TP SR04

Partie 1 : Le modèle TCP/IP

L'objectif de cette première partie est d'utiliser l'analyseur de paquets Wireshark pour mieux comprendre le modèle TCP/IP.

Partie 2 : Les réseaux locaux (LAN)

L'objectif de cette deuxième partie est d'utiliser des switchs Cisco pour mettre en place et configurer des réseaux locaux (LAN).

Partie 3 : Les réseaux étendus (WAN)

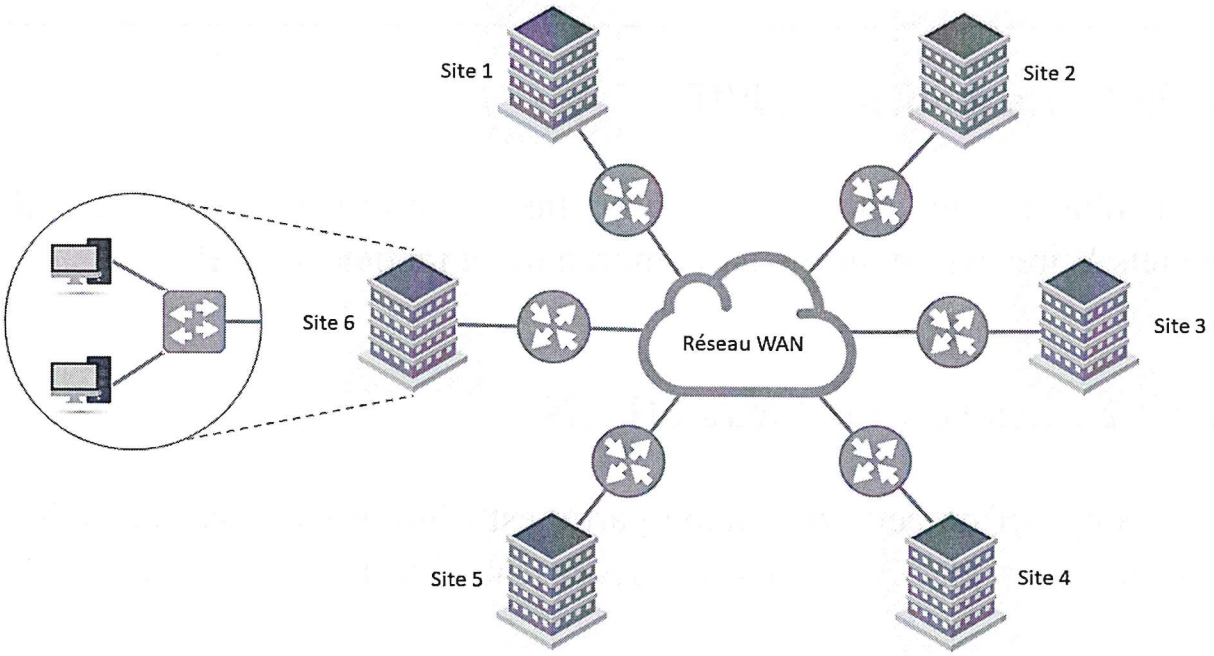
L'objectif de cette dernière partie est d'utiliser des routeurs Cisco pour connecter des réseaux locaux. Pour cela, nous allons voir comment configurer le DHCP, le routage et le NAT.

Outils et équipements utilisés:

- Analyseur de paquets Wireshark.
- Switchs et routeurs Cisco.

Préambule

L'objectif de ce TP est d'abord de comprendre le modèle TCP/IP en utilisant l'analyseur de paquets Wireshark. Nous allons ensuite utiliser des switchs et des routeurs Cisco pour mettre en place un réseau similaire à celui présenté ci-dessous.



Des groupes de 2 à 3 participants travaillent ensemble et doivent collaborer. Chaque groupe utilise un switch pour configurer un LAN qui correspond à un seul site du réseau. Il utilise ensuite un routeur pour connecter son LAN à ceux des autres groupes (les autres sites) et à mettre en place le routage entre eux.

