Travaux pratiques Réseaux

Constant COLOMBO

Travaux pratiques Réseaux

Ce document regroupe tous les sujets travaux pratiques préparés pour les cours Réseaux en 3A, 4A et 5A. Les sujets sont répartis en 3 séries de TP thématiques :

- TP Architecture des Réseaux : ces sujets couvrent les fondamentaux LAN, et accompagnent le cours et les TDs d'Architecture des Réseaux. Ces TPs sont à réaliser dans l'ordre.
  1. Commutateur
  2. VLAN
  3. Routeurs
  4. Routage
  5. Redondances LAN
- TP Contrôle d'accès : ces sujets sont orientés cybersécurité. Pour des raisons de quantité de matériel, il est conseillé de faire des groupes tournants.
  - DHCP, NAT et Syslog
  - ACL
  - Firewall
  - VPN et Proxy
- TP Infrastructure des réseaux opérateurs : ces sujets ont pour but d'illustrer des techniques et des problématiques d'opérateur. Pour des raisons de quantité de matériel, il est conseillé de faire des groupes tournants.
  - Audiovisuel : RTP et Multicast
  - BGP
  - IPv6
  - Management de réseau
  - QoS
- TP Complémentaires : ces sujets sont des anciens sujets, ou des thématiques annexes. Ils ne sont pas indispensables, mais disponibles si le temps le permet.
  - Connectique LAN et WAN (2*2h)
  - Outils OAM (2h)
  - Utilisation élémentaire de Linux (2h)
  - Installation Linux

Travaux pratiques - Architecture des Réseaux

TP 1 - Commutateur

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

Ce TP a pour but de vous faire découvrir les Commutateurs, l'utilisation de l'interface de configuration, et de vous sensibiliser à la notion de VLAN.

Éléments de cours

Un commutateur est une unité réseau de couche 2 (couche liaison de données) qui agit comme point de concentration pour le raccordement de stations de travail, de serveurs, de concentrateurs et d'autres commutateurs. Les interfaces des commutateurs Ethernet sont disponibles en plusieurs débits, y compris 10 Mbits/s (Standard Ethernet), 100 Mbits/s (Fast Ethernet) et 1 000 Mbits/s (Gigabit Ethernet).

Un LAN (Local Area Network) est un réseau d'interconnexion d'hôtes, situés dans un même lieu (une salle, un bâtiment, un campus). On lui oppose en général les WANs (Wide Area Network) qui ont une portée et des architectures différentes (ville, pays, etc). Les LANs regroupent en général les utilisateurs par emplacement, mais il est parfois également nécessaire de segmenter le réseau par fonction ou besoins. C'est la qu'interviennent les VLANs (Virtual LAN). Ils ne dépendent pas des segments physiques, mais doivent être déclarés sur des interfaces.

Matériel nécessaire

- 2 commutateurs CISCO
- 3 PC sous Windows ou Ubuntu
- 1 câble console (à paires inversées) pour connecter le port série du PC au port console des commutateur

1 Première partie : Vue d'ensemble d'un commutateur

Cette première partie a pour objectif de vous apprendre les différentes commandes communes utiles à l'administration d'un commutateur.

1. Examinez le commutateur (relevez le numéro de modèle, les différents ports, type d'interfaces ...).
2. Connectez votre station de travail au commutateur à l'aide d'un câble console.
3. Il faut identifier le port auquel vous êtes connecté sur l'hôte.
   - Sur Linux, l'interface par défaut est "ttyS0". Si vous utilisez un adaptateur USB, utilisez la commande `cd /dev; ls -ltr *tty*` pour trouver le nom de l'interface la plus récente.
   - Sur Windows, l'interface par défaut est "COM0". Si vous utilisez un adaptateur USB, utilisez le Gestionnaire de périphériques pour trouver le nom de l'interface dans la catégorie "Ports (COM et LPT)".
4. Connectez-vous au commutateur à l'aide du programme Putty avec les paramètres suivants :

Port	Valeur relevée au point précédent
Bits par seconde	9600
Bits de données	8
Parité	Aucun
Bits d'arrêt	1
Contrôle de flux	Aucun

5. Lancez la commande `show version`. Quelle est la version de l'IOS ? Quel est le nom du fichier image ? À partir d'où le fichier image a-t-il été lancé ?
6. Testez la commande `show ver`. Que remarquez-vous ?
7. Testez les commandes : `?` et `show ?`. À quoi sert le caractère ? ?
8. Vous êtes en mode d'exécution simple. Utilisez la commande `enable` pour passer en mode privilégié.
9. Testez à nouveau les commandes : `?` et `show ?`. Que remarquez-vous ?
10. Effectuez les commandes `show running-config` et `show startup-config`
    Sur IOS $\leq$ 12.0, utilisez les commandes `show running` et `show config`.
    Quelle est la différence entre ces deux commandes ?
11. Remplissez le tableau suivant avec les commandes `show` correspondantes :

Commande	**Effet**
show running-config	
show startup-config	
	Historique des commandes
	Utilisateurs connectés au commutateur
	Table des adresses MAC

2 Deuxième partie : Configuration de base d'un commutateur

Vous savez maintenant vous connecter à un commutateur, consulter l'aide des commandes et lire la configuration. L'objectif de cette deuxième partie est d'éditer la configuration du commutateur.

2.1 Modes de configuration

Comme vu dans la première partie, l'interface de commande possède différents modes d'exécution. Completez le tableau suivant contenant les modes les plus courants.

Mode	Invite affiché	Commandes d'entrée et de sortie
Exécution utilisateur	`commutateur>`	-
Exécution privilégiée	`commutateur#`	
Configuration globale	`commutateur (config)#`	
Configuration d'interface	`commutateur (config-if)#`	

2.2 Mode Setup

Le mode Setup est un menu interactif permettant la configuration initiale d'un nouveau commutateur, ou d'un commutateur dont la `startup-config` a été effacée.

1. Connectez-vous au commutateur en mode d'exécution privilégiée et consultez le sommaire des interfaces en cours (relevez les interfaces, les adresses IP, leur état).
2. Utilisez la commande `setup` et définissez les paramètres généraux puis d'interface en conservant les options par défaut :
   a. Acceptez d'entrer dans le dialogue de configuration, puis dans la configuration de management
   b. Nommez la machine comme vous le souhaitez
   c. Mot de passe `secret` : polytech
   d. Mot de passe `enable` : cisco *(Le mot de passe secret est plus fort, car chiffré)*
   e. Mot de passe `Terminal virtuel` : polytech
   f. Ne configurez pas le SNMP
   g. Choisissez l'interface `VLAN1` comme interface de management.
   h. Attribuez-lui l'adresse IP 192.168.0.252/24
   i. Répondez `no` à la question sur le clustering de switch.
   j. Enregistrez la configuration.
3. Où a été enregistrée cette nouvelle configuration ? Quelle est la particularité de cette mémoire ?
4. Utilisez la commande `write erase` pour effacer cette configuration, puis reload pour redémarrer.

Tout ce qui apparait dans le mode Setup est réalisable en CLI. Dans les TPs, on évitera de l'utiliser, étant donné qu'il remplace les configurations de démarrage.

3 Troisième partie : Utilisation basique

3.1 Adressage

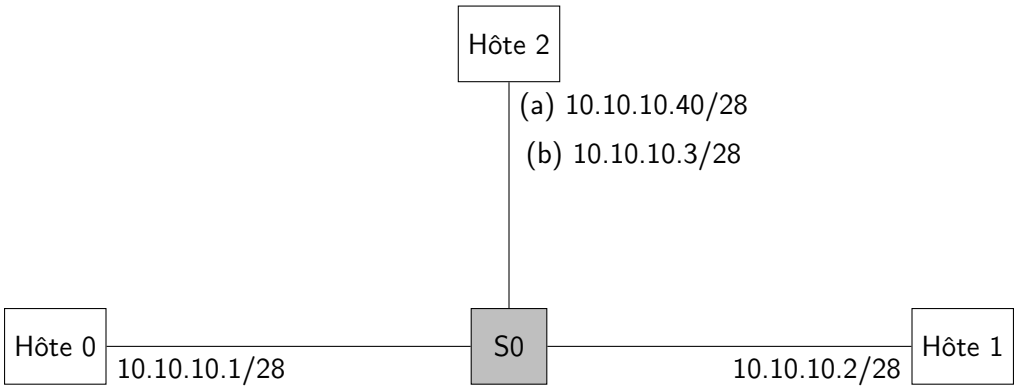


FIGURE 1 – Configuration du commutateur

1. Réalisez le câblage de la maquette présentée à la figure 1 à l'aide de câbles RJ45 droits en utilisant les ports de votre choix.
2. Donnez aux hôtes 0 et 1 les adresses IP indiquées.
3. Donnez à l'hôte 2 l'adresse IP (a) : 10.10.10.40/28.
4. Testez la configuration à l'aide de la commande `ping`. Que constatez-vous ?

5. Affectez à l'hôte 2 l'adresse IP (b) : 10.10.10.3/28. Testez à nouveau la connectivité.
6. Affichez la table des adresses MAC du commutateur 0.
7. Lancez un ping en continu entre l'hôte 1 et l'hôte 0.
8. A l'aide de Wireshark, observez le trafic entrant et sortant sur les trois hôtes. Qu'en déduisez-vous sur le comportement du commutateur ?

