

M2 MMI - Cloud Computing et Virtualization

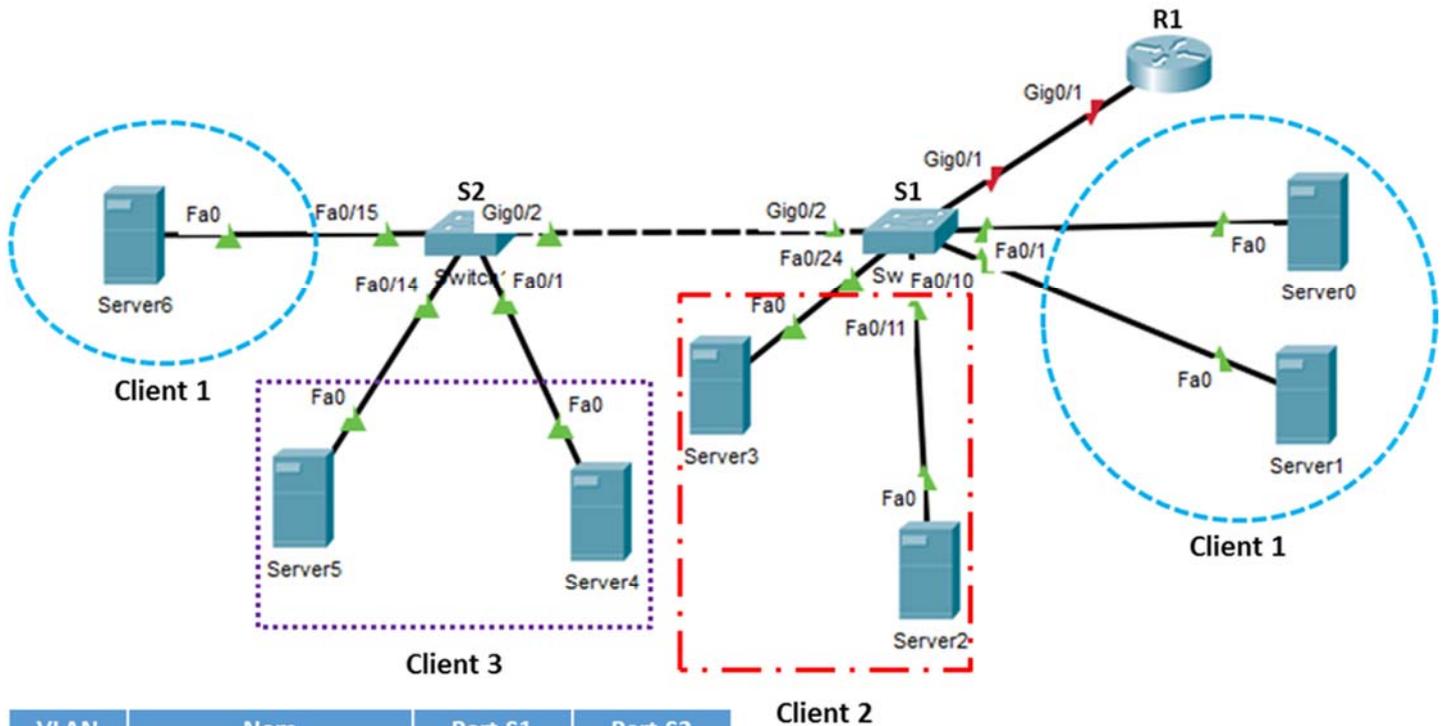
Travaux Pratiques N°2 : Virtualisation des Réseaux – Routage inter-vlan & contrôle d'accès

Objectifs :

Dans cette deuxième partie, l'étudiant implémentera une solution dite « Router on the stick » en vue de permettre la communication inter-vlan. Un filtrage sera, par la suite, imposé afin de ne permettre l'accès qu'aux serveurs publics de chaque client, protégeant ainsi les serveurs locaux, privés.

Topologie :

Réutiliser la topologie créée précédemment dans la partie 1.



VLAN	Nom	Port S1	Port S2
10	Client1	Fa0/1-10	F0/15-20
20	Client2	Fa0/11-24	----
30	Client3	----	Fa0/1-14

