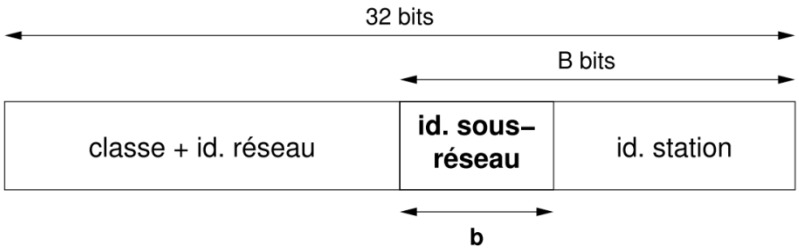
TD1. Partie I. Routage : règles de décision, sous-réseaux et tables de routage

Rappel. Le subnetting est une technique qui permet d'attribuer une seule adresse de réseau à plusieurs réseaux physiques, gérés par une seule organisation



Soit B le nombre de bits réservés que l'administrateur d'un réseau peut gérer.
Le nombre de bits b réservés à l'identifiant de sous-réseau dépend du nombre de sous-réseaux : s'il y a n sous-réseaux, alors le nombre de bits nécessaires est le plus petit b tel que $n \leq 2^b$
Puisque b bits sont réservés sur les B bits disponibles, il ne reste que B − b bits pour l'identifiant de station

Cas d'étude : un sous-réseau est constitué de machines dont l'adresse IP est dans l'intervalle 193.51.25.64 et 193.51.25.127 (B=8, b=2, n=2)

Calcul d'adresse réseau : on garde tel quel tous les bits de réseau et de sous-réseau, et on met les bits machine à 0
11000001 00110011 00011001 01000000 **193.51.25.64**

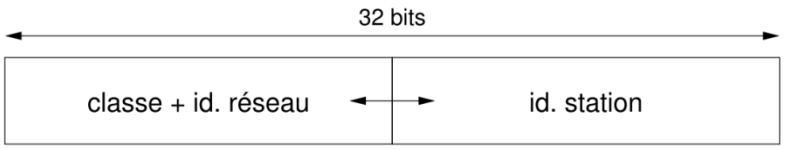
Calcul d'adresse de diffusion (broadcast) : on garde tel quel tous les bits de réseau et de sous-réseau, et on met les bits machine à 1
11000001 00110011 00011001 01111111 **193.51.25.127**

Calcul du masque : on met tous les bits de réseau et de sous-réseau à 1 et tous les bits machine à 0
11111111 11111111 11111111 11000000 **255.255.255.192**

Notation CIDR : adresse suivi d'un "/" et du nombre de bits de poids fort à 1 dans le masque de sous-réseau
193.51.25.64/26

Avec ce masque et l'adresse de son sous-réseau, il est aisé de savoir si la remise d'un datagramme doit être directe ou indirecte

---



Adresses privées :
10.0.0.0 à 10.255.255.255
172.16.0.0 à 172.31.255.255
192.168.0.0 à 192.168.255.255
169.254.0.0 à 169.254.255.255

Classes d'adresses IP
Classe A : 0 (0.0.0.0 à 127.255.255.255; /8; 255.0.0.0)
Classe B : 10 (128.0.0.0) à 191.255.255.255; /16; 255.255.0.0)
Classe C : 110 (192.0.0.0) à 223.255.255.255; /24; 255.255.255.0)

Exercice 1. Adresses IP sous forme binaire

Soient les 3 adresses IP suivantes, codées sur 32 bits, où les bits sont regroupés ici en octets pour en faciliter la lecture :

1. 10010011 11011000 01100111 10111110
2. 01101100 10100100 10010101 11000101
3. 11010110 01011100 10110100 11010001

Ecrivez chaque adresse en notation décimale pointée, déterminez sa classe, isolez sa partie classe+id, écrivez son adresse réseau en notation décimale pointée.

Exercice 2. Adresses IP en notation décimale pointée

Soient les 4 adresses IP suivantes, exprimées selon la notation décimale pointée :

1. 139.124.5.25
2. 194.199.116.255
3. 12.34.56.78

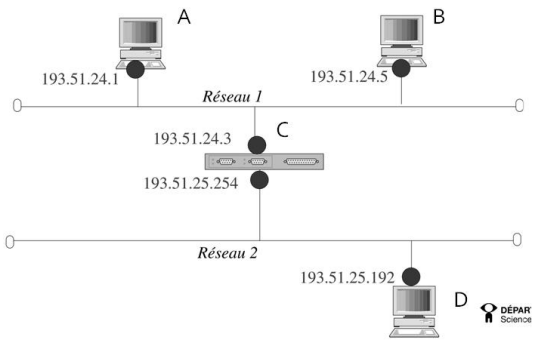
Calculez leur classe et en déduire leur adresse réseau en notation décimale pointée.