3.1.1 Cascade de commutateurs

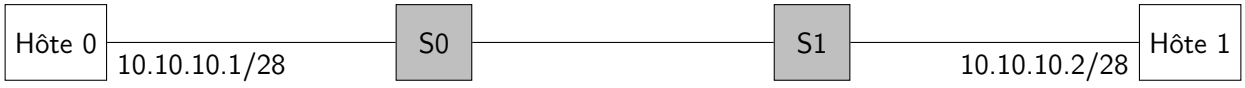


FIGURE 2 – Configuration des commutateurs

1. Réalisez le réseau de la figure 2. Pensez à utiliser des câbles croisés entre le commutateur 0 et le commutateur 1.
2. Testez la connectivité entre l'hôte 0 et l'hôte 1 à l'aide de la commande `ping`.
3. Utilisez la commande `tracert` (Windows) ou `traceroute` (Linux) depuis l'hôte 0 vers l'hôte 1. Qu'en concluez-vous ?

4 Quatrième partie : Les réseaux locaux virtuels (VLAN)

Les réseaux locaux virtuels peuvent être utilisés pour diviser des groupes d'utilisateurs selon les fonctions plutôt que les emplacements physiques. Par défaut, tous les ports d'un commutateur se trouvent dans le même réseau local virtuel. Un administrateur réseau peut créer des réseaux locaux virtuels supplémentaires et transférer des ports dans ces réseaux. Cette opération créé des domaines de diffusion plus petits qui aident à réduire et à circonscrire le trafic réseau.

4.1 Configuration à un seul commutateur

Par défaut, tous les ports du commutateur sont affectés au même domaine de diffusion. L'objectif est de créer un nouveau VLAN pour séparer en deux groupes de travail les étudiants et les enseignants. On décide d'affecter les ports 1 à 4 du commutateur au VLAN étudiants, et les ports 5 à 10 au VLAN enseignants.

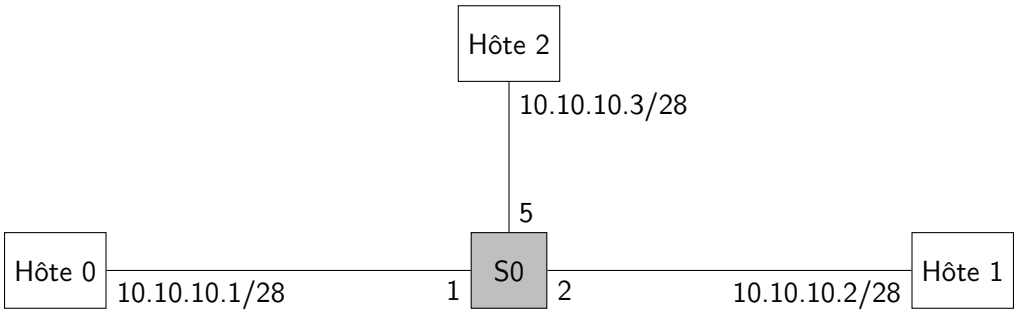


FIGURE 3 – Configuration du commutateur

1. Réalisez le réseau de la figure 3.
2. Observez le trafic entrant avec Wireshark sur tous les hôtes.
3. Réalisez un `ping` vers l'adresse de broadcast du réseau depuis l'hôte 0. Quels hôtes reçoivent les paquets ? Utilisez Wireshark sur les différents hôtes.
4. Connectez-vous au commutateur.
5. À partir du mode de configuration, créez un VLAN 10 avec la commande `vlan`.
6. Vous venez de basculer en mode gestion du VLAN. Nommez le VLAN "students".
7. Revenez au mode de configuration globale.
8. Passez en mode de configuration d'interface pour le port 1.
9. Assurez vous que le port soit en mode `access` à l'aide de la commande `switchport mode access`.
10. Affectez le port au VLAN étudiants en adoptant le mode d'accès statique `switchport access vlan`.
11. Vérifiez à quel VLAN le port 1 est maintenant affecté avec la commande `show vlan`.
12. De la même manière, affectez les ports 2, 3 et 4 au VLAN étudiants. Pour configurer plusieurs éléments, vous pouvez utiliser la syntaxe `interface range Fa0/2 - 4`.
13. De la même manière créez le VLAN "teachers" qui regroupe les ports allant de 5 à 10.
14. Testez la connectivité de l'hôte 0 avec l'hôte 1. Le test a-t-il réussi ? Pourquoi ?

15. Testez la connectivité de l'hôte 0 avec l'hôte 2. Le test a-t-il réussi ? Pourquoi ?
16. Réalisez à nouveau un `ping` en broadcast depuis l'hôte 0. Quels hôtes reçoivent les paquets ?
17. Copiez la configuration active **vers la** configuration de sauvegarde avec la commande `copy running-config startup-config`.
18. Rechargez le commutateur (commande `reload`) puis visualiser le fichier de configuration active pour vérifier la bonne prise en compte des configurations précédemment effectuées.
19. Passez en mode d'exécution privilégié.
20. A l'aide de la commande `write erase`, effacez la configuration initiale.

4.2 Configuration à deux commutateurs en cascade

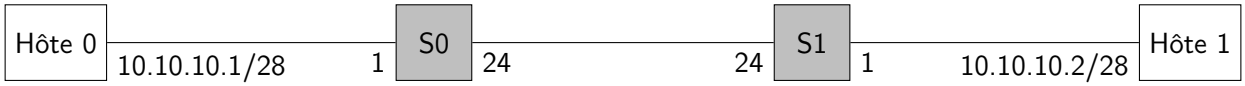


FIGURE 4 – Configuration des commutateurs

1. Redémarrez le commutateur pour revenir à la configuration initiale.
2. Réalisez le câblage de la figure 4. Pensez à utiliser des câbles croisés entre le commutateur 0 et le commutateur 1. Reliez les commutateurs par le port 24.
3. Configurer les deux commutateurs afin d'affecter les ports 1 à 4 au VLAN étudiants, et 5 à 10 au VLAN enseignants.
4. Connectez l'hôte 0 au commutateur 0 par le port 1.
5. Connectez l'hôte 1 au commutateur 1 par le port 1.
6. Testez la connectivité.
7. Connectez l'hôte 0 au commutateur 0 par le port 1.
8. Connectez l'hôte 1 au commutateur 1 par le port 5.
9. Testez la connectivité.

Quand les VLAN sont distribués sur plusieurs commutateurs, il faut mettre en place un étiquetage de trames sur le lien inter-commutateurs. Les trames circulant d'un commutateur à l'autre sont marquées pour que ceux-ci puissent reconnaître le VLAN auxquelles elles appartiennent. Vous allez configurer sur les deux commutateur le port 24 pour qu'il fonctionne en mode étiquetage de trame

10. Passez en mode de configuration d'interface sur le port 24.
11. Assurez vous que le port soit en mode `trunk` à l'aide de la commande `switchport mode trunk`.
12. Faites en sorte que le port autorise les VLANs "students" et "teachers" de manière statique avec la commande `switchport trunk allowed vlan A,B,C`.
13. Vérifiez votre configuration à l'aide de la commande `show interfaces trunk`.
14. Vérifiez que les communications dans les VLANs "students" et "teachers" sont désormais possibles quand les stations de travail sont connectées à des commutateurs différents.

5 Nettoyage

Sur tous vos ordinateurs :

- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions.
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:/vlan.dat`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Travaux pratiques - Architecture des Réseaux

TP 2 - VLAN et Utilisation avancée

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

Ce TP a pour but de vous faire aborder une utilisation plus avancée des VLAN, avec les notions de Trunking, de routage inter-VLAN et de VTP.

Matériel nécessaire

- 2 commutateurs CISCO
- 1 routeur CISCO
- 3 PC sous Windows ou Ubuntu
- 1 câble console

1 Première partie : Rappels sur les réseaux locaux virtuels (VLAN)

Les réseaux locaux virtuels peuvent être utilisés pour diviser des groupes d'utilisateurs selon les fonctions plutôt que les emplacements physiques. Par défaut, tous les ports d'un commutateur se trouvent dans le même réseau local virtuel. Un administrateur réseau peut créer des réseaux locaux virtuels supplémentaires et transférer des ports dans ces réseaux. Cette opération crée des domaines de diffusion plus petits qui aident à réduire et à circonscrire le trafic réseau.

1.1 Déployer des VLANs manuellement

Par défaut, tous les ports du commutateur sont affectés au même domaine de diffusion.

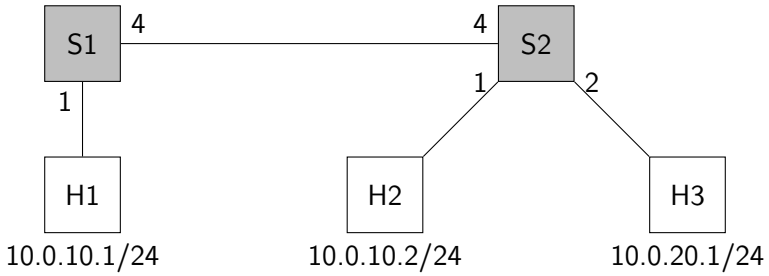


FIGURE 5 – Topologie à déployer

1. Déployez le réseau de la figure 5 en respectant les numéros de port indiqués et l'adressage.
2. H1 peut-il pinger H2 ?
3. Sur le commutateur S1, créez un VLAN 10 "red".
4. Sur le commutateur S2, créez un VLAN 10 "red" et un VLAN 20 "blue".
5. Sur le commutateur S1, configurez les ports en mode access et affectez le VLAN 10 au port 1 et 4.
6. Sur le commutateur S2, configurez les ports en mode access et affectez le VLAN 10 au port 1 et 4, et le 20 au port 2.
7. H1 peut-il pinger H2 ?
8. H2 peut-il pinger H3 ?

