TD réseau - Réseau : interconnexion de réseau

Réseau : Interconnexion de réseaux, routage et application de règles de filtrage.

Un réseau de grande importance ne peut pas seulement reposer sur du matériel de bas niveau comme les switchs ou les hubs. Les grands réseaux fonctionnent par interconnexion. Des ordinateurs particuliers vont jouer le rôle de lien entre deux réseaux distincts et faire circuler l'information de l'un vers l'autre. Ces noeuds particuliers qui divisent un réseau s'appellent des passerelles. L'intérêt de cette distribution est de limiter l'usage du réseau Ethernet à un nombre réduit d'ordinateurs et d'utiliser le protocole IP pour la transmission d'un réseau vers l'autre.
Nous utiliserons l'outil de simulation Certa pour tester l'architecture de ces réseaux et configurer les services de plus haut niveau, des couches transport et application. Les tests de transmission de paquets sont fait en mode "pas de démonstration", le mode "pas à pas" sera utilisé si vous rencontrez des problèmes.

1) Interconnexion et routage entre deux réseaux

Nous allons travailler à partir du résultat du TP précédent "Couches basses". Reprenez vos travaux. Normalement, les clients et les deux pirates doivent avoir leur IP configurés sur deux réseaux différents (10.2.0.0/16 et 10.3.0.0/16).

Opération 1.1:

- Ajoutez un switch et connectez y deux stations (vendeur1 et vendeur2)
- Configurez leur IP et masque dans le réseau 10.4.0.0/16 (10.4.0.1 et 10.4.0.2)
- Vérifiez que les vendeurs arrivent a communiquer (ping entre vendeur1 et vendeur2)

Nous aimerions mettre en relation vendeurs et clients. La solution en réseau commuté est simple, il suffit de connecter les switchs entre eux pour que la communication soit possible. Toutefois pour éviter les contraintes liés à la commutation dans les grands réseaux, nous allons utiliser un matériel spécial : les passerelles. Une passerelle est un ordinateur particulier équipé de deux ou plus cartes réseau et qui se connecte sur des réseaux différents. Les paquets transitent par la passerelle pour aller d'un réseau vers un autre.

Opération 1.2 :

- Ajoutez deux stations entre les deux réseaux (10.2.0.0/16-10.3.0.0/16 et 10.4.0.0/16), nommez les "G1" et "G2" pour Gateway (passerelle en anglais)
- Configurez ces stations pour les équiper d' une carte normale et d'une carte d'accès distant
- Liez les cartes d'accès distant par une ligne télécom
- Configurez les IPs des cartes d'accès distant sur le réseau 120.1.0.0/16, passez en mode IP et verifiez que la communication entre les deux passerelles fonctionne

Il faut bien sur ensuite relier les passerelles à leurs switchs respectifs

Opération 1.3 :

- Liez G1 et G2 par leur cartes réseaux Ethernet aux switchs des réseaux 10.2.0.0/16-10.3.0.0/16 et 10.4.0.0/16 (cf. Figure1)
- Nous voulons que les clients 1 à 4 puissent communiquer avec les vendeurs. Attribuez le numéro de poste 254 dans le réseau des clients à la carte Ethernet de G1.
- Attribuez l'IP 10.4.0.254 à la carte Ethernet de G2
- Vérifiez la communication entre un vendeur et G2

Question 1.1 :

- Vérifiez la communication entre un client et G1. Cela ne fonctionne pas, pourquoi ? Corrigez ce problème

