Configurer OSPF, ACL, QoS.

MATHIS DOUANGPANYA (6229633)

# Partie 1-sur packet

## Topologie logique

Configurer les adresses IP selon la topologie donnée suivante :

Une image contenant horloge, diagramme, cercle

Description générée automatiquement

## Configurer les vlans suivants

Switch1 est votre commutateur d'accès.

Multilayer Switch2 est votre commutateur de distribution qui gère le routage inter-VLAN.

Vlan 10 va servir pour les **Profs**

**La passerelle par défaut sera dans ce cas : 10.1.10.1/24**

Vlan 20 va servir pour les **Étudiants**

**La passerelle par défaut sera dans ce cas : 10.1.20.1/24**

**Utiliser la méthode « Router on a Stick » pour configurer la gestion du routage entre plusieurs VLANs à travers une seule interface physique sur le routeur.**

**(Créer des sous-interfaces du routeur pour chaque vlan**

**Exemple : interface** g0/0/0.10 pour le vlan 10 et interface g0/0/0.20 pour le vlan 20**).**

A black text on a white background

AI-generated content may be incorrect.

Le ping entre PC1 et PC2 devrait fonctionner. Le switch fonctionne comme un routeur. Donc assurez-vous de configurer les vlans et les adresses ip.

A purple square with black text

AI-generated content may be incorrect.

## Configurer routeurs avec OSPF

**Comme on pense faire évoluer le réseau, on aimerait que vous utilisiez le protocole OSPF sur les composants qui en ont besoin.**

Pour simplifier, disons que vous voulez configurer OSPF dans une seule aire (l'aire 0, qui est l'aire backbone d'OSPF).

Le numéro de processus qui est un identifiant local sera : 1.

**Switch1 :**

Id : 1.1.1.1

A number of numbers and letters

AI-generated content may be incorrect.

**Router-3:**

Id : 3.3.3.3

A number of numbers on a white background

AI-generated content may be incorrect.

**ISP:**

Id: 2.2.2.2

A number of numbers and letters

AI-generated content may be incorrect.

## Vérifier la connectivité

Vérifier la connectivité entre les 2 PCs vers un des serveurs de votre choix (Capture d’écran)

Si cela ne fonctionne pas, faire du dépannage réseau pour trouver votre erreur. (C’est votre travail de trouver l’erreur, comme on vous a engagé pour cela).

Si cela n’a pas fonctionné du premier coup, écrivez ici comment vous avez fait pour résoudre votre problème.

A screenshot of a computer

AI-generated content may be incorrect.

**Lors des tests de connectivité entre les PC et les serveurs situés dans la DMZ, tous les pings ont échoué malgré une configuration correcte des adresses IP, des routes statiques et des interfaces réseau sur les routeurs et les switches. Après vérification, l’erreur provenait du fait que les serveurs ne disposaient pas de passerelle par défaut. Sans cette information, les serveurs pouvaient recevoir les requêtes ICMP des PC, mais ne savaient pas comment renvoyer les réponses, ce qui bloquait la communication. La solution a été d’ajouter manuellement la passerelle 8.8.8.1 sur chaque serveur, correspondant à l’interface du routeur ISP connectée au réseau DMZ. Une fois cette modification effectuée, les pings entre les PC et les serveurs ont réussi, confirmant le bon fonctionnement du routage entre les VLAN internes et la DMZ.**

## Configurer le NAT sur le routeur 3

Configurer le **PAT** pour permettre aux hôtes de votre réseau interne d'accéder à la DMZ. On veut donc que les PC qui sont sur le **VLAN 10** puissent accéder à tous les serveurs de la DMZ.

Utiliser une ACL nommée standard sur le routeur Router-3 : **NAT\_TRAFFIC\_WEB**



A yellow square with black text

AI-generated content may be incorrect.

A yellow text on a white background

AI-generated content may be incorrect.