Nous commençons par la mise en place d'un routage statique entre deux sites afin de mieux comprendre le routage IP. Nous configurons par la suite des protocoles de routage dynamique pour assurer le routage entre tous les sites. Nous abordons enfin l'une des solutions utilisées pour pallier au problème de pénurie d'adresses publiques IPv4, à savoir la translation d'adresse réseau (NAT).

Partie 1 : Le modèle TCP/IP

L'objectif de cette première partie est d'utiliser Wireshark pour mieux comprendre le modèle TCP/IP. Wireshark est un analyseur de paquets libre et gratuit. Téléchargez le logiciel et installez-le sur vos PC. Lancez Wireshark et suivez le trafic de l'interface connectée à Internet.

1.1. Utilisez le filtre « arp » sur Wireshark puis sélectionnez une trame ARP (Si la liste est vide, accédez à ligne de commande et tapez « arp –d »). Quelles sont les couches utilisées par le protocole? Que peut-on déduire ?

1.2. En observant les trames ARP, expliquez brièvement le fonctionnement du protocole.

1.3. Utilisez le filtre « icmp » sur Wireshark puis sélectionnez une trame ICMP (Si la liste est vide, accédez à ligne de commande et pingez une adresse IP quelconque ; p.ex. ping google.fr). Quelles sont les couches utilisées par le protocole? Que peut-on déduire ?

1.4. Utilisez le filtre « ssl » sur Wireshark puis sélectionnez une trame TLSv1.2 (Si la liste est vide, utilisez un navigateur pour accéder à un site web). Quelles sont les couches utilisées par le protocole? Que peut-on déduire ?

1.5. Utilisez le filtre « http » sur Wireshark puis sélectionnez une trame http (Si la liste est vide, utilisez un navigateur pour accéder à un site web quelconque). Quelles sont les couches utilisées par le protocole http ? Que peut-on déduire ?

1.6. Utilisez le filtre « http && tcp.dstport==80 » sur Wireshark. Sélectionnez une trame http et remplissez les informations suivantes :

Source		Destination	
Adresse MAC	A quoi cela correspond ?	Adresse MAC	A quoi cela correspond ?
Adresse IP	A quoi cela correspond ?	Adresse IP	A quoi cela correspond ?
Port TCP	A quoi cela correspond ?	Port TCP	A quoi cela correspond ?

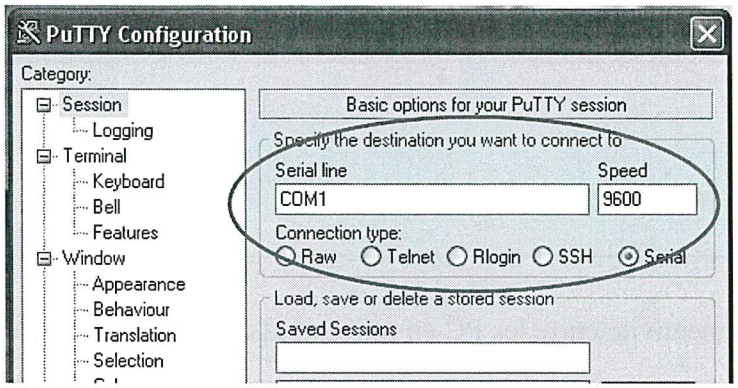
1.7. Lancez un navigateur et accédez au site web « google.fr ». Utilisez le filtre « http.request.uri contains "google.fr" » sur Wireshark. Sélectionnez une trame http, cliquez sur le bouton droit de la souris puis choisissez l'option « follow TCP Stream ». Expliquez brièvement le principe de fonctionnement de TCP et les messages échangés.

Partie 2 : Les réseaux locaux (LAN)

L'objectif de cette deuxième partie est d'utiliser des switchs Cisco pour mettre en place des réseaux locaux et de tester leur bon fonctionnement.

Etape 1 : Accès à l'interface de configuration d'un switch Cisco

2.1.1. Mettez le switch sous tension puis connectez-le à une machine de la salle à l'aide d'un câble console. Lancez ensuite PuTTY, cochez la case Serial puis cliquez sur « Open ».



