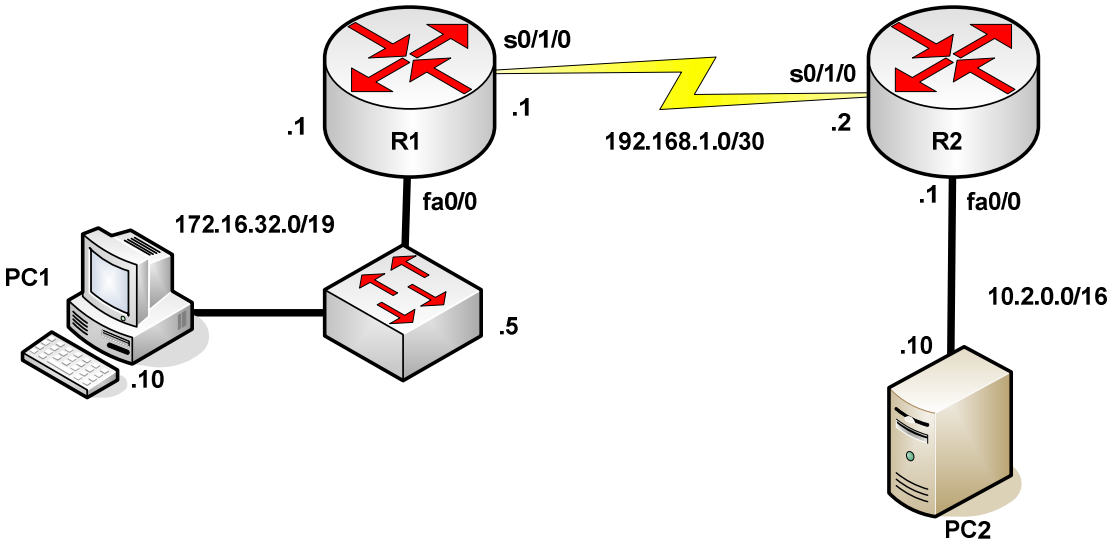
Institut Universitaire de Technologie
Aix*Marseille Université

Réseaux & Télécoms

# Analyse IP

## 1. Mise en place de la maquette

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




Et en utilisant les commandes `ipconfig` sur les PCs, `show interfaces` sur le routeur, et `sh version` sur le commutateur, compléter le tableau suivant :

| | @MAC | @IP |
|---|---|---|
| PC1 | | |
| PC2 | | |
| Fa0/0 de R1 | | |
| S0/1/0 de R1 | | |
| Fa0/0 de R2 | | |
| S0/1/0 de R2 | | |
| commutateur | | |

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.

Configurez les paramètres IP du commutateur.

Vérifiez que les tests ci-dessous **sont couronnés de succès pour les deux membres du binôme** :

| 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 | |
| Ping entre votre PC et le commutateur | |

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)

## 2. Capture d'un trafic IP

Lancer une capture de trames sur le PC1, faites un ping **depuis le PC1 vers le commutateur**, Si le ping est couronné de succès, arrêtez la capture. En examinant cette capture complétez le tableau ci-dessous et répondez aux questions qui suivent :

| | Message `icmp-request` au départ de PC1 | Nom de l'équipement |
|---|---|---|
| Adresse IP Source | | |
| Adresse IP Destination | | |
| Adresse Mac Source | | |
| Adresse Mac Destination | | |

Y a-t-il eu une requête `arp` envoyée par PC1 ?
Si oui pourquoi ?
Si non pourquoi ?

A quoi sert le champ `TTL` du paquet IP ?

A quoi sert le champ `Protocol` du paquet IP ?

Quelle est la valeur du champ `Protocol` ?

Lancer une capture de trames sur le PC2, faites un ping **depuis le PC2 vers le commutateur**, Si le ping est couronné de succès, arrêtez la capture. En examinant cette capture complétez le tableau ci-dessous et répondez aux questions qui suivent :

| | Message `icmp-request` au départ de PC2 | Nom de l'équipement |
|---|---|---|
| Adresse IP Source | | |
| Adresse IP Destination | | |
| Adresse Mac Source | | |
| Adresse Mac Destination | | |

Y a-t-il eu une requête `arp` envoyée par PC2 ?
Si oui pourquoi ?
Si non pourquoi ?