1.2 Trunking

Quand les VLAN sont distribués sur plusieurs commutateurs, il faut mettre en place un étiquetage de trames (ou Trunking) sur le lien inter-commutateurs. Les trames circulant d'un commutateur à l'autre sont marquées pour que ceux-ci puissent reconnaître le VLAN auxquelles elles appartiennent. Vous allez configurer sur S1 et S2 le port 4 pour qu'il fonctionne en mode étiquetage de trame.

1. Sur les commutateurs S1 et S2, assurez vous que le port 4 soit en mode `trunk` à l'aide de la commande `switchport mode trunk`.
2. Vous pouvez vérifier l'état des ports avec la commande `show interfaces switchport`.
3. Faites en sorte que le trunk autorise les VLANs "red" et "blue".
4. H1 peut-il pinger H2 ?
5. H3 peut-il pinger H1 et H2 ?

Afin d'éviter les erreurs de configuration sur les ports Trunk, il existe le protocole Dynamic Trunking Protocol (DTP). Il sert à définir automatiquement si le port doit être défini en accès ou en trunk, et quel protocole de trunking utiliser (802.1Q ou ISL, protocole propriétaire Cisco). Les deux modes possibles sont les suivants :

- `dynamic auto` : le port est prêt à négocier un passage en trunk, mais sans requête il restera en accès
- `dynamic desirable` : le port lance des négociations pour un passage en trunk

6. Sur les commutateurs S1 et S2, configurez le port 4 en mode `dynamic auto`. Coupez-le avant d'effectuer la modification. Il se peut que vous ayez besoin de la commande `no switchport nonegotiate`.
7. Si vous l'avez retiré, pensez à ré-autoriser le passage des VLANs sur un éventuel Trunk avec la commande `switchport trunk allowed-vlan 10,20`
8. H1 peut-il pinger H2 ?
9. Sur le commutateur S2, changez le port 4 en mode `dynamic desirable`. H1 peut-il pinger H2 ?
10. Sur le commutateur S1, changez le port 4 en mode `dynamic desirable`. H1 peut-il pinger H2 ?

2 Deuxième partie : Adresse système d'un commutateur

Il est possible d'utiliser les VLAN pour définir une adresse IP pour le commutateur, et en prendre le contrôle à distance.

1. Conservez votre topologie actuelle.
2. Sur le commutateur S1, définissez l'adresse 10.0.10.10/24 sur le VLAN 10.
3. Pouvez vous pinger cette adresse depuis H1 ?
4. Activez le Telnet sur S1, et vérifiez son fonctionnement.
5. Répétez l'opération sur S2 avec l'adresse 10.0.10.20/24 sur le VLAN 10.

3 Troisième partie : Routage Inter-vlan

3.1 Routage Inter-VLAN natif

On souhaite maintenant que les VLANs puissent échanger entre eux. Dans un premier temps, nous allons utiliser le routage natif pour comprendre. Conservez le Trunk dynamique mis en place dans la partie précédente.

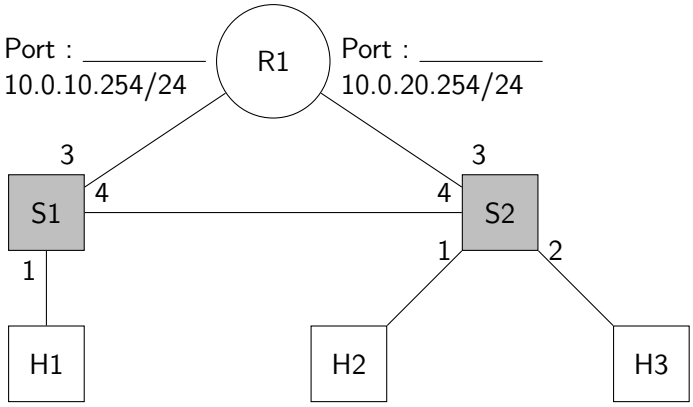


FIGURE 6 – Topologie à déployer

1. Rajoutez le routeur R1 pour obtenir le réseau de la figure 6, et observez sa table de routage. N'oubliez pas de définir des passerelles sur les hôtes.
2. H1 peut-il pinger H3 ? H2 peut-il pinger H3 ?
3. Sur le commutateur S1, configurez le port 3 en mode access et affectez-lui le VLAN 10.
4. Sur le commutateur S2, configurez le port 3 en mode access et affectez-lui le VLAN 20.
5. H1 peut-il pinger H3 ? H2 peut-il pinger H3 ? Expliquez le trajet suivi par les paquets.

3.2 Router-on-a-stick

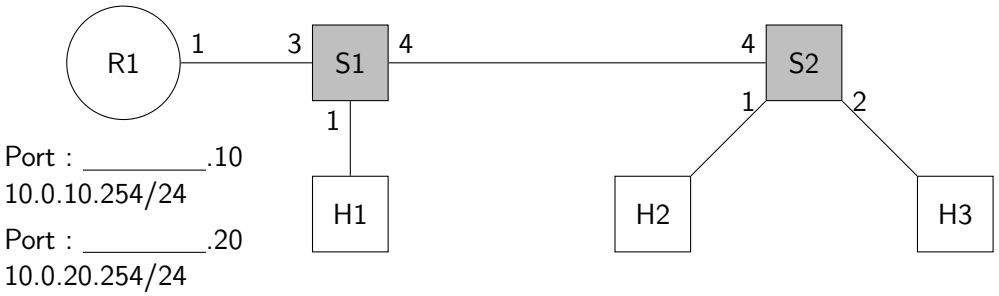


FIGURE 7 – Topologie à déployer

En pratique, on utilise plutôt une technique appelée "Router-on-a-stick".

1. Déconnectez la liaison entre R1 et S2 pour obtenir le réseau indiqué en figure 7.
2. Configurez un trunk dynamique sur la liaison R1-S1, et autorisez les VLANs 10 et 20.
3. Sur le routeur R1, supprimez l'adresse affectée à l'interface 1.
4. Sur le routeur R1, créez des sous interfaces virtuelles .10 et .20, et affectez-y les VLAN 10 et 20, ainsi que la dernière adresse des deux LANs du TP. La syntaxe est la suivante :

```
Router(config)#interface Fa0/0.10
Router(config-int)#encapsulation dot1Q 10
Router(config-int)#ip address ...
```

5. H3 peut-il pinger l'interface virtuelle .20 du routeur R1 ?
6. Dans la partie suivante nous verrons le protocole VTP permettant de propager les VLANs. Pour l'instant, déclarez le VLAN 20 sur S1.
7. H3 peut-il maintenant pinger l'interface virtuelle .20 du routeur R1 ?
8. H1 peut-il pinger H3 ? H2 peut-il pinger H3 ? Expliquez le trajet suivi par le paquet.

4 Quatrième partie : VTP

VLAN Trunking Protocol (VTP) est un protocole propriétaire Cisco qui diffuse les définitions des VLAN sur un LAN. Un équivalent non-propriétaire est le Multiple VLAN Registration Protocol (MVRP).

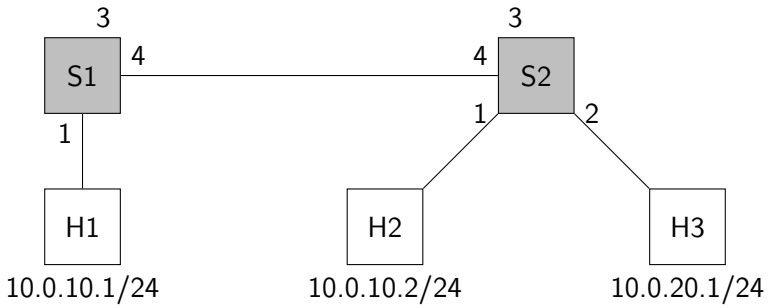


FIGURE 8 – Topologie à déployer

1. Sur S1 et S2, supprimez vos configurations VLAN, et retirez R1 de la topologie pour revenir au réseau de la figure 8.
2. Configurez un trunk dynamique sur la liaison S1-S2, et autorisez les VLANs 10 et 20.
3. Dans la configuration VTP, utilisez "polytech" comme nom de domaine et mot de passe.
4. Configurez S1 pour être client VTP, et S2 pour être serveur VTP.
5. Essayez d'ajouter le VLAN 10 "red" au commutateur S1. Qu'observez-vous ?
6. Ajoutez le VLAN 10 "red" au commutateur S2.
7. À l'aide de la commande `show vlan brief`, observez les VLANs appliqués sur S1 et S2.
8. Configurez maintenant le VLAN 20 "blue".
9. H1 peut-il pinger H2 ?
10. Sur le commutateur S1, affectez le VLAN 10 au port 1.
11. Sur le commutateur S2, affectez le VLAN 10 au port 1, et le 20 au port 2.
12. H1 peut-il pinger H2 ?

5 Partie Bonus : Mode transparent

Cette partie est optionnelle, assurez-vous d'avoir compris le reste du TP au préalable. Il vous faudra un troisième commutateur.