2.1.2. Si la console se lance comme sur la figure ci-dessous, ignorez les étapes suivantes :

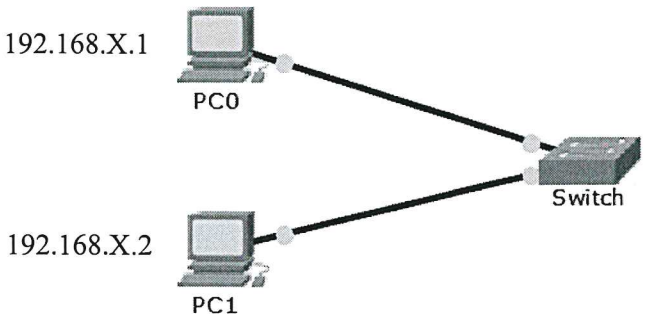
- Si rien ne s'affiche, vérifiez le nom de votre port COM. Pour cela, allez à « Panneau de configuration/Gestion des périphériques », puis cherchez le nom de votre port COM dans Ports (COM et LPT).
- Si des caractères bizarres appariassent, essayer de relancer PuTTY avec une vitesse de 115200 au lieu de 9600.

```
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!
Switch#
```

Etape 2 : Mise en place d'un LAN

2.2.1. Connectez les PC au switch à l'aide de câbles Ethernet de la manière suivante :



2.2.2. Attribuez des adresses IP aux PC. Chaque groupe **X** devra utiliser une adresse du réseau 192.168.**X**.0 et un masque 255.255.255.0 pour son LAN. Pour attribuer à un PC une adresse IP statique il faut :

- Sous Windows : aller à « Panneau de configuration/Réseau et Internet/Centre Réseau et partage/Modifier les paramètres de la carte/Ethernet/Protocole Internet Version 4 ». Cocher ensuite la case « Utiliser l'adresse IP suivante » et attribuer à votre PC une adresse IP et un masque.
- Sous Linux: utilisez la commande « ifconfig *nom_interface adresse_IP* netmask *masque* ».

2.2.3. Vérifiez votre configuration en utilisant la commande « ipconfig/all » sous Windows et « ifconfig » sous Linux. Pour chaque PC connecté, notez les informations suivantes:

Adresse MAC:
Adresse IP:
Masque réseau:

2.2.4. Testez la connectivité entre les PC en utilisant la commande « ping *adresse_IP* ».

Note: Désactivez le pare-feu si vous êtes sous Windows (Panneau de configuration/ Système de sécurité/Pare-feu Windows Defender). N'oubliez pas de déconnecter votre PC d'Internet avant de le faire et de réactiver le pare-feu à la fin de la séance.

2.2.5. Utilisez la commande « arp –a » sur les PC pour afficher le contenu de la table ARP. Notez les entrées de la table.

2.2.6. Utilisez la commande « # show mac address-table » sur le switch pour afficher la table de commutation. Notez les entrées de la table.

Partie 3 : Les réseaux WAN

L'objectif de cette dernière partie et d'utiliser des routeurs Cisco pour relier les différents LAN.

Etape1 : Accès à l'interface de configuration d'un routeur Cisco

3.1.1. Mettez le routeur sous tension puis connectez-le à une machine de la salle à l'aide d'un câble console. De la même manière qu'avec le switch, lancez PuTTY et renseignez les paramètres adéquats (revoir 2.1.1 et 2.1.2). Cliquer sur « Open » pour lancer la console. Passez l'utilitaire de configuration « configuration dialog ». Si la console s'affiche comme sur la figure ci-dessous, le routeur est prêt à être configuré.

```
         --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!
Router>
```

3.1.2. Pour accéder aux fonctions d'administration du router, il faut passer en mode privilégié à l'aide de la commande *enable*. Le chevron (>) de la ligne de commande se transforme en dièse (#).

3.1.3. Les commandes de configuration doivent être rentrées en mode configuration, sinon elles ne seront pas interprétées. La commande pour passer en mode configuration est *configure terminal*.

