FIT1047 Applied Session Week 9

NETWORKS: LOCAL AREA NETWORKS AND WIRELESS LOCAL AREA NETWORKS

OBJECTIVES

- The purpose of this applied session is getting to know about data movements in LANs, WLANs and WANs.

INSTRUCTIONS

- For some of the questions, you may have to refer to the pre-class video and associated slides available in the Moodle.
- You may work in a small group.

Activity 1: Data Link Layer (Ethernet): Analysing Packets Captured in LANs

In this activity you will use Wireshark to capture the network traffic (Figure: 2) from and to your client computer and also at different network sections leading up to the destination server computer in the network shown in Figure 2.

We will investigate the MAC addresses present in the frames captured in different network sections. Ethernet frames have the following structure:

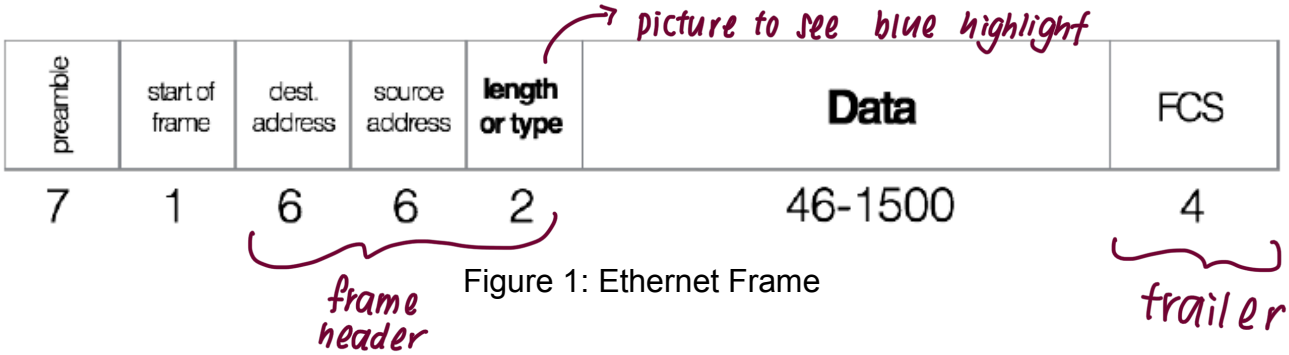


Figure 1: Ethernet Frame

Fields visible in Wireshark:

- 6-byte destination and 6-byte source MAC addresses
- 2-byte length or type of frame field.

  Example: a type of 0x0800 means the frame contains an IPv4 packet, 0x086dd means IPv6, and 0x0806 indicates an ARP frame
- Variable length data field – 46 to 1500 bytes.

Hardware fields (not visible in Wireshark):

- 7-byte preamble: repeating pattern of ones and zeros
- 1-byte start of frame delimiter (SFD): 10101011
- 4-byte CRC-32 frame check sequence

