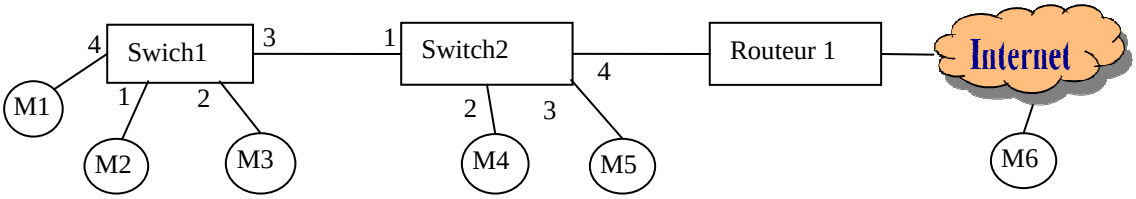
Exercice 1 [10pts]:

Soit RES le réseau Ethernet câblé suivant où les cercles sont des stations de travail. Ce réseau est relié à Internet à travers le routeur 1. Une description des attaques est donnée en annexe.



1) En utilisant le format ARP simplifié suivant ***(@IP source, @MAC source, @IP destination, @MAC destination)***, donner les deux paquets ARP envoyés par M2 pour exécuter une attaque ARP spoofing (Man in the middle) sur M1 et M3?

   ⇨ **(IP_M1, MAC_M2, IP_M3, MAC_M3) et (IP_M3, MAC_M2, IP_M1, MAC_M1)**

2) Préciser l'effet de ces messages sur les tables ARP de M1 et M3 ?

   ⇨ **Pour M1 : (IP_M3, MAC_M2) et pour M3 : (IP_M1, MAC_M2)**

3) Préciser l'effet de ces messages sur la table de commutation du switch1 (correctement remplit à l'état initial)? Expliquer ?

   ⇨ **Pas de modification : les adresse MAC source(niveau Ethernet sont celles de M2)**

4) Pour lutter contre l'attaque d'inondation des tables de commutation des commutateurs (switchs), l'administrateur a configuré le switch1 de telle façon qu'il n'accepte, par port, que N adresses MAC distinctes au maximum. Soit (NTC, NP) le nombre d'entrée de la table de commutation et le nombre de ports de chaque commutateur.

   a. Déterminer le nombre d'entrée de la table de commutation du switch1 qu'un attaquant peut fausser ? expliquer ?

   ⇨ **Il peut fausser NP x N entrées en parcourant tous les ports (ou N entrées pour un seul port)**

   b. On suppose que l'attaquant n'arrive pas à consommer toute les entrées de la table de commutation du switch1 et que cette dernière peut contenir tous les nœuds légitimes. Est-ce qu'il y aura des trames qui seront rejetées par le switch1 ? Discuter le cas où l'attaquant appartient au switch1 et le cas où il appartient au switch2 ?

   ⇨ **Cas du switch 1 : pas de rejet**

   ⇨ **Cas du switch 2 : toutes les trames envoyé par les nœuds rattachés au switch 2 et entrant par le port 3 du switch 1 seront rejetées.**

5) Les nœuds du réseau RES sont configurés par un serveur DHCP installé sur M5. Le nœud M6 peut-il exécuter l'attaque DHCP starvation sur le nœud M5 ? Expliquer ?

   ⇨ **Non, c'est une attaque interne**

6) L'administrateur du réseau a changé le port de M5 (du port 3 vers le port 10 du même switch2). Il a remarqué que les nœuds du réseau n'arrivent pas à obtenir une configuration IP d'une façon automatique ? Préciser la cause de ce problème sachant que le serveur DHCP fonctionne correctement?

   ⇨ **DHCP snooping (ports spécifiques pour les serveurs DHCP)**

7) Expliquer pourquoi un attaquant a besoin du sniffing **actif** pour pouvoir écouter les messages échangés entre les nœuds de ce réseau ?

   ⇨ **Existence de switchs (réseau commuté)**

8) M6 peut-il sniffer le réseau RES? Si oui comment ?