Puis tester la connectivité en tentant d’ouvrir une page web a partir du PC1 (du vlan 10) vers le serveur Web 1 et le serveur web 2 de la DMZ (Captures d’écran)

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## Création d’une ACL pour empêcher l’accès du PC2 vers les serveurs web.

Maintenant, on voudrait créer une ACL qui permette d’empêcher l’accès du PC2 (Vlan 20) d’accéder aux serveurs (empêche tout trafic qui viendrait d'un PC appartenant au vlan 20 d'aller vers le réseau qui se trouve dans la DMZ).

Donc créé une ACL étendue la plus proche de la source et donc sur le routeur Router-3 sur l’interface entrante pour réduire la charge inutile sur le réseau.

Nommer cette ACL étendue : **BLOCK\_VLAN20\_WEB**





Tester que cela a bien bloqué en tentant d’ouvrir une page web à partir du PC du VLAN20 et aussi à partir du PC du VLAN10 (**Captures** **d’écran**)

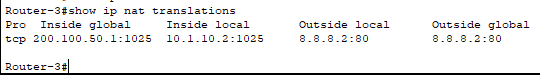
A blue and white box with text

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Rentrer la commande dans le routeur Router-3 (translations NAT) qui montre que le PAT a bien fonctionné (Capture d’écran)



Complété le tableau suivant selon la commande entré pour avoir ces informations :

Quelle commande avez-vous entré ?

show ip nat translations (quand j’ai ouvert la page web sur mon pc)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protocole | Inside global | Inside local | Outside local | Outside global |
| tcp | 200.100.50.1 :1033 | 10.1.10.2 :1033 | 8.8.8.2 :80 | 8.8.8.2 :80 |

## Création d’une ACL pour empêcher l’accès des étudiants vers le serveur web 8.8.8.2 via les pings.

Création d’une ACL étendue pour empêcher les étudiants du Vlan 20 de communiquer avec le serveur 8.8.8.2 via les pings seulement, tout en permettant tout autre trafic de passer librement.

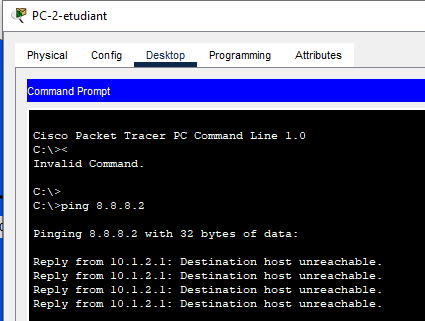
Nommer cette ACL étendue : **BLOCK\_PING**

A yellow text on a white background

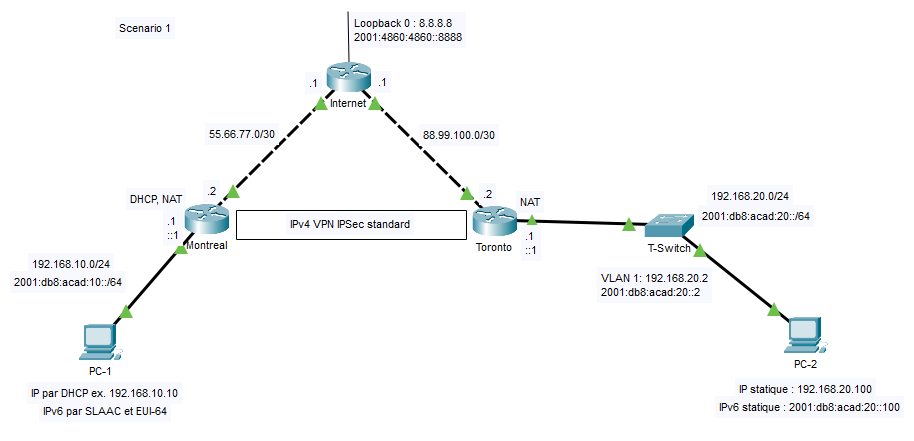
AI-generated content may be incorrect.

