



THE INTERNATIONAL INSTITUTE OF
SUPINFO
INFORMATION TECHNOLOGY



Cisco CCNA 1

Théorie des réseaux

Cahier de Travaux Pratiques

www.supinfo.com
Copyright SUPINFO. All rights reserved

Campus Booster ID : 318
Version 3.0

Contenu

1. MODULE 1 : INTRODUCTION AUX RESEAUX	3
1.1. QUESTION 1 – CONFIGURATION MATERIELLE	3
1.2. EXERCICE 1 – CONVERSION DANS LES DIFFERENTES BASES	4
1.3. QUESTION 2 – TERMES ET UNITES DE MESURE	4
2. MODULE 2 : MODELES OSI ET TCP/IP	6
2.1. QUESTION 1 – MODELE OSI.....	6
2.2. QUESTION 2	6
2.3. QUESTION 3	6
2.4. QUESTION 4 – COMPARAISON ENTRE MODELES OSI ET TCP / IP	7
2.5. QUESTION 5	7
3. MODULE 3 : COUCHE 1 – MEDIAS ET EQUIPEMENTS RESEAU	8
3.1. EXERCICE 1 – IDENTIFICATION DES CODES COULEUR	8
3.2. TP 1 – REALISATION D'UN CABLE UTP	9
3.3. QUESTION 1 – THEORIE SUR LES CABLES UTP	9
3.4. EXERCICE 2 – VERIFICATION DES CABLES.....	9
3.5. EXERCICE 3 – MEDIAS OPTIQUES	10
3.6. EXERCICE 4 – RESEAUX WIRELESS - GENERALITES	10
3.7. EXERCICE 5 – RESEAUX WIRELESS – CAS PRATIQUE	11
4. MODULE 4 : COUCHE 2 – TECHNOLOGIES ETHERNET	12
4.1. EXERCICE 1 – ANALYSE DE TRAMES	12
4.2. EXERCICE 2 – DOMAINES DE COLLISION	13
5. MODULE 6 : COUCHE 3 – PROTOCOLE IP	16
5.1. EXERCICE 1 – RESOLUTION D'ADRESSES	16
5.2. EXERCICE 2 – CLASSES D'ADRESSES	16
5.3. EXERCICE 3 – DOMAINE DE BROADCAST.....	17
6. MODULE 5 : COUCHE 3 – SUBNETTING	18
6.1. EXERCICE 1 – OBSERVATIONS	18
6.2. EXERCICE 2 – EXERCICES SIMPLES.....	18
6.3. EXERCICE 3 – ETUDE DE CAS 1	19
6.4. EXERCICE 4 – ETUDE DE CAS 2	20
6.5. EXERCICE 5 – ETUDE DE CAS 3	21
6.6. EXERCICE 1.....	22
6.7. EXERCICE 2.....	24
7. MODULE 8 : COUCHE 3 – INTRODUCTION AU ROUTAGE	25
7.1. EXERCICE 1 – ETUDE DE CAS	25
8. MODULE 9 : COUCHES 4, 5, 6 ET 7	27
8.1. QUESTION 1 – NUMEROS DE PORTS	27
8.2. EXERCICE 1 – ANALYSE D'UNE REQUETE WEB.....	27
8.3. EXERCICE 2 – RECHERCHES ET DOCUMENTATION.....	31
8.4. EXERCICE 3 – ANALYSE DE DONNEES	34

1. Module 1 : Introduction aux réseaux

1.1. Question 1 – Configuration matérielle

- On souhaite monter un ordinateur de type PC à partir de pièces détachées, sachant que les besoins sont :
 - Connectivité Réseau
 - Connectivité Audio
 - Connectivité Vidéo
 - Disque dur interne et externe (la connectique est à votre libre choix)
 - Possibilité de lecture de média externe (CD, DVD)

Donner ci-dessous les principaux éléments nécessaires à cette configuration :

Configuration

1.2. Exercice 1 – Conversion dans les différentes bases

- Complétez les deux tableaux de nombres ci-dessous :

Base	Nombre	Base	Nombre
10	125	2	
10	92	2	
10	27	2	
10	203	2	
10	255	2	
2	0000 0110	10	
2	0110 0101	10	
2	1000 1110	10	
2	1010 1111	10	
2	1100 0000	10	
16	A1	10	
16	F2	10	
16	E2A	10	
16	3B	10	
16	14D	10	
16	1F	2	
16	2C	2	
16	9E	2	
16	3B	2	
16	B6	2	

Base	Nombre	Base	Nombre
10	18	8	
10	24	7	
10	44	6	
10	19	5	
10	120	4	
16	80	10	
16	D7	10	
16	3F	10	
16	AD	10	
16	FF	10	
2	0001 0110	16	
2	0010 0101	16	
2	1100 1110	16	
2	1000 1111	16	
2	1100 0011	16	
10	112	16	
10	28	16	
10	236	16	
10	59	16	
10	18	16	

1.3. Question 2 – Termes et unités de mesure

- Quel est l'acronyme désignant un réseau géographiquement limité, et que signifie cet acronyme ?

- Quel est le type de réseau en émergence que l'on retrouve généralement en ville dans les endroits publics ?

- Quel type de réseau a un besoin énorme en bande passante ?

- Quel type de réseau utilise-t-on avec un périphérique Bluetooth ?

- Quel terme désigne la capacité de débit d'un réseau ?

- Quelle unité utilise-t-on pour mesurer celle-ci ?

- Combien représentent 512 Kbits/s dans l'unité standard utilisée ?

- Un téléchargement se déroule à 37 Ko/s. Le débit théorique de la liaison est de 512 Kbits/s. Quel pourcentage de la bande passante est utilisé ?

2. Module 2 : Modèles OSI et TCP/IP

2.1. Question 1 – Modèle OSI

- Associez au numéro de chaque couche du modèle OSI son nom ainsi que sa fonction principale :

Numéro de couche	Nom	Fonction principale
7		
6		
5		
4		
3		
2		
1		

2.2. Question 2

- Indiquez l'unité de données de protocole pour chaque couche du modèle OSI :

Numéro de couche	PDU correspondant
7	
6	
5	
4	
3	
2	
1	

2.3. Question 3

- Dans le tableau suivant, il faut faire correspondre quelques exemples de protocoles et dispositifs à chacune des couches du modèle OSI :

Numéro de couche	Exemples	Dispositifs
7		
6		
5		
4		
3		
2		
1		

2.4. Question 4 – Comparaison entre modèles OSI et TCP / IP

- Donnez la correspondance entre les couches du modèle OSI et celles du modèle TCP/IP :

Couche du modèle OSI	Couche du modèle TCP/IP
Application	
Présentation	
Session	
Transport	
Réseau	
Liaison de données	
Physique	

2.5. Question 5

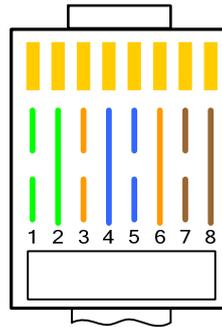
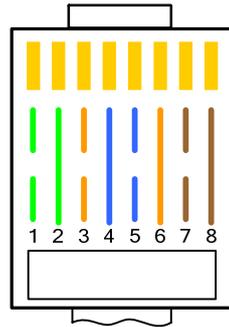
- Quelles sont les utilités du modèle OSI ?

- Pourquoi existe-t-il deux modèles ?