   ⇨ **oui par « remote sniffing »**

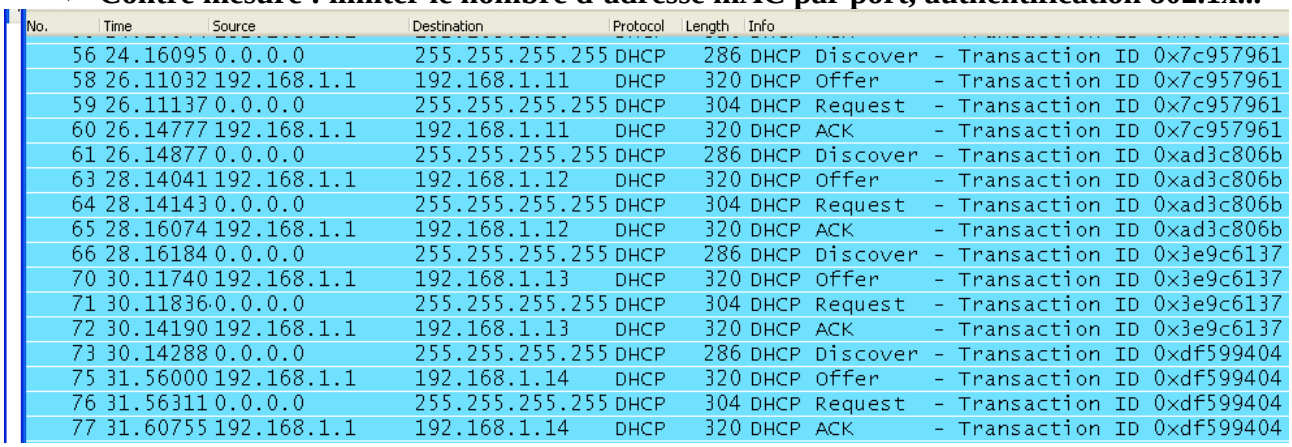
9) En se basant sur DHCP, expliquez comment un attaquant du réseau RES peut faire passer le trafic destiné à Internet par lui ?

   ⇨ **Tuer le vrai serveur DHCP (DHCP starvation), se transformer en serveur DHCP (faux serveur DHCP) et déclarer son adresse comme passerelle par défaut.**

Exercice 2 [6pts]:

Chacune des trois figures ci-dessous représente un ensemble de paquets écoutés (sniffés) suite à l'exécution d'une attaque. Sachant que tous les paquets sont envoyés par un même nœud, déterminez l'attaque correspondante à chaque figure en expliquant votre raisonnement. Précisez, pour chaque attaque, une contre-mesure possible.

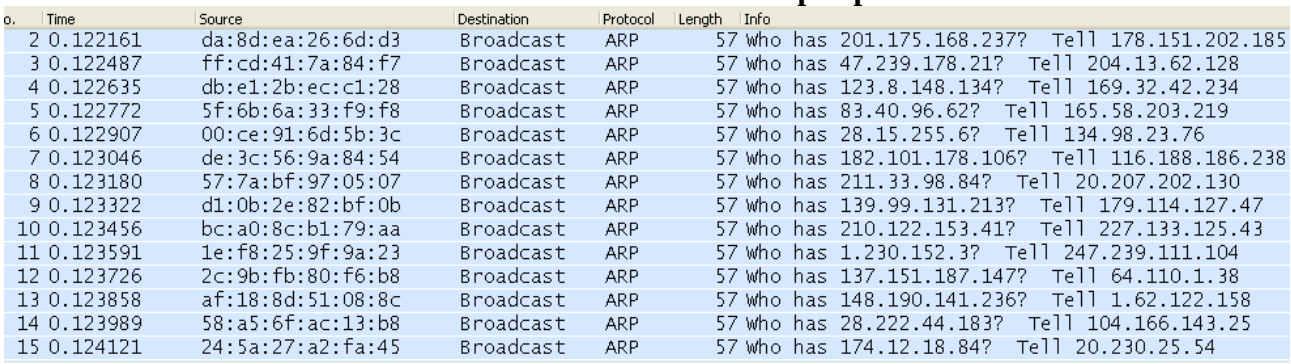
   ⇨ **Attaque1 : dhcp starvation car l'attaquant change à chaque fois son adresse MAC et demande une configuration IP (la figure montre qu'il a déjà pris les adresse 11, 12, 13 et 14).**
   ⇨ **Contre mesure : limiter le nombre d'adresse mAC par port, authentification 802.1x...**