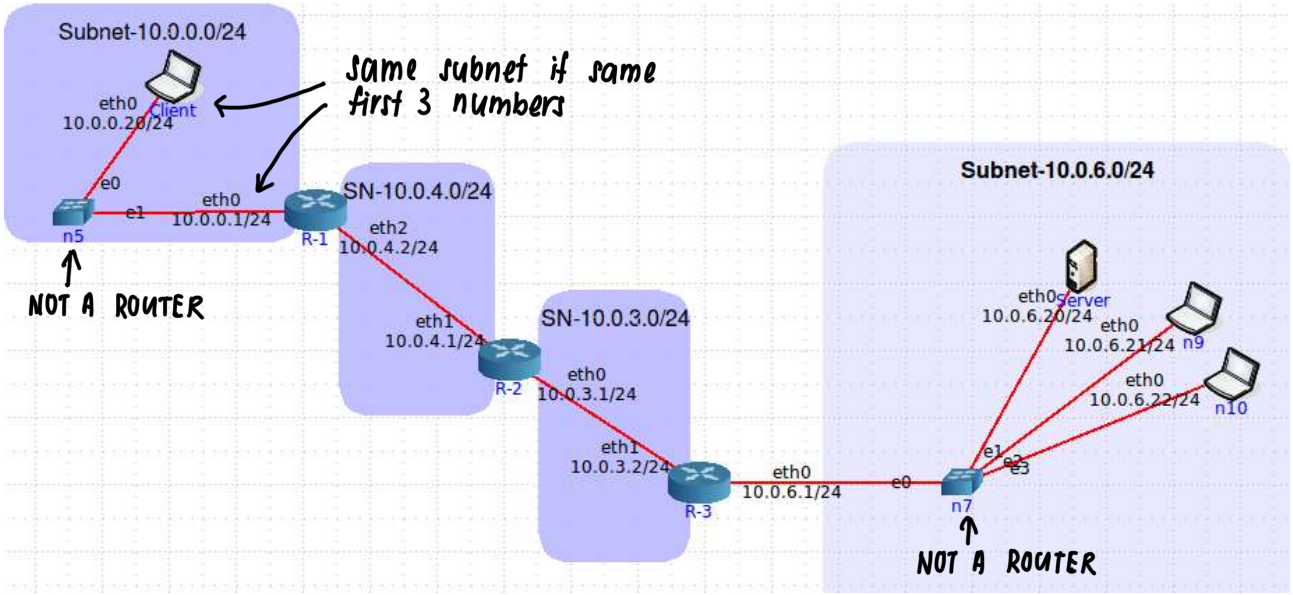


Figure 2: A Client-server pair with supporting networks

physical address (permanent)

Table 1: Addresses Used in the network in Figure 2

Device	Interface	MAC	IP
Client	eth0	00:00:00:aa:00:08	10.0.0.20
Router R-1	eth0 eth2	00:00:00:aa:00:09 00:00:00:aa:00:03	10.0.0.1 10.0.4.2
Router R-2	eth0 eth1	00:00:00:aa:00:00 00:00:00:aa:00:02	10.0.3.1 10.0.4.1
Router R-3	eth0 eth1	00:00:00:aa:00:07 00:00:00:aa:00:01	10.0.6.1 10.0.3.2
Server	eth0	00:00:00:aa:00:04	10.0.6.20

Why need 2 addresses? different layers have different address to do different functions / actions

(i) Analyze the frame 1 captured in "FIT1047-2022-Applied-W9-Q1a.pcapng" and answer the following questions. Please note that this file captures packets in the subnet 10.0.0.0/24.

a. What is the value of the Ethernet address of the client computer?
b. What is the destination address in the Ethernet frame? Is this the Ethernet address of the Server or a router?
c. Give the hexadecimal value for the two-byte Frame type field.
d. What are the source and destination IP addresses?

(ii) Analyze the frame 1 captured in "FIT1047-2022-Applied-W9-Q1b.pcapng" and answer the following questions. Please note that this file captures packets in the subnet 10.0.4.0/24.

a. What is the value of the Ethernet source address? Is this the address of the client computer, or of a router?
b. What is the destination address in the Ethernet frame? Is this the Ethernet address of a router?
c. Give the hexadecimal value for the two-byte Frame type field.
d. Are there any changes in the source and destination IP addresses?

(iii) Analyze the frame 1 captured in "FIT1047-2022-Applied-W9-Q1c.pcapng" and answer the following questions. Please note that this file captures packets in the subnet 10.0.3.0/24.

a. What is the value of the Ethernet source address? Is this the address of a router?

b. What is the destination address in the Ethernet frame? Is this the address of a router?
c. Give the hexadecimal value for the two-byte Frame type field.
d. Are there any changes in the source and destination IP addresses?

(iv) Analyze the frame 1 captured in “FIT1047-2022-Applied-W9-Q1d.pcapng” and answer the following questions. Please note that this file captures packets in the subnet 10.0.6.0/24.

a. What is the value of the Ethernet source address? Is this the Ethernet address of the client computer?
b. What is the destination address in the Ethernet frame? Is this the address of the server, or of a router?
c. Give the hexadecimal value for the two-byte Frame type field.
d. Are there any changes in the source and destination IP addresses?

Activity 2: Detection of Wireless Networks

In this activity we will run software that can capture wireless signals from the surroundings of your laptop equipped with a wireless network interface card (WNIC).

War-Driving and War-Walking

Wireless LANs are often not secure. It is simple to bring your laptop computer into a public area and listen for wireless networks. This is called War-Driving (if you are in a car) or War-Walking (if you're walking). As long as you do not attempt to use any networks without authorization, War-Driving and War-Walking are quite legal. There are many good software tools available for War-Driving.