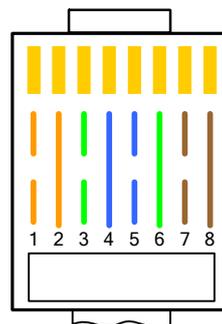
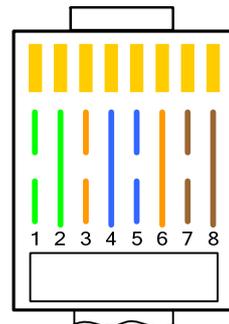
- Dans quel(s) but(s) a été créé le modèle TCP/IP ?

3. Module 3 : Couche 1 – Médias et équipements réseau

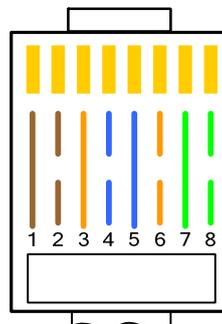
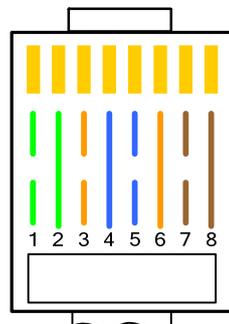
3.1. Exercice 1 – Identification des codes couleur



Les 2 schémas ci-dessus représentent les 2 extrémités d'un câble RJ45 de catégorie 5, face à vous. Identifiez le type de câble.



Les 2 schémas ci-dessus représentent les 2 extrémités d'un câble RJ45 de catégorie 5, face à vous. Identifiez le type de câble.



Les 2 schémas ci-dessus représentent les 2 extrémités d'un câble RJ45 de catégorie 5, face à vous. Identifiez le type de câble.

3.2. TP 1 – Réalisation d'un câble UTP

- Réalisez au choix l'un des câbles suivants :
 - o Câble droit
 - o Câble croisé
- Aidez-vous des codes couleurs normalisés présents dans l'essentiel de cours.
- Testez votre câble à l'aide d'un testeur, afin de vous assurer de son bon fonctionnement.

3.3. Question 1 – Théorie sur les câbles UTP

- Quel avantage tire-t-on des câbles à paires torsadées ?

- Quels appareils ou équipements peuvent causer du bruit sur un signal transmis sur un câble en cuivre ?

- D'après la norme EIA/TIA-568, quelles sont les paires utilisées pour l'émission/réception des données ?

3.4. Exercice 2 – Vérification des câbles

- Le dB est une unité de mesure permettant de quantifier la variation de puissance d'un signal (aussi appelé le gain). Il est donc utile pour vérifier la qualité d'un câble ou d'une transmission plus généralement (radio ou fibre optique).
- Voici les formules vous permettant d'effectuer tous les calculs :

$$G = 10 \log (P_{\text{final}}/P_{\text{init}})$$

$$G = \text{Gain en dB, } P = \text{Puissance du signal en Watts}$$

$$G = 20 \log (V_{\text{final}}/V_{\text{init}})$$

$$V = \text{Voltage du signal en Volts}$$

$$\text{Inverse de } f(x) = \log (x) \text{ est } f(y) = 10^y$$

- A l'aide des formules ci-dessus, compléter le tableau :

Type de média	Signal initial	Signal final	Gain	Cause(s) possible(s)
Câble UTP	1 Volt	2 μ V		
Câble STP	5 Volts		3 dB	
Liaison radio	1 mW	2 μ W		
Fibre optique	1 mW		-84 dB	

3.5. Exercice 3 – Médias optiques

- Complétez ce tableau de comparaison entre les modes de transmission monomode et multimode :

Caractéristique	Monomode	Multimode
Source lumineuse utilisée		
Connecteur utilisé		
Nombre de faisceaux lumineux		
Distance maximale		
Lieu(s) d'utilisation		

- Quels sont les 3 matériaux qui composent un câble en fibre optique et quelle est leur fonction ?

3.6. Exercice 4 – Réseaux Wireless - Généralités

- Donnez les caractéristiques des 3 types de standard de réseaux Wireless IEEE 802.11 actuellement utilisés en remplissant ce tableau :

Norme	Vitesse théorique maximale	Plage de fréquence utilisée
802.11b		
802.11a		
802.11g		

- Une entreprise dispose actuellement d'un réseau IEEE 802.11b. Celle-ci souhaiterait augmenter la bande passante de son réseau sans fil, sans pour autant demander à tous ses utilisateurs clients de changer leurs équipements. Quelle norme(s) les nouveaux Access Points devraient supporter pour remplir toutes les conditions énumérées précédemment ?

- A quel équipement réseau filaire peut-être assimilé la partie radio d'un Access Point ?

3.7. Exercice 5 – Réseaux Wireless – Cas pratique

- Dans une pièce de 80 mètres de largeur sans obstacles (conditions optimales), votre entreprise souhaite installer un WLAN. vous disposez de 2 Access Points, et le roaming doit être possible.
- Faites un schéma représentant l'implémentation, en prenant soin d'indiquer un maximum d'informations :

Schéma d'implémentation



- Quel est le rayon d'action maximal d'un Access Point dans ces conditions optimales ?

- Quelle distance maximale peut séparer les 2 Access Points ?

- Quelle longueur maximale va-t-on pouvoir couvrir ?

- Vérifiez que la zone de roaming est assez large :

- On détecte des interférences sur ce WLAN, quels appareils peuvent être l'origine de ces interférences ?

4. Module 4 : Couche 2 – Technologies Ethernet

4.1. Exercice 1 – Analyse de trames

- Voici ci-dessous une capture de trame ARP :

Capture de trames

```
Frame 1 (60 bytes on wire, 60 bytes captured)
  Arrival Time: Aug 23, 2004 10:51:56.093398000
  Time delta from previous packet: 0.000000000 seconds
  Time since reference or first frame: 0.000000000 seconds
  Frame Number: 1
  Packet Length: 60 bytes
  Capture Length: 60 bytes
Ethernet II, Src: 00:04:23:8b:ac:1b, Dst: ff:ff:ff:ff:ff:ff
  Destination: ff:ff:ff:ff:ff:ff (Broadcast)
  Source: 00:04:23:8b:ac:1b (172.16.104.4)
  Type: ARP (0x0806)
  Trailer: 00000000000000000000000000000000...
Address Resolution Protocol (request)
  Hardware type: Ethernet (0x0001)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (0x0001)
  Sender MAC address: 00:04:23:8b:ac:1b (172.16.104.4)
  Sender IP address: 172.16.104.4 (172.16.104.4)
  Target MAC address: 00:00:00:00:00:00 (00:00:00_00:00:00)
  Target IP address: 172.16.157.63 (172.16.157.63)
```

- Quel est le rôle des trames ARP ?

- Quelle est la longueur d'une trame ARP ?

