Réseaux 2
TCP/IP, NAT/PAT et Firewall

Nicolas Baudru & Nicolas Durand

Année 2011-2012 2e année IRM – ESIL

Attention !
Vous devez rendre pour chaque exercice un fichier .xml correspondant à votre simulation.
Vous devez aussi rendre un document contenant les conclusions obtenues tout au long du TP.
Vous nous les enverrez à l'une des adresses suivantes (selon votre groupe) :
nicolas.durand@univmed.fr nicolas.baudru@univmed.fr

Exercice 1. Mode IP et mode transport

Vous connaissez déjà ce simulateur, nous l'avons utilisé précédemment, pour la partie "Ethernet et VLAN" et pour la partie "IP, routage et sous-réseaux". Nous allons maintenant essayer de configurer les couches supérieures (IP et UDP/TCP) en abordant aussi le NAT/PAT et les firewalls.

Nous repartirons de la simulation obtenue à la fin du TP "Ethernet et VLAN", dans laquelle nous supprimons
- le câble entre les swichs 4 et 5,
- le câble entre les swichs 1 et 5,
- un des deux cables entre les swichs 2 et 3.

Le résultat obtenu correspond à la figure 1 ci-dessous.

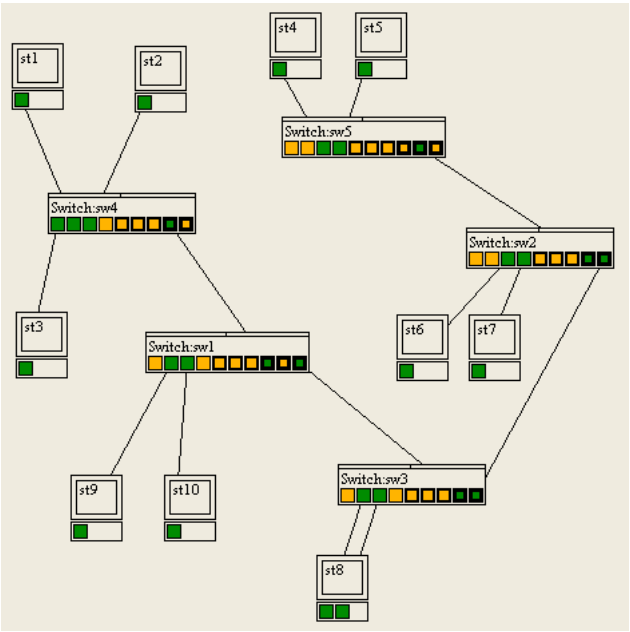

FIGURE 1 – Réseau de départ

Rappel : les switchs gèrent les Vlans de niveau 2, les postes impaires sont sur le Vlan 5 et les paires sur le Vlan 6. Dans ce TP nous utiliserons le mode "pas à pas", l'intérêt de ce mode est de montrer chaque étape effectuée par tous les noeuds du réseau. L'intérêt est donc de lire ce qu'il se passe et non pas de faire « suivant » sans rien lire. Notamment lorsqu'une erreur se produit, votre premier réflexe doit être de constater à quel moment il y a un problème : il ne trouve pas de correspondance ARP, une règle de filtrage ne s'applique pas, il n'y a pas de route correspondante, ...