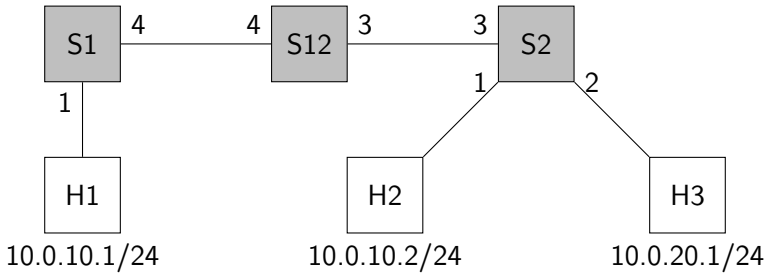


FIGURE 9 – Topologie à déployer

1. Sur S1 et S2, supprimez vos configurations VLAN, y compris le trunk.
2. Déployez la topologie présentée en figure 9.
3. Configurez un trunk dynamique sur les liaison S1-S12 et S12-S2, et autorisez les VLANs 10 et 20.
4. Configurez S1 pour être client VTP, et S2 pour être serveur VTP. Utilisez "polytech" comme nom de domaine VTP, et le mot de passe "polytech".
5. Configurez S12 pour être en mode VTP transparent.
6. Définissez sur S2 les VLAN 10 et 20.
7. Les VLANs sont-ils propagés sur S1 ? Et sur S12 ?
8. Sur le commutateur S1, affectez le VLAN 10 au port 1.
9. Sur le commutateur S2, affectez le VLAN 10 au port 1, et le 20 au port 2.
10. Vérifiez le fonctionnement des pings.

6 Nettoyage

Sur tous vos ordinateurs :

- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions.
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:/vlan.dat`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Travaux pratiques - Architecture des Réseaux

TP 3 - Routeur

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

L'objectif de ce TP est de la prise en main d'un routeur et de son système de configuration.

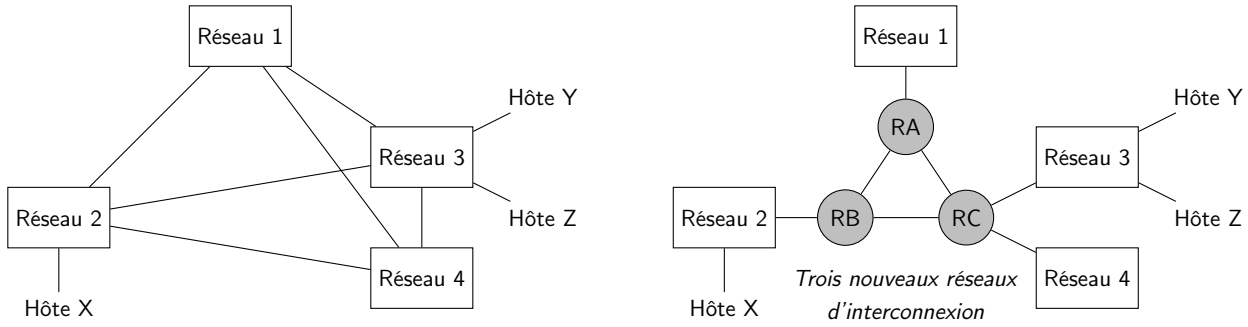
Éléments de cours

On appelle inter-réseau ("Internet") un ensemble de réseaux inter-connectés. On parle de réseau de réseaux. Un inter-réseau regroupe des centaines ou des milliers de machines. Pour que toutes ces unités puissent communiquer de façon efficace, elles doivent obligatoirement s'accorder sur les procédures à mettre en œuvre. Il est effectivement impossible pour un ordinateur particulier de connaître l'adresse personnelle de tous les autres dans l'inter-réseau.

Un mécanisme a donc été mis en œuvre, permettant de réduire au minimum l'information dont chaque ordinateur doit disposer pour communiquer avec les autres. Le procédé adopté consiste à découper un inter-réseau en un grand nombre de réseaux disjoints et inter-connectés. Ceux-ci peuvent d'ailleurs être à leur tour découpés en sous-réseaux. Vous êtes peut-être déjà familiers avec ce concept dans les protocoles IP.

Ce sont les routeurs qui ont pour tâche d'établir le lien entre les réseaux disjoints. Avec cette méthode, un ordinateur particulier se contente d'identifier les divers réseaux de l'inter-réseau, et non plus l'adresse personnelle de chacune des machines qui les compose.

Le message envoyé sur l'inter-réseau atteint un routeur connecté au réseau de destination. La figure 10 illustre un inter-réseau, dans lequel les routeurs sont utilisés pour interconnecter différents numéros de réseaux.



Un inter-réseau **Exemple de connectivité avec trois routeurs**

FIGURE 10 – Inter-connexion de réseaux et de sous-réseaux en un inter-réseau

Matériel nécessaire

- 2 routeur CISCO
- 2 PC sous Windows ou Ubuntu
- 1 câble console pour connecter le port série du PC au port console du routeur

1 Première partie : Vue d'ensemble d'un routeur

Cette première partie a pour objectif de vous apprendre les différentes commandes communes utiles à l'administration d'un routeur.

1. Examinez le routeur (relevez le numéro de modèle, les différents ports, type de câbles ...). À quoi sert le port AUX associé au port console ?
2. Connectez votre station de travail au routeur à l'aide d'un câble console.
3. Il faut identifier le port auquel vous êtes connecté sur l'hôte. Sur Linux, utilisez la commande `cd /dev; ls -ltr *tty*`. Utilisez le nom de l'interface la plus récente.
4. Connectez-vous au routeur à l'aide du programme Putty avec les paramètres suivants :

Port	Valeur relevée au point précédent
Bits par seconde	9600
Bits de données	8
Parité	Aucun
Bits d'arrêt	1
Contrôle de flux	Aucun

5. Lancez la commande `show version`. Quelle est la version de l'IOS ? Quel est le nom du fichier image ? À partir d'où le fichier image a-t-il été lancé ?
6. Testez la commande `show ver`. Que remarquez-vous ?
7. Testez les commandes : `?` et `show ?`. À quoi sert le caractère `?` ?
8. Utilisez la commande `enable` pour passer en mode d'exécution privilégié.
9. Testez à nouveau les commandes : `?` et `show ?`. Que remarquez-vous ?
10. Effectuez les commandes `show running-config` et `show startup-config`
    Sur IOS $\leq$ 12.0, utilisez les commandes `show running` et `show config`.
    Quelle est la différence entre ces deux commandes ?

11. Remplissez le tableau suivant avec les commandes `show` correspondantes :

Commande	**Effet**
show running-config	
show startup-config	
	Historique des commandes
	Adresses et noms d'hôtes contenus en mémoire
	Table ARP du routeur
	Statistiques des interfaces
	État rapide des interfaces IP
	Protocoles configurés sur le routeur

2 Deuxième partie : Configuration de base d'un routeur

Vous savez maintenant vous connecter à un routeur, consulter l'aide des commandes et lire la configuration. L'objectif de cette deuxième partie est d'éditer la configuration du routeur.

2.1 Modes de configuration

Comme vu dans la première partie, l'interface de commande possède différents modes d'exécution.

1. Complétez le tableau suivant contenant les modes les plus courants.

Mode	Invite affiché	Commandes d'entrée et de sortie
Exécution utilisateur	`commutateur>`	-
Exécution privilégiée	`commutateur#`	
Configuration globale	`commutateur (config)#`	
Configuration d'interface	`commutateur (config-if)#`	

2. Passez en mode de configuration globale et modifiez le nom d'hôte du routeur.

2.2 Configuration d'interface

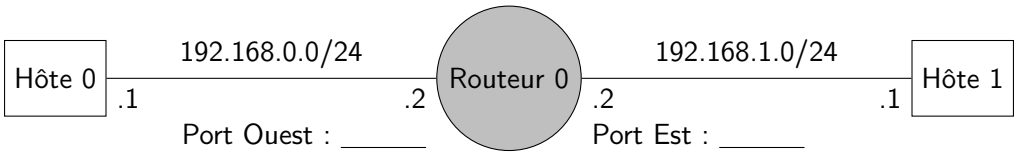


FIGURE 11 – Configuration du routeur

1. Réalisez les connexions indiquées dans la figure 11 à l'aide de câbles Ethernet RJ45 croisés.
2. Connectez vous au routeur à l'aide de l'un des deux hôtes par le port console.
3. Accédez au mode de configuration de l'interface Ouest. Si votre interface est `FastEthernet0`, vous pouvez raccourcir en `Fa0`.
4. Observez les commandes intéressantes à disposition dans ce mode.
5. Entrez une description pour cette interface.
6. Configurez l'adresse IP pour l'interface Ouest avec la commande `ip address`. Utilisez l'adresse IP et le masque de sous-réseau indiqués sur la figure 11.
7. Activez le routage à l'aide de la commande `ip routing`.
8. Testez la connectivité de la couche 3 : envoyez une requête `ping` vers l'interface Ouest depuis l'hôte 0.
9. Revenez au mode de configuration global.
10. Comparez les fichiers de configuration et de sauvegarde.
11. Copiez la configuration active **vers la** configuration de sauvegarde avec la commande `copy running-config startup-config`.
12. Rechargez le routeur (commande `reload`) puis visualiser le fichier de configuration active pour vérifier la bonne prise en compte des configurations précédemment effectuées.
13. Répétez les opérations pour l'interface Est.
14. Testez la connectivité globale : envoyez une requête `ping` vers l'hôte 1 depuis l'hôte 0. Vérifier la bonne émission et réception des paquets du `ping` avec Wireshark.
15. Affichez la table des routes avec la commande `show ip route`. Quelles routes observez-vous ?
16. Laissez la configuration telle quelle pour la suite.

2.3 Configuration du protocole Telnet

Vous contrôlez actuellement le routeur par son port console. C'est un accès nécessaire à la mise en place d'un équipement. Dans cette partie nous allons voir comment configurer un accès distant à l'équipement. Pour le login et mot de passe utilisez (polytech, polytech).

1. Assurez vous que le routeur est toujours dans la configuration précédente.
2. Configurez un mot de passe sur l'environnement d'exécution privilégié. Aucun accès distant ne peut être configuré sans cette étape.
3. Configurez l'accès Telnet.
4. Utilisez l'un des hôtes pour vous connecter au routeur à l'aide de Putty.