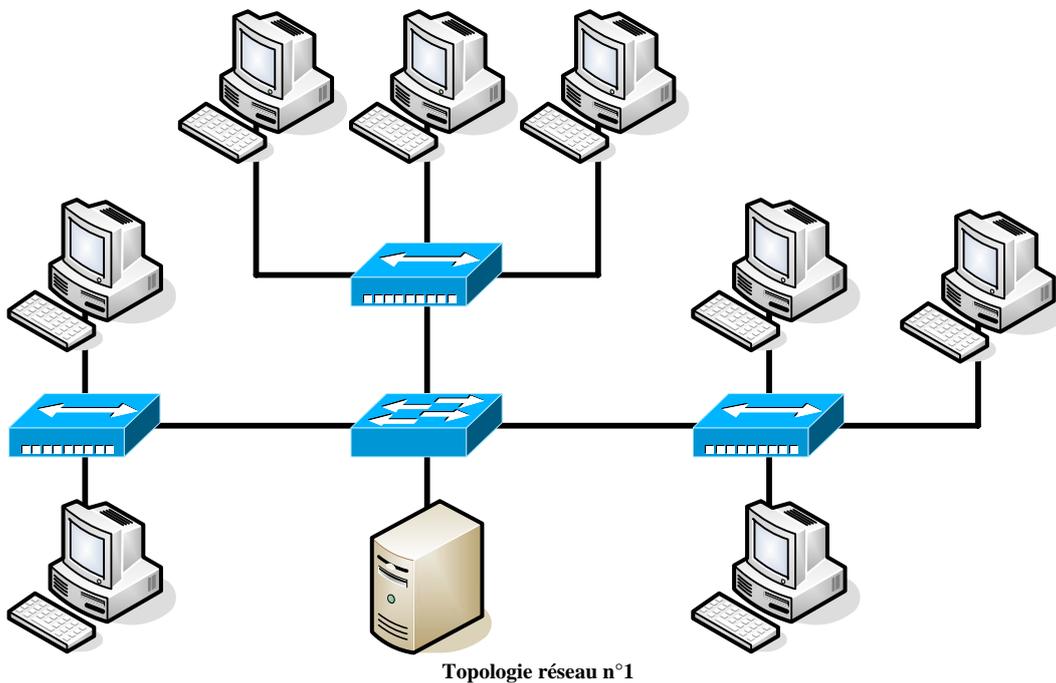
- Dans une trame Ethernet, le type de protocole (ARP, TCP, etc.) est précisé et a une valeur en hexadécimal. Quelle est la valeur hexadécimale représentant le protocole ARP ?

- Sur quel protocole de couche 3 reposent les requêtes ARP ? Quelle est la valeur hexadécimale le représentant ?

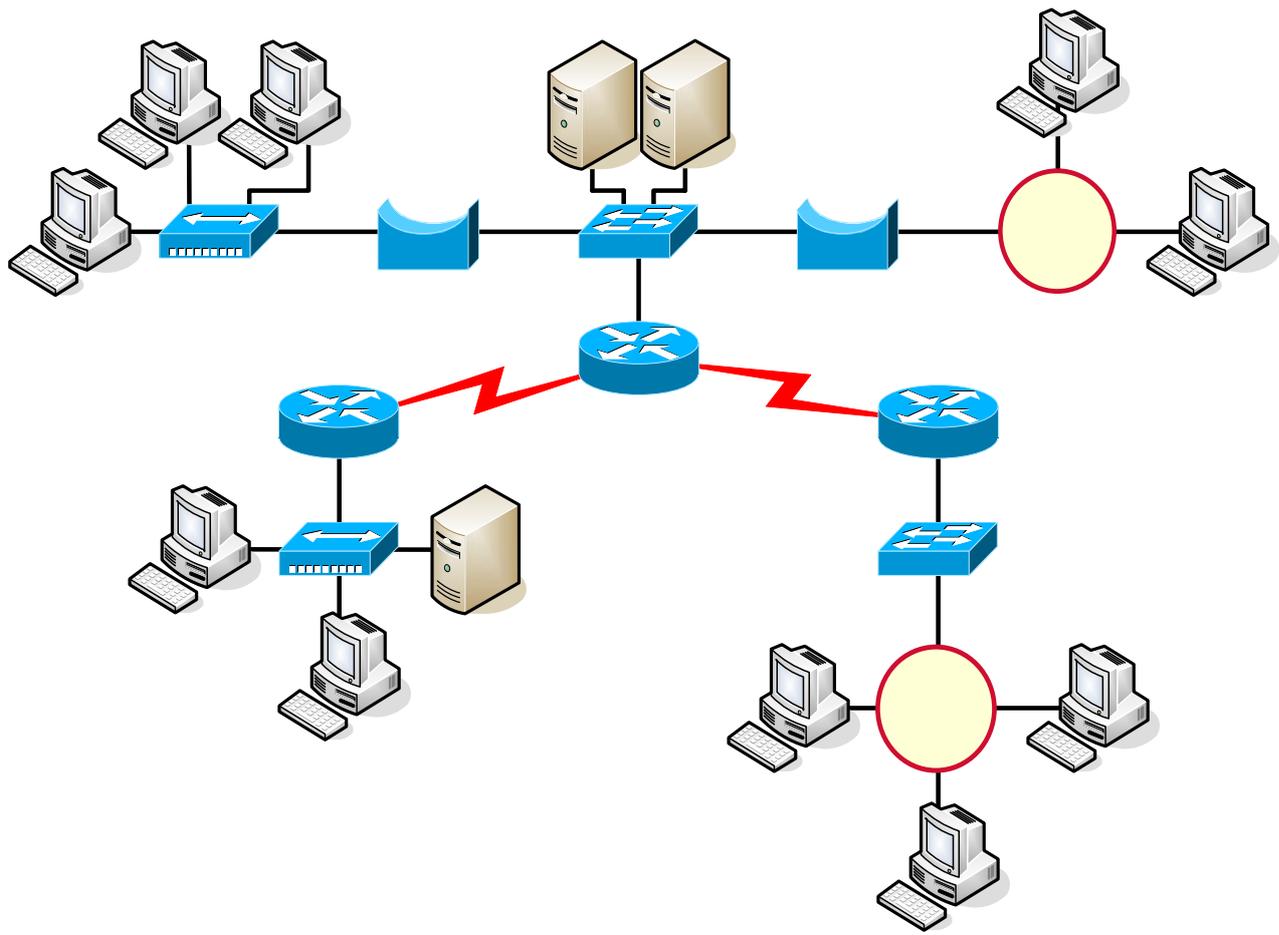
4.2. Exercice 2 – Domaines de collision

- Indiquez dans les cas suivants le nombre de domaines de collision résultant :

Contexte	Nombre de domaines de collision
2 stations, un répéteur, 2 stations	
4 stations reliées à un concentrateur ainsi qu'un serveur	
1 concentrateur avec 3 stations, relié à un autre concentrateur interconnectant 4 stations	
1 concentrateur avec 4 stations, relié par 1 routeur à 1 concentrateur avec 3 stations	

