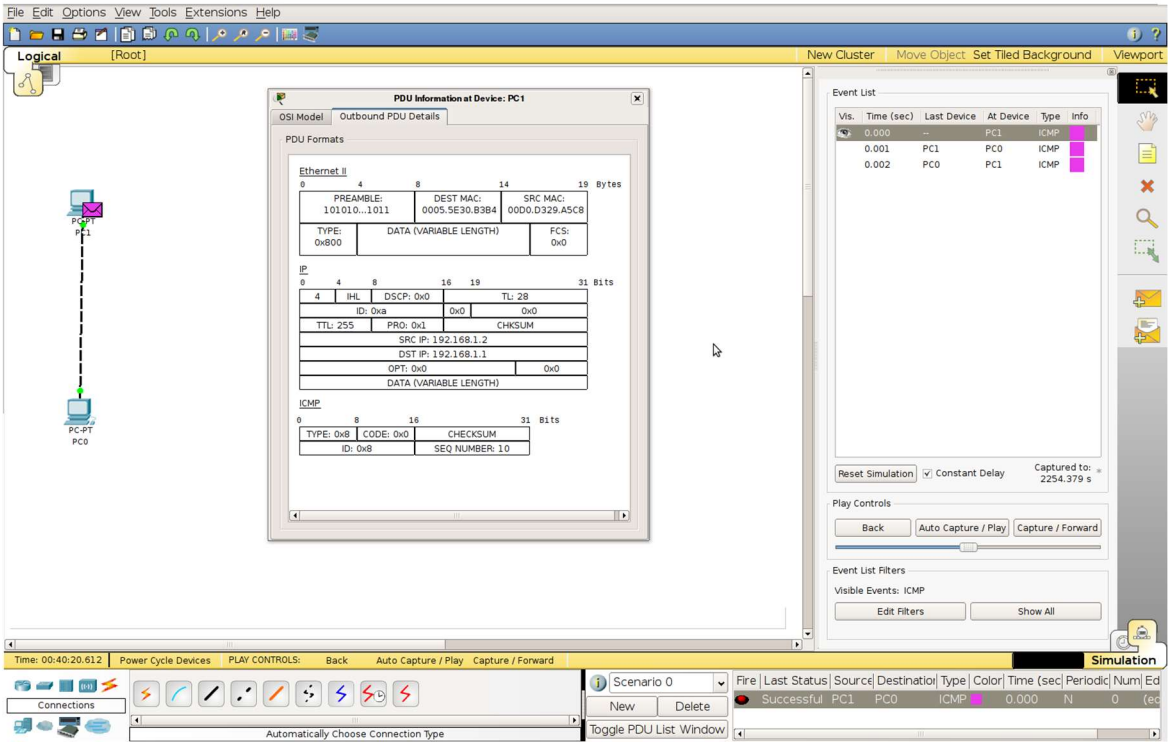
Université de Biskra/Département d'informatique
Master 1 RTIC
Module : Réseaux sans fil (RSF)
Enseignant : Dr. AYAD Soheyb

- TP4 -

Les objectifs de ce TP sont**:**

- Etude de de la commande ping avec l'environnement de simulation réseau PackeTracer
- Se familiarisé avec l'environnement du sniffer WIRESHARK
- Analyse des trames dans les réseaux sans fil.

