

CCNA (200-301) Cisco Certified Network Associate

Prepared by Eng. Taghreed Elsayed

Lecture 2

جامعة الجميع الذكية

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

مزيد من التفاصيل

*Internet Protocol version 4
& ARP protocol*



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Objectives

- ☐ What is IPv4?
- ☐ What is Sub netting?
- ☐ What is ARP ?
- ☐ Ethernet what does it mean ?

Chapter 01

Internet Protocol version 4

Five Different Classes of IPv4 Addresses

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID
Class A	0 — 127	0XXXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24} - 2$
Class B	128 — 191	10XXXXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16} - 2$
Class C	192 — 223	110XXXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^8 - 2$
Class D (Multicast)	224 — 239	1110XXXXX	224.0.0.0-239.255.255.255		
Class E (Experimental)	240 — 255	1111XXXXX	240.0.0.0-255.255.255.255		



❖ For example : 10.1.1.1

1. Class A

2. network bits = 8 bits

3. host bits = 24 bits

3. 173.16.30.1

4. Class B

5. network bits = 16 bits

6. host bits = 16 bits

Binary To Decimal Conversion

128	64	32	16	8	4	2	1	Answers	Scratch Area	
1	0	0	1	0	0	1	0	<u>146</u>	128	64
									16	32
0	1	1	1	0	1	1	1	<u>119</u>	2	16
									146	4
1	1	1	1	1	1	1	1	<u>255</u>		2
										1
1	1	0	0	0	1	0	1	<u>197</u>		119
1	1	1	1	0	1	1	0	<u>246</u>		
0	0	0	1	0	0	1	1	<u>19</u>		
1	0	0	0	0	0	0	1	<u>129</u>		
0	0	1	1	0	0	0	1	<u>49</u>		
0	1	1	1	1	0	0	0	<u>120</u>		
1	1	1	1	0	0	0	0	<u>240</u>		

Decimal To Binary Conversion

Use all 8 bits for each problem

128	64	32	16	8	4	2	1	=	255	Scratch Area	
1	1	1	0	1	1	1	0		238	238	34
										-128	-32
0	0	1	0	0	0	1	0		34	110	2
										-64	-2
0	1	1	1	1	0	1	1		123	46	0
										-32	
0	0	1	1	0	0	1	0		50	14	
										-8	
1	1	1	1	1	1	1	1		255	6	
										-4	
1	1	0	0	1	0	0	0		200	2	
										-2	
0	0	0	0	1	0	1	0		10	0	
1	0	0	0	1	0	1	0		138		
0	0	0	0	0	0	0	1		1		
0	0	0	0	1	1	0	1		13		

Determine : network Id , broadcast IP

193.30.11.1

class c → no of network bits = 24bits

no of host bits = $32 - 24 = 8$ bits

Network id = 193.30.11.0

First ip = 193.30.11.1

Last ip = 193.30.11.254

Broadcast ip = 193.30.11.255

ANDING With Default subnet masks

Every IP address must be accompanied by a subnet mask. By now you should be able to look at an IP address and tell what class it is. Unfortunately your computer doesn't think that way. For your computer to determine the network and subnet portion of an IP address it must "AND" the IP address with the subnet mask.

Default Subnet Masks: Class A 255.0.0.0
 Class B 255.255.0.0
 Class C 255.255.255.0

ANDING Equations: $1 \text{ AND } 1 = 1$ $1 \text{ AND } 0 = 0$ $0 \text{ AND } 1 = 0$ $0 \text{ AND } 0 =$

For example: 192.168.1.1 class c /24 prefix

Network address o network ip

192.168.1.1 = 192 . 168 . 1 . 1

AND = 192.168.1.0

255.255.255.0 = 1111 . 1111 . 1111 . 0

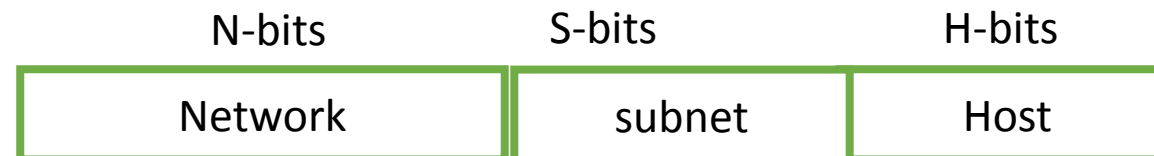
Last ip address = 192.168.1.254

broadcast ip = 192.168.1.255

No of hosts = $2^H - 2$

Sub netting

- ❑ **Sub netting means making subnet from network**
- ❑ **Sub netting is done by taking some bits from host bits and add it to network bits**



For example: 172.16.0.0 /16

Calculate the subnet mask required to make :

- 1. 200 subnet**
- 2. 200 host /subnet**

Solution :

To get no of bits required to make 200 subnets

$$2^s \geq 200 \quad s=8\text{bits} \quad \text{prefix} = n\text{-bits} + s\text{-bits} = 16+8=24 \quad /24$$

Subnet mask = 255.255.255.0

H-bits= 8bits

No of hosts = $2^s - 2 = 254$

Design example1: 192.168.1.0 /24

- ❖ If we need to make 4 subnets
- ❖ Calculate the ranges of ip addresses

Sol:

