Exercices donnés en TD ainsi qu'aux examens.

MASQUE ACTIVé

Table des matières

Chapitre N°01 - Notions Fondamentales

Chapitre N°02 - Modèle OSI ou l'architecture de communication en couches

Chapitre N°03 - TCP IP

N°04 - Les trames Ethernet

Exercice N°1 Quizz *

Exercice N°2 Question de cours *

1. De quelle couche du modèle TCP/IP fait parti le protocole IP ? Quel est son rôle ?

Couche 3, permettre un service d'adressage unique pour l'ensemble des terminaux connectés.

2. Comment le protocole IP détermine-t-il le destinataire ?

grâce à 3 champs :
- Le champ adresse IP : adresse de la machine
- Le champ masque de sous-réseau : détermine la partie de l'@ IP qui concerne le réseau
- Le champ passerelle par défaut : détermine la machine à remettre le datagramme

3. Dans quoi est encapsulé un paquet IP ?

Segment TCP

4. Quelle est la taille de l'en-tête d'un paquet IP ?

20 octets

5. Quelle est la particularité du champ IHL ?

la taille maximum de l'entête IP est de 15 x 32bits/8 = 60 octets

6. Quel est le rôle du champ "LEN" ?

représente la longueur du paquet incluant l'entête IP et les Data en octets

7. Quel est le rôle du champ "TTL" ?

éviter de faire circuler des trames en boucle infinie.

8. Quel est le rôle du champ "PROTOCOL" ?

représente le type de données (TCP, UPD, ...)

Exercice N°1 Trame HTML **

```
0000 00 12 17 41 c2 c7 00 1a  73 24 44 89 08 00 45 00 ..A.... s$D...E.
0010 01 bb da c2 40 00 3c 06  fc 9d d5 e4 00 2a 3e 93 ....@.<......*>.
0020 51 3b 00 50 04 85 87 c7  14 d5 00 12 b0 cb 50 19 Q;.P..........P.
0030 19 20 95 45 00 00 3e 20  0a 3c 74 64 20 77 69 64 . .E..> .<td wid
0040 74 86 3d 22 33 30 25 22  20 20 68 65 69 67 68 74 th="30%" height
```

Q.1 Entourer en rouge, les octets composant la trame Ethernet.

Q.2 Extraire :

l'adresse MAC SOURCE

L'adresse MAC Destination

Le contenu du champ type de protocole.

Q.3 En déduire le protocole encapsulé dans la trame. 08 00 (IPv4)

Q.4 Entourer en vert les octets composant le paquet IP contenu dans la trame Ethernet Extraire :

- La version du protocole
- La longueur de l'entête
- La valeur du champ TOS
- La longueur totale du datagramme IP
- L'identifiant affecté au datagramme
- La valeur des champs DF, MF et fragment offset. En déduire si datagramme est fragmenté.
- La valeur du champ TTL
- Le contenu du champ protocole. En déduire le protocole encapsulé dans le paquet IP.
- Les adresses IP source et destination.

Q.5 Quel est le problème avec la longueur totale du datagramme IP ?

Elle dépasse la taille maximale qui est de 66 octets

CORRECTION

```
0000 00 12 17 41 c2 c7 00 1a  73 24 44 89 08 00  ..A.... s$D...E.
45 00
0010 01 bb da c2 40 00 3c 06  fc 9d d5 e4 00 2a  ....@.<......*>.
3e 93
0020 51 3b 00 50 04 85 87 c7  14 d5 00 12 b0 cb  Q;.P.........P.
50 19
0030 19 20 95 45 00 00 3e 20  0a 3c 74 64 20 77  . .E..> .<td wid
69 64
0040 74 86 3d 22 33 30 25 22  20 20 68 65 69 67  th="30%" height
68 74
```

```
00 12 17 41 C2 C7 00 1A 73 24 44 89 08 00 45 00 01 BB DA C2 40 00 3C 06
FC 9D D5 E4 00 2A 3E 93 51 3B 00 50 04 85 87 C7 14 D5 00 12 B0 CB 50 19
19 20 95 45 00 00 3E 20 0A 3C 74 64 20 77 69 64 74 86 3D 22 33 30 25 22
20 20 68 65 69 67 68 74
```

- **Ethernet II**
  - **Destination: CiscoLinksys_41:c2:c7 (00:12:17:41:c2:c7)**
    - Address: CiscoLinksys_41:c2:c7 (00:12:17:41:c2:c7)
    - .... ..0. .... = LG bit: Globally unique address (factory default)

        - ....0 .... = IG bit: Individual address (unicast)
    - **Source: GemtekTechno_24:44:89 (00:1a:73:24:44:89)**
        - Address: GemtekTechno_24:44:89 (00:1a:73:24:44:89)
        - .... ..0. .... = LG bit: Globally unique address (factory default)
        - ....0 .... = IG bit: Individual address (unicast)
    - Type: IPv4 (0x0800)
- **Internet Protocol Version 4**
    - 0100 .... = Version: 4
    - .... 0101 = Header Length: 20 bytes (5)
    - **Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)**
        - 0000 00.. = Differentiated Services Codepoint: Default (0)
        - .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    - **Total Length: 443**
        - **Expert Info (Error/Protocol): IPv4 total length exceeds packet length (66 bytes)**
            - IPv4 total length exceeds packet length (66 bytes)
            - Severity level: Error
            - Group: Protocol
    - Identification: 0xdac2 (56002)
    - **010. .... = Flags: 0x2, Don't fragment**
        - 0... .... = Reserved bit: Not set
        - .1.. .... = Don't fragment: Set
        - ..0. .... = More fragments: Not set
    - ...0 0000 0000 0000 = Fragment Offset: 0
    - Time to Live: 60
    - Protocol: TCP (6)
    - Header Checksum: 0xfc9d
    - Header checksum status: Unverified
    - Source Address: 213.228.0.42
    - Destination Address: 62.147.81.59
- **Transmission Control Protocol**
    - Source Port: 80
    - Destination Port: 1157
    - Stream index: 0
    - **Conversation completeness: Incomplete (0)**
        - ..0. .... = RST: Absent
        - ...0 .... = FIN: Absent
        - .... 0... = Data: Absent
        - .... .0.. = ACK: Absent
        - .... ..0. = SYN-ACK: Absent

        - ....0 = SYN: Absent
        - Completeness Flags: [Null]
    - TCP Segment Len: 26
    - Sequence Number: 0x87c714d5
    - Sequence Number (raw): 2277971157
    - Next Sequence Number: 28
    - Acknowledgment Number: 0x0012b0cb
    - Acknowledgment number (raw): 1224907
    - 0101 .... = Header Length: 20 bytes (5)
    - **Flags: 0x019 (FIN, PSH, ACK)**
        - 000. .... = Reserved: Not set
        - ...0 .... = Accurate ECN: Not set
        - .... 0... .... = Congestion Window Reduced: Not set
        - .... .0.. .... = ECN-Echo: Not set
        - .... ..0. .... = Urgent: Not set
        - ....1 .... = Acknowledgment: Set
        - .... 1... = Push: Set
        - .... .0.. = Reset: Not set
        - ....0. = Syn: Not set
        - **.... ....1 = Fin: Set**
            - **Expert Info (Chat/Sequence): Connection finish (FIN)**
                - Connection finish (FIN)
                - Severity level: Chat
                - Group: Sequence
        - **TCP Flags: ·····AP··F**
            - **Expert Info (Note/Sequence): This frame initiates the connection closing**
                - This frame initiates the connection closing
                - Severity level: Note
                - Group: Sequence
    - Window: 6432
    - Calculated window size: 6432
    - Window size scaling factor: -1 (unknown)
    - Checksum: 0x9545
    - Checksum Status: Unverified
    - Urgent Pointer: 0
    - **Timestamps**
        - Time since first frame in this TCP stream: 0.000000000 seconds
        - Time since previous frame in this TCP stream: 0.000000000 seconds
    - **SEQ/ACK analysis**
        - Bytes in flight: 26
        - Bytes sent since last PSH flag: 26
    - TCP payload (26 bytes)

Exercice N°2 Trame abcde

```
0000  00 1a 73 24 44 89 00 12  17 41 c2 c7 08 00 45 00      ..s$D...
.A....E.
0010  00 3c 00 29 00 00 96 01  a0 dd c0 a8 01 01 c0 a8      .<.)....
........
0020  01 69 00 00 55 56 00 01  00 05 61 62 63 64 65 66      .i..UV..
..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76      ghijklmn
opqrstuv
```

Q.1 Entourer en bleu, les octets correspondant au message ICMP encapsulé dans le datagramme IP.

Q.6 Extraire:

La valeur du champ type et du champ code.

Q.7 En déduire la nature du message ICMP.

Q.8 Le contenu du champ de donnée du message ICMP.

```
00 1A 73 24 44 89 00 12 17 41 C2 C7 08 00 45 00 00 3C 00 29 00 00 96 01
A0 DD C0 A8 01 01 C0 A8 01 69 00 00 55 56 00 01 00 05 61 62 63 64 65 66
67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76
```

- **Frame 1: 64 bytes on wire (512 bits)**
- **Ethernet II**
- **Internet Protocol Version 4**
- **Internet Control Message Protocol**
  - Type: 0 (Echo (ping) reply)
  - Code: 0
  - **Checksum: 0x5556 incorrect, should be 0x6251**
  - Checksum Status: Bad
  - Identifier (BE): 1 (0x0001)
  - Identifier (LE): 256 (0x0100)
  - Sequence Number (BE): 5 (0x0005)
  - Sequence Number (LE): 1280 (0x0500)
  - **Data ????**
    - Data: 61626364656667686 96a6b6c6d6e6f70717273747576
    - Length: 22
  -

Exercice N°3 Trame 00 00 C0

```
Length : 64 byte
```

Analyse de l'en-tête Ethern

Q.1 Remplir le tableau suivant

Champ	Valeur en Hexa	Description
Adresse Destination		

Adresse Source		
EtherType		

Analyse de l'en-tête IP

Q.2 Remplir le tableau suivant

Champ	Hexa	Description
Version 4 bits		
Longueur d'en-tête 4 bits		
Type de service		
Longueur totale		En décimale =
Total de contrôle		
@IP source		En décimale pointé =
@IP Destination		En décimale pointé =

Analyse de l'en-tête TCP

Q.3 Remplir le tableau suivant

Champ	Hexa	Description
Port source		En décimale =
Port destinataire		En décimale =
N° de la séquence		
N° seq acquitté		
Longueur d'en-tête (4 bits)		
Reserved (3 bits)		
Drapeau(9 bits)		
Fenêtre		
Total de contrôle		
Pointeur data URG		

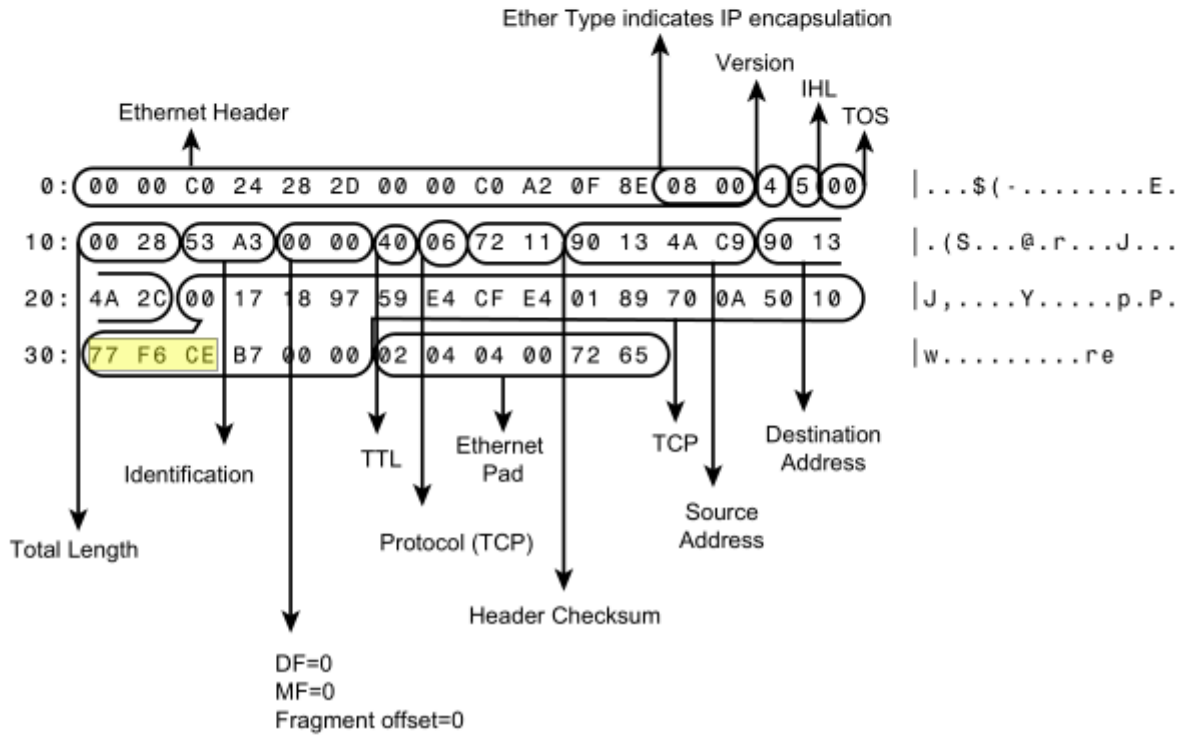
Données :

