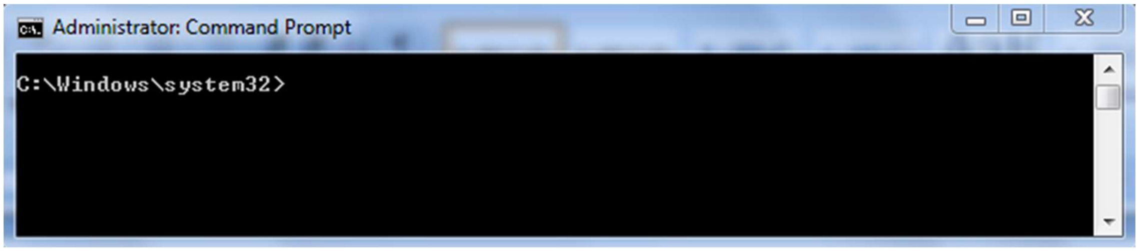
To perform these operations, we use an **arp** command offered by the Windows Operating System.

List and Display ARP entries:

You can display the ARP entries by using the command **arp -a**. This list of entries is displayed in the terminal according to the interfaces.

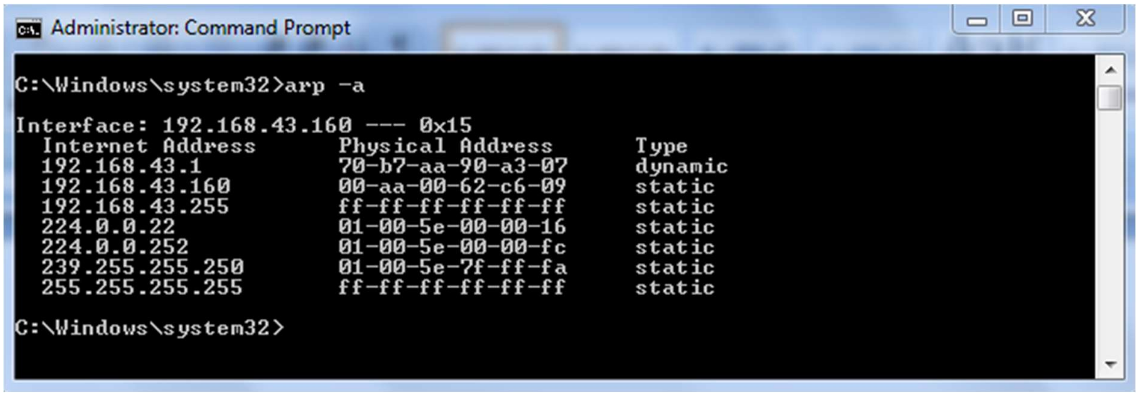
Steps for displaying the ARP entries

Step 1: Go to the start menu. Open the command **prompt.**



```
C:\Windows\system32>
```

Step 2: Type **arp -a** command in the command prompt or terminal and press **enter button**. After pressing the **enter button**, all the ARP entries will display in the command prompt.



```
C:\Windows\system32>arp -a

Interface: 192.168.43.160 --- 0x15
  Internet Address      Physical Address      Type
  192.168.43.1          70-b7-aa-90-a3-07     dynamic
  192.168.43.160        00-aa-00-62-c6-09     static
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Windows\system32>
```

Add static ARP entry:

The ARP table also provides a feature that is adding a static ARP entry to the AP table. With the help of this, we can add the **IP address** and **MAC address** to the **ARP table** (ARP cache). These entries will be stored until the computer restarts. The type of these entries will remain static when they are listed in the table.

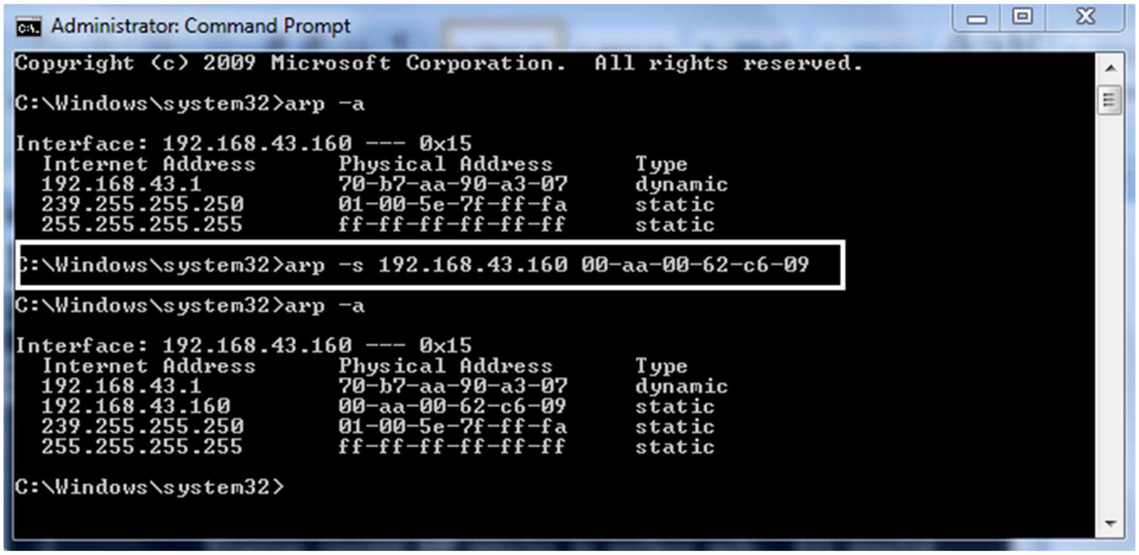
Steps to add a static ARP entry:

To add a static entry, type **arp -s command** along with the **IP address** and **MAC address** in a command prompt and then press **enter**.

1. Syntax: arp -s 192.168.43.160 00-aa-00-62-c6-09

Where, IP address = 192.168.43.160

MAC address = 00-aa-00-62-c6-09



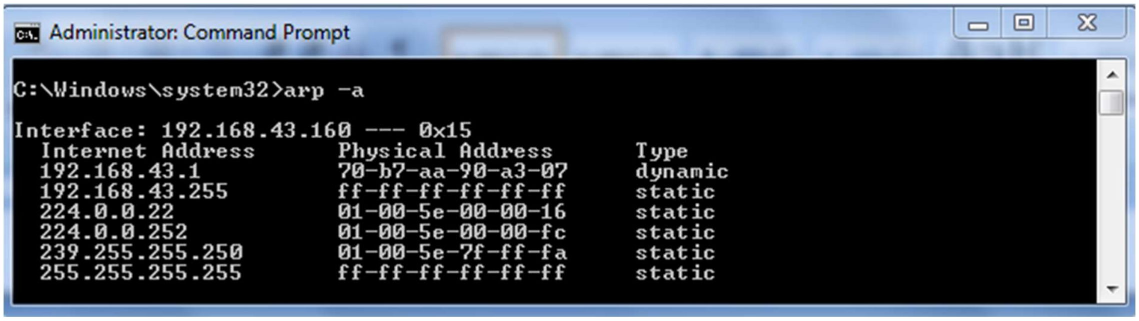
```
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>arp -a

Interface: 192.168.43.160 --- 0x15
  Internet Address      Physical Address      Type
  192.168.43.1          70-b7-aa-90-a3-07     dynamic
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Windows\system32>arp -s 192.168.43.160 00-aa-00-62-c6-09

C:\Windows\system32>arp -a

Interface: 192.168.43.160 --- 0x15
  Internet Address      Physical Address      Type
  192.168.43.1          70-b7-aa-90-a3-07     dynamic
  192.168.43.160        00-aa-00-62-c6-09     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Windows\system32>
```

Remove ARP entry:

We can also remove the arp entries irrespective of the entry type, such as **static** and **dynamic**.

