# TP 2 : Switches et Hubs

## Consignes générales :

- Un compte-rendu par binôme
- Justifiez vos réponses mais soyez concis.

## Objectifs

Expérimenter la découverte d'adresses MAC, les domaines de broadcast et de collision

## Pré-requis

Adresses IP, déploiement sous Marionnet

## Introduction

### Domaine de broadcast, domaine de collision

En communication, une collision se produit lorsque le médium est occupé par n>=2 messages simultanément. Par exemple, lorsque dans une classe deux personnes parlent en même temps, il y a collision et les messages peuvent difficilement être décodés. On dira qu'ils ont été corrompus et une retransmission sera nécessaire.

Un domaine de collision sera défini comme l'ensemble des interfaces tel que si deux interfaces transmettent simultanément, leurs messages entrent en collision.

Un message sera dit diffusé ou broadcasté s'il est destiné à être traité par tout nœud en mesure de le recevoir. Un nœud sera en mesure de recevoir un message moyennant qu'il soit à portée (rattachement physique au réseau) et qu'il dispose de la technologie adaptée. Le nœud émetteur spécifie le caractère boradcasté de sa transmission en modifiant certains champs du message. De manière générale, une adresse de broadcast de niveau 2 sera définie par le protocole régissant la communication. Cette adresse sera renseignée dans le champ « Adresse de destination » des messages diffusés. Dans le TP1, cette adresse spéciale codée sur 16 bits était 0xFFFF.

Un domaine de broadcast sera donc formé par l'ensemble des interfaces tel que tout message émis par l'une des interfaces est reçu par toutes les autres.

### Equipements de réseau

Une fois que nous disposons d'un câble et de quelques postes de travail, il est possible (moyennant des dérivations) de créer un réseau. Ce réseau, néanmoins, ne pourra être très grand en raison des temps de propagation de bout en bout et de l'atténuation des signaux dans le médium. Pour passer outre ces limitations, des équipements réseau tels que les concentrateurs et les commutateurs ont été introduits.

Le concentrateur ou hub a un fonctionnement simple : tout ce qui est reçu sur une interface A est retransmis sur toutes les autres interfaces du hub après mise en forme du signal. Les champs de la trame ne sont pas interprétés lors de la prise de décision du hub.

Le commutateur ou *switch* est un équipement capable de lire les en-têtes de couche 2 des trames le traversant. Il maintient une table de correspondance entre le numéro de ses ports et les adresses MAC des nœuds rattachés. Ainsi, le *switch* fonctionne à la manière d'un aiguilleur : à la réception d'une trame, il récupère l'adresse de destination et cherche dans sa table de correspondance le numéro de port correspondant. Dans une configuration simple, le nœud destinataire est rattaché au même *switch* et la trame est relayée au port. La figure 1 présente ce cas de base.

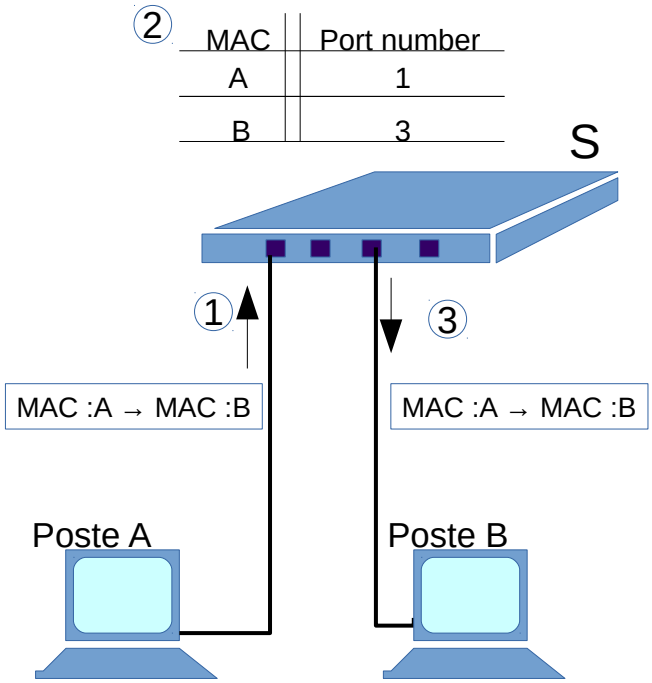

Figure 1 : Relais de trame impliquant les postes A et B et le *switch* S

**Switches et Hubs sous Marionnet**

Durant le TP précédent, vous avez déployé un switch et un hub sous Marionnet. Vous aurez noté que l'interface de contrôle de votre équipement vous indique les interfaces auxquelles un équipement a été raccordé par un voyant vert. Utilisez les résultats du TP précédent pour choisir les moyens de raccordement (câble droit, câble croisé...) durant cette séance.