- NetSpot for Windows or Mac OS (http://www.netspotapp.com)
- Acrylic Wifi for Windows (https://www.acrylicwifi.com/en/)

The first step is to download and install a WLAN sniffing tool on a laptop computer that has wireless capability. Once you have installed the software, simply walk or drive to a public area and start it up. For each network, note the BSS-ID of the access point (similar to a MAC address) which also can be termed as a physical address. Please note: BSS-ID is Basic Services Set ID and SS-ID is Services Set ID. You can notice other data items listed such as the SSID, the channel number the Wireless Access Point (AP) is configured to use, the mode of the network (g, n a etc.), the access point vendor, and the type of encryption in use (if any). Also note the signal strength shown by color coding (green is good). The signal-to-noise ratio (SNR) and the noise data is only available in the mac OS. You will see a list of WLANs in your capture.

The channels we usually use for 802.11b and 802.11g are channels 1, 6, and 11. 802.11b and 802.11g can be configured to use four channels (1, 4, 8, and 11), although the channels overlap to some extent. So if you run an AP on channel 1 and another on channel 4, there will be some interference between the two APs. The best practice recommendation that most companies follow is to use a three-channel configuration.

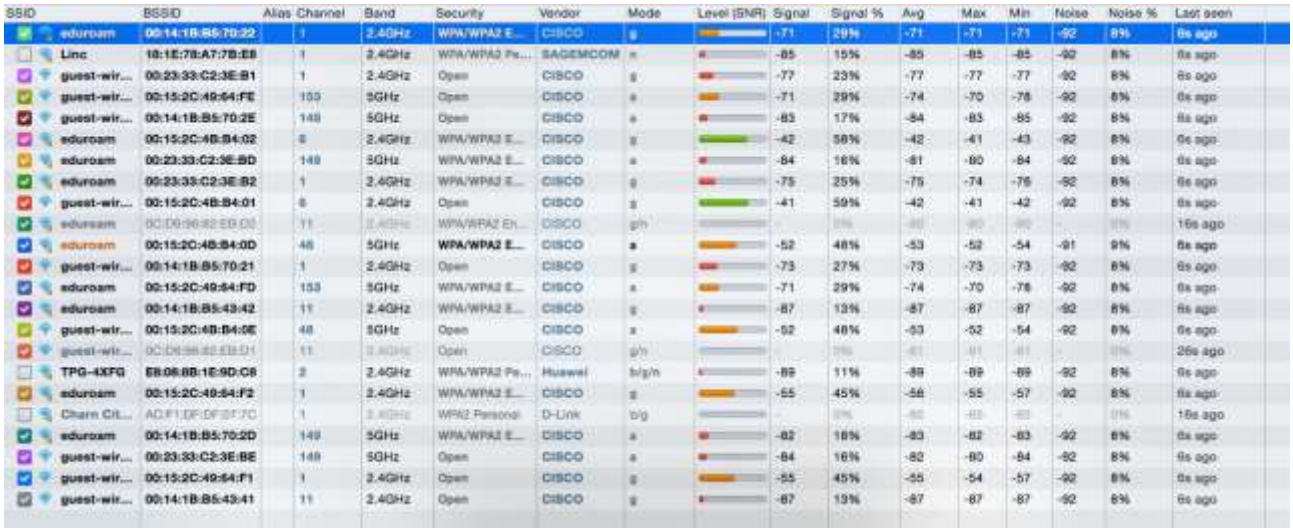


Figure 3: Wireless LAN capture in netspot

If you click on an access point in the left panel, the tool shows you a real time graph of the signal and noise for that network. You will see how the signal strength changes for one of the networks as you walk through any building. In Figure 5, the left edge of the graph shows that the network started with a good signal (the green or light colored area at the top of the bars) was much higher than the noise (the red or dark colored area at the hot- tom of the bars). As the signal capturing device (i.e. PC with netspot software running) moved around, the signal became weaker; the signal was barely higher than the noise. As the device moved more, the signal dropped so that it was too weak for it to be detected from the noise.

Figure 4: Signal vs Time

Activity 3: IPv4 Addresses, Subnets and Masks (repeat)

(i) Each IP address identifies one particular device (or more precisely, one network interface of one device). But IP addresses have structure: a certain number of bits are used to identify thesubnet that the device belongs to, and the remaining bits identify the concrete device in that subnet.

