Ingénieur Réseau Apprentissage ESIEE
2011/2012

Introduction Réseaux – Topologies – Protocoles – Architectures en couches Modèles OSI, IEEE, TCP/IP

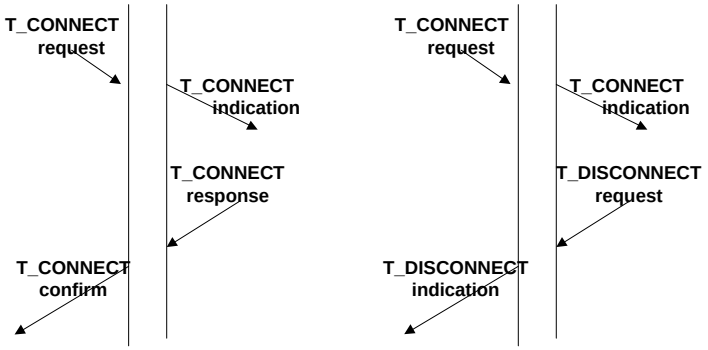
Travaux Dirigés

Catherine Bernard

Exercice 1 : Architectures en couches – Modèle OSI

1. Citer les couches du modèle OSI et préciser brièvement leurs fonctions principales.
2. Quel est le rôle des couches basses ? Quel est le rôle des couches hautes ?

   Les couches hautes sont dites « de bout en bout ». Que signifie cette expression ?
3. Qu'est-ce qu'une trame ?
4. Qu'appelle-t-on primitives de service et quelles sont les quatre primitives de service fondamentales ? Lesquelles sont utilisées en mode non connecté ?
   Commenter les figures suivantes.



5. Comment s'appelle la communication « virtuelle » entre 2 couches de même niveau ? Comment se passe réellement la communication entre 2 couches de même niveau ?
6. Dans le modèle OSI est ce que ce sont les TPDU qui encapsulent les paquets ou le contraire ? Que sont les TPDU ?
7. Topologies réseau

   a) Quelle différence faites-vous entre la topologie logique et la topologie physique ?
   b) On considère trois réseaux à commutation de paquets comportant chacun N nœuds (stations). Le premier est de type étoile avec un commutateur unique, le second a la forme d'un anneau bidirectionnel, le troisième est constitué de stations entièrement connectées deux à deux.
      - Expliquer le principe de la commutation par paquets.
      - Représenter chacune de ces topologies.
        Quel est pour chacun de ces réseaux le nombre de segments nécessaires à une mise en relation entre deux stations quelconques dans la situation la plus favorable et dans la situation la plus défavorable.
        Mettre en évidence les avantages et inconvénients de ces différentes topologies. Laquelle vous paraît la plus fiable ?

Exercice 2 : Imbrication de voies – Notion d'Encapsulation

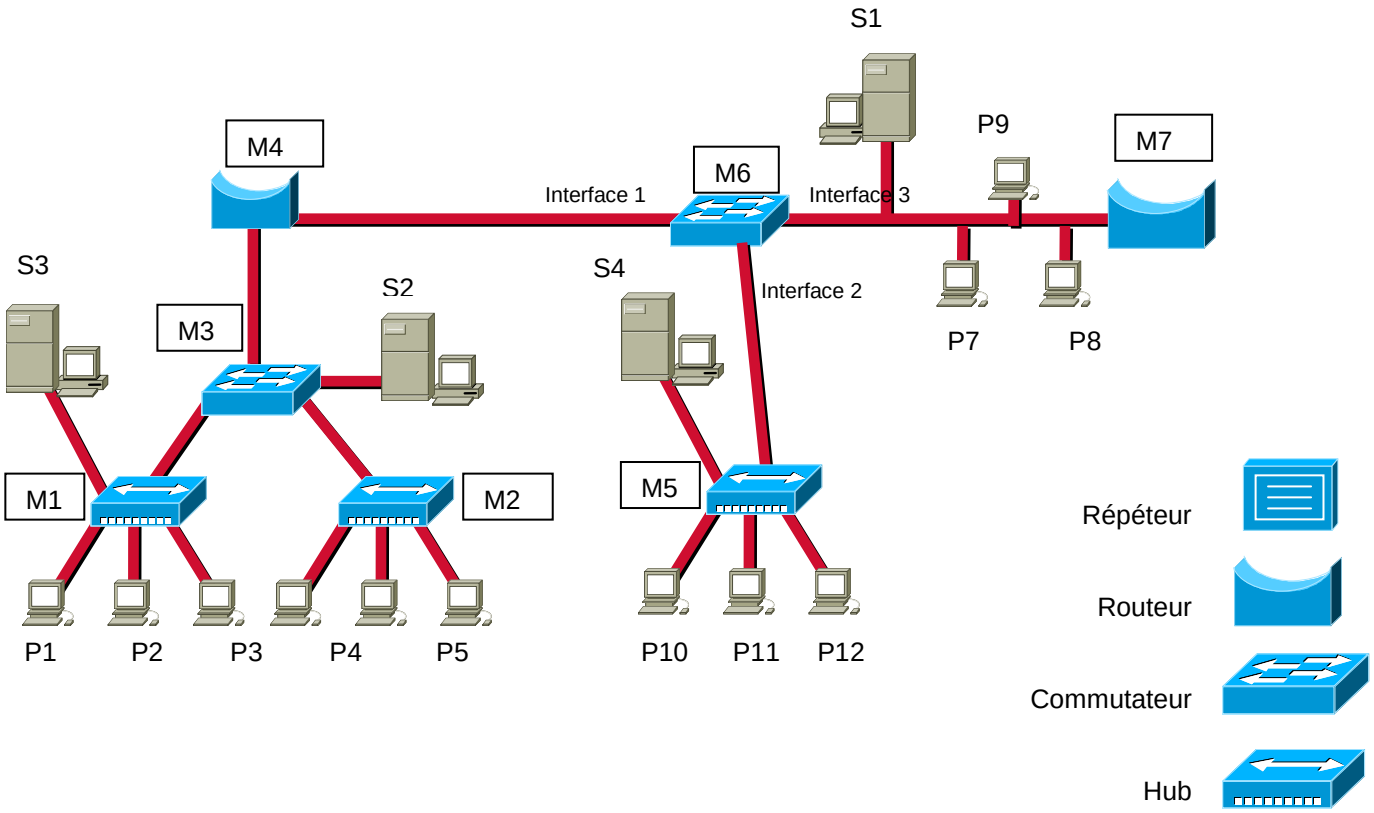
Une voie entre C et D offre un service sur connexion de niveau 3 (appelé X25). Une voie entre A et C et une seconde entre D et B offrent un service à datagramme de niveau 4 (pile de protocole appelée TCP/IP, TCP pour le niveau 4 – transport et IP pour le niveau 3 réseau). La taille des paquets sur la voie CD est limitée à 128 octets (à l'entrée du service). La taille des paquets sur les voies AC et DB est limitée à 1000 octets (à l'entrée du service). Pour les besoins de l'exercice, on suppose que chaque enveloppe, à chaque niveau, a une taille de 20 octets.

1. Peut-on construire une voie entre A et B ? Quelle solution proposez-vous pour construire une telle voie ? Représenter le modèle en couches de ce système d'interconnexion.
2. Un bloc de données de 50 octets est soumis par A pour B sur cette voie. Quel est le rendement du protocole ?

