Université Mohammed Premier Oujda
École Nationale des Sciences Appliquées
Département : Électronique, Télécommunications et Informatique
Filière : GI/GSEIR / Niveau : GI5/GSEIR5
Module : Interconnexion des réseaux

TP4 Security :

Configuration de la fonction NAT statique, dynamique, la surcharge de pool NAT et de la fonction PAT

Enseignant : Mohammed SABER

Année Universitaire : 2017/2018

Objectifs pédagogiques de TP :

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

Partie 1 : Configuration de la topologie et initialisation des périphériques

- Configurez l'équipement pour qu'il corresponde à la topologie du réseau.
- Initialisez et redémarrez les routeurs et les commutateurs.

Partie 2 : Configuration des périphériques et vérification de la connectivité

- Attribuez une adresse IP statique aux PC.
- Configurez les paramètres de base sur les routeurs.
- Configurez les paramètres de base sur les commutateurs.
- Configurez le routage (RIP, EIGRP, OSPF) sur R1, ISP et R3.
- Vérifiez la connectivité entre les périphériques.

Partie 3 : Configuration et vérification de la fonction NAT statique

- Configurez, appliquez et vérifiez la fonction NAT statique.

Partie 4 : Configuration et vérification de la fonction NAT dynamique

- Configurez, appliquez et vérifiez la fonction NAT dynamique.

Partie 5 : Configuration et vérification de surcharge de pool NAT

- Configurez, appliquez et vérifiez la surcharge de pool NAT.

Partie 6 : Configuration et vérification de la fonction PAT

- Configurez, appliquez et vérifiez la fonction PAT.

Scénarios

La traduction d'adresses réseau (NAT) est le processus par lequel un périphérique réseau, tel qu'un routeur Cisco, attribue une adresse publique aux périphériques hôtes à l'intérieur d'un réseau privé. La raison principale de l'utilisation de la fonction NAT est la diminution du nombre d'adresses IP publiques utilisées par une entreprise, car le nombre d'adresses publiques IPv4 disponibles est limité.

Dans **les scénarios 1 et 2** de ces travaux pratiques, un fournisseur d'accès Internet (FAI) a attribué l'espace d'adressage IP public **196.200.156.224/27** à une entreprise. Cela permet à l'entreprise de disposer de 30 adresses IP publiques. Les adresses **196.200.156.225** à **196.200.156.254** concernent l'attribution statique (**Scénario 1**) tandis que les adresses **196.200.156.225** à **196.200.156.25** concernent l'attribution dynamique (**Scénario 2**). Une route statique est utilisée entre le FAI et le routeur **R1(passerelle)**, et une route par défaut est utilisée entre la passerelle et le routeur **R2(ISP)**. La connexion à Internet (FAI) est simulée par une adresse de bouclage au niveau du routeur **R2(ISP)**.

Dans **le scénario 3** de ces travaux pratiques, votre fournisseur d'accès Internet (FAI) alloue la plage d'adresses IP publiques **196.200.156.225/27** à votre entreprise. Cela permet à votre entreprise

de posséder des adresses IP publiques. La surcharge de pool NAT dynamique utilise un pool d'adresses IP dans une relation de type «**plusieurs vers plusieurs**». Le routeur utilise la première adresse IP du pool et attribue des connexions à l'aide de cette adresse IP et d'un numéro de port unique. Une fois que le nombre maximal de traductions pour une même adresse IP a été atteint sur le routeur (en fonction de la plate-forme et du matériel), il utilise l'adresse IP suivante du pool.

Dans **le scénario 4** de ces travaux pratiques, le fournisseur d'accès Internet (FAI) a attribué une adresse IP unique, à savoir **80.80.80.81**, à votre entreprise en vue d'une utilisation sur la connexion Internet à partir du routeur de passerelle de l'entreprise vers le FAI. Vous utiliserez la traduction d'adresses de port (PAT) pour convertir plusieurs adresses internes en une adresse publique utilisable. Vous testerez, afficherez et vérifierez les traductions, et interpréterez les statistiques NAT/PAT pour contrôler le processus.

Remarque : Assurez-vous que les routeurs et commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre enseignant.

Ressources requises

Ressources nécessaires :

1. Trois routeurs, chacun équipé des interfaces de type Ethernet et série ;
2. Deux ordinateurs Windows 7, dont un avec un programme d'émulation de terminal (PuTTY) et le virtualbox pour manipuler les machines virtuelles ;
3. Quatre machines virtuelles Windows 7 pour les tests ;
4. Quatre câbles Ethernet directs (PC-A à SW1, SW1 à R1, SW2 à PC-D et R1 à SW2) ;
5. Un câble série null modem (R1 à R2) ;
6. Deux câbles console avec connecteur RJ-45 vers DB-9 (PC-A à R1 et PC-D à R2) ;
7. Accès à l'invite de commandes des hôtes PC-A, PC-B, PC-C, PC-D, PC-E et PC-F ;
8. Accès à la configuration TCP/IP du réseau des hôtes PC-A, PC-B, PC-C, PC-D, PC-E et PC-F.
9. Deux commutateurs (Switch) ;