Table d'adressage

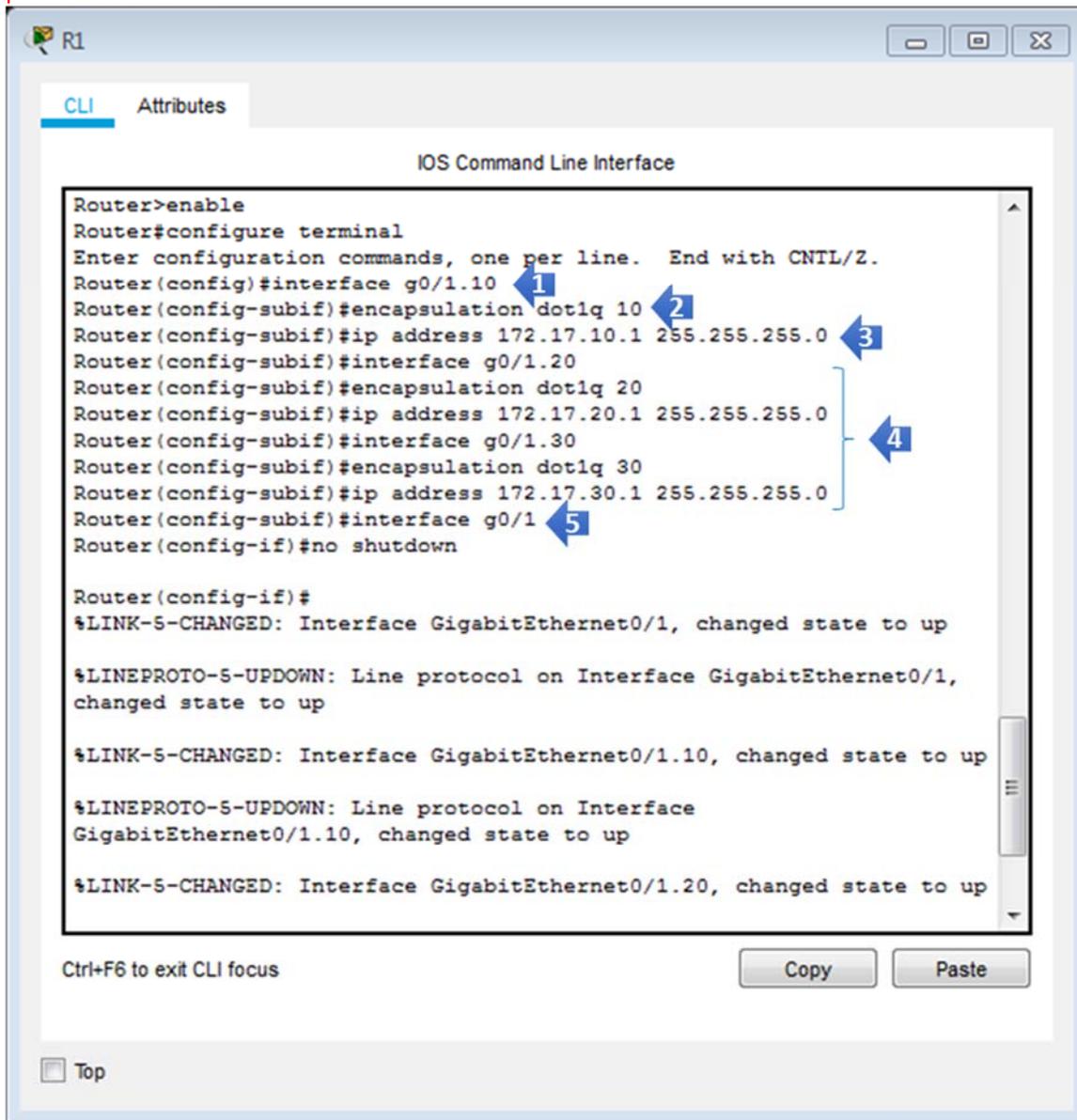
Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/1,10	172.17.10.1	255.255.255.0	N/A
	G0/1,20	172.17.20.1	255.255.255.0	N/A
	G0/1,30	172.17.30.1	255.255.255.0	N/A
Server0	Carte réseau	172.17.10.10	255.255.255.0	172.17.10.1
Server1	Carte réseau	172.17.10.11	255.255.255.0	172.17.10.1
Server2	Carte réseau	172.17.20.10	255.255.255.0	172.17.20.1
Server3	Carte réseau	172.17.20.11	255.255.255.0	172.17.20.1
Server4	Carte réseau	172.17.30.10	255.255.255.0	172.17.30.1
Server5	Carte réseau	172.17.30.11	255.255.255.0	172.17.30.1
Server6	Carte réseau	172.17.10.12	255.255.255.0	172.17.10.1

Conditions requises

Partie 2 : routage inter-vlan

a) Configurez le routage inter-VLAN sur R1 en fonction de la table d'adressage.

Afin d'assurer le routage, chaque Vlan doit disposer d'une passerelle, or un routeur est connu pour son nombre réduit de ports physiques. La solution serait donc de créer à la base d'un port physique, plusieurs ports virtuels chacun servant comme passerelle d'un Vlan.



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface g0/1.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 172.17.10.1 255.255.255.0
Router(config-subif)#interface g0/1.20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 172.17.20.1 255.255.255.0
Router(config-subif)#interface g0/1.30
Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip address 172.17.30.1 255.255.255.0
Router(config-subif)#interface g0/1
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.10, changed state to up