No.	Time	Source	Destination	Protocol	Length	Info
56	24.16095	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x7c957961
58	26.11032	192.168.1.1	192.168.1.11	DHCP	320	DHCP Offer - Transaction ID 0x7c957961
59	26.11137	0.0.0.0	255.255.255.255	DHCP	304	DHCP Request - Transaction ID 0x7c957961
60	26.14777	192.168.1.1	192.168.1.11	DHCP	320	DHCP ACK - Transaction ID 0x7c957961
61	26.14877	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0xad3c806b
63	28.14041	192.168.1.1	192.168.1.12	DHCP	320	DHCP Offer - Transaction ID 0xad3c806b
64	28.14143	0.0.0.0	255.255.255.255	DHCP	304	DHCP Request - Transaction ID 0xad3c806b
65	28.16074	192.168.1.1	192.168.1.12	DHCP	320	DHCP ACK - Transaction ID 0xad3c806b
66	28.16184	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x3e9c6137
70	30.11740	192.168.1.1	192.168.1.13	DHCP	320	DHCP Offer - Transaction ID 0x3e9c6137
71	30.11836	0.0.0.0	255.255.255.255	DHCP	304	DHCP Request - Transaction ID 0x3e9c6137
72	30.14190	192.168.1.1	192.168.1.13	DHCP	320	DHCP ACK - Transaction ID 0x3e9c6137
73	30.14288	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0xdf599404
75	31.56000	192.168.1.1	192.168.1.14	DHCP	320	DHCP Offer - Transaction ID 0xdf599404
76	31.56311	0.0.0.0	255.255.255.255	DHCP	304	DHCP Request - Transaction ID 0xdf599404
77	31.60755	192.168.1.1	192.168.1.14	DHCP	320	DHCP ACK - Transaction ID 0xdf599404

Figure 1 : attaque 1

   ⇨ **Attaque2 : ARP flooding : l'attaquant change à chaque fois son adresse MAC source, l'adresse IP source et destination et diffuse ensuite le paquet ARP (voir colonne protocol)**
   ⇨ **Contre mesure : limiter le nombre d'adresse MAC par port**



o.	Time	Source	Destination	Protocol	Length	Info
2	0.122161	da:8d:ea:26:6d:d3	Broadcast	ARP	57	Who has 201.175.168.237? Tell 178.151.202.185
3	0.122487	ff:cd:41:7a:84:f7	Broadcast	ARP	57	Who has 47.239.178.21? Tell 204.13.62.128
4	0.122635	db:e1:2b:ec:c1:28	Broadcast	ARP	57	Who has 123.8.148.134? Tell 169.32.42.234
5	0.122772	5f:6b:6a:33:f9:f8	Broadcast	ARP	57	Who has 83.40.96.62? Tell 165.58.203.219
6	0.122907	00:ce:91:6d:5b:3c	Broadcast	ARP	57	Who has 28.15.255.6? Tell 134.98.23.76
7	0.123046	de:3c:56:9a:84:54	Broadcast	ARP	57	Who has 182.101.178.106? Tell 116.188.186.238
8	0.123180	57:7a:bf:97:05:07	Broadcast	ARP	57	Who has 211.33.98.84? Tell 20.207.202.130
9	0.123322	d1:0b:2e:82:bf:0b	Broadcast	ARP	57	Who has 139.99.131.213? Tell 179.114.127.47
10	0.123456	bc:a0:8c:b1:79:aa	Broadcast	ARP	57	Who has 210.122.153.41? Tell 227.133.125.43
11	0.123591	1e:f8:25:9f:9a:23	Broadcast	ARP	57	Who has 1.230.152.3? Tell 247.239.111.104
12	0.123726	2c:9b:fb:80:f6:b8	Broadcast	ARP	57	Who has 137.151.187.147? Tell 64.110.1.38
13	0.123858	af:18:8d:51:08:8c	Broadcast	ARP	57	Who has 148.190.141.236? Tell 1.62.122.158
14	0.123989	58:a5:6f:ac:13:b8	Broadcast	ARP	57	Who has 28.222.44.183? Tell 104.166.143.25
15	0.124121	24:5a:27:a2:fa:45	Broadcast	ARP	57	Who has 174.12.18.84? Tell 20.230.25.54

Figure 2 : attaque 2

   ⇨ **Attaque3 : TCP syn flooding : l'attaquant a envoyé plusieurs segment TCP/ SYN**
   ⇨ **Contre mesure : authentification, minimiser le temps d'attente dans l'état SYN_RECIEVED**

No.	Time	Source	Destination	Protocol	Info
9987	27.842666	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9988	27.845329	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9989	27.847992	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9990	27.850654	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9991	27.854647	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9992	27.857310	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9993	27.859973	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9994	27.862635	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9995	27.865297	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9996	27.867960	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9997	27.870621	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9998	27.873284	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9999	27.875931	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
10000	27.878618	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le

Figure 3 : attaque 3

Exercice 3 [4pts]:

2) Donner deux attaques possibles qu'on peut lancer en exploitant cette page Web qui permet l'administration du site web en question après authentification.

⇨ **SQL injetcion, buffer overflow**

2) Les deux figures suivantes représentent deux étapes pour l'inscription à grand tirage d'un jeu. Donner une attaque possible pouvant être lancée sur ce site Web et proposer une solution de sécurisation.

⇨ **Inonder le serveur par des demandes d'inscription d'une façon automatique (robot)**

⇨ **Solution : procédé anti-automation tel que l'utilisation des captcha**