Consignes pour le TP

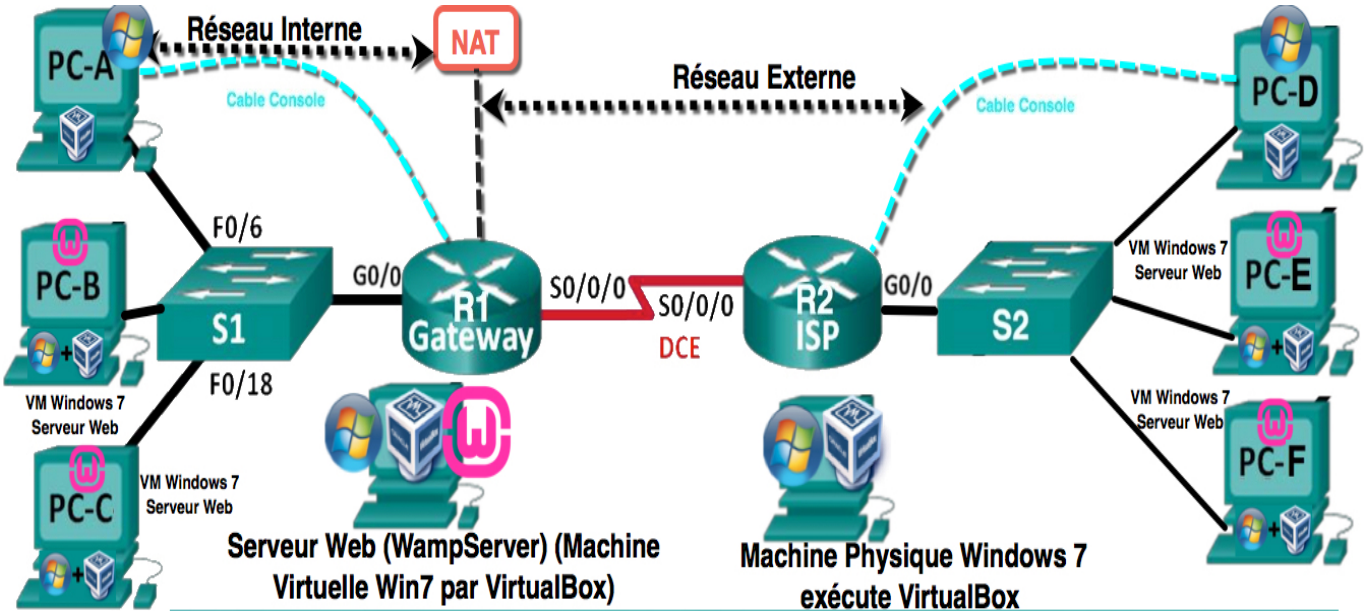
1. Suivez les instructions pour chaque étape.
2. Ne déplacez pas le matériel.
3. **N'utilisez pas les Clés USB sur les machines**.
4. A la fin de TP, SVP réorganiser votre table :
   - Éteindre toutes les machines.
   - Réorganiser les chaises à ces places avant de sortir.
   - MERCI d'avance.
5. Un rapport de TP individuel est rendu sur la plateforme Moodle à la fin de TP (en format PDF ou DOC).
6. **Chaque étudiant ne respect pas les consignes de TP sera sanctionné.**

PARTIE 1 : Atelier pour les Scénarios 1 et 2

Étape 1 : Préparation du réseau

Atelier de TP

L'architecture de l'atelier pour les scénarios S1 et S2 est la suivante :



Câblez le réseau conformément à la topologie

Les informations pour chaque équipement pour ces travaux pratiques sont présentées sur le tableau suivant :

Périphérique	Interface	Adresse IP	Masque réseau	Passerelle
R1	G0/0 (Type Ethernet)	192.168.10.1	255.255.255.0	N/D
	S0/0/0 (Type Serial)	80.80.80.81	255.255.255.252	N/D
R2 (ISP)	S0/0/0 (Type Serial)	80.80.80.82	255.255.255.252	N/D
	G0/0 (Type Ethernet)	196.200.157.1	255.255.255.0	N/D
PC-A	N/D	192.168.10.10	255.255.255.0	192.168.10.1
PC-B (VM-WebServer)	N/D	192.168.10.20	255.255.255.0	192.168.10.1
PC-C (VM-WebServer)	N/D	192.168.10.30	255.255.255.0	192.168.10.1
PC-D	N/D	196.200.157.10	255.255.255.0	196.200.157.1
PC-E (VM-WebServer)	N/D	196.200.157.20	255.255.255.0	196.200.157.1
PC-F (VM-WebServer)	N/D	196.200.157.30	255.255.255.0	196.200.157.1

Étape 2 : Installation, suppression et rechargement des routeurs

Tâche 1 : Connexion des périphériques

Connectez les périphériques de réseau similaire à celui de la topologie de l'atelier.

Tâche 2 : Suppression des configurations existantes sur les routeurs

Il est nécessaire de commencer avec un routeur non configuré. L'utilisation d'un routeur comportant déjà une configuration peut produire des résultats imprévisibles. Les étapes suivantes permettent de préparer le routeur avant d'effectuer les travaux pratiques pour que les options de configuration précédentes ne créent pas d'interférence.

1. Passez en mode d'exécution privilégié.
2. **Effacement de la configuration :** Pour effacer la configuration, lancez la commande `erase startup-config`. Lorsque vous êtes invité à confirmer (via **[confirm]**) que vous voulez vraiment effacer la configuration actuellement enregistrée en mémoire NVRAM, appuyez sur **Entrée**.
3. **Rechargement de la configuration :** Au retour de l'invite, lancez la commande ***reload***. Si vous êtes invité à enregistrer les modifications, répondez par **no** [**Que se passerait-il si vous répondiez yes à la question**].
4. Lorsque vous êtes invité à confirmer (via **[confirm]**) que vous voulez vraiment recharger le routeur, appuyez sur **Entrée**. Dès que le routeur a terminé l'amorçage, choisissez de ne pas utiliser la fonction **AutoInstall**.
5. Répétez les questions 1 à 4 sur le routeur R2 ?

Étape 2 : Configuration des routeurs Cisco

Tâche 1 : Configuration de base des routeurs

1. Configurez le nom d'hôte du routeur 1 en tant que **R1**.
2. Configurez le nom d'hôte du routeur 2 en tant que **R2**.
3. Attribuez "**ensao**" au mot de passe de mode d'exécution privilégié sur les routeurs.
4. Attribuez "**ensao**" au mot de passe de **console** sur les routeurs.
5. Attribuez "**ensao**" au mot de passe **vty** sur les routeurs.
6. Affichez la configuration à l'aide de la commande `show running-config`.
7. Vérifier les mots de passe sont en clair sur les routeurs.
8. Sauvegardez la configuration actuelle "**running-config**" dans la configuration de démarrage "**startup-config**" sur les deux routeurs.