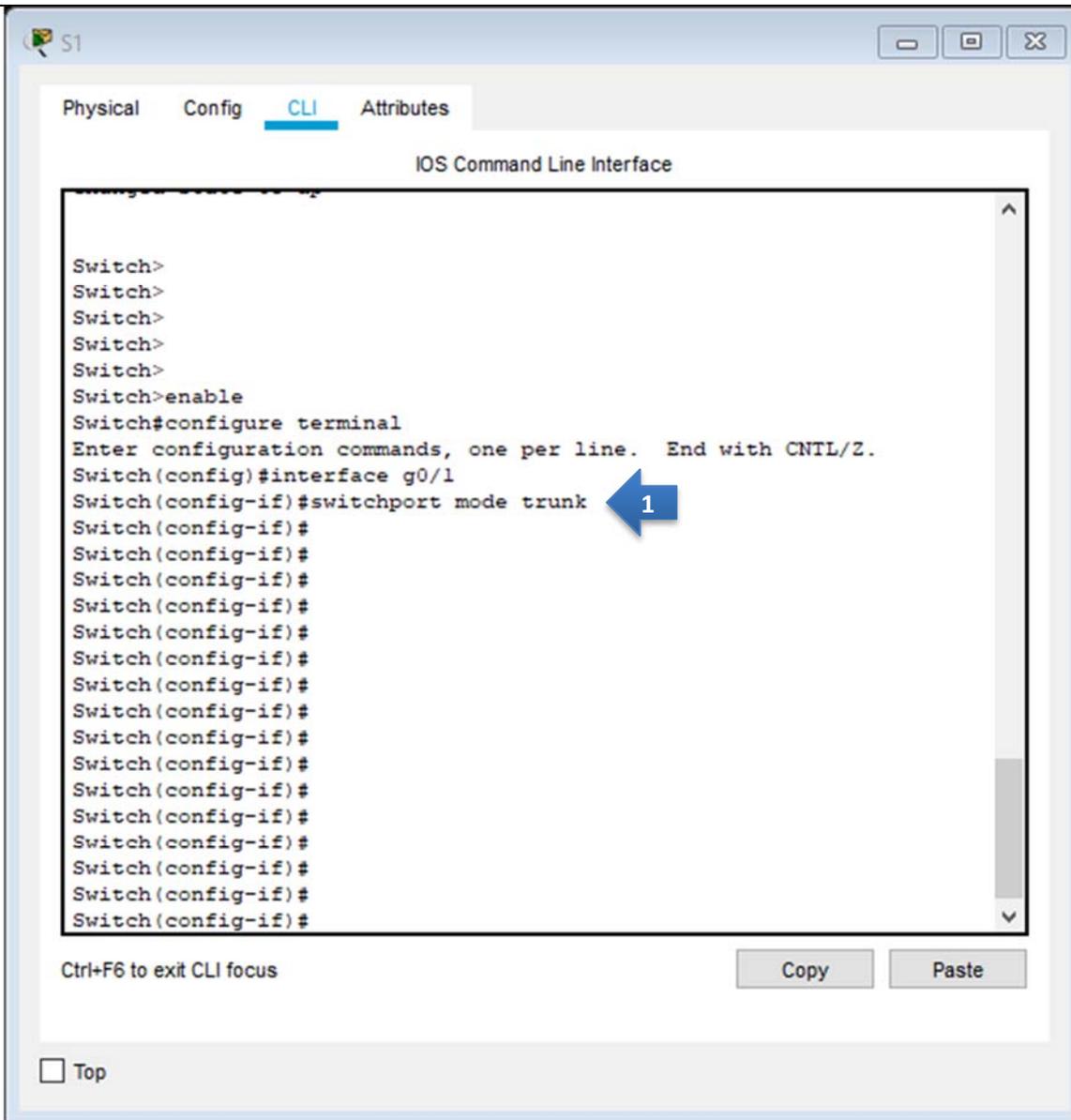
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.10, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.20, changed state to up
```

- 1) Afin de créer un port virtuel à partir du port physique « g0/1 », il suffit d'ajouter le suffixe « .10 », le nom complet du port virtuel est donc « g0/1.10 ». Il est recommandé d'employer le même numéro que l'identificateur du vlan associé, ainsi, g0/1.10 représentera la passerelle du vlan 10. Pour ce faire, exécuter la commande : **interface g0/1.10**
- 2) Avant de configurer l'adressage IP du port virtuel, il est impératif d'activer le protocole de trunking 802.1q puis associer ce port au vlan 10. C'est ce qui rend effectivement « g0/1.10 » une passerelle pour le vlan 10. Exécuter la commande : **encapsulation dot1q 10**
- 3) Attribuer la première adresse d'hôte au port virtuel ainsi que le masque sous réseau. Commande : **ip address 172.17.10.1 255.255.255.0**
- 4) Procéder pareillement à la configuration des ports virtuels « g0/1.20 », « g0/1.30 », représentant, respectivement, les passerelles des vlans 20 et 30.