3. Un bloc de données de 1500 octets est soumis par A pour B. Sur la voie X25 (service de niveau 3), un mécanisme de fragmentation/réassemblage permet de soumettre des données de taille supérieure à 128 octets. Ces messages sont fragmentés en paquets de 128 octets puis réassemblés à l'arrivée de la voie X25. Le service X25 garantit le séquencement des paquets et la correction de pertes. Il offre un mécanisme qui permet d'identifier la fin de chaque bloc.
   Dans ce cas, quel est le nouveau rendement du protocole ?

Exercice 3 : Etude d'un réseau local

Soit un réseau local dont l'architecture est donnée par la figure suivante :



1. Indiquer pour chaque équipement d'interconnexion à quel niveau du modèle OSI correspond-il ?
2. Quelle est la topologie logique du hub ?
3. A quoi correspondent les adresses physiques dans un LAN ? Comment un commutateur Ethernet apprend-il les adresses physiques des machines présentes sur ses ports ?
4. P1 envoie une requête dont l'adresse MAC du destinataire est FF.FF.FF.FF.FF.FF., qui reçoit cette trame ?
5. Le poste P4 envoie une trame destinée au serveur S3. Citez tous les éléments qui vont recevoir la trame et précisez ce que chacun des éléments va faire de la trame reçue.
6. Le commutateur M6 reçoit une trame comportant en adresse MAC émetteur (MAC-P7). Il ne recopie pas la trame sur ses autres interfaces. Citez les adresses MAC destinataires possibles ? Justifiez votre réponse.
7. Donner la table de commutation de M6 en supposant que toutes les stations présentes sur le réseau ont au moins parlé une fois.
8. Sur le schéma du réseau représentez par un cercle le ou les domaines de collision
9. Si on remplace le routeur M4 par un commutateur, en quoi cela modifie-t-il les échanges entre les différents points du réseau ?

Exercice 4 : Adresses IP

1. Donner la classe d'adresse pour les adresses IP suivantes en expliquant pourquoi :

   172.16.8.127, 192.16.45.89, 25.25.25.25, 137.168.45.23, 193.165.28.68, 239.25.265.4

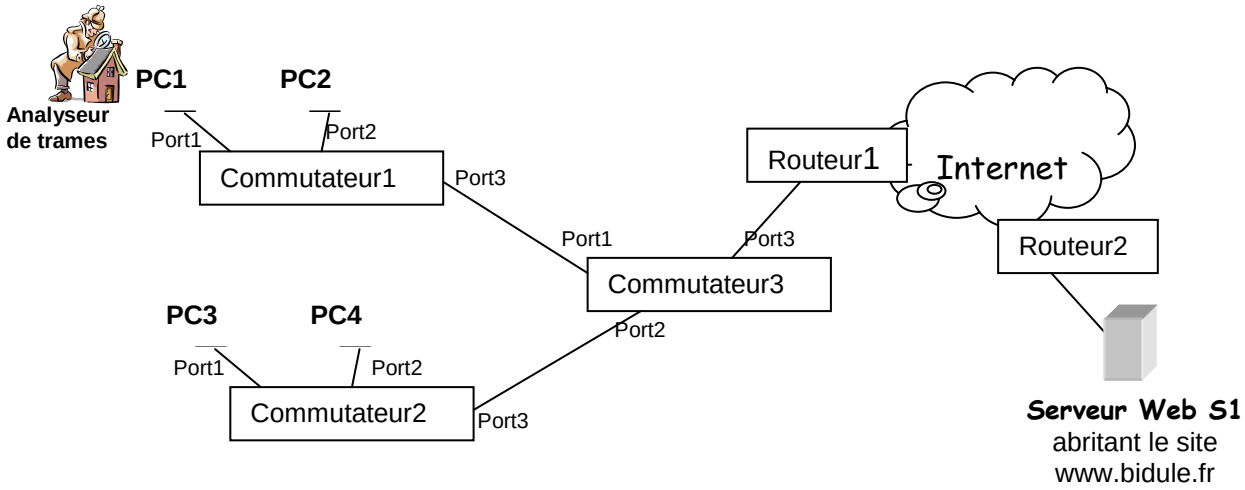
   Identifier la partie NetId et HostId pour chacune des adresses.

2. Parmi les adresses IP suivantes, donner celles qui sont affectées à un hôte (pour ces adresses, donner l'adresse réseau et l'adresse de broadcast associées). Si cette adresse n'est pas affectée à un hôte, expliquer pourquoi.

   - 131.107.256.80
   - 222.222.255.222
   - 231.200.1.1
   - 126.1.0.0
   - 0.127.4.100
   - 190.7.2.0
   - 127.1.1.1
   - 198.121.254.255
   - 255.255.255.255

Exercice 5 : Analyse de trame

Soit le réseau suivant :



Les PC1, 2, 3, 4, les commutateurs et le routeur1 sont sur un même réseau IP (adressage qui leur permet de communiquer entre eux)

Le tableau suivant donne pour chaque équipement son adresse MAC et son adresse IP.

PC1	@MAC1	@IP : 192.134.106.1
PC2	@MAC2	@IP : 192.134.106.2
PC3	@MAC3	@IP : 192.134.106.3
PC4	@MAC4	@IP : 192.134.106.4
Commutateur1	@MAC commut1	@IP : 192.134.106.10
Commutateur2	@MAC commut2	@IP : 192.134.106.11
Commutateur3	@MAC commut3	@IP : 192.134.106.12
Routeur1	@MAC routeur1	@IP : 192.134.106.100
Serveur S1	@MAC S1	@IP : 194.52.130.1

1. Quelle différence y a-t-il entre les adresses physiques de la trame Ethernet et les adresses logiques du paquet IP ?

2. Vous allez utiliser un analyseur de trame pour observer le trafic du réseau. Comment fonctionne un analyseur de trame ?

   Quel est le champ d'une trame Ethernet qui va permettre par exemple de différencier les trames ARP des trames de ping (demande et réponse d'écho) ?

Vous êtes connecté sur le PC1, vous observez le trafic du réseau à l'aide d'un analyseur de trames.

A partir de vos observations, complétez pour les échanges suivants les champs adresse source, adresse destination IP et MAC.

Demande d'écho du PC1 vers le PC2 (ping)

Trame1 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Requête ARP

Trame2 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Réponse ARP

Trame3 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Echo requête

Trame4 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Echo réponse

Demande d'écho du PC1 vers le site www.bidule.fr (ping)

Trame1 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Requête ARP *Address Resolution Protocol*

Trame2 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Réponse ARP

Trame3 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Echo requête

Trame4 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Echo réponse

Demande d'écho du PC1 vers le site PC4 (ping)

Trame1 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Echo requête

Trame2 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Echo réponse

Demande d'écho du PC2 vers le site PC4 (ping)

Trame1 :