Tâche 2 : Désactivation des messages débogage non sollicités

1. Configurez les routeurs de sorte que les messages de console n'interfèrent pas avec l'entrée des commandes. Ceci est utile lorsque vous quittez le mode de configuration, car vous retournez à l'invite de commandes et l'option évite alors que des messages s'affichent dans la ligne de commande `logging synchronous` en **mode line** soit **console** soit **terminal virtuel VTY**.

2. Configurez le routeur de sorte que pas de délai d'attente, dans la ligne de commande `exec-timeout 0 0` en **mode line** soit **console** soit **terminal virtuel VTY**.
3. Désactivez la recherche DNS avec la commande `no ip domain-lookup`.
4. Sauvegardez la configuration actuelle `running-config` dans la configuration de démarrage `startup-config` sur les deux routeurs.

Tâche 3 : Configuration des interfaces de R1

1. En mode de configuration globale, configurez l'adresse IP pour l'interface série **S0/0/0** sur **R1** vers **R2**. Reportez-vous à la table Synthèse des interfaces de routeur.
2. Affectez la description suivante "**WAN link to R2**" pour cette interface.
3. Vérifiez, est ce que l'interface série du R1 c'est elle l'interface DCE ? **Remarque :** Le type de câble (**DCE** ou **DTE**) est gravé à chaque extrémité du **câble série Null**. En cas de doute, entrez la commande ***clock rate*** sur les interfaces série des deux routeurs. La commande est ignorée sur le routeur auquel le **DTE** est connecté.
4. Si l'interface série de R1 est DCE, configurez la fréquence d'horloge (**128000**).
5. Activez l'interface série.
6. En mode de configuration globale, configurez l'adresse IP pour l'interface de type Ethernet **G0/0** sur **R1**. Reportez-vous à la table Synthèse des interfaces de routeur.
7. Affectez la description suivante "**LAN link to LAN1**" pour cette interface.
8. Activez l'interface de type Ethernet.
9. Affichez la table de routage.
10. Sauvegardez la configuration actuelle "**running-config**" dans la configuration de démarrage "**startup-config**".

Tâche 4 : Configuration des interfaces de R2

1. En mode de configuration globale, configurez l'adresse IP pour l'interface série **S0/0/0** sur **R2** vers **R1**. Reportez-vous à la table Synthèse des interfaces de routeur.
2. Affectez la description suivante "**WAN link to R1**" pour cette interface.
3. Vérifiez, est ce que l'interface série du R2 c'est elle l'interface DCE ? **Remarque :** Le type de câble (**DCE** ou **DTE**) est gravé à chaque extrémité du **câble série Null**. En cas de doute, entrez la commande ***clock rate*** sur les interfaces série des deux routeurs. La commande est ignorée sur le routeur auquel le **DTE** est connecté.
4. Si l'interface série de R2 est DCE, configurez la fréquence d'horloge (**128000**).
5. Activez l'interface série.
6. En mode de configuration globale, configurez l'adresse IP pour l'interface de type Ethernet **G0/0** sur **R1**. Reportez-vous à la table Synthèse des interfaces de routeur.
7. Affectez la description suivante "**LAN link to LAN2**" pour cette interface.
8. Activez l'interface de type Ethernet.
9. Affichez la table de routage.
10. Sauvegardez la configuration actuelle "**running-config**" dans la configuration de démarrage "**startup-config**".

Tâche 5 : Configuration de routage statique sur les routeurs

Rappel 1 : Pour activer le routage statique, en mode de configuration globale, utilisez la commande `ip route adresse-réseau masque-réseau adresse-passerelle`.

Rappel 2 : Pour ajouter une route par défaut, en mode de configuration globale, utilisez la commande `ip route 0.0.0.0 0.0.0.0 adresse-passerelle`.

1. Créez une route statique depuis le routeur **R2(ISP)** jusqu'au routeur de **R1 (passerelle)** en utilisant la plage d'adresses réseau publiques **196.200.156.224/27** attribuée.
2. Créez une route par défaut sur le routeur de **R1 (passerelle)** vers le routeur **R2(ISP)**.

Tâche 6 : Enregistrez la configuration en cours en tant que configuration initiale

Sauvegardez la configuration actuelle `running-config` dans la configuration de démarrage `startup-con` sur les deux routeurs.

Tâche 7 : Configuration des interfaces Ethernet des machines

Configurez les interfaces Ethernet de PC-A, PC-B, PC-C, PC-D, PC-E et PC-F à l'aide des adresses IP et des passerelles par défaut indiquées dans le tableau sous le diagramme de la topologie.

Tâche 8 : Vérifiez la connectivité entre les périphériques

Remarque : il est très important de vérifier si la connectivité fonctionne avant de configurer et d'appliquer des translations NAT ! Veuillez à vous assurer que votre réseau fonctionne correctement selon nos besoins.

1. Affichez les tables de routage sur les deux routeurs afin de vérifier que les routes statiques figurent dans cette table et qu'elles sont configurées correctement sur les deux routeurs. Que remarquez-vous ?
2. A partir de **PC-A**, envoyez une requête `ping` vers **PC-B**, **PC-C** et l'interface (**G0/0** sur **R1**. Les requêtes `ping` ont-elles abouti ?
3. A partir de **PC-B**, envoyez une requête `ping` vers **PC-A**, **PC-C** et l'interface (**G0/0** sur **R1**. Les requêtes `ping` ont-elles abouti ?
4. A partir de **PC-C**, envoyez une requête `ping` vers **PC-B**, **PC-A** et l'interface (**G0/0** sur **R1**. Les requêtes `ping` ont-elles abouti ?
5. A partir les machines de **réseau interne**, envoyez une requête `ping` vers les interfaces (**G0/0** et **S0/0/0**) sur **R2** et les machines du **réseau externe**. Les requêtes `ping` ont-elles abouti ? Justifier vos réponses ?
6. A partir de **R1**, envoyez une requête `ping` vers les interfaces (**S0/0/0** et **G0/0**) sur **R2**. Les requêtes `ping` ont-elles abouti ?
7. A partir de **PC-D**, envoyez une requête `ping` vers **PC-E**, **PC-F**, et l'interface (**G0/0** sur **R2**. Les requêtes `ping` ont-elles abouti ?
8. A partir de **PC-E**, envoyez une requête `ping` vers **PC-D**, **PC-F**, et l'interface (**G0/0** sur **R2**. Les requêtes `ping` ont-elles abouti ?
9. A partir de **PC-F**, envoyez une requête `ping` vers **PC-E**, **PC-D**, et l'interface (**G0/0** sur **R2**. Les requêtes `ping` ont-elles abouti ?