1. Ajouter un switch indépendant avec 3 postes (cf. figure 2).

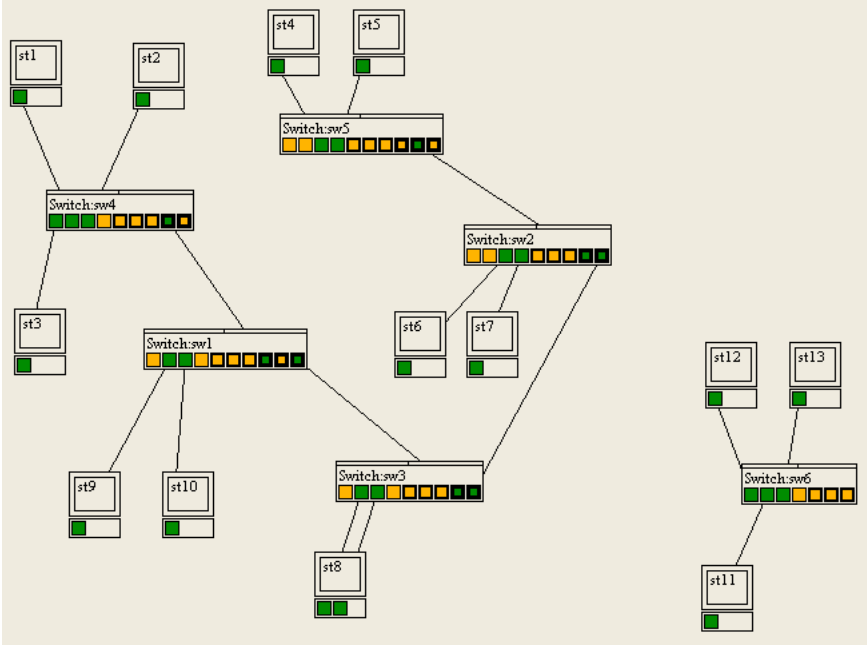

FIGURE 2 – Réseau de la question 1

2. En mode IP (F4) ; donner une adresse IP à chaque poste de ce nouveau réseau dans la plage 192.168.0.0/24 (en cliquant droit sur la carte réseau). Ne pas mettre de passerelle par défaut pour l'instant. En mode IP, quand on passe la souris sur la carte, la configuration s'affiche, sur la machine c'est la passerelle qui s'affiche.
3. Envoyer un ping depuis st12 vers st13. Observer le fait que pour faire le ping le poste st12 doit d'abord effectuer une requête ARP.
4. Observer la table de cache ARP de la station st12, st13 et st11. Refaire un ping depuis st12 vers st13 et observer la différence.
5. Faire un ping depuis st11 vers st12, observer que st11 connaît l'adresse mac de st12.
6. Ajouter une carte réseau à st11, puis ajouter un nouveau switch auquel on connecte la nouvelle carte de st11 et un nouveau poste st14 (cf. figure 3).
7. Configurer la seconde carte de st11 et st14 sur le réseau 192.168.1.0/24. Essayer un ping depuis st12 et st14 vers st11.
8. Quand on teste un ping depuis st12 vers st14, cela ne marche pas car st11 n'est pas encore un routeur. Configurer la station st11 comme un routeur (activer le routage) et tester à nouveau un ping depuis st12 vers st14.
9. Le ping ne devrait toujours pas fonctionner si on n'a pas mis de passerelle par défaut car la station st12 n'a aucune idée de comment atteindre le réseau de la station st14. Mettre dans st12, st11 comme passerelle par défaut. Tester encore une fois le ping de st12 vers st14.
10. Le ping doit maintenant atteindre la station st14 mais ne revient pas et un message délai trop long s'affiche. Cela vient du fait que st12 est maintenant correctement configurée mais que st14 ne l'est pas (il n'a pas de passerelle par défaut) et ne peut donc pas renvoyer le message de retour vers st12. Corriger le problème et configurer correctement tous les postes du réseau pour qu'on puisse faire un ping de n'importe quel poste vers n'importe quel autre poste (de st11 à st14).
11. En mode transport, simuler un serveur Web sur le poste st14 en écoutant le port TCP 80.
12. Envoyer une requête TCP depuis st12 vers st14 (navigateur web vers un serveur web).
13. Écouter le port UDP 53 sur le poste st14 et envoyer une requête UDP depuis st12 vers st14.
14. En mode transport, on ne peut plus envoyer un ping mais on peut envoyer un message ICMP (le ping est un message ICMP ...). Envoyer une requête ICMP depuis st12 vers st14.