Steps for removing an ARP entry

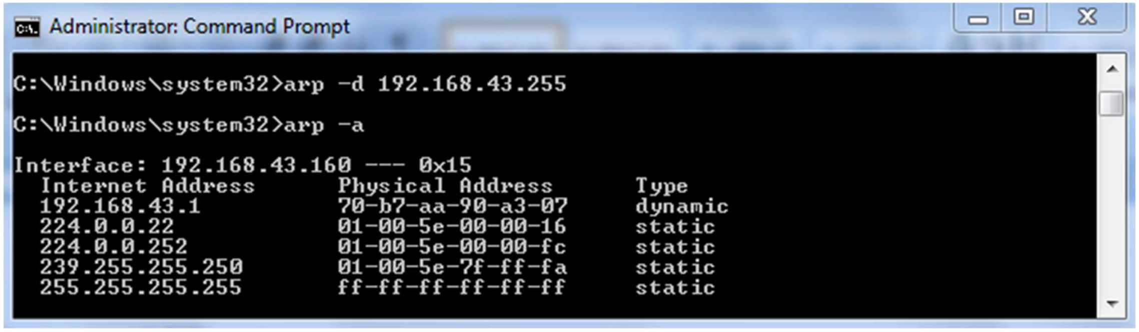
Step 1: To remove an ARP entry type, the command **arp -a**. This command will display all the ARP entries with their IP address, MAC address, and the entry type.



```
C:\Windows\system32>arp -a

Interface: 192.168.43.160 --- 0x15
  Internet Address      Physical Address      Type
  192.168.43.1          70-b7-aa-90-a3-07     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Step 2: Now, type the **arp -d** command along with the IP address, which we want to delete and then press enter. It is necessary that the **IP address** must be from the listed entries.

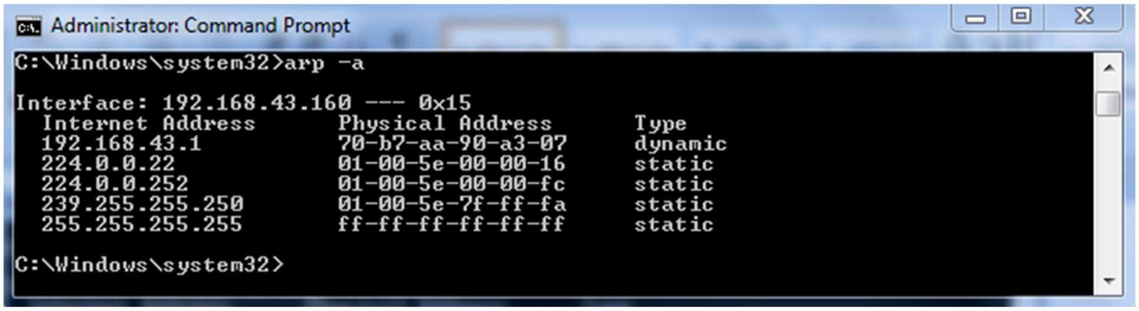
Syntax: arp -d 192.168.43.255



```
C:\Windows\system32>arp -d 192.168.43.255

C:\Windows\system32>arp -a

Interface: 192.168.43.160 --- 0x15
  Internet Address      Physical Address      Type
  192.168.43.1          70-b7-aa-90-a3-07     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

In the above example, we have deleted the entry having IP address 192.168.43.255.

Step 3: To check whether the entry is deleted or not again type **arp -a** command and press enter key. After pressing enter key, all the entries will be displayed in the command prompt except the deleted one.



```
C:\Windows\system32>arp -a

Interface: 192.168.43.160 --- 0x15
  Internet Address      Physical Address      Type
  192.168.43.1          70-b7-aa-90-a3-07     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Windows\system32>
```

Working of ARP (Address Resolution Protocol)

Mostly, the computer programs use IP address (Logical address) to send or receive messages, hence the actual communication takes place over physical address (MAC address). So, our aim is to find out the MAC address of the destination that allows us to communicate with other devices. In this case, the ARP is required as it converts the IP address to a physical address.

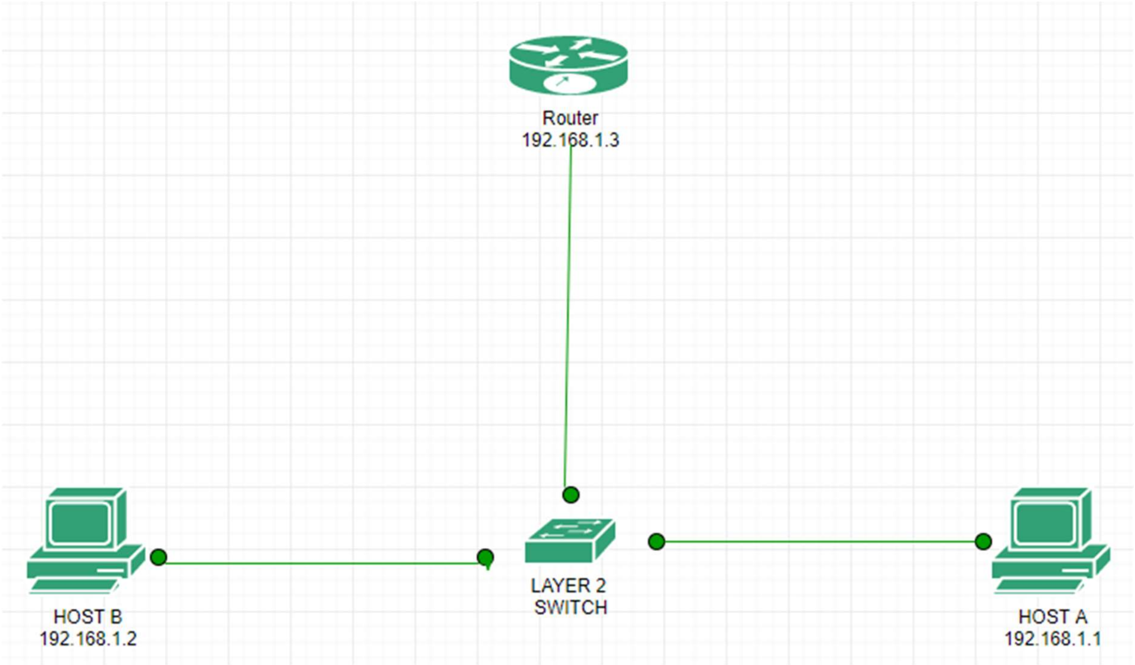
Working of ARP

- At the network layer, when the source wants to communicate with the destination. Firstly, the source needs to find out the MAC address (Physical Address) of the destination. For this, the source will check the ARP cache and ARP table for the MAC address of the destination. If the MAC address of the destination is present in the ARP cache or ARP table, then the source uses that MAC address for the communication.

- If the MAC address of the destination is not in the ARP cache or ARP table, then the Source generates an ARP Request message. The ARP Request message consists of the MAC address and the IP address of the source. It also contains the IP address and MAC address of the destination. The MAC address of the destination left null because the user has requested this.
- The ARP Request message will be broadcasted to the local network by the source computer. All the devices in the LAN network receive the broadcast message. Now, each device compares its own IP address with the IP address of the destination. If the IP address of the device match with the IP address of the destination, then that device will send an ARP to reply message. If the IP address of the device does not match the IP address of the destination, then the device will automatically drop the packet.
- The destination sends an ARP reply packet when the destination address matches the device. That ARP Reply packet consists of the MAC address of the device. The destination device automatically updates the table and stores the source's MAC address because this address will be required for the communication from the source.
- Now the source acts as a target for the destination device, and the destination device sends the ARP Reply message.
- The ARP Reply message is unicast instead of broadcast. This is because the device (destination) that is sending the ARP Reply message knows the MAC address of the device (source) to which the ARP Reply message is sent.
- When the source device receives the ARP Reply message, then it will know the MAC address of the destination because the ARP Reply packet contains the MAC address of the destination along with the other addresses. The source will update the MAC address of the destination in the ARP cache. Now the sender can communicate directly to the destination.

Now, we have taken an idea about the ARP protocol. Let’s see about the **packet flow**.

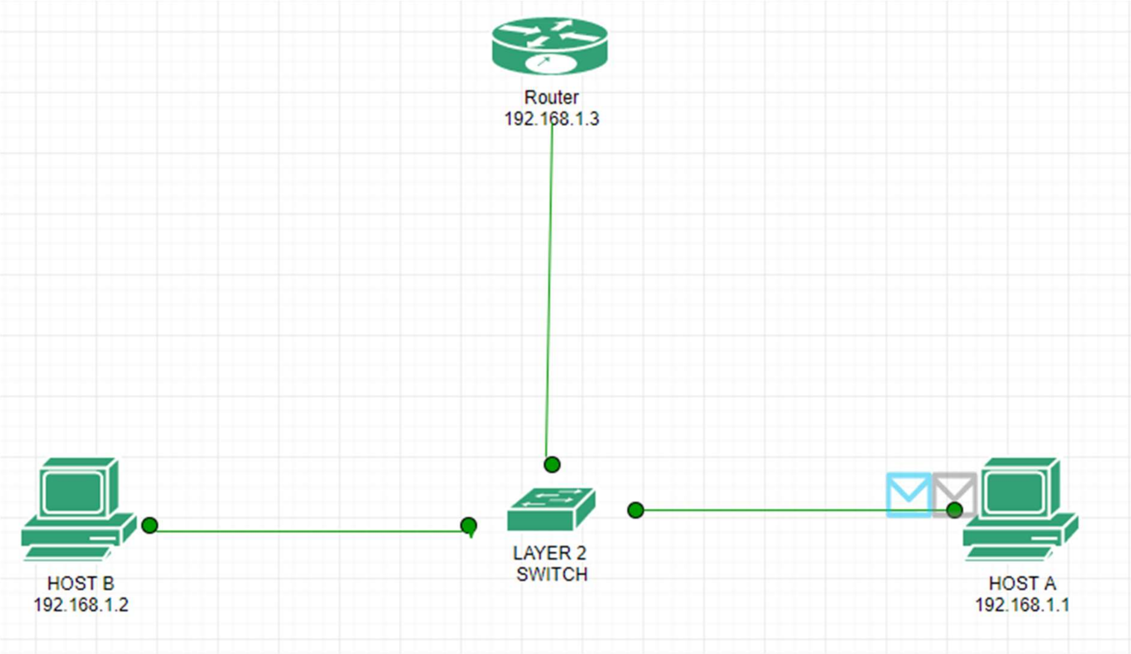
Now we will understand how the packet is delivered to the destination when the destination is present in the same network (network of the source).