Note : Telnet est un protocole non-sécurisé. Le protocole SSH est plus généralement utilisé, avec du chiffrement. Dans le cadre des TPs, on utilisera Telnet pour sa simplicité.

3 Troisième partie : Configuration du routage

L'objectif de cette section est d'apprendre à configurer une route statique puis du routage dynamique avec le protocole RIP.

3.1 Mise en place

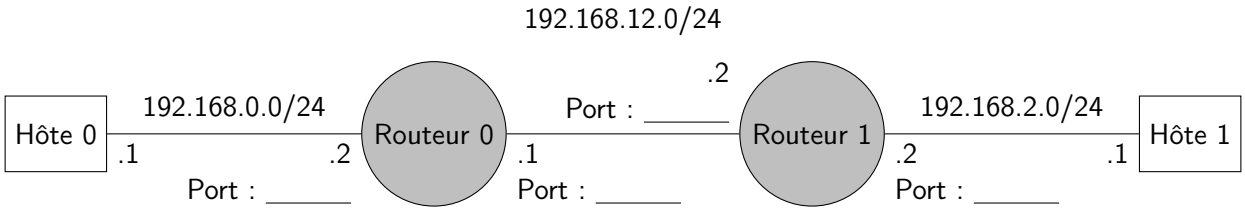


FIGURE 12 – Configuration des routeurs

1. Passez en mode d'exécution privilégié.
2. A l'aide de la commande `write erase`, effacez la configuration initiale.
3. Redémarrez les routeurs (sans sauvegarder la configuration `running-config`) pour revenir à une configuration vierge.
4. Activez le routage à l'aide de la commande `ip routing`.
5. De la même manière que dans la partie précédente, réalisez les connexions indiquées dans la figure 12 à l'aide de câbles Ethernet RJ45 croisés.
6. Pour vous faciliter la suite, renommez les routeurs.
7. Testez la connectivité entre le routeur 0 et le routeur 1.
8. Testez la connectivité entre l'hôte 0 et l'hôte 1. Que remarquez-vous (utilisez Wireshark sur les deux hôtes) ? Expliquez à l'aide des tables de routage du routeur 0 et du routeur 1.

3.2 Configuration d'une route statique

1. Connectez vous sur le routeur 0.
2. Passez en mode de configuration globale et étudiez les possibilités de la commande `ip route`.
3. Entrez une route statique vers l'hôte 1.
4. Testez la connectivité entre l'hôte 0 et l'hôte 1 à l'aide d'un `ping`. Que se passe-t-il ? Que remarquez vous avec Wireshark sur l'hôte 0 ? Sur l'hôte 1 ? Cela est-il normal ?

5. Connectez vous sur le routeur 1.
6. Passez en mode de configuration globale et étudiez les possibilités de la commande `ip route`.
7. Entrez une route statique vers l'hôte 0.
8. Testez à nouveau la connectivité entre l'hôte 0 et l'hôte 1 à l'aide d'un `ping`.

3.3 Configuration du protocole RIP

1. Supprimez les routes statiques à l'aide de la commande `no ip route`
2. Vérifiez que seules les routes directement connectées apparaissent dans les tables de routage du routeur 0 et du routeur 1.
3. Passez en mode de configuration globale et activez le protocole de routage RIP (un nouvel invite s'affiche).
4. Déclarez les réseaux connus du routeur qui doivent participer au protocole. De quels réseaux s'agit-il pour le routeur 0 ? Et pour le routeur 1 ?
5. Affichez les protocoles IP. Quelle est la date de la prochaine mise à jour ?
6. Affichez la base de données du protocole RIP.
7. Affichez la table de routage. Combien de routes ont été découvertes par le protocole IP ?
8. Testez à nouveau la connectivité entre l'hôte 0 et l'hôte 1 à l'aide d'un `ping`.
9. À l'aide de Wireshark, observez les échanges RIP qui parviennent aux hôtes.
10. Modifiez la configuration du routeur 1 pour qu'il utilise RIP en version 2.
11. À l'aide de Wireshark, observez à nouveau les échanges RIP réguliers entre les équipements. Que remarquez-vous ? Quelle différence observez-vous entre les paquets RIP version 1 et 2 ?
12. Redémarrez les routeurs pour recharger la configuration initiale. N'enregistrez pas vos modifications.

4 Partie Bonus : Configuration SSH

Cette partie est optionnelle, assurez-vous d'avoir compris le reste du TP au préalable.

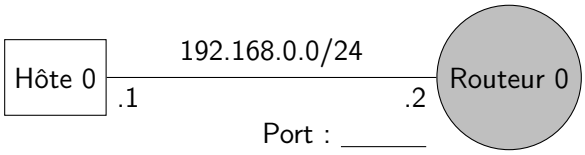


FIGURE 13 – Configuration du routeur

1. Réalisez les connexions indiquées dans la figure 13 à l'aide de câbles Ethernet RJ45 croisés.
2. Connectez vous au routeur à l'aide de l'hôte en Telnet, et observez des échanges avec Wireshark. (par exemple, changez le nom d'hôte du routeur).
3. Assurez-vous d'avoir paramétré un nom d'hôte au routeur.
4. En mode de configuration privilégié, configurez le nom de domaine avec la commande `ip domain-name`.
5. Utilisez la commande `crypto key generate rsa` pour générer une clé RSA modulo 1024.
6. Configurez maintenant l'accès SSH à l'aide des lignes suivantes :
   a. `username admin privilege 15 secret Cisco1`
   b. `line vty 0 4`
   c. `login local`
   d. `transport input ssh`
7. Connectez-vous en SSH vers le routeur, et observez à nouveau les échanges avec Wireshark. Que remarquez-vous ?

5 Nettoyage

Sur tous vos ordinateurs :

- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Travaux pratiques - Architecture des Réseaux

TP 4 - Routage et convergence

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

L'objectif de ce TP est d'approfondir vos connaissances sur les routeurs, et en particulier sur les protocoles de routage RIP et OSPF. À la fin de ce TP vous serez capable de mettre en place un petit réseau de routeurs opérant un routage dynamique.

Organisation du TP

Pour ce TP, vous partagerez la topologie entre 2 groupes. Vous aurez besoin du matériel suivant :

- 2 commutateurs CISCO
- 4 routeurs CISCO
- 4 PC sous Windows ou Ubuntu
- 2 câbles console

Le groupe A aura sous sa responsabilité :

- Les routeurs R1 et R2
- Les hôtes H1 et H2
- Le commutateur SA

Le groupe B aura sous sa responsabilité :

- Les routeurs R3 et R4
- Les hôtes H3 et H4
- Le commutateur SB

1 Première partie : Mise en place du réseau

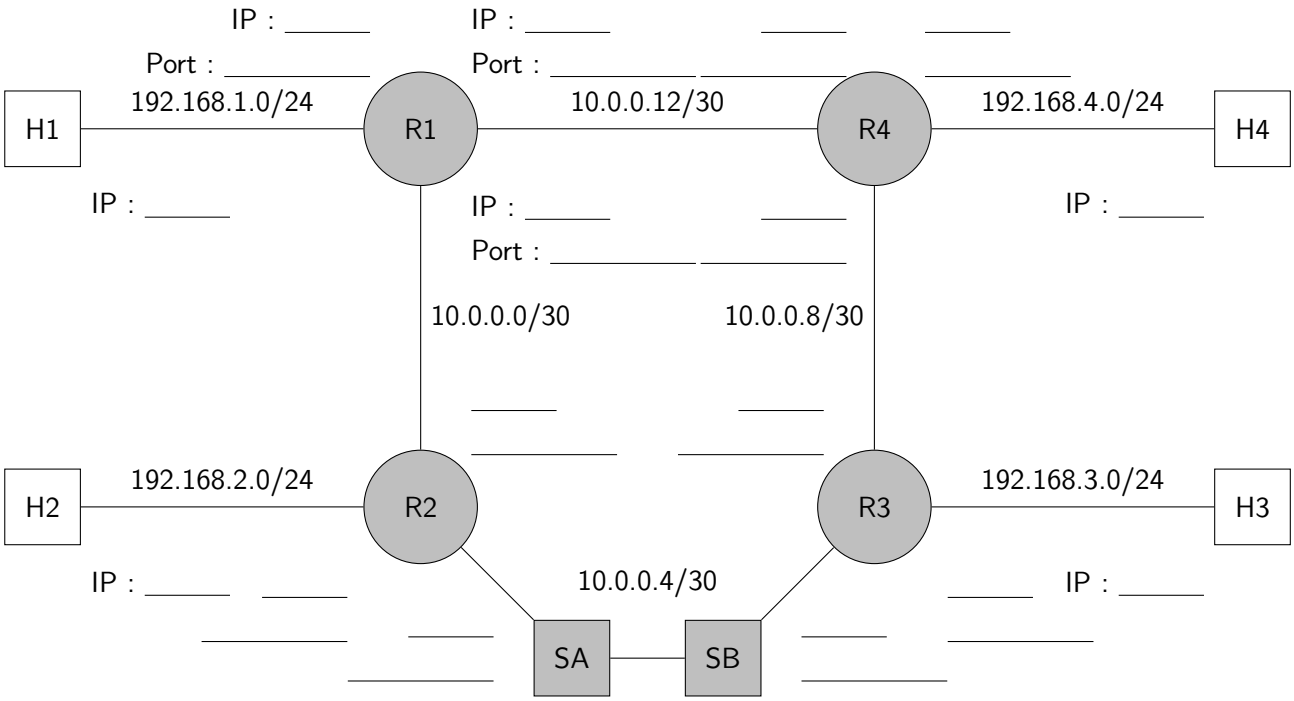


FIGURE 14 – Topologie du réseau

1. Complétez le plan avec les adresses et les ports que vous allez utiliser.
2. Déployez le réseau présenté en Fig. 14.
   a. R1, R2, R3 et R4 : routeurs possédant au moins trois ports
   b. SA et SB : commutateurs sans configuration particulière
   c. H1, H2, H3 et H4 : hôtes avec adresse IP statique
3. Quels équipements avez-vous choisi ?
4. Que pouvez-vous dire de la connectivité entre routeurs voisins ?
5. Que pouvez-vous dire de la connectivité entre les réseaux locaux ?