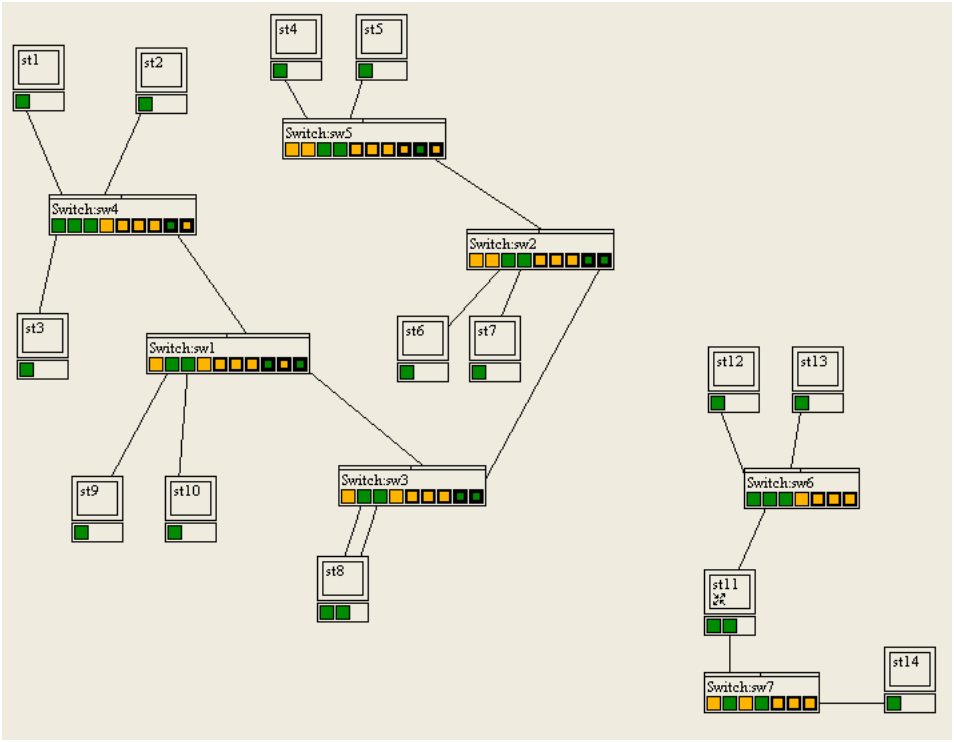

FIGURE 3 – Réseau de la question 6

15. Sur le poste st14 consulter les échanges en cours : un poste mémorise toutes les requêtes reçues en attendant qu'on renvoie une réponse. Répondre aux requêtes précédentes en utilisant "répondre à une requête" dans le menu de st14.
16. Tester l'envoi d'une requête TCP depuis st12 vers le port 110 de st14 sans l'avoir écouter avant sur st14 pour observer l'erreur produite.

Exercice 2. NAT/PAT

17. Faire encore un autre réseau indépendant avec un switch et 2 postes, st15 et st16 (cf. figure 4). La plage d'adresse utilisée sera 172.16.0.0/16, st15 sera la passerelle par défaut de ce reseau (à configurer dans st16).
18. Ajouter Internet, une carte d'accès à distance à st15 et st11 (ces 2 postes doivent être des routeurs) et connecter ces 2 routeurs à Internet, attention à bien utiliser des lignes de télécom.
19. Sur notre réseau Internet il y a 2 FAI différents, connecter st15 et st11 chacun à un FAI différent. Le FAI attribue automatiquement une adresse IP aux postes connectées. Observer les adresses IP attribuées.
20. Envoyer un ping (en mode IP) de st15 vers st11 (vers son adresse attribuée par le FAI bien sûr) et exécuter la réponse. (Avez-vous pensé à mettre une passerelle par défaut à vos routeurs vers le routeur du FAI ?)
21. Envoyer maintenant une autre requête ICMP (en mode transport) depuis st16 vers st11. Le message devrait bien arriver à destination. Essayer d'exécuter la réponse. Cette dernière ne revient pas à st16, pourquoi ?
22. En effet st16 possède une adresse privée dans un réseau privé, il peut envoyer des paquets vers l'extérieur mais personne ne peut lui répondre. Pour pouvoir donner accès à Internet aux postes du réseau privé il faut que le routeur d'accès fasse une translation d'adresse de type NAT. Ajouter la fonction Nat/Pat à st15 en sélectionnant bien l'interface ppp. Essayer ensuite de nouveau d'envoyer une requête ICMP depuis st16 vers st11 et d'exécuter la réponse (observer la translation d'adresse et le retour possible).
23. Essayer d'envoyer maintenant une requête TCP depuis st16 vers le serveur web de st14. En fait st14 est sur un réseau privé, on ne peut donc pas le joindre depuis l'extérieur à moins que ... on utilise une redirection statique de port grâce au NAT du routeur d'entrée de son réseau. Activer donc le Nat/Pat sur st11 (en sélectionnant l'interface ppp) et ajouter dans la table de Nat/Pat une entrée pour rediriger les paquets arrivant sur le port 80 de st11 vers le port 80 de st14.