We use notation such as 130.196.13.5/24 to denote that the first 24 bits identify the subnet. In this case, it means any device whose IP address also starts with 130.196.13. belongs to the same subnet. This is important: Let's say 130.196.13.5 wants to send a message to 130.196.13.32; it can just look at the IP address to know that the destination is in the same subnet, which means that it can send the message directly. But if the destination is, e.g., 130.196.42.3, the IP address tells us that it's in a different subnet, so we have to send the message to our router.

We call /24 the subnet mask. An alternative notation, called "dotted-decimal", is 255.255.255.0, which when written in binary is simply a sequence of 24 ones, followed by 8 zeroes:

11111111.11111111.11111111.00000000

1st Octet	2nd Octet	3rd Octet	4th Octet
1111 1111.	1111 1111.	1111 1111.	0000 0000

The subnet address (which identifies the subnet) can be obtained by replacing the host part of an IP address with zero bits. e.g. the subnet address of 130.196.13.5/24 is 130.196.13.0/24.

(a) Write the subnet mask /22 using "dotted-decimal" notation.
(b) Write the subnet mask 255.255.0.0 using "slash" notation.

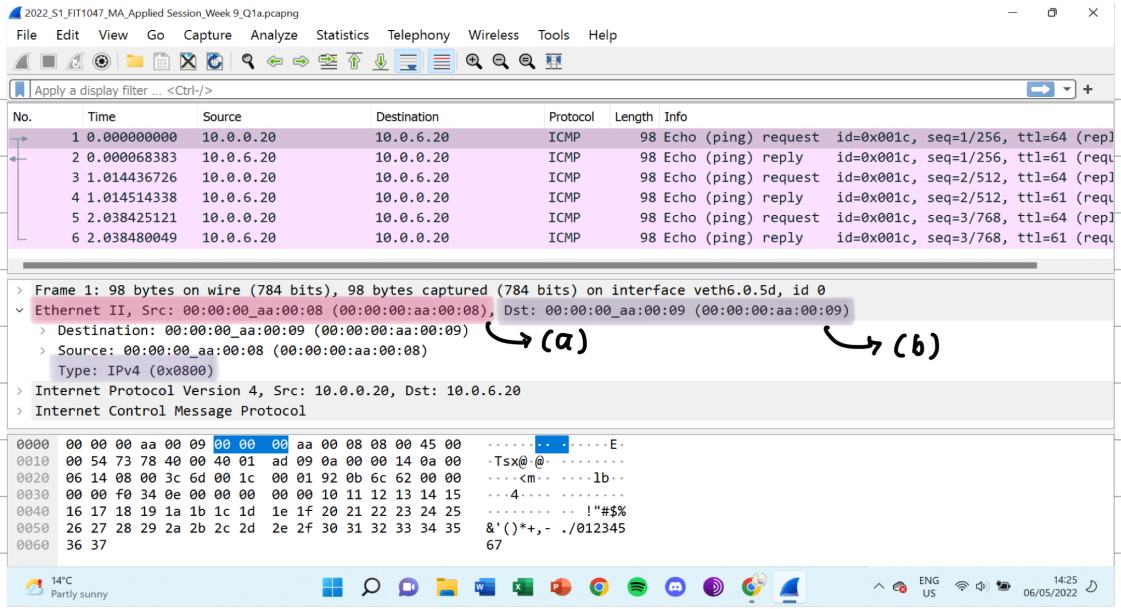
(ii) You are required to provide a detailed IP addressing plan for a company using the network address 202.169.63.0/24. How many IP addresses are available in this network? The networking team has decided to create three subnets for a varying number of hosts in each.

- Subnet A – 202.169.63.0/25
- Subnet B – 202.169.63.128/26
- Subnet C – 202.169.63.192/27

To complete the IP addressing plan, you are required to provide the following details for each subnet:

a) Usable IP address range
b) Broadcast IP address
c) Subnet address

1)(i)