Q.4 Indiquez les données de la trame

CORRECTION

Length : 64 byte

```
Packet Number : 7           6:38:38 PM
Length : 64 bytes
ether: ==================== Ethernet Datalink Layer ====================
       Station: 00-00-C0-A2-0F-8E ----> 00-00-C0-24-28-2D
       Type: 0x0800 (IP)
  ip: ====================== Internet Protocol ======================
       Station:144.19.74.201 ---->144.19.74.44
       Protocol: TCP
       Version: 4
       Header Length (32 bit words): 5
       Precedence: Routine
              Normal Delay, Normal Throughput, Normal Reliability
       Total length: 40
       Identification: 21411
       Fragmentation allowed, Last fragment
       Fragment Offset: 0
       Time to Live: 64  seconds
       Checksum: 0x7211(Valid)
 tcp: ================= Transmission Control Protocol ================
       Source Port: TELNET
       Destination Port: 6295
       Sequence Number: 1508167652
       Acknowledgement Number: 25784330
       Data Offset (32-bit words): 5
       Window: 30710
       Control Bits: Acknowledgement Field is Valid (ACK)
       Checksum: 0xCEB7(Valid)
       Urgent Pointer: 0
```



La longueur est de 64 octets ce qui correspond au minimum

- L'analyseur nous indique que la trame a une longueur de 64 octets, ce qui correspond à la longueur minimale d'une trame MAC Ethernet.
- Quand les données ont une longueur inférieure, il y a un bourrage (bit-stuffing) qui consiste à ramener octets la longueur du champ de données à 46 octets.

- Trame Ethernet = 6 octets @MAC destination + 6 octets @MAC source + 2 octets EtherType + 4 octets FCS = **18 octets**
- Longueur total du Datagramme IP 0x28 = 40
- **Total Ethernet + ip = 18 + 40 = 58 octets, il en manque 64-58 = 6 octets !!!**

Exercice N°4 Trame 00 0c 29

```
00 0c 29 65 20 48 00 0c  29 a6 7d b4 08 00
00 34 83 63 40 00 80 06  00 00 c0 a8 64 65
64 78 d0 a1 00 50 3b 65  37 d4 00 00 00 00
fa f0 4a 55 00 00 02 04  05 b4 01 03 03 08
04 02
```

Q.1 Complétez le texte suivant avec les valeurs qui conviennent. Le format demandé est repéré hex pour hexadécimal et dec pour décimale. Par exemple le TTL est demandé en décimal (il faut donc convertir) et le type de protocole en hexadécimal (pas de conversion)

Dans l'entête Ethernet :

L'adresse MAC source est _____ (hex) et celle de destination est _____(hex)

Le type de protocole est_____ __(hex) qui a comme numéro le _____(hex)

Dans l'entête IP :

La taille est de _____(dec)

Le TTL est de _____(dec)

@ source est _____ (dec pointé) et celle de destination est _____(dec pointé)

Le protocole encapsulé est ICMP – TCP (entourez la bonne réponse)

Si vous avez repéré que c'est TCP qui est encaspulé :

Le port source est le _____ (dec) et celui de destination le _____ (dec).

Le drapeau SYN est à _____ et ACK est à _____. Le numéro de séquence est ____(dec).

Si vous pensez que c'est ICMP :

Le type est le numéro _____ (dec) et le code est _____ (dec)

CORRECTION

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{CFE53DB0-8204-43CB-9A8F-03DB252CAFE4}, id 0
v Ethernet II, Src: VMware_a6:7d:b4 (00:0c:29:a6:7d:b4), Dst: VMware_65:20:48 (00:0c:29:65:20:48)
  > Destination: VMware_65:20:48 (00:0c:29:65:20:48)
  > Source: VMware_a6:7d:b4 (00:0c:29:a6:7d:b4)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.100.101, Dst: 192.168.100.120
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x8363 (33635)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.100.101
    Destination Address: 192.168.100.120
v Transmission Control Protocol, Src Port: 53409, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 53409
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 996489172
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x4a55 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  > [Timestamps]
```

Exercice N°1 Évaluation 2017

Q.1 Pour ces trois trames :

Donnez :

Q.2 Les adresses MAC source et destination

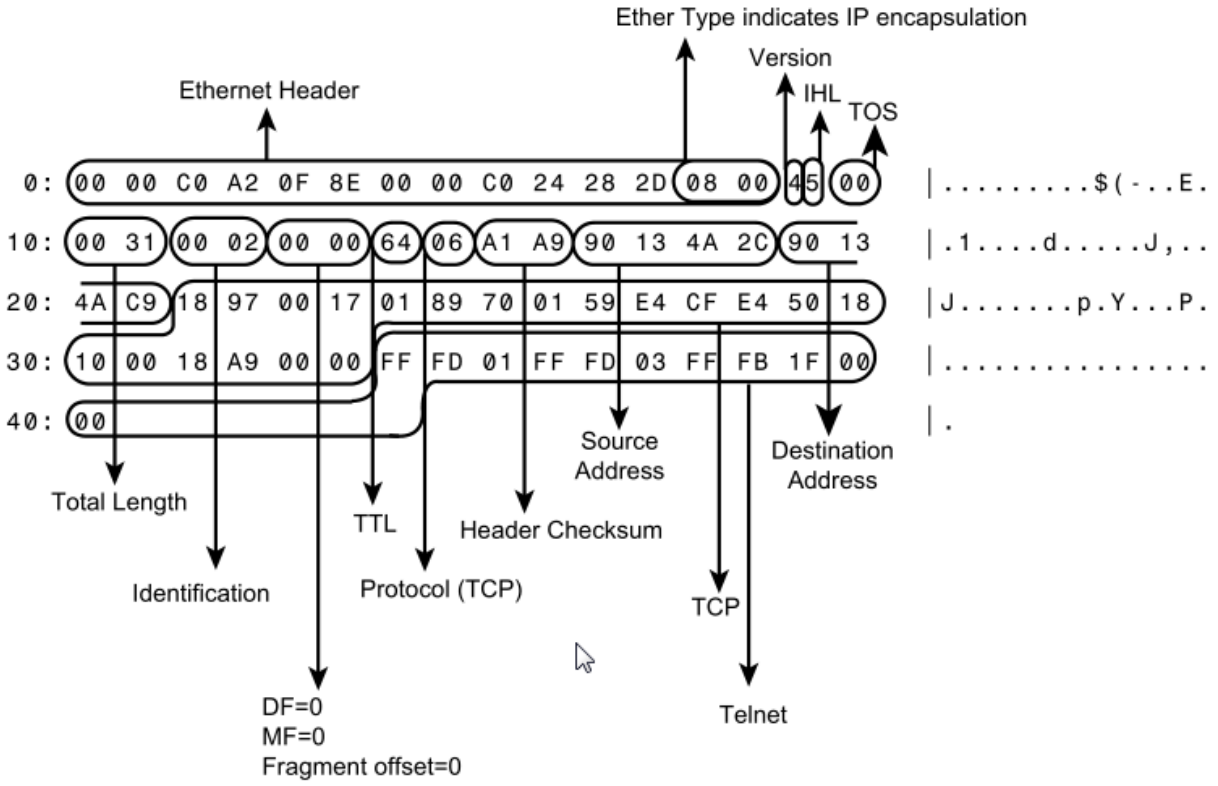
Q.3 Le protocole de niveau 3 encapsulé dans Ethernet

Q.4 Les adresses IP source et destination

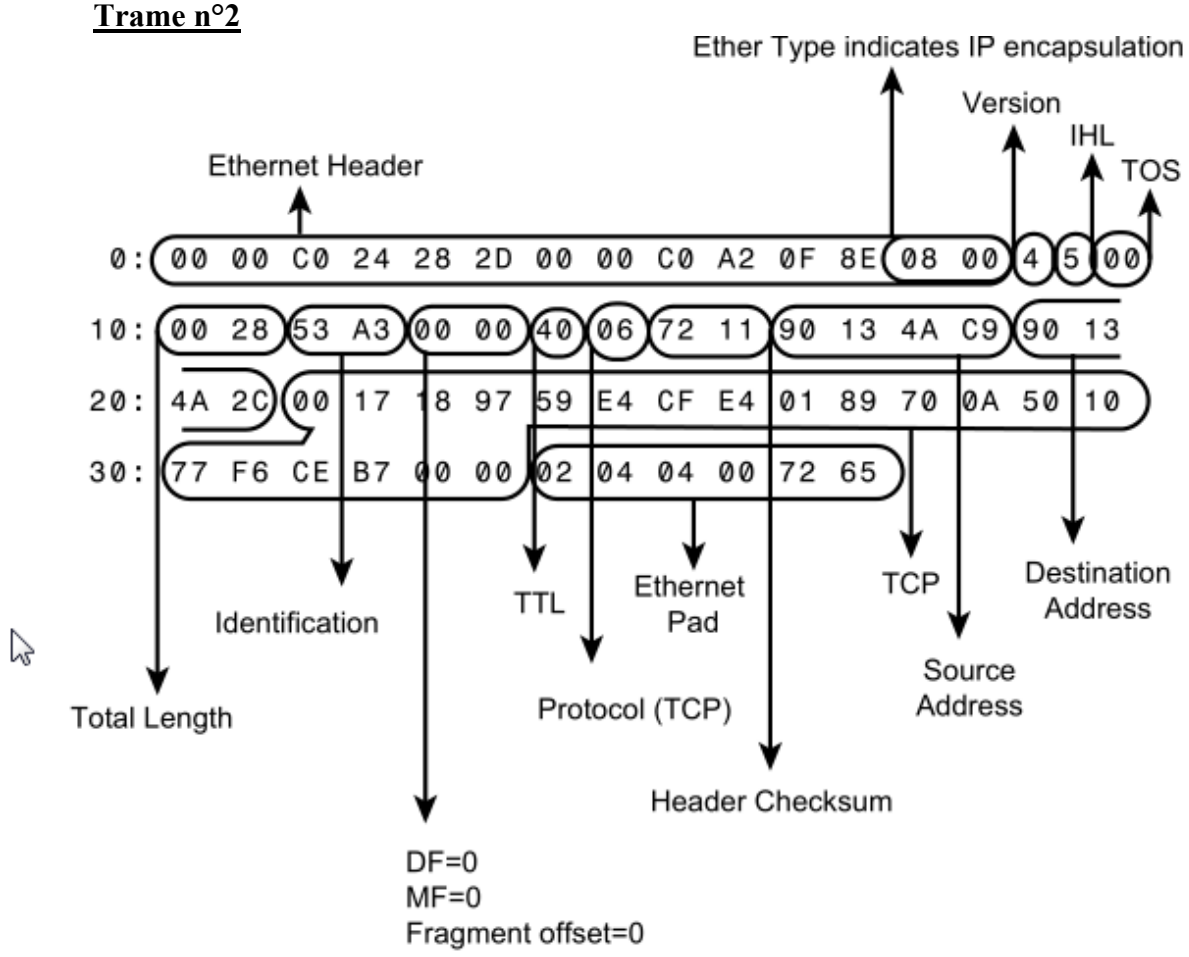
Q.5 Le nom du protocole niveau 4

Q.6 Port source et destination ainsi que leurs signification (c.f. lien moodle)

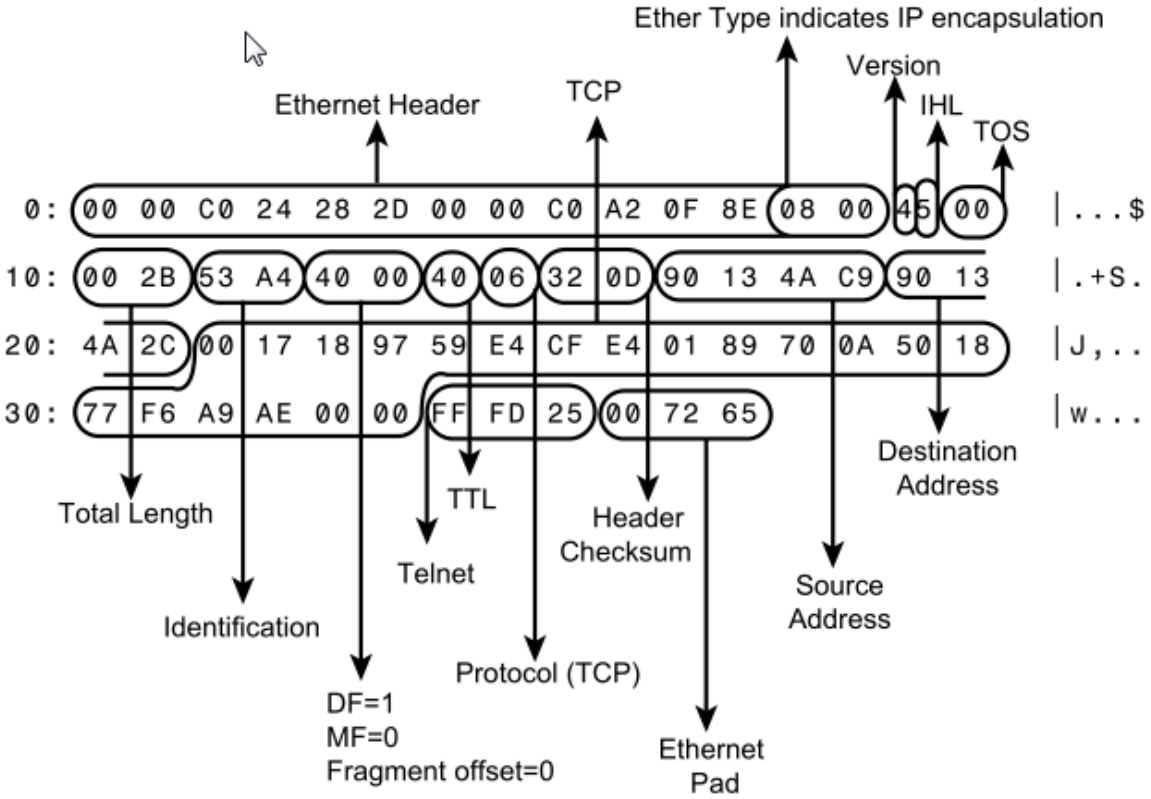
Trame n°1


Ether Type indicates IP encapsulation
Version
IHL
TOS
Ethernet Header
0: 00 00 C0 A2 0F 8E 00 00 C0 24 28 2D 08 00 45 00 |.....$(-..E.
10: 00 31 00 02 00 00 64 06 A1 A9 90 13 4A 2C 90 13 |.1....d.....J,..
20: 4A C9 18 97 00 17 01 89 70 01 59 E4 CF E4 50 18 |J.......p.Y...P.
30: 10 00 18 A9 00 00 FF FD 01 FF FD 03 FF FB 1F 00 |................
40: 00 |.
Source Address
Destination Address
Total Length
TTL
Header Checksum
Identification
Protocol (TCP)
TCP
DF=0
MF=0
Fragment offset=0
Telnet

Trame n°2


Ether Type indicates IP encapsulation
Version
IHL
TOS
Ethernet Header
0: 00 00 C0 24 28 2D 00 00 C0 A2 0F 8E 08 00 45 00
10: 00 28 53 A3 00 00 40 06 72 11 90 13 4A C9 90 13
20: 4A 2C 00 17 18 97 59 E4 CF E4 01 89 70 0A 50 10
30: 77 F6 CE B7 00 00 02 04 04 00 72 65
Identification
TTL
Ethernet Pad
TCP
Destination Address
Source Address
Total Length
Protocol (TCP)
Header Checksum
DF=0
MF=0
Fragment offset=0

Trame n°3



Exercice N°2 Trame ff ff ff