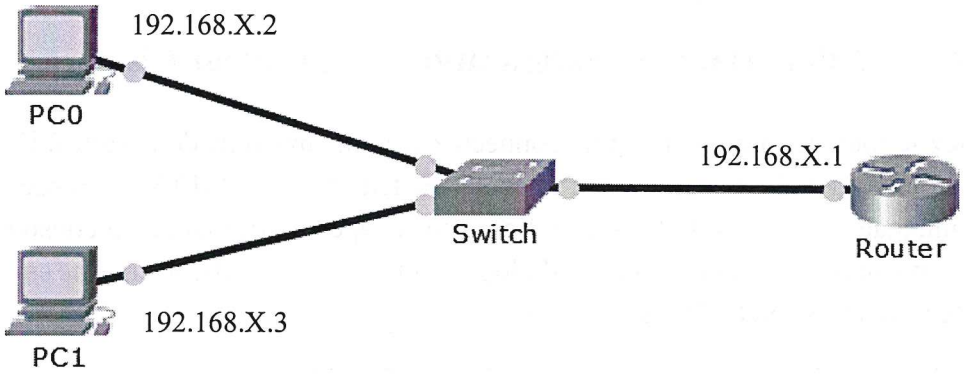
3.1.4. En utilisant la commande *hostname* changez le nom de votre router. Donnez le nom RouterX à votre routeur (par exemple le routeur du groupe 1 aura le nom Router1).

Astuces

- Utilisez la touche tab pour compléter les commandes (et ainsi diminuer les erreurs de frappe !).
- ? permet d'afficher une aide contextuelle.
- Les commandes peuvent être abrégées à condition qu'elles ne soient pas ambigües (ex : conf t au lieu de configure terminal).
- Pour sauvegarder une configuration utiliser la commande « write »
- Pour supprimer une configuration, la plupart du temps il suffit de taper « no » suivi de la commande à retirer.
- Pour afficher diverses informations, utilisez la commande « show ... » (pas en mode config). Par exemple, pour afficher la configuration courante, tapez « show running-config ».

Etape 2 : Configuration du DHCP

3.2.1. Connectez un port du switch à une interface WAN du routeur de la manière suivante :



3.2.2. Activer l'interface du routeur et attribuez-lui une adresse IP (192.168.X.1) et un masque (255.255.255.0). Les commandes à utiliser sont les suivantes (Les noms des interfaces sont écrits sur le dos de l'équipement):

```
RouterX(config)#interface <interface name>
RouterX(config-if)#ip address <ip> <mask>
RouterX(config-if)#no shutdown
```

3.2.3. Configurez le routeur pour qu'il assure le rôle de serveur DHCP.

```
RouterX(config)#ip dhcp pool pool2
RouterX(dhcp-config)#network 192.168.X.0 255.255.255.0
RouterX(dhcp-config)#default-router 192.168.X.1
```

3.2.4. Activer l'obtention automatique d'adresse IP par DHCP au niveau des PC:

- Sous Windows : allez à « Panneau de configuration/Réseau et Internet/Centre Réseau et partage/Modifier les paramètres de la carte/Ethernet/Protocole Internet Version 4 ». Cochez ensuite « Obtenir automatiquement une adresse IP ».
- Sous Linux : utilisez la commande « dhclient *nom_interface* ».

3.2.5. Si l'adresse IP d'un PC n'a pas changée, essayez de la résilier puis d'en demander une nouvelle au serveur DHCP. Les commandes à utiliser sont les suivantes :