- 5) Un port du routeur est désactivé par défaut. Afin de pouvoir activer, à la fois, tous les ports virtuels, exécuter la commande **no shutdown** au niveau du port physique parent « g0/1 ».

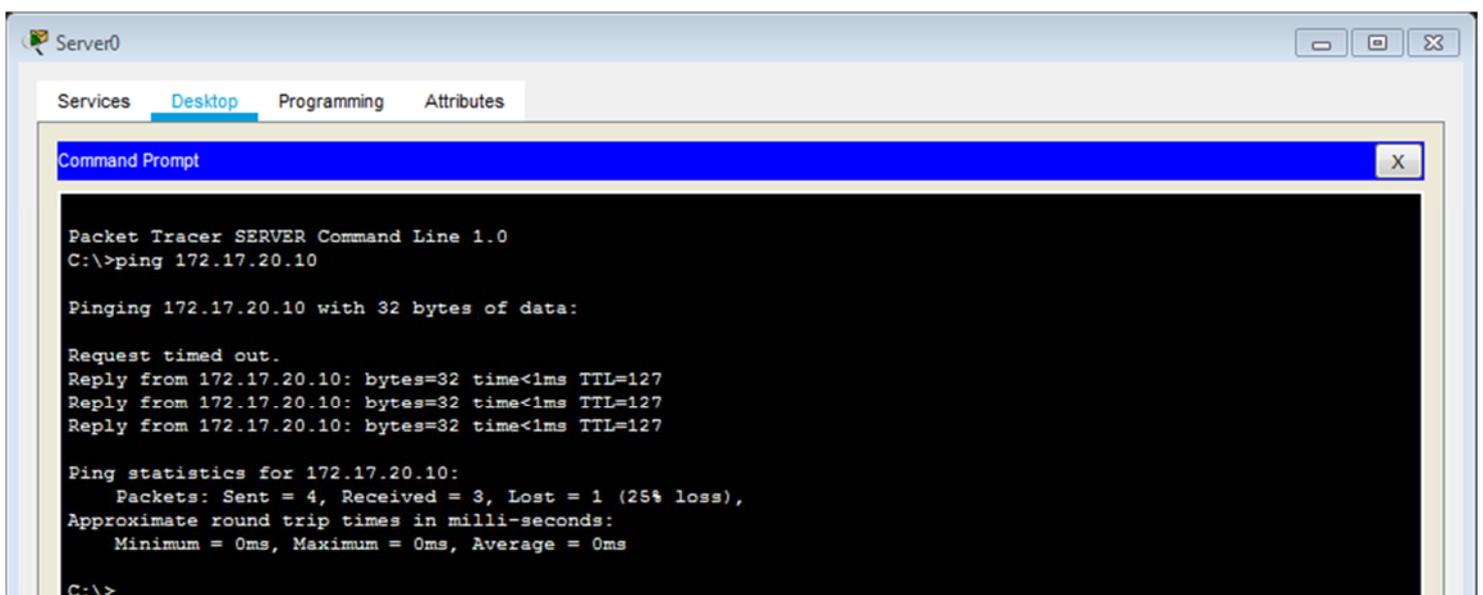
b) Configurer la liaison Trunk entre le commutateur S1 et le routeur R1.

La liaison entre le routeur et le commutateur doit permettre le transfert des trafics de tous les vlans. C'est pourquoi elle doit être en mode trunk.



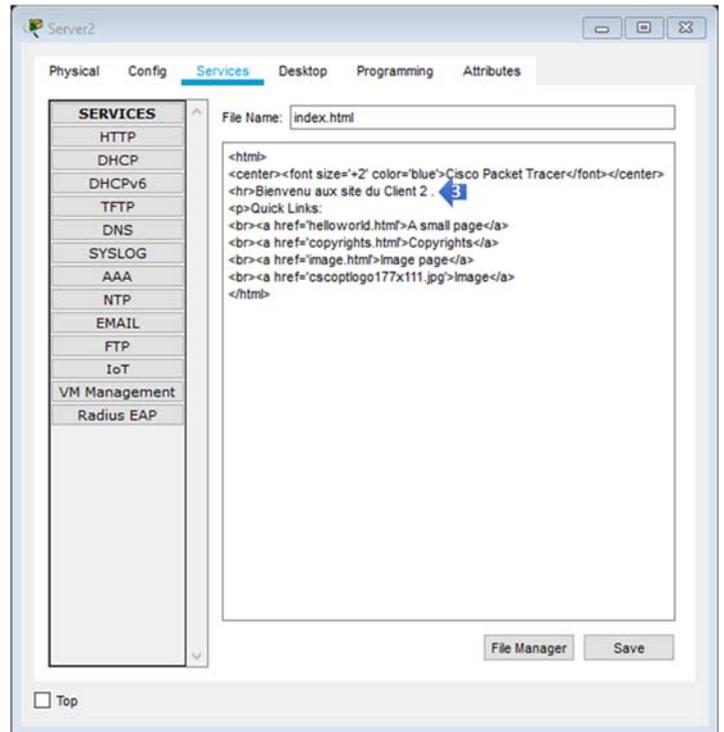
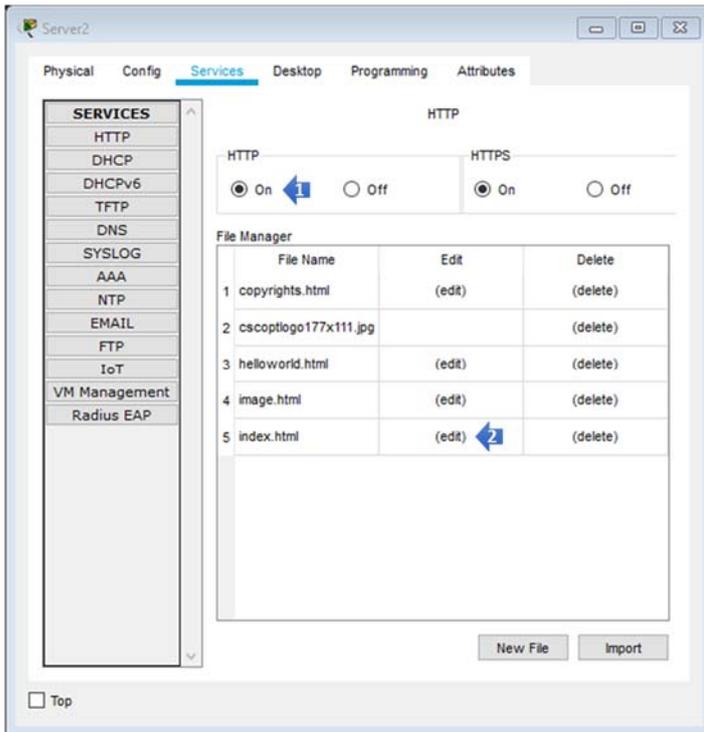
1) Mettre le port g0/1 du commutateur S1 au mode Trunk. Exécuter la commande : **switchport mode trunk**

c) Vérifiez la connectivité. Tous les Serveurs doivent pouvoir s'envoyer des requêtes *ping* les uns aux autres.



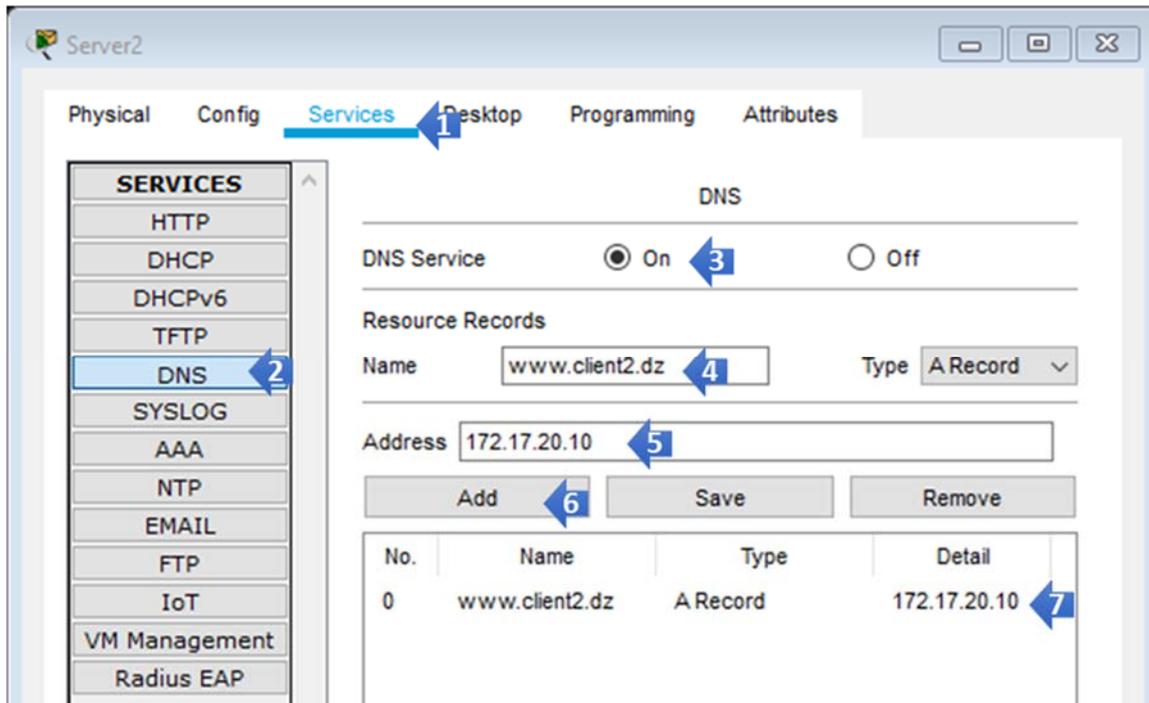
Partie 3 : Filtrage et contrôle d'accès

a) Configurer un service Web au niveau de « Server2 » du client 2. Ce dernier sera un serveur à accès publique avec une page d'accueil nommée « index.html »



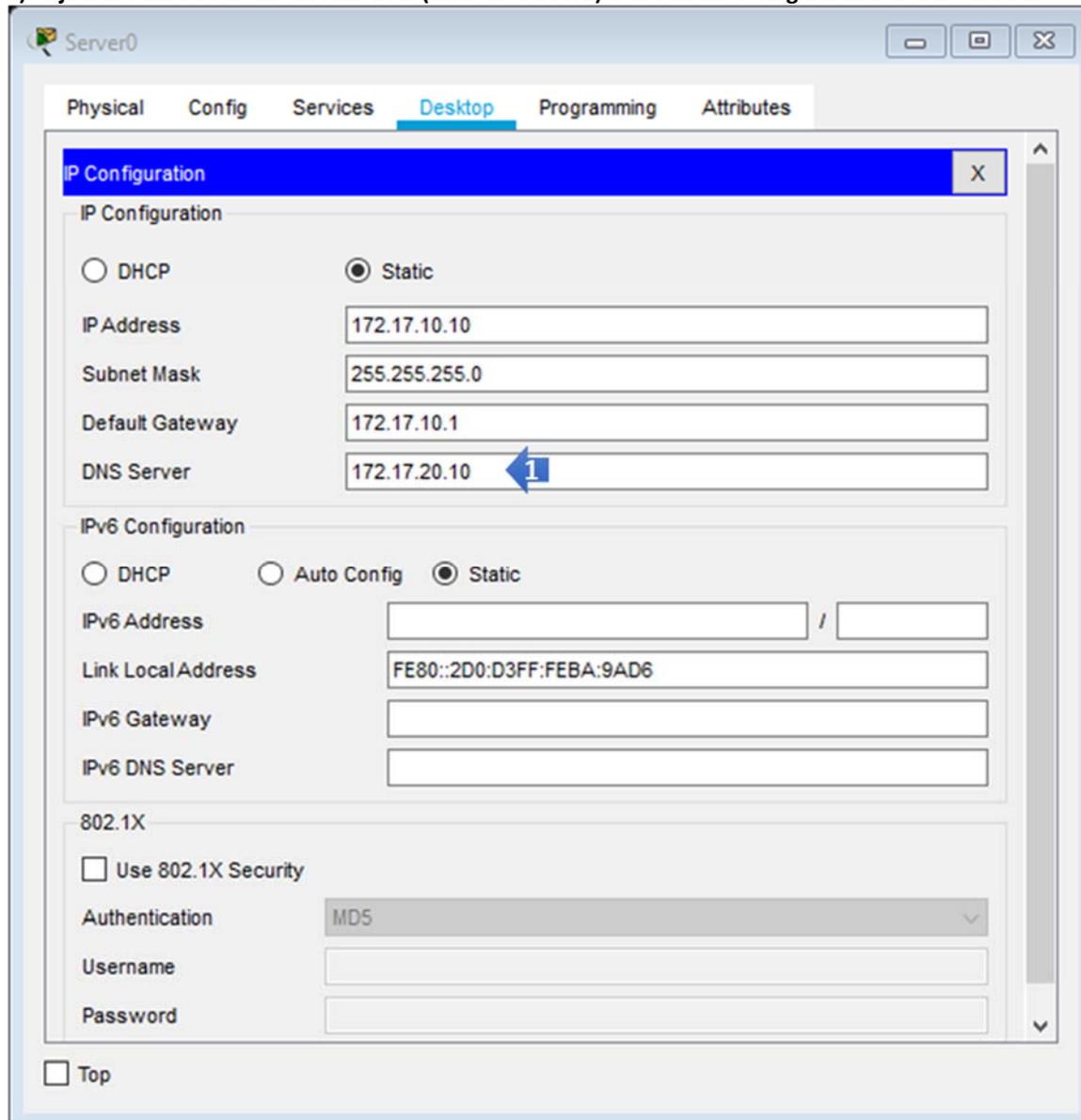