```
0000  ff ff ff ff ff ff 00 15  5d f2 d9 03 08 06 00 01
0010  08 00 06 04 00 01 00 15  5d f2 d9 03 ac 10 00 c9
0020  00 00 00 00 00 00 ac 10  03 6f 00 00 00 00 00 00
0030  00 00 00 00 00 00 00 00  00 00 00 00
```

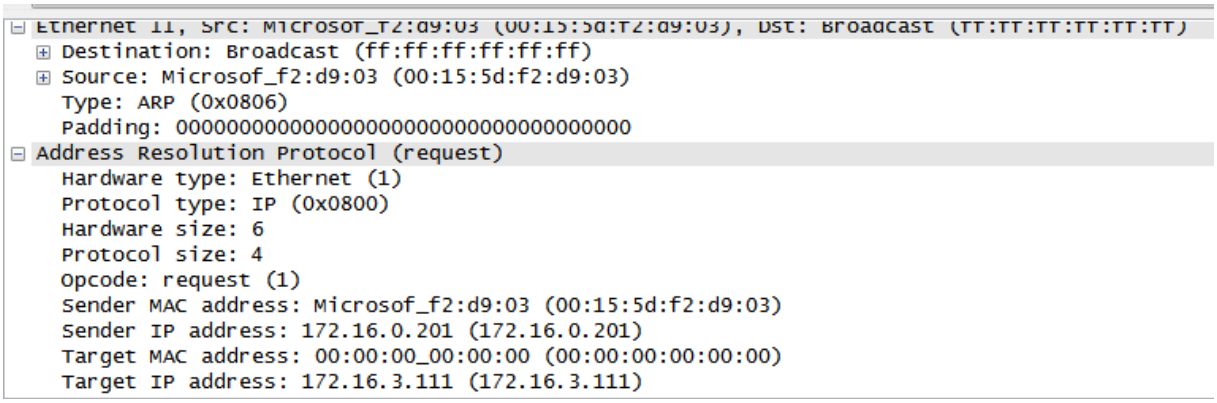
Q.1 Donnez :

Les adresses MAC source et destination

Le protocole de niveau 3 encapsulé dans Ethernet

Les adresses IP source et destination

Le type de la trame



Chapitre N°05 - Les protocoles de niveau 3 Réseaux

Exercice N°1 Quizz ARP

- Qu'est-ce que l'acronyme ICMP signifie ?
  - Réponse: ICMP signifie "Internet Control Message Protocol".
- Quel est le rôle principal du protocole ICMP ?
  - Réponse: ICMP est principalement utilisé pour gérer les messages d'erreur et de contrôle du trafic IP.
- Quel est le code associé au message ICMP "écho demande" (ping) ?
  - Réponse: Le code associé est 8.
- Quel est le code associé au message ICMP "écho réponse" (pong) ?
  - Réponse: Le code associé est 0.
- Quel est le message ICMP utilisé pour indiquer qu'un paquet a été abandonné car sa durée de vie (TTL) a expiré ?

  Réponse: Le message ICMP utilisé est "Time Exceeded".

Exercice N°2 Quizz ICMP

- Qu'est-ce que l'acronyme ICMP signifie ?
  - Réponse: ICMP signifie "Internet Control Message Protocol".
- Quel est le rôle principal du protocole ICMP ?
  - Réponse: ICMP est principalement utilisé pour gérer les messages d'erreur et de contrôle du trafic IP.
- Quel est le code associé au message ICMP "écho demande" (ping) ?
  - Réponse: Le code associé est 8.
- Quel est le code associé au message ICMP "écho réponse" (pong) ?
  - Réponse: Le code associé est 0.
- Quel est le message ICMP utilisé pour indiquer qu'un paquet a été abandonné car sa durée de vie (TTL) a expiré ?

  Réponse: Le message ICMP utilisé est "Time Exceeded".

Exercice N°3 Quizz IP

- Qu'est-ce que l'acronyme IP signifie ?
  - Réponse: IP signifie "Internet Protocol".

- Quel est le numéro de version actuel du protocole IP ?
- Réponse: La version actuelle est IPv4.

- Quelle est la taille d'une adresse IP en IPv4 ?
- Réponse: Une adresse IPv4 est composée de 32 bits.

- Quel est le rôle du protocole ARP ?
- Réponse: ARP (Address Resolution Protocol) permet de faire correspondre une adresse IP à une adresse MAC.

- Quel est le rôle du protocole ICMP ?
- Réponse: ICMP (Internet Control Message Protocol) permet de gérer les messages d'erreur et de contrôle du trafic IP.

- Quel est le rôle du protocole DHCP ?
- Réponse: DHCP (Dynamic Host Configuration Protocol) permet d'assigner automatiquement des adresses IP à des ordinateurs sur un réseau.

- Qu'est-ce que la fragmentation IP ?

Réponse: La fragmentation IP est un mécanisme qui permet de diviser un paquet IP en plusieurs morceaux pour faciliter sa transmission sur des réseaux qui imposent des restrictions de taille maximale des paquets.

Exercice N°4 Ping et ICMP *

1. Que mesure la commande ping ?
2. Suite à l'envoi d'une commande Ping, un message ICMP portant le numéro de type 11 est retourné. Ce message signale qu'un paquet IP, transportant la demande d'écho ICMP, a atteint sa limite de vie, également appelée TTL (Time To Live). Que peut-on en déduire ?
3. Si l'on est sûr de l'adresse IP du correspondant mais que le message de retour soit un message ICMP avec Destinataire inaccessible, que peut-on en déduire ?
4. En règle générale, la commande Ping ne génère pas une seule commande d'écho mais plusieurs, quelle en est la raison ?
5. Si la valeur initiale du TTL d'une trame ICMP est de 64 et qu'elle traverse 4 routeurs, quelle sera la valeur de ce champ à l'arrivée ?

1. **Que mesure la commande ping ?**
   La commande ping mesure le temps aller-retour (Round Trip Time - RTT) d'un

paquet envoyé à un hôte distant pour recevoir une réponse d'écho ICMP. Cela vérifie la connectivité et mesure la latence de la connexion.

2. **Suite à l'envoi d'une commande Ping, un message ICMP portant le numéro de type 3 est retourné. Ce message signale qu'un paquet IP, transportant la demande d'écho ICMP, a atteint sa limite de vie, également appelée TTL (Time To Live). Que peut-on en déduire ?**
   En réalité, le message ICMP de type 3 signifie "Destination Unreachable". Si le message ICMP reçu était plutôt de type 11, cela signifierait que le paquet a atteint sa limite de vie (TTL expiré). Si vous recevez un type 3 en réponse à un ping, cela signifie généralement que la destination est inaccessible pour diverses raisons (réseau non joignable, hôte non joignable, port non joignable, etc.).

3. **Si l'on est sûr de l'adresse IP du correspondant mais que le message de retour soit un message ICMP avec Destinataire inaccessible, que peut-on en déduire ?**
   Cela peut indiquer plusieurs problèmes, comme un pare-feu bloquant les paquets ICMP, un problème de routage, ou que l'hôte de destination est hors ligne. Cela signifie que le paquet a été correctement transmis à travers le réseau, mais quelque chose empêche la connexion au destinataire final.

4. **En règle générale, la commande Ping ne génère pas une seule commande d'écho mais plusieurs, quelle en est la raison ?**
   La commande ping envoie plusieurs requêtes pour fournir un résultat de test plus fiable. Cela permet de vérifier la constance de la connectivité et de calculer une moyenne ou une statistique sur la qualité de la connexion, comme la perte de paquets et la latence moyenne.

5. **Si la valeur initiale du TTL d'une trame ICMP est de 64 et qu'elle traverse 4 routeurs, quelle sera la valeur de ce champ à l'arrivée ?**
   Le TTL est décrémenté de 1 par chaque routeur que le paquet traverse. Si la valeur initiale est de 64 et que le paquet traverse 4 routeurs, la valeur du TTL à l'arrivée sera de 60.

Exercice N°5 Analyse de ping et de tracert *

La réponse à un ping est la suivante :

