

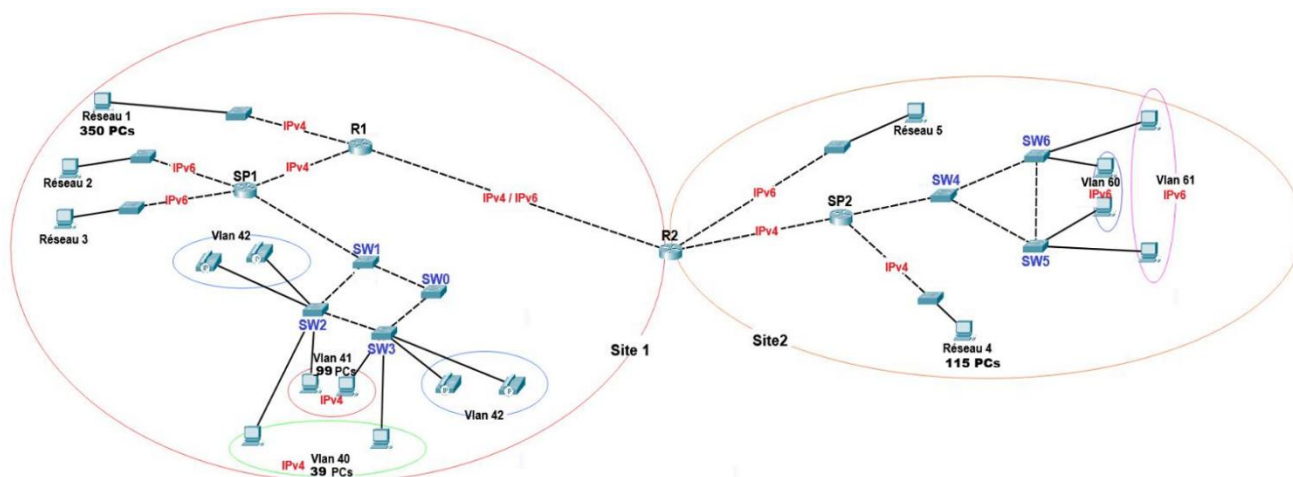
GTI611 Réseaux de communication IP

Laboratoire 1 : Adressage IPv4 et IPV6, configuration de vlans, Dual-stack, Routage statique, tunneling IPv6, Routage OSPFv2 et Routage BGP

Objectif :

Le but du laboratoire est la configuration de l'adressage et du routage IPv4 et IPv6 ainsi que des vlans. Vous apprendrez à subdiviser une adresse IPv4 ou IPv6 entre plusieurs sous-réseaux et vlans et à configurer les différents équipements appartenant à ces derniers. Une fois l'adressage complété, le routage statique puis dynamique (OSPF) seront appliqués pour permettre l'interconnexion entre ces différents sous-réseaux et vlans. Le routage BGP sera ensuite mis en place pour tester un routage inter-domaines entre plusieurs systèmes autonomes.

Première partie : Planification d'adressage IPv4 et IPv6 et configuration de vlans



Téléchargez le fichier **Labo1_partie1.pkt** disponible sur le site du cours. Il contient le schéma de réseau de deux parmi les **10 sites** d'une entreprise. Ces sites comprennent plusieurs sous-réseaux et vlans à configurer, certains en IPv4 et d'autres en IPv6. Pour cette partie, vous devez configurer l'adressage IPv4 et IPv6 sur les différents équipements conformément à ce qui est demandé.

- La topologie contient 13 sous-réseaux se décomposant en 10 sous-réseaux d'extrémité et 3 d'interconnexion. Dans notre cas, un sous-réseau d'interconnexion est celui formé par le lien point à point entre deux routeurs.

