2. Introduction aux VLANs

> 1. Donnez deux avantages concrets de l’utilisation des VLANs.

1. Les VLANs isolent des groupes d'utilisateurs ou de périphériques sur un même réseau physique. En les segmentant, ils renforcent la sécurité en limitant l'accès aux ressources sensibles. Par exemple, un VLAN peut être attribué aux ressources financières et un autre aux ventes, protégeant ainsi les données de chaque groupe.
2. Les VLAN optimisent les performances du réseau en segmentant le trafic selon les besoins spécifiques des utilisateurs ou des services. Ce qui permet de garantir une bande passante et d'éviter les congestions et les retards dans la transmission des données, améliorant ainsi l'efficacité globale du réseau.

> 2. Pour chaque affirmation, spécifiez si elle est vraie ou fausse :
> a) Tous les membres d'un même VLAN sont dans le même domaine de broadcast.
> b) Tous les membres d'un même VLAN sont dans le même domaine de collision.
> c) Tous les membres d'un même VLAN doivent être connectés physiquement au même switch.
> d) Tous les membres d'un même VLAN requièrent la capacité de travailler dans le mode full-duplex.

a. Vraie
b. Faux, car avec les switchs chaque port constitue un domaine de collision. Cependant, les membres d'un même VLAN sont sur des ports différents.
c. Faux, les membres d'un VLAN peuvent être connectés via des trunk links ce qui fait apparaître logiquement comme dans le même réseau virtuel.
d. Faux, il n'est pas strictement nécessaire que les membres d'un même VLAN fonctionnent correctement.

> 3. Quelle est la fonction du protocole 802.1Q (VLAN tagging) ?

La fonction du protocole 802.1Q est de marquer les trames Ethernet avec des identifiants de VLAN afin de permettre aux switchs de différencier les différents VLAN.

> 4. Une école d’ingénieurs dispose de deux VLANs : un VLAN ‘professeur-e-s’ et un VLAN ‘étudiant-e-s’. Comment est-il possible qu’étudiant accède au même serveur que son professeur ?

Les VLAN sont des réseaux virtuel indépendant créer sur un même équipement physique.

> 5. Décrivez brièvement le principe des VLAN par port.

Le VLAN par port est une méthode de segmentation d'un réseau, ou chaque port est associé à un VLAN spécifique. Les appareils connectés à un port ne peuvent communiquer seulement avec ceux connectés au même VLAN.

> 6. Donnez deux inconvénients des VLAN par port.

1. Une configuration lourde et contraignante sur chaque switch.
2. Il n'y a pas d'architecture centralisée qui pourrait permettre d'éviter la lourdeur de la configuration. Chaque switch possède sa table de correspondance indépendamment du contenu des autres switch.

2.1 Configuration des ports access

> 8. Adapter ces mêmes commandes pour configurer le switch S2. Indiquer les commandes utilisées dans votre rapport

```
Switch>en
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch(vlan)#vlan 1
VLAN 1 modified:
Switch(vlan)#vlan 2
VLAN 2 added:
    Name: VLAN0002
Switch(vlan)#vlan 3
VLAN 3 added:
    Name: VLAN0003
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#inte
Switch(config)#interface e0/1
Switch(config-if)#switch
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#interface e0/2
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#interface e0/3
Switch(config-if)#switchport access vlan 1
Switch(config-if)#exit
Switch(config)#
```

10. Testez la configuration sur S1. Depuis PC1, effectuez un ping sur une adresse IP 172.16.1.x inexistante. Quels PCs reçoivent la requête ARP ? Conclusion ?

Les 2 PCs a recevoir les requêtes ARP sont le PC2 et PC6.
Le switch S1 interface e0/2 à l'adresse aa:bb:cc:00:70:20 qui est connecté au PC2 et le S2 interface e0/1 à l'adresse aa:bb:cc:00:80:30 qui est connecté au PC6.