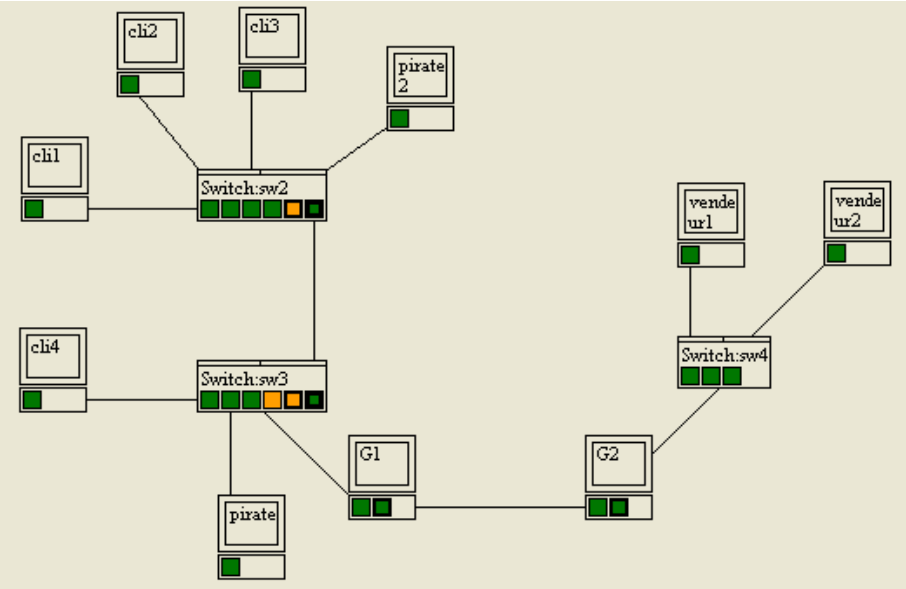

Figure 1 : Interconnexion des réseaux Clients/Pirates et Vendeurs

La communication entre les réseaux n'est pas encore possible. Il faut pour cela configurer G1 et G2 pour le routage et s'occuper d'enregistrer les passerelles respectives pour chaque station du réseau.
Pour configurer les passerelles, un élément du réseau (station, G1 ou G2) se pose la question "par où faire circuler les paquets qui ne sont pas destinées à l'un des réseau auquel j'appartiens?". Par exemple imaginons que "cli1" veuille envoyer un paquet à "vendeur1" :

- L'IP de son réseau est 10.3.0.0/16,
- L'IP du réseau de destination est 10.4.0.0/16
- Le réseau destination est différent de son réseau, il faut faire passer les paquets vers un autre réseau.
- La porte de sortie de son réseau est G1 (10.3.0.254), ce qui correspond à sa passerelle.

On se pose ensuite de la même façon la question de la transition des paquets depuis G1 vers le réseau suivant jusqu'à ce que les paquets arrivent dans le réseau de destination.

Opération 1.4 :

- Dans la configuration IP de G1 et G2, cochez "activer le routage"
- Configurez les passerelles de chaque station du réseau (clients, vendeurs et passerelles ; on ne s'occupe pas des pirates pour le moment). En cas de difficultés, aidez vous des simulations pas à pas pour voir le détail des passages de paquets

Il faut encore écrire des règles de routages qui vont permettre de donner une route pour chaque paquet au travers de l'ensemble du réseau. Pour chaque station du réseau, on définit deux règles :
tout paquet à destination de mon réseau est dirigé via "moi-même" par l'interface appartenant à mon réseau
tout paquet vers un autre réseau est dirigé vers ma passerelle via la l'interface appartenant au réseau de ma passerelle

!! Videz toutes les tables de routages des clients, pirates, vendeurs et G1/G2 !!

Opération 1.5 :

- Créez deux règles dans la table de routage de G1 configurés avec les informations suivantes:
  Règle 1 :
  Adresse de Destination du paquet : "mon réseau" -> "10.3.0.0 masque 255.255.0.0"

Passerelle utilisée : "moi-même" -> "10.3.0.254"
Interface utilisée -> carte appartenant au réseau 10.3.0.0/16 -> "10.3.0.254"

Règle 2 :

Adresse de Destination du paquet : "tout autre réseau" -> "0.0.0.0 masque 0.0.0.0"
Passerelle utilisée : "ma passerelle" -> "120.1.0.2"
Interface utilisée : carte appartenant au réseau 120.1.0.0/16 -> "120.1.0.1"

Opération 1.6 :

- En vous inspirant de l'opération 1.5, Créez les règles des tables de routages de G2, des clients et des vendeurs (deux règles dans chaque table)
- Testez le bon fonctionnement des communications entre vendeurs et clients

2) Interconnexion de VLAN

Au niveau liaison, nous avons isolé les stations pirates sur un VLAN (n°2). Nous souhaitons pourtant pouvoir faire transiter des paquets depuis le VLAN des pirates vers les autres stations. Au niveau IP, le VLAN n°2 des pirates correspond au réseau 10.2.0.0/16 . Nous allons utiliser la passerelle G1 pour cette interconnexion.

Opération 2.1 :

- Ajoutez une carte réseau Ethernet à G1 et câblez le port vers le switch du réseau 10.2.0.0/16-10.3.0.0/16 (Figure 2). Pensez à configurer le port du switch sur le bon VLAN
- L'IP de la passerelle du réseau 10.2.0.0/16 sur G1 est logiquement 10.2.0.254, ajoutez dans G1 une règle de routage des paquets à destination du réseau 10.2.0.0/16
- Configurez les passerelles et les tables de routage sur les stations pirates et testez les communications depuis et vers les pirates

3)Mise en place d'un réseau de serveurs

Il nous maintenant faut mettre en place l'infrastructure d'accueil des services de haut niveau, de la couche application. Nous voulons qu'un serveur WEB et qu'un serveur FTP soient disponibles sur le réseau (Figure2).

