Une image contenant Graphique, capture d’écran, graphisme, conception

Description générée automatiquement

1

Atelier 8 : Mise en oeuvre d’un serveur DHCP et agent de relais DHCP, dispositif multifonction Linksys WRT300N, NAT/PAT, serveur DNS, WEB

VENTRE

ADRIEN

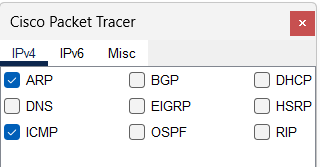
# Schéma réseau apprès installation de tous les appareille.

# Examen de la fonction NAT du routeur Linksys WTR300N

En mode Simulation, nous allons maintenant envoyer un PDU simple de PC1 vers Server1, en mode pas à pas, afin d’observer la fonction NAT du routeur WR0 :

Dans **Simulation Panel**, sélectionnez l’option **Edit Filters** et cochez uniquement les cases ARP et ICMP.

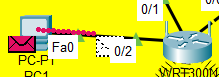




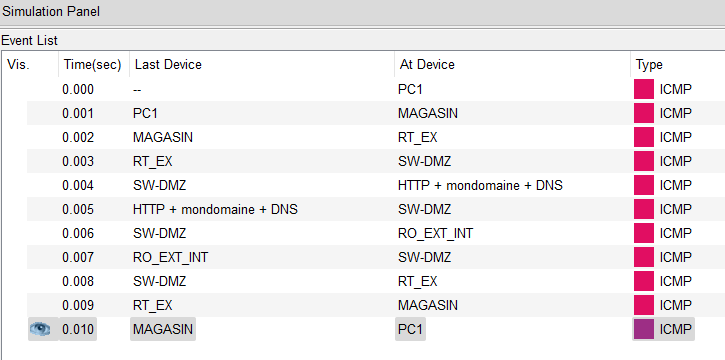
Cliquer sur l’enveloppe fermée (**Add Simple PDU**) située au-dessus de l’icône de mode de simulation.



Lancer la démonstration en mode pas à pas ; lorsque le PDU est arrivé sur **WR0**, cliquer dessus et afficher son contenu (onglet *Inbound PDU Details*).

Dans le mode simulation, les enveloppes doivent se déplacer sans erreur.

Puis la requête ICMP doit revenir au PC1 car c’est lui qui a envoyé cette requête au serveur1



|  |  |
| --- | --- |
| **Trame obtenue** | **Lorsqu’il arrive dans le routeur, quelle est l’adresse IP source émetteur du paquet IP ?** |
|  | Lorsqu’il arrive dans le routeur l’adresse IP source émetteur du paquet IP et 200.100.51.97 |

Cliquer maintenant sur l'onglet *Outbound PDU Details* pour observer le contenu du PDU lorsqu’il repart du routeur **WR0**.

|  |  |
| --- | --- |
| **Trame obtenue** | **Lorsqu’il repart du routeur, quelle est l’adresse IP source émetteur du paquet IP ?** |
|  | Lorsqu’il repart du routeur, l’adresse IP source émetteur du paquet IP et 200.100.51.29 |

La fonction NAT du routeur a-t-elle bien opéré la translation de l’adresse IP source locale en une adresse IP globale ?

Comme nous pouvons le voir sur les deux captures d’écran l’adresse de source d’émetteur du paquet IP a bien été modifiée. Je peux donc en conclure que la translation de l’adresse IP source locale se transforme bien en adresse IP globale.

Le mécanisme NAT (Network Address Translation) opère à la couche de réseau (couche 3) du modèle OSI. Plus précisément, il intervient généralement au niveau de la couche de réseau Internet (couche 3 dans le modèle TCP/IP). Le NAT est utilisé pour traduire les adresses IP et les numéros de port entre les réseaux locaux (LAN) privés et Internet.

Poursuivre la simulation jusqu’à ce que l’enveloppe atteigne la destination, puis jusqu’à ce qu’elle revienne dans le routeur **WR0** (lors du retour de la réponse).

Lorsque l’enveloppe est dans le routeur, on pourra vérifier dans les onglets *Inbound PDU Details* et *Outbound PDU Details* le mécanisme inverse de translation.

|  |  |
| --- | --- |
|  |  |
|  |  |

A la fin de la simulation nous avons le résultat suivant.



Conjointement au protocole NAT, le protocole PAT (Port Address Translation) utilise le champ Port Source du segment TCP pour y stocker un identifiant de la machine source

Le routeur garde la correspondance entre ce numéro identifiant la machine et son adresse IP source, dans une table NAT**.**

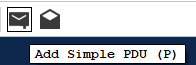
Cliquer sur le bouton **Inspect** représenté par une loupe, puis cliquer sur le routeur **WR0**. Dans le menu contextuel, sélectionnez **NAT Table** : une fenêtre affichant la table NAT du routeur s'ouvre :

# Mettre en place les scénarii d’utilisation

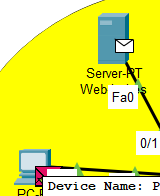
Tout d'abord, pour s'assurer que tout fonctionne, nous pouvons tester les différents réseaux. Pour cela, nous allons utiliser des scénarios pour simplifier la mise en place de ces tests.

Pour ajouter un scénario, il faut :

Récupérer un PDU ;



Cliquer sur un poste puis sur un autre ;

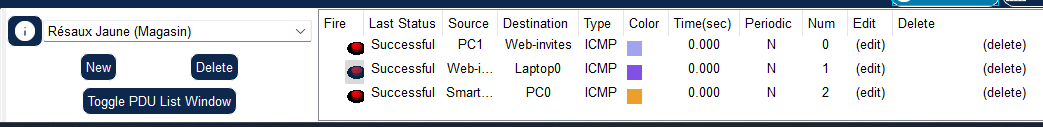


Pour commencer la réalisation des tests on peut commencer par vérifier si une machine communique avec une machine dans son réseau.