10. A partir les machines de **réseau externe**, envoyez une requête `ping` vers les interfaces (**G0/0** et **S0/0/0**) sur **R1** et les machines du **réseau interne**. Les requêtes `ping` ont-elles abouti ? Justifier vos réponses ?
11. A partir de **R2**, envoyez une requête `ping` vers les interfaces (**S0/0/0** et **G0/0**) sur **R1**. Les requêtes `ping` ont-elles abouti ?
12. Démarrer les serveurs web dans les réseaux interne et externe. (Démarrer à partir l'application WampServer).
13. Ouvrez un navigateur Web sur la machine **PC-A** et accédez à `http://adresse-IP-PC-B` et à `http://adresse-IP-PC-C`. Les requêtes `WEB` ont-elles abouti ?
14. Ouvrez un navigateur Web sur la machine **PC-A** et accédez à `http://adresse-IP-PC-E` et à `http://adresse-IP-PC-F` du réseau externe. Les requêtes `WEB` ont-elles abouti ?
15. Ouvrez un navigateur Web sur la machine **PC-D** et accédez à `http://adresse-IP-PC-E` et à `http://adresse-IP-PC-F`. Les requêtes `WEB` ont-elles abouti ?
16. Ouvrez un navigateur Web sur la machine **PC-D** et accédez à `http://adresse-IP-PC-B` et à `http://adresse-IP-PC-C` du réseau externe. Les requêtes `WEB` ont-elles abouti ?
17. A partir n'importe quelle machine (**PC-A**, **PC-B** et **PC-C**), envoyez une requête `telnet` vers les interfaces de routeur **R2**. La requête `telnet` a-t-elle abouti ?

Scénario 1 : Configuration et vérification de la fonction NAT statique

La fonction NAT statique utilise un mappage de type «**un à un**» des adresses locales et globales, et ces mappages restent constants. La fonction NAT statique est particulièrement utile pour les serveurs Web ou les périphériques qui doivent posséder des adresses statiques accessibles depuis Internet.

Étape 3 : Configuration et vérification de la fonction NAT statique

La configuration d'un mappage statique permet d'indiquer au routeur d'établir une traduction entre l'adresse privée du serveur interne **192.168.10.20** et l'adresse publique **196.200.156.225**. Cela permet à un utilisateur d'accéder à **PC-B** depuis Internet. **PC-B** est un serveur web avec une adresse constante qui est accessible depuis Internet.

Tâche 1 : Configurez un mappage statique sur R1

Rappel : Pour activer un mappage (NAT) statique, en mode de configuration globale, utilisez la commande `ip nat inside source static adresse-ip-local adresse-ip-global`.

1. Sur le routeur **R1**, entrez en mode de configuration globale.
2. Configurez un mappage entre l'adresse `ip-local` (**192.168.10.20**) et l'adresse `ip-global` (**196.200.156.225**).

Tâche 2 : Indiquez les interfaces de mappage statique sur R1

Rappel : Pour indiquer les interfaces de mappage (NAT) statique, en mode de configuration d'interfaces, utilisez la commande `ip nat inside` pour signaler l'interface à l'intérieure et `ip nat outside` pour spécifier l'interface externe.

1. Sur le routeur **R1**, entrez en mode de configuration d'interface.
2. Indiquez que **G0/0** du **R1** comme interface **interne**.
3. Sur le routeur **R1**, revenez en mode de configuration d'interface.
4. Indiquez que **S0/0/0** du **R1** comme interface **externe**.

Tâche 3 : Vérification de la configuration de fonction NAT statique sur R1

Rappel : Pour vérifier de la configuration de mappage (NAT) statique, en mode de privilégié, utilisez la commande `show ip nat translations`.

1. Sur le routeur **R1**.
2. Affichez la table NAT statique.
3. A partir les résultats affichés sur la table NAT statique, répondez aux questions suivantes :
   (a) Quelle est la traduction de l'adresse d'hôte local interne ?
   (b) Qui est chargé d'attribuer l'adresse globale interne ?
   (c) Qui est chargé d'attribuer l'adresse locale interne ?

Tâche 4 : Test de la configuration de fonction NAT statique Interne vers Externe

1. A partir de **PC-B**, envoyez une requête `ping` vers **PC-D**, **PC-E**, **PC-F** et l'interface (**G0/0** sur **R2**. Les requêtes `ping` ont-elles abouti ? Si la requête `ping` échoue, dépannez et corrigez les problèmes. Sur le routeur **R1**.
2. On peut observer le résultat de la translation du côté de **R2(ISP)** aussi à l'aide de la commande « `debug ip packet` » qui va afficher le détail de chaque paquet IP traité par le routeur (**Attention** : dans un environnement réel cette commande peut gravement saturer le routeur). Que remarquez-vous ?
3. Lancez la commande `no debug ip packet` sur le routeur **R2(ISP)**.
4. Affichez la table NAT.
5. Quel numéro de port a été utilisé dans cet échange **ICMP** ?
6. A partir de **PC-B**, envoyez une requête **Telnet** vers l'interface **G0/0** du routeur R2(ISP).
7. Affichez la table NAT.
8. Quel est le protocole utilisé dans cette traduction ?
9. Quels sont les numéros de port utilisés ? Justifier vos réponses ?
   (a) Global/local interne ?
   (b) Global/local externe ?
10. Vérifiez les statistiques NAT à l'aide de la commande `show ip nat statistics` sur le routeur de passerelle.
11. Ouvrez un navigateur Web sur la machine **PC-B** et accédez à `http://adresse-IP-PC-E` et à `http://adresse-IP-PC-F` du réseau externe. Les requêtes `WEB` ont-elles abouti ?