- 1) Assurez-vous que le protocole http est activé
- 2) Cliquez sur « edit » afin de modifier la page d'accueil « index.html »
- 3) Remplacer la phrase "Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open" par «Bienvenus au Site de Client 2 »
- 4) Cliquer **save**

b) Dans « Server2 », configurer également le service DNS et ajouter une entrée associant l'URL www.client2.dz à l'adresse IP de « Server2 » (voir la table d'adressage)

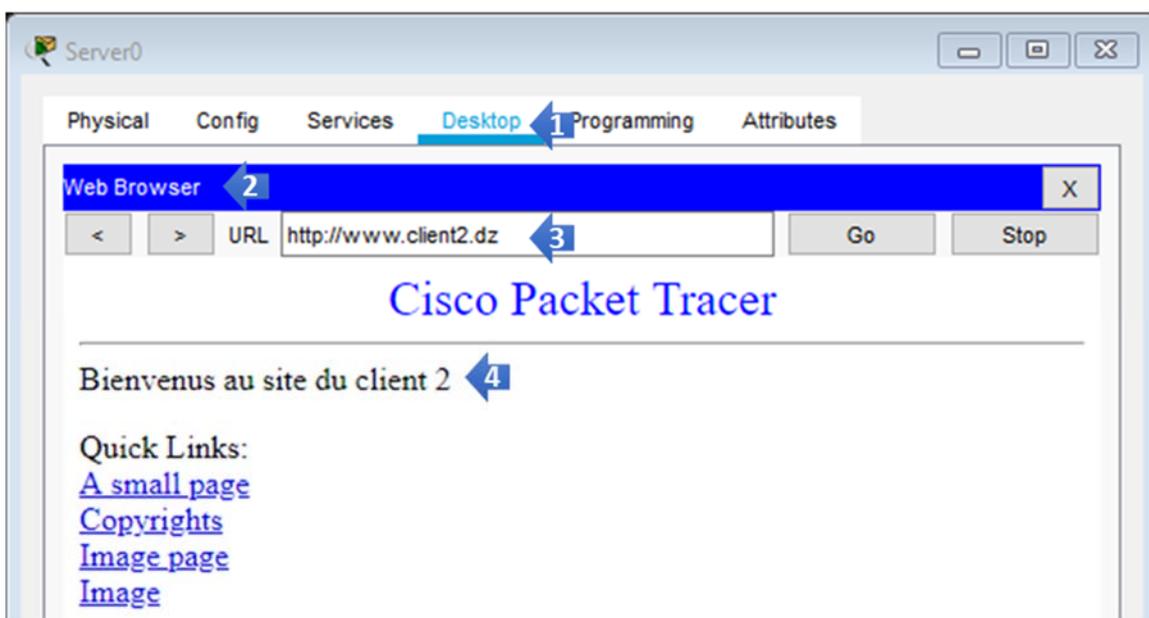


- 1) Cliquer sur « Server2 » puis choisir l'onglet « service »
- 2) Dans la bannière à gauche, cliquer sur « DNS »
- 3) Activer le DNS en cliquant sur « ON »
- 4) Saisir l'URL www.client2.dz dans le champ « Name »
- 5) Saisir l'adresse IP de Server2 dans le champ « Address »
- 6) Cliquer sur « Add » pour créer l'association URL/Adresse IP
- 7) Assurez-vous que l'enregistrement a été créé avec succès puis cliquez sur « Save »

c) Ajouter l'adresse IP du serveur DNS (celle de Server2) à toutes les configurations IP des Serveurs

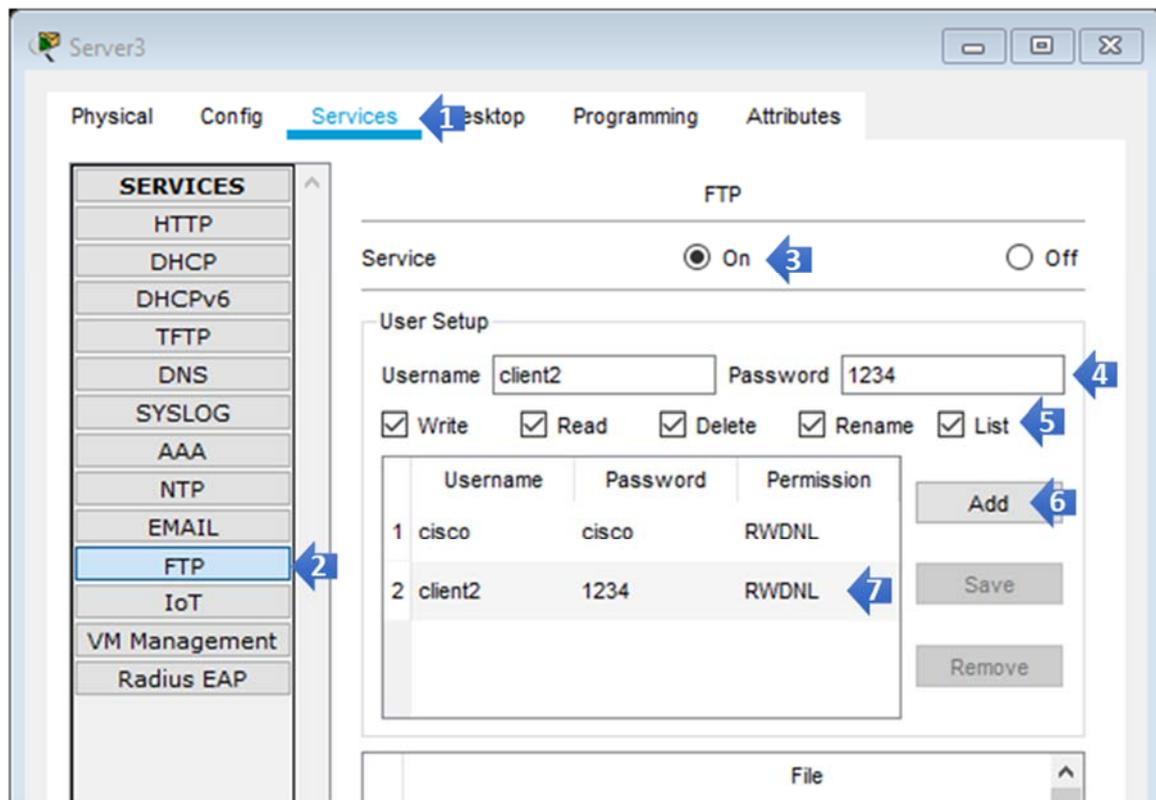


