Travaux Dirigés

MODULE M2103

2020-2021

Sommaire

TCP-IP (Adressage classique) - 1

1. Convertissez les nombres binaires donnés en nombres décimaux :

Valeur								
Exposant	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position	128	64	32	16	8	4	2	1
Bit	1	0	0	0	0	1	0	0

Valeur								
Exposant	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position	128	64	32	16	8	4	2	1
Bit	0	1	1	0	1	0	1	1

Valeur								
Exposant	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position	128	64	32	16	8	4	2	1
Bit	1	1	0	1	0	1	0	1

Valeur								
Exposant	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position	128	64	32	16	8	4	2	1
Bit	0	1	0	1	1	0	0	1

Valeur								
Exposant	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position	128	64	32	16	8	4	2	1
Bit	1	0	1	1	1	1	0	0

2. Effectuez les conversions suivantes de décimal en binaire

Valeur décimale	106							
Exposant	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position	128	64	32	16	8	4	2	1
Bit	0	1	1	0	1	0	1	0

Valeur décimale	135							
Exposant	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position	128	64	32	16	8	4	2	1
Bit	1	0	0	0	0	1	1	1

Valeur décimale	216							
Exposant	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position	128	64	32	16	8	4	2	1
Bit	1	1	0	1	1	0	0	0

Valeur décimale	45							
Exposant	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position	128	64	32	16	8	4	2	1
Bit	0	0	1	0	1	1	0	1

Valeur décimale	93							
Exposant	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position	128	64	32	16	8	4	2	1
Bit	0	1	0	1	1	1	0	1

3. Vous devez calculer l'adresse réseau, les adresses des hôtes et l'adresse de diffusion des réseaux donnés.

Adresse/préfixe donnés de 178.8.2.193 /25

.11000001

Pour chaque ligne, entrez les valeurs du type d'adresse.

Type d'adresse	Entrez le DERNIER octet en binaire	Entrez le DERNIER octet en notation décimale	Entrez l'adresse complète en notation décimale
Réseau	10000000	128	178.8.2.128
Diffusion	11111111	255	178.8.2.255
Première adresse d'hôte utilisable	10000001	193	178.8.2.193
Dernière adresse d'hôte utilisable	11111110	254	178.8.2.254

Adresse/préfixe donnés de 142.200.21.108 /30

.01101100

Pour chaque ligne, entrez les valeurs du type d'adresse.

Type d'adresse	Entrez le DERNIER octet en binaire	Entrez le DERNIER octet en notation décimale	Entrez l'adresse complète en notation décimale
Réseau	01101100	108	142.200.21.108
Diffusion	01101111	111	142.200.21.111
Première adresse d'hôte utilisable	01101101	109	142.200.21.111
Dernière adresse d'hôte utilisable	01101110	110	142.200.21.110

Adresse/préfixe donnés de 146.91.239.247 /20

.1110*1111*.*11110111*

Pour chaque ligne, entrez les valeurs du type d'adresse.

Type d'adresse	Entrez le DERNIER octet en binaire	Entrez le DERNIER octet en notation décimale	Entrez l'adresse complète en notation décimale
Réseau	.1110*0000*	224	146.91.224.0
Diffusion	.1110*1111*	239	146.91.239.255
Première adresse d'hôte utilisable	.1110*0000*	224	146.91.224.1
Dernière adresse d'hôte utilisable	.1110*1111*	239	146.91.239.254

Adresse/préfixe donnés de 156.232.206.63 /17

.1 1 0 0 1 1 1 0. 0 0 1 1 1 1 1 1

Pour chaque ligne, entrez les valeurs du type d'adresse.

Type d'adresse	Entrez le DERNIER octet en binaire	Entrez le DERNIER octet en notation décimale	Entrez l'adresse complète en notation décimale
Réseau	.1 0 0 0 0 0 0 0	128	156.232.128.0
Diffusion	.1 1 1 1 1 1 1 1	255	156.232.255.255
Première adresse d'hôte utilisable	.1 0 0 0 0 0 0 0	128	156.232.128.1
Dernière adresse d'hôte utilisable	.1 1 1 1 1 1 1 1	255	156.232.255.254

4. Pour chaque paire de masques et d'adresses d'hôte, vous devez déterminer l'adresse réseau correspondante.

Adresse d'hôte	10	38	99	22
Masque de sous-réseau	255	255	224	0
Adresse d'hôte en binaire	00001010	00100110	01100011	00010110
Masque de sous-réseau en binaire	11111111	11111111	11100000	00000000
Adresse réseau en binaire	**00001010**	**00100110**	**01100000**	**00000000**
Adresse réseau en décimale	**10**	**38**	**96**	**0**

Adresse d'hôte	10	101	195	222
Masque de sous-réseau	255	255	254	0
Adresse d'hôte en binaire	00001010	01100101	11000011	11011110
Masque de sous-réseau en binaire	11111111	11111111	11111110	00000000
Adresse réseau en binaire	**00001010**	**01100101**	**11000000**	**00000000**
Adresse réseau en décimale	**10**	**101**	**194**	**0**

Adresse d'hôte	10	132	33	185
Masque de sous-réseau	255	255	255	252
Adresse d'hôte en binaire	00001010	10000100	00100001	10111001
Masque de sous-réseau en binaire	11111111	11111111	11111111	11111100
Adresse réseau en binaire	**00001010**	**10000100**	**00100001**	**10111001**
Adresse réseau en décimale	**10**	**132**	**33**	**184**

5. Pour chaque paire de masques et d'adresses d'hôte, vous devez déterminer le nombre maximal d'hôtes pour le réseau donné

Adresse réseau	10	0	0	0
Masque de sous-réseau	255	255	255	128
Adresse réseau en binaire	00001010	00000000	00000000	00000000
Masque de sous-réseau en binaire	11111111	11111111	11111111	10000000
Nombre d'hôtes	**2^7-2 = 126**			

Adresse réseau	10	0	0	0
Masque de sous-réseau	255	255	248	0
Adresse réseau en binaire	00001010	00000000	00000000	00000000
Masque de sous-réseau en binaire	11111111	11111111	11111000	00000000
Nombre d'hôtes	**2^11-2 = 2046**			

Adresse réseau	10	0	0	0
Masque de sous-réseau	255	255	255	252
Adresse réseau en binaire	00001010	00000000	00000000	00000000
Masque de sous-réseau en binaire	11111111	11111111	11111111	11111100
Nombre d'hôtes	**2^2-2 = 2**			

6. Pour chaque paire de masques et d'adresses d'hôte, vous devez définir les hôtes et les adresses réseau et de diffusion.

