TP1-VLAN-AKOBI BANCONLE

Sommaire:

Exercice 1: Question de cours !

1-En quoi un VLAN améliore t-il la sécurité des réseaux ainsi que le trafic ?

Un Vlan améliore la sécurité en isolant les dispositifs en groupe logique indépendamment de leur emplacement physique . Cela va donc permettre de restreindre la communication entre les Vlans et donc empêcher la propagation non autorisée de données et aussi renforcer la sécurité du réseau.Les politiques de confidentialité appliquées au vlan permettent aussi de gérer plus efficacement le trafic inter-VLAN.

2- Il existe 3 niveau de VLAN, expliquez rapidement ces trois types:

On a

-Le VLAN de niveau 1 :Ici la répartition des stations dans les VLANs est en fonction des ports des switchs.La mise en place est simple sauf lorsque les VLANs sont sur plusieurs switchs.

-Le VLAN de niveau 2:Chaque VLAN est défini par la liste des adresses MAC des stations.Ainsi la configuration est ici centralisée.

-Le VLAN de niveau 3: Chaque VLAN est défini par son adresse IP de réseau. Ainsi l'appartenance d'une station est automatique par son adresse IP.

3-Qu'est que le protocole 802.1Q ?

C'est une norme définit la manière dont les trames Ethernet sont marquées pour identifier à quel VLAN elles appartiennent.Il ajoute en fait un en-tête VLAN aux trames Ethernet pour indiquer le numéro de VLAN auquel la trame est associée. Ainsi le trafic réseau sera segmenté sur un réseau commuté en fonction des VLAN.

4- Qu'est ce que TRUNK ?

C'est un lien de communication entre deux commutateurs ou routeurs qui transporte le trafic de plusieurs VLANs.Il permet donc le passage de plusieurs VLANs sur un seul câble ou liaison.

Exercice 2 : Configuration de base

1-Expliquez ce que enable permet de faire ?

Enable permet de passer en mode d'exécution privilégiée pour effectuer des opérations de configuration telles que les interfaces, la gestion des VLAN , l'accès au commandes de diagnostic et plus encore.

2-Est ce que cela existe sur tous les switch ?

Non elle n'est pas spécifique à tous les switchs , elle est typique des switchs Cisco vu que d'autres fabricants ont leurs méthodes d'accès à ce type de privilège.

```
Switch(config)#hostname sw1
sw1(config)#
```

Le nom d'hôte du switch a été configuré pour sw1 .On a donc attribué le nom:"sw1" à de switch

2.2 Attribution de mot de passe de sécurité :

1. Expliquez la notion de line con 0:

Elle fait référence à la configuration de la ligne de console sur le switch .C'est en fait une interface qui permet de se connecter physiquement à l'appareil à l'aide d'un cable de console.

```
sw1>enable
sw1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw1(config)#line con 0
sw1(config-line)#password discipline
sw1(config-line)#login
sw1(config-line)#exit
```

```
sw1(config)#exit
sw1#
%SYS-5-CONFIG_I: Configured from console by console

sw1#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]yC2960 Boot Loader (C2960-HBOOT-M)
Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
```

```
User Access Verification

Password:
Password:

sw1>
```

On remarque qu'après redémarrage, il est demandé le mot de passe qu'on avait entré pécedemment vu que les modifications ont été sauvergadées avant le redémarrage.

Nous allons maintenant configurer un accès au switch en mode sécurisé pour plusieurs utilisateurs (jean, sarah).

```
sw1>enable
sw1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw1(config)#line con 0
sw1(config-line)#username sarah password croche
sw1(config)#username jean password serien
sw1(config)#exit
sw1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
.
username jean privilege 1 password 0 serien
username sarah privilege 1 password 0 croche
!
.
```

Que pouvez vous dire de la sécurité du password des utilisateurs ?

Le password n'est pas très sécurisé vu qu'il est facilement lisible par tout utilisateur externe.

Utilisez service passwordencryption:

```
sw1#enable
sw1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw1(config)#service password-encryption
sw1(config)#username sarah password croche
sw1(config)#username jean password serien
sw1(config)#exit
sw1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
!
username jean privilege 1 password 7 0832495C001C0B
username sarah privilege 1 password 7 08225E410A1100
!
```

La différence est là. On remarque que le mot de passe est en hexadécimal ce qui n'est pas directement lisible donc la sécurité y est grandement plus élevée.