12. A partir les autres machines de réseau interne (**PC-A** et **PC-C**), envoyez une requête `ping` vers **PC-D**, **PC-E**, **PC-F** et l'interface (**G0/0** sur **R2**. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
13. A partir les autres machines de réseau interne (**PC-A** et **PC-C**), envoyez une requête **Telnet** vers l'interface **G0/0** du routeur R2(ISP). Les requêtes `ping` ont-elles abouti ? Pourquoi ?
14. Ouvrez un navigateur Web sur les autres machines de réseau interne (**PC-A** et **PC-C**) et accédez à `http://adresse-IP-PC-E` et à `http://adresse-IP-PC-F` du réseau externe. Les requêtes `WEB` ont-elles abouti ? Pourquoi ?

Tâche 5 : Test de la configuration de fonction NAT statique Externe vers Interne

1. A partir les machines de réseau externe (**PC-D**, **PC-E** et **PC-F**), envoyez une requête `ping` vers **196.200.156.225**. Les requêtes `ping` ont-elles abouti ? Si la requête `ping` échoue, dépannez et corrigez les problèmes. Sur le routeur **R1**. Que remarquez-vous ?
2. Ouvrez un navigateur Web sur les machines de réseau externe (**PC-D**, **PC-E** et **PC-F**) et accédez à `http://196.200.156.225`. Les requêtes `WEB` ont-elles abouti ? Que remarquez-vous ?
3. A partir les machines de réseau externe (**PC-D**, **PC-E** et **PC-F**), envoyez une requête `ping` vers les autres machines de réseau interne (**PC-A** et **PC-C**). Les requêtes `ping` ont-elles abouti ? Pourquoi ?

Tâche 6 : Effacez les traductions NAT et les statistiques

Rappel : Pour effacer les traductions NAT, en mode de privilégié, utilisez la commande `clear ip nat translation *`. Ainsi que les statistiques, utilisez la commande `clear ip nat statistics`.

1. Sur le routeur **R1**, entrez en mode de configuration globale.
2. Lancer la commande : `clear ip nat translation *`.

Scénario 2 : Configuration et vérification de la fonction NAT dynamique

La NAT dynamique utilise un pool d'adresses publiques et les attribue selon la méthode du premier arrivé, premier servi. Lorsqu'un périphérique interne demande l'accès à un réseau externe, la NAT dynamique attribue une adresse IPv4 publique disponible du pool. La fonction NAT dynamique se traduit par un mappage d'adresses de type «plusieurs vers plusieurs» entre les adresses locales et globales.

Étape 4 : Configuration et vérification de la fonction NAT dynamique pour un pool de deux adresses

La NAT dynamique utilise un pool d'adresses publiques et les attribue selon la méthode du premier arrivé, premier servi. Dans cette étape, nous utiliserons un pool d'adresses de deux adresses publiques (**196.200.156.226** et **196.200.156.227**).

Tâche 1 : Définition d'une liste de contrôle d'accès correspondant à la plage d'adresses IP privées du LAN sur le routeur R1

1. Sur le routeur **R1**, entrez en mode de configuration globale.
2. Créez une liste de contrôle d'accès standard **1**, pour permettre la traduction du réseau **192.168.10.0/** sauf la machine **192.168.10.20**.

Tâche 2 : Définition du pool d'adresses IP publiques utilisables

Rappel : Pour créer un pool d'adresses pour le (NAT) dynamique, en mode de configuration globale, utilisez la commande `ip nat pool VOTRE-NOM-POOL adresse-ip-début adresse-ip-fin`.

1. Sur le routeur **R1**, entrez en mode de configuration globale.
2. Créez un pool d'adresses nommée **POOL-NAT-IN** allant de **196.200.156.226** à **196.200.156.227**

Tâche 3 : Définition la NAT à partir de la liste source interne vers le groupe externe

Remarque : rappelez-vous que les noms de pool NAT sont sensibles à la casse et que le nom de pool entré ici doit correspondre à celui utilisé à l'étape précédente.

Rappel : Pour établir une traduction dynamique de la source, en spécifiant la liste d'accès et le pool définis lors des étapes précédentes. En mode de configuration globale, utilisez la commande `ip nat inside source list access-list-number pool VOTRE-NOM-POOL`.

1. Sur le routeur **R1**, entrez en mode de configuration globale.
2. Établissez une traduction dynamique de la source liste d'accès **1** et le pool `POOL-NAT-IN`.

Tâche 4 : Indiquez les interfaces de mappage dynamique sur R1

Rappel : Pour indiquer les interfaces de mappage (NAT) statique, en mode de configuration d'interfaces, utilisez la commande `ip nat inside` pour signaler l'interface à l'intérieure et `ip nat outside` pour spécifier l'interface externe.

1. Sur le routeur **R1**, entrez en mode de configuration d'interface.
2. Indiquez que **G0/0** du **R1** comme interface **interne**.
3. Sur le routeur **R1**, revenez en mode de configuration d'interface.
4. Indiquez que **S0/0/0** du **R1** comme interface **externe**.