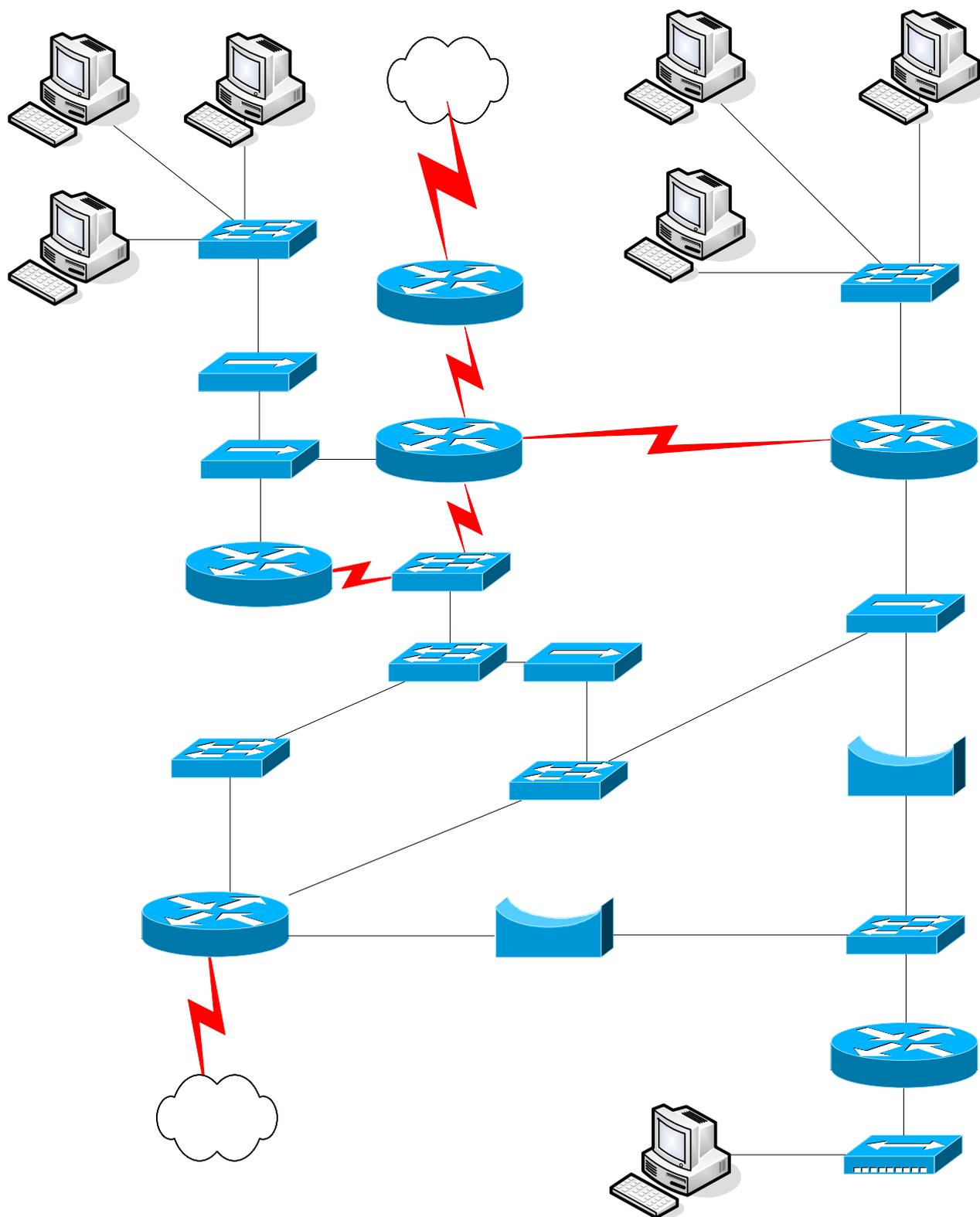


- Quel est le nombre de domaines de collision dans le réseau ci-dessus :
-



Topologie réseau n°2

- Quel est le nombre de domaines de collision dans le réseau ci-dessus :



Topologie réseau n°3

- Quel est le nombre de domaines de collision dans le réseau ci-dessus :

5. Module 6 : Couche 3 – Protocole IP

5.1. Exercice 1 – Résolution d'adresses

- Le tableau ci-dessous montre les adresses IP et MAC de 5 stations interconnectées et faisant partie du même réseau IP :

Adresse	Station 1	Station 2	Station 3	Station 4	Station 5
MAC	0028AF86CE51	0028AF86CF51	0028AFG6CD51	0028AF86CFF1	0028AF86CD1
IP	126.0.0.128	126.0.0.213	126.0.0.317	126.0.0.244	126.0.0.99

- Relevez les 3 erreurs existant dans les adresses de ces 5 stations :

Station			
Problème avec explications			

5.2. Exercice 2 – Classes d'adresses

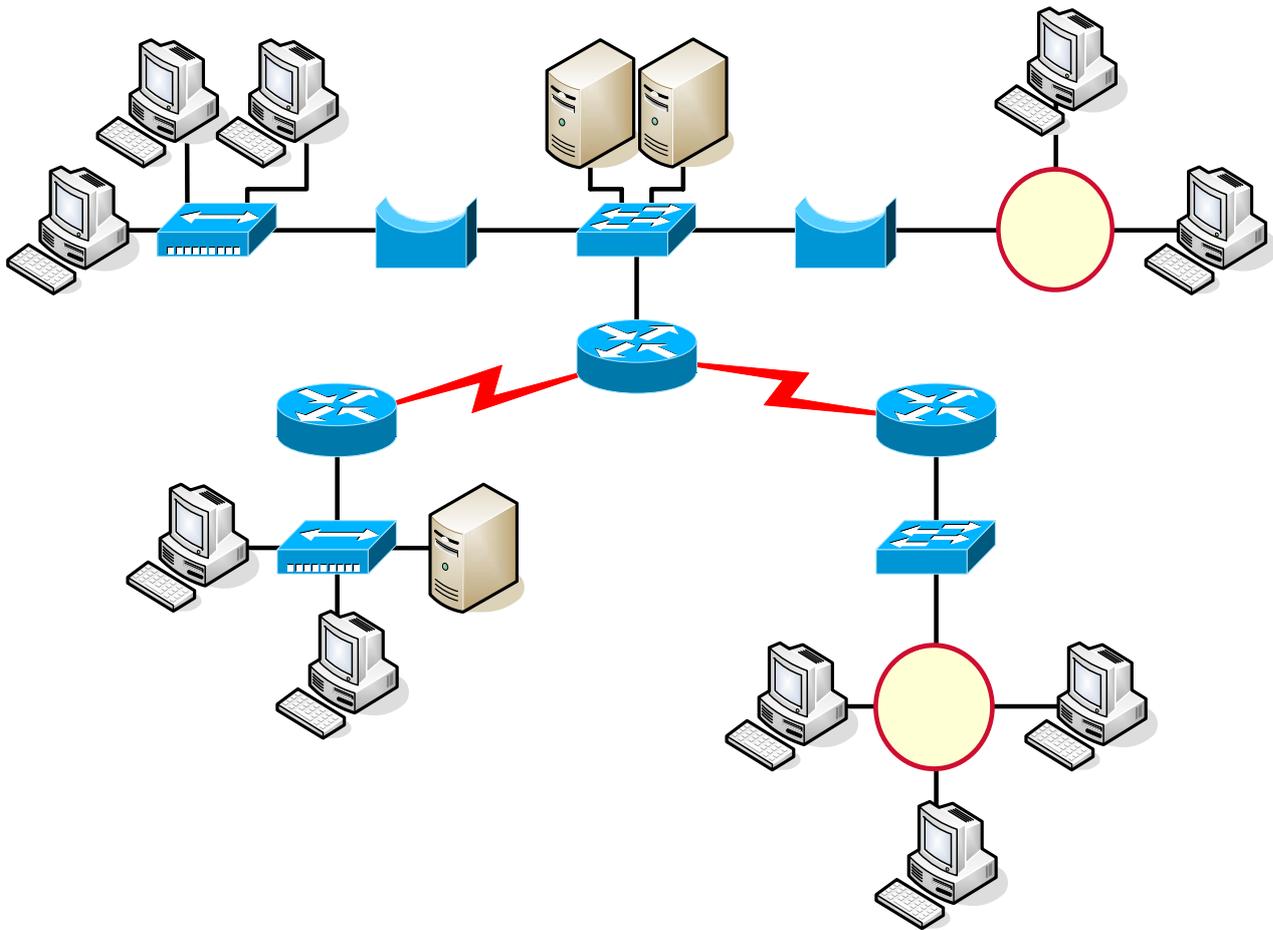
- Complétez le tableau suivant :

Adresse IP	Classe	Privée/publique/réservée ?
10.0.3.45		
	B	Privée
121.34.0.34		
134.156.87.5		
192.168.0.2		
	D	Réservée
221.12.21.75		
172.16.8.3		
	C	Privée
127.0.0.1		
	E	Réservée

- Parmi les adresses du tableau suivant, quelles sont celles pouvant être attribuées par un FAI ?