No.	Time	Source	Destination	Protocol	Length	Info
535	428.008174	aa:bb:cc:00:80:30	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/1/aa:bb:cc:00:70:00
536	429.702760	NexoComm_00:01:00	Broadcast	ARP	42	Who has 172.16.1.84? Tell 172.16.1.11
537	430.008322	aa:bb:cc:00:80:30	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/1/aa:bb:cc:00:70:00
538	430.705423	NexoComm_00:01:00	Broadcast	ARP	42	Who has 172.16.1.84? Tell 172.16.1.11
539	431.708441	NexoComm_00:01:00	Broadcast	ARP	42	Who has 172.16.1.84? Tell 172.16.1.11
540	432.008163	aa:bb:cc:00:80:30	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/1/aa:bb:cc:00:70:00
541	433.703830	NexoComm_00:01:00	Broadcast	ARP	42	Who has 172.16.1.84? Tell 172.16.1.11
542	434.008183	aa:bb:cc:00:80:30	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/1/aa:bb:cc:00:70:00
543	434.705194	NexoComm_00:01:00	Broadcast	ARP	42	Who has 172.16.1.84? Tell 172.16.1.11
544	435.708607	NexoComm_00:01:00	Broadcast	ARP	42	Who has 172.16.1.84? Tell 172.16.1.11
545	436.008171	aa:bb:cc:00:80:30	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/1/aa:bb:cc:00:70:00

No.	Time	Source	Destination	Protocol	Length	Info
548	469.290372	NexoComm_00:01:00	Broadcast	ARP	42	Who has 172.16.1.84? Tell 172.16.1.11
549	470.165446	aa:bb:cc:00:70:20	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/2/aa:bb:cc:00:70:00
550	470.293379	NexoComm_00:01:00	Broadcast	ARP	42	Who has 172.16.1.84? Tell 172.16.1.11
551	471.296839	NexoComm_00:01:00	Broadcast	ARP	42	Who has 172.16.1.84? Tell 172.16.1.11
552	472.169516	aa:bb:cc:00:70:20	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/2/aa:bb:cc:00:70:00
553	472.200121	aa:bb:cc:00:70:20	CDP/VTP/DTP/PAgP/UDLD	CDP	351	Device ID: Switch Port ID: Ethernet0/
554	473.291531	NexoComm_00:01:00	Broadcast	ARP	42	Who has 172.16.1.84? Tell 172.16.1.11
555	474.169556	aa:bb:cc:00:70:20	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/2/aa:bb:cc:00:70:00
556	474.293589	NexoComm_00:01:00	Broadcast	ARP	42	Who has 172.16.1.84? Tell 172.16.1.11
557	475.296992	NexoComm_00:01:00	Broadcast	ARP	42	Who has 172.16.1.84? Tell 172.16.1.11
558	476.173558	aa:bb:cc:00:70:20	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/2/aa:bb:cc:00:70:00
559	477.292682	NexoComm_00:01:00	Broadcast	ARP	42	Who has 172.16.1.84? Tell 172.16.1.11

Le PC6 sur le switch 2 fait partie du vlan 1, il n'a donc pas connaissance des différents vlan du switch 1.

2.2 Configuration des ports trunk

> 11. Testez la configuration. Depuis PC11, envoyez un ping sur une adresse 172.16.1.x inexistante. Qui reçoit la requête ARP ?

Cette fois-ci, il s'agit du PC 2 et PC4.
Le switch S1 interface e0/2 à l'adresse aa:bb:cc:00:70:20 qui est connecté au PC2 et le S2 interface e0/1 à l'adresse aa:bb:cc:00:80:10 qui est connecté au PC4.

21	35.867266	NexoComm_00:01:00	Broadcast	ARP
22	36.022189	aa:bb:cc:00:70:20	Spanning-tree-(for-bridges)_00	STP
23	36.869272	NexoComm_00:01:00	Broadcast	ARP
24	37.872612	NexoComm_00:01:00	Broadcast	ARP
25	38.022330	aa:bb:cc:00:70:20	Spanning-tree-(for-bridges)_00	STP
26	39.904036	aa:bb:cc:00:70:20	CDP/VTP/DTP/PAgP/UDLD	DTP
27	39.904115	aa:bb:cc:00:70:20	ISL-Frame_00	LLC
28	40.022202	aa:bb:cc:00:70:20	Spanning-tree-(for-bridges)_00	STP
29	42.022184	aa:bb:cc:00:70:20	Spanning-tree-(for-bridges)_00	STP
13	23.855021	NexoComm_00:01:00	Broadcast	ARP
14	24.009973	aa:bb:cc:00:80:10	Spanning-tree-(for-bridges)_00	STP
15	24.857033	NexoComm_00:01:00	Broadcast	ARP
16	25.860382	NexoComm_00:01:00	Broadcast	ARP
17	26.010060	aa:bb:cc:00:80:10	Spanning-tree-(for-bridges)_00	STP
18	27.551066	aa:bb:cc:00:80:10	CDP/VTP/DTP/PAgP/UDLD	DTP
19	27.551076	aa:bb:cc:00:80:10	ISL-Frame_00	LLC
20	28.010073	aa:bb:cc:00:80:10	Spanning-tree-(for-bridges)_00	STP
21	30.010059	aa:bb:cc:00:80:10	Spanning-tree-(for-bridges)_00	STP

12.Analysez les trames échangées entre les deux switches.