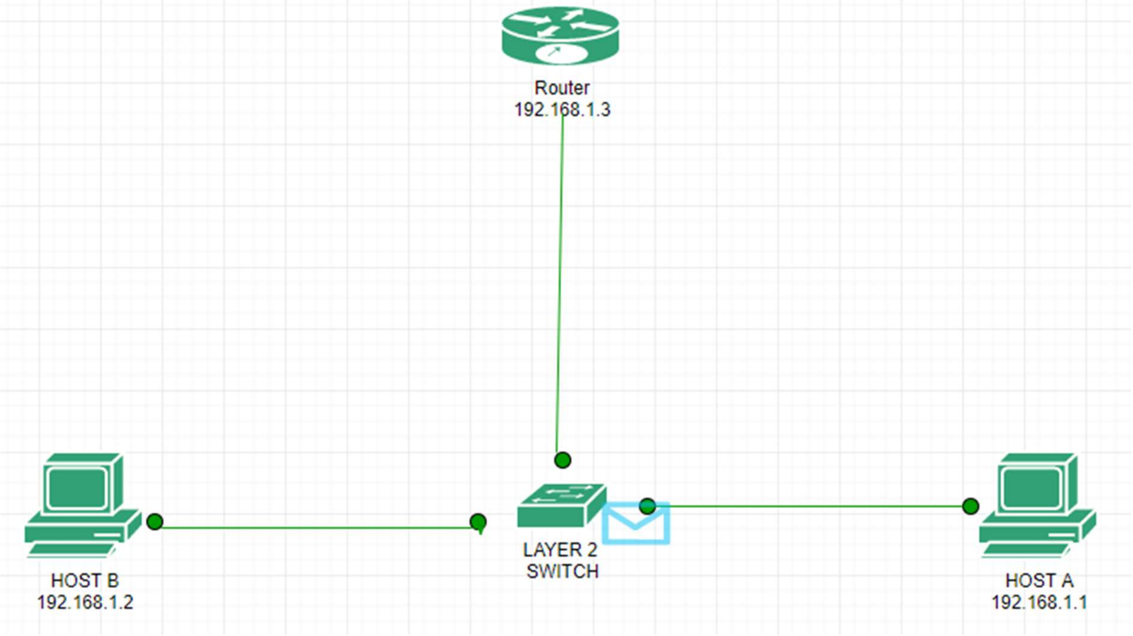
Here is the topology in which host A has IP address 192.168.1.1, host B has IP address 192.168.1.2, and the router has IP address 192.168.1.3 on interface fa0/0.

Now how to source device will know that the destination is present in the same or different network. Let us understand: -

AND Operation is performed between the source IP address, source subnet mask and destination IP address, source subnet mask. If the resultant of both is the same, then the destination is present in the same network otherwise in a different network.
Let us try to ping host B from host A.

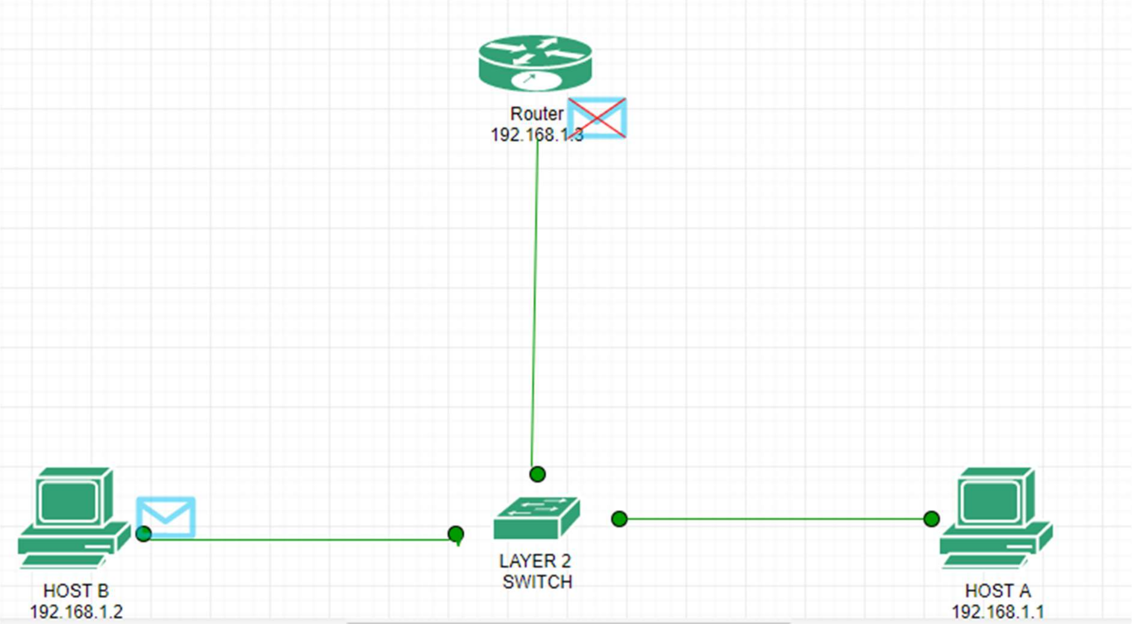


As you can see 2 packets are generated, one of ICMP and the other of ARP (green). ARP frame is generated because host A has not yet communicated to host B i.e., the ARP has not been resolved i.e., ARP will be resolved first so that host A has an entry for host B MAC address.

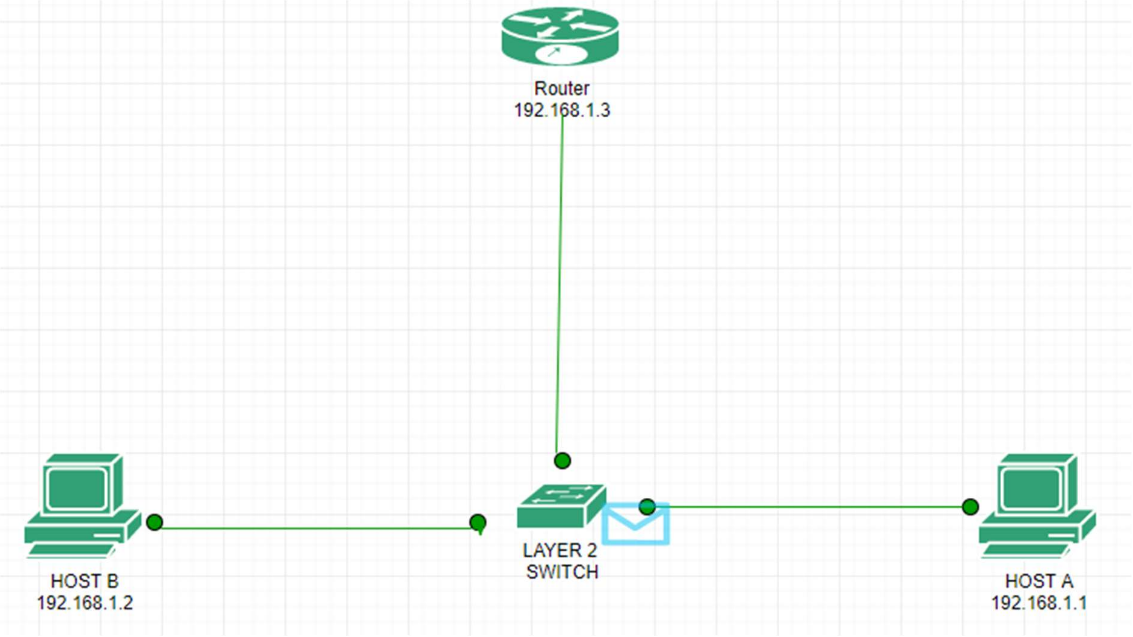


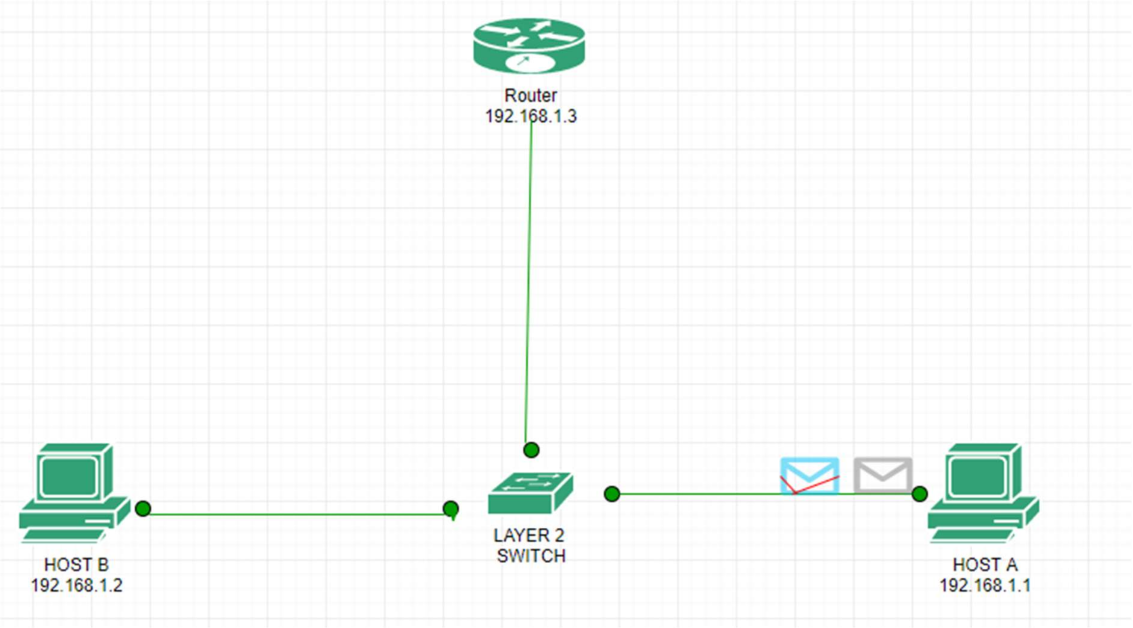
As already explained the ARP request will be broadcast first for the target IP address within the network because routers do not forward broadcast packets. The broadcast request is received by the switch as shown in the above figure.