2 Deuxième partie : Routage dynamique RIP

1. Configurez le routage dynamique RIPv2 sur toutes vos interfaces.
2. Observez votre configuration courante, que remarquez-vous ?
3. Contrôlez la connectivité globale.
4. À l'aide de Wireshark, observez les échanges RIP réguliers qui parviennent sur les hôtes. La récapitulation de réseau privé en configuration que vous avez relevé plus haut empêche-t-il le bon fonctionnement du protocole ?
5. En mode d'exécution privilégié, activez le debug RIP sur R1 et R4. Attendez la prochaine annonce RIP. Qu'observez-vous ?
6. Par mesure de sécurité, vous désirez déclarer les réseaux locaux mais ne pas envoyer de message RIP sur ces interfaces. Pour cela, il est possible de déclarer une interface *passive*. Réalisez la configuration correspondante sur les LAN 1 et 4.
7. À l'aide de Wireshark, contrôlez qu'aucun message RIP n'est envoyé sur les LAN.
8. Vous allez maintenant tester l'efficacité de RIP :
   a. Notez la table de routage des routeurs R1 et R4.
   b. Effectuez une requête ping continue de l'hôte H1 vers H4, et de l'hôte H4 vers H1.
   Utilisez l'option "-t" de la commande ping.
   c. **Préparez-vous** à couper le lien R1-R4 en déconnectant le câble.
   d. Vous allez observer le debug RIP sur R1 et R4. Observez également le temps de rétablissement des pings.
   e. Coupez le lien R1-R4.
   f. À quoi est dû le délai de rétablissement du ping ? Comment appelle-t-on ce temps ?
   g. Observez à nouveau la table de routage de vos routeurs.
   h. Rétablissez le lien et observez.
   i. Répétez la panne 3 fois, et notez les temps de panne observés.

3 Troisième partie : Routage dynamique OSPF

OSPF se configure en aires. Les aires les plus grandes peuvent supporter près de 200 routeurs (sur les Cisco 2600 Series pas plus de 40). Dans ce TP, on utilisera une seule aire, l'aire 0.

1. Désactivez le routage RIP sur tous les routeurs.
2. Configurez le protocole OSPF pour qu'il annonce tous les réseaux. Vous aurez besoin d'utiliser les masques génériques (rappels en Annexe).
3. Quels éléments de configuration vous ont été utiles ?
4. Observez les contiguïtés établies avec la commande `show ip ospf neighbor`.
5. Contrôlez la connectivité globale.
6. De manière similaire à RIP, il est important de configurer les interfaces LAN en mode passif. En effet, dans les protocoles à état de lien, on annonce l'intégralité des réseaux connus ! Configurez l'interface vers les LAN 1 et 4 en mode passif et contrôlez le bon fonctionnement.
7. En mode d'exécution privilégié, activez et observez le debug OSPF sur la Routing Information Base (RIB) sur R1 et R4.
8. Comme précédemment, vous allez tester l'efficacité d'OSPF.
    a. Notez la table de routage des routeurs R1 et R4.
    b. Effectuez une requête ping continue de l'hôte H1 vers H4 et de l'hôte H4 vers H1.
    c. Coupez le lien R1-R4. Observez et expliquez comme précédemment.
    d. Observez à nouveau la table de routage de votre routeur.
    e. Rétablissez le lien et observez à nouveau.
    f. Répétez la panne 3 fois, et notez les temps de panne observés.
    g. Que pouvez-vous dire des performances d'OSPF par rapport à RIP ?

Le protocole OSPF se base sur la perte de signal sur son port pour détecter rapidement la coupure.

9. Effectuez une requête ping continue de l'hôte H2 vers H3 et de l'hôte H3 vers H2.
10. Effectuez une coupure entre les commutateurs SA et SB.
11. Quelle différence observez-vous ?
12. Par quel mécanisme le protocole OSPF s'aperçoit-il de la coupure ?
13. Dans ce cas, peut-on accélérer la convergence ?
14. Y a-t-il un risque ?

Annexe : Masques génériques (Wildcard)

OSPF, ainsi que d'autres protocoles, utilisent des masques génériques ou "wildcards" plutôt que des masques IP usuels.

3.1 Cas simples

Dans les cas simple que nous allons rencontrer, il est difficile de comprendre pourquoi les masques génériques existent, et pourquoi ils se calculent de manière complexe. Pour l'instant, vous devez retenir que le masque générique se calcule comme complément du masque pour les cas que nous allons rencontrer.

Par exemple :

1. 192.168.0.0 255.255.255.0 → 0.0.0.255
2. 10.4.4.0 255.255.255.252 → 0.0.0.3
3. 172.0.0.0 255.0.0.0 → 0.255.255.255
4. Un hôte 192.168.0.1 255.255.255.255 → 0.0.0.0

3.2 But des masques génériques

En réalité, le masque générique permet de filtrer beaucoup plus finement les adresses que par hôte ou par sous-réseau. Pour le calculer, il faut repasser en binaire. Chaque bit de valeur 0 correspond à une valeur fixe sur l'adresse. Tous les autres bits (valeur 1) peuvent varier.

Par exemple dans l'un des cas précédents : 192.168.0.0 255.255.255.0. On souhaite ici que les trois premiers octets soient figés. On a alors le masque générique :
0000 0000.0000 0000.0000 0000.1111 1111 soit 0.0.0.255. Dans ce cas, le calcul correspond au complément du masque.

Prenons un exemple plus complexe : on souhaite noter toutes les adresses en 192.168.0.0/16 dont le troisième octet est toujours impair. Il est impossible de noter cet ensemble avec un masque classique. Par exemple la notation 192.168.1.0/16 est une erreur. Essayons alors d'écrire un masque générique correspondant à ces critères.

Pour obtenir un octet impair, il faut que le dernier bit ait pour valeur 1, et soit invariant. Tous les autres bits peuvent varier. On peut alors écrire le masque :
0000 0000.0000 0000.1111 1110.1111 1111 ce qui donne la notation 192.168.1.0 0.0.254.255

Un autre exemple, si l'on souhaite noter toutes les adresses du sous-réseau 192.168.1.0/24 dont le dernier octet est supérieur à 2. C'est-à-dire la plage 192.168.0.2-192.168.0.255. La notation avec masque générique correspondante est
192.168.0.2 0000 0000.0000 0000.0000 0000.1111 1101 soit 192.168.0.2 0.0.0.253.

4 Nettoyage

Sur tous vos ordinateurs :

- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions.
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:/vlan.dat`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Travaux pratiques - Architecture des Réseaux

TP 5 - Redondances LAN

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

Organisation du TP

Ce TP est divisé en trois parties indépendantes :

1. Redondance de commutateur et STP (1h)
2. Redondance de lien : LAG (1h)
3. Redondance de passerelle : HSRP (2h)

Étant donné que nous sommes limités en matériel, la moitié des groupes commencera par les partie 1 et 2, l'autre moitié par la partie 3.

Pour les parties 1 et 2, vous aurez besoin du matériel suivant :

- 3 commutateurs CISCO
- 3 PC sous Windows ou Ubuntu
- 1 câble console

Pour la partie 3, vous aurez besoin du matériel suivant :

- 3 routeurs CISCO
- 2 commutateurs CISCO
- 2 PC sous Windows ou Ubuntu
- 1 câble console

1 Redondance de commutateur et STP (1h)

Le protocole Spanning-Tree est un indispensable des réseaux LAN, pour assurer une redondance de chemins niveau 2 tout en évitant (entre autres) les tempêtes de diffusion.

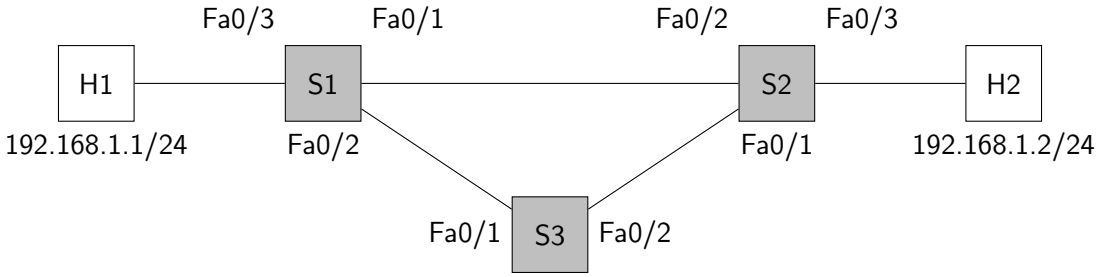


FIGURE 15 – Topologie du réseau

1. Déployez le réseau de la Fig. 15.
2. Vérifiez la connectivité.
3. Utilisez la commande `show interfaces` sur les différents ports des différents commutateurs pour essayer de comprendre par où est diffusé le trafic grâce aux compteurs de paquets.
4. Avec la commande `show spanning-tree` observez l'état des différents ports.
5. Observez les LEDs des différents ports. Notez leur état.
6. Que pouvez-vous dire du protocole STP sur des équipements Cisco vierges ? D'après vous, pourquoi ?