- L'adresse IPv4 assignée à l'entreprise est **142.137.144.0/21** et le préfixe IPv6 de routage global est **2001:34a7:cd0::/44**.
 - Vous devez partitionner les adresses fournies de la façon la plus optimale, de sorte à attribuer des plages de valeurs distinctes à ces 13 sous-réseaux. Les indications quant au nombre d'interfaces nécessaires pour chacun des sous-réseaux IPv4 vous sont fournies au niveau du fichier **Labo1_partiel.pkt**.
 - Pour l'adressage IPv4, chacun des deux sites aura la moitié de l'espace d'adresses disponible. Pour l'assignation des adresses aux différents sous-réseaux, utilisez le VLSM pour minimiser les pertes d'adresses ce qui permettra de maximiser l'espace d'adressage résiduel.
 - Pour l'adressage IPv6, respectez la règle des préfixes de sous-réseaux multiples de 4 bits : ceci vous permettra d'avoir un préfixe plus lisible. Prévoyez une extension future qui permettra l'intégration d'autres sous-réseaux.
 - Un sous-réseau étant lui-même un réseau, on ne va utiliser dans le reste de cet énoncé que le terme réseau.
1. Complétez le tableau 1 ci-dessous en donnant pour chacun des réseaux IPv4 la taille du bloc d'adresses que vous devriez lui réserver.

Réseaux IPv4	Taille du bloc (unité)
Réseau 1 (350 PCs)	
Réseau 4 (115 PCs)	
Vlan40 (39 PCs)	
Vlan41 (99 PCs)	
Vlan42 (VoIP) (4 téléphones)	
Interconnexion R1 – R2	
Interconnexion R1 – SP1	
Interconnexion R2 – SP2	

Tableau 1

2. Complétez les tableaux 2 et 3 ci-après en donnant :
- pour chacun des réseaux IPv4, son adresse réseau, son masque, et son adresse de diffusion
 - pour chacun des réseaux IPv6, son adresse réseau (préfixe global + identificateur de sous-réseau).

<u>Réseau IPV4</u>	<u>Adresse de Réseau</u>	<u>Masque</u>	<u>Diffusion</u>
Réseau 1			
Réseau 4			
Vlan40			
Vlan41			
Vlan42 (VoIP)			
R1 – R2			
R1 – SP1			
R2 – SP2			

Tableau 2

Réseau IPv6	Adresse du réseau
Réseau 2	
Réseau 3	
Réseau 5	
Vlan 60	
Vlan 61	
R1 – R2	

Tableau 3

3. Après avoir attribué des adresses à tous les réseaux IPv4, calculez le nombre d'adresses encore libres dans chacun des deux sites.

Configuration de Vlans par VTP

Le but de cette partie est de configurer et de faire communiquer entre eux des Vlans. Deux vlans, 40 et 41 nommés **admin** et **labo** qui doivent être configurés en IPv4 sur les commutateurs SW0, SW1, SW2 et SW3, et deux autres vlans, 60 et 61 nommés **conseil** et **service** qui doivent être configurés en IPv6 sur les commutateurs SW4, SW5 et SW6.

Pour éviter de refaire les mêmes configurations sur tous les commutateurs, vous devez faire appel au protocole VTP (Virtual Trunking Protocole).

En VTP, les commutateurs peuvent fonctionner en mode *VTP Server*, *VTP Client* ou *VTP Transparent*.

- Configurez le commutateur SW1 comme serveur VTP. Sur l'interface de commande (CLI) accédez au mode de configuration générale et configurez les 3 paramètres VTP, la version, le mode et le domaine avec les commandes:
 - ***vtp version 2***
 - ***vtp mode server***
 - ***vtp domain lab1_IPv4***.
- De la même manière que pour SW1 et en utilisant les mêmes commandes, configurez le commutateur SW4 comme serveur VTP pour la partie IPv6 du réseau. Utilisez comme nom de domaine ***lab1_IPv6***.
- Configurez les commutateurs SW2 et SW3 (ainsi que SW5 et SW6 pour IPv6) comme clients VTP avec la commande :
 - ***vtp mode client***
 - ***vtp domain lab1_IPv4 (lab1_IPv6 pour SW5 et SW6)***
- Configurez le commutateur SW0 comme VTP transparent
 - ***vtp mode transparent***
 - ***vtp domain lab1_IPv4***

- Créez les vlans sur les commutateurs serveurs. Les vlans IPv4 au niveau du commutateur SW1 et les vlans IPv6 au niveau du commutateur SW4. Les commandes à utiliser pour le vlan **admin**, par exemple, sont (toujours lancées à partir du mode de configuration générale) :
 - ***vlan 40***
 - ***name admin***
 - ***exit***