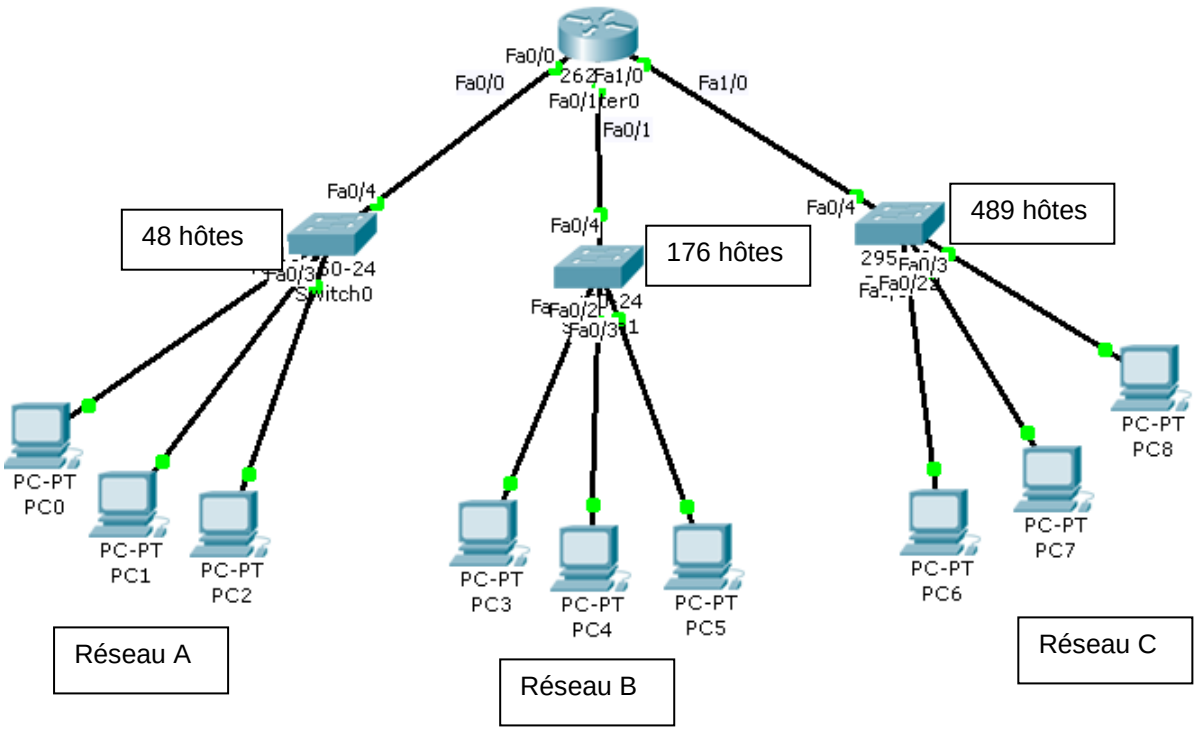
Adresse réseau en décimale	10	139	148	0
Masque de sous-réseau en décimale	255	255	252	0
Adresse réseau en binaire	00001010	10001011	10010100	00000000
Masque de sous-réseau en binaire	11111111	11111111	11111100	00000000
Première adresse IP d'hôte utilisable en décimale	Premier octet	Deuxième octet	Troisième octet	Quatrième octet
Dernière adresse IP d'hôte utilisable en décimale	Premier octet	Deuxième octet	Troisième octet	Quatrième octet
Adresse de diffusion en décimale	Premier octet	Deuxième octet	Troisième octet	Quatrième octet
Prochaine adresse réseau en décimale	Premier octet	Deuxième octet	Troisième octet	Quatrième octet

Adresse réseau en décimale	10	249	128	0
Masque de sous-réseau en décimale	255	255	128	0
Adresse réseau en binaire	00001010	11111001	10000000	00000000
Masque de sous-réseau en binaire	11111111	11111111	10000000	00000000
Première adresse IP d'hôte utilisable en décimale	Premier octet	Deuxième octet	Troisième octet	Quatrième octet
Dernière adresse IP d'hôte utilisable en décimale	Premier octet	Deuxième octet	Troisième octet	Quatrième octet
Adresse de diffusion en décimale	Premier octet	Deuxième octet	Troisième octet	Quatrième octet
Prochaine adresse réseau en décimale	Premier octet	Deuxième octet	Troisième octet	Quatrième octet

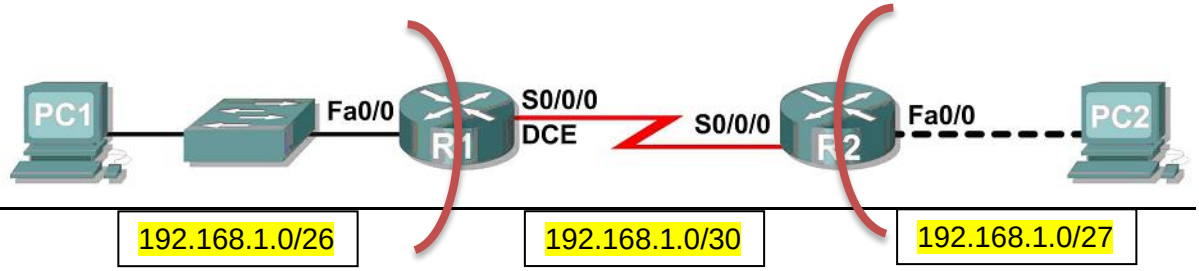
Adresse réseau en décimale	10	107	252	128
Masque de sous-réseau en décimale	255	255	255	128
Adresse réseau en binaire	00001010	01101011	11111100	10000000
Masque de sous-réseau en binaire	11111111	11111111	11111111	10000000
Première adresse IP d'hôte utilisable en décimale	Premier octet	Deuxième octet	Troisième octet	Quatrième octet
Dernière adresse IP d'hôte utilisable en décimale	Premier octet	Deuxième octet	Troisième octet	Quatrième octet
Adresse de diffusion en décimale	Premier octet	Deuxième octet	Troisième octet	Quatrième octet
Prochaine adresse réseau en décimale	Premier octet	Deuxième octet	Troisième octet	Quatrième octet

7. D'après la topologie illustrée et la liste d'adresses IP possibles, affectez une adresse IP et un masque de sous-réseau appropriés aux interfaces du routeur Router0 répondant aux conditions requises des hôtes de chaque réseau, tout en occasionnant le moins d'adresses IP inutilisées possible.

Adresse réseau	Nombre d'hôtes	Attribué au réseau …
10.3.105.190/16	65 534	
10.0.1.186/23	510	Réseau C
10.0.10.14/27	30	
10.2.7.195/21	2 046	
10.0.2.72/24	254	Réseau B
10.0.4.31/26	62	Réseau A



8. Vous devez concevoir et appliquer un système d'adressage IP pour la topologie présentée dans le schéma de topologie suivant. On vous fourni un bloc d'adresses que vous devez diviser en sous-réseaux pour proposer un schéma d'adressage logique pour le réseau. Les interfaces des routeurs et des PCs pourront alors être configurés en respectant votre système d'adressage IP.



Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	Fa0/1.20	192.168.1.65/27	255.255.255.224	S/O
	S0/0/0	192.168.1.97/30	255.255.255.252	S/O
R2	Fa0/1.20	192.168.1.1/26	255.255.255.192	S/O
	S0/0/0	192.168.1.98/30	255.255.255.252	S/O
PC1	Carte réseau	192.168.1.66/27	255.255.255.224	
PC2	Carte réseau	192.168.1.2/26	255.255.255.192	

Tâche 1 : découpage en sous-réseaux de l'espace d'adressage

Étape 1 : examen des besoins du réseau

L'espace d'adressage 192.168.1.0/24 a été mis à votre disposition pour votre conception de réseau. Le réseau est constitué des segments suivants :

- Le réseau local connecté au routeur R1 a besoin d'adresses IP en nombre suffisant pour prendre en charge 15 hôtes (15 adresses + 1 adresse routeur = 16 <=2^5-2= 30).
- Le réseau local connecté au routeur R2 a besoin d'adresses IP en nombre suffisant pour prendre en charge 30 hôtes (30 adresses + 1 adresse routeur = 31<=2^6-2= 62).
- La liaison entre le routeur R1 et le routeur R2 nécessite des adresses IP à chacune de ses
- extrémités (2 adresses = 2 <=2^2-2=2).