7. Lancez un ping continu entre H1 et H2.
8. Supprimez le lien par lequel passait le ping.
9. Combien de temps faut-il avant que le ping ne se rétablisse ?
10. Observez à nouveau l'état des différents ports ainsi que les LEDs.
11. À quoi est du le temps de rétablissement ?
12. En théorie, il est possible de réduire ce temps. Quels éléments du protocole STP pourriez-vous modifier pour réduire le temps de rétablissement ? Quels peuvent être les risques associés à ces modifications ?

2 Redondance de lien : LAG (1h)

Dans cette première partie, vous allez utiliser le protocole LACP pour l'aggrégation de lien.

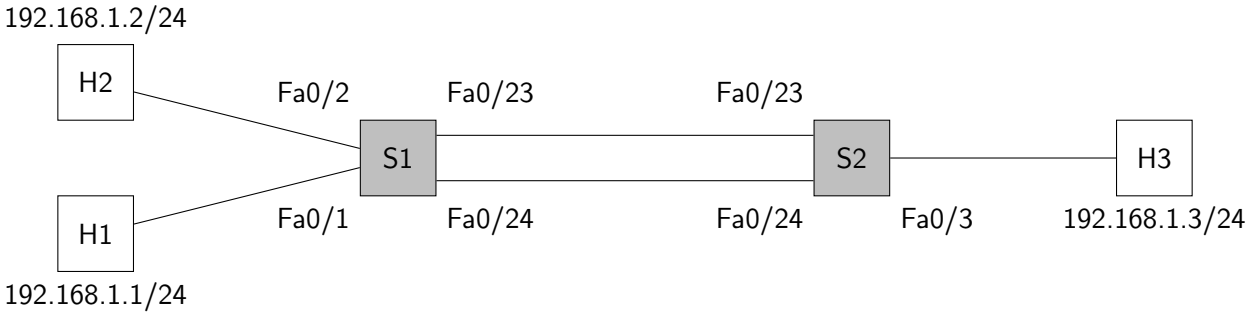


FIGURE 16 – Topologie du réseau

1. Déployez le réseau de la Fig. 16 et vérifiez la connectivité.
2. Utilisez la commande `show interfaces status`. Qu'observez-vous ?
   Consignez le nombre d'interfaces affichées.
3. Utilisez la commande `show etherchannel summary`. Qu'observez-vous ?
4. Que pouvez-vous dire de l'état du protocole STP dans cette situation ?

5. En mode de configuration d'interface, utilisez la commande `channel-protocol` pour configurer les interfaces de S1 et S2 pour qu'elles utilisent le protocole LACP.
6. En mode de configuration d'interface, utilisez la commande `channel-group` pour configurer les interfaces de S1 vers S2 en mode actif sur le groupe 1.
7. Configurez maintenant les interfaces de S2 vers S1 en mode passif sur le groupe 1.
8. Vérifiez la connectivité.
9. Utilisez à nouveau la commande `show etherchannel summary`. Qu'observez-vous ?
10. Utilisez à nouveau la commande `show interfaces status`. Qu'observez-vous ?
11. Rendez-vous en mode de configuration d'interface sur la nouvelle interface.
    Observez les commandes de configuration disponibles. Qu'en concluez-vous ?

12. Effectuez un ping continu de H1 vers H3. Utilisez plusieurs la commande `show interfaces` sur le port Fa0/23 et Fa0/24 du commutateur S1, et observez le nombre de paquets transmis. Quel est le port par lequel est transmis le ping ?
13. Effectuez la même opération pour un ping continu de H2 vers H3.
14. En mode de configuration globale, à quoi sert la commande `port-channel load-balance` ?
15. Configurez le load-balancing sur l'adresse IP source. Observez à nouveau successivement les pings continus. Que pouvez-vous dire des ports physiques de sortie utilisés ?

16. Lancez maintenant vos pings continus simultanément. Supprimez de la topologie l'une des deux liaisons entre S1 et S2. Qu'observez-vous ?

3 Redondance de passerelle : HSRP (2h)

Hot Standby Router Protocol (HSRP) est un protocole propriétaire de Cisco implémenté sur les routeurs et les commutateurs de niveau 3 permettant une continuité de service. Son équivalent non-propriétaire est le Virtual Router Redundancy Protocol (VRRP), défini dans la RFC 5789. HSRP est principalement utilisé pour assurer la disponibilité de la passerelle par défaut. Le principe est de définir la passerelle pour les hôtes du réseau comme étant une adresse virtuelle référençant un groupe de routeurs.

Les routeurs participants à HSRP appartiennent à un groupe, et l'un d'entre eux (dont la priorité est plus élevée) est élu "actif". C'est lui qui servira de passerelle, en affichant les adresses IP et MAC virtuelles du groupe. Des messages "Hello" périodiques permettent aux différents routeurs de détecter une défaillance du routeur actif, et d'activer le suivant dans l'ordre de priorité.

3.1 Configuration initiale

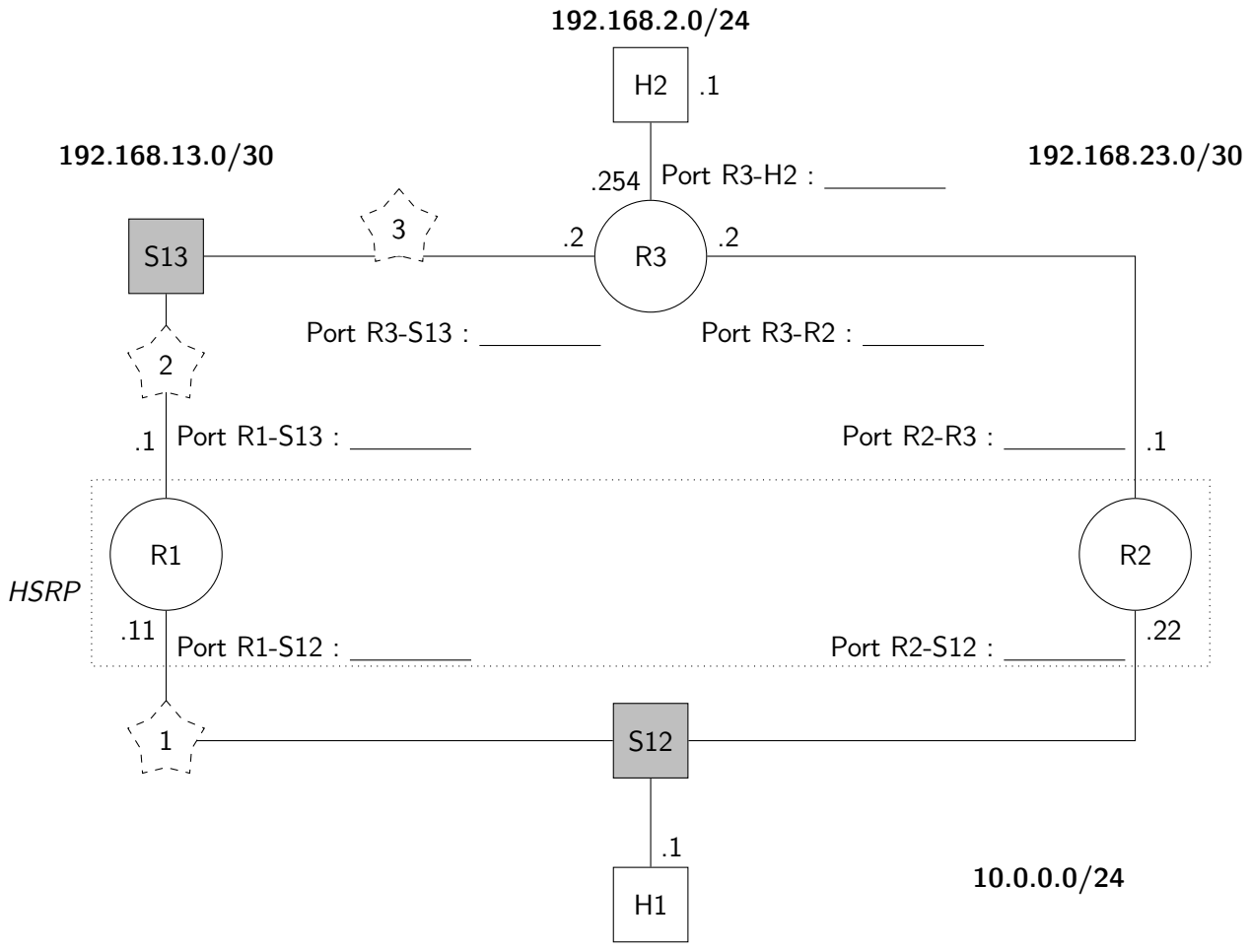


FIGURE 17 – Topologie du réseau

1. Mettez en place le réseau présenté sur la Fig. 17 avec un routage dynamique OSPF. Utilisez un câble croisé entre R2 et R3. Les étoiles représentent les pannes de la suite du sujet.
   Pour rappel, vous devez déclarer les réseaux connectés à un routeur participant au protocole OSPF. Vous devez également définir les interfaces vers les LAN en `passive-interface`. Vous trouverez ci-dessous les modèles de configuration pour R1, R2 et R3. Remplacez les valeurs entre crochets par le nom du port que vous avez utilisé.