2.3 Vérification de la connexion à distance:

L'adressage IP du switch va nous servir à superviser celui-ci à distance. Un VLAN dédié au management du switch est configuré. Par défaut nous avons un VLAN1.

1. A quoi peut servir ce VLAN1 ?

Ce VLAN1 peut permettre l'accès à distance et la configuration du switch .Il traite le trafic de gestion et le trafic non étiqueté .

2-Non, il n'est pas possible de changer le nom du VLAN1 comme on peut le voir:

```
sw1>enable
sw1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw1(config)#vlan 1
sw1(config-vlan)#name nouveaunom
Default VLAN 1 may not have its name changed.
```

• Pourquoi à partir du pc enseignant le ping ne fonctionne pas ?

Il ne fonctionne pas parce que vlan est désactivé donc il faudrait le réactiver avec la commande no shutdown

TP1-VLAN-AKOBI BANCONLE

```
sw1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw1(config)#interface vlan 1
sw1(config-if)#no shutdown

sw1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up

sw1(config-if)#exit
sw1(config)#exit
sw1#
%SYS-5-CONFIG_I: Configured from console by console

sw1#show interface vlan 1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 0010.1103.eedb (bia
0010.1103.eedb)
```

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=255
Reply from 192.168.1.10: bytes=32 time=1ms TTL=255
Reply from 192.168.1.10: bytes=32 time<1ms TTL=255
Reply from 192.168.1.10: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Le telnet ne marche pas parce que l'accès au mode privilégié n'a pas été activé , donc on passera par la création d'une ligne virtuelle

```
sw1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw1(config)#line vty 0 15
sw1(config-line)#password uphf
sw1(config-line)#login
sw1(config-line)#end
sw1#
%SYS-5-CONFIG_I: Configured from console by console
```

Et voilà

```
C:\>telnet 192.168.1.10
Trying 192.168.1.10 ...Open


User Access Verification

Password:
sw1>
```

Exercice 3: Configuration de VLAN :

Vous avez la configuration suivante pour l'entreprise à mettre en place. Il existe 2 services (développement et réseau).

***Etape 1** : Mettre en place l'architecture (sans VLAN) avec les adresses IP correspondantes.*
Fait!

Etape 2 : Mettre en place le(s)s VLAN(s) afin d'avoir la partie « Développement » d'un côté et la partie « Réseau » de l'autre. ● Que permet la mise en place de VLAN ?

Il permet de segmenter le réseau local en plusieurs réseaux logiques au sein d'un même switch .Il va donc simplifier la gestion du réseau et améliorer la sécurité en évitant la propagation de données non autorisées. De plus, la bande passante est optimisée en dirigeant le trafic vers des segments spécifiques en fonction des besoins de l'entreprise.

Nommer le(s) VLAN(s).

2	Developpement
3	Reseau

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	2	--	00E0.A35B.7401
FastEthernet0/2	Up	2	--	00E0.A35B.7402
FastEthernet0/3	Up	2	--	00E0.A35B.7403
FastEthernet0/4	Up	2	--	00E0.A35B.7404
FastEthernet0/5	Up	3	--	00E0.A35B.7405
FastEthernet0/6	Up	3	--	00E0.A35B.7406
FastEthernet0/7	Up	3	--	00E0.A35B.7407

L'entreprise veut mettre en place un serveur de ressources (DHCP) afin de faciliter la connectivité. Après avoir définit l'intérêt de la mise en œuvre d'un serveur DHCP, vous expliquerez le ou les éléments à mettre en œuvre.