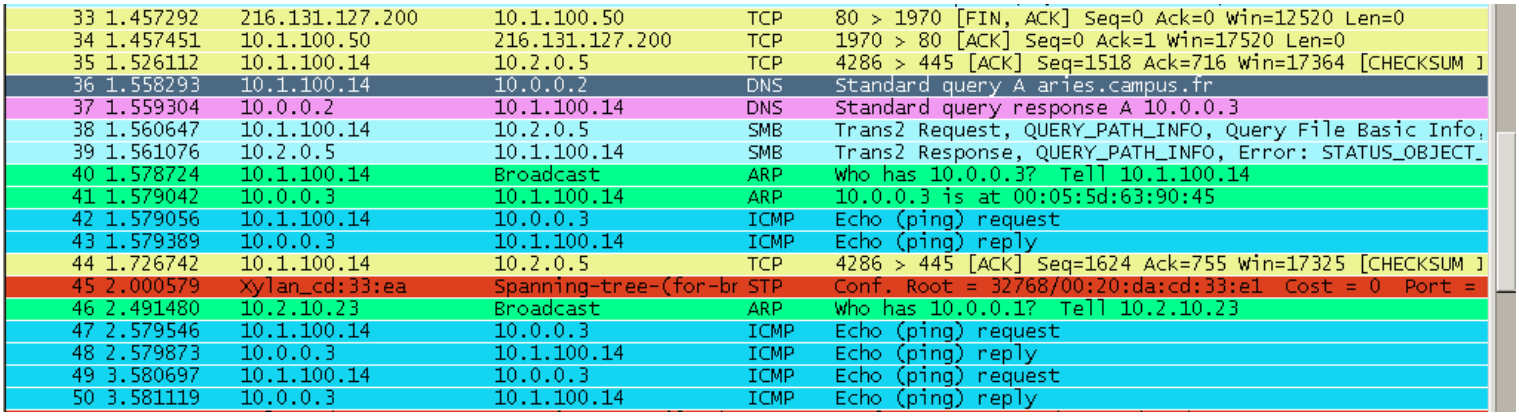
@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Echo requête

Trame2 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Echo réponse

Le fait de ne pas avoir fait figurer de trames ARP dans les deux derniers échanges, que cela signifie-t-il ? Quel est le rôle de l'ARP ?

3. Le résultat d'une capture de trame est le suivant :



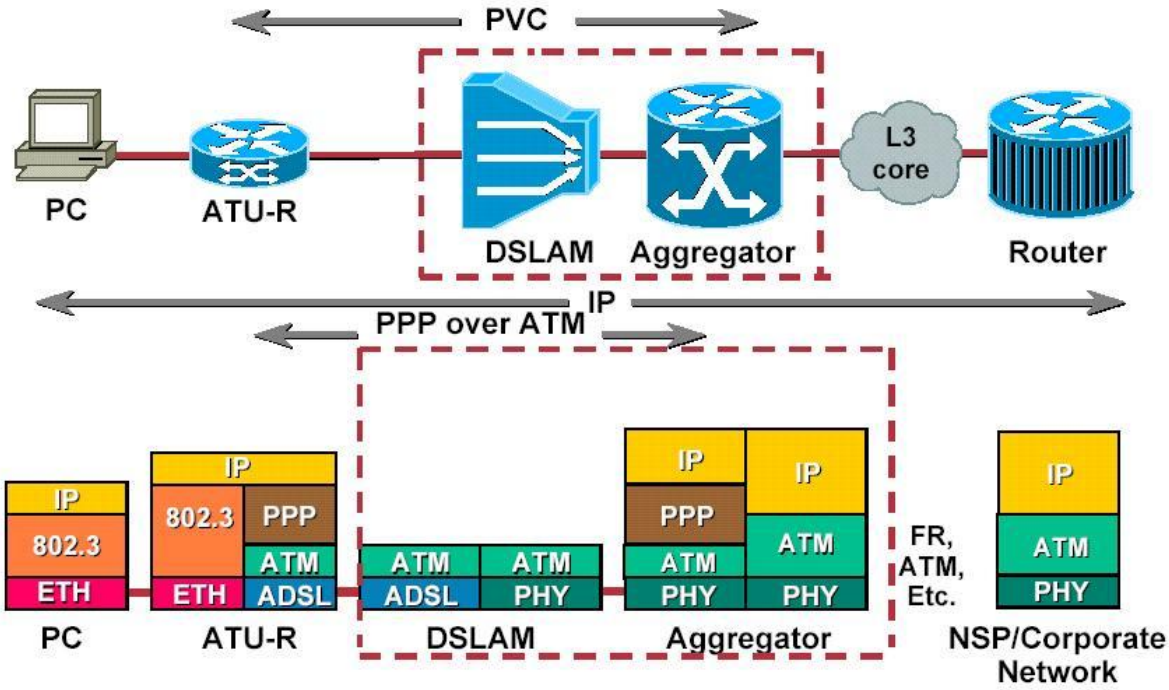
33 1.457292	216.131.127.200	10.1.100.50	TCP	80 > 1970 [FIN, ACK] Seq=0 Ack=0 Win=12520 Len=0
34 1.457451	10.1.100.50	216.131.127.200	TCP	1970 > 80 [ACK] Seq=0 Ack=1 Win=17520 Len=0
35 1.526112	10.1.100.14	10.2.0.5	TCP	4286 > 445 [ACK] Seq=1518 Ack=716 Win=17364 [CHECKSUM]
36 1.558293	10.1.100.14	10.0.0.2	DNS	Standard query A aries.campus.fr
37 1.559304	10.0.0.2	10.1.100.14	DNS	Standard query response A 10.0.0.3
38 1.560647	10.1.100.14	10.2.0.5	SMB	Trans2 Request, QUERY_PATH_INFO, Query File Basic Info,
39 1.561076	10.2.0.5	10.1.100.14	SMB	Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_
40 1.578724	10.1.100.14	Broadcast	ARP	Who has 10.0.0.3? Tell 10.1.100.14
41 1.579042	10.0.0.3	10.1.100.14	ARP	10.0.0.3 is at 00:05:5d:63:90:45
42 1.579056	10.1.100.14	10.0.0.3	ICMP	Echo (ping) request
43 1.579389	10.0.0.3	10.1.100.14	ICMP	Echo (ping) reply
44 1.726742	10.1.100.14	10.2.0.5	TCP	4286 > 445 [ACK] Seq=1624 Ack=755 Win=17325 [CHECKSUM]
45 2.000579	Xylan_cd:33:ea	Spanning-tree-(for-br	STP	Conf. Root = 32768/00:20:da:cd:33:e1 Cost = 0 Port =
46 2.491480	10.2.10.23	Broadcast	ARP	Who has 10.0.0.1? Tell 10.2.10.23
47 2.579546	10.1.100.14	10.0.0.3	ICMP	Echo (ping) request
48 2.579873	10.0.0.3	10.1.100.14	ICMP	Echo (ping) reply
49 3.580697	10.1.100.14	10.0.0.3	ICMP	Echo (ping) request
50 3.581119	10.0.0.3	10.1.100.14	ICMP	Echo (ping) reply

Analyse des trames 36-37-40 à 43

- Quel est le rôle du DNS ? Quelle est l'adresse du serveur DNS pour ce réseau ? Sur quel protocole de transport repose le DNS ?
- Quels sont les deux protocoles de la couche transport et quelle et leur différence ?
- Quelle commande a généré ces trames ? Depuis quelle machine cette commande a-t-elle été lancée ?
- Cette communication est-elle restée sur le LAN ou est-elle sortie du LAN ? Expliquer.

Exercice 6 : Etude d'une architecture ADSL

L'architecture d'un accès ADSL est représentée sur la figure suivante :



ADSL : Asymetric Digital Subscriber Line
ATM : Asynchronous Transfer Mode
ATU-R : ADSL Transfer Unit-Remote
DSLAM : Digital Subscriber Line Multiplexer
PPPoA : Point to Point Protocol over ATM
PVC : Permanent Virtual Channel

Le PC client est connecté sur un LAN de type **Ethernet**, et accède au réseau ADSL via un routeur (ATU-R). Le réseau d'accès s'appuie sur une technologie **ATM.** Le routeur ATU-R, afin de faciliter l'interconnexion au réseau ATM utilise un protocole du type **PPP over ATM.**

L'objectif de cet exercice est d'étudier chaque partie de ce système d'interconnexion.

