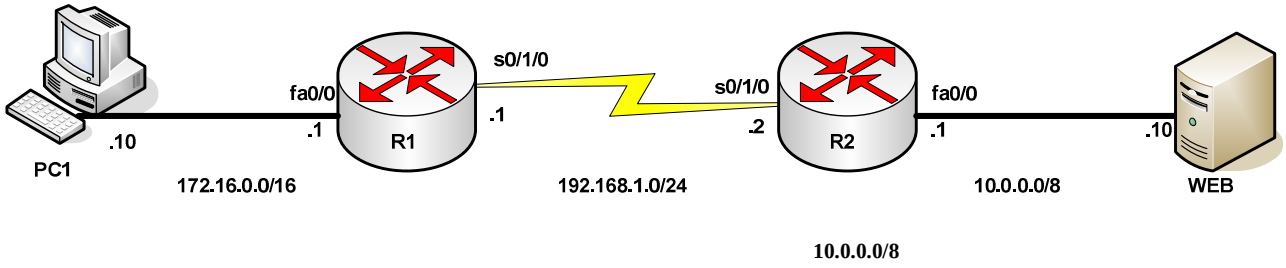
Institut Universitaire de Technologie
Aix*Marseille Université

Réseaux & Télécoms

Analyse TCP et UDP

1. Mise en place de la maquette

Le but de cette première partie est de mettre en place la maquette réseau suivante :



Après avoir branché tous les câbles, vous allez maintenant configurer votre routeur via la connexion à la console :

- Fixez le nom du routeur (attention pas d'espace) ;
- Fixez le mot de passe super utilisateur à `class` ;
- Supprimez la recherche DNS ;
- Fixez le mot de passe pour tous les accès telnet à `cisco.`
- Fixez le mot de passe de l'accès console à `cisco,` synchroniser l'affichage sur la console et fixer le délai d'attente à 2mn et 30s ;
- Affichez un message de bienvenue lors de votre connexion à la console
- Configurez les interfaces de votre routeur ;
- Configurez le routage statique.

Vérifiez que les tests suivants sont couronnés de succès

Test	Résultat
Ping entre votre PC et votre passerelle	
Ping entre votre PC et celui de votre binôme	
Telnet de votre PC sur le routeur de votre binôme	

Si tel n'était pas le cas, corriger les problèmes en :

1. **vérifiant votre câblage**
2. **vérifiant la couche réseau (paramètres IP de votre machine, adresses IP et masque des interfaces de vos routeurs)**

Complétez le tableau suivant en vous aidant de la commande `show interfaces` :

Interface	@MAC	@IP
Fa0/0 de R1		
S0/1/0 de R1		
Fa0/0 de R2		
S0/1/0 de R2		

2. Capture d'un trafic HTTP

L'un d'entre vous fera office de serveur WEB tandis que l'autre officiera en tant que client. Celui dont le PC sera le serveur web, lancera l'application `ZazouMiniWebServer`.

Celui qui agira en tant que client, lancera une capture de trame, ouvrira un navigateur internet et tapera dans la barre de navigation l'adresse du PC "serveur web". Une fois la page chargée, la capture sera arrêtée et vous pourrez répondre aux questions suivantes :

Sur quel protocole de la couche transport `http` s'appuie t-il ?

En étudiant la première trame correspondant à l'envoi du segment `SYN`, complétez les informations suivantes :

@ MAC de la source :	@ MAC de la destination :
@ IP de la source :	@ IP de la destination :
Numéro de port source :	Numéro de port destination :

L'adresse MAC de la destination est-elle l'adresse MAC de la machine de votre binôme ? A quelle machine cette adresse mac correspond-elle ?

Pourquoi le port source n'est il pas celui normalement réservé au protocole HTTP ?

Combien d'ouvertures et de fermetures y a-t-il eu ?
Qui du client ou du serveur a effectué la première ouverture ?
Comment est appelée l'ouverture lorsque c'est le client qui l'a fait ?

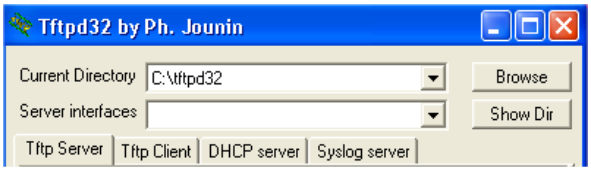
Quelle commande du protocole HTTP, le client envoie t-il au serveur pour récupérer la page d'accueil (examiner le premier segment contenant des données HTTP) ?

En regardant dans la requête contenant cette demande HTTP , répondez aux questions suivante :

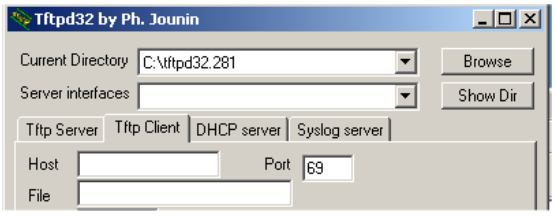
- L'adresse IP du serveur est elle présente ?
- Quelle est la version du protocole HTTP utilisé ?
- Le client indique t-il au serveur les formats d'images qu'il supporte à l'affichage ? Quelle est la couche du modèle OSI en charge de cette fonction ?

3. Capture d'un trafic `tftp`

Avant toute chose, là encore vous devez décider qui sera le serveur et qui sera le client.



Coté serveur rien à faire, vous lancerez juste l'utilitaire `tftpd32`!!!



Coté client vous créerez un fichier texte `essai.txt`. Puis vous lancerez l'utilitaire `tftpd32`, vous sélectionnerez l'onglet `Tftp Client`, et enfin vous indiquerez le nom du fichier et l'adresse IP du serveur.

Lancez alors une capture de trames sur le serveur, puis réalisez le transfert du fichier en cliquant coté client sur le bouton `Put`. Une fois le fichier transféré, arrêtez la capture et répondez aux questions suivantes :

Sur quel protocole de la couche transport `tftp` s'appuie t-il ?

Sur quel numéro de port le serveur est-il à l'écoute de la requête du client ?

Quels sont les numéros de ports utilisés lors des autres échanges ?
Lors de la configuration de son firewall, que devrait faire un administrateur réseau pour que le protocole `tftp` puisse être utilisé ?

Le protocole `tftp`, utilise t-il une fenêtre pour contrôler le flux ?

Quelles sont les valeurs rencontrées pour le champ `opcode` du protocole `tftp` ?

Parmi ces valeurs, lesquelles désignent une requête d'écriture et un acquittement ?
En combien de trames le fichier a-t-il été transféré ?

Avec ce que vous connaissez sur les protocoles `tcp` et `ftp` (ouverture, fermeture, utilisation du port 20 pour le transfert), en supposant que l'échange du password pour `ftp` prennent une dizaine de trames, et en supposant qu'une seule trame suffise pour transférer les données, évaluer le nombre de trames nécessaires au protocole `ftp` pour échanger ce même fichier.

Pourquoi `ftp` nécessite t-il autant de trames ?

Utiliseriez-vous `tftp` sur un LAN ou sur un WAN ?

4. Capture du trafic `telnet` vers le routeur

Capturer une connexion `telnet` entre votre PC et votre routeur, et retrouvez le mot de passe envoyé.

5. Fin

Effacez vos configurations

Débranchez tous les câbles et remettez les en place.

Mettez enfin les PCs en demande d'adresse automatique, puis éteignez les