Adresse	Attribuable par un FAI ?
10.0.1.2	
115.3.4.5	
244.0.1.7	
151.34.65.2	
127.34.78.2	
172.23.89.23	
181.45.63.89	
192.168.34.73	

5.3. Exercice 3 – Domaine de broadcast



Topologie réseau n°1

- Combien y a-t-il de domaines de broadcast dans le réseau ci-dessus ?

6. Module 5 : Couche 3 – Subnetting

6.1. Exercice 1 – Observations

- On dispose d'un réseau de classe B avec un masque de sous-réseau de 255.255.240.0.
Combien de bits ont été empruntés à la partie hôte pour la partie sous-réseau ?

- Combien de sous-réseaux utilisables avons-nous à notre disposition dans ce contexte ?

- Considérons le réseau 192.168.33.0. Nous utilisons le masque de sous-réseau /28. Quelles sont, parmi les suivantes, les adresses IP utilisables pouvant être attribuées à des hôtes ?

Adresse IP	Utilisable ?	Si non, pourquoi ?
192.168.33.3		
192.168.33.15		
192.168.33.16		
192.168.33.17		
192.168.33.63		
192.168.33.65		

- Considérons une station d'un réseau ayant pour adresse IP 134.157.130.45.
Quelle est la classe d'adresse utilisée ?

- Le masque de sous-réseau étant 255.255.255.128, combien de sous-réseaux peuvent être utilisés ?

- Quelle est l'adresse de sous-réseau pour cette station ?

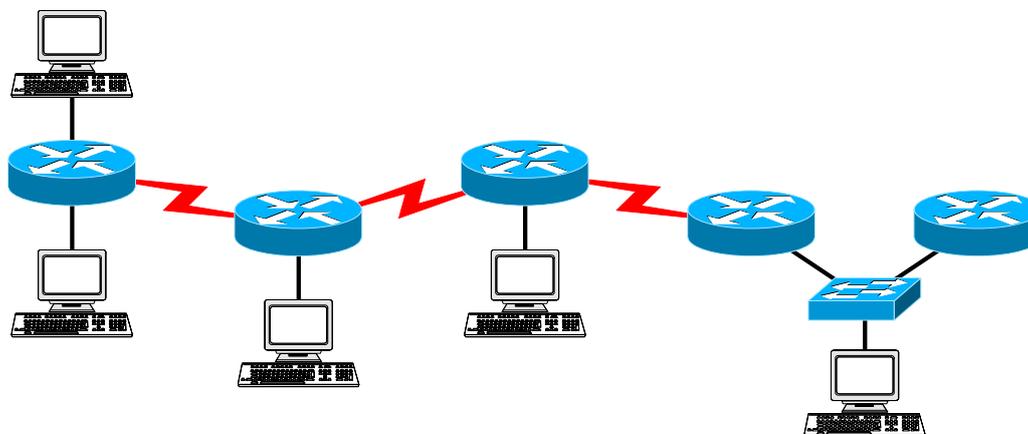
6.2. Exercice 2 – Exercices simples

- Un ordinateur a pour adresse IP 136.14.2.174/28. Est-ce que cette IP est valide et quelle est l'adresse du sous-réseau de cette station ?

- Un ordinateur a pour adresse IP 10.1.35.14/17. Est-ce que cette IP est valide et quelle est l'adresse de broadcast de cette station ?

- Une interface de routeur a pour IP 192.168.17.3/30. Est-ce que cette IP est valide et quelle est l'adresse du sous-réseau pour cette interface de routeur ?

6.3. Exercice 3 – Etude de cas 1



Topologie réseau n°1

- Nous allons utiliser la classe d'adresse 192.168.1.0/24 pour ce cas.
- Combien de sous-réseaux doit-on créer au minimum ?

- Combien de bits doit-on emprunter à la partie hôte et combien de sous-réseaux seront ainsi créés ?

- Quel est le masque de sous-réseau ainsi créé ?

- Nous allons utiliser la classe d'adresse 192.168.1.0/24.
- Complétez enfin le tableau d'attribution des plages d'adresses :

Sous-réseau	IP de sous-réseau IP de broadcast	Plage d'adresses utilisables
LAN n°1		
LAN n°2		
LAN n°3		
LAN n°4		
LAN n°5		
WAN n°1		
WAN n°2		
WAN n°3		

6.4. Exercice 4 – Etude de cas 2

- Une entreprise dispose d'un réseau Ethernet avec 60 hôtes, supportant le protocole TCP/IP.
- Les informations dont nous disposons sur ce réseau sont :
 - Classe d'adresse utilisée : 193.250.17.0
 - 3 départements : Administratif, commercial et production
 - Ces départements sont reliés à l'aide de routeurs (2 liaisons WAN)
- Les contraintes pour ce réseau sont les suivantes :
 - Chaque département doit avoir son propre sous-réseau.
 - Certaines stations du département de production utilisées sur les chaînes de montage ont déjà une plage d'adresses IP à ne pas modifier (attribuée statiquement). Celle-ci va de 193.250.17.110 à 193.250.17.117.
 - Le département administratif contient 25 hôtes, le département commercial 15 et le département production 20.

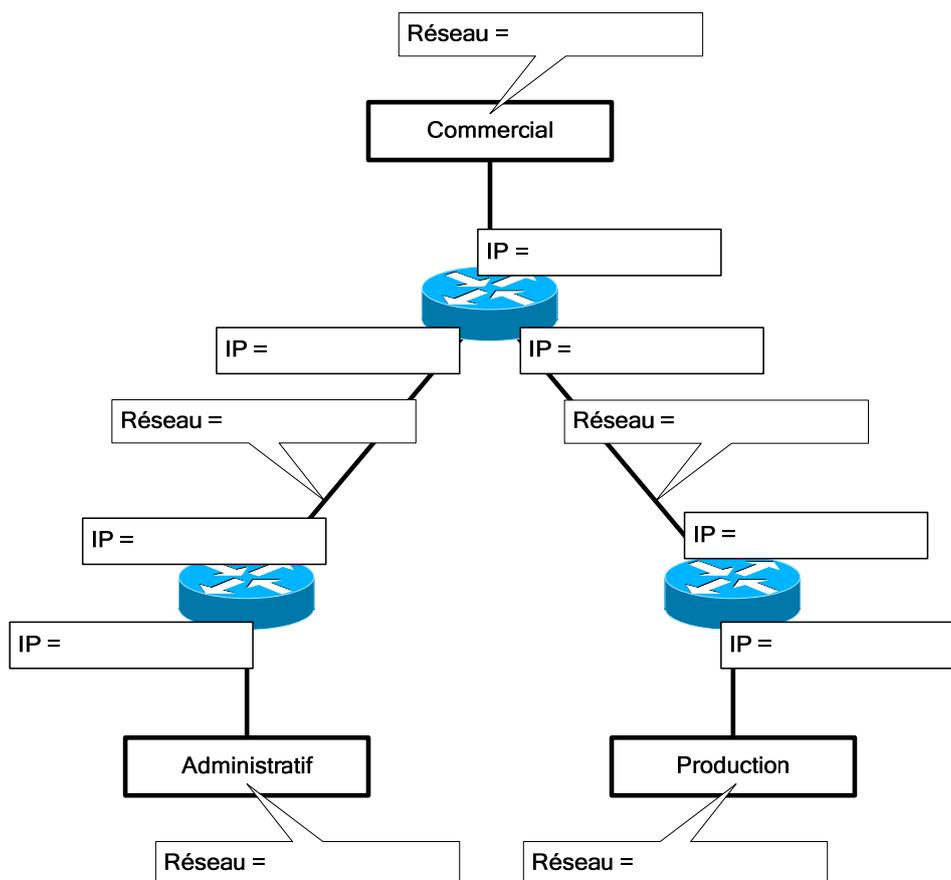
- Proposez un masque de sous-réseau en justifiant votre choix :