1) Etude des paquets du protocole ICMP sous PacketTracer

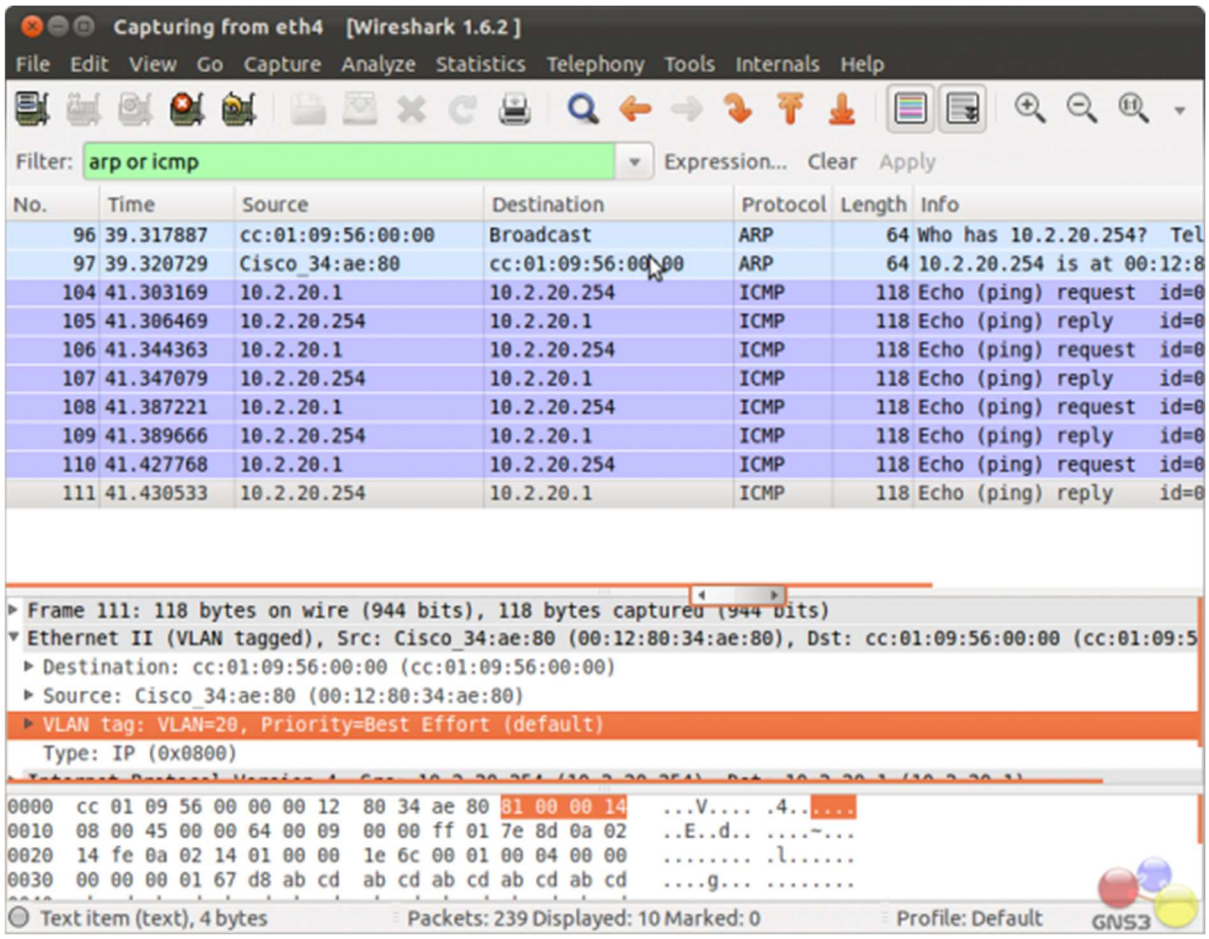


Tache:

- Suivez les instructions de l'enseignant pour créer le scénario ci-dessus
- Etudiez le résultat obtenu

2) Analyse des trames avec Wireshark

Le logiciel Wireshark est un analyseur de protocoles. Celui-ci peut utiliser directement l'interface de votre machine pour capturer des trames circulant sur le réseau.



- Lancez Wireshark et suivez l'enseignant pour la présentation de l'environnement

3) Etude détaillée de la commande ping avec Wireshark

Tache 1 :

- Lancez wireshark
- Lancez la capture sur l'interface Wireless dans la fenêtre Wireshark en spécifiant un filtre ICMP.
- Revenez au terminal sur votre machine et exécutez un ***ping*** vers le serveur dans votre salle TP en limitant le nombre de requêtes ICMP à 3.
- Retournez dans la fenêtre Wireshark et arrêtez la capture dès que la commande ping est terminée.
- Etudiez le résultat obtenu et renseignez les informations sur une trame ICMP.