Le plan doit disposer de **sous-réseaux de taille différente** et utiliser **les tailles de sous-réseaux les plus petites** pour s'ajuster au nombre approprié d'hôtes.

Étape 2 : questions à prendre en considération lors de la conception de réseau

- De combien de sous-réseaux ce réseau a-t-il besoin ? _____3_____

Sous-réseau 1

- Sur combien de bits sera définie la partie HOST_ID ? _____5_____

- Quel est le masque de sous-réseau de ce réseau dans la notation en décimale à point ? 255.255.255.252 (1110 0000)

Sous-réseau 2

- Sur combien de bits sera définie la partie HOST_ID ? _____6_____
- Quel est le masque de sous-réseau de ce réseau dans la notation en décimale à point ? 255.255.255.192 (1100 0000)

Sous-réseau 3

- Sur combien de bits sera définie la partie HOST_ID ? _____2_____
- Quel est le masque de sous-réseau de ce réseau dans la notation en décimale à point ? 255.255.255.252 (1111 1100)

Sous-réseau 1

	Octet 1	**Octet2**	**Octet 3**	**Octet 4**
@réseau binaire	1100 0000	1010 1000	0000 0001	0100 0000
Masque sous-réseau binaire	1111 1111	1111 1111	1111 1111	1110 0000
@réseau décimal	192	168	1	64
Masque sous-réseau décimal	255	255	255	252

Sous-réseau 2

	Octet 1	**Octet2**	**Octet 3**	**Octet 4**
@réseau binaire	1100 0000	1010 1000	0000 0001	0000 0000
Préfixe sous-réseau binaire	1111 1111	1111 1111	1111 1111	1100 0000
@réseau décimal	192	168	1	0
Préfixe sous-réseau décimal	255	255	255	192

Sous-réseau 3

	Octet 1	**Octet2**	**Octet 3**	**Octet 4**
@réseau binaire	1100 0000	1010 1000	0000 0001	0110 0000
Préfixe sous-réseau binaire	1111 1111	1111 1111	1111 1111	1111 1100
@réseau décimal	192	168	1	96

Préfixe sous-réseau décimal	255	255	255	252

Étape 3 : affectation des adresses de sous-réseau au schéma de topologie

1. Le sous-réseau au réseau raccordé à R1.

   192.168.1.64/27

2. Le sous-réseau à la liaison entre R1 et R2.

   192.168.1.96/30

3. Le sous-réseau au réseau raccordé à R2.

   192.168.1.0/26

Tâche 2 : définition des adresses d'interface

Notez aussi les adresses à utiliser dans le tableau fourni sous le schéma de topologie !!!!

Attribuer les adresses appropriées aux interfaces des périphériques

1. l'interface du réseau local sur R1. 192.168.1.65/27
2. Le PC1. 192.168.1.66/27
3. L'interface du réseau étendu sur R1. 192.168.1.97/30
4. L'interface du réseau étendu sur R2. 192.168.1.98/30
5. L'interface du réseau local sur R2. 192.168.1.1/26
6. Le PC2. 192.168.1.2/26

TCP-IP (Adressage classique) – 2

Exercice 1

1. Quelles informations statiques sont à configurer dans une machine pour l'insérer dans un réseau TCP/IP raccordé à Internet ? @IP + Masque + passerelle
2. Convertir la représentation hexadécimale C22F1582 d'une adresse IP en sa représentation décimale.= C2.2F.15.82=194.47.21.130
3. Imaginons qu'on ait codé à l'origine la partie réseau des adresses de classe B sur 20 bits au lieu de 16. Combien de réseaux de classe B y aurait-il eu ? = 2^20=1 048 576

Exercice 2

1. Quelles sont les classes des adresses réseaux suivantes?
   a) 192.18.97.39 (adresse IP de www.javasoft.com) => **classe** C
   b) 138.96.64.15 (www.inria.fr) => **classe** B
   c) 193.49.184.6 (www.u-picardie.fr) => **classe** C
   d) 18.181.0.31 (www.mit.edu) => **classe** A
   e) 226.192.60.40 => **classe** D
2. Pour chacune de ces classes, étant donné un réseau y appartenant, combien d'adresses de machines peuvent, a priori, être utilisées?
3. Un réseau sur l'internet utilise le masque de sous-réseau 255.255.240.0. Quel est le nombre maximal d'hôtes qu'il peut gérer ?
4. Soit une adresse IP de classe B décomposée en sous-réseaux de façon à disposer d'au moins 76 sous-réseaux. Combien d'ordinateurs peut-il y avoir par réseau ?

Exercice 3

Votre entreprise vient de se voir attribuer l'adresse IP 214.123.115.0. Vous devez créer 10 sous-réseaux distincts pour les 10 succursales de l'entreprise, à partir de cette adresse IP.

1. Quel masque de sous-réseau devez vous utiliser ? (donner le masque en notation décimal (ex: 255.255.0.0) ou en nombre de bits (ex: 255.255.0.0 → /16)
2. Combien d'adresses IP (machines ou routeurs) pourra recevoir chaque sous-réseau ?
3. Quelle est l'adresse de broadcast du 5ième sous-réseau utilisable?
4. Combien d'adresses IP distinctes est-il possible d'utiliser avec un tel masque, tous sous-réseaux possibles confondus?

Exercice 4

Un ordinateur a pour adresse IP « 193.222.8.98 » et le masque de sous-réseau associé est « 255.255.255.192 »

1. Quelle est la classe du réseau? (A, B, ou C)
2. Quelle est l'adresse du sous-réseau?
3. Quel est l'adresse de broadcast qui permet de diffuser les datagrammes sur ce réseau?

Il faut se connecter à un serveur d'adresse IP 193.222.8.171

4. Appartient-il au même sous réseau?
5. Si non, indiquer le mécanisme qui permet au paquet d'atteindre sa destination.

Exercice 5

Soient 3 stations IP connectées sur le même câble Ethernet :

@IP_A = 192.168.32.97
@IP_B = 192.168.32.65
@IP_C = 192.168.32.49

Aucune passerelle par défaut n'est configurée dans les stations.

1. Le masque de sous réseau est 255.255.255.128.
   La station A peut-elle communiquer avec la station B, avec la station C ? Justifier.
   Quelle est l'adresse de broadcast pour la station A, pour la station B, pour la station C ?