La mise en oeuvre d'un serveur DHCP simplifie la gestion des adresses IP au sein de l'entreprise en attribuant dynamiquement des adresses IP aux dispositifs du réseau , évitant donc les conflits d'adresses IP et réduit la charge de gestion manuelle .
Pour le mettre en place il faut:
-configurer le serveur DHCP notamment la plage d'adresses IP disponibles , la passerelle par défaut , les serveurs DNS ,.. et la durée de bail des adresses IP.
-Configurer le commutateur pour rediriger les requêtes DHCP vers le serveur DHCP et donc l'activation du relais DHCP

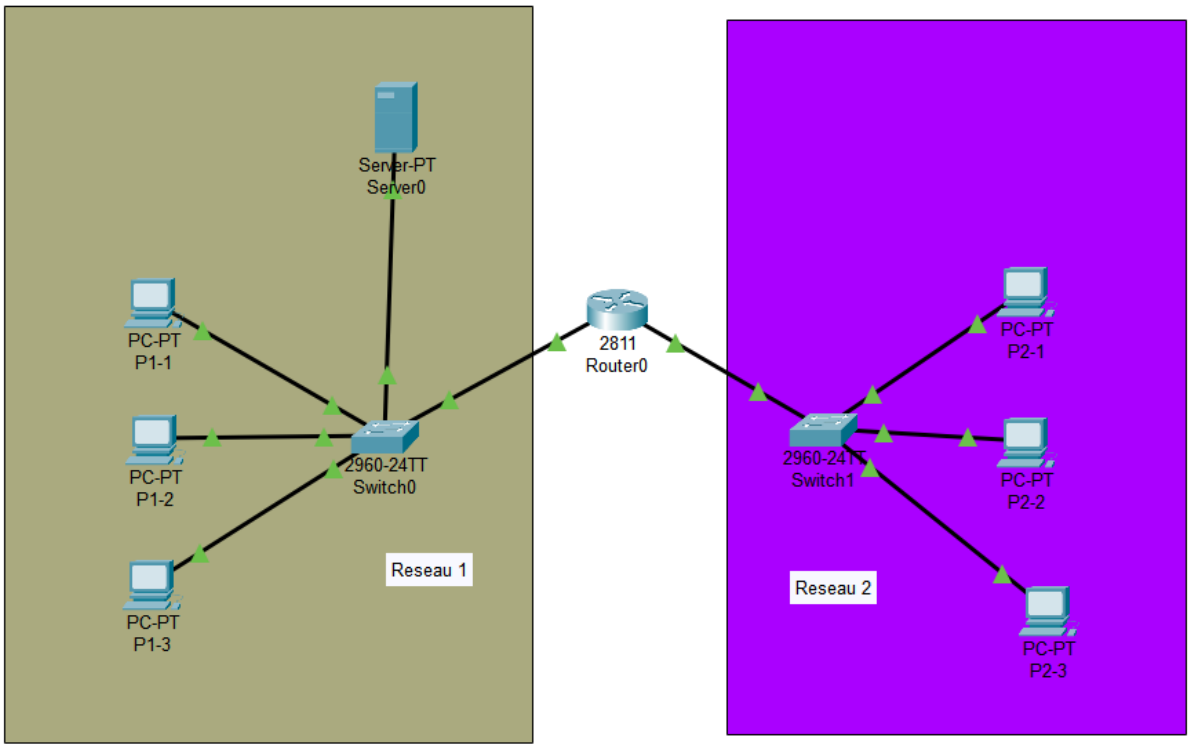
Etape 3 :

Maquette faite.

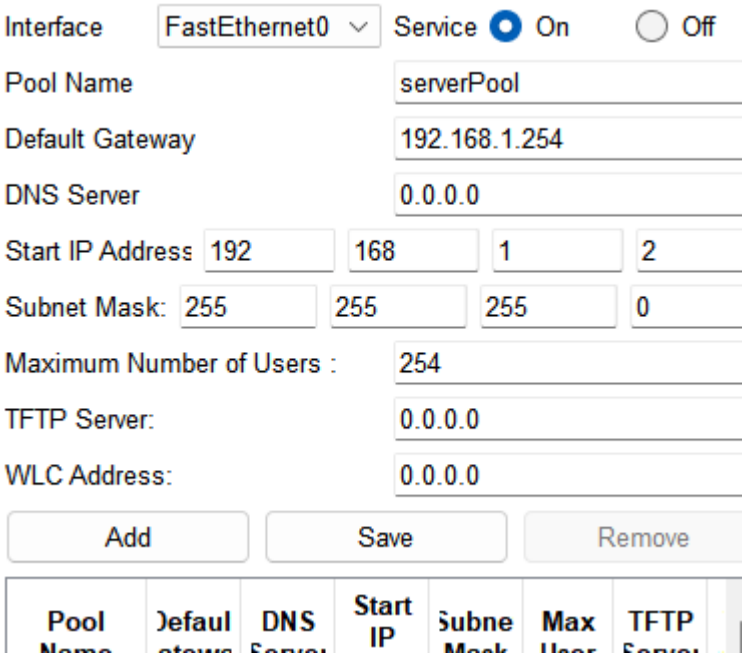
Question : Le switch peut il faire office de relai DHCP ? Si oui pourquoi ?