The switch broadcasts the ARP request as the entry in the ethernet header is FFFF.FFFF. FFFF (broadcast MAC address).



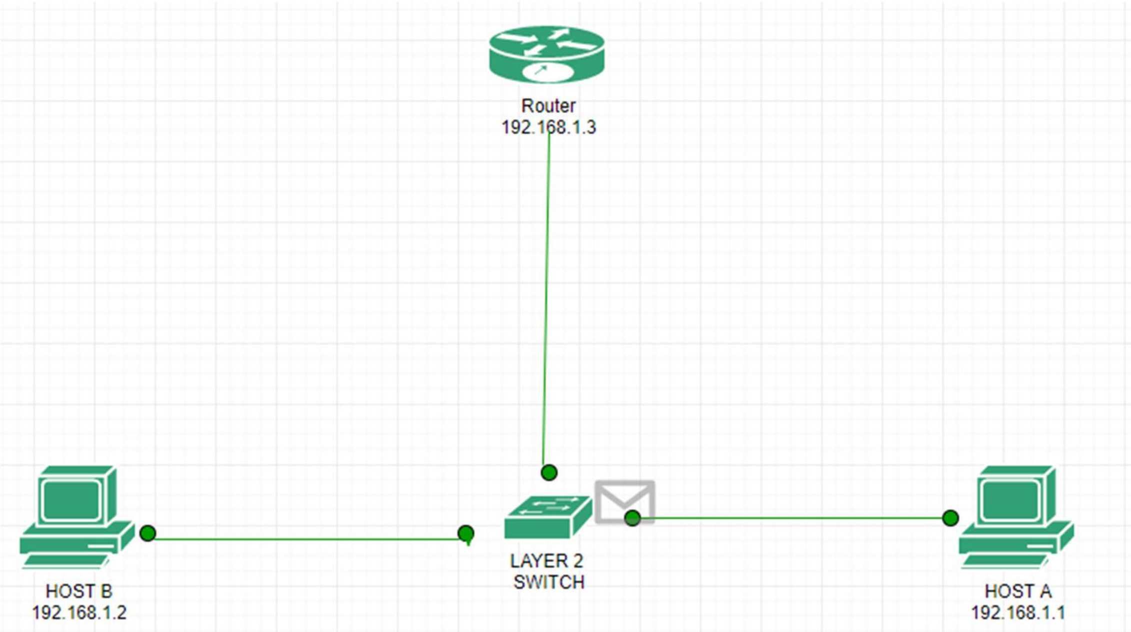
The request is received by Host B as shown in the above figure. Host B generates an ARP reply immediately specifying its own MAC address.

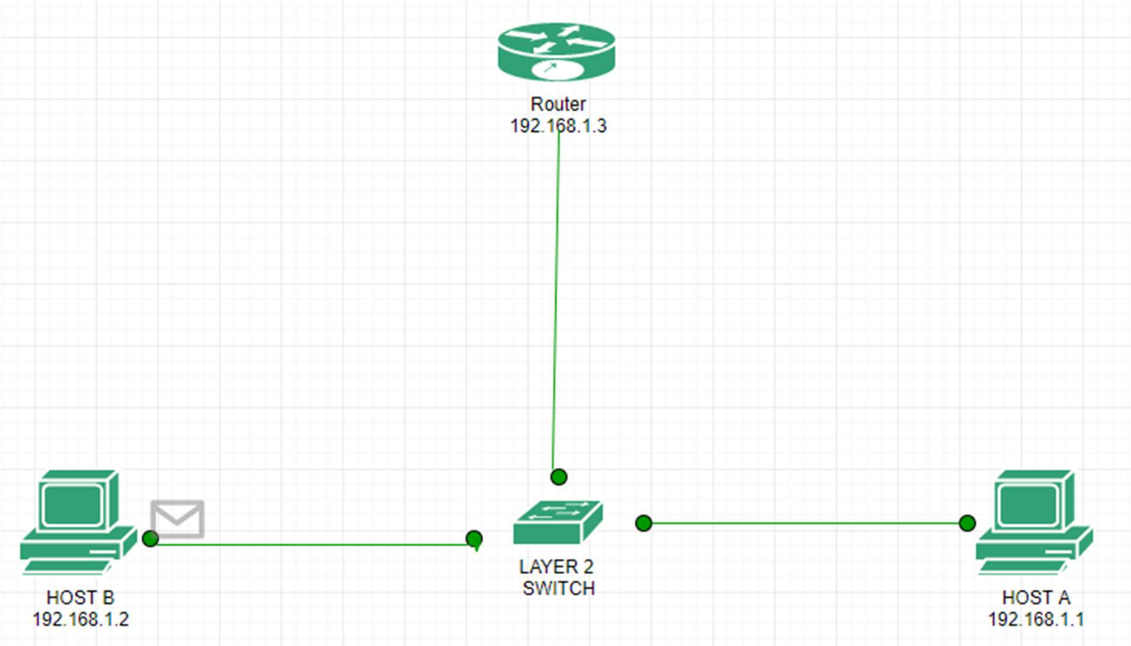




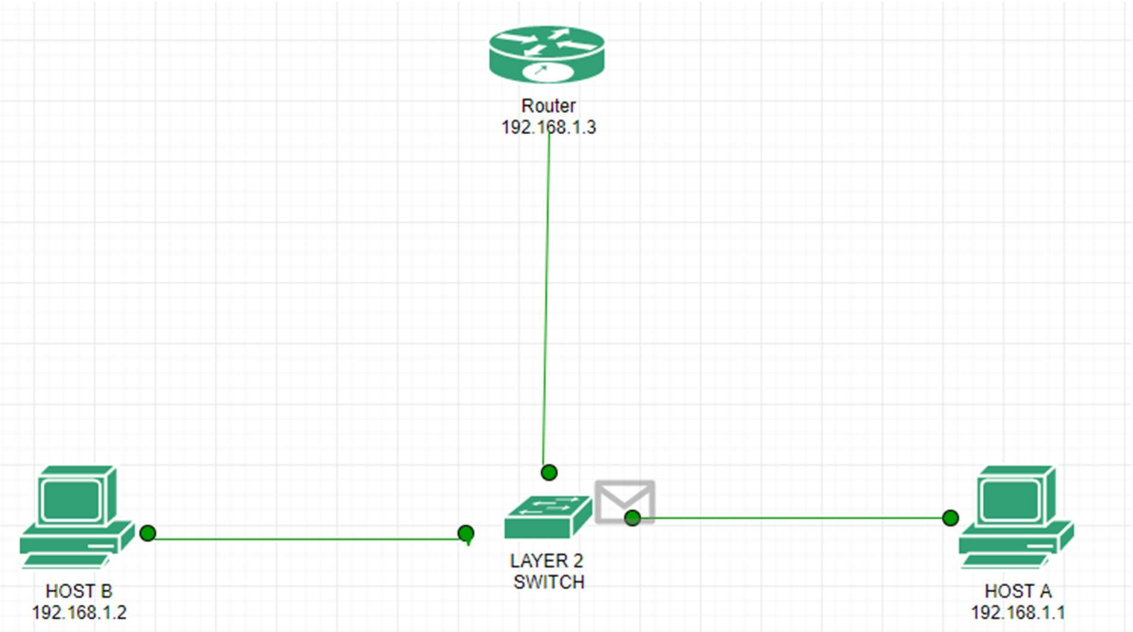
Now the host B unicast the ARP reply to host A which is received by the switch which in turn forward it to host A as shown in the above 2 figures.