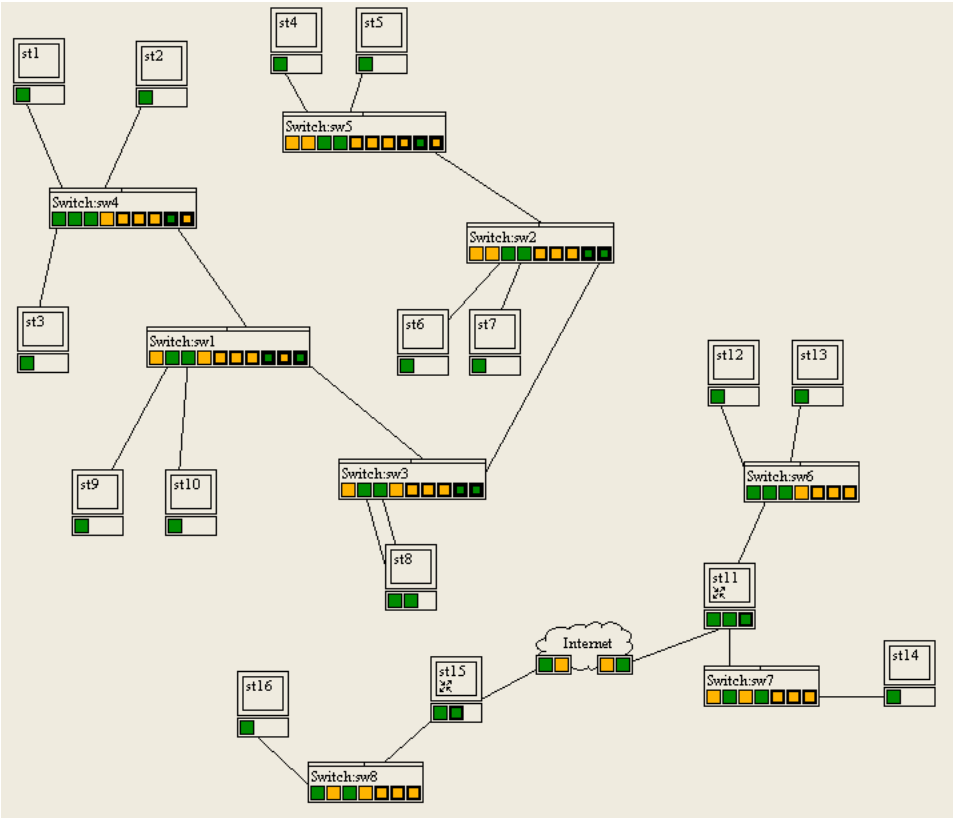

FIGURE 4 – Réseau de la question 17

24. Envoyer donc une requête TCP depuis st16 vers le serveur web de st14 et renvoyer la réponse.
25. Configurer les postes st1 à st10, le vlan 5 utilisera la plage d'adresse 10.0.5.0/24, le vlan 6 la plage d'adresse 10.0.6.0/24. Vérifier la bonne configuration en envoyant des ping entre les postes du vlan 5, puis entre les postes du vlan 6.
26. Activer le routage sur st8 et configurer sa table de routage pour permettre le trafic entre les deux Vlans. Mettre st8 comme passerelle par défaut dans chaque poste du réseau.
27. Tester votre configuration en envoyant un ping de st1 vers st2, et inversement (vérifier bien les tables de routage des stations présentes dans les deux Vlans).
28. Connecter st8 à internet, et lui ajouter la fonction de NAT/PAT.
29. Envoyer une requête TCP depuis st1 (puis st2) vers st14 et renvoyer les réponses.
30. Écouter le port 80 sur st1 et sur st2, sur le routeur Nat d'entrée de ce réseau rediriger le port 8080 vers le serveur Web du Vlan 5 et le port 80 vers le serveur Web du Vlan6.
31. Depuis st12 envoyer une requête vers le serveur web du Vlan 5 et une autre vers le serveur Web du Vlan 6. Ne pas oublier de renvoyer les réponses.