1. Etude du LAN client

Le PC utilisateur est connecté à un réseau local type Ethernet.

1.1. Architectures de câblage d'Ethernet

1.1.1. Les premières architectures de réseaux locaux reposaient sur des réseaux de type 10Base2 (10Mbit/s Bande de Base sur câbles coaxiaux, 200m max) et 10BaseT (10Mbit/s Bande de Base sur câbles paires torsadées) avec un hub.
Que signifie « bande de base » ?
Quelle est la topologie logique de ces deux architectures de câblage ?

1.1.2. La passage aux architectures utilisant un hub a-t-il modifié le fonctionnement du protocole d'accès CSMA/CD. Expliquer. Rappeler le principe de fonctionnement du CSMA/CD.

1.1.3. Les architectures ont évolué avec l'utilisation de commutateur. En quoi l'utilisation de commutateur améliore-t-elle les performances sur un LAN ?

1.1.4. Le tableau ci-dessous donne les caractéristiques d'un commutateur Ethernet du constructeur Cisco.

Cisco Catalyst 2950C-24
Commutateur - 24 ports - EN, Fast EN - 10Base-T, 100Base-TX + 2x1000BaseFX (uplink) - 1 U externe

Description du produit	Cisco Catalyst 2950C-24 - commutateur - 24 ports
Caractéristiques	Surveillance de réseau, Fonction duplex intégral, uplink, Prise en charge du réseau local (LAN) virtuel, Contrôle de flux, Administrable, Empilable
Dimensions (LxPxH) – Poids	44.5 cm x 24.2 cm x 4.4 cm - 3 kg
Alimentation	CA 110/230 V CA 110/220 V ± 10% (50/60 Hz)
Nombre de ports	24 x Ethernet 10Base-T, Ethernet 100Base-TX Autosense - 1 port de gestion
Protocole de liaison de données	Ethernet, Fast Ethernet, Gigabit Ethernet
Normes	IEEE 802.3, IEEE 802.3U, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.3x, IEEE 802.1x
Mode de communication	Semi-duplex, duplex intégral
Mode de configuration console	9600 8N1
Ports réseau auxiliaires	2x1000BaseFX (uplink)
Taille de la table d'adresses MAC	8 000 entrées

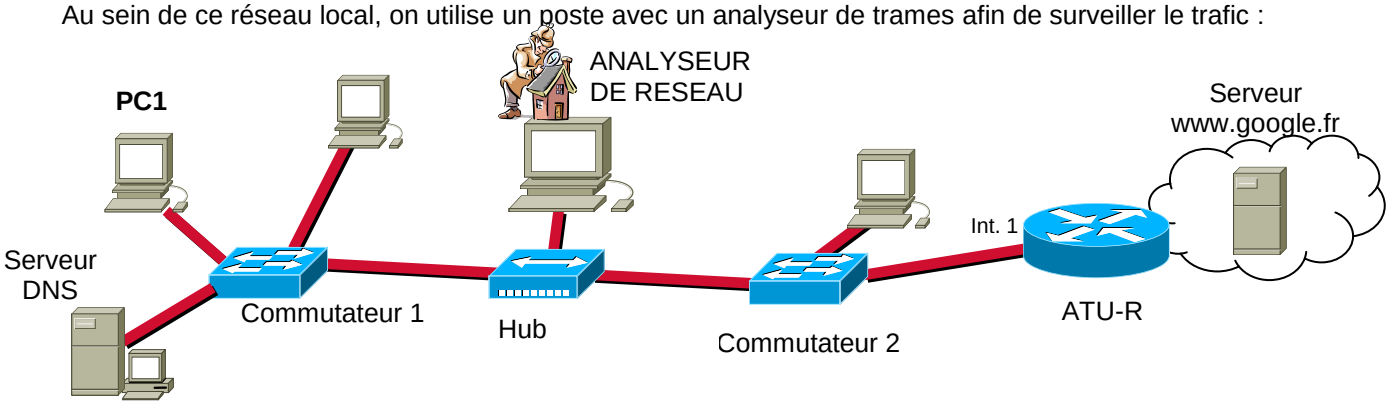
a) Quel est le rôle de la fonction contrôle de flux sur le commutateur ? Quelle est la différence entre contrôle de flux et contrôle de congestion ?
La technique consistant à détruire des trames qui risqueraient de faire « déborder » le buffer du commutateur est-elle un contrôle de flux ou un contrôle de congestion ?

b) Le port de gestion est de quel type ? Quel type de câble utilisez-vous pour ce port de gestion ?
Quelles sont les différentes techniques pour manager un commutateur ?
Que signifie la définition donnée au mode de configuration console ?

c) Les ports Ethernet 10BaseT, 100BaseTx sont qualifiés d'Autosense, que cela signifie-t-il ?

d) Mécanismes de surveillance du réseau local

Au sein de ce réseau local, on utilise un poste avec un analyseur de trames afin de surveiller le trafic :



Le tableau suivant donne les adresses MAC et IP de chacun des éléments connectés à ce réseau.

Eléments concernés	**Adresse MAC**	**Adresse IP**
PC1	@MAC1	192.168.0.1/24
PC Analyseur Réseau	@MAC2	192.168.0.200/24
Commutateur1	@$MAC_{commut1}$	192.168.0.100/24
Commutateur2	@$MAC_{commut2}$	192.168.0.200/24
Routeur (interface1)	@$MAC_{routeur1}$	192.168.0.254/24
Serveur DNS	@MAC_{DNS}	192.168.0.253/24

1.1.5. Le routeur implémente une fonction de NAT. Quel est le rôle de cette fonction ? Justifier son utilisation.

1.1.6. Quel est le rôle du hub dans cette architecture ? Expliquer. Que se passe-t-il si on place l'analyseur réseau sur un des commutateurs ? Quelle autre solution pouvez vous préconiser afin de permettre la surveillance du réseau local. Expliquer.

1.1.7. Le PC1 lance une requête web vers le serveur www.google.fr.
Vous observez les requêtes échangées sur le lien entre les commutateurs 1 & 2. Remplissez alors les différents champs dans les échanges suivants :

Trame1 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Requête DNS

Trame2 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Réponse DNS

Trame3 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Requête ARP

Trame4 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Réponse ARP

Trame5 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Ouverture de connexion HTTP (vers www.google.fr)

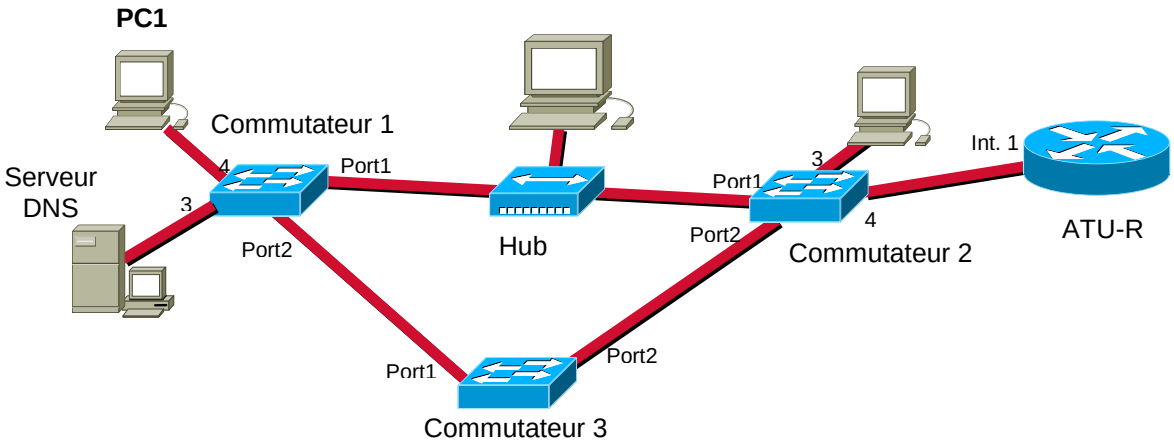
Trame6 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Acquittement de connexion HTTP (de (www.google.fr)

Pour chacun des protocoles observés ci-dessus, quel est le protocole de transport utilisé ? Expliquer.