d) Depuis Server0, accéder au site du client2 en saisissant l'URL www.client2.dz dans le navigateur, afin de tester le DNS.



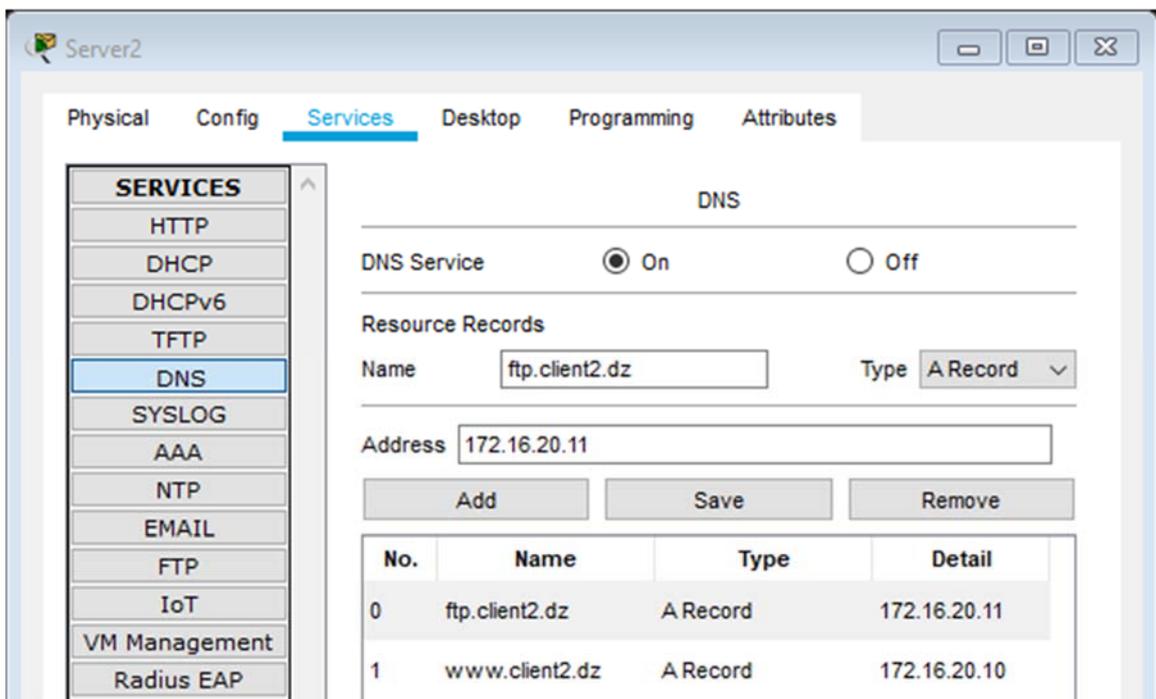
- 1) Cliquer sur Server0 puis choisir l'onglet « Desktop »
- 2) Cliquer sur « Web Browser »
- 3) Saisir www.client2.dz dans la barre d'adresse
- 4) Vous devez voir la page d'accueil après une courte période de temps. Cela prouvera que les serveurs ; Web et DNS sont fonctionnels

- e) Dans Server3, activer et configurer le service FTP. Ajouter l'utilisateur « client2 » avec le mot de passe « 1234 ». Ajouter une entrée DNS pour ce serveur en lui attribuant l'URL <ftp.client2.dz>

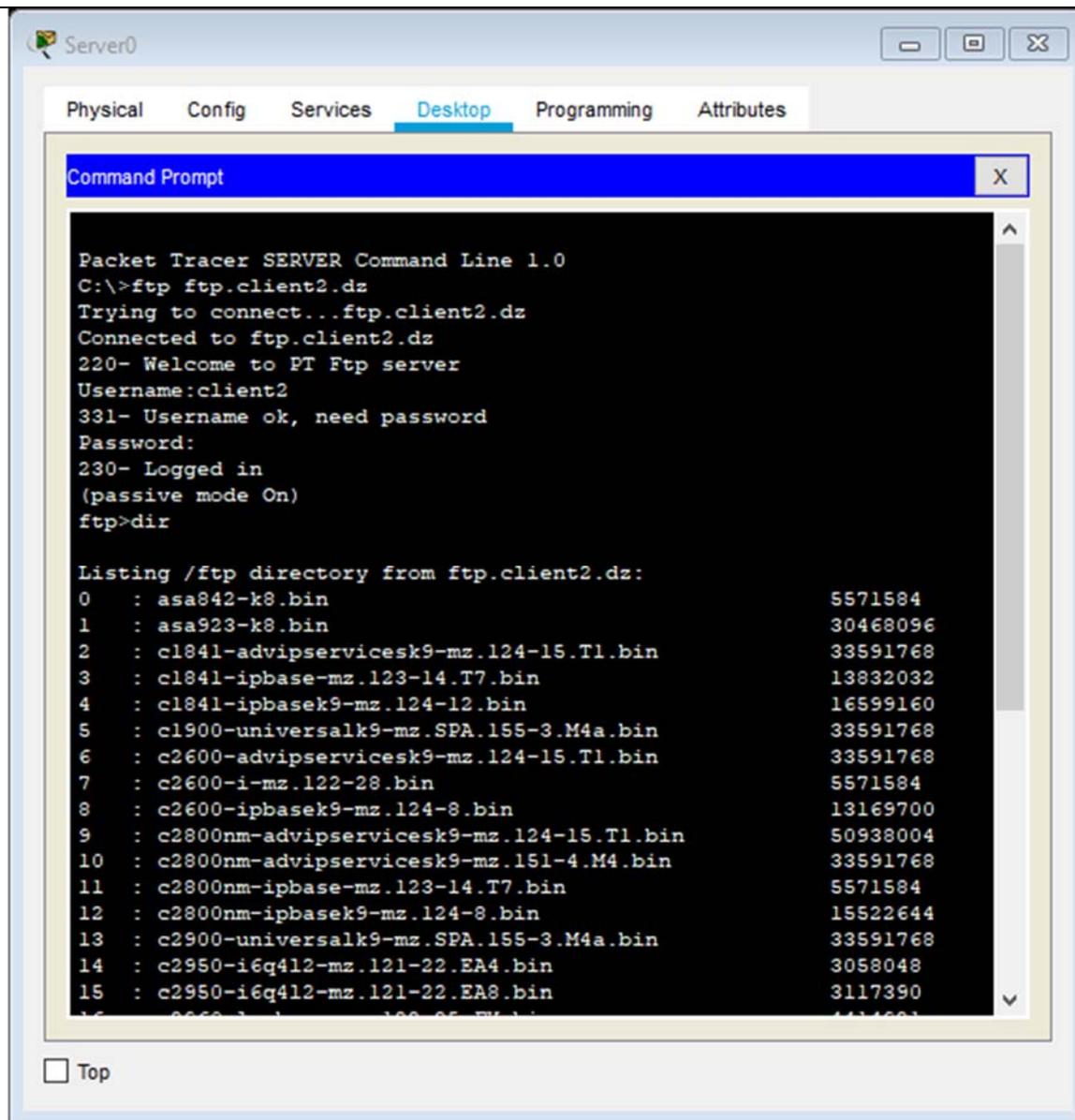


- 1) Cliquer sur Server3, choisir l'onglet « Service »
- 2) Cliquer sur « FTP »
- 3) S'assurer que le service FTP est activé
- 4) Créer un nouvel utilisateur « client2 » ayant le mot de passe « 1234 »
- 5) Attribuer à cet utilisateur tous les privilèges
- 6) Ajouter le nouvel utilisateur
- 7) Vous devez voir le nouvel utilisateur dans la liste des utilisateurs

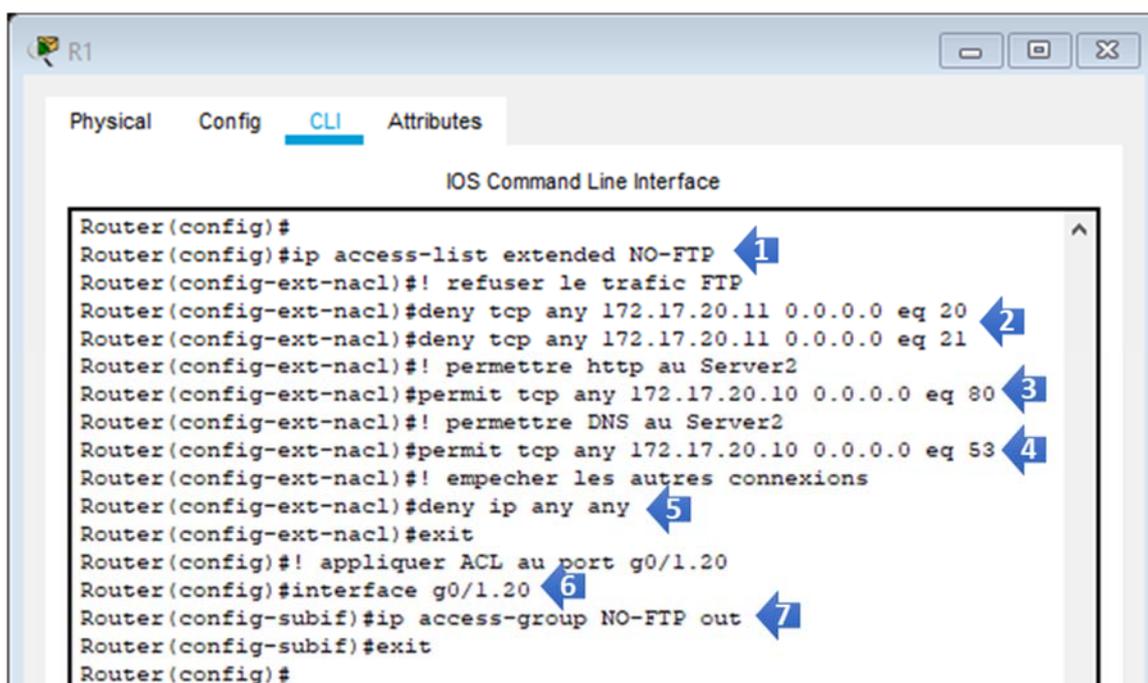
Création d'entrée DNS du service FTP de Server3