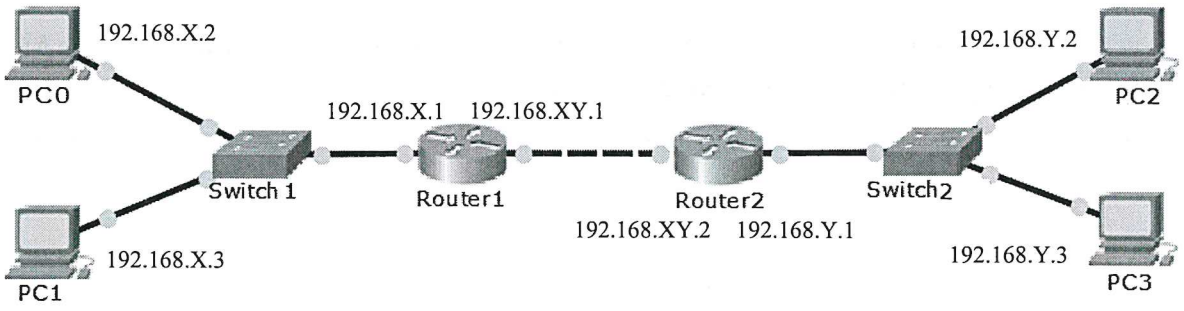
- Sous Windows: utilisez la commande « ipconfig/release » ensuite « ipconfig/renew ».
- Sous Linux : utilisez la commande « dhclient –r *nom_interface* » ensuite « dhclient *nom_interface* ».

3.2.6. En utilisant la commande « ping », testez la connectivité entre :

- Deux PC du même réseau.
- Un PC et la passerelle par défaut.

Etape 3 : Connecter les LAN

3.3.1. Nous allons maintenant configurer les interfaces WAN de deux routeurs (le votre X et celui du groupe voisin Y) pour qu'ils puissent communiquer entre eux. Pour cela, commencez par connecter les deux routeurs entre eux via les interfaces WAN de la manière suivante:



3.3.2. Pour l'adressage du réseau d'interconnexion des routeurs, on a besoin de deux adresses IP (une pour l'interface WAN de chaque routeur). Afin de ne pas gaspiller d'adresses IP, quel est le plus petit sous-réseau possible, qui ne contient que deux adresses IP ? Donnez le masque correspondant et l'adresse de broadcast:

Réseau	IP Routeur X	IP Routeur Y	Masque	Broadcast
192.168.XY.0	192.168.XY.1	192.168.XY.2		

3.3.3. En réutilisant les commandes de la question 3.2.2, activez les interfaces des routeurs et configurez leurs adresses IP.

3.3.4. En utilisant la commande « ping », testez la connectivité entre :

- Les deux routeurs.
- Un PC et le routeur du site distant (routeur de groupe voisin).
- Un PC et un autre PC du réseau local du site distant.

Quels sont les ping qui ne fonctionnent pas et pourquoi ?

Etape 4 : Mise en place du routage statique

Pour que les deux sites puissent communiquer, les routeurs doivent savoir où envoyer les paquets qu'ils reçoivent. Il faut donc configurer le routage. Cela peut se faire de manière statique en renseignant les routes manuellement. La commande à utiliser est la suivante :

```
RouterX(config)#ip route <destination> <mask> <next hop ou interface de sortie>
```

3.4.1. Configurez des routes statiques pour que les PC n'appartenant pas au même LAN puissent communiquer. Notez les commandes utilisées :

3.4.2. Utilisez la commande « #show ip route » pour afficher la table de routage. Expliquer brièvement son contenu.

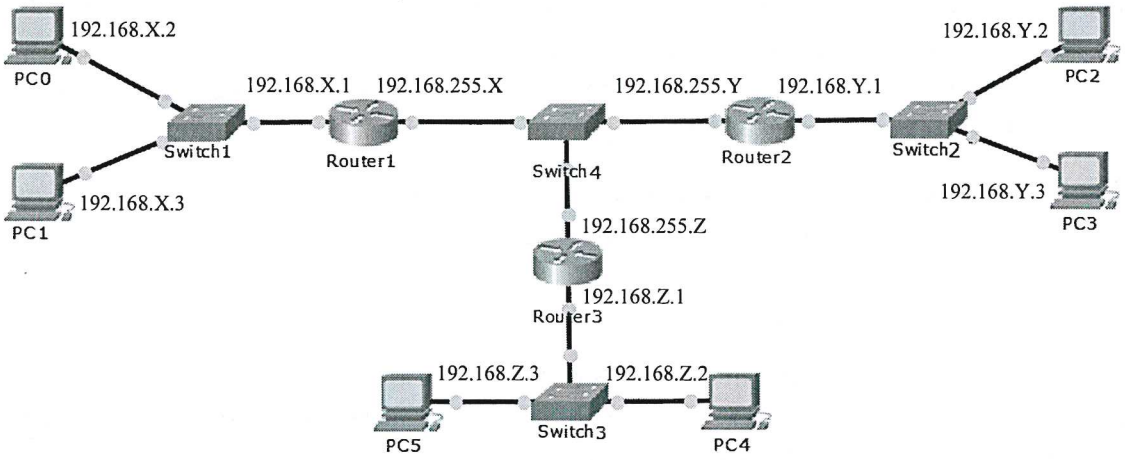
3.4.3. Utilisez la commande ping pour tester la connectivité entre deux PC n'appartenant pas au même LAN.