```
64 bytes from 192.93.28.7. icmp_seq=0 ttl=255 time =0.7 ms
1 packet transmitted, 1 packet received, 0 % packet loss
round-trip (ms) min/avg/max = 0.7/0.7/0.7
```

Q.1 Est-ce que la machine est accessible ?

Q.2 Combien a-t-on traversé de routeur ?

Ttl = 255 donc aucun

Vous avez lancé un tracert, voici la réponse :

1	193.51.91.1	1 ms	1 ms	1 ms
2	2.0.0.1	23 ms	23 ms	23 ms
3	11.6.1.1	105 ms	35 ms	35 ms
4	11.6.13.1	37 ms	35 ms	34 ms
5	189.52.80.1	37 ms	60 ms	36 ms
6	193.48.58.41	51 ms	39 ms	46 ms
7	193.48.53.49	39 ms	47 ms	44 ms
8	193.220.180.9	44 ms	*	*
9	195.48.58.43	48 ms	38 ms	44 ms
10	195.48.58.50	145 ms	170 ms	64 ms
11	194.206.207.18	61 ms	146 ms	44 ms
12	194.207.206.5	166 ms	261 ms	189 ms

Questions :

Q.3 Pourquoi le délai est-il au plus égal à 1 milliseconde pour la première ligne ?

Q.4 Que peuvent signifier les * ?

Q.5 Comment expliquez-vous que pour la même destination les délais varient ?

Q.6 Combien de réseaux différents ont été traversés ?

La première ligne correspond au réseau local dans lequel se trouve l'utilisateur, le premier
datagramme avec une durée de vie 1 a été détruit par le routeur de sortie du réseau. Il est
donc normal que le délai soit très faible.

Les étoiles correspondent à des datagrammes qui se sont perdus, à l'aller ou au retour :
au-delà d'un certain délai, on les considère comme manquants.

Les délais varient car rien n'est garanti dans l'interconnexion de réseaux : il peut y avoir
des « embouteillages » momentanés et/ou des pannes qui provoquent des changements de
route.

Pour connaître le nombre de réseaux traversés, il suffit de calculer l'adresse réseau de cha-
que routeur et de compter le nombre de réseaux différents. Il y en a 10, comme le montre
le tableau 6.5.
193.51.91.1 193.51.91.0 (réseau 1)
2.0.0.1 2.0.0.0 (réseau 2)
11.6.1.1 11.0.0.0 (réseau 3)
11.6.13.1 11.0.0.0 (réseau 3)
189.52.80.1 189.52.0.0 (réseau 4)
193.48.58.41 193.48.58.0 (réseau 5)
193.48.53.49 193.48.53.0 (réseau 6)
193.220.180.9 193.220.180.0 (réseau 7)
195.48.58.43 195.48.58.0 (réseau 8)
195.48.58.50 195.48.58.0 (réseau 8)
194.206.207.18 194.206.207.0 (réseau 9)
194.207.206.5 194.207.206.5 (réseau 10)

On ne peut pas connaître les protocoles utilisés au-delà de IP.

Exercice N°6 Un datagramme IP peut être segmenté en plusieurs fragments. *

Questions

1. Quels éléments indiquent qu'un datagramme est fragmenté et comment reconnaît-on spécifiquement le dernier fragment ?
2. Dans quel(s) fragment(s) le champ "Fragment Offset" (Déplacement de fragment) est-il différent de zéro ?
3. Comment un datagramme fragmenté est-il réassemblé une fois arrivé à destination ?
4. Lorsqu'un routeur reçoit deux fragments ayant les mêmes adresses source et destination ainsi que le même identifiant de fragmentation, comment distingue-t-il ces fragments pour éviter toute confusion ?

A Le bit MF (More Fragments) est à 1 dans tous les fragments sauf le dernier ;

le champ Déplacement n'est pas nul, sauf dans le premier fragment,

alors qu'un datagramme non fragmenté possède un bit MF à 0 et un champ Déplacement à 0.

B Tous les fragments portent le même identificateur (celui du datagramme initial). On utilise alors le champ Déplacement pour reconstituer le datagramme. Le bit MF est à 0 dans le dernier fragment, à 1 dans tous les autres.

C Un routeur ne peut pas confondre deux fragments qui auraient les mêmes élément ssource, destination et place de fragment, car le champ Identifiant du datagramme est forcément différent !

Exercice N°7 recherche de protocoles

Soit la trame suivante :

```
AA AA AA AA AA AA AA AB 08 00 02 4B 01 C3 08 00 02 4B 02 D6 08 00 45 00
00 50 20 61 00 00 80 01 C5 64 C7 F5 B4 0A C7 F5 B4 09 08 00 00 1C 01 02
03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A
1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32
33 34 35 36 37 38 5F A6 8C 04
```

Q.1 Quel est le protocole est porté par IP ?

AA AA AA AA AA AA AA AB -> Synchronisation
Protocole 10ème octets : Le 8 octets est TTL 80 puis le procole 01 ->ICMP

--- début d'une trame Ethernet ---
AA AA AA AA AA AA AA AB -> Synchronisation
08 00 02 4B 01 C3 -> @mac destinataire (constructeur = 080020)
08 00 02 4B 02 D6 -> @mac émetteur (même constructeur)
08 00 -> Type (ici IP). Si < à 1500 c'est une longueur
[ici 08 00 = 2048, cette valeur ne peut donc pas être la longueur des données de la trame] --- 46 <= contenu (ici datagramme IP)<= 1500 --- le contenu de cette trame est le « ping » de l'exercice précédent
---fin du contenu---
5F A6 8C 04 \ bloc de contrôle d'erreur Ethernet
Conclusion. Cette trame Ethernet a été capturée dans le réseau de classe C 199.245.180.0. Deux machines sont concernées par cet échange : la machine X d'adresse MAC 08 00 02 4B 02 D6 et d'adresse IP 199.245.180.10 a envoyé une requête d'écho (ping) à la machine Y d'adresse MAC 08 00 02 4B 01 C3 et d'adresse IP 199.245.180.9, située sur le même réseau local. Les cartes Ethernet sont du même constructeur. Les protocoles utilisés sont IP et ICMP.

Solution

----------Début d'une trame Ethernet ----------

AA AA AA AA AA AA AA AB → Synchronisation (préambule et début de trame).

08 00 20 0A 70 66 → adresse MAC destinataire (constructeur = 080020).

08 00 20 0A AC 96 → adresse MAC émetteur (carte de même constructeur).

08 00 → Type (ici IP) [si ce champ a une valeur inférieure à 1500, il s'agit d'une longueur].

------Début du contenu de la trame de longueur = 1 500 octets (ici datagramme IP) ------

4→ Version du protocole IP (IPv4).

5→ Longueur de l'en-tête (5*32 bits = 160 bits ou 5*4 octets = 20 octets).

00 00 28 A6 F5 0000 1A 06 75 94 C0 5D 02 01 84 E3 3D 05→ en tête IP.

- 00 : pas de qualité de service (ToS).
- 00 28 : Longueur totale (ici 00 28 en hexadécimal, soit : 2*16 + 8 en décimal donc 40 octets).
- A6 F5 : *ID* du datagramme (numéro quelconque, ne sert que si le datagramme est amené à être fragmenté).
- 0000 : Drapeau + Déplacement (0=inutl, 0=*DF* [fragmentation autorisée]) 0=*MF* (pas de fragments à suivre, donc dernier fragment). 0000000000000 = déplacement, c'est-à-dire position du 1er octet du fragment par rapport au 1er octet du datagramme initial. Ce fragment est le premier et le dernier du datagramme : il s'agit donc d'un datagramme non fragmenté.
- 1A : *TTL* (ici 1A = 1*16 + 10 = 26 routeurs ou secondes).
- 06 : Protocole (ici TCP).
- 75 94 : Bloc de contrôle d'erreur (sur l'en tête du datagramme seulement).
- C0 5D 02 01 : @ *IP* émetteur 192.92.2.1.
- 84 E3 3D 05 : @ *IP* destinataire 132.227.61.5.

Soit la trame suivante :TD_OLD

```
FF FF FF FF FF FF 00 04 80 5F 68 00 08 06 00 01
08 00 06 04 00 01 00 04 80 5F 68 00 89 C2 A2 03
00 00 00 00 00 00 89 C2 A2 F3 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00
```

Q.2 Quel est le protocole mise en œuvre ? Est-il porté par IP ?

la trame Ethernet II

@destination 6 octets	@source 6 octets	Protocole 2 octets	Données 1 à 1500 octets	Bourrage Si données <46 octets	FCS 4 octets

<----------
---------->
Taille minimale = 46 octets

C'est 08 06 ARP non pas supporté

Chapitre N°06 - Les protocoles de niveau 4 Transport

Exercice N°1 Quizz *

Exercice N°2 Trame frame ***

Soit la trame suivante :

