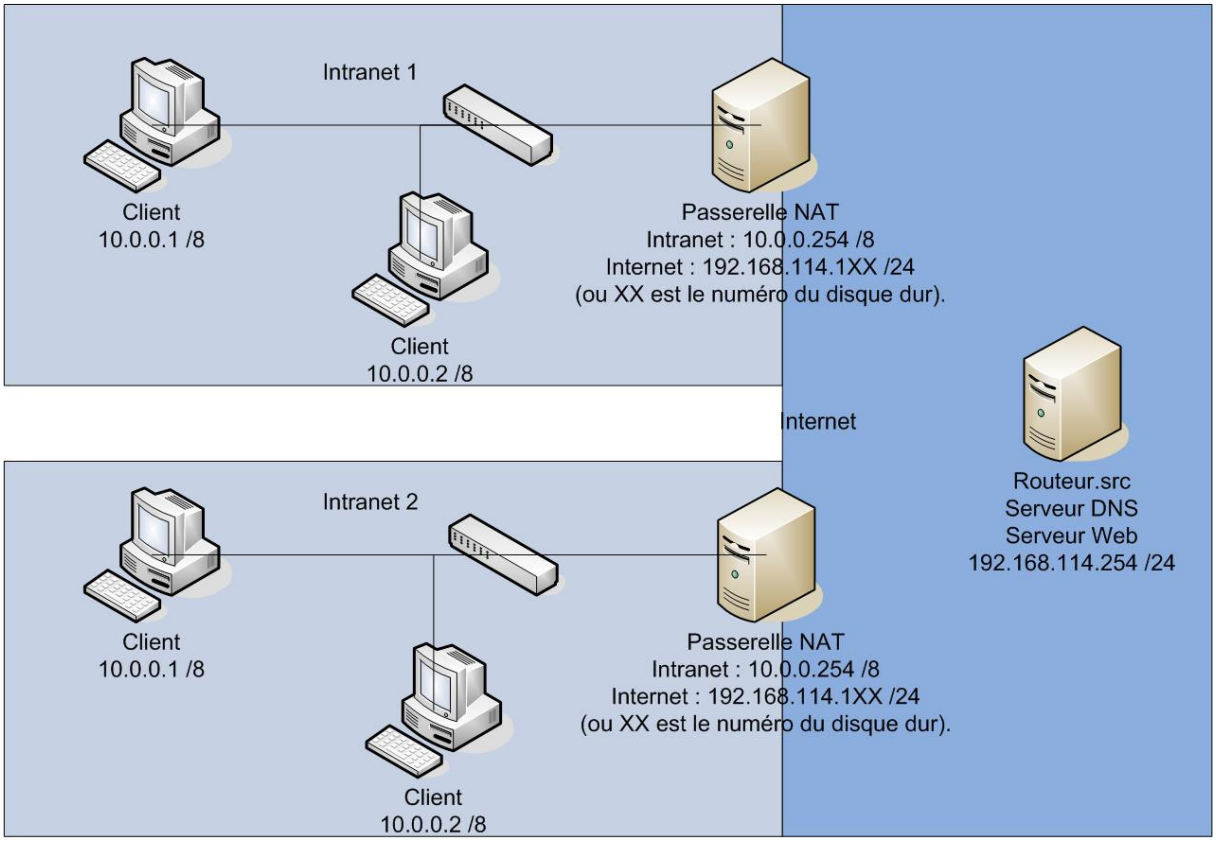
NAT et DHCP

Nous allons dans ce TP mettre en place un intranet composé d'une machine et du passerelle permettant un partage de connexion vers Internet.