3.4.4. Quels sont les inconvénients du routage statique :

Pour pallier aux inconvénients du routage statique, nous allons utiliser des protocoles de routage dynamique. Nous allons tester successivement des protocoles à vecteur de distances puis des protocoles à état de liens.

Etape 5 : Mise en place du routage dynamique

Pour pouvoir connecter tous les sites, commencez par relier tous les routeurs via un switch de la manière suivante (modifiez les adresses reliant les routeurs et choisissez un nouveau masque en fonction du nombre de routeurs):



Le protocole RIP (à vecteur de distance)

Routing Information Protocol (RIP) est un protocole de routage IP à vecteur de distances basé sur l'algorithme de routage décentralisé Bellman-Ford. Il permet à chaque routeur de communiquer aux autres sa table de routage. Les routes sont mises à jour toutes les 30 secondes.

3.5.1. Supprimez les routes statiques ajoutées auparavant puis configurez le protocole de routage RIP sur chaque routeur. Utilisez les commandes :

```
RouterX(config)#no ip route ...
RouterX(config)#router rip
RouterX(config-router)#version 2
RouterX(config-router)#network ...
```

`network` sert à indiquer les réseaux qui sont directement connectés au routeur et qu'il doit annoncer à ses voisins.

3.5.2. Pingez un PC d'un autre site pour tester votre configuration et affichez la table de routage. Comment sait-on que les routes ont été apprises par le protocole RIP ? Quelle est la distance administrative de RIP ?

3.5.3. Est-il utile de diffuser les annonces vers les PC d'extrémités ? Comment ne pas diffuser des paquets RIP sur cette interface ?

3.5.4. Désactivez une interface d'extrémité d'un routeur et observez le temps de convergence en visualisant la table de routage sur l'autre routeur.

Le protocole EIGRP (à vecteur de distance)

Interior Gateway Routing Protocol (IGRP) est un protocole de routage à vecteur de distance créé par Cisco. IGRP a été créé en partie pour remédier aux limitations de RIP quand il est utilisé dans de grands réseaux (nombre maximal de sauts 15, une seule métrique de routage). IGRP permet des métriques multiples pour chaque route, en incluant la bande passante, la charge, le délai, MTU et la fiabilité. Pour comparer 2 routes, ces métriques sont combinées en utilisant une formule ajustable. Le nombre maximum de « hop » pour les paquets routés en IGRP est de 255. Le successeur de IGRP a été nommé EIGRP.

3.5.5. Supprimez les routes statiques (si elles existent) et configurez EIGRP sur chaque routeur. Utilisez les commandes suivantes (Les routeurs doivent utiliser le même numéro d'AS):

```
RouterX(config)#router eigrp <as number>
RouterX(config-router)#network ...
```

3.5.6. Pingez un PC d'un autre site pour tester votre configuration puis affichez la table de routage. Comment sait-on sans regarder la configuration que la route a été apprise grâce au protocole EIGRP ? Quelle est la distance administrative de EIGRP ?