- f) Depuis Server0 tester le service FTP configuré dans Server3. Dans le « Command Prompt », saisir la commande `ftp ftp.client2.dz`.



g) Les services Web et DNS du client2 sont censés être publics, alors que l'FTP doit être à accès privé. En vue d'appliquer ces contraintes, créer une ACL étendue nommée NO-FTP, au niveau du port g0/1.20 du routeur R1.



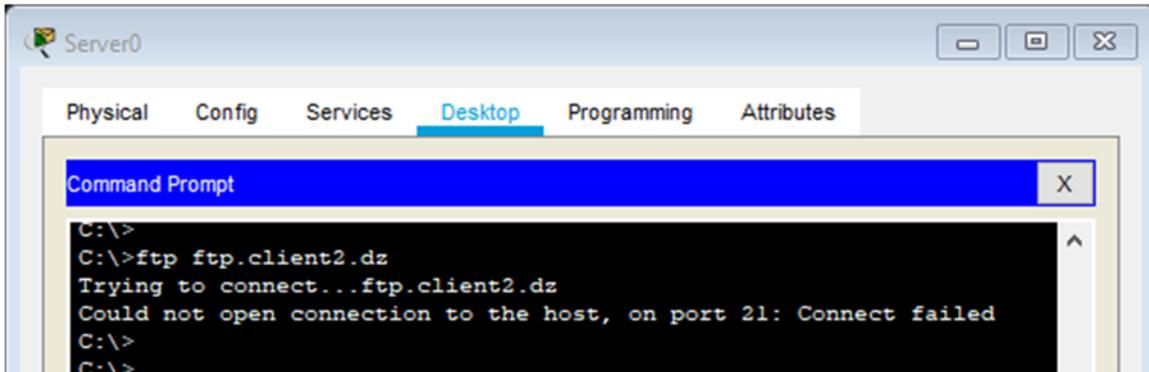
Référez-vous au cours Routage inter-Vlan et Filtrage, de la séance du jeudi 16/01/2020

1) Création du corps de l'ACL étendue, nommée NO-FTP

- 2) Le service FTP requiert 2 connexion, l'une pour le transfert des données (port 20), l'autre pour contrôler le transfert (port 21), par conséquent, deux règle **Deny** sont nécessaires pour refuser les connexions à chaque port.
- 3) Permettre les connexion Http (port 80) au Server2
- 4) Permettre les connexions DNS (port 53) au Server2
- 5) Interdire toute autre connexion. Cette commande est facultative puisqu'elle sera ajoutée implicitement à la fin de l'ACL
- 6) Une ACL est appliquée au niveau d'un port du routeur. Client2 a une autorité sur le port g0/1.20