```
+ FRAME : Base frame properties
+ ETHERNET : ETYPE = 0x0800 : Protocol = IP : DOD Internet Protocol
+ IP : ID = 0x8C11 ; Proto = TCP ; Len : 1496
+ TCP :. A…., len : 1456, seq : 23624030-23625485, ack : 8810360, win : 8385, src : 80 dst : 1125
HTTP : Response (to client using port 1125)
HTTP : Protocol Version = HTTP/1.0
HTTP : Status Code = OK
HTTP : Reason = OK
HTTP : Undocumented Header = Via : 1.0 PROXYA
HTTP : Undocumented Header Fieldname = Via
HTTP : Undocumented Header Value = 1.0 PROXYA
HTTP : Content-Type = text/html
HTTP : Date = Thu, 20 Jan 2010 09 : 27 : 08 GMT
HTTP : Server = Apache/1.3.9 (Unix)
HTTP : Data : Number of data bytes remaining = 1329 (0x0531)
```

Q.1 Quelle est la taille de la trame ? (Il n'y a pas d'options)

Q.2 Quels sont les ports sources et destination, à quoi correspond-ils ?

Q.3 Décrivez les différents champs de l'en-tête HTTP et leurs contenus

a) Justifier les valeurs des différents champs longueur pour les différentes couches.

a) 1 329 octets de données HTTP + 127 octets d'en-tête HTTP = 1 456 octets.

1 456 octets HTTP + 20 octets d'en-tête TCP + 20 octets d'en-tête IP = 1 496 octets.

b) À quoi correspondent les valeurs des ports source et destination ?

Le port source est égal à 80, il correspond au protocole HTTP, le port destination 1125 est un port client. Il s'agit donc d'une réponse d'un serveur web à un client

c) Commenter les différents champs de l'en-tête HTTP et leurs contenus

L'en-tête HTTP nous donne successivement : la version (HTTP 1.0), le code de réponse (OK), le nom du proxy (PROXYA), le type de contenu (text /html), la date et l'heure, le type du serveur web (Apache).

Q.4 Compléter le tableau suivant :

Éléments	Taille
Trame complète	
Entête Ethernet	
Datagramme IP	
Entête IP	
Trame TCP	
Entête TCP	
Trame HTTP	
Entête HTTP	
Données HTTP	

CORRECTION

- The **Entête Ethernet** (Ethernet header) size is 14 bytes in a typical Ethernet II frame.
- The **Entête IP** (IP header) size would typically be 20 bytes (without options).
- The **Entête TCP** (TCP header) size would typically be 20 bytes (without options).

Donc taille trame = `Len : 1496` de datagagramme IP +tailleEnteteEthernet = 14 = 1496+14 =1510
La tailleIP = 1496 donné
L'entête IP = 20 donc
la taille de TCP = tailleIP – EnteteIP=1496-20=1476 et non pas 1496

1496 c'est la taille du paylod
La taille de TCP n'est pas un champ de la trame TCP

La taille de http = tailleTCP-enteteteTCP = 1476-20 = 1456

La taille de la DATA donnée est de 1329
Donc taille entête = tailleHTTP – donnéesHTTP = 1456-1329 =127

Éléments	Taille	
Trame complète	1510	
Entête Ethernet	14	Par défaut
Datagramme IP	1496	Donnée
Entête IP	20	Par défaut
Trame TCP	~~1456~~ 1476	~~Donnée ERREUR~~ Taille entière
Entête TCP	20	Par défaut
Trame HTTP	1456	LEN de TP calculé
Entête HTTP	127	
Données HTTP	1329	donnée

Exercice N°3 TCP ** Exercice sur la Segmentation et l'Acquittement

Rappel

Dans le protocole TCP (Transmission Control Protocol), c'est chaque segment TCP qui est acquitté, et non le paquet TCP recomposé. Lorsque des données sont envoyées sur un réseau TCP, elles sont divisées en segments. Chaque segment est envoyé individuellement et peut être acquitté indépendamment des autres segments.

TCP est un protocole orienté connexion, ce qui signifie qu'avant qu'une communication de données ne commence, les deux extrémités établissent une connexion en utilisant le processus de synchronisation des numéros de séquence, communément appelé "three-way handshake". Une fois la connexion établie, les données peuvent être transmises.

Pour le contrôle de flux et la fiabilité, TCP utilise des accusés de réception (ACKs). Lorsqu'un segment arrive à destination, le destinataire envoie un ACK pour ce segment spécifique, indiquant que le segment a été reçu correctement. L'ACK contient le numéro de séquence du prochain segment attendu, ce qui permet au destinataire de signaler au sender quel est le premier octet de données qu'il attend de recevoir. Si un segment est perdu ou endommagé, il n'est pas acquitté par le destinataire, et après un délai, l'émetteur le renvoie.

Cette méthode permet de garantir l'intégrité des données et de s'assurer que tous les segments arrivent à destination dans l'ordre correct, permettant ainsi une reconstruction fiable et ordonnée des données originales.

Contexte :

Imaginez que vous êtes en charge de superviser une communication TCP entre deux machines, A (émetteur) et B (récepteur).
A souhaite envoyer un message de 4000 octets à B.
La taille maximale d'un segment que A peut envoyer est de 1000 octets.
Le processus de segmentation et d'acquittement s'effectue comme suit :

- Divisez le message en segments conformément à la taille maximale autorisée.
- Envoyez chaque segment de A vers B.
- Pour chaque segment reçu par B, B envoie un accusé de réception (ACK) à A.
- Si A ne reçoit pas un ACK pour un segment dans un délai déterminé, A doit renvoyer ce segment.

Questions :

Q.1 Combien de segments A doit-il créer pour envoyer le message complet ?
Q.2 Quel est le numéro de séquence initial si le premier octet du message est numéroté 1 ?
Q.3 Quels seront les numéros de séquence de chaque segment ?
Q.4 Comment B acquitte-t-il chaque segment reçu ? E. Si le troisième segment est perdu pendant la transmission, que se passe-t-il ?

Correction
A. A doit créer 4 segments, car 4000 octets / 1000 octets par segment = 4 segments.
B. Le numéro de séquence initial du premier segment est 1.
C. Les numéros de séquence de chaque segment sont :
Segment 1 : 1 - 1000
Segment 2 : 1001 - 2000
Segment 3 : 2001 - 3000
Segment 4 : 3001 - 4000
D. B acquitte chaque segment reçu en envoyant un ACK avec le numéro de séquence du prochain segment qu'il attend. Les ACKs seraient :
Pour le segment 1 : ACK 1001
Pour le segment 2 : ACK 2001
Pour le segment 3 : ACK 3001
Pour le segment 4 : ACK 4001
E. Si le troisième segment est perdu, B ne l'acquitte pas. A, après un délai sans recevoir d'ACK pour ce segment, renvoie le segment 3. B envoie ensuite un ACK 4001 après avoir reçu correctement le segment 3 retransmis.

Chapitre N°08 - L'adressage IPv4

1. Exercices Adresses IP

Exercice N°1 Quizz

Exercice N°2 Classes de réseaux

1. Déterminer, les ***classes de réseaux*** pour les hôtes d'adresses :

1.1. PC1 : **132.100.0.20**

132(d) = 1000 0100 l'adresse commence par 10 donc classe B

1.2. PC2 : **194.50.3.16**

194(d) = 1100 0010 l'adresse commence par 110 donc classe C

Exercice N°3 Adresses de diffusion et masque niveau *

2. Déterminer les ***adresses des réseaux*** ainsi que les adresses de diffusion (broadcast) pour les machines/hôtes suivants :

Vous utiliserez les masques par défaut et les règles suivantes :

IP & Masque => adresse réseau
IP OU inverse(Masque) => adresse de broadcast

2.1.PC1 : **132.10.3.9**

Réseau classe B, donc les 16 bits de poids forts correspondent à l'adresse réseau soit : 132.10.0.0
Adresse de broadcast : 132.10.255.255

2.2.PC2 : **10.2.7.1**

Réseau classe A, donc les 8 bits de poids forts correspondent à l'adresse réseau soit : 10.0.0.0
Adresse de broadcast : 10.255.255.255

2.3.PC3 : **192.168.5.10**

Réseau classe C, donc les 24 bits de poids forts correspondent à l'adresse réseau soit : 192.168.5.0
Adresse de broadcast : 192.168.5.255

2.4.PRINTER1 : **194.168.2.100**

Réseau classe C, donc les 24 bits de poids forts correspondent à l'adresse réseau soit : 192.168.2.0
Adresse de broadcast : 192.168.2.255

Exercice N°4 Réseau 192.168.1.0

On considère le réseau d'adresse **194.168.1.0**.

3.1. Déterminer, le masque par défaut et l'adresse de diffusion.

Réseau classe C, l'adresse hôtes est sur les 8 bits de poids faible donc le masque sera 255.255.255.0
L'adresse de diffusion sera 194.168.1.255

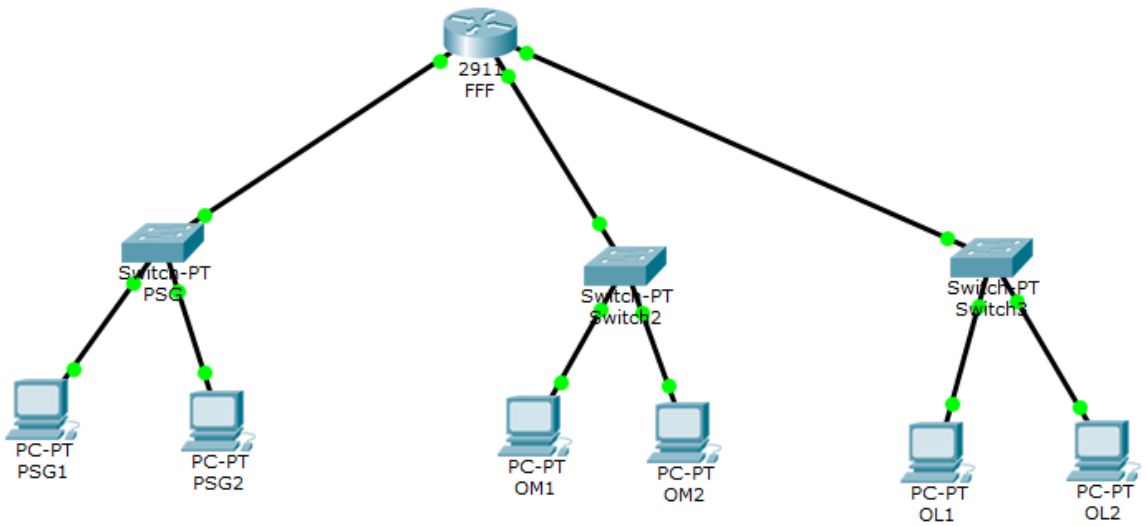
3.2. Quelle est la première adresse utilisable ? Et la dernière adresse ? Combien peut-on adresser de composants (équipements adressables) dans ce réseau ?

L'adresse la plus basse sera 194.168.1.1
L'adresse la plus haute sera 194.168.1.254
Sot un total de 254 adresses.

3.3. Soit une adresse avec n bits de host_id, donnez la formule permettant de connaitre le nombre maximal de machine sur un réseau en fonction de n ?

Exercice N°5 PSG OM et OL

C'est la période du mercato hivernal, le routeur de la fédération française de football doit permettre d'établir des communications entre les réseaux des différents clubs.
Nous allons étudier la configuration pour trois réseaux.



Les différents réseaux ont les besoins suivants :

- Le *Réseau* PSG: 250 hôtes, adresse réseau 100.100.100.0
- Le Réseau OM: 120 hôtes, adresse réseau 150.150.150.0.
- Le Réseau OL: 50 hôtes, adresse réseau 50.50.50.0.

Pour chaque réseau, proposez une configuration qui n'utilise pas plus d'adresses que nécessaire :

- Adresse du réseau :
- Masque de sous- réseau :
- Nombre d'hôtes maximum avec cette configuration :
- Nombre d'adresses perdues
- Adresse la plus basse des hôtes :
- Adresse la plus haute des hôtes :

```
Réseau PSG :
 Adresse du réseau : 100.100.100.0
Masque de sous- réseau : 255.255.255.0
Passerelle : 100.100.100.3
Nombre d'hôtes maximum avec cette configuration : 254
Adresse la plus basse des hôtes : 100.100.100.1
Adresse la plus haute des hôtes : 100.100.100.254

Réseau OM :
 Adresse du réseau : 150.150.150.0
Masque de sous- réseau : 255.255.255.128
Passerelle : 150.150.150.3
Nombre d'hôtes maximum avec cette configuration : 127
Adresse la plus basse des hôtes : 150.150.150.1
Adresse la plus haute des hôtes :  150.150.150.127


Réseau OL :
 Adresse du réseau : 50.50.50.0
Masque de sous- réseau : 255.255.255.192
Passerelle : 50.50.50.3
Nombre d'hôtes maximum avec cette configuration : 63
Adresse la plus basse des hôtes :50.50.50.1
Adresse la plus haute des hôtes : 50.50.50.63
```

```
Tester votre configuration avec Cisco Packet Tracer en connectant pour
chaque réseau deux hôtes configurés avec les adresses extrêmes du
réseau.
```

Exercice N°6 Box

Vous avez un box à votre domicile qui se trouve entre l'internet et votre réseau domestique. Une machine vous sert de site web personnel et son adresse est 192.168.1.111

Comment devez-vous configurer votre box pour que votre site web soit accessible de l'extérieur ?

Comment s'appelle cette fonctionnalité ?

a) Il est nécessaire de définir une règle de redirection de port sur le NAPT, redirigeant tous les paquets TCP reçus sur son port 80 vers la machine 192.168.0.110.
b) Ce procédé s'appelle redirection de port, Port Forwarding ou Port mapping.

2. Exercices Sous réseaux

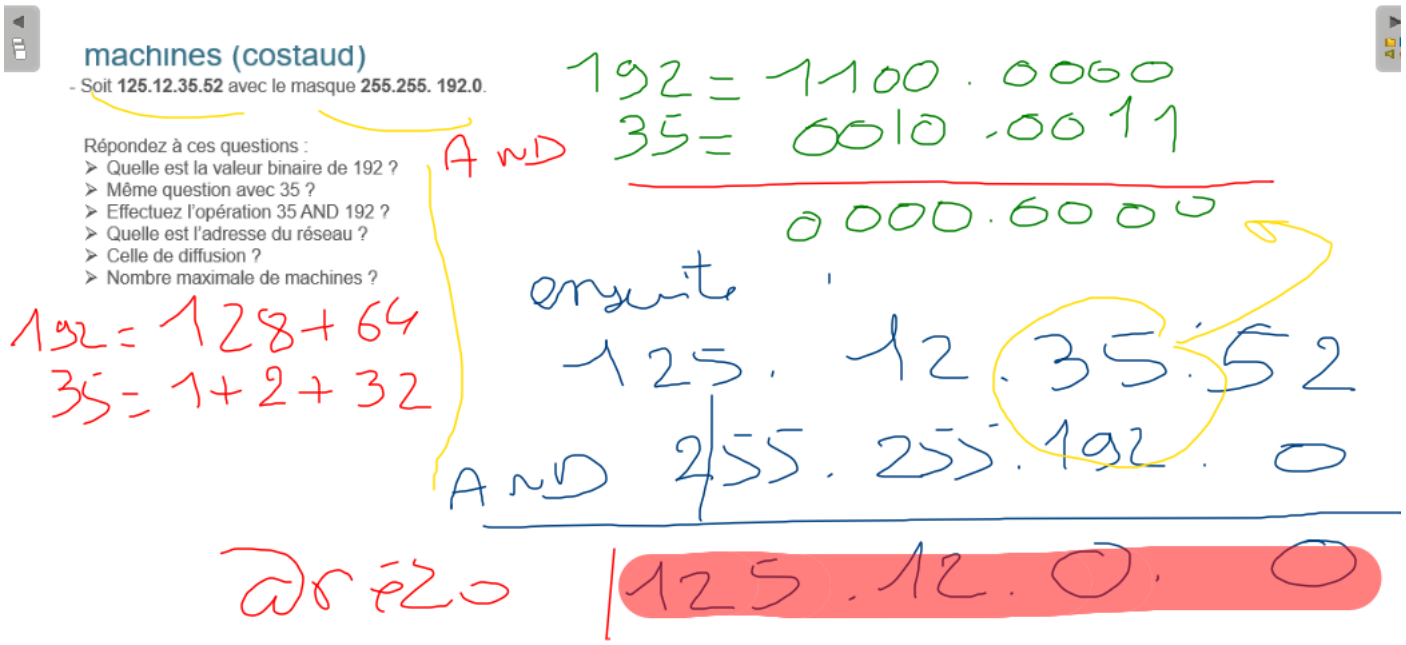
Exercice N°1 pas de sous-réseau

Soit l'adresse IP 125.12.35.52 avec le masque 255.255. 192.0

Quelle est l'adresse du sous-réseau ?

Même question avec celle de diffusion du sous-réseau

Correction




```
A REVOIR …….