1. No of s- bits = $2^s \geq 4$ s=2bits

2. 192.168.1. xx 00 0000

1st

192.168.1. 0 /26

2nd

192.168.1.64 /26

3rd

192.168.1.128 /26

4th

192.168.1.192 /26



For the **first subnet** , the range of **ip addresses** :
192.168.1.0 /26

First ip	192.168.1.1
Last ip	192.168.1.62
Broadcast ip	192.168.1.63

Design example2: 193.168.30.207 /29

Get network Id, First ip , Last ip , Broadcast ip

Sol:

1.Subnet mask 255.255.255. 248
255.255.255. 1111 1000

2.Network id 193.168.30 . 1100 1111 =207
255.255.255. 1111 1000 =248

193.168.30. 1100 1000= 200

Network ip address = 193.168.30.200

First ip 193.168.30.201

Last ip 193.168.30.206

Broadcast ip 193.168.30 .xxxx x 111=
193.168.30.1100 1 111 = 193.168.30.207

IPv4 Header

Version	IHL	ToS	Total Length	
Identification			Flgs	Fragment Offset
Time To Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options				Padding

most IP packets have a 20-byte header, with a maximum of **60 bytes** being used for this data. TCP segments also have their own header information, with a minimum value of 20 bytes (the most common), and a maximum size of 60 bytes.

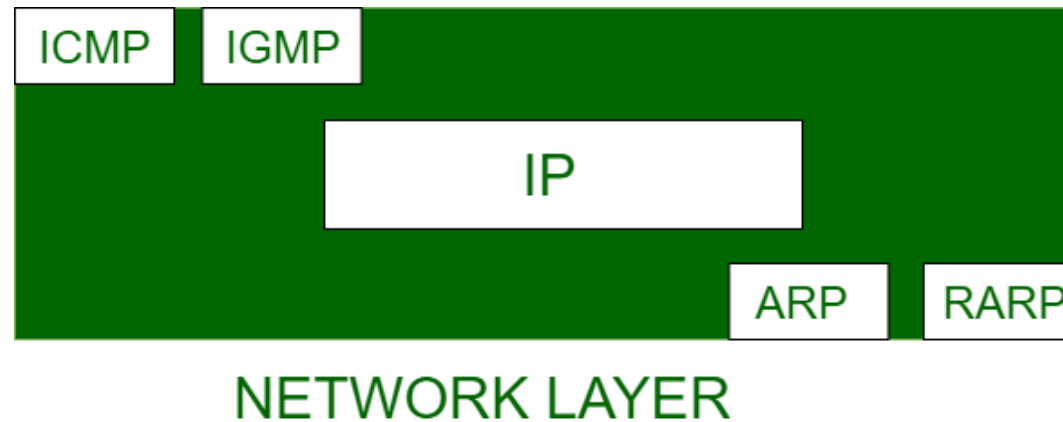
- ❑ **VERSION:** Version of the IP protocol (4 bits), which is 4 for IPv4
- ❑ **HLEN:** IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.
- ❑ **Type of service:** Low Delay, High Throughput, Reliability (8 bits)
- ❑ **Total Length:** Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.
- ❑ **Identification:** Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)

- ❑ **Flags:** 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)
- ❑ **Fragment Offset:** Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.
- ❑ **Time to live:** Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.
- ❑ **Protocol:** Name of the protocol to which the data is to be passed (8 bits)

- ❑ **Header Checksum:** 16 bits header checksum for checking errors in the datagram header
- ❑ **Source IP address:** 32 bits IP address of the sender.
- ❑ **Destination IP address:** 32 bits IP address of the receiver.
- ❑ **Option:** Optional information such as source route, record route.
Used by the Network administrator to check whether a path is working or not.

❖ **Address Resolution Protocol (ARP)** which is one of the most important protocols of the Network layer in the OSI model.

Note: ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.