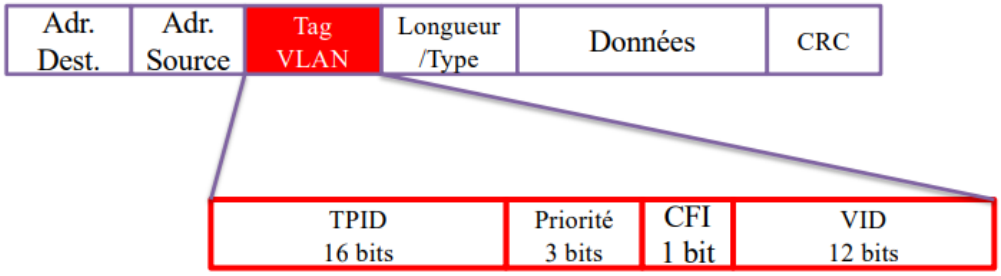
a) Indiquez l'emplacement et le format du 'VLAN tag' 802.1Q dans une trame Ethernet.

b) Quel champ identifie le VLAN d'une trame ?

c) Comparez deux trames de deux VLAN différentes pour vérifier vos propos.

Attention : souvenez-vous que l'encapsulation 802.1Q n'a pas lieu sur tout le réseau

a)

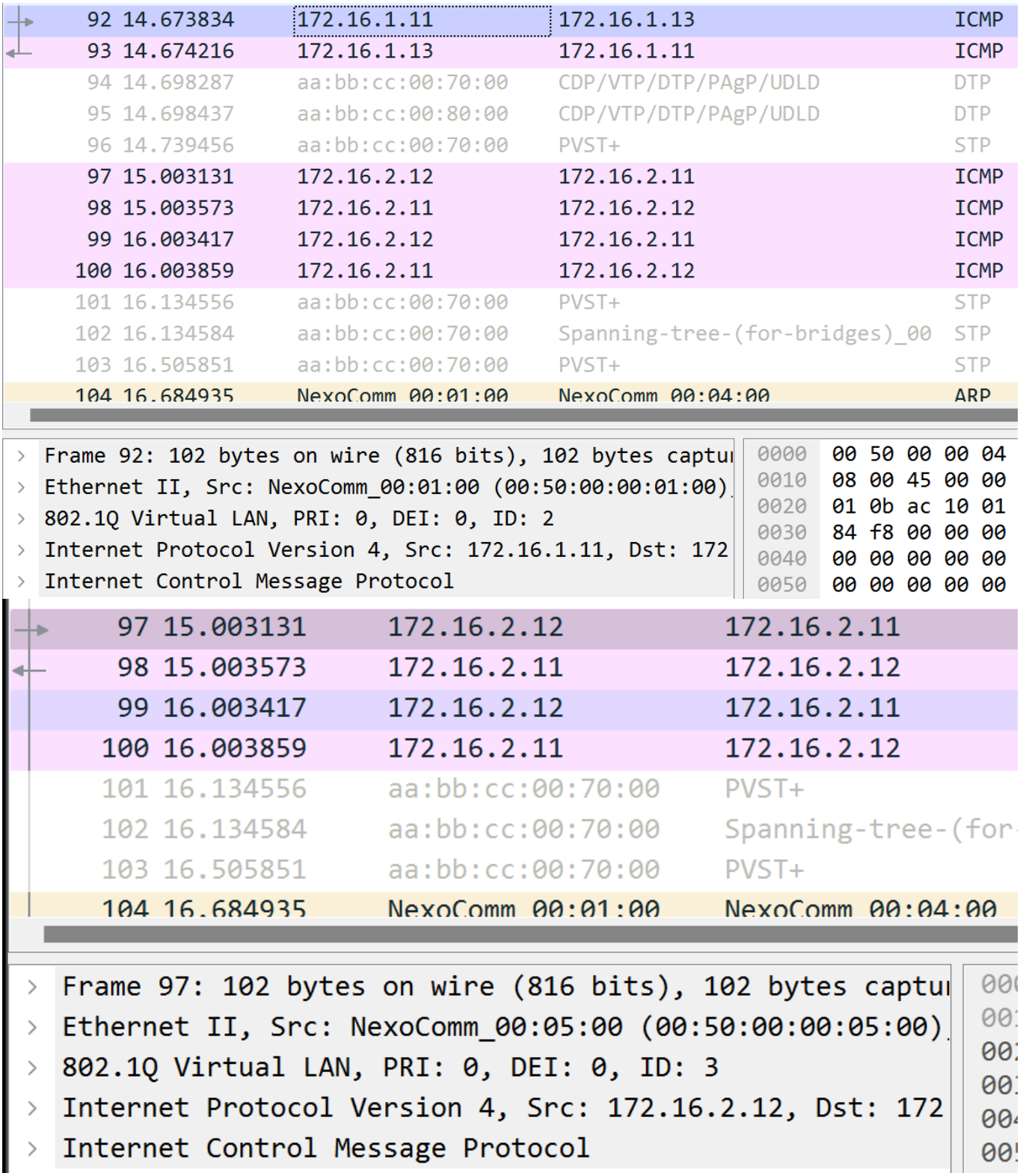


- TPID (Tag Protocol Identifier) : Identifie la trame come une trame tag 802.1Q. Sa valeur est 0x8100
- Priorité : Permets d'indiquer le niveau de priorité de la trame (Voir 802.1p - QoS)
- CFI (Canonical Format Indicator) : 0 indique que l'adressage MAC se fait en format canonique. 1 indique que le format non-canonique est utilisé
- VID (VLAN Identifier) : Identifie à quel VLAN appartient la trame

Le VLAN Tag se situe juste après l'adresse de source au format de 32bits

b) Le champ VID correspond au numéro du VLAN

c)



Comme nous pouvons le voir sur ces deux captures d'écran une requête ping est à destination du VLAN 2 et l'autre à destination du VLAN 3.

> 13. Combien de VLANs différents peuvent être gérés avec l'encapsulation 802.1Q ?

4096 est le maximum de VLAN différents que peut supporter 802.1Q.

> 14. L'encapsulation 802.1Q est-elle également utilisée sur les ports access ?

Il est possible de configurer des ports access pour qu'ils utilisent également l'encapsulation 802.1Q, mais cela est moins courant. En général, les ports access sont utilisés pour les appareils qui ne sont associés qu'à un seul VLAN.

> 15.Quelle est la longueur maximum d'une trame avec 802.1Q ?