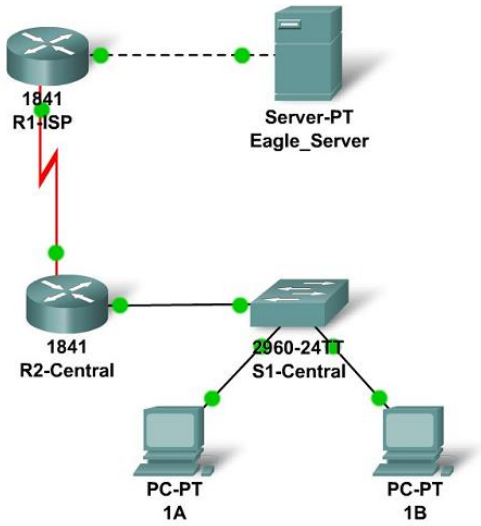
2. Le masque de sous réseau est 255.255.255.192.
   La station A peut-elle communiquer avec la station B, avec la station C ? Justifier.
   Quelle est l'adresse de broadcast pour la station A, pour la station B, pour la station C ?

3. Le masque de sous réseau est 255.255.255.224.
   La station A peut-elle communiquer avec la station B, avec la station C ? Justifier. Quelle est l'adresse de Broadcast pour la station A, pour la station B, pour la station C ?

Configuration de sous-réseaux

Planification de sous-réseaux et configuration d'adresses

Vous avez été chargé de mettre en œuvre la topologie suivante mais avec un nouveau modèle d'adressage IP. On vous a attribué le bloc d'adresses IP **192.168.12.0 /24**. Vous devez configurer les réseaux existants et prévoir les évolutions futures.



Les attributions de sous-réseaux sont les suivantes :

- 1er sous-réseau, réseau étendu WAN existant, liaison série point à point (2 adresses);
- 2e sous-réseau futur réseau WAN, liaison série point à point (2 adresses);
- 3e sous-réseau futur réseau WAN, liaison série point à point (2 adresses);
- 4e sous-réseau, réseau local existant du fournisseur de services Internet (ISP), jusqu'à 10 hôtes (R1-ISP <-> Eagle Serveur) ;
- 5e sous-réseau, réseau local existant des participants (connecté au routeur R2-Central), jusqu'à 58 hôtes ;
- 6e sous-réseau, futur réseau local des participants, jusqu'à 30 hôtes ;
  =====
- Pour le serveur, configurez la deuxième adresse IP utilisable la plus élevée sur le sous-réseau LAN existant du fournisseur de services Internet.
- Pour l'interface Fa0/0 du routeur R1-ISP, configurez l'adresse IP utilisable la plus élevée sur le sous-réseau LAN existant du fournisseur de services Internet.
- Pour l'interface S0/0/0 du routeur R1-ISP, configurez l'adresse utilisable la plus élevée sur le sous-réseau WAN existant.

- Pour l'interface S0/0/0 du routeur R2-Central, utilisez l'adresse utilisable la plus basse sur le sous-réseau WAN existant.
- Pour l'interface Fa0/0 du routeur R2-Central, utilisez l'adresse utilisable la plus élevée sur le sous-réseau LAN existant des participants.
- Pour les hôtes 1A et 1B, utilisez les deux premières adresses IP (les deux adresses utilisables les plus basses) du sous-réseau LAN existant des participants.

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	Fa0/0			S/O
	S0/0/0			S/O
R2-Central	Fa0/0			S/O
	S0/0/0			S/O
PC1A	Carte réseau			
PC1B	Carte réseau			
Eagle Server	Carte réseau			

TCP-IP (Adressage CIDR)

Exercice 1

Un grand nombre d'adresses IP consécutives sont disponibles ; elles commencent à 198.16.0.0. Supposons que quatre organisations, A, B, C et D, réclament l'une après l'autre, respectivement 4000, 2000 (2^11), 4000 (2^12) et 8000 (2^13) adresses. Pour chacune des ces organisations, donnez les premières et dernières adresses IP assignées et le masque en utilisant la notation w.x.y.z/s.

Exercice 2

Un routeur vient de recevoir les nouvelles adresses IP suivantes : 57.6.96.0/21, 57.6.104.0/21, 57.6.112.0/21 et 57.6.120.0/21. Si elles utilisent, toutes, la même ligne de sortie, peuvent elles être agrégées ? Si oui, jusqu'où ? Sinon, pourquoi ?

57.6.96.0/21 → 57.6.0110 0000.0
57.6.104.0/21 → 57.6.0110 1000.0
57.6.112.0/21 → 57.6.0111 0000.0
57.6.120.0/21 → 57.6.0111 1000.0

Route agrégée 57.6.96.0/19

Exercice 3

La plage d'adresses IP de 29.18.0.0 à 29.18.127.255 a été agrégée en 29.18.0.0/17 dans la table de routage d'un routeur. Un bloc de 1024 adresses, qui étaient jusque-là non assignées, de 29.18.60.0 à 29.18.63.255, est subitement affecté à un hôte sur une ligne de sortie différente de la table. Faut-il subdiviser l'adresse agrégée en ses blocs consécutifs, ajouter le nouveau bloc dans la table et voir s'il existe une autre possibilité d'agrégation ? Sinon, que peut-on faire à la place ?

Route agrégée
29.18.0.0/17 → 29.18.0000 0000.0 - 29.18.0111 1111.255

Nouvelle adresses assignées sur une ligne de sortie différente !!
29.18.60.0/22 → 29.18.0011 1100.0 - 29.18.0011 1111.255
Il faut donc subdiviser l'adresse agrégée en ses blocs consécutifs, ajouter le nouveau bloc dans la table et voir s'il existe une autre possibilité d'agrégation.

Exercice 4

Un routeur possède les entrées (CIDR) suivantes dans sa table de routage :

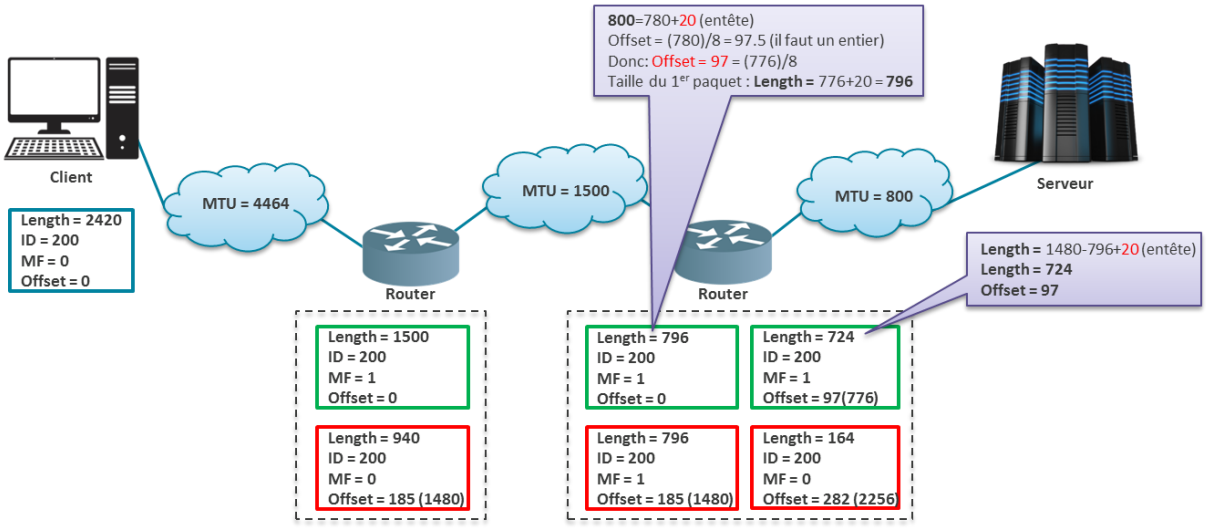
Adresse/masque	Prochain saut
135.46.56.0/22	Interface E0
135.46.60.0/22	Interface E1
192.53.40.0/23	Routeur R1
Par défaut	Routeur R2