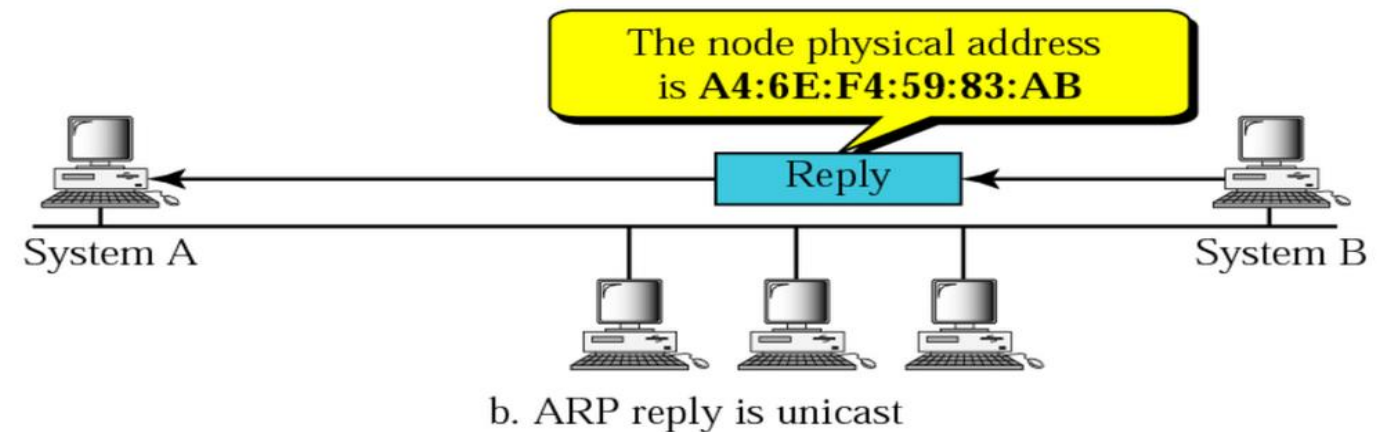
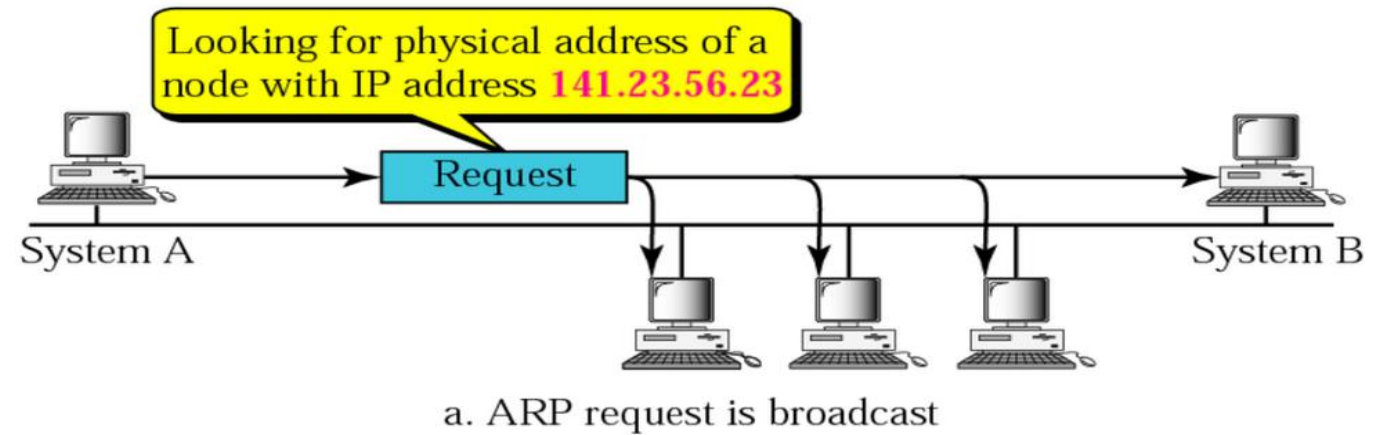
1.ARP Cache Timeout: It indicates the time for which the MAC address in the ARP cache can reside

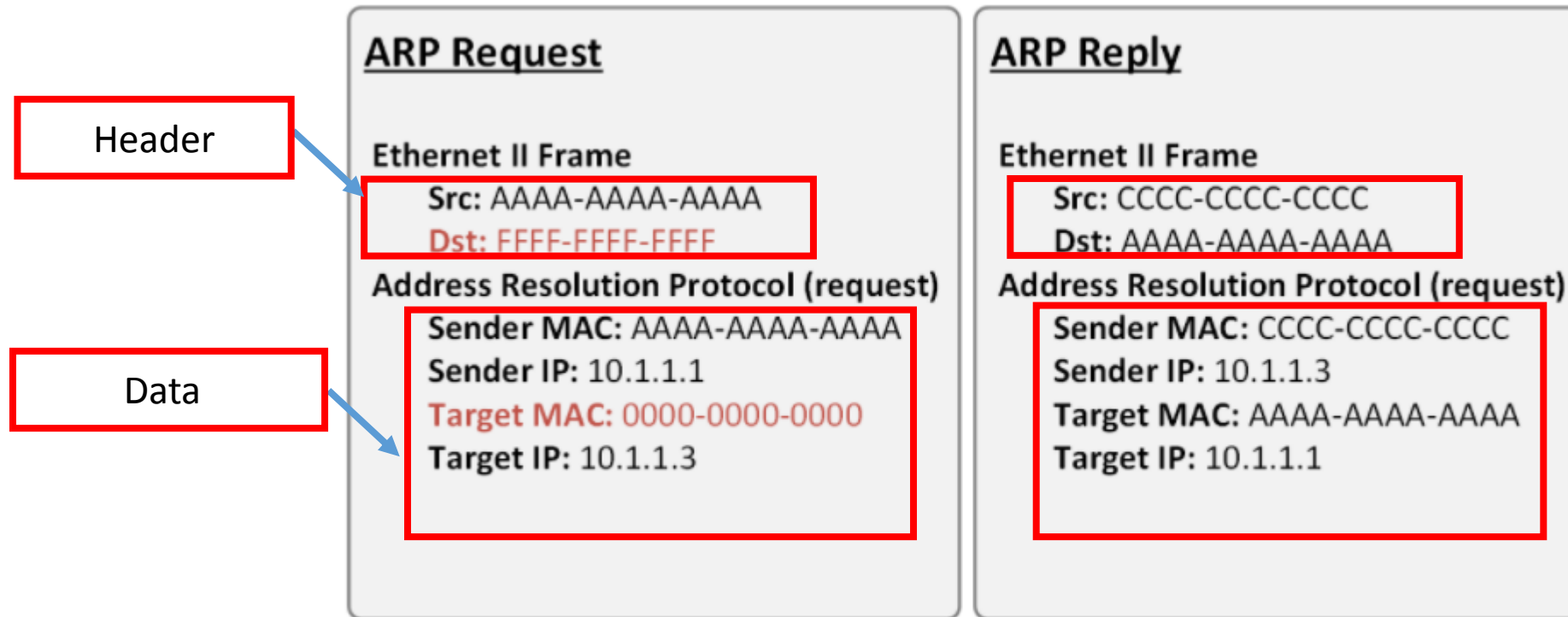
2.ARP request: This is nothing but broadcasting a packet over the network to validate whether we came across the destination MAC address or not.