192= 1100 0000 l'inverse est 0011 1111 = 63
125.12.35.52
OR         0.   .0.63.255
35 = 0010 0011
63 = 0011 1111
OR=0011 1111 = 63

@ de diff = 125.12.63.255
```

Exercice N°2 Réseau 194.44.77.

Une machine faisant partie d'un réseau local est reliée à l'internet et sa configuration est la suivant :

- Adresse IP: **192.44.77.7**
- Masque: **255.255.255.192**

1. Quelle est sa classe, l'adresse du réseau local et celle de diffusion ?
2. Quelle est l'adresse du sous-réseau dans lequel se trouve la station ? Quelle est l'adresse de diffusion associée ?
3. Combien de sous-réseaux sont utilisables dans ce réseau local ?
4. Combien peut-on déclarer de stations dans chacune des sous-réseaux ?
5. Quelles sont les adresses des sous-réseaux ?

1)

CLASSE C

192.44.77.0

192.44.77.255

2)

Adresse IP :
192.44.77.7= 1100 0000 . 0010 1100 . 0100 1101 . 0100 1111

Masque :
255.255.255.192= 1111 1111 . 1111 1111 . 1111 1111 . 1100 0000

1100 0000 . 0010 1100 . 0100 1101 . 0100 1111
AND 1111 1111 . 1111 1111 . 1111 1111 . 1100 0000
1100 0000. 1111 1111. 1111 11111. 0100 0000

Adr. sous réseau :
1100 0000 . 0010 1100 . 0100 1101 . 0100 0000
soit 192.44.77.64
Car les bits à 1 désignent la partie sous réseau de l'adresse,

Adresse de diffusion
1100 0000 . 0010 1100 . 0100 1101 . 0100 1111
OR 0000 0000 0000 0000 . 00000000 . 0011 1111
1100 0000 . 0010 1100 . 0100 1101. 0111 1111
192.44.77.127

3 Cmbien de sous-réseaux sont utilisables dans ce réseau local ?

Dans cet exemple de réseau de classe C, les 2 bits de poids fort des 8 bits disponibles (Host_id) sont utilisés pour identifier le sous réseau LE SUB-NET ID

Classe C -> nbr bits stations sur 8 bits.

Or 2 BITS SONT UTILIS2S POUR LES SOUS-RESEAU£Donc l'administrateur réso va pouvoir faire 11b=4 réso

4° Combien peut-on déclarer de stations dans chacune des sous-réseaux ?
Il reste 8-2 -> 6 bits dond 2^6-2=64-2=62
5° Quelles sont les adresses des sous-réseaux ?
d'@ 192.44.77.00 (00 + 6*0),
192.44.77.64(01+6*0)
,128(10+6*0)
,192(11+6*0)

Exercice N°3 Nombre de machines et de sous-réseaux

- Adresse IP: **192.44.77.7**

Q.1 L'entreprise désire un sous-reseau avec au plus 300 machines. Proposez un masque

Q.2 Elle change d'avis et veut maintenant 13 sous-réseaux. Proposez un nouvel masque

Exercice N°4 Avec masque 255.255.255.192

On considère le réseau d'adresse **194.168.1.0**.

3.1. Déterminer, le masque par défaut et l'adresse de diffusion.

```
Réseau classe C, l'adresse hôtes est sur les 8 bits de poids faible donc
le masque sera 255.255.255.0
L'adresse de diffusion sera 194.168.1.255
```

3.2. Combien peut-on adresser de composants (équipements adressables) dans ce réseau ?

```
L'adresse la plus basse sera 194.168.1.1
L'adresse la plus haute sera 194.168.1.254
Sot un total de 254 adresses.
```

3.3. L'administrateur décide d'utiliser le masque suivant : 255.255.255.**192** pour créer des sous-réseaux.

3.3.1-Combien peut-il en créer avec ce masque ?

```
192(d) = 1100 0000
On a deux bits pour créer des adresses de sous réseaux, donc quatre
sous-réseaux possibles.
```

3.3.2-Donner les adresses de ces sous-réseaux.

```
SR1 : 194.168.1.0
SR2 : 194.168.1.64
SR3 : 194.168.1.128
SR4 : 194.168.1.192
```

Note : au début il était interdit de prendre le premier et le dernier sous-réseau, ce n'est plus dorénavant le cas.

3.3.3-Déduire les adresses de diffusion.