Que fait le routeur s'il reçoit un paquet avec les adresses suivantes :

a) 135.46.63.10 → il envoie le paquet à l'Interface E1
b) 135.46.57.14 → il envoie le paquet à l'Interface E0
c) 135.46.52.2 → il envoie le paquet à l'Interface R2
d) 192.53.40.7 → il envoie le paquet à l'Interface R1
e) 192.53.56.7 → il envoie le paquet à l'Interface E0

TCP-IP (Fragmentation)

Clarifications de l'exercice fait en cours :



Exercice 1

Un datagramme IP contenant 2000 octets de données est émis sur un réseau A de MTU = 4096.
En passant par un routeur R1, il atteint le réseau B de MTU = 1024 octets. Il passe ensuite par un routeur R2 pour atteindre un réseau C de MTU = 512 octets.
La structure de l'en-tête du datagramme dans le réseau A est présentée ci-dessous :

0	4	8	16	24	31
4	5	0	? ? ?=2020		
1234			x00	0	
9		Protocole	Total de contrôle en-tête		
Adresse IP source					
Adresse IP destination					

a) Compléter le champ en-tête ci-dessus
b) Indiquer la structure de l'en-tête des datagrammes dans les réseaux B et C. Le total de contrôle de l'en-tête n'est pas à calculer.

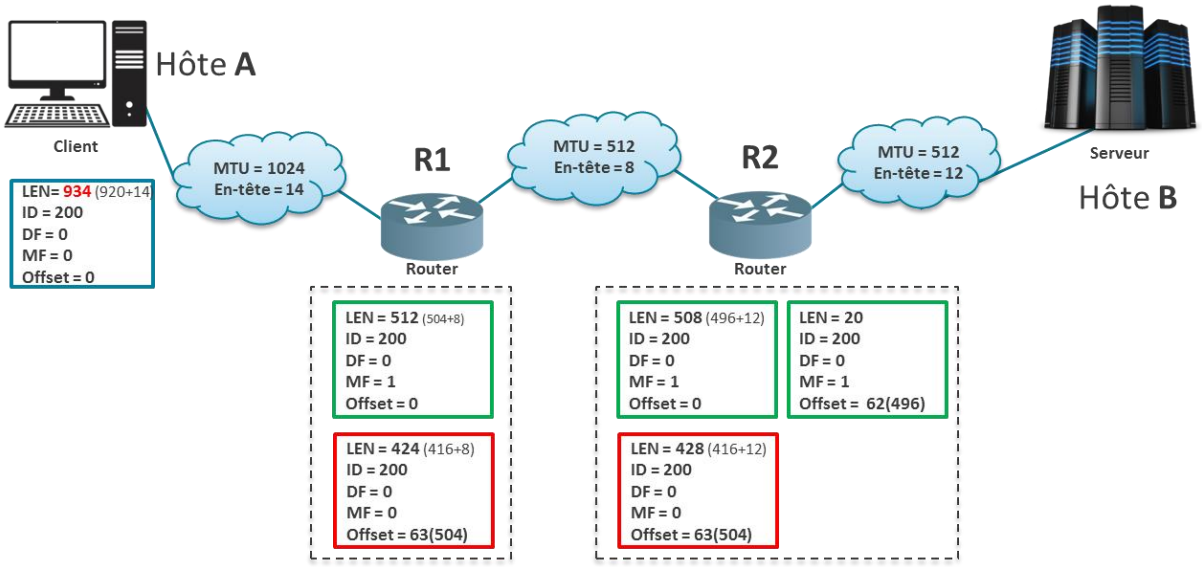
Vu pendant le cours :

A) 2020=2000+20 (00)
B) 1024=1004+20 (11) [0] / 1016=996+20 (10) [125->1004]
C) 512=492+20 / 512= 492+20 / 40=20+20 / / 512=492+20 / 512= 492+20 / 32=12+20
(11) [0] (11) [492] (10) [948] (11) [1004] (11) [1496] (10)[1988]

Exercice 2

Soit une ligne de communication reliant dans cet ordre : un hôte A, un routeur R1, un routeur R2 et un hôte B. Supposons qu'un message TCP contenant 900 octets de données et 20 octets d'en-tête soit remis au protocole IP sur l'hôte A pour transmission à l'hôte B. Indiquez la valeur des champs *LEN (Longueur totale)*, *ID (Identification)*, *DF*, *MF* et Fragment Offset de l'en-tête IP dans chaque paquet transmis sur les trois liaisons. On supposera que les tailles maximales de trames générées sur les liaisons entre A et R1, R1 et R2, R2 et B sont respectivement de :

- 1024 octets avec un en-tête de 14 octets inclus (A et R1),
- 512 octets avec un en-tête de 8 octets inclus (R1 et R2),
- 512 octets avec un en-tête de 12 octets inclus (R2 et B).



Exercice 3

Un datagramme IP utilisant l'option *Routage strict par la source* doit être fragmenté. Pensez-vous que l'option est copiée dans chaque fragment ou qu'il suffit de la placer dans le premier fragment ? Justifier votre réponse.

Le bit copie indique comment le routeur traite les options pendant la fragmentation.
1→ Copie indique que l'option doit être recopiée dans tous les fragments
Donc il faut avoir la même information sur chaque fragment pour respecter le Routage strict.

Exercice 4

La plupart des algorithmes de réassemblage de datagrammes IP utilisent un temporisateur pour éviter qu'un fragment perdu n'occupe indéfiniment les tampons de réassemblage. Supposons qu'un datagramme soit découpé en 4 fragments. Les trois premiers fragments arrivent, mais le dernier est retardé. Finalement, le temporisateur expire et les trois fragments sont éliminés de la mémoire du récepteur. Un peu plus tard, le dernier fragment arrive. Quel traitement lui réserver ?

Le dernier fragment sera également éliminé de la mémoire du récepteur

TCP-IP (Décodage)

Exercice 1

1. Décoder la trame suivante:
00 40 05 13 65 80 00 40 05 13 65 7D 08 00 45 10 00 2C 00 11 00 00 40 06 60 EC 80 DE 0C 02 80 DE 0C 01 3F 09 00 15 0D 99 04 A9 00 00 00 01 60 02 08 00 25 06 00 00 02 04 05 B4 0D 0A

En-tête Ethernet

Adresse destination	Adresse Source	Protocole
00 40 05 13 65 80	00 40 05 13 65 7D	08 00

Ethernet de type 0x0800 → **IPv4**

Paquet IPv4

Protocol 0x06 → **TCP**

0x4	0x5	0x10	Long. Total 0x00 2C → 44 octets	
ID: 0x00 11			x00	Offset : 0x0 00
Durée de vie : 0x40	Protocole : 0x**06** (TCP)		Total de contrôle en-tête : 0x60 EC	
@ IP source: **128.222.12.2**				
@ IP destination: **128.222.12.1**				
Message: 3F 09 00 15 0D 99 04 A9 00 00 00 01 60 02 08 00 25 06 00 00 02 04 05 B4 0D 0A				

2. Décoder les trames Ethernet suivantes et en déduire le but de l'échange (les trames sont données sans préambule et sans CRC).