1.2. Mécanismes de Spanning Tree dans le LAN

Afin d'améliorer la disponibilité du réseau, on ajoute un commutateur supplémentaire (commutateur 3) raccordé aux commutateurs 1 et 2, ce qui permet de créer un lien de secours.



1.2.1. Comment fonctionne la construction des tables de commutation ? La construction de la table de commutation est-elle indépendante du Spanning Tree ? Expliquer.
Que se passe-t-il au niveau de cette table de commutation si l'algorithme de Spanning Tree n'est pas activé ?

1.2.2. Election du commutateur racine à partir des données suivantes :

Commutateur 1 : @MAC 00-B0-D7-00-00-01, Identificateur 001B00B0D7000001
Commutateur 2 : @MAC 00-B0-D7-00-00-02, Identificateur 000A00B0D7000002
Commutateur 3 : @MAC 00-B0-D7-00-00-03, Identificateur 800000B0D7000003

Pour cette architecture, l'algorithme de Spanning Tree permet d'élire un commutateur racine, qu'est-ce qu'un commutateur racine ?
D'après les données précédentes, qui est élu le commutateur racine. Expliquer votre raisonnement.

1.2.3. Chaque commutateur a conservé les paramètres par défaut de configuration du Spanning Tree à savoir un coût de 19 et une priorité de 128.

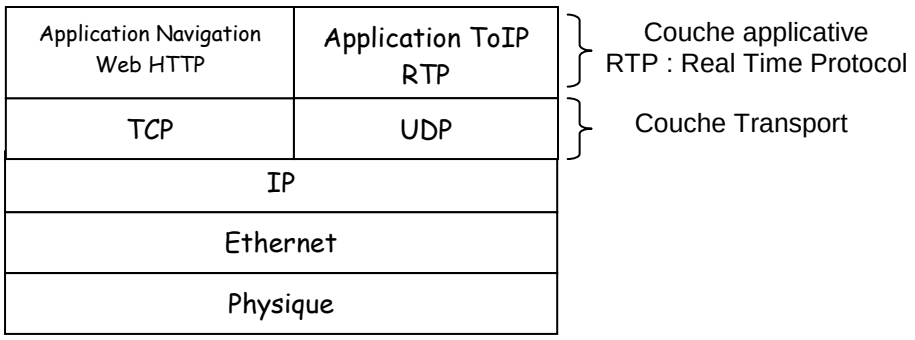
Commutateur N : $Port_x$ coût 19 priorité 128, $Port_y$ coût 19 priorité 128

Qu'est ce qu'un port racine ? Comment est-il choisi ? Quels sont pour chaque commutateur les ports racines
Quel port est alors inhibé ? Expliquer.

1.2.4. Après un fonctionnement suffisamment long du réseau (algorithme de Spanning Tree déroulé, chaque station a parlé au moins une fois), donner pour chaque commutateur sa table de commutation.

1.3. Application ToIP au sein du LAN

On profite du lien ADSL entièrement dégroupé pour faire au sein du LAN de la Téléphonie sur IP. Sur le poste client, l'architecture protocolaire de l'application de **ToIP (Telephony over IP)** est la suivante :



1.3.1. Le protocole RTP utilise les services de UDP. Justifier ce choix.

1.3.2. Existe-t-il dans le modèle OSI la notion de qualité de service ? Si oui, à quel niveau ? Quels sont les critères de qualité de service à assurer pour le transfert de la voix ? En déduire alors les fonctionnalités que devra fournir le protocole RTP pour cette application de ToIP.

1.3.3. Les primitives de transport sont données ci-dessous :

```
T_CONNECT.request                T_CONNECT.response
T_CONNECT.indication             T_CONNECT.confirm
T_DATA.request                   T_DATA.indication
T_DISCONNECT.request             T_DISCONNECT.indication
```

Rappeler le rôle des primitives de services.
Représenter sur un schéma l'enchaînement de ces primitives correspondant à la navigation web. Celles correspondant à l'application de ToIP.

2. Le réseau d'accès

2.1. Caractéristiques du réseau ADSL

2.1.1. Expliquer en quelques mots les techniques de transmission utilisées pour une transmission ADSL (on suppose que le lien autorise une transmission de Triple&Play)

2.1.2. La technologie ReADSL (Reach extended ADSL) consiste à apporter plus de puissance aux basses fréquences exploitées pour une liaison ADSL. Quel est l'intérêt d'utiliser cette technique ? Pourquoi ne pas avoir augmenté la puissance sur toute la bande de fréquence ADSL ?

2.2. Les protocoles du réseau d'accès

2.2.1. Le protocole PPP (Point to Point Protocol)

Le protocole PPP est une adaptation du format de trame de niveau 2 aux spécificités d'une liaison avec un modem. Le format de la PPP-PDU est donné figure suivante :

1 octet	1 octet	2 octets	2 octets	N octets	2 octets	1 octet
Fanion 01111110	adresse	contrôle	protocole	PPP-SDU	CRC	Fanion 01111110

a) Qu'est ce qu'une PDU ? Expliquer le lien entre PDU et SDU, le principe d'encapsulation. Est ce que ce sont les R-PDU qui encapsulent les PPP-PDU ou le contraire ?

b) Quel est le rôle du fanion ? En fonction de la séquence choisie pour le fanion (01111110), que doit-on faire au niveau de la PPP-SDU ?

2.2.2. Le protocole ATM

a) Le réseau ATM est un réseau haut débit **à commutation de cellules orienté connexion**. Expliquer cette phrase.

b) Une application de type voix fait appel au niveau du réseau ATM à un service de type Emulation de circuits, que cela signifie-t-il ?

2.3. Calcul du rendement de cette interconnexion

Afin d'optimiser cette interconnexion, le protocole PPPoA adapte la taille des données afin que le nombre d'octets de la PPP-PDU soit multiple de 48 octets, taille des données de la cellule ATM.

Calculer le rendement si on envoie un fichier de taille **400 octets** via un accès web.

Les en-têtes des différentes couches ont les tailles suivantes :

- NIVEAU TCP : En-têtes ajoutées par la couche TCP de taille 20 octets.
- NIVEAU IP : En-têtes ajoutées par la couche IP de taille 20 octets.
- NIVEAU MAC : En-têtes ajoutées par la couche MAC de taille 20 octets.
  La taille des données d'une trame Ethernet est au maximum de 1500 octets.
- FORMAT DE L'ATM – PDU (appelée aussi cellule) : En-tête de 5 octets pour une taille maximale de données de 48 octets (taille maximum d'une cellule : 53 octets).
- FORMAT DE LA PPP– PDU : Format donné ci-dessus, taille des données de sorte que la taille de la PPP-PDU soit multiple de 48 octets.
- NIVEAU PHYSIQUE : En tête de taille nulle.