Vous devez refaire la même procédure pour les autres vlans (IPv4 et IPv6)

- Configurez les interfaces des commutateurs serveurs en mode trunk avec les commandes :
 - ***interface range fastEthernet 0/1–2***
 - ***switchport mode trunk***
- Vous pouvez, en tout temps, entrer les commandes : ***do show vlan brief*** pour voir l'état des vlans que vous avez créés et ***show vtp status*** pour afficher les états vtp/vlan de vos commutateurs.
- Configurez les interfaces reliant les commutateurs entre eux en mode trunk avec la commande : ***switchport mode trunk***

À chaque fois que vous configurez une interface en mode trunk, l'interface qui lui est reliée sur le commutateur voisin est mise à ce même mode automatiquement. Et les informations des vlans sont transmises à travers ces interfaces.

4. Quels sont les avantages d'avoir un commutateur en mode VTP serveur ?
5. En utilisant la commande **show vlan brief**, donnez la liste des vlans configurés sur le commutateur SW0 et celle de ceux configurés sur le commutateur SW3. Donnez une capture d'écran de ces vlans.
6. Est-ce que les deux commutateurs ont configuré les mêmes vlans? Expliquer votre réponse.
 - Changer le mode de SW0 de transparent à client
 - Essayez de configurer manuellement le vlan 42 sur le commutateur SW3.
7. Quel est le résultat de la console ? Pourquoi un tel résultat ?
 - Configurez, sur chacun des commutateurs, les interfaces qui sont reliées à des PCs en mode access. Assurez-vous qu'elles soient associées aux bons vlans. Les commandes à utiliser sont :
 - ***interface numeroInterface***
 - ***switchport access vlan numVLAN***
 - ***exit***
8. Vérifiez que les PCs sont dans les vlans appropriés en les affichant grâce à la commande **show vlan brief** (inclure une capture d'écran dans votre rapport).
 - Utilisez le plan d'adressage que vous avez conçu pour attribuer des adresses IP aux différents équipements (**PCs et routeurs**). Pour configurer les passerelles par défaut des différents réseaux et vlans utilisez les premières adresses disponibles pour ces réseaux. Noter que pour une passerelle par défaut IPv6, l'identificateur de l'interface sera dans ce cas **::1**). Pour ce qui est des

PCs de test (représentés dans **Labo1_partie1.pkt**) que ce soit en IPv4 ou en IPv6, vous pouvez choisir n'importe quelles autres adresses disponibles au niveau de ces réseaux.

- Vous devriez être en mesure, à ce niveau, de faire communiquer les PCs d'un même vlan entre eux.

Configuration de la communication Inter-vlans

- Pour faire communiquer les vlans entre eux, on doit passer par des routeurs. Pour ce faire, vous devez subdiviser, en sous-interfaces logiques, les interfaces des routeurs SP1 et SP2 reliées aux commutateurs SW1 et SW4 respectivement. Chaque sous-interface logique est associée à un vlan. (Le nombre de sous-interfaces correspond au nombre de vlans devant être connectés au routeur).
- Pour le vlan *conseil* par exemple (qui est un vlan IPv6 ayant comme numéro 60), vous devez utiliser les commandes suivantes sur le routeur SP2:
 - *interface GigabitEthernet 0/1.60*
 - *encapsulation dot1Q 60*
 - *ipv6 address adrPasserelleVlanConseil masquePasserelle*
 - *exit*

Vous devez faire la même configuration pour le vlan 61 et les vlans IPv4. Pour IPv4, la commande qui permet de configurer l'adresse IP (de l'interface Ethernet1/2 du routeur SP1) serait de la forme *ip address adrPasserelleVlanConseil masquePasserelle*.

- N'oubliez pas de :
 - Activer le routage IPv6 sur le routeur SP2 avec la commande *ipv6 unicast-routing*.
 - Mettre les interfaces qui relient SW1 au routeur SP1 et SW4 à SP2 en mode **trunk**
- Vous devriez être en mesure, à ce niveau, de faire de la communication inter-vlans.