Opération 3.1 :

- Dans un nouveau réseau 10.5.0.0/16, ajoutez deux stations reliées à un switch que vous appellerez WEB et FTP. Leurs IPs sont respectivement 10.5.0.1 et 10.5.0.2
- Ajoutez une carte Ethernet à la passerelle G2 que vous lierez au réseau 10.5.0.0/16 (IP 10.5.0.254), complétez la table de routage de G2
- Configurez les passerelles et tables de routage de FTP et de WEB pour qu'ils puissent être joint et joindre tout autre station du réseau

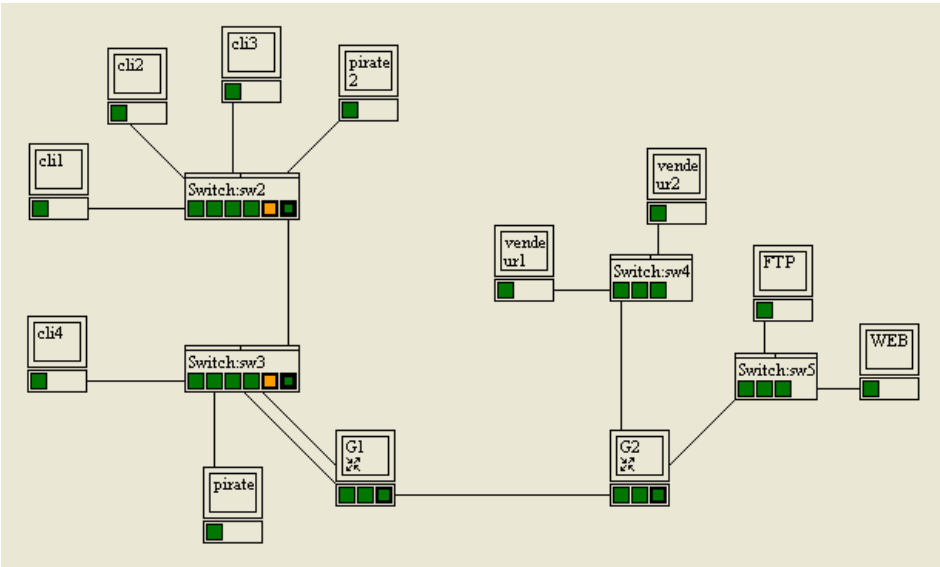

Figure 2 : ajout du réseau Serveurs à l'architecture

Si tout fonctionne, chaque station de votre réseau doit être capable de joindre toute les autres stations. Nous allons maintenant décider qui à le droit de parler à qui dans le réseau.

4) Transport de paquet et règles de tri

Les applications serveur qui utilisent le réseau communiquent via des ports virtuels avec les clients. Le serveur WEB se configure en général pour être actif sur le port 80, le FTP utilise le port 21 ... On pourrait comparer un serveur à un immeuble ou l'appartement 80 est le service WEB. Un client doit sonner à la porte 80 pour accéder au service. Rien n'empêche d'avoir plusieurs services (WEB, FTP, POP, IMAP ...) sur un même serveur. Pourtant dans un soucis d'efficacité et de sécurité, il est souvent préférable de diviser les services entre plusieurs serveurs. Ainsi, dans notre maquette, WEB et FTP sont deux machines physiques différentes.
Dans notre réseau, nous allons imaginer que les clients vont communiquer avec les vendeurs via le port 40. Les vendeurs (au sens logique) deviennent ainsi des serveurs (au sens réseau) écoutant leurs clients sur le port 40

Opération 4.1 :

- Passez en mode "Transport"
- Configurez WEB, FTP, vendeur1 et vendeur2 pour qu'ils écoutent respectivement les ports 80, 21, 40 et 40

En mode transport, on communique à l'aide de requêtes, celles-ci ce composent de l'adresse de destination plus le numéro de port de destination. Vous pouvez essayer l'envoi de requêtes vers les serveurs et constater que ceux-ci n'acceptent la requête que lorsque le port de destination correspond à leur port d'écoute.