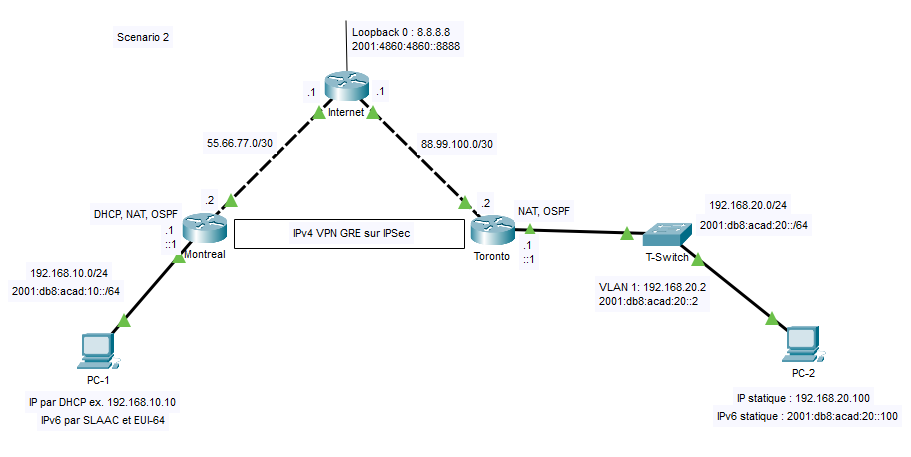
Faites une capture d’écran qui montre que le ping ne fonctionne pas vers 8.8.8.2, mais qu’on puisse accéder au site web à partir du PC2.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Partie au Minilab (sur 100 points; compte pour 13%; par équipe de deux étudiants; temps : 60 min; pénalité : 1 point/min)**

Voici deux topologies logiques (2 scénarios) à mettre en place d’un IPv4 VPN IPSec standard et IPv4 VPN GRE sur IPSec:



***Déroulement de la présentation :***

Vous disposez de 40 minutes pour réaliser le scénario 1. Une fois terminé, veuillez faire valider les fonctionnalités de cette étape par votre enseignant. Après validation, vous pourrez entamer le scénario 2, que vous devrez compléter en 20 minutes.

***Consignes pour chaque scénario :***

1. Nommer vos 3 routeurs et le commutateur. /4
2. Configurer les adresses IPs sur les 3 routeurs (Pas de OSPF pour le **scénario 1**). /8
3. Configurez le loopback 0 sur le router Internet. /2
4. Activez un serveur DHCP sur le routeur de Montréal pour le réseau 192.168.10.0/24. /5
5. Activez le SLAAC sur le routeur de Montréal pour le réseau 2001:db8:acad:10::/64. /5
6. Activez le NAT sur le routeur de Montréal. /5
7. Activez le NAT sur le routeur de Toronto. /5
8. Activez OSPF sur les routeurs de Montréal et Toronto pour le **scénario 2**. /6
9. Configurez le VPN sur le routeur de Montréal. /8+8
10. Configurez le VPN sur le routeur de Toronto. /8+8
11. Vérifiez le ping IPv4 de PC-1 vers PC-2 et vice versa. /2+2
12. Vérifiez le ping IPv6 de PC-1 vers PC-2 et vice versa. /2+2
13. Activez ssh sur le commutateur T-Switch. /4
14. Connectez-vous à partir de PC-1 par ssh avec IPv4 sur le commutateur T-Switch. /2+2
15. Connectez-vous à partir de PC-1 par ssh avec IPv6 sur le commutateur T-Switch. /2+2
16. Vérifiez le ping de PC-1 vers 8.8.8.8 et 2001:4860:4860::8888 (Simuler internet). /2+2
17. Vérifiez le ping de PC-2 vers 8.8.8.8 et 2001:4860:4860::8888 (Simuler internet). /2+2