1. The physical address of the sender.
2. The IP address of the sender.
3. The physical address of the receiver is FF:FF:FF:FF:FF:FF or 1's.
4. The IP address of the receiver

3.ARP response/reply: It is the MAC address response that the source receives from the destination which aids in further communication of the data

CASE-1: The sender is a host and wants to send a packet to another host on the same network.
Use ARP to find another host's physical address



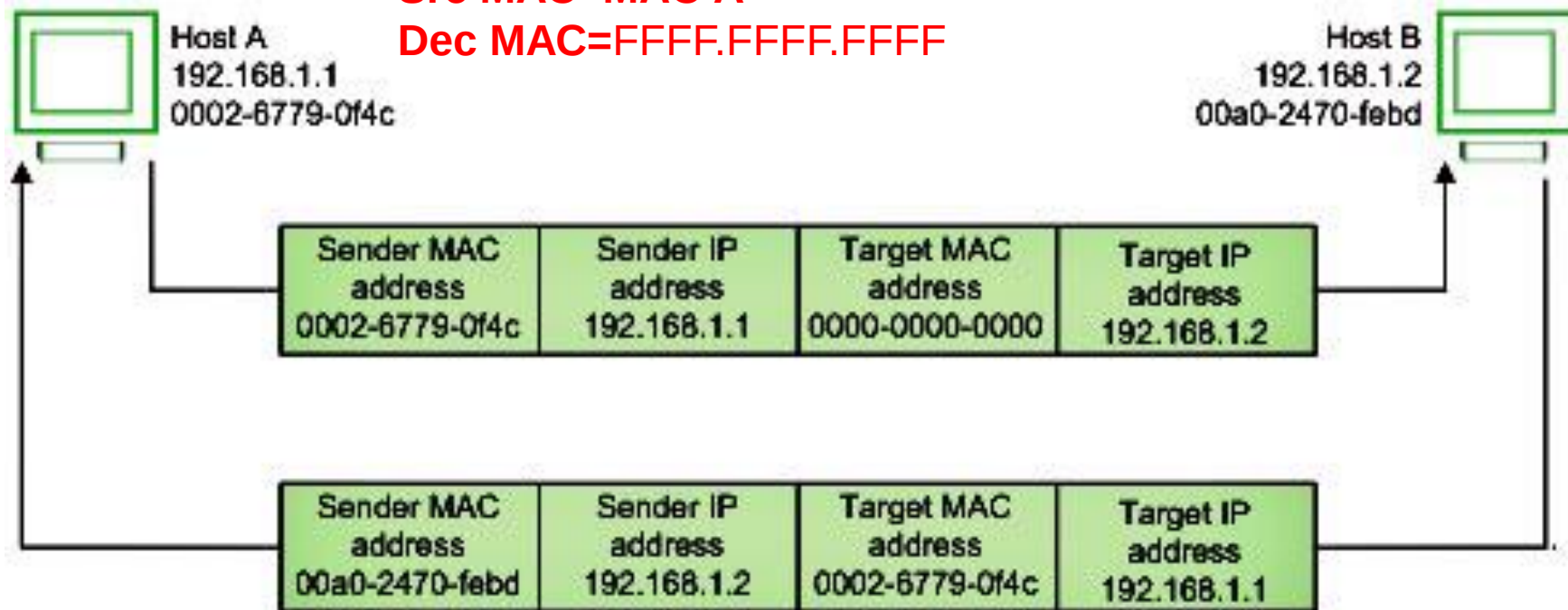


ARP request (broadcast)

Header :