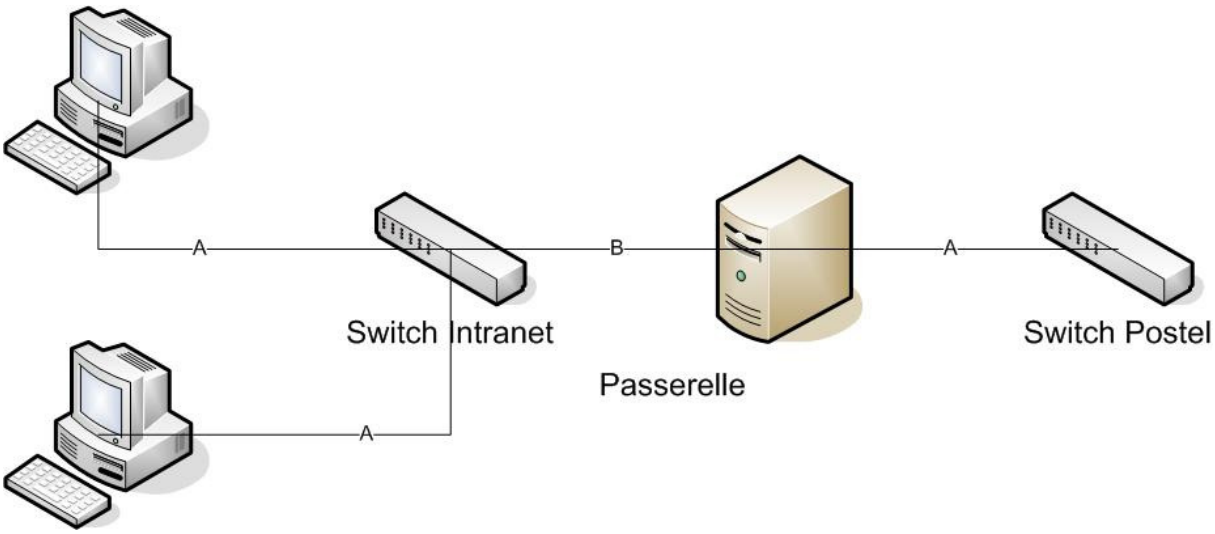
Vous allez mettre en place une passerelle NAT (Network Address Translation).
Le NAT est une technique permettant de masquer les adresses du réseau local par translation d'adresse. C'est cette technique qui est utilisée chez vous pour partager votre connexion Internet, vous disposez de plusieurs machines sur votre intranet avec des adresses IP privées et une adresse publique fournie par votre fournisseur d'accès à Internet. Pour sortir de votre intranet vous allez translater vos adresses privées vers votre adresse publique et inversement vous allez translater une adresse publique en une adresse privée pour rentrer dans votre intranet.

Gestionnaire des adresses privées de votre intranet vous allez mettre en place un serveur DHCP (Dynamic Host Configuration Protocol), ce serveur fournira dynamiquement une configuration IP aux clients DHCP.

Plan d'adressage et câblage



Pour mettre en place votre passerelle NAT, vous utiliserez une machine de numéro impair et deux machines de numéros pairs comme machines de votre intranet.
Sur la passerelle NAT vous laisserez le câble A branché sur le switch de la salle et vous utiliserez le câble B pour accéder au switch de votre Intranet. Sur les machines clientes vous relierez le câble A à votre switch.



Une fois le câblage mis en place, les interfaces reconnues par l'OS vous réaliserez le plan d'adressage précédant. Vous choisirez bien entendu les bonnes passerelles par défaut, puis avec des « pings » vous testerez la connectivité entre le client et la passerelle, entre la passerelle et les autres passerelles.
Pourquoi un « ping » depuis le client vers 192.168.114.254 ne marche t-il pas ?
La condition d'unicité de l'adresse IP vous semble-t-elle réalisée sur l'ensemble du réseau, sur ce que va devenir votre Intranet.

NAT

La mise en place de la translation d'adresse et réalisée par l'utilisation du service de Routage et d'accès distant (Remote Access Service).

Nat Basique

Vous choisirez une configuration personnalisée avec NAT et routage réseaux.
Puis vous ajouterez pour le NAT une interface publique (Internet) sans *firewall* et une interface privée (Intranet).
Enfin vous testerez votre configuration depuis le client avec un ping vers 192.168.114.254 et la consultation de l'URL : http://192.168.114.254.