Message 1:

FF FF FF FF FF FF 08 00 20 02 45 9E 08 06 00 01 08 00 06 04 00
01 08 00 20 02 45 9E 81 68 FE 06 00 00 00 00 00 00 81 68 FE 05

En-tête Ethernet

Adresse destination	Adresse Source	Protocole
FF FF FF FF FF FF	08 00 20 02 45 9E	0x08 06

Ethernet de type 0x0806 → **ARP**

Paquet ARP

Type de réseau N2: 0x00 01		Type de réseau N3: 0x08 00
LEN @ N2 : 0x06	LEN @ N2 : 0x04	Code opération : 0x**00 01** (Requête)
@ Eth source: 08 00 20 02 45 9E		
		@ IP source: 129.104.254.6
		@ Eth destination:
00 00 00 00 00 00		
@ IP destination: 129.104.254.5		

Message 2:

08 00 20 02 45 9E 08 00 20 07 0B 94 08 06 00 01 08 00 06 04 00
02 08 00 20 07 0B 94 81 68 FE 05 08 00 20 02 45 9E 81 68 FE 06

En-tête Ethernet

Adresse destination	Adresse Source	Protocole
08 00 20 02 45 9E	08 00 20 07 0B 94	0x08 06

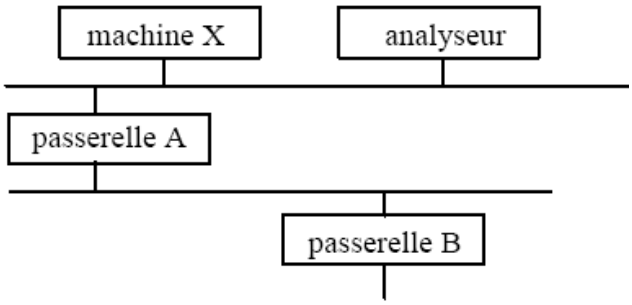
Ethernet de type 0x0806 → **ARP**

Paquet ARP

Type de réseau N2: 0x00 01		Type de réseau N3: 0x08 00
LEN @ N2 : 0x06	LEN @ N2 : 0x04	Code opération : 0x**00 02** (Réponse)
@ Eth source: 08 00 20 07 0B 94		
		@ IP source: 129.104.254.5
		@ Eth destination:
08 00 20 02 45 9E		
@ IP destination: 129.104.254.6		

Exercice 2

Un analyseur de réseau est disposé sur un réseau local Ethernet afin de permettre l'observation des trames circulant effectivement sur le support physique de communication. La structure du dispositif de mesure est la suivante :



On y voit deux réseaux Ethernet appartenant à la même organisation, interconnectés via un routeur A, ainsi qu'une connexion vers l'extérieur réalisée via le routeur B. Une trace a été obtenue par l'analyseur:

08 00 20 0a ac 96 08 00 20 0a 70 66 08 00 4f 00 00 7c cb c9 00 00 ff 01 b9 7f 84 e3 3d 05 c0 21 9f 06 07 27 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 a2 56 2f 00 00 00 29 36 8c 41 00 03 86 2b 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

En-tête Ethernet

Ethernet de type 0x0800 → **IPv4**

Adresse destination	Adresse Source	Protocole
08 00 20 0a ac 96	08 00 20 0a 70 66	0x08 00

En-tête IPv4

Long. en-tête 0xF → **15** (15x4 = 60)

Protocol 0x01 → **ICMP**

0x4	0xF	0x00	Long. Total 0x00 7C → 124 octets
ID: 0xCB C9		0x0	Offset : 0x0 00
Durée de vie : 0xFF	Protocole : 0x01 (ICMP)		Total de contrôle en-tête : 0xB9 7F
@ IP source: **132.227.61.5**			
@ IP destination: **192.33.159.6**			
07 27 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (40 octets)			

En-tête ICMP

Type 0x01 → **Echo Request**

Type : 0x08	Code : 0x00	Checksum : 0xA2 56
Bourrage ou données : 0x2F 00 00 00		
Données : 29 36 8c 41 00 03 86 2b 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		

08 00 20 0a 70 66 08 00 20 0a ac 96 08 00 4f 00 00 7c 3f 86 00 00 fb 01 49 af c0 21 9f 06 84 e3 3d 05 07 27 28 84 e3 3c 20 c0 2c 41 12 c0 46 47 05 c0 21 9f 02 c0 21 9f 06 c0 46 47 06 c0 2c 41 1a 84 e3 3c 1e 84 e3 3d 87 00 00 00 aa 56 2f 00 00 00 29 36 8c 41 00 03 86 2b 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

En-tête Ethernet

Ethernet de type 0x0800 → **IPv4**

Adresse destination	Adresse Source	Protocole
08 00 20 0a 70 66	08 00 20 0a ac 96	0x08 00

En-tête IPv4

Long. en-tête 0xF → **15** (15x4 = 60)

Protocol 0x01 → **ICMP**

0x4	0xF	0x00	Long. Total 0x00 7C → 124 octets
ID: 0x3F 86		0x0	Offset : 0x0 00

Durée de vie : 0xFB	Protocole : 0x01 (ICMP)	Total de contrôle en-tête : 0x49 AF
@ IP source: **192.33.159.6**		
@ IP destination: **132.227.61.5**		
07 27 28 84 e3 3c 20 c0 2c 41 12 c0 46 47 05 c0 21 9f 02 c0 21 9f 06 c0 46 47 06 c0 2c 41 1a 84 e3 3c 1e 84 e3 3d 87 00 (40 octets)		

En-tête ICMP

Type 0x01 → **Echo Reply**

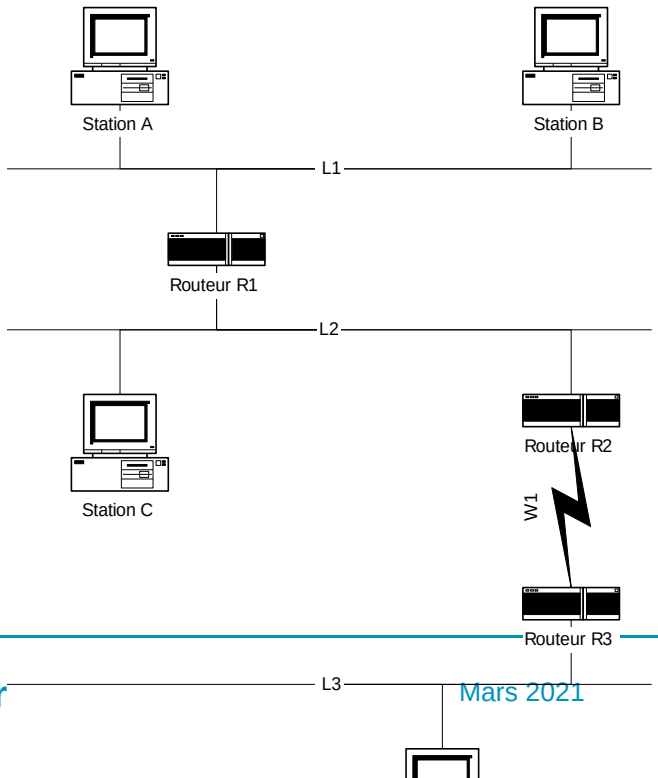
Type : 0x00	Code : 0x00	Checksum : 0xAA 56
Bourrage ou données : 0x2F 00 00 00		
Données : 29 36 8c 41 00 03 86 2b 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37		