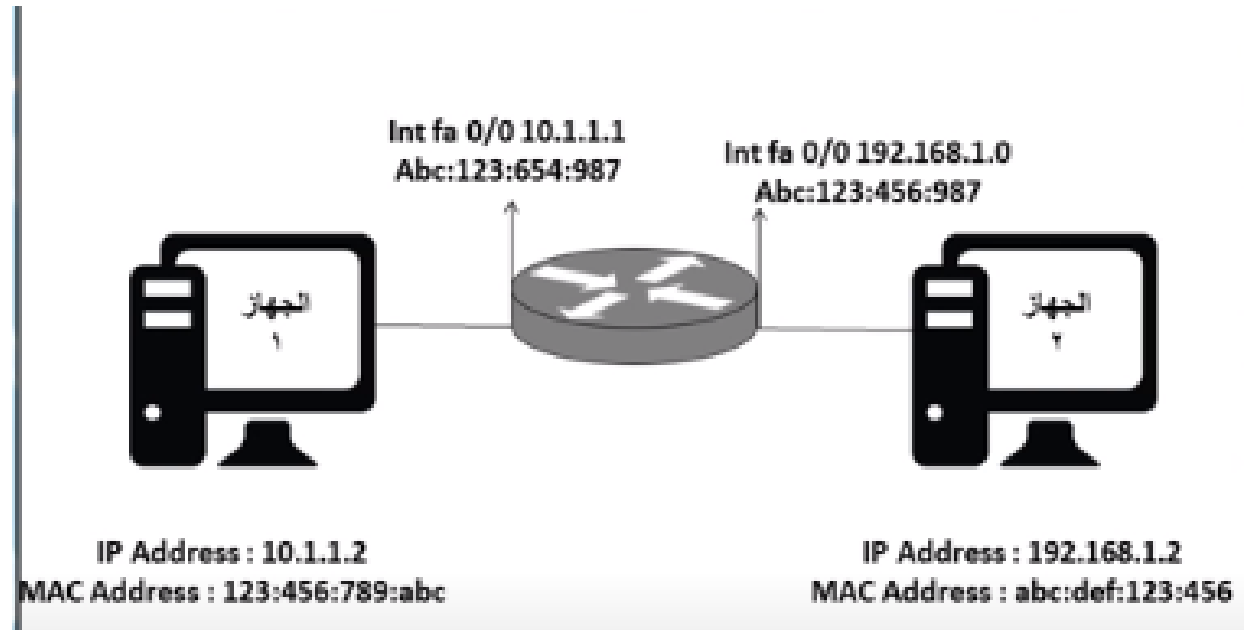
Src MAC=MAC A

Dec MAC=FFFF.FFFF.FFFF



CASE-2: The sender is a host and wants to send a packet to another host on another network.

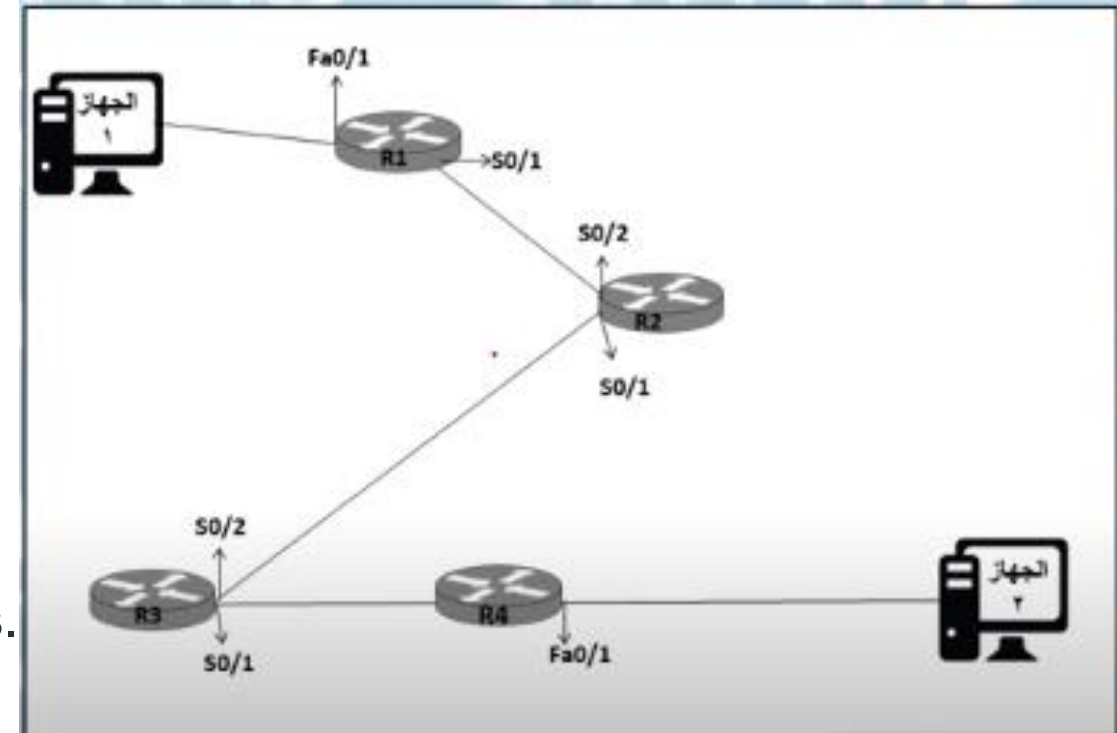
Find the IP address of the next-hop (router) for this destination.
Use ARP to find the router's physical address



CASE-3: the sender is a router and received a datagram destined for a host on another network.

- ❖ The router checks its routing table.
- ❖ Find the IP address of the next router.
- ❖ Use ARP to find the next router's physical address.
- ❖ Use ARP to find this host's physical address.

NOTE: An ARP request is a broadcast, and an ARP response is a Unicast.