La configuration précédente permet à un client d'accéder aux services d'Internet mais une machine d'Internet peut-elle accéder à un service rendu par une de vos machines ?

Réaliser deux captures simultanées sur la passerelle, une sur l'interface de l'Intranet et une autre l'interface de l'Internet et consulter l'url : http://192.168.114.254. Observez les modifications dans les adresses IP et les ports.
Proposer une explication du fonctionnement du NAT.

Tous les services sur la passerelle

Pour placer un serveur visible sur Internet la solution la plus simple et de le placer sur la passerelle.
Dans un premier temps, nous allons donc mettre en place un serveur http et un serveur ftp sur la passerelle puis désactiver ces serveurs si ils sont présents sur les clients. Une fois la

configuration mise en place nous allons tester depuis les clients et les passerelles l'accès à ces services. Vous testerez d'abord depuis vos clients puis depuis les clients de vos voisins.

Pour ne pas surcharger le travail de la passerelle, il est d'usage de placer les serveurs sur des machines de l'intranet et de mettre en place au niveau de la passerelle du « port forwarding » ou du « port mapping ».
Avant d'aller plus loin vous devez désactiver le serveur http et le serveur ftp présents sur la passerelle et activer les serveurs sur l'un de vos serveurs.

Le ftp et l'http sur le client (miroir de port)

Activer le serveur Web et le serveur ftp sur un client, vous les personnaliserez avec une page html pour le premier et une bannière pour le second. Puis vous testerez votre configuration depuis vos machines, depuis une des passerelles de vos voisins, conclusion ?

Sur la passerelle activez le miroir de port pour ces deux services et renouvelez vos tests avec les adresses des passerelles réalisant le miroir de port et non plus les adresses des clients où les serveurs s'exécutent physiquement.

DHCP

Le serveur DHCP offert par Windows avec le NAT n'est pas très performant, il ne permet pas par exemple de réaliser une affection de configuration IP en d'une adresse MAC. Nous allons donc utiliser le serveur DHCP fourni avec windows.
Vous allez devoir activater et configurer le serveur DHCP puis configurer les postes client en client DHCP.

Création d'une étendue simple

Ajouter le rôle serveur DHCP à votre machine, puis laissez vous guider pour créer une étendue. Dans les options de l'étendue vous pourrez fournir aux clients une passerelle et un serveur DNS (vous-même) ainsi qu'un nom de domaine fantaisiste.
Configurer les clients pour qu'ils utilisent le DHCP, et vérifier leur configuration (ipconfig /all, ipconfig /release, ipconfig /renew).

Affection des adresses IP en fonction des adresses MAC

Modifiez la configuration du serveur DHCP pour le client possédant les serveurs ait toujours la même adresse IP en fonction de son adresse MAC (réservation). Cette adresse IP sera bien évidement celle utilisée par la passerelle pour le port forwarding.

DNS

Utiliser sur l'intranet des adresses IP et non des noms d'hôte n'est pas une chose simple, il peut être intéressant de mettre en place sur l'intranet un serveur gérants un nom de domaine fantaisiste et redirigeant les autres requêtes DNS vers un des serveurs d'Internet.

Vous allez mettre en place un tel serveur sur la passerelle. Ce serveur contiendra une zone de recherche directe, une zone de recherche inverse et un « redirecteur » vers 192.168.114.254.

Le service DNS et le service DHCP ne sont pas naturellement compatible le premier résout les noms d'hôtes en adresse IP et le second attribut dynamiquement des adresses IP. Il y a donc un risque d'incohérence entre les noms d'hôtes et les adresses IP. Pour remédier à ce problème une solution est l'utilisation du Dynamique DHCP. Le serveur DHCP va dynamiquement modifier les fichiers de zone du serveur DNS.

Pour réaliser cette opération sur le serveur DNS vous autoriserez les mises à jour dynamiques et sur le serveur DHCP vous indiquerez dans le serveur DNS à mettre ajour. Attention le comportement est de demander au client d'informer le DNS, vous choisirez l'autre option celle qui consiste au serveur DHCP de mettre à jour les zones du serveur DNS.