- Décoder les deux trames précédentes.
- Quel est le but de cet échange ? ICMP (Ping)
- Quelles sont les classes d'adressage IP utilisées sur les réseaux émetteur et destinataire? IPv4
- Quel est le type de message ICMP
  - Packet 1: Echo Request
  - Packet 2: Echo Reply

TCP-IP (Routage)

1) **Exploitation des tables de routage des postes et des routeurs**

Un réseau est constitué de 3 segments Ethernet (L1, L2 et L3), de 3 routeurs IP (R1, R2 et R3), d'une liaison spécialisée (W1) et de 4 stations de travail (A, B, C et D), conformément au schéma ci-dessous



Les passerelles par défaut des stations sont :

Station	A	B	C	D
Passerelle par défaut	R1	-	R2	R3

Les tables de routage des routeurs sont:

R1	
Réseau cible	Routeur à utiliser
L1	Local
L2	Local
L3	R2

R2	
Réseau cible	Routeur à utiliser
W1	local
L2	local
L1	R1
L3	R3

R3	
Réseau cible	Routeur à utiliser
W1	local
L3	local
L1	R2
L2	R2

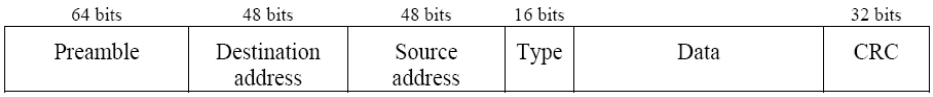
Pour chacun des cas suivants, indiquer si la réponse du ping arrive et quelles trames sont générées sur quels réseaux. On précisera les Mac adresses source et cible de chaque trame (on ne représentera pas les trames ARP).

- D ping A
  - Le ping arrive. ICMP request et ICMP replay
  -

- B ping A
- B ping R2
- R3 ping C
- R3 ping A
- A ping C

Aide-Mémoire

1. La trame Ethernet



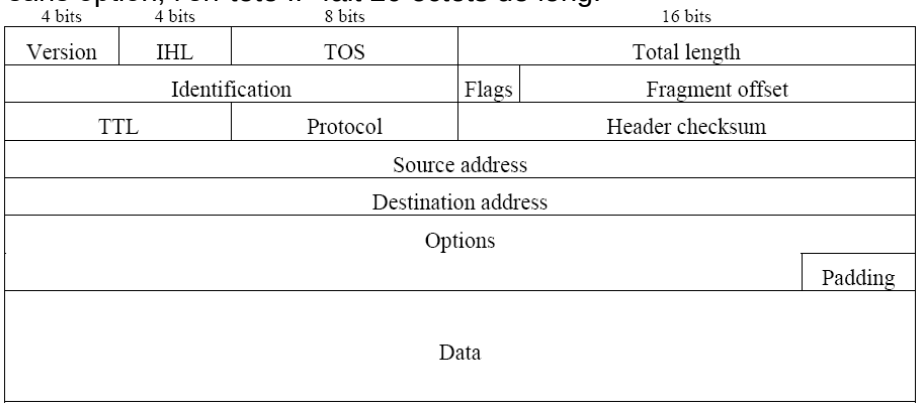
- «preamble» détermine le début d'une trame ;
- «Destination address» détermine la destination de la trame ;
- «Source address» détermine l'expéditeur de la trame ;
- «Type» définit le type de contenu de la trame ; ainsi il est possible de déterminer quel protocole va utiliser le paquet reçu :

Type	Utilisation
0800	IP
0805	X.25 niveau 3
0806	ARP
0807	XNS
6001 à 6006	DEC
8035	RARP
8098	Appletalk

- «Data» : les données brutes de la trame à passer au protocole déterminé par le champ «type»
- «CRC» : le checksum (contrôle de parité) de la trame permettant d'assurer son intégrité.

2. Le datagramme IP

L'en-tête IP est aligné sur des mots de 32 bits. Sa longueur est donc multiple de 4 octets. Par défaut, sans option, l'en-tête IP fait 20 octets de long.



- «Version» indique le format de l'en-tête. Ce champ sert à l'identification de la version courante du protocole. La version décrite ici (et aujourd'hui utilisée) porte le n°4 ;

- «IHL (*IP Header Length*)» est la longueur de l'en-tête IP exprimée en mots de 32 bits (5 au minimum) ;
- «TOS (*Type Of Service*)» définit le type de service à appliquer au paquet en fonction de certains paramètres comme le délai de transit, la sécurité. Codé sur 8 bits, il comprend les champs suivants :

P	D	T	R	0	0

Champ	Valeur
« P (*Precedence*) » (3 bits) décrit la priorité	111 contrôle du réseau 110 contrôle inter-réseaux 101 CRITIC/ECP 100 flash prioritaire 011 flash 010 immédiat 001 prioritaire 000 routine
« D (*Delay*) » décrit le souhait en matière de temps de traversée	0 normal 1 privilégier les chemins à temps de traversée faible
« T (*Throughput*) » décrit le souhait en matière de débit	0 normal 1 privilégier les chemins à débit élevé
« R (*Reliability*) » décrit le souhait en termes de fiabilité	0 normal 1 privilégier les chemins à fiabilité élevée

- «Total Length» est la longueur totale du datagramme, en-tête et données inclus, exprimée en octets ;
- «Identification» est une valeur fournie par l'émetteur aidant au réassemblage des différents fragments du datagramme. Le seul usage de ce champ est donc de permettre à une entité réceptrice de reconnaître les datagrammes qui appartiennent à un même datagramme initial et qui doivent donc faire l'objet d'un réassemblage ;
- «Flags» est utilisé par la fragmentation. Il est composé de deux indicateurs : DF (*Don't Fragment*) pour interdire la fragmentation et de MF (*More Fragment*) pour signifier des fragments à suivre :

0	DF	MF

DF : 0 = *May Fragment*
1 = *Don't Fragment*

MP : 0 = *Last Fragment*
1 = *More Fragments*

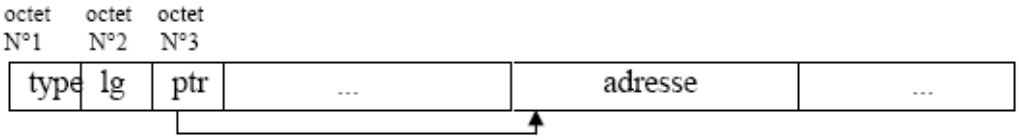
- «Fragment Offset» indique la position relative du fragment dans le datagramme initial, le déplacement étant donné en unités de 64 bits ;
- «Time To Live» représente une indication de la limite supérieure du temps de vie d'un datagramme. Cette valeur est comprise entre 0 et 255 ;
- «Protocol» indique le protocole (de niveau supérieur) utilisé pour le champ de données du datagramme :