> a) Justifiez avec une capture Wireshark et comparez le résultat avec les trames sans 802.1Q. Grâce à l'option -s du ping, envoyez une trame d'une taille supérieure à 2000 bytes. La longueur de la trame affichée sur Wireshark (on wire) ne prend pas compte du CRC (+ 4bytes).
> b) Expliquez comment un ping avec une payload plus grande que le maximum peut nous permettre de déterminer de manière rigoureuse la taille maximum d'une trame. (question bonus)

a)
Test

- ping 172.16.1.13 -s 1470 => 1496 Echo
- ping 172.16.1.13 -s 1472 => 1516 Echo
- ping 172.16.1.13 -s 1473 => 1518 Fragemented, 56 Echo

178	64.368032	172.16.1.11	172.16.1.13	ICMP	1476 Echo (ping) request
182	65.368343	172.16.1.11	172.16.1.13	ICMP	1476 Echo (ping) request
186	66.368833	172.16.1.11	172.16.1.13	ICMP	1476 Echo (ping) request
201	71.997354	172.16.1.11	172.16.1.13	ICMP	1496 Echo (ping) request
206	72.998072	172.16.1.11	172.16.1.13	ICMP	1496 Echo (ping) request
209	73.998857	172.16.1.11	172.16.1.13	ICMP	1496 Echo (ping) request
230	83.157122	172.16.1.11	172.16.1.13	ICMP	1516 Echo (ping) request
234	84.158371	172.16.1.11	172.16.1.13	ICMP	1516 Echo (ping) request
238	85.159629	172.16.1.11	172.16.1.13	ICMP	1516 Echo (ping) request
242	86.160727	172.16.1.11	172.16.1.13	ICMP	1516 Echo (ping) request
270	96.872261	172.16.1.11	172.16.1.13	IPv4	1518 Fragmented IP proto
271	96.872539	172.16.1.11	172.16.1.13	ICMP	56 Echo (ping) request
275	97.872722	172.16.1.11	172.16.1.13	IPv4	1518 Fragmented IP proto

La taille maximale d'une trame avec 802.1Q est de 1516 bytes.