Tache 2 :

La couche Ethernet

A partir de la capture réalisée précédemment complétez le tableau suivant:

+------------------ 48 bits --------------------+---------------------- 48 bits --------------------+----16bits---+

@MAC Source						@MAC Destination						Type	

Sachant que le champ **Type** peut avoir les valeurs: 0x0800 = IP
0x0806 = ARP
0x8035 = RARP

La couche IP

A partir de la capture réalisée précédemment complétez le tableau suivant:

+---4b----+-----4b-----+------------8b--------------+----- 3b-----+--------------13b----------------------+

Ver:	IHL:	TOS:	Longueur Totale:	
ID:			ind:	Fragment Offset:
TTL:		Protocole:	Somme de ctrl d'entête:	
@IP source :				
@IP destination :				
……				

Sachant que :

Ver = Version d'IP

IHL = Longueur de l'entête IP (en mots de 32 bits)

TOS = Ce champ permet de distinguer différentes qualité de service différenciant la manière dont les paquets sont traités. Composé de 3 bits de priorité (donc 8 niveaux) et trois indicateurs permettant de différencier le débit, le délai ou la fiabilité.

```
Bits 0-2:  Precedence.
Bit    3:  0 = Normal Delay,      1 = Low Delay.
Bits   4:  0 = Normal Throughput, 1 = High Throughput.
Bits   5:  0 = Normal Reliability, 1 = High Reliability.
Bit  6-7:  Reserved for Future Use.
```

Longueur totale = Nombre total d'octets du datagramme, en-tête IP comprise.

ID (identifcateur)= Numéro permettant d'identifier les fragments d'un même paquet.

Ind (indicateur) =

Bit 1 : actuellement inutilisé.
Bit 2 : DF (Don't Fragment)lorsque ce bit est positionné à 1, il indique que le paquet ne peut pas être fragmenté. Si le routeur

ne peut acheminer ce paquet (taille du paquet supérieure à la MTU), il est alors rejeté.

Bit 3 : MF (More Fragments) quand ce bit est positionné à 1, on sait que ce paquet est un fragment de données et que d'autres doivent suivre. Quand il est à 0, soit le fragment est le dernier, soit le paquet n'a pas été fragmenté.

Fragment Offset = Position du fragment par rapport au paquet de départ.

TTL = Time To Live. Ce champ indique le nombre maximal de routeurs a travers lesquels la trame peut passer. Ce champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit la trame. Cela évite l'encombrement du réseau.

Protocole = Ce champ indique quel protocole est utilisé

```
Quelques protocoles transportés :
       1 = ICMP       8 = EGP
       2 = IGMP       11 = GLOUP
       4 = IP    (encapsulation)   17 = UDP
       5 = Stream     36 = XTP
       6 = TCP        46 = RSVP
```

Somme de contrôle de l'en-tête ou Header Checksum = Ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de la trame.

Adresse IP source = Ce champ représente l'adresse IP de la machine émettrice.

Adresse IP destination = Adresse IP du destinataire du message.

Couche ICMP

A partir de la capture réalisée précédemment complétez le tableau suivant:

Type :	Code :	Somme ctrl :
……		

Sachant que :

```
Voici quelques types ICMP : 8 = Demande d'écho
                            0 = Réponse d'écho
                            11 = Durée de vie écoulée
                      12  Erreur de paramètre
```

3) Analyse des trames dans les réseaux sans fil

Ouvrir le fichier trace **Wireshark 802 11.pcap**. Cette trace a été collectée par AirPcap et wireshark dans un environnement plusieurs points d'accès. L'hôte collecteur est déjà associé à l'AP quand la trace commence.

En se basant sur le volet information au milieu de l'interface de WIRESHARK renseignez les informations suivantes :

- Quels sont les SSID des deux points d'accès émettant la plupart des trames **beacon** ?

……

……

- Quel est l'intervalle de temps entre deux trames beacon dans chaque point d'accès.

……

……

- Quel est la norme WiFi utilisé ?

……

……

- Quel est le canal de transmission dans chaque PA ?

……

……

- Les trames beacon du premier AP détecté avertissent qu'il supporte 4 débits de base et 8 Débits étendus. Quels sont ces débits ?

……

……

- Dans la requête http quelle est l'adresse IP du domaine **gaia.cs.umass.edu**

……

……

- Observer les trames dans T 49 s, que s'est-il passer ?

……

……