**Wireshark/Tshark sous Marionnet**

Afin d'explorer les communications, vous disposez d'outils comme Wireshark et Tshark. Leur aide en ligne est disponible en tapant man tshark par exemple sur une CLI.

## Activités

### Création du réseau de base

Le réseau à déployer comporte un hub H1, un switch S1 et 6 postes de travail m1 à m6. Les postes m1, m2 et m5 sont branchés sur H1, les postes m3, m4 et m6 sont branchés sur S1. Finalement, S1 et H1 sont interconnectés.

Les postes de travail exécutent une debian Lenny.

### Questions

1. Une fois que vous aurez créé votre réseau, précisez les liens sur lesquels vous avez utilisé des câbles droits/croisés et expliquez vos choix.
2. Sur l'onglet Interfaces, configurez les adresses IP de vos postes de travail en choisissant des adresses dans la plage 192.168.1.0/24 : vous ferez à chaque fois changer le dernier octet de l'adresse (l'identifiant machine) en conservant les 3 premiers octets (l'identifiant de réseau). Listez dans un tableau les adresses choisies pour chaque machine sur votre CR.

Démarrez votre système en cliquant sur *Sart all*.

3. Connectez-vous à m3 et lancez Tshark. Il s'agit d'un outil en ligne de commande équivalent à Wireshark. Il capture sur une interface réseau (par exemple wlan0 sur votre ordinateur portable) les trames détectées sur le médium.
   - Quelle est l'interface choisie par Tshark ?
   - Comment pourriez-vous spécifier l'interface visée ? (vous pouvez vous aider du manuel)

Par défaut, Tshark vous propose un résumé des trames capturées ; a minima, il affiche l'instant de

réception du message par l'espion, les adresses source et destination et le protocole en exécution. Un bref commentaire est souvent inclus pour permettre de comprendre les objectifs du protocole. Il est possible de le paramétrer pour qu'il produise une trace plus détaillée mais ce sera pour une autre fois…

4. Pendant que Tshark tourne sur le nœud m3, lancez un ping du nœud m1 vers une adresse ne faisant pas partie de votre déploiement mais faisant partie de votre réseau :
   - Quelle adresse avez-vous choisie ? Interprétez le résultat du ping.
   - Comment est affectée la trace produite par Tshark sur m3 ? Quel(s) est (sont) le(s) protocole(s) impliqué(s) ?
5. Pendant que Tshark tourne sur le nœud m3, lancez un ping du nœud m1 vers une adresse ne faisant partie ni de votre déploiement ni de votre réseau :
   - Quelle adresse avez-vous choisie ? Interprétez le résultat du ping.
   - Comment est affectée la trace produite par Tshark sur m3 ? Quel(s) est (sont) le(s) protocole(s) impliqué(s) ?
6. Lancez Tshark sur m5 et exécutez à nouveau le ping de m1 vers l'adresse choisie à la question 4. Comparez les traces de m5 et m3 (collez-les dans un fichier que vous rendrez à la fin de la séance). Les contenus sont-ils les mêmes ? Pourquoi ?

Arrêtez le ping et les sniffeurs. Faites un *clear* de vos terminaux.

7. Redémarrez Tshark sur m3 et m5 puis lancez un ping de m1 vers m2.
   Comment se comportent vos traces de Tshark ? Expliquez (le nombre de lignes, les informations présentées, la durée d'exécution...)

8. Recommencez l'expérience avec les mêmes nœuds exécutant Tshark et un ping de m2 vers m6. Interprétez les résultats du ping et les traces de Tshark.

9. A présent, ajoutez un routeur R1, un switch S2 et deux postes de travail m7 et m8. Branchez S1 et S2 à R1 puis branchez m7 et m8 à S2. Assignez des adresses aux interfaces du routeur et aux nouveaux postes de travail : vous les choisirez dans le réseau 192.168.3.0/24. Activez Tshark sur m7 et lancez un ping de m1 vers m8. Analysez la trace de Tshark produite.

10. En 10 lignes max, mettez en relation les résultats de votre expérimentation et les concepts de domaines de diffusion et de collision.
11. En 5 lignes max, résumez ce que vous avez compris des notions vues durant ce TP.

## Compte-rendu

Le CR contiendra les explications, les analyses de traces et fera référence aux images contenues numérotées.

**NB : Les deux membres du binôme doivent exécuter les manipulations et discuter des résultats pour produire un rapport final à la fin de la séance.**