Configuration du vlan VoIP

- Si ce n'est pas déjà fait, vous devez créer le vlan 42 au niveau du commutateur serveur SW1. Vous devez suivre la même procédure que celle utilisée pour créer les vlan 40 et 41.
- Les paramètres du vlan voix seront configurés sur le routeur SP1. Pour ce faire, ajoutez une sous-interface à l'interface Ethernet1/2 pour le vlan 42 (vlan VoIP) avec comme adresse IP, l'adresse de la passerelle par défaut de ce vlan.
- Pour que les téléphones IP puissent récupérer automatiquement leurs configurations réseau (IP, masque...) vous devez configurer le DHCP en utilisant les commandes suivantes :
 - *ip dhcp pool VOICE*
 - *network adresseVlan42 masque*
 - *default-router adrPasserelle*
 - *option 150 ip adrPasserelle*
 - *exit*

- *ip dhcp excluded-address adrPasserelle*

L'option 150 permet au téléphone d'identifier le protocole utilisé, ici le **protocole propriétaire de Cisco, SCCP**, "Skinny Call Control Protocol". Si nous avons utilisé le protocole standard, le **protocole SIP** pour "Session Initiation Protocol", l'**option** aurait alors été **66**.

- Pour que les téléphones puissent être dans le vlan voix vlan 42, il faut mettre les interfaces Fa0/5 et Fa0/6 des commutateurs SW2 et SW3 dans le vlan VOICE avec la commande :
 - *Switchport VOICE vlan 42*
- Revenez au routeur SP1 et activer les services de téléphonie en utilisant les commandes :
 - *telephony-service*
 - *max-ephones 5*
 - *max-dn 5*
 - *ip source-address adrPasserelle port 2000*
 - *auto assign 1 to 4*
- Et enfin vous devez déclarer les numéros de lignes internes à utiliser (à partir du mode de configuration générale) :
 - *ephone-dn 1*
number 100
exit

(Refaites ces mêmes configurations pour les 3 autres téléphones en utilisant 200 pour le 2, 300 pour le 3 et 400 pour le 4)

- Un téléphone IP a deux interfaces réseaux, une à connecter au réseau et une autre pouvant être connectée à un PC. Pour ce dernier, le téléphone jouera le rôle d'un commutateur. Pour tester cela,
 - Ajouter un PC qui doit appartenir au vlan 41 et connectez-le au **IP Phone 1**.
 - Configurez-lui une adresse IP et une passerelle par défaut.
 - Vous devez mettre l'interface du commutateur SW3, connectée au **IP Phone 1**, dans le vlan approprié (en mode access associée vlan 41).
 - La communication entre le nouveau PC et les différents PCs des vlans IPv4 doit fonctionner.
9. Lancez un ping d'un des PCs du vlan 40 vers le nouveau PC et remettez une capture d'écran montrant que le ping a bien réussi.
- Enregistrez votre fichier Labo1_part1.pkt ainsi configuré et faite une copie, que vous appellerez Labo1_OSPF.pkt. Cette dernière va être utilisée pour la configuration du routage dynamique.

Deuxième partie : Le routage statique

Dans cette partie, vous devez faire les configurations qu'il faut pour permettre aux différents sous-réseaux de communiquer entre eux.