- 7) Une ACL est appliquée sur un trafic entrant ou sortant du routeur. Le trafic en provenance de l'extérieur et sortant de R1 via g0/1.20 sera filtré afin de ne permettre que les connexions Http et DNS.

h) Vérifier si l'ACL a bien assuré le filtrage du trafic FTP. Lancer une connexion FTP depuis Server0 du client1, ensuite à partir de Server2 du client2.

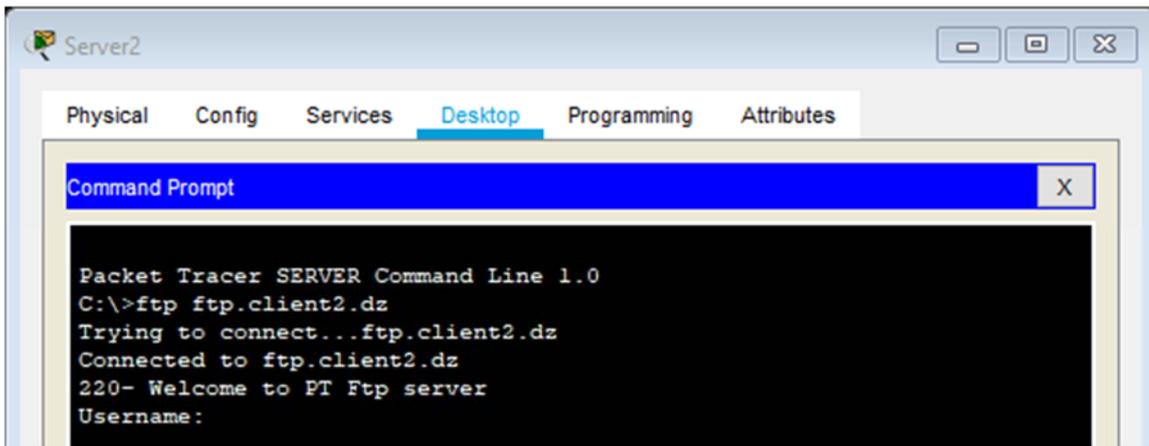
Connexion depuis Server0



The screenshot shows a Packet Tracer desktop environment for Server0. A Command Prompt window is open, displaying the following text:

```
C:\>
C:\>ftp ftp.client2.dz
Trying to connect...ftp.client2.dz
Could not open connection to the host, on port 21: Connect failed
C:\>
C:\>
```

Connexion depuis Server2



The screenshot shows a Packet Tracer desktop environment for Server2. A Command Prompt window is open, displaying the following text:

```
Packet Tracer SERVER Command Line 1.0
C:\>ftp ftp.client2.dz
Trying to connect...ftp.client2.dz
Connected to ftp.client2.dz
220- Welcome to PT Ftp server
Username:
```