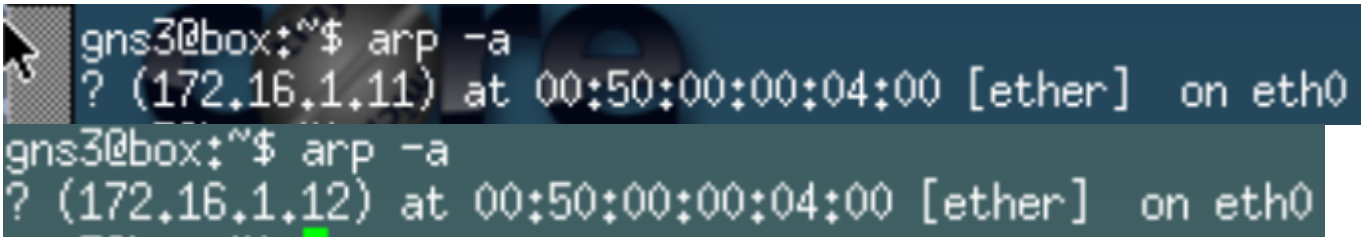
b)
Lorsque les paquets commencent à être fragmentés, cela indique que la taille de la trame maximale a été atteinte. Nous avons donc de manière rigoureuse la taille maximale de la trame.

3. Sécurité des VLANs

3.1 ARP spoofing

> 17. Consultez la table ARP de PC1 et de PC2 pour en vérifier le contenu, à l'aide de la commande arp -a.

> Il se peut que le contenu s'ePace rapidement. Refaites la manipulation jusqu'à obtenir la MAC de PC4 dans la table de PC1 et PC2. Joignez des captures d'écran.



3.2 Attaque « Man-in-the-middle »

> 18. Est-ce qu'un attaquant est capable d'effectuer une attaque man-in-the-middle avec la segmentation en VLANs s'il veut s'attaquer à un VLAN différent du sien ?

L'attaque Man-in-the middle est possible sur un VLAN différent du sien. Si l'attaquant parvient à accéder au réseau en utilisant des techniques telles que l'ARP spoofing ou le DNS spoofing. Il pourra alors altérer ou intercepter les communications du VLAN.

3.3 Attaque « VLAN hopping »

> 19. Renseignez-vous et décrivez en quoi consiste le VLAN hopping.

Le VLAN hopping est un exploit de sécurité sur les switchs dû à une mauvaise configuration des ports trunk.

> 20. Quelles attaques (écoute clandestine, déni de service) peuvent être menées avec cette méthode ?

Cette méthode peut permettre plusieurs attaques comme :

- Double Tagging : un attaquant peut envoyer des trames Ethernet avec deux en-têtes VLAN, une avec son VLAN et l'autre avec le VLAN cible. Si le switch est mal configuré pour rejeter ce type de trame, il pourrait transférer ses trames au VLAN cible, puis y accéder.
- Switch Spoofing : un attaquant peut exploiter les vulnérabilités des protocoles de trunk et forcer un port d'accès à devenir un port trunk, lui permettant de recevoir les trames de plusieurs VLAN.

> 21. Proposez une approche pour empêcher cette attaque.

Pour se protéger contre le VLAN hopping, nous pouvons mettre en place certaines actions comme : la désactivation des protocoles de trunking non utilisé, mettre une configuration appropriée sur les ports du switch et une surveillance active du réseau.

4. Recherche d’information et compréhension détaillée

> 22. Faites maintenant un ping depuis PC4 vers PC1 et capturez simultanément avec Wireshark à l’interface e0/0 de PC1 et e0/0 de PC4.
> Utilisez le filtre de capture ARP dans les deux captures. Dans un des deux interfaces, vous devriez voir seulement les requêtes ARP tandis que dans l’autre, vous devriez voir les requêtes et aussi les réponses ARP. Expliquez la raison. Pour ce faire, vous pouvez par exemple observer avec Wireshark le trajet parcouru par les requêtes ARP ainsi que celui des réponses ARP pour comprendre les différences entre les deux interfaces.

Sur le PC4, nous voyons à la fois les requêtes ARP et les réponses ARP. Cela est dû au fait que PC4 émet des requêtes ARP pour résoudre l'adresse IP de PC1 et reçoit des réponses.

Sur le PC1, nous ne voyons que les requêtes ARP. Cela est dû au fait que PC1 ne répond pas aux requêtes ARP de PC4. Le PC1 ne répond qu'aux requêtes ARP pour les adresses IP associées à son interface réseau.

> 23. Faites un ping de PC1 vers PC6. Est-ce que le ping passe ? Si oui, pourquoi ?

Les pings ne passe pas.

```
gns3@box:~$ ping 172.16.0.11
PING 172.16.0.11 (172.16.0.11): 56 data bytes
^C
--- 172.16.0.11 ping statistics ---
7 packets transmitted, 0 packets received, 100% packet loss
```