Vous allez maintenant lancer maintenant une capture de trames sur les 2 PCs, puis faire un ping **depuis le PC1 vers le PC2**, et enfin compléter les informations suivantes en croisant les captures sur chacun des PCs :

| | Message `icmp-request` au départ de Pc1 | Message `icmp-request` à l'arrivée de Pc2 |
|---|---|---|
| Adresse IP Source | | |
| Adresse IP Destination | | |
| Adresse Mac Source | | |
| Adresse Mac Destination | | |

Pendant le voyage du paquet, les adresses IP ont elles changé ?
Qu'en est-il pour les adresses MAC ?

Complétez le tableau suivant pour un paquet partant de PC1 et à destination de PC2 :

| | Entre PC1 et R1 | Entre R1 et R2 | Entre R2 et PC2 |
|---|---|---|---|
| @MAC src | | | |
| @MAC dst | | | |
| @IP src | | | |
| @IP dst | | | |

Pour terminer cette partie et préparez la suite, en vous aidant des captures réalisées donnez :

la taille en octet de l'entête du paquet `IP` ?

la taille en octet de l'entête du message `ICMP` ?

## 3. Etude de la fragmentation `IP`

Pour étudier la fragmentation d'un paquet `IP`, nous allons nous servir des options $-\ell$ et `-f` de la commande ping.

A quoi sert l'option –f de la commande ping ?

A quoi sert l'option $-\ell$ de la commande ping ?

Pour commencer, au moyen de la commande `show interfaces` vous allez relever la valeur du `MTU` des interfaces fastEthernet du routeur.

Quelle est la valeur de ce `MTU` ?

Une trame sortant par une interface fastEthernet ne pouvant pas transporter plus de MTU octets, connaissant la taille d'un entête IP et d'un entête ICMP, quelle est la taille maximale d'un message ICMP ? [1]

Afin de vérifier votre calcul, vous allez maintenant lancer une capture de trame sur le PC1, puis **sur le PC1** exécuter successivement les commandes :

1. `ping –ℓ 1472 10.2.0.10`
2. `ping –f –ℓ 1473 10.2.0.10`

Puis, **après avoir arrêter la capture**, vous répondrez aux questions suivantes :

Le premier ping a t-il correctement fonctionné ?

Le deuxième ping a t-il correctement fonctionné ?
Quel message avez-vous eu ?
Qu'est-ce qui dans le paquet IP a empêché ce bon fonctionnement ?

Vous allez maintenant relancer une capture de trames sur le PC1, puis exécuter la commande `ping –ℓ 4500 10.2.0.10`

Puis, **après avoir arrêter la capture**, vous répondrez aux questions suivantes :

Combien de paquets IP ont été nécessaires pour envoyer ces 4500 octets ?

Quelle est la valeur du champ identification sur les fragments et le message `ICMP` envoyé ?
Que constatez-vous ?

Sur le premier fragment l'un des champs `Flag` est-il positionné à 1. Si oui quel est son nom ?
Comment se champ évolue t-il avec les autres fragments ?

En examinant le message `ICMP` qui suit les fragments[2], examiner comment les données ont été découpées, puis complétez le schéma ci-dessous en indiquant les limites du découpage réalisé :

0 4500 - 4507

[1] Si vous ne trouvez pas la valeur 1472, appelez votre enseignant
[2] C'est en fait un fragment, mais Wireshark le présente comme le message ICMP envoyé

## 4. Etude de quelques messages "classiques"

Il s'agit maintenant de modifier notre maquette en y introduisant une erreur consistant en l'occurrence à **supprimer la passerelle par défaut dans les paramètres de configuration du PC2.**

Ensuite, à partir du PC1 vous lancerez une capture, puis vous réaliserez les tests suivants et compléterez, en analysant votre capture, le tableau associé.

| | Nom du message icmp revenu | Valeur du champ type | Valeur du champ code |
|---|---|---|---|
| ping 200.200.200.1 | | | |
| ping 10.2.0.1 | | | |
| ping –i 1 10.2.0.1 | | | |
| ping 10.2.0.10 | | | |

Enfin, pour chacun de tests qui ont "échoués", indiquez l'équipement qui est la cause de l'échec, et précisez pourquoi cet échec a eu lieu

```
ping 200.200.200.1:

ping –i 1 10.2.0.1:

ping 10.2.0.10:
```

## 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**