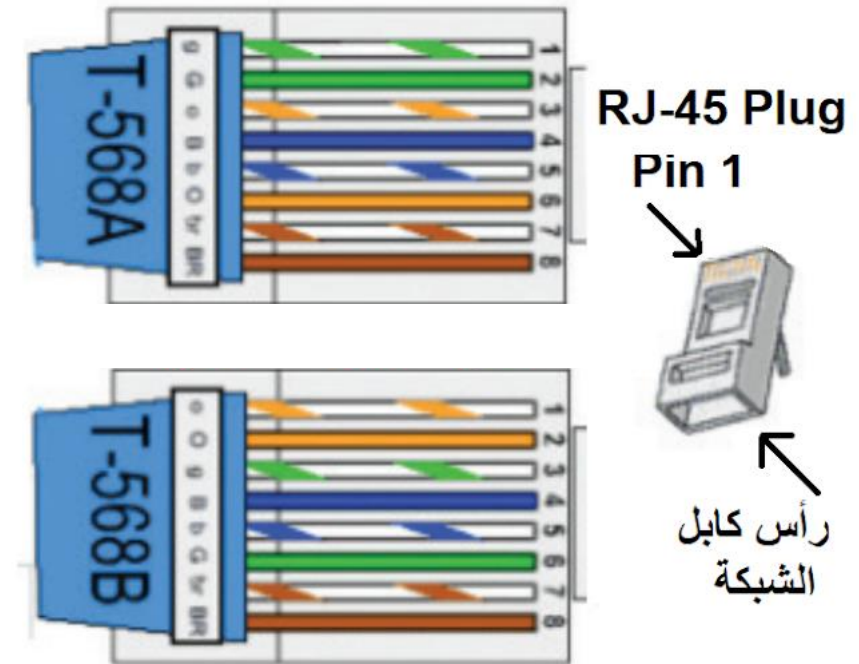
Ethernet is the traditional technology for connecting devices in a wired local area network ([LAN](#)) or wide area network (WAN).

- ❑ It enables devices to communicate with each other via a [protocol](#), which is a set of rules or common network language.
- ❑ Ethernet describes how network devices format and transmit data so other devices on the same LAN or campus network can recognize, receive and process the information.
- ❑ An Ethernet cable is the physical, encased wiring over which the data travels.
- ❑ Connected devices that use cables to access a geographically localized network -- instead of a wireless connection -- likely use Ethernet. From businesses to gamers, diverse end users rely on the benefits of Ethernet connectivity, which include reliability and security.

How Ethernet works

- ❑ IEEE specifies in the family of standards called IEEE [802.3](#) that the Ethernet protocol touches both Layer 1 (physical layer) and Layer 2 (data link layer) on the Open Systems Interconnection ([OSI](#)) model.
- ❑ Ethernet defines two units of transmission: packet and frame. The frame includes the payload of data being transmitted as well as the following:
 - ❑ the physical media access control (MAC) addresses of both the sender and receiver;
 - ❑ Each frame is wrapped in a packet that contains several bytes of information to establish the connection and mark where the frame starts.

When you connect two devices of different types together, you use a straight through cable. When you connect two devices of the same type together, you use a **crossover cable**. All cables are straight through if you insert a network device between two devices of the same kind



MDI and MDI-X

Away from the CCNA exams, **there is one more complication** to take into account when you are buying network cables. If your device implements **MDI and MDI-X**, you don't need to worry about crossover cables. MDI is the **Medium Dependent Interface** standard and it operates inside the socket of a NIC. It can detect which wire transmissions arrive on rather than doggedly listening on pins 3 and 6. MDI-X stands for **Medium Dependent Interface – Crossover**. So, if your computer, printer, switch, router or modem has **MDI** printed on the box, you only need to buy a straight through cable.

Crossover cables

A **crossover cable** does exactly as its name suggests, it crosses over the wire from pin 1 at one end to pin 3 at the other connector. The wire that is crimped to pin 2 at one end is attached to pin 6 at the other end and the pins 3 and 6 wires go to pins 1 and 2 respectively in the other connector. The crossover cable follows both **EIA-568A** and **EIA-568B**. It is A at one end and B at the other. **So those conflicting standards did end up being useful.**

To pass your CCNA exams, you just need to know that the pin that the striped orange wire connects to on the left of the diagram takes the striped green wire on the right of the diagram. The pin that takes the solid green wire on the left, takes the solid orange wire on the right. You could also write down orange left and green right and you would still get full marks.

What Is Straight Through Cable?

A straight through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal. On a straight through cable, the wired pins match. Straight through cable use one wiring standard: both ends use T568A wiring standard or both ends use T568B wiring standard.

The Main Differences-Straight Through and Crossover Cable

Straight through and crossover cables are wired differently from each other. One easy way to tell what you have is to look at the order of the colored wires inside the RJ45 connector. If the order of the wires is the same on both ends, then you have a straight through cable. If not, then it's most likely a crossover cable or was wired wrong.



What Are the Various Types of Ethernet Networks?

Fiber optic media converters connect an Ethernet device with CAT5/CAT6 copper cables to a fiber optic cable. An Ethernet network usually is active in a 10-km periphery. This extension to fiber optic cable significantly increases the distance covered by the network. Here are some types of Ethernet networks:

- Fast Ethernet:** As the term suggests, this is quite a high-speed internet, and can transmit or receive data at about 100 Mbps. This type of network is usually supported by a twisted pair or CAT5 cable. If a laptop, camera, or any other device is connected to a network, they operate at 10/100Base Ethernet and 100Base on the fiber side of the link.