```
SR1 : 194.168.1.63
SR2 : 194.168.1.127
SR3 : 194.168.1.192
SR4 : 194.168.1.255
```

3.3.4-A quel sous-réseau appartient l'imprimante d'adresse 194.168.1.**130** ?

Au sous-réseau 3.

3. Exercices CIDR

Exercice N°5 192.168.1.100/24 ?

Question 3-2 : quel est le **masque de sous-réseau** correspondant à l'adresse IP 192.168.1.100/24 ?
255.255.255.0

Le masque de sous-réseau correspondant à l'adresse IP 192.168.1.100/24 serait : 255.255.255.0

La notation CIDR indique combien de bit sont utilisés pour identifier le sous-réseau, dans cette adresse IP/24, 24 bits sont utilisés pour identifier le sous-réseau, donc le masque de sous-réseau est égal aux 24 bits les plus à gauche de l'adresse IP 255.255.255.255 en notation binaire, c'est : 11111111.11111111.11111111.00000000 qui correspond à 255.255.255.0 en notation décimale.

Exercice N°6 le masque 255.255.248.0

Pour ces questions, il faut obligatoirement mettre les étapes permettant d'arriver au résultat.

Question 3-1 : écrivez l'adresse IP **130.12.35.52** avec le masque **255.255.248.0** en notation CIDR.
130.12.35.52/22L'adresse IP complète est : 125.12.35.52/22
La notation CIDR (Classless Inter-Domain Routing) est utilisée pour spécifier une adresse IP et un masque de sous-réseau en utilisant un seul nombre après l'adresse IP séparé par un slash "/". Cela permet de spécifier le nombre de bits utilisés pour identifier le sous-réseau, plutôt que d'utiliser une notation décimale séparée pour le masque de sous-réseau.
Pour calculer la notation CIDR, vous devez convertir le masque de sous-réseau en binaire, compter le nombre de bits à 1 (les bits qui définissent le sous-réseau) et ajouter /devant cette valeur.
Le masque de sous-réseau 255.255.248.0 en binaire est :
11111111.11111111.11111000.00000000
Il y a 22 bits à 1, donc l'adresse IP 125.12.35.52 avec ce masque de sous-réseau en notation CIDR est: 125.12.35.52/22

Question 3-3 : quel est le **masque de sous-réseau** correspondant à l'adresse IP 192.168.1.50/28 ?

- L'adresse de réseau: Pour trouver l'adresse de réseau, il faut faire un ET logique entre l'adresse IP et le masque de sous-réseau. Pour l'adresse IP 192.168.10.12 avec le masque 255.255.255.0, l'adresse de réseau sera : 192.168.10.0
- L'adresse de diffusion: L'adresse de diffusion est l'adresse IP qui est utilisée pour transmettre les paquets à tous les hôtes d'un sous-réseau. Cette adresse est obtenue en changeant les bits de hôte de l'adresse de réseau à des 1. Pour l'adresse IP 192.168.10.12 avec le masque 255.255.255.0, l'adresse de diffusion sera : 192.168.10.255

- Le nombre de postes pour ce réseau : Le nombre de postes pour un réseau dépend du nombre de bits de hôte dans l'adresse IP, en utilisant le masque de sous-réseau. Dans ce cas, le masque de sous-réseau 255.255.255.0 indique qu'il y a 24 bits utilisés pour identifier le sous-réseau, et 8 bits restants pour identifier l'hôte. Ce qui donne 2^8 (256) postes disponibles dans ce réseau.

255. À I Want255.255.240

Exercice N°7 Cider Niv **

Pour ces questions, il faut obligatoirement mettre les étapes permettant d'arriver au résultat.

Question 3-1 : écrivez l'adresse IP **130.12.35.52** avec le masque **255.255.248.0** en notation CIDR.

130.12.35.52/22L'adresse IP complète est : 125.12.35.52/22

La notation CIDR (Classless Inter-Domain Routing) est utilisée pour spécifier une adresse IP et un masque de sous-réseau en utilisant un seul nombre après l'adresse IP séparé par un slash "/". Cela permet de spécifier le nombre de bits utilisés pour identifier le sous-réseau, plutôt que d'utiliser une notation décimale séparée pour le masque de sous-réseau.

Pour calculer la notation CIDR, vous devez convertir le masque de sous-réseau en binaire, compter le nombre de bits à 1 (les bits qui définissent le sous-réseau) et ajouter /devant cette valeur.

Le masque de sous-réseau 255.255.248.0 en binaire est : 11111111.11111111.11111000.00000000

Il y a 22 bits à 1, donc l'adresse IP 125.12.35.52 avec ce masque de sous-réseau en notation CIDR est: 125.12.35.52/22

Exercice N°8 Complétez ces tableaux

D'après https://www.editions-eni.fr/open/mediabook.aspx?idR=84e4bfc5a8bdc5eb50e482ac05a786b1

Masque décimal	Écriture CIDR
255.0.0.0	
255.255.255.0	
255.255.0.0	
255.240.0.0	
255.255.224.0	
255.255.255.248	
255.252.0.0	

Masque décimal	Écriture CIDR
255.0.0.0	**/8**
255.255.255.0	**/24**
255.255.0.0	**/16**
255.240.0.0	**/12 _->128+64(192)+ 32(224)+16(240)+8(248)+4(252)+2(254)**
255.255.224.0	**/19**
255.255.255.248	**/5+24=29**
255.252.0.0	**/6+8=14**

255.0.0.0 Écriture CIDR : **/8** Explication : Il y a 8 bits à 1 dans la partie réseau du masque (les 8 premiers bits).

255.255.255.0 Écriture CIDR : **/24** Explication : Il y a 24 bits à 1 dans la partie réseau du masque (les 24 premiers bits).

255.255.0.0 Écriture CIDR : **/16** Explication : Il y a 16 bits à 1 dans la partie réseau du masque (les 16 premiers bits).

255.240.0.0 Écriture CIDR : **/12** Explication : Il y a 12 bits à 1 dans la partie réseau du masque (les 8 premiers bits, plus les 4 premiers bits du deuxième octet).

255.255.224.0 Écriture CIDR : **/19** Explication : Il y a 19 bits à 1 dans la partie réseau du masque (les 16 premiers bits, plus les 3 premiers bits du troisième octet).

255.255.255.248 Écriture CIDR : **/29** Explication : Il y a 29 bits à 1 dans la partie réseau du masque (les 24 premiers bits, plus les 5 premiers bits du quatrième octet).

255.252.0.0 Écriture CIDR : **/14** Explication : Il y a 14 bits à 1 dans la partie réseau du masque (les 8 premiers bits, plus les 6 premiers bits du deuxième octet).

Écriture CIDR	Masque décimal
/9	
/13	
/30	
/17	
/21	
/23	
/10	

Écriture CIDR	Masque décimal
/9	255.128.0.0
/13	255.248.0.0.
/30	255.255.255.252
/17	255.254.0.0.
/21	255.248.0.0
/23	255.255.254.0
/10	255.192.0.0

- **128+64(192)+ 32(224)+16(240)+8(248)+4(252)+2(254**
- **/9** Le préfixe CIDR est /9, ce qui signifie que les 9 premiers bits du masque sont définis sur 1. En binaire, cela donne :

11111111.10000000.00000000.00000000. En notation décimale, cela équivaut à **255.128.0.0.**

-
- **/13** Le préfixe CIDR est /13, ce qui signifie que les 13 premiers bits du masque sont définis sur 1. En binaire, cela donne : 11111111.11110000.00000000.00000000. En notation décimale, cela équivaut à **255.248.0.0.**
-
- **/30** Le préfixe CIDR est /30, ce qui signifie que les 30 premiers bits du masque sont définis sur 1. En binaire, cela donne : 11111111.11111111.11111111.11111100. En notation décimale, cela équivaut à **255.255.255.252.**
-
- **/17** Le préfixe CIDR est /17, ce qui signifie que les 17 premiers bits du masque sont définis sur 1. En binaire, cela donne : 11111111.11111110.00000000.00000000. En notation décimale, cela équivaut à **255.254.0.0.**
-
- **/21** Le préfixe CIDR est /21, ce qui signifie que les 21 premiers bits du masque sont définis sur 1. En binaire, cela donne : 11111111.11111000.00000000.00000000. En notation décimale, cela équivaut à **255.248.0.0.**
-
- **/23** Le préfixe CIDR est /23, ce qui signifie que les 23 premiers bits du masque sont définis sur 1. En binaire, cela donne : 11111111.11111111.11111110.00000000. En notation décimale, cela équivaut à **255.255.254.0.**
-
- **/10** Le préfixe CIDR est /10, ce qui signifie que les 10 premiers bits du masque sont définis sur 1. En binaire, cela donne : 11111111.11000000.00000000.00000000. En notation décimale, cela équivaut à **255.192.0.0.**

Adresse	Masques	@rése	@diffusion	Nb d'@IP utilisable
131.108.78.235 /21	**255.255.248.0**	**131.108.72.0**	131.108.79.255	2^11 -2
63.69.48.211 /11				
168.94.197.13 /19				
200.249.145.227 /28				
192.154.88.133 /26				
100.189.64.38 /13				
150.34.222.131 /17				

- L'adresse de réseau (Masques) est calculée en appliquant l'opération AND logique entre l'adresse IP et le masque de sous-réseau.

- L'adresse de broadcast (@diffusion) est déterminée en appliquant l'opération OR logique entre l'adresse de réseau et l'inverse du masque de sous-réseau.
- Le nombre d'hôtes disponibles (Nbe d'@IP) est calculé avec la formule 2^(32−masque)−2

Adresse	Masques	@rése	@diffusion	Nbe d'@IP	Formule
131.108.78.235 /21	255.255.248.0	131.108.72.0	131.108.79.255	2046	(2^{11}-2)
63.69.48.211 /11	255.224.0.0	63.64.0.0	63.95.255.255	2097150	(2^{21}-2)
168.94.197.13 /19	255.255.224.0	168.94.192.0	168.94.223.255	8190	(2^{13}-2)
200.249.145.227 /28	255.255.255.240	200.249.145.224	200.249.145.239	14	(2^{4}-2)
192.154.88.133 /26	255.255.255.192	192.154.88.128	192.154.88.191	62	(2^{6}-2)
100.189.64.38 /13	255.248.0.0	100.184.0.0	100.191.255.255	524286	(2^{19}-2)
150.34.222.131 /17	255.255.128.0	150.34.128.0	150.34.255.255	32766	(2^{15}-2)

131.108.78.235/21 21 = 2*6+5
Masque de sous-réseau : **255.255.248.0** (car 21 bits sont utilisés pour le réseau)
78= **0100 1110**->64+8=72
248= **1111 1000**
AND = 0100 1000 = 8 + 64 =72

Adresse du réseau : **131.108.72.0**

Adresse diffusion
Le masque est
255.255.248.0
Son inverse
0.0. inverse de 1111 1000.255
0.0. 0000 0111.255

On fait un or avec l'adresse ip
78= **0100 1110**->64+8=72
inver248= **0000 0111**
or = 0100 1111.= 15+64 = 79

et 235 or 111.1111 = 255

(les 21 premiers bits de l'adresse IP sont conservés)
Adresse de diffusion : 131.108.79.255 (les 11 derniers bits sont remplacés par des 1)
Nombre d'adresses IP maximales : 2^(32-21) = 2^11 = 2048 adresses IP (dont 2046 adresses IP utilisables)
63.69.48.211/11 8+3
Masque de sous-réseau : 255.224.0.0 (car 11 bits sont utilisés pour le réseau)
69= 01000101 -> 64=

Adresse du réseau : 63.64.0.0 (les 11 premiers bits de l'adresse IP sont conservés)
Adresse de diffusion : 63.95.255.255 (les 21 derniers bits sont remplacés par des 1)
Nombre d'adresses IP maximales : 2^(32-11) = 2^21 = 2,097,152 adresses IP (dont 2,097,150 adresses IP utilisables)
168.94.197.13/19 2*6+3
Masque de sous-réseau : 255.255.224.0 (car 19 bits sont utilisés pour le réseau)
197= 11000101 -> 128+64 =192
Adresse du réseau : 168.94.192.0 (les 19 premiers bits de l'adresse IP sont conservés)
Adresse de diffusion : 168.94.223.255 (les 13 derniers bits sont remplacés par des 1)
Nombre d'adresses IP maximales : 2^(32-19) = 2^13 = 8,192 adresses IP (dont 8,190 adresses IP utilisables)
200.249.145.227/28 3*8+4
Masque de sous-réseau : 255.255.255.240 (car 28 bits sont utilisés pour le réseau)
227= 11100011 -> 128+62+32=224
Adresse du réseau : 200.249.145.224 (les 28 premiers bits de l'adresse IP sont conservés)
Adresse de diffusion : 200.249.145.239 (les 4 derniers bits sont remplacés par des 1)
Nombre d'adresses IP maximales : 2^(32-28) = 2^4 = 16 adresses IP (dont 14 adresses IP utilisables)
192.154.88.133/26 3*8+2
Masque de sous-réseau : 255.255.255.192 (car 26 bits sont utilisés pour le réseau)

Adresse du réseau : 192.154.88.128 (les 26 premiers bits de l'adresse IP sont conservés)
Adresse de diffusion : 192.154.88.191 (les 6 derniers bits sont remplacés par des 1)
Nombre d'adresses IP maximales : 2^(32-26) = 2^6 = 64 adresses IP (dont 62 adresses IP utilisables)
100.189.64.38/13
Masque de sous-réseau : 255.248.0.0 (car 13 bits sont utilisés pour le réseau)
Adresse du réseau : 100.184.0.0 (les 13 premiers bits de l'adresse IP sont conservés)
Adresse de diffusion : 100.191.255.255 (les 19 derniers bits sont remplacés par des 1)
Nombre d'adresses IP maximales : 2^(32-13) = 2^19 = 524,288 adresses IP (dont 524,286 adresses IP utilisables)
150.34.222.131/17
Masque de sous-réseau : 255.255.128.0 (car 17 bits sont utilisés pour le réseau)

Adresse du réseau : 150.34.128.0 (les 17 premiers bits de l'adresse IP sont conservés)
Adresse de diffusion : 150.34.255.255 (les 15 derniers bits sont remplacés par des 1)
Nombre d'adresses IP maximales : 2^(32-17) = 2^15 = 32,768 adresses IP (dont 32,766 adresses IP utilisables)

I

Exercice N°9 Cider avec 172.16.0.0/16

Supposons que vous avez été chargé de diviser une plage d'adresses IP en sous-réseaux à l'aide du CIDR.

La plage d'adresses IP suivante vous a été attribuée : 172.16.0.0/16. Vous devez diviser cette plage en sous-réseaux de tailles variables pour répondre aux besoins de votre entreprise.

Votre entreprise dispose de 5 départements différents, chacun nécessitant un sous-réseau distinct. Les exigences de chaque département en matière de nombre de nœuds sont les suivantes :

- Département A : 1000 machines
- Département B : 500 machines
- Département C : 250 machines
- Département D : 100 machines
- Département E : 50 machines

Divisez la plage d'adresses IP de manière à fournir des sous-réseaux pour chaque département, tout en utilisant le moins d'adresses IP possible.

Pour diviser la plage d'adresses IP de manière à fournir des sous-réseaux pour chaque département tout en utilisant le moins d'adresses IP possible, nous devons déterminer les préfixes CIDR les plus appropriés pour chaque département en fonction de leurs besoins en matière de nœuds.
Pour ce faire, nous utilisons la formule :

Nombre de nœuds ≤ 2^(32 - préfixe CIDR) - 2
Voici la répartition des préfixes CIDR pour chaque département :

Département A - 1000 nœuds
Pour couvrir au moins 1000 nœuds, nous avons besoin d'un préfixe CIDR de 22 (2^(32-22) - 2 = 1022 nœuds disponibles). Sous-réseau : 172.16.0.0/22
Plage d'adresses : 172.16.0.1 - 172.16.3.254

Département B - 500 nœuds
Pour couvrir au moins 500 nœuds, nous avons besoin d'un préfixe CIDR de 23 (2^(32-23) - 2 = 510 nœuds disponibles). Sous-réseau : 172.16.4.0/23
Plage d'adresses : 172.16.4.1 - 172.16.5.254

Département C - 250 nœuds

```
 Pour couvrir au moins 250 nœuds, nous avons besoin d'un préfixe CIDR de
24 (2^(32-24) - 2 = 254 nœuds disponibles). Sous-réseau : 172.16.6.0/24
Plage d'adresses : 172.16.6.1 - 172.16.6.254

Département D - 100 nœuds
Pour couvrir au moins 100 nœuds, nous avons besoin d'un préfixe CIDR de
25 (2^(32-25) - 2 = 126 nœuds disponibles). Sous-réseau : 172.16.7.0/25
Plage d'adresses : 172.16.7.1 - 172.16.7.126

Département E - 50 nœuds
Pour couvrir au moins 50 nœuds, nous avons besoin d'un préfixe CIDR de
26 (2^(32-26) - 2 = 62 nœuds disponibles). Sous-réseau : 172.16.7.128/26
Plage d'adresses : 172.16.7.129 - 172.16.7.190

Résumé des sous-réseaux :
Département A : 172.16.0.0/22
Département B : 172.16.4.0/23
Département C : 172.16.6.0/24
Département D : 172.16.7.0/25
Département E : 172.16.7.128/26
```

Exercice N°10 FAI – Sans VLSM

Un fournisseur d'accès Internet (FAI) dispose d'un bloc d'adresses IP de 195.27.16.0/20. Un client nécessite un sous-réseau capable de supporter environ 500 machines.

Question 1 : Combien de sous-réseaux de classe C sont inclus dans le bloc d'adresses fourni par le FAI ?

Réponse : Il y a 16 sous-réseaux de classe C dans un bloc /20.