Pour le réseau Jaune (Magasin) :

Les tests qui sont réalisés consistent à vérifier la communication entre les différentes machines via des câbles RJ45. Tout d'abord, un test est effectué du serveur vers le PC1 pour vérifier si les machines peuvent communiquer entre elles via un câble RJ45. Ensuite, un test est réalisé du serveur vers le Laptop pour vérifier si le réseau câblé peut communiquer avec le réseau sans fil. Enfin, un test est effectué entre le PC0 et le Smartphone0 pour vérifier si les appareils câblés peuvent communiquer entre eux.

Sur cette image, on peut constater que la communication entre tous les appareils fonctionne correctement.

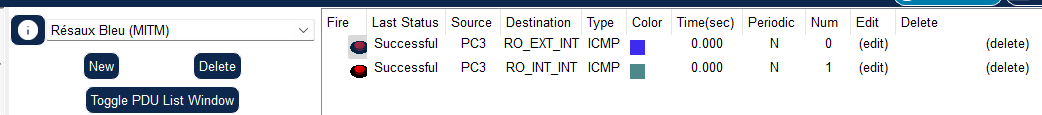


Pour le réseau Rouge (DMZ) :

Nous pouvons accéder à la configuration du PC2 pour vérifier si le DHCP a bien été récupéré à partir du routeur le plus à droite.Une image contenant texte, capture d’écran, logiciel, ligne

Description générée automatiquement

Pour le réseau bleu (MITM)

Dans ce réseau, il n'y a que PC3. Donc, les tests doivent partir de PC3 vers les deux routeurs pour vérifier s'il peut communiquer avec eux. Sur cette image, on peut voir que PC3 parvient à communiquer avec les deux routeurs avec succès.

En deuxième, nous allons vérifier si les réseaux communiquent entre eux. Pour cela, nous allons le faire en deux parties : d'abord du réseau le plus à droite vers celui le plus à gauche, puis inversement, afin que les requêtes ICMP puissent passer entre tous les routeurs.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Le dernier test est l'interconnexion entre plusieurs Packet Tracer. Dans ce test, je suis connecté avec deux personnes : Anissa et Nathan.

Une image contenant diagramme, texte, cercle, capture d’écran

Description générée automatiquementComme nous pouvons le voir, la connexion entre les deux réseaux fonctionne car il y a la présence des flèches pointant vertes.

Pour être parfaitement sûre que les réseaux sont bien connectées, il faut faire un ping entre les réseaux pour cela il faut mettre des adresse IP sur les deux ports.

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur  Description générée automatiquement |  |

Une fois les adresse IP rentrées il faut faire les pings pour voir s’il y a une réponse.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

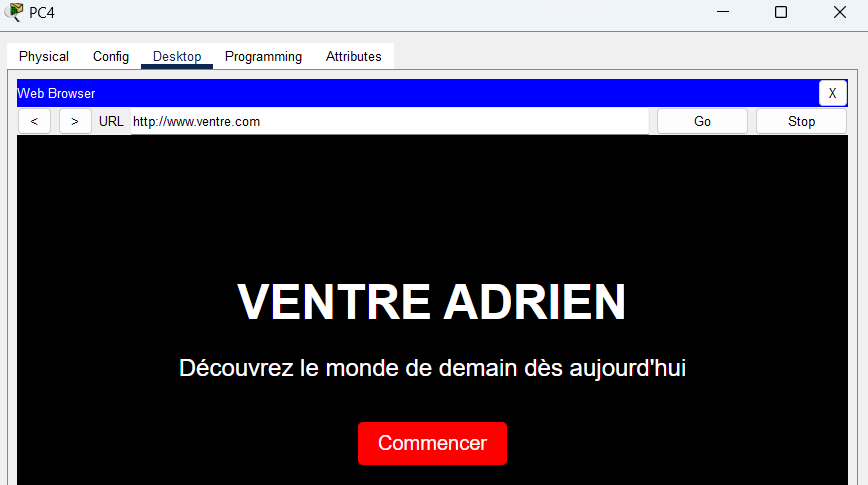
Description générée automatiquement

Une image contenant texte, Police, ligne, capture d’écran

Description générée automatiquement

On peut voir que la connexion entre les routeurs fonctionne pour les deux réseaux.

Le dernier test à faire est de vérifier si le site est disponible sur l'un des postes. Pour cela, il faut ouvrir le navigateur web et saisir son nom de domaine. Cela permet de vérifier plusieurs aspects tels que la bonne communication avec le serveur, le DNS et le protocole HTTP du serveur.

On peut constater que tous les protocoles fonctionnent correctement."

# Analyser le réseau :

|  |  |  |
| --- | --- | --- |
| Point forts | Points faibles | Incohérences |
| Séparation du réseau en plusieurs zone. | Poste dans la DMZ  DNS dans la DMZ  DHCP qui rentre dans la DMZ  Plage de restriction du DHCP | PC dans la DMZ  Un seul poste dans la zone bleue (seuil au milieu des deux réseaux). |

|  |
| --- |
| Pistes d’améliorations |
| 1. Enlever toutes les adresses publiques pour en avoir plus que 2 (une dans le magasin et une pour l’autre réseaux) 2. Mettre des masques les plus rapproche des machines existent pour éviter les insertions de machine non désirée. 3. Simplification des tables de routage avec deux tables de routage pour chaque routeur. 4. Mettre le serveur DNS dans la zone la plus éloignée |

Conclusion

Webographie