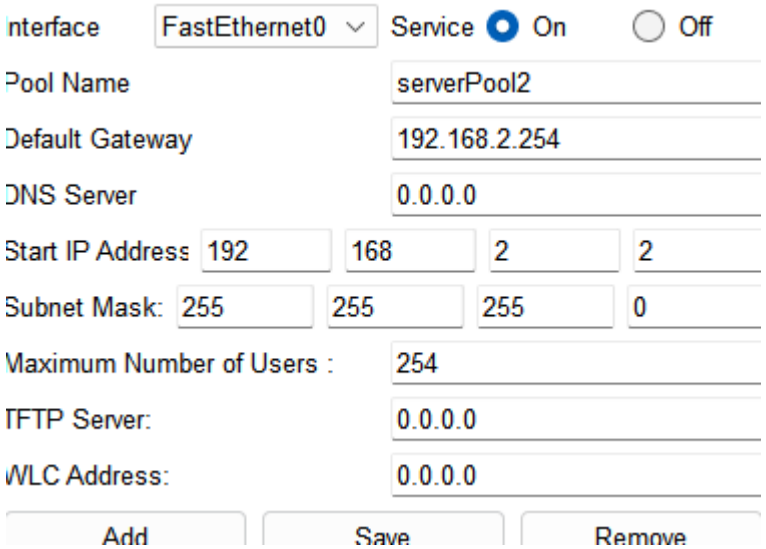
Oui il peut office de relai DHCP car les requêtes DHCP ne sont généralement par routées .Ainsi la fonction relai (IP Helper) va permettre d'intercepter ces requêtes et les rediriger vers le serveur DHCP qui peut leur attribuer une adresse IP appropriée.

Exercice 4 : Le relais DHCP autre solution (routeur)



TP1-VLAN-AKOBI BANCONLE





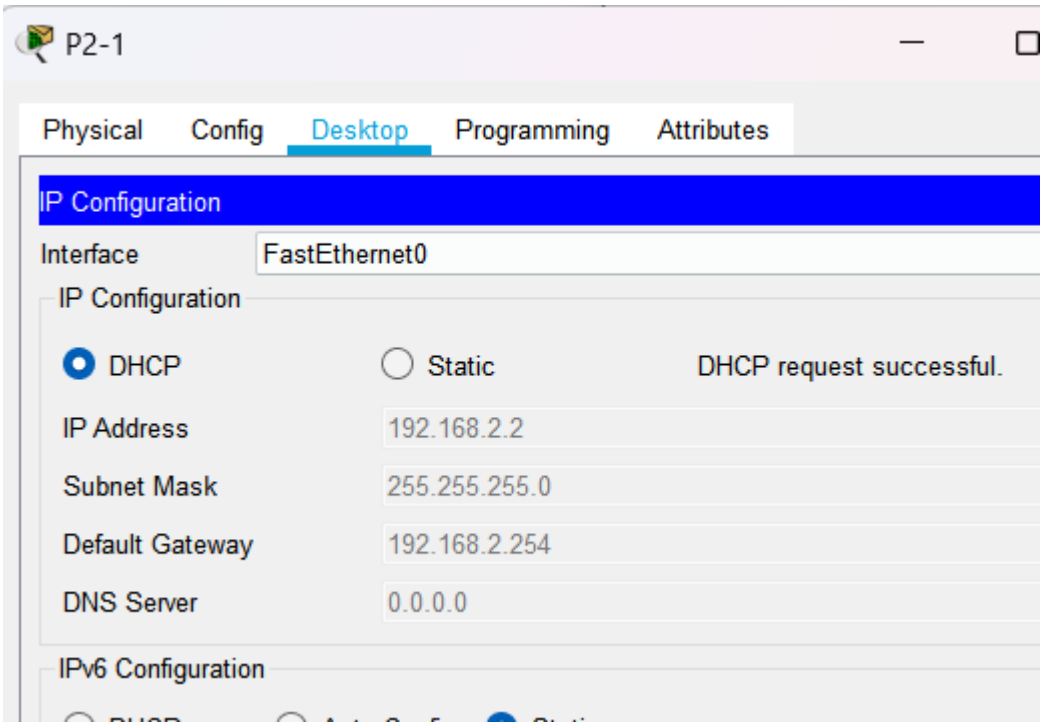
Que faut il activer pour que le routeur soit relais DHCP ? Expliquez la démarche Peut on faire la même chose sur 2 VLAN ?