Tâche 5 : Test de la configuration de fonction NAT dynamique

1. A partir de la machine **PC-A**, envoyez une requête `ping` à la machine **PC-D** (Lancez `ping -n 1000`). Les requêtes `ping` ont-elles abouti ?Si la requête `ping` échoue, dépannez et corrigez les problèmes. Sur le routeur **R1**. (Vous n'arrêtez pas le `ping`).
2. Affichez la table NAT.
3. Quelle est la traduction de l'adresse d'hôte local interne de **PC-A** ?
4. Quel numéro de port a été utilisé dans cet échange **ICMP** ?
5. A partir de la machine **PC-C**, envoyez une requête `ping` à la machine **PC-F** (Lancez `ping -n 1000`). Les requêtes `ping` ont-elles abouti ? (Vous n'arrêtez pas le `ping` même s'il y a des erreurs).

6. Affichez la table NAT.
7. A partir de la machine **PC-B**, envoyez une requête `ping` à la machine **PC-E** (Lancez `ping -n 1000`). Les requêtes `ping` ont-elles abouti ?
8. Affichez la table NAT.
9. Quelle est la traduction de l'adresse d'hôte local interne de **PC-B** ?
10. Quel numéro de port a été utilisé dans cet échange **ICMP** ?
11. Arrêter le `ping` sur la machine **PC-A**. Que remarquez-vous sur la machine **PC-C** ?
12. Quelle est la traduction de l'adresse d'hôte local interne de **PC-C** ?
13. Quel numéro de port a été utilisé dans cet échange **ICMP** ?
14. A partir de **PC-C**, ouvrez un navigateur et entrez l'adresse IP du serveur Web sur la machine **PC-E**. Les requêtes `WEB` ont-elles abouti ?
15. Affichez la table NAT.
16. Quel protocole a été utilisé dans cette traduction ?
17. Quels sont les numéros de port utilisés ? (Interne / Externe).
18. Quel numéro de port réservé et quel service ont été utilisés ?
19. Vérifiez les statistiques NAT sur le routeur **R1**.
20. Ouvrez un navigateur Web sur les machines de réseau externe (**PC-D**, **PC-E** et **PC-F**) et accédez à `http://196.200.156.226`. Les requêtes `WEB` ont-elles abouti ? Que remarquez-vous ?
21. Arrêter tous les `ping`.

Tâche 6 : Effacez les traductions NAT et les statistiques

Rappel : Pour effacer les traductions NAT, en mode de privilégié, utilisez la commande `clear ip nat translation *`. Ainsi que les statistiques, utilisez la commande `clear ip nat statistics`.

1. Sur le routeur **R1**, entrez en mode de configuration globale.
2. Lancer les commandes :
   (a) `clear ip nat translations *`.
   (b) `no ip nat inside source list 1 pool POOL-NAT-IN`.
   (c) `no ip nat pool POOL-NAT-IN 196.200.156.226 196.200.156.227`.

Étape 5 : Configuration et vérification de la fonction NAT dynamique pour un pool de plusieurs adresses

La NAT dynamique utilise un pool d'adresses publiques et les attribue selon la méthode du premier arrivé, premier servi. Dans cette étape, nous utiliserons un pool d'adresses de deux adresses publiques (**196.200.156.225** et **196.200.156.254**).

Tâche 1 : Définition du pool d'adresses IP publiques utilisables

Rappel : Pour créer un pool d'adresses pour le (NAT) dynamique, en mode de configuration globale, utilisez la commande `ip nat pool VOTRE-NOM-POOL adresse-ip-début adresse-ip-fin`.

1. Sur le routeur **R1**, entrez en mode de configuration globale.
2. Créez un pool d'adresses nommée **POOL-NAT-LAN** allant de **196.200.156.225** à **196.200.156.2**

Tâche 2 : Définition la NAT à partir de la liste source interne vers le groupe externe

Remarque : rappelez-vous que les noms de pool NAT sont sensibles à la casse et que le nom de pool entré ici doit correspondre à celui utilisé à l'étape précédente.

Rappel : Pour établir une traduction dynamique de la source, en spécifiant la liste d'accès et le pool définis lors des étapes précédentes. En mode de configuration globale, utilisez la commande `ip nat inside source list access-list-number pool VOTRE-NOM-POOL`.

1. Sur le routeur **R1**, entrez en mode de configuration globale.
2. Établissez une traduction dynamique de la source liste d'accès **1** et le pool `POOL-NAT-LAN`.

Tâche 3 : Indiquez les interfaces de mappage dynamique sur R1

Rappel : Pour indiquer les interfaces de mappage (NAT) statique, en mode de configuration d'interfaces, utilisez la commande `ip nat inside` pour signaler l'interface à l'intérieure et `ip nat outside` pour spécifier l'interface externe.

1. Sur le routeur **R1**, entrez en mode de configuration d'interface.
2. Indiquez que **G0/0** du **R1** comme interface **interne**.
3. Sur le routeur **R1**, revenez en mode de configuration d'interface.
4. Indiquez que **S0/0/0** du **R1** comme interface **externe**.

Tâche 4 : Test de la configuration de fonction NAT dynamique

1. A partir de la machine **PC-A**, envoyez une requête `ping` à la machine **PC-D** (Lancez `ping -n 1000`). Les requêtes `ping` ont-elles abouti ?Si la requête `ping` échoue, dépannez et corrigez les problèmes. Sur le routeur **R1**. (Vous n'arrêtez pas le `ping`).
2. Affichez la table NAT.
3. Quelle est la traduction de l'adresse d'hôte local interne de **PC-A** ?
4. Quel numéro de port a été utilisé dans cet échange **ICMP** ?
5. A partir de la machine **PC-C**, envoyez une requête `ping` à la machine **PC-F** (Lancez `ping -n 1000`). Les requêtes `ping` ont-elles abouti ? (Vous n'arrêtez pas le `ping`).
6. Affichez la table NAT.
7. Quelle est la traduction de l'adresse d'hôte local interne de **PC-A** ?
8. Quel numéro de port a été utilisé dans cet échange **ICMP** ?
9. A partir de la machine **PC-B**, envoyez une requête `ping` à la machine **PC-E** (Lancez `ping -n 1000`). Les requêtes `ping` ont-elles abouti ?
10. Affichez la table NAT.
11. Quelle est la traduction de l'adresse d'hôte local interne de **PC-B** ?
12. Quel numéro de port a été utilisé dans cet échange **ICMP** ?
13. A partir les machines de réseau interne (**PC-A** et **PC-C**), ouvrez un navigateur et entrez l'adresse IP du serveur Web sur les machines (**PC-E** et **PC-F**). Les requêtes `WEB` ont-elles abouti ?
14. Affichez la table NAT.