Pour finir, nous voulons établir un certain nombre de privilèges dans les communications entre les clients et serveurs. Ainsi par exemple, pas question pour les pirates de pouvoir interroger les serveurs. L'écriture de ces contraintes se fait au moyen d'un ensemble de règles. Toute requête entrante ou sortante d'un réseau doit satisfaire à ces règles sous peine d'être bloquée. Le logiciel qui se charge de vérifier les contraintes est connu sous le nom de "Firewall" (pare-feu).
Les Firewalls se situent sur les points d'entrée-sortie des réseaux, nous en configurerons 2, un dans chaque passerelle.
formalisons la contrainte "un client peut interroger un serveur sur le port 70, en transmission TCP" :

- Dans notre maquette les clients sont situés sur le réseau 10.3.0.0/16
- Le serveur est localisé ailleurs, nous n'avons pas de précision sur son réseau d'appartenance, cela peut être n'importe lequel
- Nous savons que l'interrogation se fait sur le port 70
- Nous n'avons pas d'information sur le port utilisé par le client pour émettre sa requête, cela peut être n'importe lequel
- A priori, le Firewall qui doit contenir cette règle est G1 puisque G1 est le point d'entrée-sortie du réseau 10.3.0.0/16
- La transmission se fait en TCP
- Nous savons enfin qu'il faut autoriser cette règle

La règle s'écrit de cette façon :

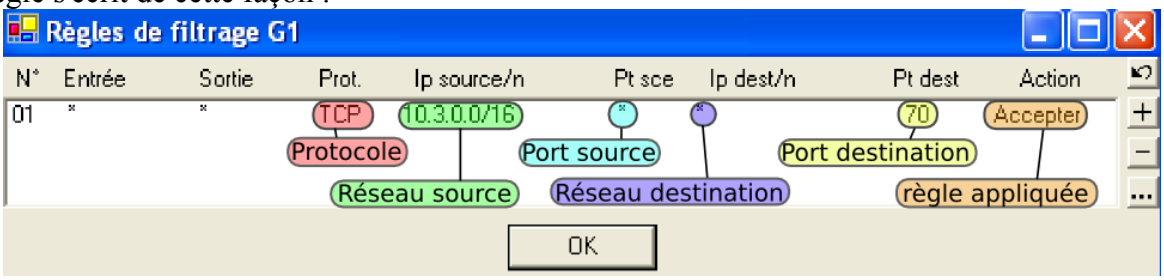

Figure 3 : exemple de règle de filtrage

Les règles s'écrivent en mode transport, dans tables et règles de filtrage. Le comportement par défaut est de tout refuser, il faut donc écrire des règles qui autorisent les paquets à circuler.

Cahier des charges :

- Toutes les communications se font en TCP
- Les pirates doivent êtres bloqués sur leur réseau
- Un client doit pouvoir transmettre des données vers des stations ou serveurs écoutant les ports 80 (Web) et 40 (Vendeurs)
- Les serveurs doivent recevoir les paquets dont le port de destination est 80
- Les vendeurs reçoivent les paquets dont le port de destination est 40
- Seuls les vendeurs peuvent accéder aux serveurs via le port 21
- Serveurs et vendeurs doivent pouvoir répondre aux requêtes TCP
- Les clients doivent accepter les réponses des serveurs et des vendeurs (celles-ci s'effectuent sur des ports de destination aléatoires mais ont pour ports source 80,21(serveurs) et 40(vendeurs))

Question 4.1 :

- Pour chaque règle, donnez sur feuille les adresses des réseaux de destination et d'origine

Opération 4.2 :

- Répartissez les règles entre les deux firewalls de G1 et G2
- Écrivez et testez ces règles dans l'outil de simulation.

Si les règles sont bien écrites, on doit pouvoir changer les IPs des stations dans les différents réseaux (10.2.0.0/16, 10.3.0.0/16, 10.4.0.0/16 et 10.5.0.0/16) sans avoir à modifier les règles de filtrage. C'est un bon moyen de savoir si vos règles sont correctes.

Opération 4.3 :

- Essayez de changer l'IP du serveur Web et testez les communications depuis et vers le serveur Web.

5) Conclusion

Vous avez maintenant de solides notions du fonctionnement des réseaux sur les couches physique, liaison, réseau et transport.

Certains sujets n'ont pas été abordé dans ce TD. Nous n'avons pas parlé du transport de paquets sur Internet, de la translation d'adresses ou encore de l'association entre un nom de machine et son IP, de la nouvelle norme pour l'adressage IPV6, etc. Le domaine des réseaux est encore très vaste...

Remerciements à Pierre Loisel pour le développement de l'outil de simulation et pour sa mise à disposition (http://www.reseaucerta.org/outils/simulateur/)