Il faut activer la fonction de relai DHCP Dans un premier temps on accède à l'interface FastEthernet0/1 connecté au switch du réseau 2 , ensuite avec la commande ip helper-address suivi de l'adresse IP du serveur DHCP,on active la fonction de relai DHCP.Dès lors, on enrégistre les changements puis on réactive l'interface FastEthernet0/1 qui a préalablement été désactivé avant la configuration.

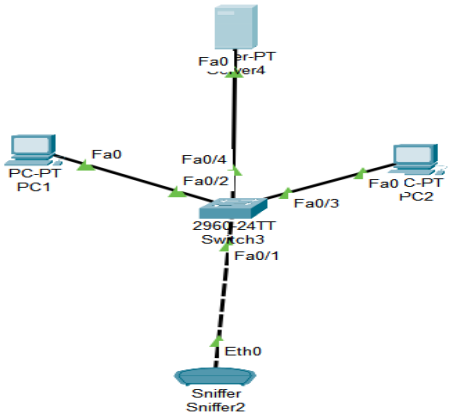
Ainsi on:

```
Router(config-if)#ip helper-address 192.168.1.1
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

On peut remarquer la requête DHCP fonctionne maintenant. Pour preuve on a:



Exercice 5 : Le port mirroring



A quoi peut servir le port mirroring ?

De façon général, le port mirroring permet de copier le trafic réseau passant par un ou plusieurs ports d'un switch et de le rediriger vers d'autres ports généralement connecté à un autre dispositif de surveillance ou d'analyse de trames comme un sniffer par exemple.

Dans notre situation il faut configurer le commutateur de manière à diriger délibérément les paquets vers le sniffer car le switch ,par defaut , envoie les paquets uniquement à leur destination prévue. De ce fait on utilisera le port mirroring afin de copier le trafic entre le pc1 , pc2 et le serveur et le rediriger vers le port du sniffer pour la capture et l'analyse des paquets .

Pourquoi utiliser le VMTS ?

Il permet de gérer plusieurs taches ou même processus.

1. Mettre en place le port mirroring afin de capturer les trames émises sur les ports de PC1 et PC2.

Pour capturer les trames émises depuis les ports de PC1 et PC2 , on devrait configurer le port mirroring en utilisant la commande "monitor session" pour spécifier les sources (les interfaces des PC) et la destination (interface reliée au sniffer sur le switch).
Pour capturer les trames émises depuis les ports de PC1 et PC2, configurez le port mirroring en utilisant la commande "monitor session" pour spécifier les sources (les interfaces des PC) et la destination (l'interface reliée au sniffer) sur le switch.

les sources sont Fa0/2 et Fa0/3(reliées respectivement au pc1 et 2) , puis la destination est Fa0/1(relié au sniffer)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#monitor session 1 source interface Fa0/2
Switch(config)#monitor session 1 source interface Fa0/3
Switch(config)#monitor session 1 destination interface Fa0/1
Switch(config)#end
Switch#
```

On peut vérifier avec un show monitor session:

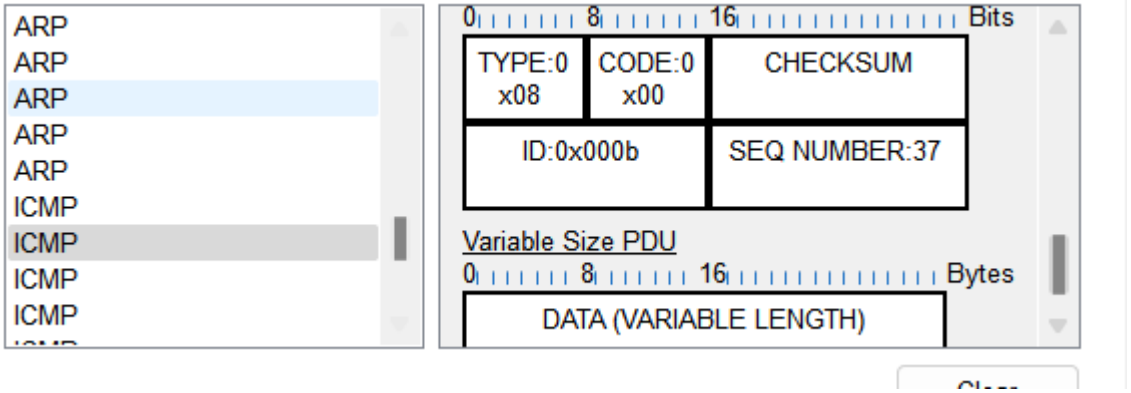
```
% Incomplete command.
Switch#show monitor session 1
Session 1
---------
Type                   : Local Session
Description            : -
Source Ports           :
    Both               : Fa0/2,Fa0/3
Destination Ports      : Fa0/1
    Encapsulation      : Native
          Ingress      : Disabled
```

2. Mettre en place la capture d'un test de connexion (ping)

On effectue la capture d'un ping de PC1 à PC2

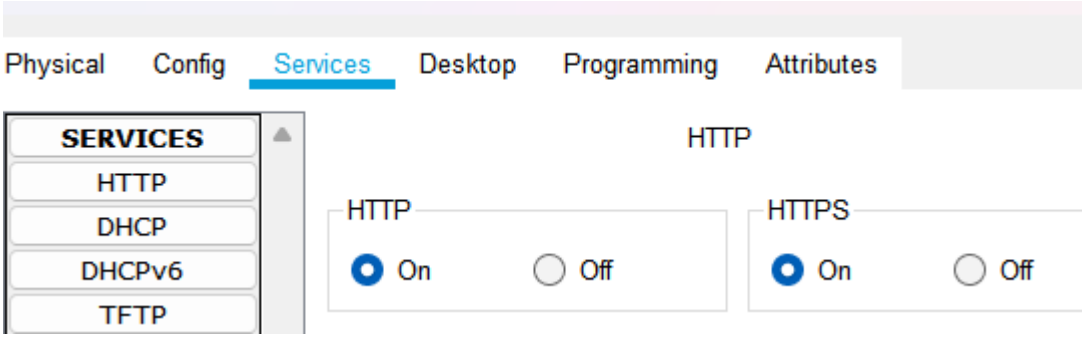
```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=3ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
```

et on voit que la capture est réussi(des paquets ICMP par exemple ont été capturés).



3. Mettre en place la capture d'une navigation web entre PC1 et le serveur

Le service HTTP est activé .



Donc dans un premier temps on va mettre en place le port-mirroring pour capturer les trames entre les serveur et PC1 comme fait précédemment(ici les sources sont fa0/2 et fa0/4 mais vu que le fa0/2 était déjà spécifié pour le le PC1 alors il ne faudrait spécifier que fa0/4 pour le serveur).

```
Switch(config)#monitor session 1 source interface fa0/4
Switch(config)#end
Switch#
```

On vérifie ensuite avec un show monitor session 1 et on a :

```
witch#show monitor session 1
ession 1
--------
ype                       : Local Session
escription                : -
ource Ports               :
    Both                  : Fa0/2,Fa0/3,Fa0/4
estination Ports          : Fa0/1
    Encapsulation         : Native
          Ingress         : Disabled
```

Consultons à présent la page web pour vérifier si la capture marche :

Et on voit que des captures on bien été effectuées(des paquets TCP , HTTP).