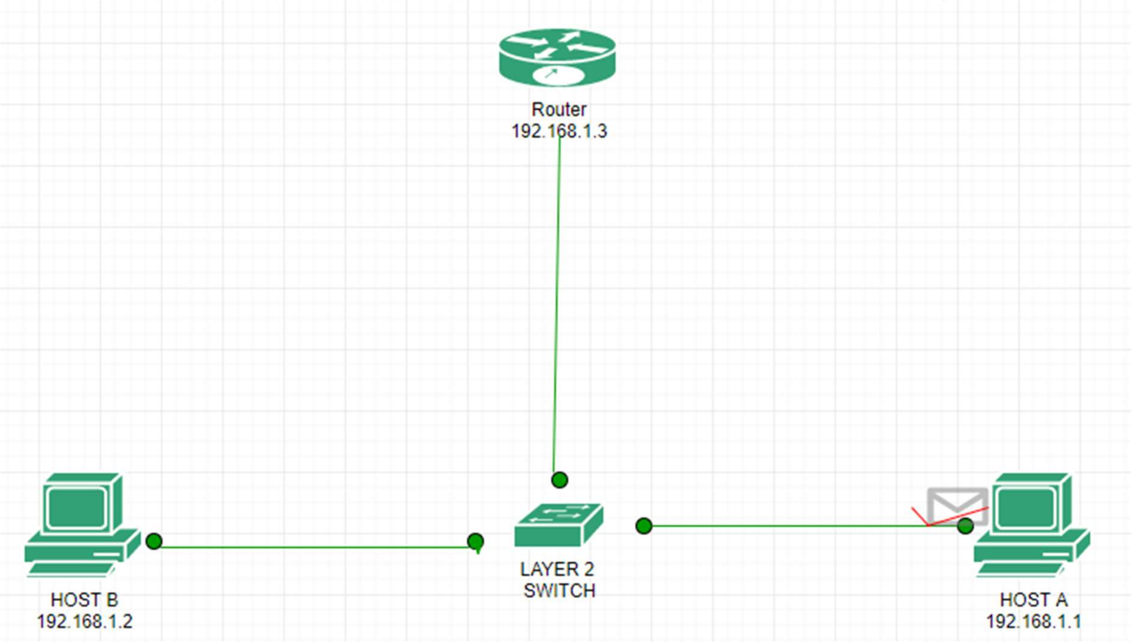
The switch can unicast the reply because the switch has put an entry for host A in its MAC table when hosting A broadcasts the ARP request.in the same way, a switch has also put an entry for the host B when the switch receives the ARP reply.





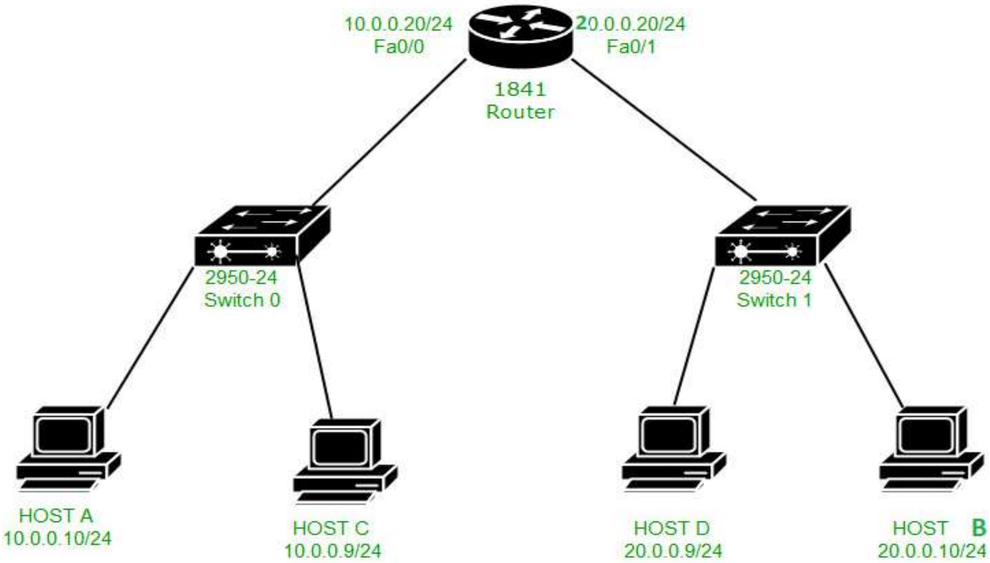
Now the ARP has been resolved and the ICMP will be unicast to the host B from host A (as shown above).





Now the ICMP acknowledgement packet will be unicast from host B to host A i.e., host B is successfully pinged from host A as shown in the above figures.

Now we will understand how the packet is delivered to the destination when the destination is present in the different network.



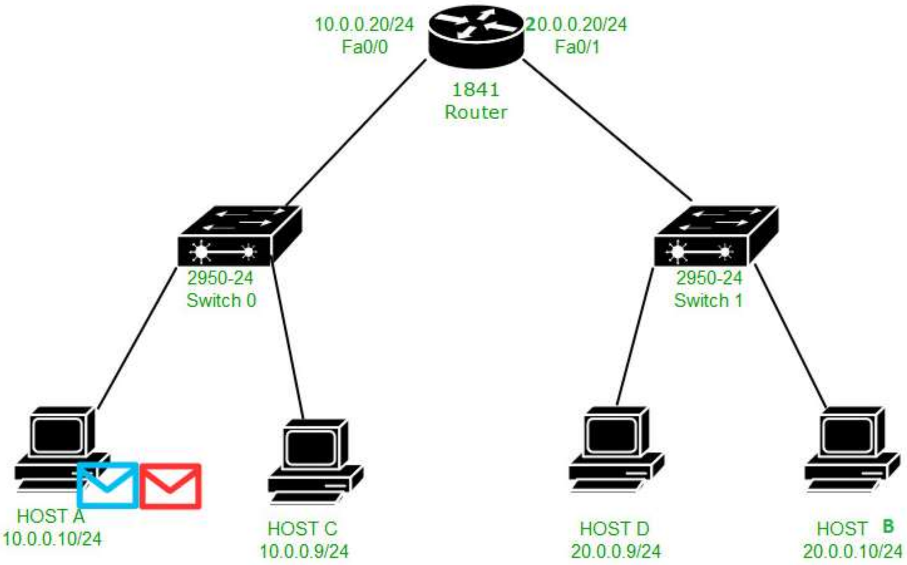
Here is a topology, in which there is host A (IP address – 10.0.0.10 and MAC address – 000D.BD22.7C22), host C (IP address – 10.0.0.9), host D (IP address – 20.0.0.9), host B (IP address-20.0.0.10 and MAC address – 00E0.A3E2.03DC) and the router (IP address – 10.0.0.20 and MAC address – 000B.BE8E.5201 on fa0/0,IP address – 20.0.0.20 and MAC address – 000B.BE8E.5202 on fa0/1).

Now we will try to ping from host A (IP address – 10.0.0.10) to host B (IP address – 20.0.0.10).

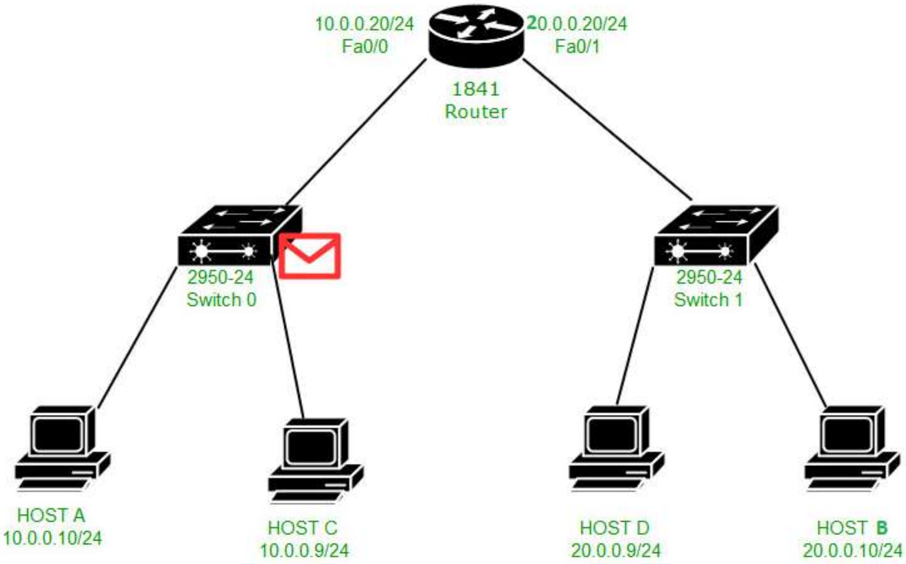
First, **AND operation** is performed by source host between source IP address, source subnet mask, and destination IP address, source subnet mask to know if the destination is present in same or different network.

If the result is the same, then the destination is in the same network otherwise in a different network.

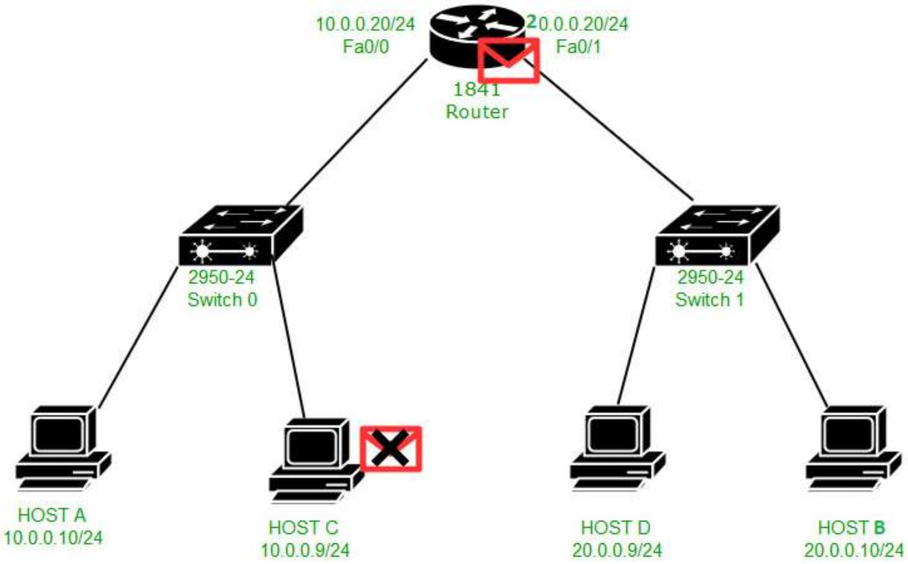
Here, the destination is present in different networks, therefore, the result will be different, and the packet will be delivered to a default gateway.