15. Quel protocole a été utilisé dans cette traduction ?
16. Quels sont les numéros de port utilisés ? (Interne / Externe).
17. Quel numéro de port réservé et quel service ont été utilisés ?
18. Vérifiez les statistiques NAT sur le routeur **R1**.
19. Arrêter tous les `ping`.

Tâche 5 : Effacez les traductions NAT et les statistiques

Rappel : Pour effacer les traductions NAT, en mode de privilégié, utilisez la commande `clear ip nat translation *`. Ainsi que les statistiques, utilisez la commande `clear ip nat statistics`.

1. Sur le routeur **R1**, entrez en mode de configuration globale.
2. Lancer les commandes :
   (a) `clear ip nat translation *`.
   (b) `no ip nat inside source list 1 pool POOL-NAT-LAN`.
   (c) `no ip nat pool POOL-NAT-LAN 196.200.156.225 196.200.156.254`.

Scénario 3 : Configuration et vérification de surcharge de pool NAT

Étape 6 : Configuration et vérification de surcharge de pool NAT

Dans le scénario 3, vous allez configurer le routeur **R1** de manière à traduire les adresses IP du réseau **192.168.10.0/24** en l'une des adresses utilisables de la plage **196.200.156.224/27**.

Tâche 1 : Définition du pool d'adresses IP publiques utilisables

Rappel : Pour créer un pool d'adresses pour le (NAT) dynamique, en mode de configuration globale, utilisez la commande `ip nat pool VOTRE-NOM-POOL adresse-ip-début adresse-ip-fin`.

1. Sur le routeur **R1**, entrez en mode de configuration globale.
2. Créez un pool d'adresses nommée **POOL-NAT-LOAD** allant de **196.200.156.225** à **196.200.156**

Tâche 2 : Définition la NAT à partir de la liste source interne vers le groupe externe

Remarque : rappelez-vous que les noms de pool NAT sont sensibles à la casse et que le nom de pool entré ici doit correspondre à celui utilisé à l'étape précédente.

Rappel : Pour établir une surcharge NAT de la source, en spécifiant la liste d'accès et le pool définis lors des étapes précédentes. En mode de configuration globale, utilisez la commande `ip nat inside source list access-list-number pool VOTRE-NOM-POOL overload`.

1. Sur le routeur **R1**, entrez en mode de configuration globale.
2. Établissez une une surcharge NAT de la source liste d'accès **1** et le pool `POOL-NAT-LOAD`.

Tâche 3 : Indiquez les interfaces de surcharge NAT sur R1

Rappel : Pour indiquer les interfaces de mappage (NAT) statique, en mode de configuration d'interfaces, utilisez la commande `ip nat inside` pour signaler l'interface à l'intérieure et `ip nat outside` pour spécifier l'interface externe.

1. Sur le routeur **R1**, entrez en mode de configuration d'interface.
2. Indiquez que **G0/0** du **R1** comme interface **interne**.
3. Sur le routeur **R1**, revenez en mode de configuration d'interface.
4. Indiquez que **S0/0/0** du **R1** comme interface **externe**.

Tâche 4 : Test de la configuration de fonction surcharge NAT

1. A partir de la machine **PC-A**, envoyez une requête `ping` à la machine **PC-D** (Lancez `ping -n 1000`). Les requêtes `ping` ont-elles abouti ?Si la requête `ping` échoue, dépannez et corrigez les problèmes. Sur le routeur **R1**. (Vous n'arrêtez pas le `ping`).
2. Affichez la table NAT.
3. Quelle est la traduction de l'adresse d'hôte local interne de **PC-A** ?
4. Quel numéro de port a été utilisé dans cet échange **ICMP** ?
5. A partir de la machine **PC-C**, envoyez une requête `ping` à la machine **PC-F** (Lancez `ping -n 1000`). Les requêtes `ping` ont-elles abouti ? (Vous n'arrêtez pas le `ping`).
6. Affichez la table NAT.
7. Quelle est la traduction de l'adresse d'hôte local interne de **PC-A** ?
8. Quel numéro de port a été utilisé dans cet échange **ICMP** ?
9. A partir de la machine **PC-B**, envoyez une requête `ping` à la machine **PC-E** (Lancez `ping -n 1000`). Les requêtes `ping` ont-elles abouti ?
10. Affichez la table NAT.
11. Quelle est la traduction de l'adresse d'hôte local interne de **PC-B** ?
12. Quel numéro de port a été utilisé dans cet échange **ICMP** ?
13. A partir les machines de réseau interne (**PC-A**, **PC-B** et **PC-C**), ouvrez un navigateur et entrez l'adresse IP du serveur Web sur les machines (**PC-E** et **PC-F**). Les requêtes `WEB` ont-elles abouti ?
14. Affichez la table NAT.
15. Quel protocole a été utilisé dans cette traduction ?
16. Quels sont les numéros de port utilisés ? (Interne / Externe).
17. Quel numéro de port réservé et quel service ont été utilisés ?
18. Affichez les statistiques NAT sur le routeur **R1**.
19. Affichez la table NAT.
    (a) Combien d'adresses IP locales internes sont répertoriées ?
    (b) Combien d'adresses IP globales internes sont répertoriées ?
    (c) Combien de numéros de port sont utilisés en association avec les adresses globales internes ?
20. Arrêter tous les `ping`.

Tâche 5 : Effacez les traductions NAT et les statistiques

Rappel : Pour effacer les traductions NAT, en mode de privilégié, utilisez la commande `clear ip nat translation *`. Ainsi que les statistiques, utilisez la commande `clear ip nat statistics`.