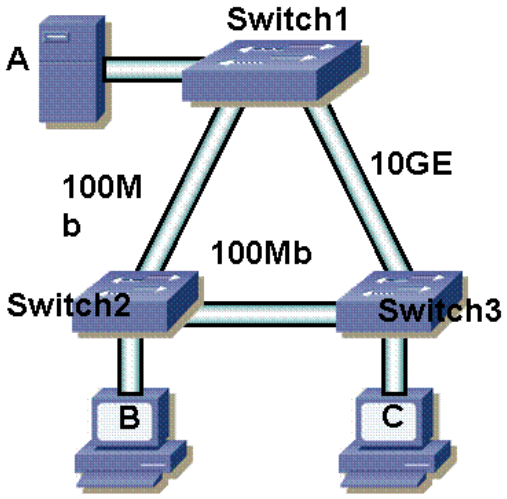
Exercice 7 : Les attaques de niveau 2

Cette exercice a pour objectif de mettre en évidence un certain nombre de vulnérabilités sur les commutateurs, et comprendre les configurations nécessaires à mettre en place pour se protéger de ces vulnérabilités.

1.1. Attaque de type Spanning Tree

1.1.1. Rappeler le rôle du Spanning Tree dans un réseau. Quel est le rôle des trames BPDU ?

1.1.2. Configuration du Spanning Tree
Soit le réseau suivant :



Quelle configuration devez-vous faire pour que le switch1 soit le switch racine ?

1.1.3. Une attaque consiste à générer des trames BPDU donnant de fausses infos aux commutateurs. Vous générez une trame BPDU indiquant que le switch racine est le switch 2 ? Que se passe-t-il ? Quelle conséquence sur le fonctionnement du réseau ?

2.2. Attaque MAC

2.2.1. La table de commutation d'un commutateur est-elle construite selon un mécanisme de signalisation ? Expliquer.

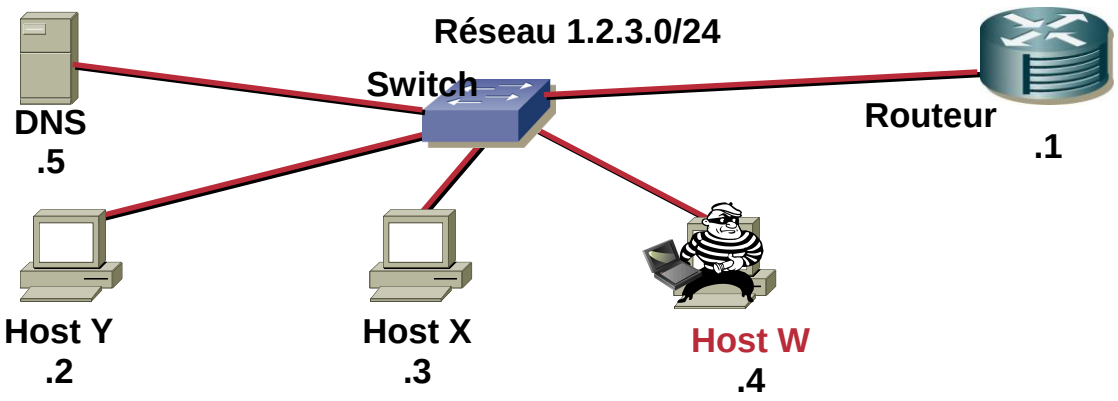
2.2.2. Quelle vulnérabilité peut exploiter un « hacker » afin que le switch se comporte comme un hub ?

2.2.3. Comment se prémunir de cette attaque ?

2.3. Attaque ARP

2.3.1. Rappeler le principe du protocole ARP. Quelles différences y a-t-il entre les adresses physiques de la trame Ethernet et les adresses logiques du paquet IP ?

2.3.2. Soit l'architecture suivante :



Hôte/Equipement	@MAC	@IP
X	$@MAC_X$	$@IP_X$
Y	$@MAC_Y$	$@IP_Y$
W	$@MAC_W$	$@IP_W$
Serveur DNS	$@MAC_{DNS}$	$@IP_{DNS}$
Switch	$@MAC_{Switch}$	$@IP_{Switch}$
Routeur	$@MAC_{Routeur}$	$@IP_{Routeur}$

Y est en train de « surfer sur le web ». Remplissez alors les champs adresses pour les trames suivantes (trames observées depuis le poste Y) :

Flux HTTP de Y vers le web

Trame1 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Requête DNS

Trame2 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Réponse DNS

Trame3 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Requête ARP

Trame4 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Réponse ARP

Trame5 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Requête HTTP

Trame6 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Réponses HTTP

Il existe la possibilité de construire des trames « `ARP who-as` », fonctionnant sur le même principe qu'une requête ARP classique. Un hôte envoie une requête ARP en indiquant : "Hello tout le monde, je suis l'hôte W avec l'adresse IP de la cible attaquée et l'adresse MAC celle du hacker".

W lance une requête « `ARP who-as` » avec le message suivant :
« Hello tout le monde, je suis l'hôte W avec l'adresse IP 1.2.3.1 et l'adresse MAC_W »

Que se passe-t-il alors au niveau des flux HTTP de Y vers le web.

2.3.3. Cette attaque est une attaque de type « Man in The Middle ». Expliquer. Que doit faire le « hacker » W pour que cette attaque soit transparente à l'utilisateur Y ?

2.3.4. Si dans votre réseau, vous avez mis en place des VLAN, cela constitue-t-il une protection vis-à-vis de cette attaque ? Expliquer.

3. Best Practices

Voici quelques règles de base afin d'assurer la sécurité sur l'utilisation des commutateurs. Pour chacune de ces règles, préciser la faille dont le système se protège.

Règle 1 : Utiliser des transmissions sécurisées pour manager les switchs.
Rappeler les différents modes vous permettant de manager un switch.

Règle 2 : Limiter le nombre d'adresses MAC possibles sur un port.