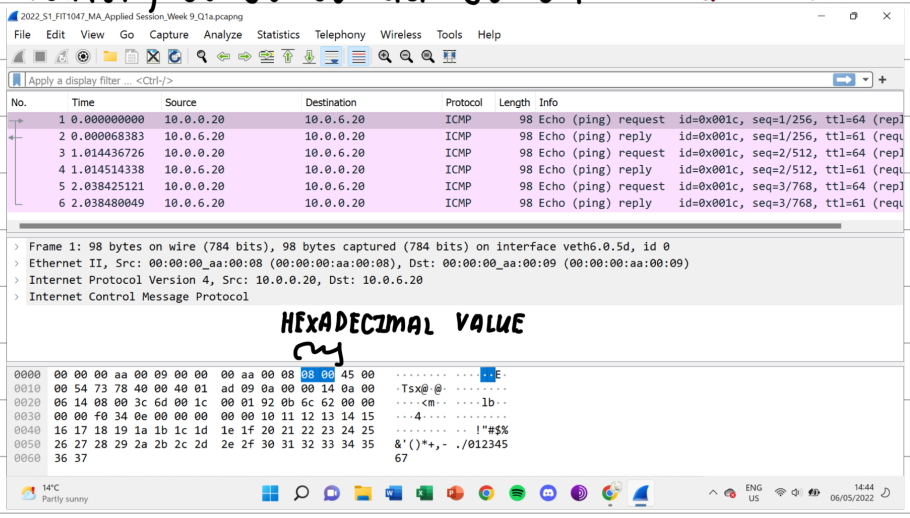
* MAC address = Ethernet address

(a) 00:00:00:aa:00:08

(b) router, 00:00:00:aa:00:09

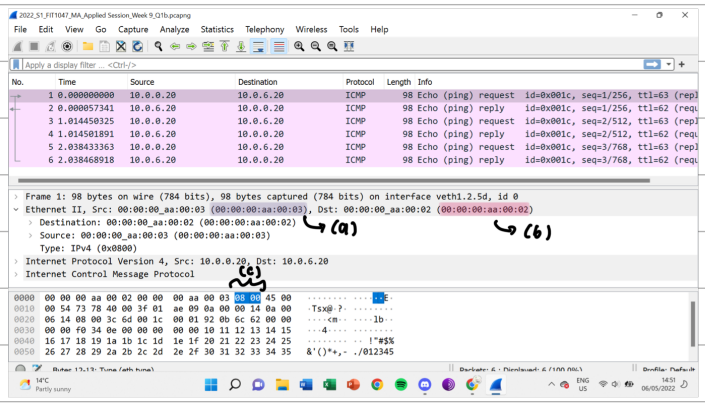
* FOR (b), why is it not a server address but a router address ?

(c)



(d) 10.0.0.20 to 10.0.6.20

(i)