```
# Question 1: Calculate the number of Class C subnets in a /20 network
# A Class C network is /24, so the difference in the subnet mask is 4 bits (24 -
20 = 4).
# Each bit represents a binary value, so 2^4 = 16 Class C networks are in a /20
network.
num_class_c_in_20 = 2 ** (24 - 20)
```

Question 2 : Combien de sous-réseaux de classe C le client nécessite-t-il pour accommoder ses 500 machines ?

Réponse : Le client nécessite 2 sous-réseaux de classe C pour accommoder environ 500 machines, car un sous-réseau de classe C peut supporter jusqu'à 254 hôtes.

Question 3 : Si le FAI attribue les sous-réseaux nécessaires au client en commençant par le troisième sous-réseau disponible, quel serait le premier sous-réseau attribué au client ?

Réponse : Le premier sous-réseau attribué au client serait le sous-réseau commençant par 195.27.18.0, car c'est le troisième sous-réseau dans le bloc d'adresses.

Question 4 : Quelle est l'adresse du sous-réseau attribué au client, exprimée en notation CIDR ?

Question 4 : Quelle est l'adresse du sous-réseau attribué au client, exprimée en notation CIDR ?
Réponse : L'adresse du sous-réseau attribué au client, exprimée en notation CIDR, est 195.27.18.0/24.

Q.1 Combien de classe C le FAI possède-t-il ?

Le fournisseur dispose de 16 classes C,
Pourquoi 16 ?
Parce que 195 est une classe C donc le masque est /24 ou les 4 bits de poids faible du troisième octet.permettent de les numéroter.

Q.2 De combien de classe C le client à t'il besoin

Le fournisseur lui attribue les blocs à partir de la 3ème.

Déterminer en notation CIDR le bloc d'adresses de classe C obtenu par le client ?

Le client a besoin de deux classes C (512 adresses).

Le fournisseur dispose de 16 classes C,
Pourquoi 16 les 4 bits de poids faible du troisième octet.permettent de les numéroter.
Si l'ISP attribue ses troisième et quatrième classes au client, nous obtenons les adresses :
• Bloc ISP :
11000011. 0001 1011. 0001.**0000**. 00000000 = 195.27.16.0 / 20
2er SS -reseau
11000011. 0001 1011. 0001.**0001**. 00000000
3èle SS -reseau
11000011. 0001 1011. 0001.**0010**. 00000000
• 1 classe C client :
11000011. 0001 1011. 0001.**0010**. 00000000 = 195.27.18.0 / 24
• 2 classe C client :
11000011. 0001 1011. 0001.**0011**. 00000000 = 195.27.19.0 / 24
• Bloc client :
11000011. 0001 1011. 0001.0010. 00000000 = 195.27.18.0 / 23

Exercice N°11 Méthode Magic Number

Remplissez ce tableau à l'aide du magic number

Adresse	Masques	@rése	@diffusion
131.108.78.235 /21	255.255.248.0	131.108.72.0	131.108.79.255
63.69.48.211 /11	255.224.0.0	63.64.0.0	63.95.255.255
168.94.197.13 /19	255.255.224.0	168.94.192.0	168.94.223.255
200.249.145.227 /28	255.255.255.240	200.249.145.224	200.249.145.239
192.154.88.133 /26	255.255.255.192	192.154.88.128	192.154.88.191
100.189.64.38 /13	255.248.0.0	100.184.0.0	100.191.255.255
150.34.222.131 /17	255.255.128.0	150.34.128.0	150.34.255.255

131.108.78.235 /21	255.255.248.0	131.108.72.0	131.108.79.255

Mc = 256-248 = 8
1 x 8 = 8
2 x 8 = 16
3 x 8 = 24
4 x 8 = 32
5 x 8 = 40
6 x 8 = 48
7 x 8 = 56
8 x 8 = 64
9 x 8 = 72
10 x 8 = 80
72<78
Donc 131.108.72.0

Fin 80-1 = 79
131.108.79.255

168.94.197.13 /19	255.255.224.0	168.94.192.0	168.94.223.255

256-224=32
1 x 32 = 32
2 x 32 = 64
3 x 32 = 96
4 x 32 = 128
5 x 32 = 160
6 x 32 = 192
7 x 32 = 224
8 x 32 = 256
192<197
224-1 = 223

4. Exercices VLSM

Exercice N°1 VLSM Niv 1

Supposons que vous ayez été chargé de diviser une plage d'adresses IP en sous-réseaux à l'aide du VLSM. La plage d'adresses IP suivante vous a été attribuée : 192.168.10.0/24.
Vous devez diviser cette plage en sous-réseaux égaux pour 4 départements différents dans une entreprise.

- Chaque département nécessite un nombre différent d'adresses IP :
- Service A 10
- Service B : ,20
- Service C : 15
- Service D : 30 machines

Q.1 Divisez cette plage en sous-réseaux pour répondre aux besoins de chaque département et indiquez la plage d'adresses IP de chaque sous-réseau.

Étapes :

Besoins en adresses par département:

Calcul des sous-réseaux:

Plages d'adresses attribuées

Donnez l'adresse de chaque réseau ainsi que l'adresse de diffusion

Pour diviser la plage d'adresses IP 192.168.10.0/24 en sous-réseaux en utilisant le VLSM (Variable Length Subnet Masking), nous commençons par allouer des sous-réseaux aux départements en fonction de leur besoin maximal d'adresses IP, en attribuant la plus grande plage au département ayant le plus grand nombre de besoins en adresses, et ainsi de suite. Cela aide à utiliser l'espace d'adressage de manière efficace.

`Besoins en adresses par département:`

- Service D : 30 machines
- Service B : 20 machines
- Service C : 15 machines
- Service A : 10 machines

Calcul des sous-réseaux:

1. **Service D (30 machines) :**
   - Nombre minimum d'adresses IP nécessaires (en comptant l'adresse de réseau et l'adresse de broadcast) : 30 + 2 = 32.
   - Taille du sous-réseau : **32** (la plus proche puissance de 2).
   - Masque : 256 - 32 = 224 ou **/27**.
   - Plage : **192.168.10.0/27**. à **192.168.10.31/27**
2. **Service B (20 machines) :**
   - Nombre minimum d'adresses IP nécessaires : 20 + 2 = 22.
   - Taille du sous-réseau : **32** (la plus proche puissance de 2, car 22 dépasse 16).
   - Masque : 256 - 32 = 224 ou /27.
   - ce sous-réseau commence à 192.168.10.32/27 à à 192.168.10.(31+32)63/27.
3. **Service C (15 machines) :**
   - Nombre minimum d'adresses IP nécessaires : 15 + 2 = 17.
   - Taille du sous-réseau : 32 (car 17 dépasse 16).
   - Masque : 256 - 32 = 224 ou /27.
   - Ce sous-réseau commence là où s'est arrêté le précédent : 192.168.10.64/27 à 192.168.10.(63+32) 95/27.
4. **Service A (10 machines) :**

- Nombre minimum d'adresses IP nécessaires : 10 + 2 = 12.
- Taille du sous-réseau : 16 (la plus proche puissance de 2).
- Masque : 256 - 16 = 240 ou /28.
- Ce sous-réseau commence là où s'est arrêté le précédent : 192.168.10.96/28. A 192.168.10.(95+16)111/28

Plages d'adresses attribuées :

- **Service D** : 192.168.10.0/27 - Adresses de .0 à .31 (Utilisables: .1 à .30)
- **Service B** : 192.168.10.32/27 - Adresses de .32 à .**63 (31+32)** (Utilisables: .33 à .62)
- **Service C** : 192.168.10.64/27 - Adresses de .64 à .95 (Utilisables: .65 à .94)
- **Service A** : 192.168.10.96/28 - Adresses de .96 à .111 (Utilisables: .97 à .110)

Cette répartition maximise l'utilisation de l'espace d'adressage disponible tout en répondant aux besoins de chaque département.

```
Pour diviser la plage d'adresses IP 192.168.10.0/24 en utilisant le
Variable Length Subnet Masking (VLSM) pour répondre aux besoins de
chaque département, procédez comme suit :

Triez les départements par ordre décroissant en fonction de leurs
besoins en adresses IP.
Département A : 50 adresses
Département B : 20 adresses
Département C : 15 adresses
Département D : 10 adresses

Trouvez le masque de sous-réseau approprié pour chaque département en
fonction de ses besoins en adresses IP.
Pour cela, utilisez la formule : Nombre d'adresses ≥ 2^(32 - préfixe
CIDR)
Département A : 50 adresses (2^6 = 64 adresses) -> Masque /26 (32-6 =
26)
Département B : 20 adresses (2^5 = 32 adresses) -> Masque /27 (32-5 =
27)
Département C : 15 adresses (2^4 = 16 adresses) -> Masque /28 (32-4 =
28)
Département D : 10 adresses (2^4 = 16 adresses) -> Masque /28 (32-4 =
28)

Attribuez les sous-réseaux en fonction de leurs masques de sous-réseau.
Département A : 192.168.10.0/26 Plage d'adresses IP : 192.168.10.1 -
192.168.10.62
Département B : 192.168.10.64/27 Plage d'adresses IP : 192.168.10.65 -
192.168.10.94
Département C : 192.168.10.96/28 Plage d'adresses IP : 192.168.10.97 -
192.168.10.110
```

Département D : 192.168.10.112/28 Plage d'adresses IP : 192.168.10.113 - 192.168.10.126
Résumé des sous-réseaux :
Département A : 192.168.10.0/26, Plage d'adresses IP : 192.168.10.1 - 192.168.10.62
Département B : 192.168.10.64/27, Plage d'adresses IP : 192.168.10.65 - 192.168.10.94
Département C : 192.168.10.96/28, Plage d'adresses IP : 192.168.10.97 - 192.168.10.110
Département D : 192.168.10.112/28, Plage d'adresses IP : 192.168.10.113 - 192.168.10.126

Exercice N°2 VLSM Niv 2

Vous avez été chargé de concevoir un plan d'adressage IP pour une entreprise avec les exigences suivantes :
Le réseau doit être divisé en 8 sous-réseaux.
Chaque sous-réseau doit avoir un nombre différent d'adresses IP : 100 80 60 50 30 20 15 et 10 machines
Le réseau doit être en mesure de prendre en charge jusqu'à 1000 hôtes.
Le plan d'adressage IP doit être optimisé pour minimiser le gaspillage d'adresses IP.

Q.1 Concevez un plan d'adressage IP en utilisant le VLSM pour répondre à ces exigences.

Pour concevoir un plan d'adressage IP en utilisant le VLSM (Variable Length Subnet Masking) pour répondre à ces exigences, procédez comme suit :

Triez les sous-réseaux par ordre décroissant en fonction de leurs besoins en adresses IP :
Sous-réseau A : 100 adresses
Sous-réseau B : 80 adresses
Sous-réseau C : 60 adresses
Sous-réseau D : 50 adresses
Sous-réseau E : 30 adresses
Sous-réseau F : 20 adresses
Sous-réseau G : 15 adresses
Sous-réseau H : 10 adresses

Calculez la taille du réseau nécessaire pour prendre en charge jusqu'à 1000 hôtes.
Dans ce cas, le réseau doit être capable de prendre en charge au moins 2^10 (1024) adresses IP. Le masque de sous-réseau approprié est donc /22.

Choisissez une adresse de réseau de base pour commencer.
Par exemple, prenons 10.0.0.0/22.

Trouvez le masque de sous-réseau approprié pour chaque sous-réseau en fonction de ses besoins en adresses IP.
Pour cela, utilisez la formule : Nombre d'adresses ≥ 2^(32 - préfixe CIDR)

Sous-réseau A : 100 adresses (2^7 = 128 adresses) -> Masque /25 (32-7 = 25)
Sous-réseau B : 80 adresses (2^7 = 128 adresses) -> Masque /25 (32-7 = 25)
Sous-réseau C : 60 adresses (2^6 = 64 adresses) -> Masque /26 (32-6 = 26)
Sous-réseau D : 50 adresses (2^6 = 64 adresses) -> Masque /26 (32-6 = 26)
Sous-réseau E : 30 adresses (2^5 = 32 adresses) -> Masque /27 (32-5 = 27)
Sous-réseau F : 20 adresses (2^5 = 32 adresses) -> Masque /27 (32-5 = 27)
Sous-réseau G : 15 adresses (2^4 = 16 adresses) -> Masque /28 (32-4 = 28)
Sous-réseau H : 10 adresses (2^4 = 16 adresses) -> Masque /28 (32-4 = 28)

Attribuez les sous-réseaux en fonction de leurs masques de sous-réseau.
Sous-réseau A : 10.0.0.0/25
Plage d'adresses IP : 10.0.0.1 - 10.0.0.126

Sous-réseau B : 10.0.0.128/25
Plage d'adresses IP : 10.0.0.129 - 10.0.0.254

Sous-réseau C : 10.0.1.0/26
Plage d'adresses IP : 10.0.1.1 - 10.0.1.62
Sous-réseau D : 10.0.1.64/26 Plage d'adresses IP : 10.0.1.65 - 10.0.1.126
Sous-réseau E : 10.0.1.128/27 Plage d'adresses IP : 10.0.1.129 - 10.0.1.158
Sous-réseau F : 10.0.1.160/27 Plage d'adresses IP : 10.0.1.161 - 10.0.1.190
Sous-réseau G : 10.0.1.192/28 Plage d'adresses IP : 10.0.1.193 - 10.0.1.206
Sous-réseau H : 10.0.1.208/28 Plage d'adresses IP : 10.0.1.209 - 10.0.1.222
Résumé des sous-réseaux :
Sous-réseau A : 10.0.0.0/25, Plage d'adresses IP : 10.0.0.1 - 10.0.0.126
Sous-réseau B : 10.0.0.128/25, Plage d'adresses IP : 10.0.0.129 - 10.0.0.254
Sous-réseau C : 10.0.1.0/26, Plage d'adresses IP : 10.0.1.1 - 10.0.1.62
Sous-réseau D : 10.0.1.64/26, Plage d'adresses IP : 10.0.1.65 - 10.0.1.126
Sous-réseau E : 10.0.1.128/27, Plage d'adresses IP : 10.0.1.129 - 10.0.1.158
Sous-réseau F : 10.0.1.160/27, Plage d'adresses IP : 10.0.1.161 - 10.0.1.190
Sous-réseau G : 10.0.1.192/28, Plage d'adresses IP : 10.0.1.193 - 10.0.1.206

Sous-réseau H : 10.0.1.208/28, Plage d'adresses IP : 10.0.1.209 - 10.0.1.222
Ceci répond aux exigences de l'exercice en utilisant le VLSM pour créer des sous-réseaux avec des tailles adaptées à chaque département, tout en minimisant le gaspillage d'adresses IP

Chapitre N°09 - Les équipements réseau

Chapitre N°10 - Le routage

Chapitre N°11 - Les commandes réseaux

Chapitre N°12 - les services TCP IP

Chapitre N°13 - PareFeu-VPN

Chapitre N°14 - L'adressage IPv6

Chapitre n°15 - CyberSecurité

Chapitre N°16 - Sécurité des IOT