- Calculer le nombre total d'adresse IP disponibles pour l'adressage d'hôtes que peut contenir chaque sous-réseau :

- Complétez le tableau d'attribution des sous-réseaux :

Sous-réseau	IP de sous-réseau IP de broadcast	Plage d'adresses utilisables	Quelles adresses doivent être configurées sur le DHCP
Administratif			
Commercial			
Production			
Liaison WAN n°1			
Liaison WAN n°2			

- Complétez le schéma suivant :



6.5. Exercice 5 – Etude de cas 3

- Une entreprise dispose d'un parc informatique de 600 machines réparties équitablement dans 6 services.
- Nous voulons construire l'architecture réseau sur une seule classe d'adresses IP. De plus chaque service doit accéder à des ressources spécifiques dont les autres services ne devront pas disposer.
- Quelle classe d'adresses allez-vous employer ?

- Expliquez, notamment par le calcul, quel masque de sous-réseau vous allez utiliser pour répondre aux contraintes de l'énoncé :

- Complétez le tableau d'attribution des sous-réseaux :

Sous-réseau n°1	
Sous-réseau n°2	
Sous-réseau n°3	
Sous-réseau n°4	
Sous-réseau n°5	
Sous-réseau n°6	

6.6. Exercice 1

Rappel : pour répondre aux questions suivantes vous devrez utiliser la règle du 2ⁿ-2 pour la création des sous-réseaux, et toujours utiliser les masques de sous-réseaux les plus optimaux.

- On souhaite subdiviser le réseau de classe C 201.125.52.0 /24 en 20 sous-réseaux égaux. Quel est le masque de sous-réseau à utiliser ?

- On souhaite subdiviser le réseau de classe A 10.0.0.0 /8 en 502 sous-réseaux égaux. Quel est le masque de sous-réseau à utiliser ?

- On souhaite subdiviser le réseau de classe C 192.168.5.0 /24 en 4 sous-réseaux égaux. Quel est le masque de sous-réseau à utiliser ?

- On souhaite subdiviser le réseau de classe B 172.16.0.0 /16 en sous-réseaux de 20 hôtes chacun. Quel est le masque de sous-réseau à utiliser ?

- On souhaite subdiviser le réseau de classe C 192.168.4.0 /24 en sous-réseaux de 80 hôtes chacun. Quel est le masque de sous-réseau à utiliser ?

- On souhaite subdiviser le réseau de classe A 21.0.0.0 /8 en sous-réseaux de 500 hôtes chacun. Quel est le masque de sous-réseau à utiliser ?

- On souhaite subdiviser le réseau de classe A 21.0.0.0 /8 en sous-réseaux de 12 hôtes chacun. Quel est le masque de sous-réseau à utiliser ?

- On souhaite que les adresses IP : 192.168.1.25 /24, 192.168.1.26 /24 et 192.168.1.27 /24 soient sur le même sous-réseau. Quel est le masque de sous-réseau à utiliser ?

- On souhaite que les adresses IP : 192.168.1.23 /24, 192.168.1.24 /24, 192.168.1.25 /24, soient sur le même sous-réseau. Quel est le masque de sous-réseau à utiliser ?

- On souhaite que les adresses IP : 192.168.1.30, 192.168.1.31, 192.168.1.32, soient sur le même sous-réseau. Quel est le masque de sous-réseau à utiliser ?

- Citez ci-dessous les plages d'adresses (première et dernière adresse IP de chaque sous-réseau) obtenues en subdivisant le réseau de classe C 192.168.1.0 /24 avec le masque de sous-réseau suivant : 225.255.255.224.

- On souhaite subdiviser le réseau de classe A 25.0.0.0 /8 en 4 sous-réseaux de 80 hôtes chacun. Plusieurs masques de sous-réseaux peuvent être utilisés, faites-en la liste ci-dessous :

- On souhaite subdiviser le réseau de classe C 192.168.10.0 /24 en 2 sous-réseaux de 50 hôtes chacun. Quel est le masque de sous-réseau à utiliser ?

- On souhaite subdiviser le réseau de classe C 192.168.10.0 /24 en 3 sous réseaux de 50 hôtes chacun. Quel est le masque de sous-réseau à utiliser ?

6.7. Exercice 2

- Déterminez les plages d'adresses auxquelles appartiennent les adresses IP suivantes et indiquez si l'adresse en question est : une adresse d'hôte, une adresse réseau ou une adresse de broadcast.

Classe A :

- 10.35.177.132 /19
- 10.164.0.0 /11
- 10.244.137.111 /10
- 10.162.255.255 /12
- 10.19.255.255 /15
- 10.141.215.63 /14
- 10.15.72.32 /20
- 10.123.2.255 /13
- 10.0.0.0 /15
- 10.172.12.144 /12
- 10.37.88.101 /6

Classe B :

- 172.16.67.255 /22
- 172.16.14.217 /25
- 172.16.153.129 /19
- 172.16.149.93 /20
- 172.16.161.35 /21
- 172.16.52.0 /23
- 172.16.172.138 /22
- 172.16.255.255 /18
- 172.16.178.208 /28
- 172.16.31.93 /26
- 172.16.207.255 /20
- 172.16.33.252 /23

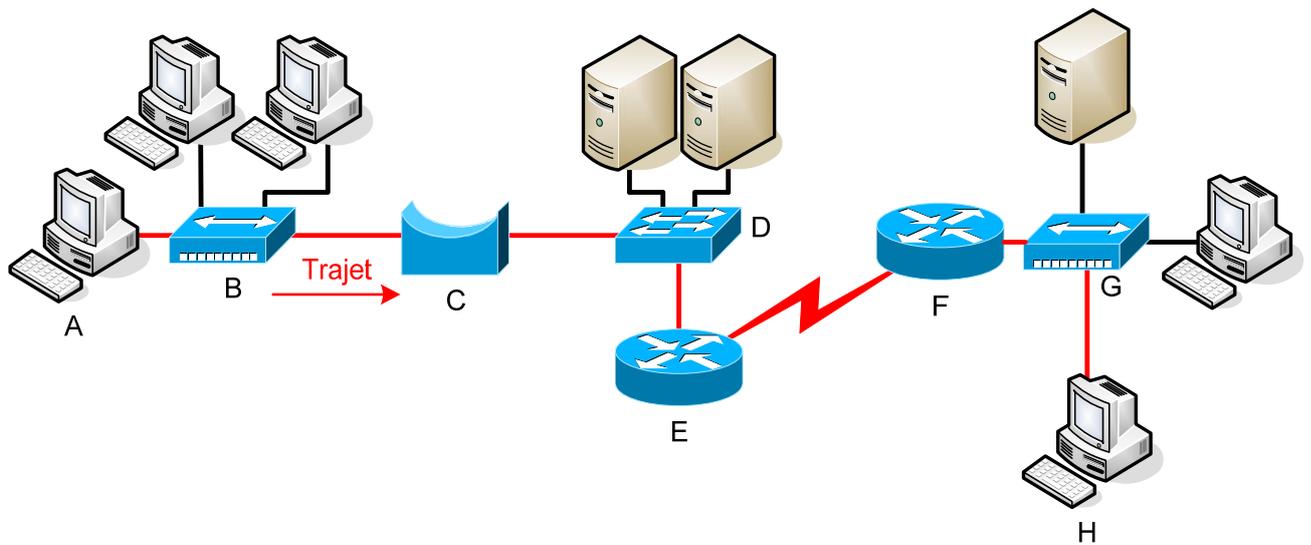
Classe C :