* (iii) & (iv) is the same

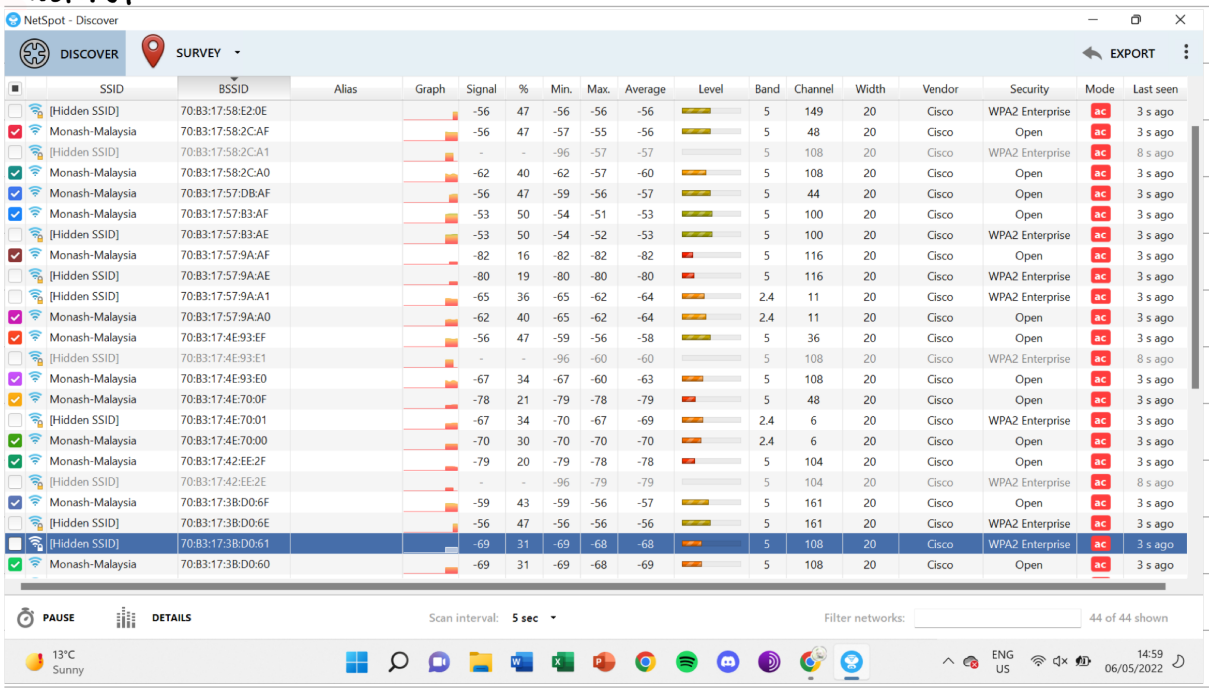
(a) router 1, 00:00:00:aa:00:03

(b) router 2, 00:00:00:aa:00:02

(c) 0800

(d) no change

NETSPOT :



- software tool for wireless network assessment, scanning & survey
- analyze Wi-Fi coverage and performance

At a glance you will be able to see specific details about each wireless network detected in the area, including:

- SSID — the name of the network
- Channel — the channel the network is broadcasting on (1, 6, 11, etc.)
- Band – the band the network is broadcasting on (2.4 GHz, 5 GHz, 20 MHz, 40 MHz)
- Security Type — the kind of security the network has (WEP, WPA, WPA2, etc.)
- Mode — which 802.11 protocol the network has (a/b/g/n/ac)
- Level (SNR) — the network's Signal-to-Noise Ratio level
- Signal level — how strong the network's signal is
- Noise level — how much noise is interfering with the network

* signal strength larger is better

↑ SNR, ↑ bit rate (?)

Signal strength same as noise to get the coverage of (?)

Noise floor cannot be eliminated

WEEK 8 APPLIED :

$w(t) = A \sin(2\pi ft + \phi)$ → no. of symbols / levels

No of bits / symbols = $\lceil \log_2(L) \rceil = \log_2(4) = 2$ bits / symbols

Physical Layer

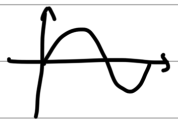
Figure 2 : modulated message

Why take 0 to 1 as a symbol instead of 0 to 2 ?

ANSWER : The frequency is 1

↳ cycle (time) = $1/f = 1/1Hz$ = 1 second

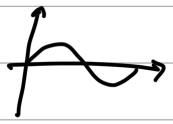
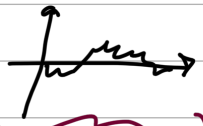
* if frequency ↑, ↑ cycle per second

what you send :  } when SNR is ↑

if it passes through a noisy channel...

what will be received :  } corrupted / distorted sine wave

* If signal-to-noise-power (SNR) ↑, can still see shape of sine wave on distorted sine wave, receiver still can distinguish

when SNR ↓ :  AND it pass through a noisy channel... 

loss original shape ← distortion corrupt the waves badly

Networking Layer

Subnet mask (network id bits + host id bits) = 32 bits

if network id = 20 ; host id = 12 :

11111111. 11111111. 11110000. 00000000 } dotted-decimal-notation

255 . 255 . 240 . 0 * 0 represents host id

subnet mask = 255.255.240.0 * 1 represents network id

number of subnet = 2^{20} ($2^{\text{network id number}}$)

number of host = $2^{12} - 2$ ($2^{\text{host id number}} - 2$) → network id number

* slash notation (/) to represent subnet (eg. /20)

Subnet A : 202.169.63.0/25

① convert 202 to 11001010 using decimal to binary converter

② 169 → 10101001

③ 63 → 00111111

④ 0 → 00000000

② ③ ④ converted using decimal → binary converter

11111111.11111111.11111111.10000000 } subnet mask

↳ 25 1's and 7 0's

↳ 25 network id with 7 hosts id

11001010.10101001.00111111.00000000

SO... network id for subnet A (11001010.10101001.00111111.0_____)

can't be changed (mail id)

host id for subnet A (_____._____._____.0000000)

can be changed

↳ change bit-by-bit

↳ first address = 11001010.10101001.00111111.00000000

↳ last address = 11001010.10101001.00111111.01111111

recording : name = 2022_S1_FIT1047_MA_Applied Session_Week 8_video.mp4

timing : 37:00