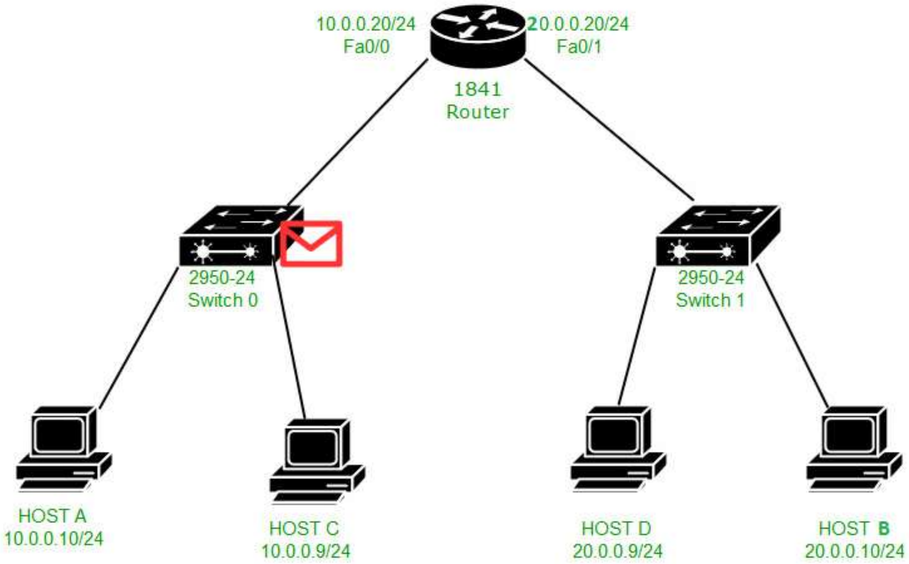
We see that 2 messages are generated ICMP (Blue) and ARP(Red). ARP has been generated because ARP has not been resolved.

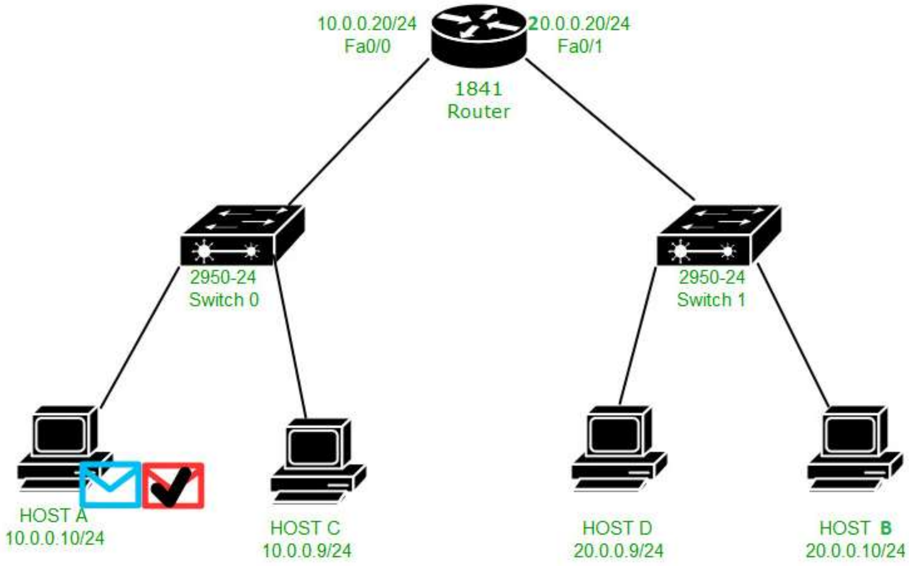


Now as the ARP should be resolved first, therefore the ARP request will be broadcast which is received by switch

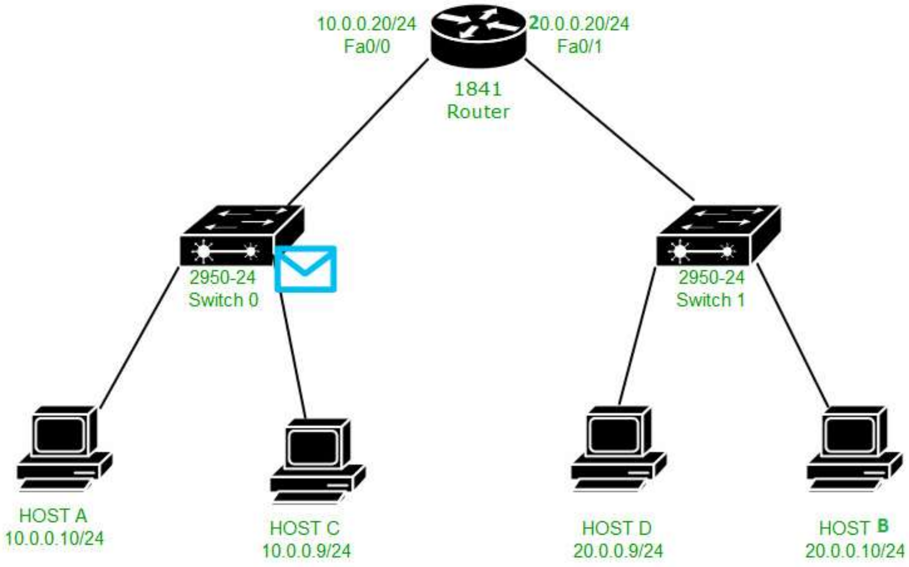


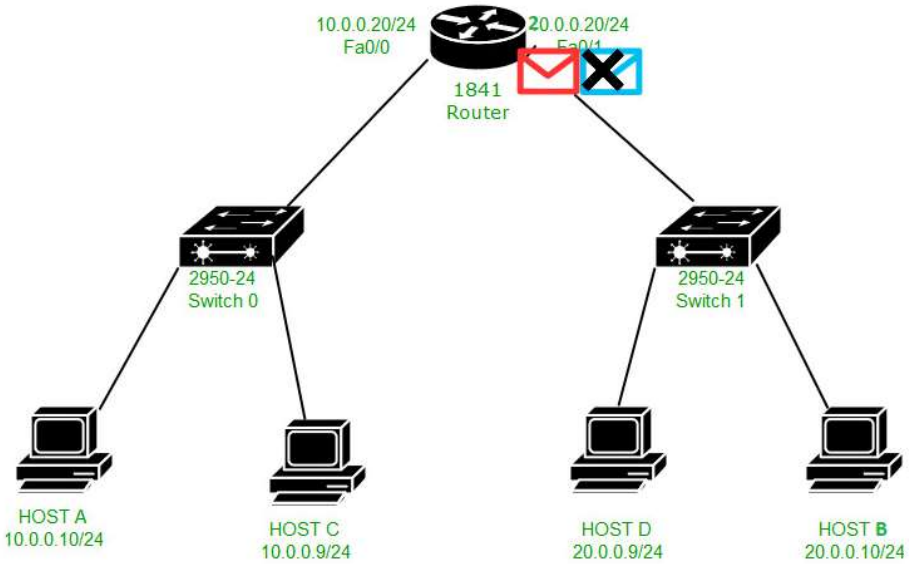
The switch in turn broadcast the ARP request to the host and the router. The PC discards the request, and the router accepts it.





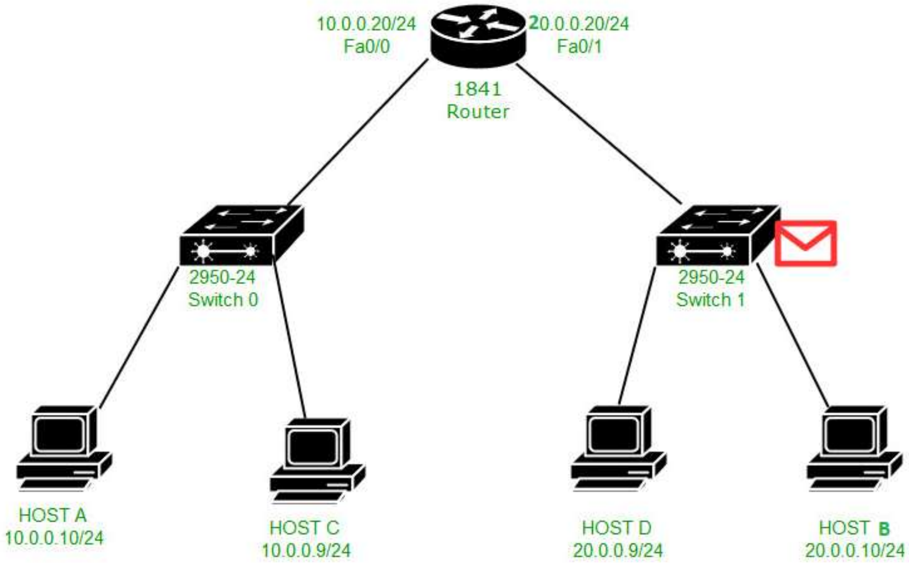
Now the ARP reply is unicast to host A by the router as shown in the above figure.