- 192.168.1.224 /28
- 192.168.2.159 /29
- 192.168.1.114 /27
- 192.168.3.142 /26
- 192.168.2.3 /30
- 192.168.4.225 /28
- 192.168.3.184 /29

7. Module 8 : Couche 3 – Introduction au routage

7.1. Exercice 1 – Etude de cas

La station A désire communiquer avec la station H :



Complétez le tableau avec les bonnes adresses de couche 2 et 3 :

	Adresse MAC Source	Adresse MAC Destination	Adresse IP Source	Adresse IP Destination
A				
Arrivée sur B				
Départ de B				
Arrivée sur C				
Départ de C				
Arrivée sur D				
Départ de D				
Arrivée sur E				
Départ de E				
Arrivée sur F				
Départ de F				
Arrivée sur G				
Départ de G				

H				
---	--	--	--	--

8. Module 9 : Couches 4, 5, 6 et 7

8.1. Question 1 – Numéros de ports

- Voici une liste avec des numéros de port et des noms de protocole. Trouvez le numéro de port ou le protocole correspondant :

Port	Protocole de couche 4	Numéro de port
		21
POP3		
		443
Telnet		
DNS		
		144
		27015
HTTP		
SSH		
		69
		25

- Compléter le tableau avec les plages réservées des ports TCP :

Type d'application	Plage de ports correspondante
Ports assignés par l'IANA	
	Supérieur à 1023

8.2. Exercice 1 – Analyse d'une requête Web

- Une requête Web sur la page <http://www.labo-cisco.com> (172.16.1.10) a été capturée depuis un ordinateur ayant pour IP 172.16.104.38. Nous allons nous intéresser aux segments TCP et UDP.

Capture – Trafic des requêtes					
No.	Time	Source	Destination	Protocol	Info
275	4.892953	172.16.104.38	172.16.1.10	TCP	3073 > http [ACK] Seq=364 Ack=20441 Win=52560 Len=0
276	4.893038	172.16.1.10	172.16.104.38	HTTP	Continuation
277	4.893163	172.16.1.10	172.16.104.38	HTTP	Continuation
278	4.893200	172.16.104.38	172.16.1.10	TCP	3073 > http [ACK] Seq=364 Ack=23361 Win=49640 Len=0
279	4.893286	172.16.1.10	172.16.104.38	HTTP	Continuation
280	4.893335	172.16.1.10	172.16.104.38	HTTP	Continuation
281	4.893365	172.16.104.38	172.16.1.10	TCP	3073 > http [ACK] Seq=364 Ack=25409
288	5.003410	172.16.104.38	172.16.1.10	TCP	[TCP Dup ACK 281#1] 3073 > http [ACK] Seq=364 Ack=25409 Win=51352 Len=0

289	5.013453	172.16.1.10	172.16.104.38	TCP	http > 3072 [ACK] Seq=80437 Ack=1373 Win=16148 Len=0
290	5.013492	172.16.1.10	172.16.104.38	TCP	http > 3073 [ACK] Seq=25409 Ack=364 Win=17157 Len=0
291	5.022946	172.16.104.38	172.16.1.10	TCP	3072 > http [ACK] Seq=1373 Ack=80437 Win=63184 Len=0
292	5.027996	172.16.104.38	172.16.1.10	TCP	[TCP Dup ACK 281#2] 3073 > http [ACK] Seq=364 Ack=25409 Win=64240 Len=0
293	5.040306	172.16.104.38	172.16.1.10	HTTP	GET /images/Charte/WebCisco_05N.gif HTTP/1.1
294	5.041092	172.16.1.10	172.16.104.38	HTTP	HTTP/1.1 200 OK (GIF89a)
295	5.041184	172.16.1.10	172.16.104.38	HTTP	Continuation
296	5.041230	172.16.104.38	172.16.1.10	TCP	3072 > http [ACK] Seq=1736 Ack=83045 Win=64240 Len=0
301	5.053659	62.161.94.199	172.16.104.38	TCP	http > 3074 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1460
302	5.053703	172.16.104.38	62.161.94.199	TCP	3074 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
303	5.054444	172.16.104.38	172.16.1.10	HTTP	GET /images/Charte/CharteWebCisco_06.gif HTTP/1.1
304	5.055175	172.16.1.10	172.16.104.38	HTTP	HTTP/1.1 200 OK (GIF89a)
305	5.055212	172.16.1.10	172.16.104.38	HTTP	Continuation
306	5.055254	172.16.104.38	172.16.1.10	TCP	3073 > http [ACK] Seq=732 Ack=27065 Win=64240 Len=0
307	5.059188	172.16.104.38	62.161.94.199	HTTP	GET /hit.xiti?s=59384&p=&hl=16x24x10&r=1024x768xundefinedx32&ref= HTTP/1.1
308	5.063936	172.16.104.38	172.16.1.10	HTTP	GET /images/Charte/CharteWebCisco_08.gif

Capture – Requête détaillée

No.	Time	Source	Destination	Protocol	Info
148	4.639100	172.16.104.38	172.16.1.10	HTTP	GET / HTTP/1.1
<p>Frame 148 (351 bytes on wire, 351 bytes captured) Arrival Time: Aug 23, 2004 16:24:10.595293000 Time delta from previous packet: 0.000188000 seconds Time since reference or first frame: 4.639100000 seconds Frame Number: 148 Packet Length: 351 bytes Capture Length: 351 bytes</p> <p>Ethernet II, Src: 00:0a:e6:bb:cf:8d, Dst: 00:e0:18:c3:59:3b Destination: 00:e0:18:c3:59:3b (172.16.1.10) Source: 00:0a:e6:bb:cf:8d (172.16.104.38) Type: IP (0x0800)</p> <p>Internet Protocol, Src Addr: 172.16.104.38 (172.16.104.38), Dst Addr: 172.16.1.10 (172.16.1.10) Version: 4 Header length: 20 bytes Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00) 0000 00.. = Differentiated Services Codepoint: Default (0x00) 0. = ECN-Capable Transport (ECT): 0 0 = ECN-CE: 0 Total Length: 337 Identification: 0x08e4 (2276) Flags: 0x04 (Don't Fragment)</p>					

```
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: TCP (0x06)
Header checksum: 0x2f72 (correct)
Source: 172.16.104.38 (172.16.104.38)
Destination: 172.16.1.10 (172.16.1.10)
Transmission Control Protocol, Src Port: 3072 (3072), Dst Port: http (80), Seq: 1, Ack: 1, Len: 297
Source port: 3072 (3072)
Destination port: http (80)
Sequence number: 1 (relative sequence number)
Next sequence number: 298 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x0018 (PSH, ACK)
0... .... = Congestion Window Reduced (CWR): 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
.... ...0 = Fin: Not set
Window size: 64240
Checksum: 0x9668 (correct)
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Request Method: GET
Accept: */*\r\n
Accept-Language: fr\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)\r\n
Host: www.labo-cisco.com\r\n
Connection: Keep-Alive\r\n
Cache-Control: no-cache\r\n
Cookie: ASPSESSIONIDCQTRQQQB=PLCMIDDAPCCHGFEBDBIJFFAI\r\n\r\n
```

- Quels sont les ports utilisés pour la communication au cours de la requête ?

- Quelle est la taille de la fenêtre initiale ?