Exercice 3. DMZ et Firewall

32. Ajouter un dernier poste (st17) directement connecté à Internet (cf. figure 5). Attention, un bug du simulateur empêchera de mettre une passerelle à st17 tant qu'il n'y aura pas d'adresse IP sur sa carte réseau même si on ne s'en servira pas ...
33. Envoyer une requête depuis st17 vers le serveur Web de st14.
34. Sur le poste st17 configurer le fichier host pour que le nom "sas" soit associé à l'adresse IP publique de st11.
35. Écouter le port 22 (SSH) sur st14 et rediriger le port 22 sur le Nat de st11 vers st14.
36. Envoyer une requête TCP depuis st17 vers le serveur SSH de "sas".

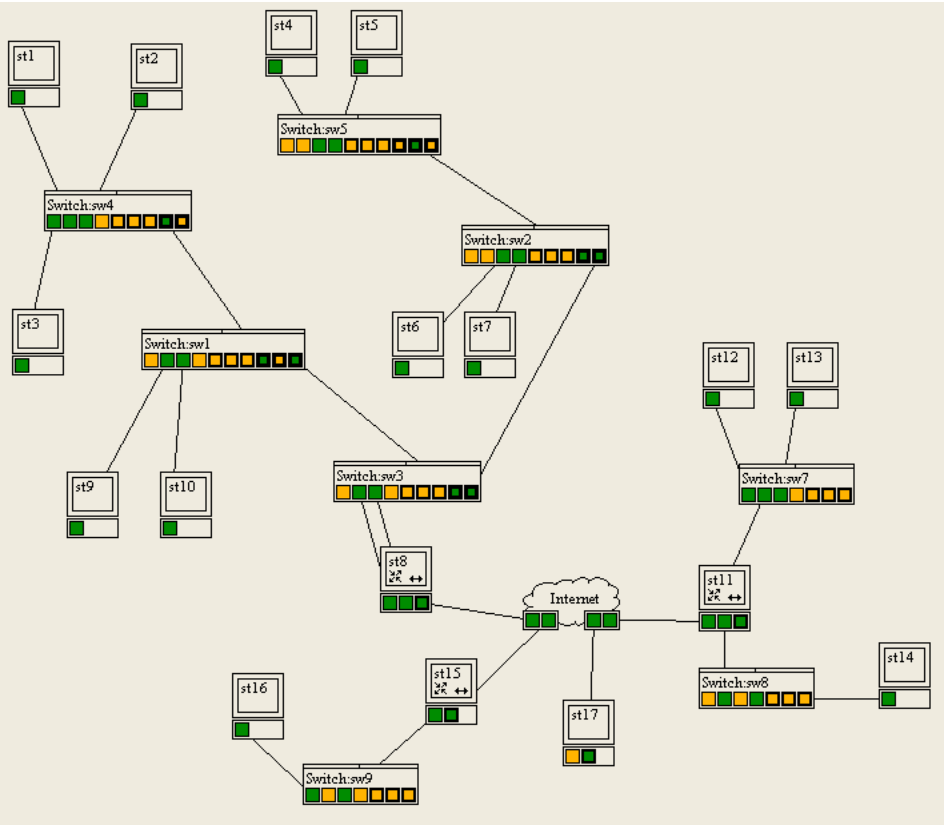

FIGURE 5 – Réseau de la question 31

37. Écouter le port 22 sur st13 et vérifier que st14 puisse envoyer une requête TCP sur le port 22 que st13.
38. Dans le réseau privé de st11 à st14, le réseau 192.168.1.0/24 représente la DMZ, le réseau 192.168.0.0/24 représente la zone à sécuriser. Configurer le firewall (règles de filtrage) de st11 pour que tout le monde puisse atteindre le serveur web dans la DMZ mais que seul st17 puisse atteindre le serveur SSH. Bloquer tout autre type de trafic. Tester depuis st16 le serveur Web et SSH de “sas”.
39. Tester depuis st17 le serveur Web et SSH de “sas”.
40. Maintenant que le firewall est actif, tester l’envoi d’une requête TCP sur le port 22 de st13 depuis st14. Tester aussi l’envoi d’un message de st12 vers l’extérieur ...
41. Corriger les règles de filtrages afin que st12 et st13 puisse accéder à Internet et que st14 puisse accéder au port 22 de st13.
42. Vérifier les règles de filtrages en essayant d’envoyer depuis st16 un paquet vers st12 ou st13. Vérifier que le firewall interdit l’accès à ces postes même si on ajoute dans le NAT/PAT une redirection statique d’un port vers st12 ou st13.