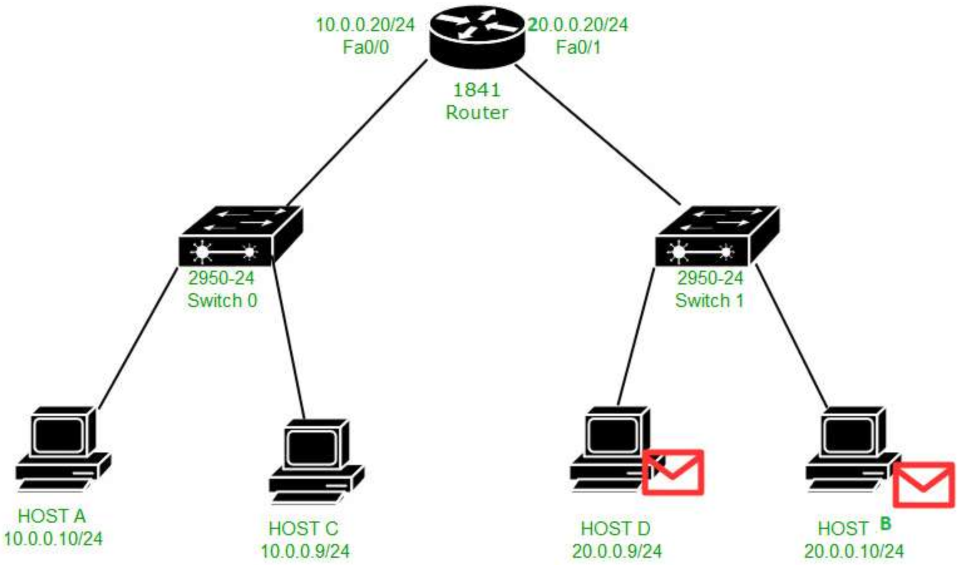




Now the ICMP packet will be unicast to the default gateway (IP address – 10.0.0.20 and MAC address – 000B.BE8E.5201) as shown in the above figures.

Note – The ICMP packet will be unicast to the default gateway as the ARP has been resolved now.



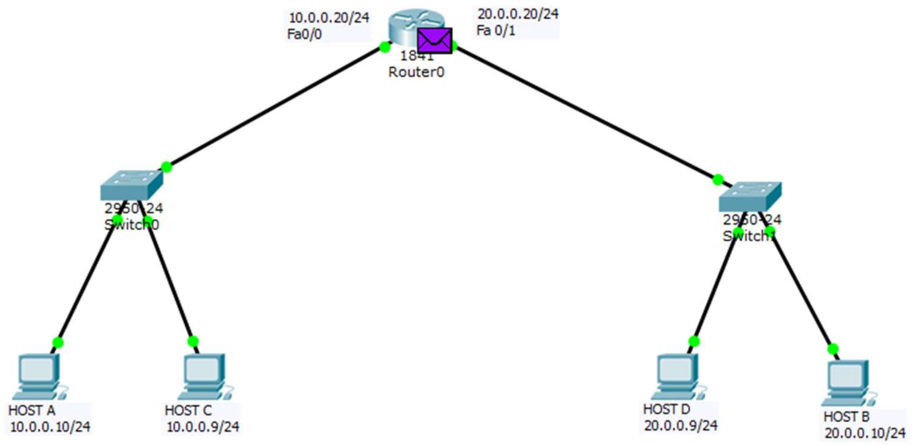


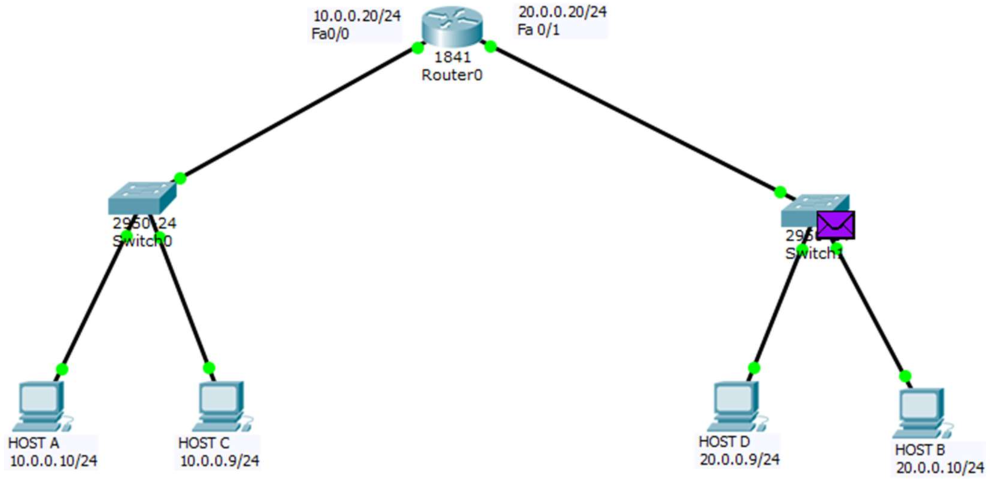
Now the ARP must be resolved again because the router must deliver the packet to host B and the ARP table has no entry for host B. Therefore, the ARP request is broadcast in the network 20.0.0.0/24. The packet is received by the Switch which in turn broadcast the request to host B and D.

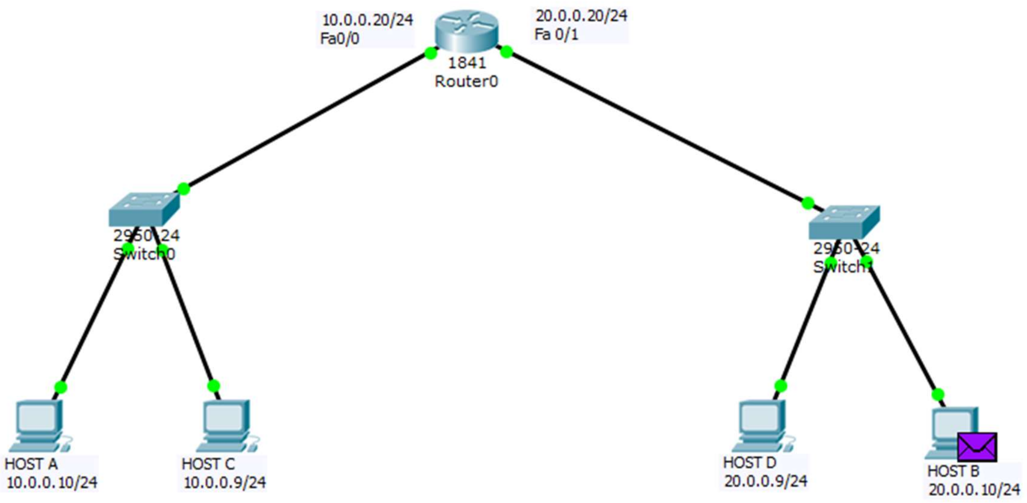
Host D will reject the request and host B will accept it and generate an ARP reply for the MAC address 000B.BE8E.5202 (router fa0/1 MAC address) because the ARP reply must be given to that MAC address from which the ARP request has been received.

Now the ARP reply packet is unicast to the router's interface fa0/1 MAC address (000B.BE8E.5202) and the source MAC is 00E0.A3E2.03DC.

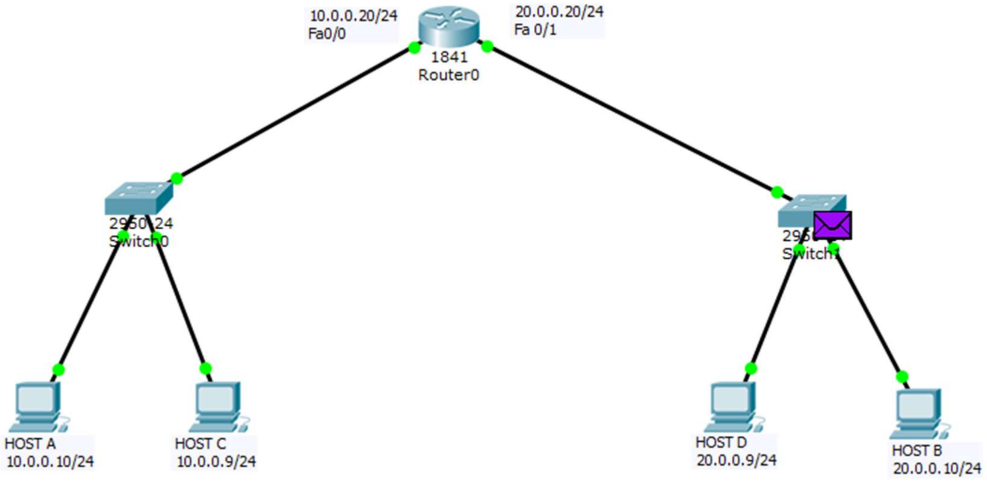
Note – Here, the target MAC address is the MAC address of host B (000B.BE8E.5202). Target MAC address is the MAC address of a device that the host wants to know through its ARP request to resolve ARP.