- Pourquoi deux accusés de réception sont présents ?

- Quelle est la différence entre les trames TCP et UDP ?

- Citez un exemple d'utilisation des segments UDP :

- Analyse de transmission

- Edward veut transférer un fichier à Bill par Microsoft messenger.
- Le transfert démarre à une vitesse de 115 Kbits/s.
- Pendant le transfert, Bill lance une application peer to peer, gourmande en bande passante.
- Edward voit alors le débit de son envoi diminuer à 25 Kbits/s.
- Il en averti aussitôt Bill qui ferme son application puis termine le téléchargement.
- Expliquer ce qui se passe au niveau du fenêtrage lors des 3 différentes étapes du transfert :

Explication

8.3. Exercice 2 – Recherches et documentation

- Expliquez le principe de l'algorithme MD5 :

MD5

- Qu'est-ce qu'un VPN ? Quel est son principe de fonctionnement, son utilité ?

VPN



- Décryptez le message suivant. L'algorithme utilisé est celui du chiffre de César :

Code

FY FUVILUNICLY MOJCHZI XYM NYWBHIFIACYM WCMWI PIOM LYGYLWCY X'UPICL
XYWIXY WY GYMMUAY.

8.4. Exercice 3 – Analyse de données

- Une requête Web sur la page <http://www.labo-cisco.com> (172.16.1.10) a été capturée depuis un ordinateur ayant pour IP 172.16.104.38. Nous allons nous intéresser aux informations HTTP.

Capture – Trafic des requêtes

No.	Time	Source	Destination	Protocol	Info
275	4.892953	172.16.104.38	172.16.1.10	TCP	3073 > http [ACK] Seq=364 Ack=20441 Win=52560 Len=0
276	4.893038	172.16.1.10	172.16.104.38	HTTP	Continuation
277	4.893163	172.16.1.10	172.16.104.38	HTTP	Continuation
278	4.893200	172.16.104.38	172.16.1.10	TCP	3073 > http [ACK] Seq=364 Ack=23361 Win=49640 Len=0
279	4.893286	172.16.1.10	172.16.104.38	HTTP	Continuation
280	4.893335	172.16.1.10	172.16.104.38	HTTP	Continuation
281	4.893365	172.16.104.38	172.16.1.10	TCP	3073 > http [ACK] Seq=364 Ack=25409
288	5.003410	172.16.104.38	172.16.1.10	TCP	[TCP Dup ACK 281#1] 3073 > http [ACK] Seq=364 Ack=25409 Win=51352 Len=0
289	5.013453	172.16.1.10	172.16.104.38	TCP	http > 3072 [ACK] Seq=80437 Ack=1373 Win=16148 Len=0
290	5.013492	172.16.1.10	172.16.104.38	TCP	http > 3073 [ACK] Seq=25409 Ack=364 Win=17157 Len=0
291	5.022946	172.16.104.38	172.16.1.10	TCP	3072 > http [ACK] Seq=1373 Ack=80437 Win=63184 Len=0
292	5.027996	172.16.104.38	172.16.1.10	TCP	[TCP Dup ACK 281#2] 3073 > http [ACK] Seq=364 Ack=25409 Win=64240 Len=0
293	5.040306	172.16.104.38	172.16.1.10	HTTP	GET /images/Charte/WebCisco_05N.gif HTTP/1.1
294	5.041092	172.16.1.10	172.16.104.38	HTTP	HTTP/1.1 200 OK (GIF89a)
295	5.041184	172.16.1.10	172.16.104.38	HTTP	Continuation
296	5.041230	172.16.104.38	172.16.1.10	TCP	3072 > http [ACK] Seq=1736 Ack=83045 Win=64240 Len=0
301	5.053659	62.161.94.199	172.16.104.38	TCP	http > 3074 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1460
302	5.053703	172.16.104.38	62.161.94.199	TCP	3074 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
303	5.054444	172.16.104.38	172.16.1.10	HTTP	GET /images/Charte/CharteWebCisco_06.gif HTTP/1.1
304	5.055175	172.16.1.10	172.16.104.38	HTTP	HTTP/1.1 200 OK (GIF89a)
305	5.055212	172.16.1.10	172.16.104.38	HTTP	Continuation
306	5.055254	172.16.104.38	172.16.1.10	TCP	3073 > http [ACK] Seq=732 Ack=27065 Win=64240 Len=0
307	5.059188	172.16.104.38	62.161.94.199	HTTP	GET /hit.xiti?s=59384&p=&hl=16x24x10&r=1024x768xundefinedx32&ref= HTTP/1.1
308	5.063936	172.16.104.38	172.16.1.10	HTTP	GET /images/Charte/CharteWebCisco_08.gif

Capture – Requête détaillée

No.	Time	Source	Destination	Protocol	Info
148	4.639100	172.16.104.38	172.16.1.10	HTTP	GET / HTTP/1.1

Frame 148 (351 bytes on wire, 351 bytes captured)
 Arrival Time: Aug 23, 2004 16:24:10.595293000
 Time delta from previous packet: 0.000188000 seconds
 Time since reference or first frame: 4.639100000 seconds
 Frame Number: 148
 Packet Length: 351 bytes
 Capture Length: 351 bytes

Ethernet II, Src: 00:0a:e6:bb:cf:8d, Dst: 00:e0:18:c3:59:3b
 Destination: 00:e0:18:c3:59:3b (172.16.1.10)
 Source: 00:0a:e6:bb:cf:8d (172.16.104.38)
 Type: IP (0x0800)

Internet Protocol, Src Addr: 172.16.104.38 (172.16.104.38), Dst Addr: 172.16.1.10 (172.16.1.10)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 0000 00.. = Differentiated Services Codepoint: Default (0x00)
 0. = ECN-Capable Transport (ECT): 0
 0 = ECN-CE: 0
 Total Length: 337
 Identification: 0x08e4 (2276)
 Flags: 0x04 (Don't Fragment)
 0... = Reserved bit: Not set
 .1.. = Don't fragment: Set
 ..0. = More fragments: Not set
 Fragment offset: 0
 Time to live: 128
 Protocol: TCP (0x06)
 Header checksum: 0x2f72 (correct)
 Source: 172.16.104.38 (172.16.104.38)
 Destination: 172.16.1.10 (172.16.1.10)

Transmission Control Protocol, Src Port: 3072 (3072), Dst Port: http (80), Seq: 1, Ack: 1, Len: 297
 Source port: 3072 (3072)
 Destination port: http (80)
 Sequence number: 1 (relative sequence number)
 Next sequence number: 298 (relative sequence number)
 Acknowledgement number: 1 (relative ack number)
 Header length: 20 bytes
 Flags: 0x0018 (PSH, ACK)
 0... = Congestion Window Reduced (CWR): 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
 0 = Fin: Not set
 Window size: 64240
 Checksum: 0x9668 (correct)

Hypertext Transfer Protocol
 GET / HTTP/1.1\r\n

```
Request Method: GET
Accept: */*\r\n
Accept-Language: fr\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)\r\n
Host: www.labo-cisco.com\r\n
Connection: Keep-Alive\r\n
Cache-Control: no-cache\r\n
Cookie: ASPSESSIONIDCQTRQQQB=PLCMIDDAPCCHGFEBDBIJFFAI\r\n\r\n
```

- Quelle instruction HTTP est utilisée pour récupérer une image sur le site ?

- Quel est le rôle des trames "Connections" ?

- En faisant un parallèle au protocole TCP, sous quelle forme se présente les acquittements dans les trames HTTP ?

- Quelle est la valeur du cookie envoyé par Xiti ?