1. Sur le routeur **R1**, entrez en mode de configuration globale.
2. Lancer les commandes :
   (a) `clear ip nat translation *`.
   (b) `no ip nat inside source list 1 pool POOL-NAT-LOAD overload`.
   (c) `no ip nat pool POOL-NAT-LOAD 196.200.156.225 196.200.156.254`.

Scénario 4 : Configuration et vérification de la fonction PAT

Dans le scénario 4, vous allez configurer la fonction PAT en utilisant une interface au lieu d'un pool d'adresses pour définir l'adresse externe.

Étape 7 : Configuration et vérification de la fonction PAT

Tâche 1 : Association de la liste source à l'interface externe

Rappel : Pour associer la traduction NAT depuis la liste source interne vers une interface externe, en mode configuration globale, utilisez la commande `ip nat inside source list access-list-number interface type-interface numéro-interface overload`.

1. Sur le routeur **R1**, entrez en mode de configuration globale.
2. Établissez une une surcharge NAT de la source liste d'accès **1** et l'interface série **S0/0/0**.

Tâche 2 : Indiquez les interfaces de surcharge NAT sur R1

Rappel : Pour indiquer les interfaces de mappage (NAT) statique, en mode de configuration d'interfaces, utilisez la commande `ip nat inside` pour signaler l'interface à l'intérieure et `ip nat outside` pour spécifier l'interface externe.

1. Sur le routeur **R1**, entrez en mode de configuration d'interface.
2. Indiquez que **G0/0** du **R1** comme interface **interne**.
3. Sur le routeur **R1**, revenez en mode de configuration d'interface.
4. Indiquez que **S0/0/0** du **R1** comme interface **externe**.

Tâche 3 : Test de la configuration de fonction surcharge NAT

1. A partir de la machine **PC-A**, envoyez une requête `ping` à la machine **PC-D** (Lancez `ping -n 1000`). Les requêtes `ping` ont-elles abouti ?Si la requête `ping` échoue, dépannez et corrigez les problèmes. Sur le routeur **R1**. (Vous n'arrêtez pas le `ping`).
2. Affichez la table NAT.
3. Quelle est la traduction de l'adresse d'hôte local interne de **PC-A** ?
4. Quel numéro de port a été utilisé dans cet échange **ICMP** ?

5. A partir de **PC-B**, envoyez une requête `ping` à à la machine **PC-E** (Lancez `ping -n 1000`). Si la requête `ping` échoue, dépannez et corrigez les problèmes. Sur le routeur **R1**. (Vous n'arrêtez pas le `ping`).
6. Affichez la table NAT.
7. Quelle est la traduction de l'adresse d'hôte local interne de **PC-B** ?
8. Quel numéro de port a été utilisé dans cet échange **ICMP** ?
9. A partir de **PC-C**, envoyez une requête `ping` à à la machine **PC-F** (Lancez `ping -n 1000`). Si la requête `ping` échoue, dépannez et corrigez les problèmes. Sur le routeur **R1**. (Vous n'arrêtez pas le `ping`).
10. Affichez la table NAT.
11. Quelle est la traduction de l'adresse d'hôte local interne de **PC-C** ?
12. Quel numéro de port a été utilisé dans cet échange **ICMP** ?
13. A partir les machines de réseau interne (**PC-A**, **PC-B** et **PC-C**), ouvrez un navigateur et entrez l'adresse IP du serveur Web sur les machines (**PC-E** et **PC-F**). Les requêtes `WEB` ont-elles abouti ?
14. Affichez la table NAT.
15. Quel protocole a été utilisé dans cette traduction ?
16. Quels sont les numéros de port utilisés ? (Interne / Externe).
17. Quel numéro de port réservé et quel service ont été utilisés ?
18. Affichez les statistiques NAT sur le routeur **R1**.
19. Affichez la table NAT.
    (a) Combien d'adresses IP locales internes sont répertoriées ?
    (b) Combien d'adresses IP globales internes sont répertoriées ?
    (c) Combien de numéros de port sont utilisés en association avec les adresses globales internes ?
20. Arrêter tous les `ping`.

Tâche 3 : Effacez les traductions NAT et les statistiques

Rappel : Pour effacer les traductions NAT, en mode de privilégié, utilisez la commande `clear ip nat translation *`. Ainsi que les statistiques, utilisez la commande `clear ip nat statistics`.

1. Sur le routeur **R1**, entrez en mode de configuration globale.
2. Lancer les commandes :
   (a) `clear ip nat translation *`.
   (b) `no ip nat inside source list 1 interface S0/0/0 overload`.

Étape 8 : Suppression des configurations sur les routeurs

Il est nécessaire de commencer avec un routeur non configuré. L'utilisation d'un routeur comportant déjà une configuration peut produire des résultats imprévisibles. Les étapes suivantes permettent de préparer le routeur avant d'effectuer les travaux pratiques pour que les options de configuration précédentes ne créent pas d'interférence.

1. Passez en mode d'exécution privilégié.

2. **Effacement de la configuration :** Pour effacer la configuration, lancez la commande ***erase startup-config***. Lorsque vous êtes invité à confirmer (via **[confirm]**) que vous voulez vraiment effacer la configuration actuellement enregistrée en mémoire NVRAM, appuyez sur **Entrée**.
3. **Rechargement de la configuration :** Au retour de l'invite, lancez la commande ***reload***. Si vous êtes invité à enregistrer les modifications, répondez par **no** [**Que se passerait-il si vous répondiez yes à la question**].
4. Lorsque vous êtes invité à confirmer (via **[confirm]**) que vous voulez vraiment recharger le routeur, appuyez sur **Entrée**. Dès que le routeur a terminé l'amorçage, choisissez de ne pas utiliser la fonction **AutoInstall**.
5. Répétez les questions 1 à 4 sur le routeur R2 ?