- Gigabit Ethernet:** This type of network transfers data at an even higher speed of about 1000 Mbps or 1Gbps. Gigabit speed is an upgrade from Fast Ethernet which is slowly being phased out. In this type of network, all the four pairs in the twisted pair cable contribute to the data transfer speed. This network type finds a large application in video calling systems which use CAT5e or other advanced cables. For extended networks, the distance of up to 500m, 1000Base SX fiber cables may be used for multimode,

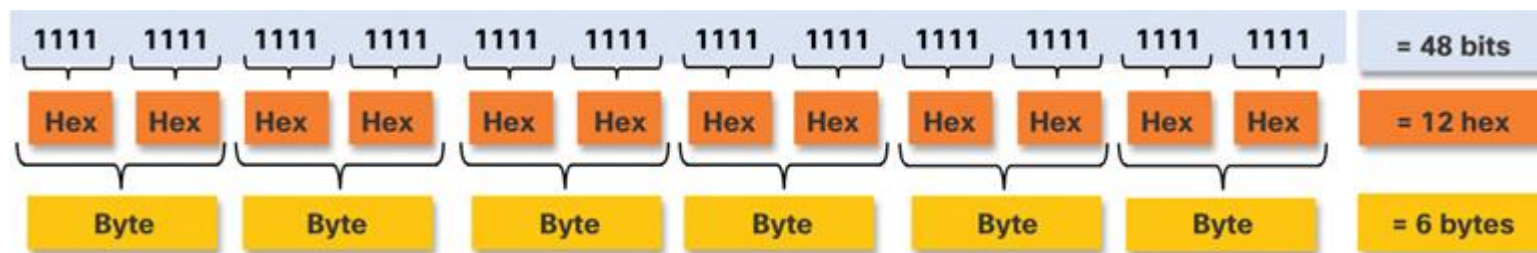


- This network type finds a large application in video calling systems which use CAT5e or other advanced cables. For extended networks, the distance of up to 500m, 1000Base SX fiber cables may be used for multimode, as well as 1000Base LX for single mode systems. VERSITRON manufactures Gigabit Ethernet Media Converters that can handle 10/100/1000Base speeds on the Ethernet side and 1000Base Gigabit speed on the fiber side by using [Fiber SFP modules](#).
- **10-Gigabit Ethernet:** This is an even more advanced and high speed network type with a data transfer rate of 10 Gigabit/second. It is supported by CAT6a or CAT7 twisted pair cables, as well as fiber optic cables. By using a fiber optic cable, this network area can be extended up to around 10,000 meters.

Ethernet MAC Address (7.2.2)

In an Ethernet LAN, every network device is connected to the same shared medium. The MAC address is used to identify the physical source and destination devices (NICs) on the local network segment. MAC addressing provides a method for device identification at the data link layer of the OSI model.

An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits, as shown in [Figure](#). Because 1 byte equals 8 bits, we can also say that a MAC address is 6 bytes in length.



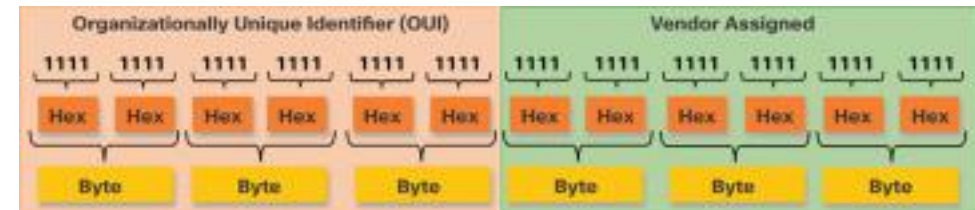
All MAC addresses must be unique to the Ethernet device or Ethernet interface. To ensure uniqueness, every vendor that sells Ethernet devices must register with the IEEE to obtain a unique 6-digit hexadecimal (that is, 24-bit or 3-byte) code called an *organizationally unique identifier (OUI)*.

When a vendor assigns a MAC address to a device or to an Ethernet interface, the

vendor must do as follows:

- Use its assigned OUI as the first 6 hexadecimal digits.
- Assign a unique value in the last 6 hexadecimal digits.

Therefore, an Ethernet MAC address consists of a 6-digit hexadecimal vendor OUI code followed by a 6-digit hexadecimal vendor-assigned value, as shown in [Figure](#) .