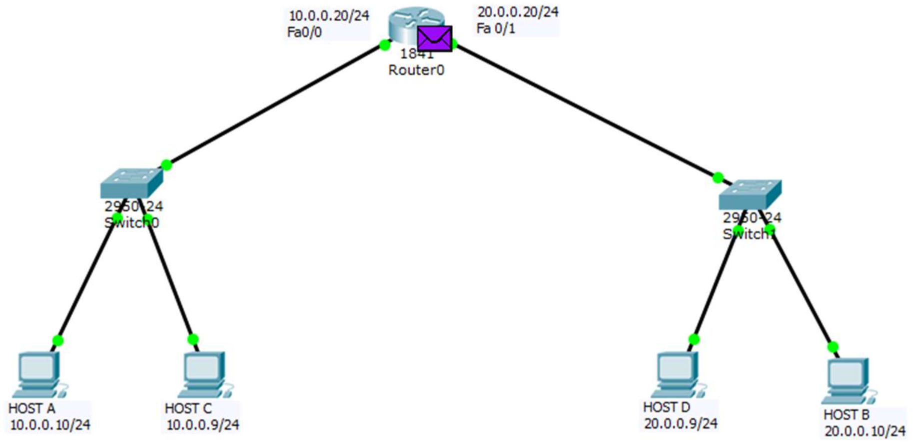

10.0.0.20/24
Fa0/0
20.0.0.20/24
Fa 0/1
1841
Router0
2950-24
Switch0
2950-24
Switch1
HOST A
10.0.0.10/24
HOST C
10.0.0.9/24
HOST D
20.0.0.9/24
HOST B
20.0.0.10/24

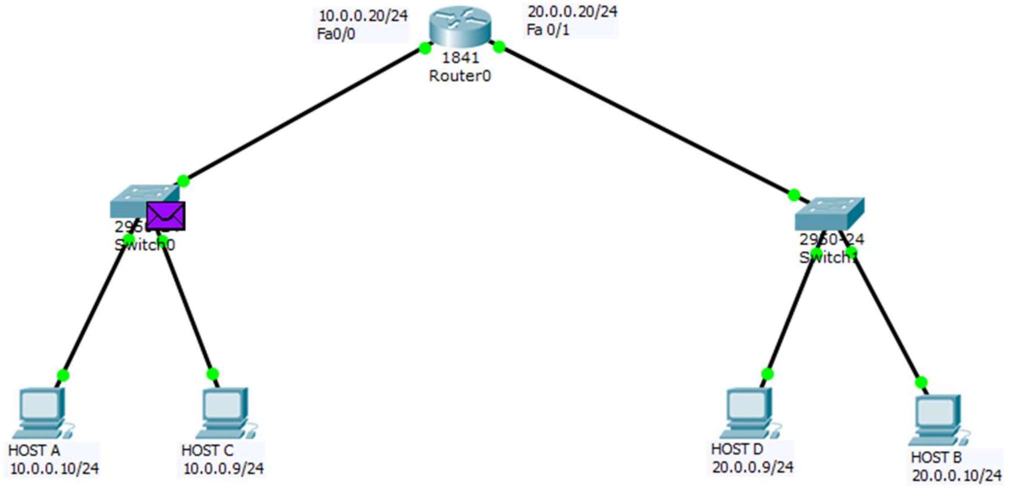

10.0.0.20/24
Fa0/0
20.0.0.20/24
Fa 0/1
1841
Router0
2950-24
Switch0
29
Switch1
HOST A
10.0.0.10/24
HOST C
10.0.0.9/24
HOST D
20.0.0.9/24
HOST B
20.0.0.10/24

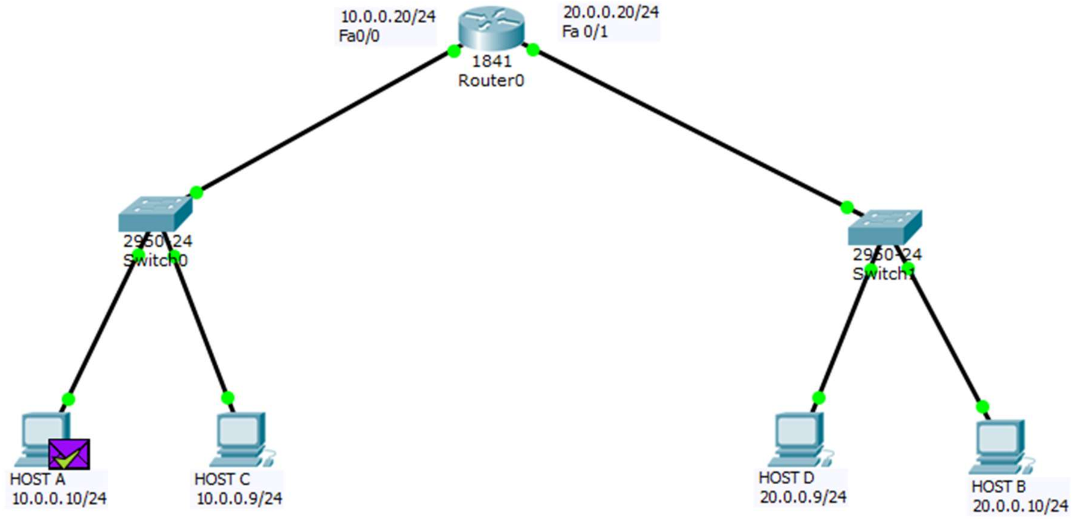


Now the ICMP echo-request packet will be unicast to the host B as shown in the above 3 figures.




10.0.0.20/24
Fa0/0
20.0.0.20/24
Fa 0/1
1841
Router0
2960-24
Switch0
2960-24
Switch1
HOST A
10.0.0.10/24
HOST C
10.0.0.9/24
HOST D
20.0.0.9/24
HOST B
20.0.0.10/24


10.0.0.20/24
Fa0/0
20.0.0.20/24
Fa 0/1
1841
Router0
2960-24
Switch0
2960-24
Switch1
HOST A
10.0.0.10/24
HOST C
10.0.0.9/24
HOST D
20.0.0.9/24
HOST B
20.0.0.10/24


10.0.0.20/24
Fa0/0
20.0.0.20/24
Fa 0/1
1841
Router0
2960-24
Switch0
2960-24
Switch1
HOST A
10.0.0.10/24
HOST C
10.0.0.9/24
HOST D
20.0.0.9/24
HOST B
20.0.0.10/24

Host B will generate an ICMP echo reply in response to the ICMP echo request for host A which will be delivered to the 20.0.0.20 (router's interface IP address) first and then unicast to host A.

Types of ARP

There are four types of Address Resolution Protocol, which is given below:

- Proxy ARP
- Gratuitous ARP
- Reverse ARP (RARP)
- Inverse ARP

Proxy ARP - Proxy ARP is a method through which a Layer 3 devices may respond to ARP requests for a target that is in a different network from the sender. The Proxy ARP configured router responds to the ARP and map the MAC address of the router with the target IP address and fool the sender that it is reached at its destination.

At the backend, the proxy router sends its packets to the appropriate destination because the packets contain the necessary information.

Example - If Host A wants to transmit data to Host B, which is on the different network, then Host A sends an ARP request message to receive a MAC address for Host B. The router responds to Host A with its own MAC address pretend itself as a destination. When the data is transmitted to the destination by Host A, it will send to the gateway so that it sends to Host B. This is known as proxy ARP.

Gratuitous ARP - Gratuitous ARP is an ARP Request of the host that helps to identify the duplicate IP address. It is a broadcast request for the IP address of the router. If an ARP request is sent by a switch or router to get its IP address and no ARP responses are received, so all other nodes cannot use the IP address allocated to that switch or router. Yet if a router or switch sends an ARP request for its IP address and receives an ARP response, another node uses the IP address allocated to the switch or router.

There are some primary use cases of gratuitous ARP that are given below:

- The gratuitous ARP is used to update the ARP table of other devices.
- It also checks whether the host is using the original IP address or a duplicate one.

Reverse ARP (RARP) - It is a networking protocol used by the client system in a local area network (LAN) to request its IPv4 address from the ARP gateway router table. A table is created by the network administrator in the gateway-router that is used to find out the MAC address to the corresponding IP address.

When a new system is set up or any machine that has no memory to store the IP address, then the user must find the IP address of the device. The device sends a RARP broadcast packet, including its own MAC address in the address field of both the sender and the receiver hardware. A host installed inside of the local network called the RARP-server is prepared to respond to such type of broadcast packet. The RARP server is then trying to locate a mapping table entry in the IP to MAC address. If any entry matches the item in the table, then the RARP server sends the response packet along with the IP address to the requesting computer.

Inverse ARP (InARP) - Inverse ARP is inverse of the ARP, and it is used to find the IP addresses of the nodes from the data link layer addresses. These are mainly used for the frame relays, and ATM networks, where Layer 2 virtual circuit addressing are often acquired from Layer 2 signalling. When using these virtual circuits, the relevant Layer 3 addresses are available.

ARP conversions Layer 3 addresses to Layer 2 addresses. However, its opposite address can be defined by InARP. The InARP has a similar packet format as ARP, but operational codes are different.