10. Affichez les tables de routage IPv4 et IPv6 du R2 en utilisant les commandes **show ip route** et **show ipv6 route** respectivement. Donnez les réseaux IPv4 et IPv6 accessibles (visibles) par ce routeur.
 11. Est-ce qu'un ping du réseau 1 vers le vlan 40 est possible? Pourquoi?
 12. Est-ce qu'un ping du réseau 1 vers l'interface Fa0/0 de SP1 est possible? Pourquoi?
 13. Est-ce qu'un ping du réseau 1 vers l'interface Eth1/2 de SP1 est possible? Pourquoi?
 14. Que manque-t-il aux routeurs pour que le réseau soit complètement opérationnel ?
- Complétez les tables de routage des routeurs R1, R2, SP1 et SP2 en leur ajoutant des routes statiques qui mènent vers les réseaux non directement connectés à eux. Vous pouvez le faire en utilisant les commandes **ip route** et **ipv6 route** (à partir du mode de configuration générale).
- Exemple : pour chacune des interfaces d'un routeur, configurez le prochain saut :
- En IPv4 : Router (conf)# **ip route** *adrIPv4 masque adrProchainSaut* (où *adrIPv4*, *masque* et *adrProchainSaut* représentent respectivement, l'adresse du réseau de destination, son masque réseau et l'adresse du prochain saut)
 - En IPv6 : Router (conf)# **ipv6 route** *adrIPv6/préfixe adrProchainSaut* (où *adrIPv6* représente l'adresse du réseau de destination, *préfixe* la longueur de son préfixe et *adrProchainSaut* l'adresse associée à l'interface du prochain saut)
- Activez le routage IPv6 sur chacun des routeurs (si ce n'est pas déjà fait) avec la commande:
Router1 (conf)# **ipv6 unicast-routing**
 - Il est aussi conseillé d'utiliser la commande **copy running-config startup-conf** pour enregistrer les informations de configuration dans la configuration de démarrage.
15. Le PC du réseau 1 réussit-il à transmettre un *ping* à un PC du Vlan40? Donnez une capture d'écran montrant le résultat du ping.
 16. Le PC du réseau 2 réussit-il à transmettre un *ping* à un PC du Vlan60? Expliquer pourquoi.
 17. Que manque-t-il au réseau pour que cela soit possible?

Tunneling IPv6 : Vous devez maintenant configurer un tunnel IPv6 entre les routeurs SP1 et R1 d'une part et les routeurs SP2 et R2 d'autre part. Chacun de ces tunnels permettra de faire passer du trafic IPv6 sur un lien IPv4.

Les adresses IPv6 pour les tunnels sont:

Tunnel 0 entre SP1 et R1 :

SP1 :2001:abcd:1234:aa::1/64, R1 : 2001:abcd:1234:aa::2/64

Tunnel 1 entre SP2 et R2 :

SP2 : 2001:abcd:1234:bb::1/64, R2 : 2001:abcd:1234:bb::2/64

Les commandes à exécuter pour créer un tunnel IPv6 sur SP1 sont les suivantes : (vous devez répéter ces instructions pour SP2 et R2) :

- Création du tunnel : *SP1(config) # interface tunnel 0*
 - Configuration de l'IPv6 : *SP1(config-if) # ipv6 address 2001:abcd:1234:aa::1/64*
 - Configuration de la source : *SP1(config-if) # tunnel source FastEthernet0/0* (*FastEthernet 0/0* est l'interface de SP1 reliée à R1)
 - Configuration de la destination : *SP1(config-if) # tunnel destination « adresse de l'interface Eth1/0 de R1 »* (*Eth1/0* est l'interface de R1 reliée à SP1)
 - Configuration du mode : *SP1(config-if) # tunnel mode ipv6ip*
 - Activez le routage IPv6 : *SP1(config) # Ipv6 Unicast-routing*
 - Configurez la route par défaut sur SP1 : *SP1(config) # Ipv6 route ::/0 2001:abcd:1234:aa::2*
- Vous devez actuellement être capable de transmettre des pings entre les PCs des vlans 60 et 61 et ceux des autres réseaux IPv6 (réseau2, 3 et 5).
 - Enregistrez votre fichier, vous devez le remettre avec votre rapport. Le fichier Packet Tracer remis sera analysé pour vérifier que tous les réseaux IPv4 peuvent communiquer entre eux et qu'il en est de même pour les réseaux IPv6.

Troisième partie : Le routage dynamique

Routage OSPF:

- Pour cette partie, vous devez reprendre le fichier Labo1_OSPF.pkt et configurer le routage OSPF pour interconnecter **les réseaux IPV4** entre eux.
- Il faut activer le protocole OSPF sur tous les routeurs.
- Les commandes à utiliser sont les suivantes (à configurer sur tous les routeurs):
 - ***router ospf IDprocess***
IDprocess est un numéro qui permet d'identifier un processus de routage OSPF sur le routeur. Mettez-le à 1 pour tous les routeurs.
 - ***network adrIP masqueGen area areaNum***
adrIP représente l'adresse du sous-réseau relié à l'interface du routeur (refaire cette commande pour tous les réseaux connectés au routeur)
masqueGen (wildcard) un masque générique représente les adresses des interfaces qui peuvent se trouver dans ce segment (c'est l'inverse du masque sous-réseau ; par exemple, pour un réseau ayant un masque 255.255.255.0, le masque générique sera 0.0.0.255).
areaNum représente le numéro de la zone OSPF à laquelle est rattaché le routeur. Une zone OSPF est un groupe de routeurs qui partagent les informations d'état des liaisons (tous les routeurs de la même zone doivent avoir les mêmes informations). Dans notre cas, on suppose que tous les routeurs font partie de la même zone 0 (donc utilisez 0 pour areanum).
 - ***passive-interface interface***