Code (déc)	Abréviation	Nom du protocole	Référence
1	ICMP	Internet Control Message Protocol	[RFC792]
2	IGMP	Internet Group Management Protocol	[RFC1112]
3	GGP	Gateway-to-Gateway Protocol	[RFC823]
4	IP	IP in IP (encapsulation)	
5	ST	Stream	[RFC1190]
6	TCP	Transmission Control Protocol	[RFC793]
7	UCL	UCL	
8	EGP	Exterior Gateway Protocol	[RFC888]
9	IGP	any private Interior Gateway Protocol	
10	BBN-RCC-MON	BBN RCC Monitoring	
11	NVP-II	Network Voice Protocol	[RFC741]
12	PUP	PUP	
13	ARGUS	ARGUS	
14	EMCON	EMCON	
15	XNET	Cross Net Debugger	
16	CHAOS	Chaos	
17	UDP	User Datagram Protocol	[RFC768]
36	XTP	XTP	
37	DDP	Datagram Delivery Protocol	
45	IDRP	Inter-Domain Routing Protocol	
46	RSVP	Reservation Protocol	
47	GRE	General Routing Encapsulation	
48	MHRP	Mobile Host Routing Protocol	
54	NHR	NBMA Next Hop Resolution Protocol	

- «Header Checksum» est une zone de contrôle d'erreur portant uniquement sur l'en-tête du datagramme ;
- «Source Address » est l'adresse IP de la source du datagramme ;
- «Destination Address» est l'adresse IP de destination du datagramme ;
- «Options» sert à des fonctions de contrôle utiles dans certaines situations (estampillage temporel, sécurité, routage particulier, etc.). Le champ est donc de longueur variable. Il est constitué d'une succession d'options élémentaires, également de longueurs variables. Les options sont codées sur le principe TLV (type, longueur, valeur). La longueur indique la taille complète de l'option en octets. Les options possibles sont :

Type (déc.)	Option	Objet
0	*End of Options List* (EOOL)	Utilisée si la fin des options ne coïncide pas avec la fin de l'en-tête.
1	*No Operation* (NOP)	Pour aligner le début de l'option suivante sur 32 bits.
130	*Security* (SEC)	Permet aux hôtes d'indiquer des restrictions liées à la sécurité (ex : non classifié, confidentiel, restreint, top secret, etc.).
131	*Loose Source Route* (LSR)	Permet à la source du datagramme de fournir des informations à utiliser par les passerelles pour le routage du datagramme vers sa destination et d'enregistrer l'information concernant la route (série d'adresses Internet) ; un routeur ou une route peut utiliser n'importe quelle route avec un nombre quelconque de passerelles intermédiaires pour atteindre la prochaine adresse indiquée dans la route.
68	*Time Stamp* (TS)	Enregistrement de l'heure de chaque passage de passerelle.
133	*Extended Security* (E-SEC)	
7	*Record Route* (RR)	Permet d'enregistrer la route d'un datagramme (en fait, l'adresse de chaque passerelle traversée).
136	*Stream ID* (SID)	Permet de véhiculer un identifieur de flux ; utilisée à des fins de débogage et de mesure.
137	*Strict Source Route* (SSR)	Idem LSR, si ce n'est qu'un routeur ou un hôte doit envoyer directement le datagramme à la prochaine adresse indiquée dans la route.

A titre d'exemple, la structure de l'option RR est :

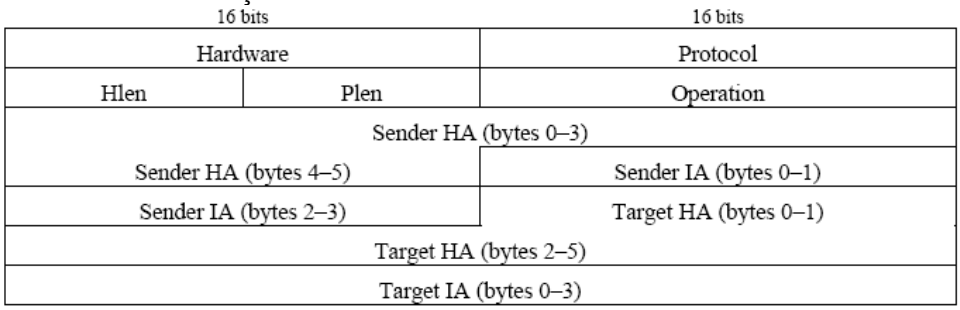


Champs Type : 7

- «Padding» permet d'aligner l'en-tête sur 32 bits.

3. Le paquet ARP (*Address Resolution Protocol*) / RARP (*Reverse ARP*)

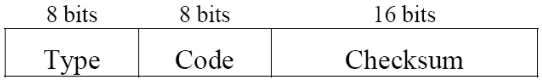
Le protocole ARP permet à une machine d'obtenir l'adresse Ethernet (physique) d'une autre machine, connaissant son adresse IP. Le protocole RARP fait l'inverse. Un paquet ARP (ou RARP) est structuré de la façon suivante :



- « Hardware» définit le type d'interface pour laquelle l'émetteur cherche une réponse ;
- « Protocol» définit le type de protocole pour lequel une requête a été émise ;
- «Hlen» définit la taille de l'adresse physique en octets ;
- «Plen» définit la taille de l'adresse au niveau protocolaire ;
- «Operation» décrit le type d'opération à effectuer par le récepteur ;
  Exemple : 00 01 pour une requête ;
  00 02 pour une réponse ;
- «Sender HA» définit l'adresse Ethernet (physique) de l'émetteur ;
- «Sender IA» définit l'adresse de niveau protocolaire (IP) demandé de l'émetteur
- «Target HA» définit l'adresse Ethernet du récepteur ;
- «Target IA» définit l'adresse de niveau protocolaire demandé du récepteur.

4. Le message ICMP (*Internet Control Message Protocol*)

Le protocole ICMP est utilisé lorsqu'un imprévu se produit ou pour tester Internet. Les messages
ICMP ont tous en commun le même format pour le premier mot de 32 bits.



Type	Message	Objet
0	Echo Reply	Réponse en écho.
3	Destination Unreachable	Destination inaccessible.
4	Source Quench	Interruption de la source.
5	Redirect	Redirection, changement de route.
8	Echo	Demande d'écho.
11	Time Exceeded	Temps de vie d'un datagramme dépassé.
12	Parameter Problem	Datagramme mal formé.
13	Timestamp	Demande de date d'estampillage.
14	Timestamp Reply	Réponse à une demande d'estampillage.
15	Information Request	Demande d'information.
16	Information Reply	Réponse à une demande d'information.
17	Address Mask Request	Demande de masque d'adresse.
18	Address Mask Reply	Réponse à une demande de masque d'adresse.

A titre d'exemple, l'échange de messages Echo et Echo Reply fonctionne de la manière suivante. L'adresse source dans un message Echo (type=8) sera l'adresse destinataire du message Echo Reply (type=0). Pour constituer un message Echo Reply, les adresses source et destination sont simplement inversées. Les données reçues dans un message Echo doivent être retournées dans le message Echo Reply. Deux champs du message, *Identifier* et *Sequence Number*, sont utilisés par l'émetteur de «l'écho» pour mettre en correspondance les réponses avec les requêtes. Par exemple, l'identificateur peut correspondre à un port TCP ou UDP pour identifier une session et le numéro de séquence être incrémenté pour chaque requête d'écho émise. Le répondeur retourne les mêmes valeurs dans sa réponse.