Exercice 3. Règles de décision

1.1 Ecrivez les adresses en binaires

1.2 Ecrivez les masques de sous-réseau en binaire

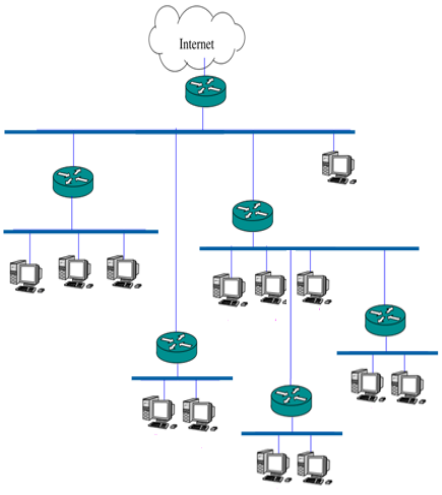
1.3 Appliquez la règle de décision de routage lorsque A communique avec B, C et D



Exercice 4. Subdivision des adresses réseau en sous-réseaux (subnetting)

A partir de l'adresse 194.167.235.0, pour le réseau ci-contre, construisez 6 adresses de sous-réseaux de taille identique

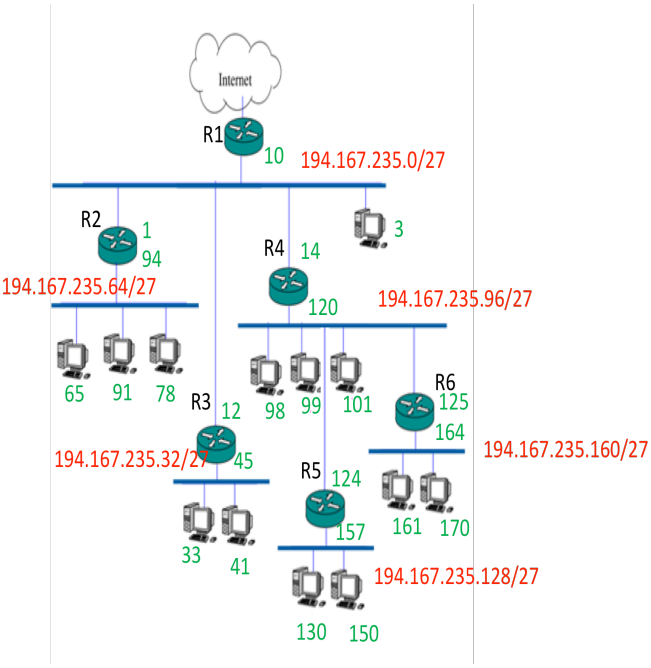
(remarque : déterminez B, n et b - cf. rappel en début de TD)



Exercice 5. Tables de routage

Construire la table de routage pour les hôtes des différents sous-réseaux (hors routeurs)

Les hôtes du sous-réseau 194.168.235.96/27 devront pouvoir accéder aux sous-réseaux 194.168.235.160/27 et 194.168.235.128/27



Hôte du réseau	adresse	Pour aller vers le réseau	Passer par	adresse
1				
2				
3				
4				
5				
6				

Construire la table de routage pour les routeurs.

Hôte	Pour aller vers le réseau	Passer par	
R1	194.168.235.32/27	194.168.235.12	R3 ext
R2			

Partie II. Attaque du protocole ARP

Introduction

Une des attaques man in the middle les plus célèbres consiste à exploiter une faiblesse du protocole ARP (Address Resolution Protocol) dont l'objectif est de permettre de retrouver l'adresse IP d'une machine connaissant l'adresse physique (adresse MAC) de sa carte réseau.

L'objectif de l'attaque consiste à s'interposer entre deux machines du réseau et à transmettre à chacune un paquet ARP falsifié indiquant que l'adresse ARP (adresse MAC) de l'autre machine a changé, l'adresse ARP fournie étant celle de l'attaquant. Les deux machines cibles vont ainsi ainsi mettre à jour leur table dynamique appelée cache ARP. On parle ainsi de ARP cache poisoning pour désigner ce type d'attaque.

Exercice 1 : Mise en œuvre du sous-réseau

Soit un réseau local : 192.168.0.0/24 constitué de plusieurs hôtes dont les adresses IPV4 et MAC sont les suivantes :

attaquant : 192.168.0.14 ; 00:12:43:4A:76:E6
cible 1 : 192.168.0.17 ; 00:1D:09:AA:70:8B
passerelle : 192.168.0.254 ; 00:11:22:33:44:55

1.1. Représentez graphiquement ce sous réseau local 192.168.0.0/24.
1.2. Précisez les configurations requises pour que la carte réseau eth0 d'un PC sous linux puisse accéder au réseau.
1.3. Donnez une commande permettant d'obtenir l'adresse IP de la passerelle ainsi que l'adresse public du sous réseau.
1.4. Quel est la commande qui permet de passer un hôte en routeur sous linux ? Quel est l'intérêt pour l'attaquant de se configurer comme routeur ?

Exercice 2 : Mise en œuvre de l'attaque

2.1. Effectuez une attaque MITM basée sur du ARP Poisonning afin d'écouter les paquets entre la cible (interface 192.168.0.17) et le réseau internet.
2.2. Donnez les adresses IP et MAC source et destination des paquets transmis par 192.168.0.17 à destination d'un hôte du même sous réseau local.
2.3. Idem mais vers un hôte sur internet.
2.4. Idem à 2.3 mais après l'attaque MITM précédente.
2.5. Effectuez une attaque de type MAC spoofing.

Complément : Expliquez la différence entre un routage par masquage d'adresse (MASQUERADE) et un routage simple.

Indication : utilisez deux hôtes A et B, d'adresses respectives 192.168.1.2/24 et 192.168.0.15/24 et un routeur C dont les interfaces réseaux ont pour adresses : 192.168.0.16/24 et 192.168.1.1/24. Représentez le parcours des requêtes de A vers B