Le protocole OSPF (à état de liens)

OSPF (Open Shortest Path First) est un protocole de routage à état de liens. Chaque routeur établit des relations d'adjacence avec ses voisins immédiats en envoyant des messages Hello à intervalle régulier. Chaque routeur communique ensuite la liste des réseaux auxquels il est directement connecté par des messages LSA (Link-State Advertisements) propagés de proche en proche à tous les routeurs du réseau. L'ensemble des LSA forme la base de données des liens Link-State Database (LSDB), qui est identique pour tous les routeurs participants. Chaque routeur utilise ensuite l'algorithme de Dijkstra, Shortest Path First (SPF), pour déterminer la route la plus courte vers chacun des réseaux connus dans la LSDB. En cas de changement de topologie, de nouveaux LSA sont propagés et SPF est exécuté à nouveau sur chaque routeur.

3.5.7. Configurez OSPF sur les routeurs sans désactiver le routage à vecteur de distance. Utilisez les commandes suivantes (une aire est un groupe de routeurs ayant la même LSDB) :

```
RouterX(config)#router ospf <id>
RouterX(config-router)#network <network address> <wildcard mask> area 0
```

3.5.8. Pingez un PC d'un autre site pour tester votre configuration puis affichez la table de routage. Comment sait-on que les routes ont été apprises par le protocole OSPF ? Quelle est la distance administrative de OSPF ?

3.5.9. Si le routeur apprend plusieurs routes vers le même réseau via des protocoles différents, laquelle il choisit? Expliquez pourquoi.

Etape 6 : Translation d'adresses NAT

Le mécanisme de translation d'adresses (en anglais Network Address Translation noté NAT) a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4 (le protocole IPv6 répondra à terme à ce problème). En effet, en adressage IPv4 le nombre d'adresses IP routables n'est pas suffisant pour permettre à toutes les machines le nécessitant d'être connectées à internet. Le principe du NAT consiste donc à utiliser une ou plusieurs adresse IP globales pour donner l'accès à l'ensemble des machines du réseau local à Internet.

3.6.1. Une partie des groupes (par exemple ceux ayant un nombre paire) doit configurer le NAT et l'autre non. Le réseau "NATé" ne doit plus être routé. Déconfigurez d'abord l'annonce de ce réseau dans le protocole de routage dynamique. Suivre ensuite les étapes suivantes pour « surcharger » l'adresse de l'interface WAN, (i.e. toutes les adresses du réseau local utiliseront cette adresse pour sortir):

1	Définir à l'aide d'une ACL les réseaux autorisés à sortir	RouterX(config)#access-list *number* permit *source wildcard*
2	Configurer la translation dynamique	RouterX(config)#ip nat inside source list *number* interface *interface* overload
3	Spécifier l'interface interne (celle qu'il faut translater)	RouterX(config-if)#ip nat inside
4	Spécifier l'interface externe (celle utilisée pour la translation)	RouterX(config-if)#ip nat outside

3.6.2. Depuis un PC du réseau interne NATé, lancez un ping vers un PC du site opposé. Est-ce que le ping passe ?

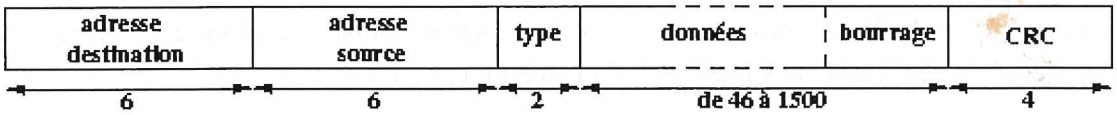
3.6.3 Affichez la table de translations à l'aide de la commande **`show ip nat translations`**.

3.6.4. Lancez un ping dans l'autre sens. Est-ce que le ping passe ? Pourquoi ?

3.6.5. Configurez le NAT sur tous les routeurs du réseau et lancez des ping.

Annexe

Entête Ethernet



En-tête IPv4 :

0	8	16	24	31

Version	I.H.L	Type de service	Longueur total	
Identification			Flags	Offset de fragmentation
Durée de vie		Protocole	Checksum de l'en-tête	
Adresse Source				
Adresse Destinataire				
Options				Padding
Données				

En-tête TCP :

0	8	16	24	31

Port Source			Port Destination
Numéro de séquence			
Numéro d'acquittement			
Offset	Réservé	Flags	Fenêtre
Checksum			Urgent Pointer
Options			Padding
Données			