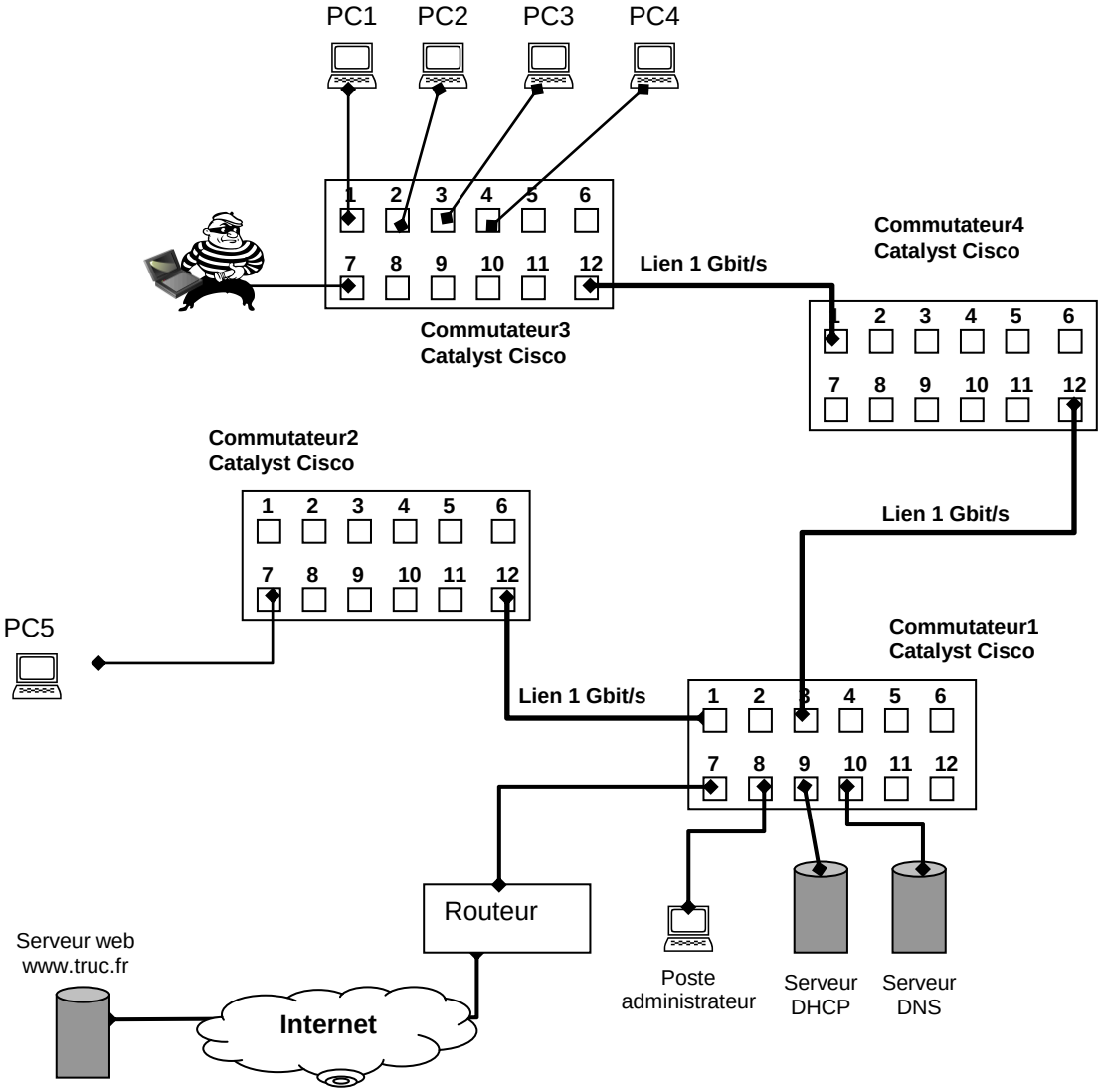
Règle 3 : Désactiver les ports non utilisés et les placer dans un VLAN non utilisé.

Règle 4 : Utiliser des VLAN avec des règles propres à chaque VLAN (Access List).

….

Exercice 8 : Etude d'une architecture réseau non sécurisée

Soit le réseau local suivant.
Un des utilisateurs en désaccord avec ses supérieurs souhaite se venger avant son départ en créant la pagaille dans ce réseau.... Comme l'administrateur de ce réseau n'est pas très doué, la tâche de ce hacker va être facilitée....



Le tableau suivant donne les adresses MAC et IP de chacun des éléments connectés à ce réseau.

Eléments concernés	Adresse MAC	Adresse IP
PC1	@MAC1	@IP1
PC2	@MAC2	@IP2
PC3	@MAC3	@IP3
PC4	@MAC4	@IP4
PC5	@MAC5	@IP5
Poste Hacker	$@MAC_{hacker}$	$@IP_{hacker}$
Poste Administrateur	$@MAC_{admin}$	$@IP_{admin}$
Commutateur1	$@MAC_{commut1}$	$@IP_{commut1}$
Commutateur2	$@MAC_{commut2}$	$@IP_{commut2}$
Commutateur3	$@MAC_{commut3}$	$@IP_{commut3}$
Commutateur4	$@MAC_{commut4}$	$@IP_{commut4}$
Routeur	$@MAC_{routeur}$	$@IP_{routeur}$
Serveur DNS	$@MAC_{DNS}$	$@IP_{DNS}$
Serveur DHCP	$@MAC_{DHCP}$	$@IP_{DHCP}$
Serveur web (www.truc.fr)	$@MAC_{WEB}$	$@IP_{WEB}$

1. Rappeler le principe de fonctionnement du CSMA/CD. Ce protocole fonctionne à quel niveau du modèle OSI ?
   En quoi l'utilisation de commutateur améliore-t-il les performances du CSMA/CD ? Expliquer.

2. Comment fonctionne la construction des tables de commutation ?
   En supposant que chaque machine s'est connectée au moins un fois au web, donner la table de commutation du commutateur 1 (le hacker ne s'est pas encore connecté au réseau).

3. Le hacker se branche sur le commutateur 3. Le serveur DHCP disposant d'une config de base fournit des paramètres réseaux à notre hacker.

   Quelles différences y a-t-il entre les adresses physiques de la trame Ethernet et les adresses logiques du paquet IP ?

   Quel est le rôle du DHCP? Quels sont les paramètres réseaux qui doivent être fournis à un utilisateur pour lui permettre d'accéder à des ressources réseau ?
   Quels conseils auriez vous donné à l'administrateur pour éviter que notre hacker récupère une adresse IP ?

4. Le hacker teste une première attaque consistant à faire en sorte que le commutateur se comporte comme un hub. Comment le hacker s'y est-il pris ? Expliquer.

5. Soit la trame suivante analysée au niveau de la couche MAC dans le réseau local de type Ethernet (ne figurent pas le préambule de synchronisation et l'octet SFD de la trame).

   Entourez la séquence envoyée à la couche **réseau**. Expliquez.
   Précisez quel est le protocole réseau utilisé. Précisez ensuite le protocole encapsulé dans le protocole réseau. Justifiez vos réponses.

Trame analysée :

00 4B 51 8C 23 26 00 80 AB 21 56 17 08 00 45 00 00 3C C6 47 00 00 80 01 5A ….. 29 AB 31 42 51

N octets

Séquence envoyée à la couche **réseau**, justifications :

.....

.....

Protocole de niveau réseau :

.....

.....

Protocole encapsulé par le protocole réseau :

.....

.....

6. Le hacker peut alors observer le trafic émis par les machines du réseau via un analyseur réseau. Il observe notamment le PC1 qui est en train de surfer sur le web. Remplissez alors les champs suivants pour les différents échanges du PC1 vers www.truc.fr

PCn°1 : requête web vers www.truc.fr

Trame1 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Requête DNS

Trame2 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Réponse DNS

Trame3 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Requête ARP

Trame4 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Réponse ARP

Trame5 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Requête web

Trame6 :

@ MAC destination	@ MAC source	@ IP source	@ IP destination	
				Acquittement pour la requête web

Rappeler le principe du protocole ARP. Quel est le rôle du DNS ?

Le protocole de transport d'une requête DNS est UDP, celui de HTTP est TCP.
Rappeler la différence entre ces deux protocoles et donner la justification de ces choix.

7. La mise en place de VLAN sur les commutateurs aurait-elle permis d'éviter cette attaque ? Expliquer la notion de VLAN, et justifier votre réponse.

8. Le hacker a pu récupérer l'adresse IP des commutateurs.
   Il se connecte au commutateur 1, et peut accéder au menu de configuration du commutateur (l'administrateur n'avait pas trouvé utile de changer les login/mot de passe par défaut).

   Peut-il accéder au switch en mode console ? Expliquer.
   Quels sont les différentes méthodes permettant d'accéder au menu de configuration du switch ?