pour désactiver les mises à jour sur les interfaces des routeurs connectées à des réseaux d'ordinateurs, puisque celle-ci ne sont pas connectées à des routeurs. Par conséquent, toute diffusion de routes sur ces interfaces est inutile.

(Cette interface ne participera plus au routage OSPF, mais son sous-réseau qui sera considéré comme étant d'extrémité continuera d'être annoncé dans les mises à jour de routage)

- Vous devez avoir la partie du réseau configurée en IPv4 complètement connectée.
- Affichez la table du routage du routeur R2

18. Quelles sont les routes apprises par OSPF? Quels sont les coûts de ces routes? Il faut inclure dans votre rapport une capture d'écran qui illustre les routes et les coûts OSPF.

- Enregistrez votre fichier, vous devez le remettre avec votre rapport. Le fichier Packet Tracer remis sera analysé pour vérifier que des communications IPv4 peuvent être établies entre les différentes PCs du réseau.

Routage BGP :

Pour cette partie, utilisez le fichier *Lab01_BGP*, disponible sur le site du cours, pour configurer le routage inter-domaine BGP.

- Assignez des adresses aux PCs et aux interfaces des routeurs en vous basant sur les adresses réseaux incluses dans le fichier.
- Pour configurer le routage BGP, vous devez exécuter les commandes suivantes sur chacun des routeurs:
 - **Router BGP** *NumeroAS*
NumeroAS représente le numéro de l'*autonomous-system* auquel le routeur appartient (il est indiqué sur la topologie).
 - **Neighbor** *adrIP remote-as* *NumeroAS*
NumeroAS est le numéro d'AS du routeur auquel vous voulez vous connecter avec BGP.
adrIP est l'adresse du prochain saut avec connexion directe.
 - **network** *adrIP mask* *masque*.
adrIP représente l'adresse du réseau terminal et le *masque* son masque réseau.

19. Affichez la table de routage du routeur 1.

a) Donnez les adresses des réseaux visibles ou accessibles par ce routeur et donnez pour chacune de ces adresses le prochain saut qui mène vers elle.

20. Exécutez la commande **show ip bgp** sur le routeur 1 et affichez le résultat

- a) Combien de routes ont été construites pour le réseau **204.15.30.64/26**?
- b) Donnez pour chacune des routes son chemin d'ASs (AS-PATH)
- c) Quelle est la meilleure route disponible vers ce réseau?

21. Exécutez la commande **show ip bgp summary** sur le routeur 1 et affichez le résultat. À quoi sert cette commande?

- Enregistrez votre fichier, vous devez le remettre avec votre rapport. Le fichier Packet Tracer remis sera analysé pour vérifier que des connexions IPv4 peuvent être établies entre les différentes PCs du réseau.

REMISE DU RAPPORT

- Remettez une copie du rapport ainsi que les fichiers Packet Tracer demandés sur le site Moodle en utilisant le lien créé à cet effet. Regroupez tous les documents dans un fichier compressé ayant un nom de la forme :
GTI611_20261_labo1_Prenom1Nom1_Premon2Nom2
- **Aucun retard ne sera toléré.** 20% de la note sera retirée par jour de retard à partir du début du laboratoire de la remise.
- Pour toute question, contactez vos chargés de laboratoire (adresses courriel disponibles sur le site Moodle du cours)

PONDÉRATION

- Présentation et qualité du français : 5%
- Introduction : 5%
- Résultats, analyses et réponses aux questions : 80%
- Discussion : 5%
- Conclusion : 5%