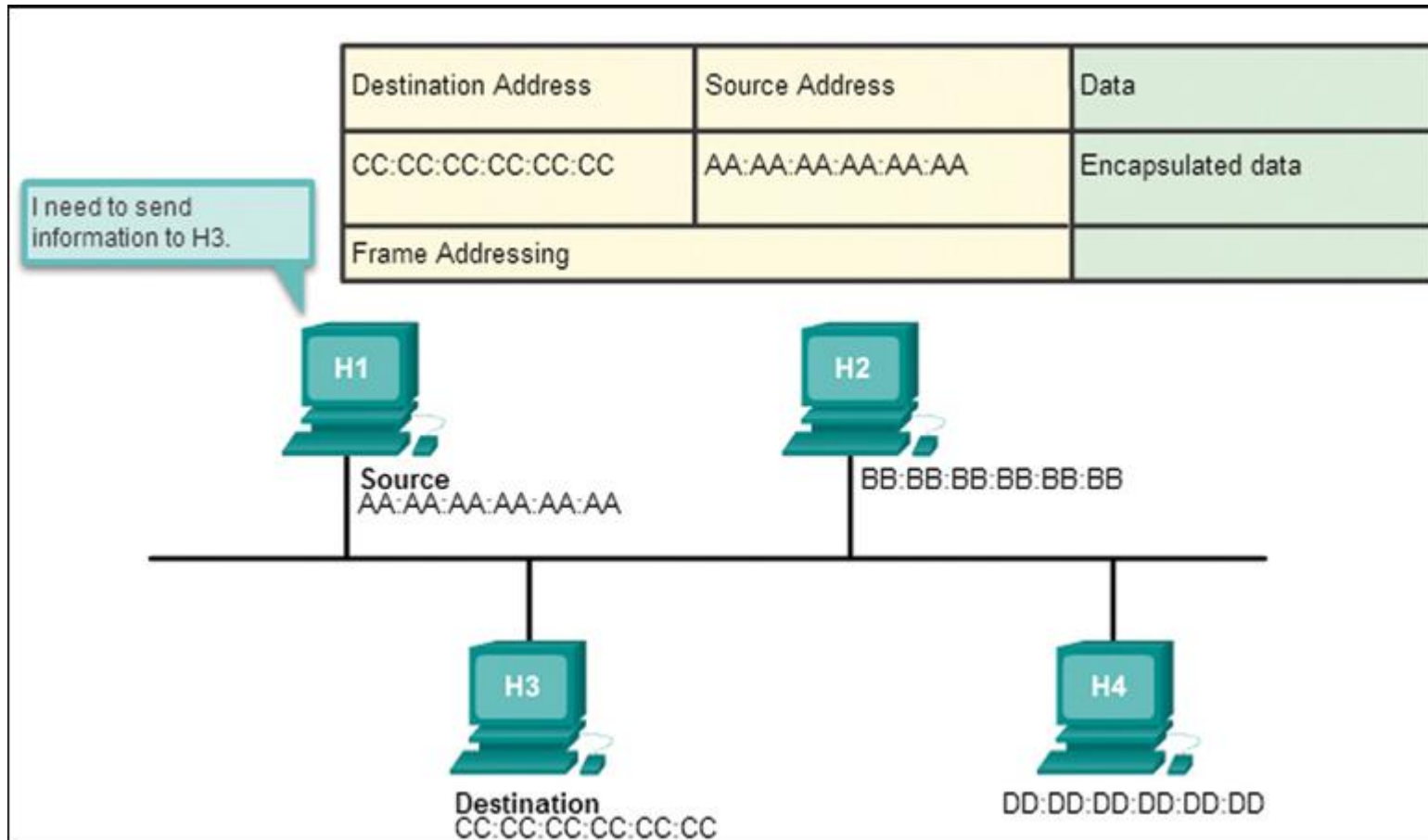


When the computer boots up, the NIC copies its MAC address from ROM into RAM. When a device is forwarding a message to an Ethernet network the Ethernet header includes the following:

- **Source MAC address:** This is the MAC address of the source device NIC.
- **Destination MAC address:** This is the MAC address of the destination device NIC.

Chapter 01

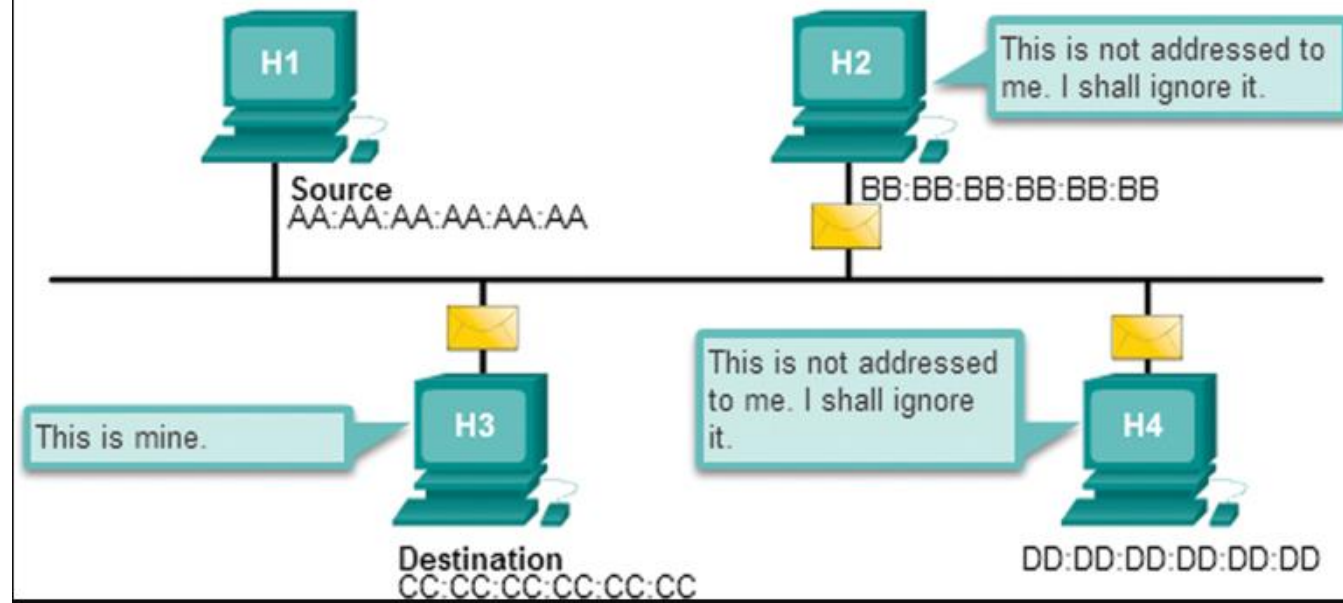
Ethernet



Chapter 01

Ethernet

Destination Address	Source Address	Data
CC:CC:CC:CC:CC:CC	AA:AA:AA:AA:AA:AA	Encapsulated data
Frame Addressing		





جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