9. Une fois connecté au commutateur 1, il lance les commandes suivantes :

```
Switch(config)# interface fastethernet0/10
Switch(config-if)# shutdown
*Sep 30 08:33:47: %LINK-10-CHANGED: Interface FastEthernet0/10, changed state to a
administratively down
```

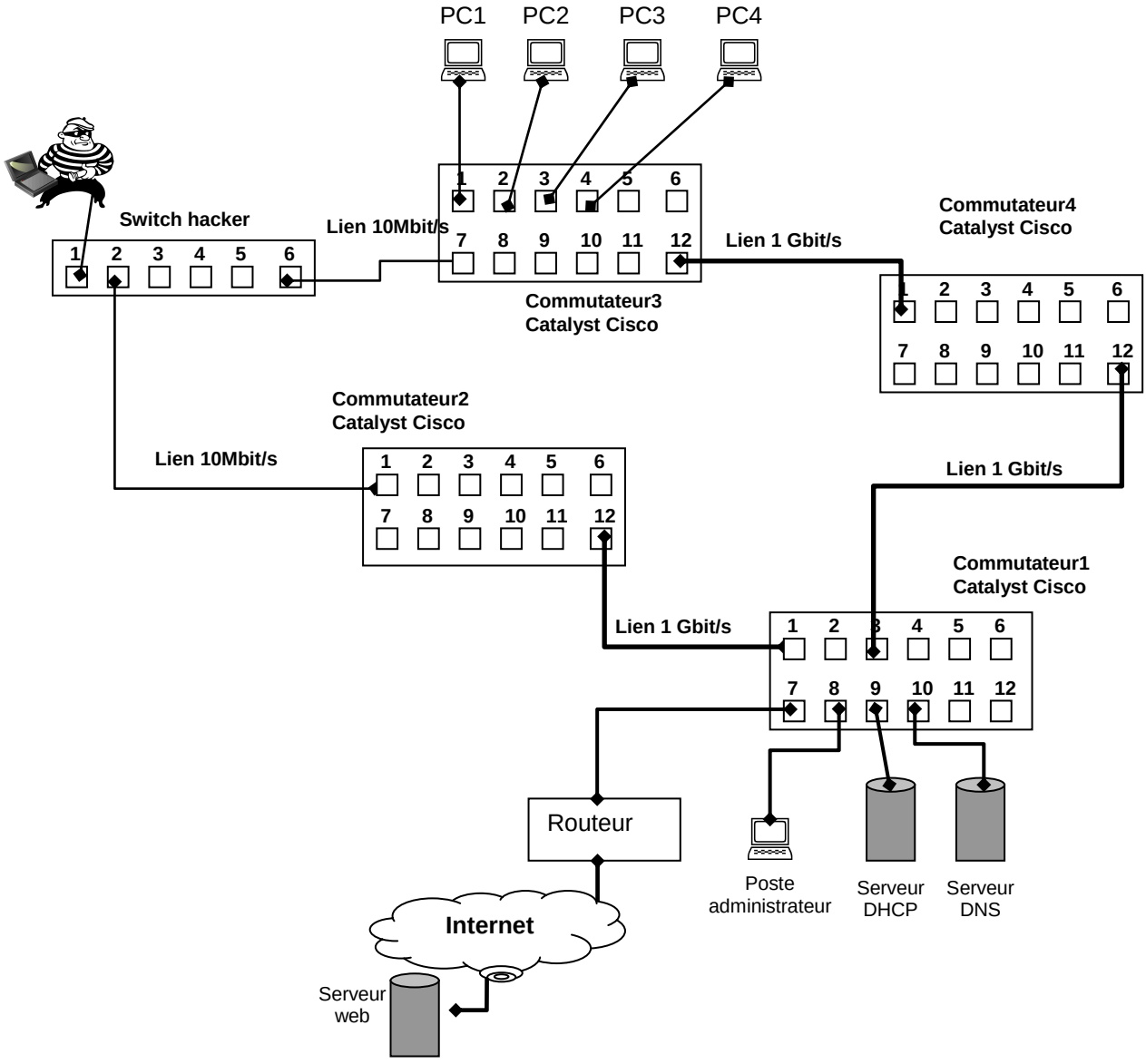
   Que se passe-t-il ? Quelle conséquence pour les utilisateurs du réseau ? Expliquer.

10. Notre administrateur revenu de sa pause café tente de résoudre le problème. Il lance un analyseur de trame installé sur son poste et fait quelques tests :
    - Ping @IP routeur : ce ping fonctionne-t-il ?
    - Même question avec un ping vers un serveur web quelconque.

    Il cherche alors à observer le trafic vers le routeur, quelles configurations doit-il mettre en œuvre ? Expliquer.

11. N'arrivant pas à se connecter, il adopte une solution assez radicale : reset du switch pour revenir aux paramètres usines.
    Cette manipulation fait perdre l'adresse IP au switch, cela pose-t-il problème dans le fonctionnement du LAN ? Expliquez.

12. Notre hacker modifie la topologie du réseau en ajoutant un nouveau switch dans le réseau.
    L'architecture du réseau est donnée ci-dessous.



Si le Spanning Tree n'est pas activé sur les commutateurs, que se passe-t-il ? Expliquer.

Le Spanning Tree était activé sur les commutateurs, avec les configurations par défaut. Quelle configuration doit faire notre hacker pour que l'ajout de son commutateur perturbe le fonctionnement du réseau. Expliquer.

ANNEXE 1 : Structure des unités de données

Trame Ethernet

INFORMATION	Taille
Préambule de synchronisation	7 octets
Délimiteur de début de trame Valeur 01111110	1 octet
Adresse physique de l'émetteur	6 octets
Adresse physique du récepteur	6 octets
Type de paquets (IP, Apple talk…)	2 octets
Données	Variable
Champ de contrôle calculé sur les données et l'en-tête	4 octets

Valeur du champ **Type**
0800_{hexa} ⇨ IP
0805_{hexa} ⇨ X25
0806_{hexa} ⇨ ARP
....

Paquet IP (datagramme IP)

INFORMATION	Taille
Version du protocole IP Longueur de l'en-tête	4 bits 4 bits
Type de service	1 octet
Taille du paquet	2 octets
Numéro du paquet	2 octets
Drapeau indiquant si la paquet est fragmenté + numéro du fragment	3 bits + 13 bits
TTL (time to live)	1 octet
Protocole	1 octet
Zone de contrôle d'erreur sur l'en-tête	2 octets
Adresse IP de l'émetteur (adresse logique)	4 octets
Adresse IP du récepteur (adresse logique)	4 octets
Données	Variable

Valeur du champ **Protocole**
1 ⇨ ICMP
2 ⇨ IGMP
6 ⇨ TCP
17 ⇨ UDP

Segment TCP

INFORMATION	Taille
Numéro de port émetteur	2 octets
Numéro de port récepteur	2 octets
Numéro de séquence	4 octets
Numéro d'acquittement	4 octets
Taille d'en-tête	4 bits
Réservé	6 bits
Code indiquant le type de paquet (urgent…)	6 bits
Quantité de bits que peut recevoir le destinataire sans attendre l'acquittement	2 octets
Calcul d'erreurs sur les données et l'en-tête	2 octets
Pointeur pour données urgentes	2 octets
Données	Variable

ANNEXE 2 : Classes d'adresses

Plages d'adresse pour les différentes classes :

Classe A	1.0.0.0-127.0.0.0
Classe B	128.0.0.0-191.255.0.0
Classe C	192.0.0.0-223.255.255.0
Classe D	224.0.0.0-239.255.255.255
Classe E	A partir de 240.0.0.0