Configuration R1

```
hostname R1
ip classless
ip routing
!
interface [R1-S12]
 ip address 10.0.0.11 255.255.255.0
 no shutdown
!
interface [R1-S13]
 ip address 192.168.13.1 255.255.255.252
 no shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface [R1-S12]
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.13.0 0.0.0.3 area 0
```

Configuration R2

```
hostname R2
ip classless
ip routing
!
interface [R2-S12]
 ip address 10.0.0.22 255.255.255.0
 no shutdown
!
interface [R2-R3]
 ip address 192.168.23.1 255.255.255.252
 no shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface [R2-S12]
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.23.0 0.0.0.3 area 0
```

Configuration R3

```
hostname R3
ip classless
ip routing
!
interface [R3-H2]
 ip address 192.168.2.254 255.255.255.0
 no shutdown
!
interface [R3-S13]
 ip address 192.168.13.2 255.255.255.252
 no shutdown
!
interface [R3-R2]
 ip address 192.168.23.2 255.255.255.252
 no shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface [R3-H2]
 network 192.168.13.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
 network 192.168.2.0 0.0.0.255 area 0
```

2. Configurez l'adresse de passerelle sur H2 : 192.168.2.254/24.
3. Configurez l'adresse de passerelle sur H1 : 10.0.0.254/24.
4. Lancez un ping continu entre H1 et H2, vous aurez à l'observer plus loin.
5. Configurez HSRP sur les interfaces LAN de R1 et R2. Utilisez l'adresse virtuelle 10.0.0.254/24. Définissez la priorité de R1 sur 110, et R2 sur 105.
6. Sur les interfaces participant au protocole HSRP, rajoutez la commande `standby preempt`.
7. Le ping fonctionne-t-il ?
8. Quelle commande utilisez-vous pour vérifier l'état du protocole ?
9. Utilisez la commande `tracert` sous Windows, `traceroute` sous Linux entre H1 et H2. Qu'observez-vous ?
10. Vous allez créer une panne en position 1. Pour cela, vous allez retirez le câble de la topologie, et observer votre ping continu. Que remarquez-vous ?
11. Rebranchez le câble, et attendez la convergence des différents protocoles.
12. Créez maintenant des pannes en position 2 puis 3. Qu'observez-vous ?

3.2 Notion de *tracking*

Le routeur actif est défini par sa valeur de priorité. Il est possible de définir des observateurs d'évènements qui vont modifier cette valeur. On parle de "tracking". On définit généralement un observateur, et une réaction associée : incrémenter la priorité, diminuer la priorité...

1. Lancez un ping continu entre H1 et H2, vous aurez à l'observer plus loin.
2. En mode de configuration globale, créez un objet de tracking "1" à l'aide de la commande `track` qui surveille l'état (`line-protocol`) de l'interface de R1 vers S13.
3. Ajoutez à la configuration HSRP de l'interface une commande `standby tracking` pour que le protocole réagisse à l'objet.
4. Créez des pannes en position 2 puis 3. Qu'observez-vous sur votre ping continu ? Qu'observez-vous sur l'état du protocole sur R1 et R2 ?
5. Créez maintenant un objet `track 2` sur la route de R1 vers le réseau 192.168.2.0/24, et ajoutez-le à la configuration HSRP.
6. Créez une panne en position 3. Qu'observez-vous sur l'état du protocole sur R1 et R2 ?

POLYTECH NANCY

4 Nettoyage

Sur tous vos ordinateurs :

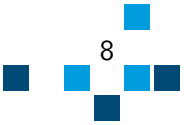
- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions.
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:/vlan.dat`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse



Travaux pratiques - Contrôle d'accès

TP - DHCP, NAT et Syslog

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

Éléments de cours

Le protocole Dynamic Host Configuration Protocol (DHCP - RFC 2132) permet d'attribuer dynamiquement des adresses IP à des hôtes. Il permet également de configurer d'autres paramètres des hôtes passerelle, DNS, proxy...

Le protocole Network Address Translation (NAT - RFC 2663) est une méthode qui permet de faire correspondre des adresses IP à d'autres adresses. Généralement, le protocole NAT est utilisé pour permettre à des réseaux privés de communiquer avec Internet, en translatant les adresses IP internes en adresse IP publique associée à un port.

Sur un LAN connecté à Internet, on trouvera généralement une association des protocoles DHCP et NAT au niveau de la passerelle. Étant donné qu'il s'agit du point d'entrée et de sortie du réseau, il est important de superviser le déroulement de ces protocoles. Pour cela, différentes méthodes existent, notamment le Syslog.

Syslog est un standard (RFC 5424) pour l'envoi et la réception de messages d'enregistrement d'évènements. Grâce au Syslog, un équipement peut émettre des messages à chaque évènement vers un serveur qui les enregistre. Le serveur peut alors les analyser et au besoin émettre des alertes. Les messages syslog contiennent un champ "Facility" qui indique le type et un niveau de sévérité.

Dans ce TP, vous allez mettre en place les protocoles DHCP et NAT puis les superviser avec le protocole Syslog.

Matériel nécessaire

- 2 routeurs CISCO
- 1 commutateurs CISCO
- 3 PC sous Windows ou Ubuntu dont 1 hôte HS sur lequel est installé Rsyslog
- 1 câble console

Partie préliminaire : Topologie

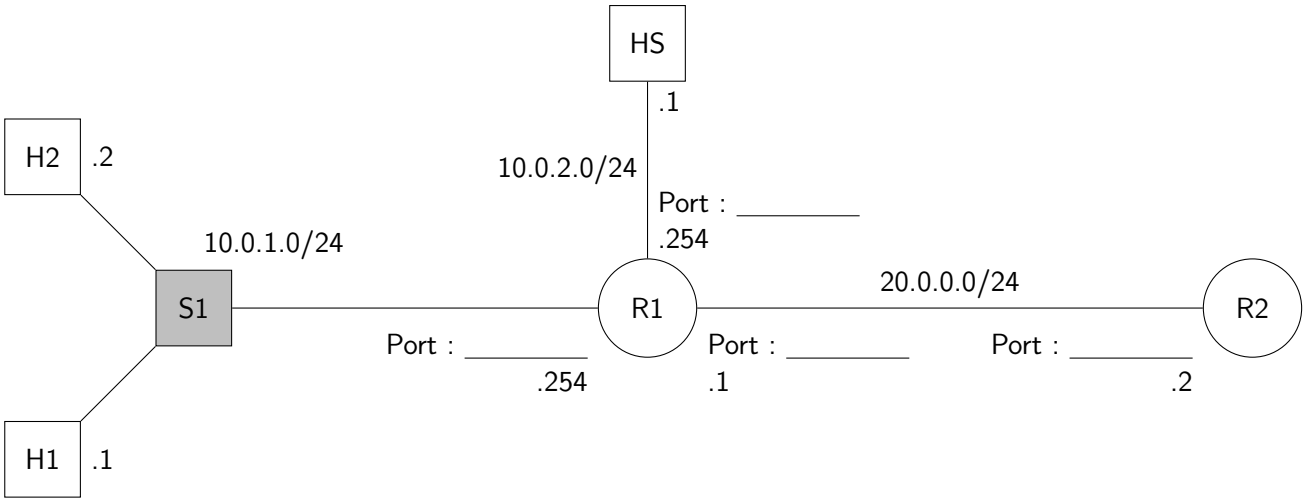


FIGURE 18 – Topologie du réseau

1. Complétez le plan avec les ports que vous allez utiliser. Si nécessaire, utilisez une liaison série entre les routeurs R1 et R2. Pensez à configurer le *clockrate* sur l'interface série maître.
2. Déployez le réseau présenté en Fig. 18.
3. Pour l'instant, vérifiez simplement que R1 peut contacter les autres éléments de la topologie. Ne configurez pas de routage.

1 Première Partie : DHCP

1. Sur votre routeur R1, créez un pool IP DHCP que vous nommerez "LAN".
2. Faites en sorte que votre pool distribue des adresses IP dans le sous-réseau 10.0.1.0/24.
3. Configurez l'adresse de passerelle (route par défaut) distribuée par le DHCP.
4. Vérifiez que les hôtes H1 et H2 sont configurés pour recevoir une configuration via DHCP. Si besoin, redémarrez les interfaces réseau.
5. Quelles adresses reçoivent les hôtes H1 et H2 ?
6. Qu'observez-vous à l'aide de la commande `show ip dhcp binding` ?
7. À qui appartiennent les adresses ?

8. Vous allez maintenant attribuer un bail statique à l'hôte H1.
   - Coupez l'interface vers le LAN.
   - Nettoyez les baux DHCP en mode `enable` à l'aide la commande `clear ip dhcp binding *`
   - Créez un nouveau pool IP DHCP "LAN_H1".
   - Relevez l'adresse MAC de l'hôte H1.
   - Attribuez l'adresse d'hôte 10.0.1.1 et définissez l'adresse de H1 comme `hardware-address`.
   - Rallumez l'interface vers le LAN.
9. Renouvelez le bail DHCP sur H1, et vérifiez l'adresse obtenue. Si besoin, redémarrez l'interface réseau.

2 Deuxième Partie : NAT

Un opérateur Internet ne propage jamais les routes vers les réseaux locaux. Vérifiez que les paquets de H1 et H2 atteignent R2, mais que la réponse n'est pas transmise. Dans un cas réel, les requêtes du LAN avec des adresses privées seraient abandonnées. C'est pourquoi nous allons mettre en place le protocole NAT, afin que les requêtes transitent en dehors du LAN avec une adresse publique.

1. Sur l'interface externe de R1, spécifiez l'activation du NAT IP extérieur.
2. Sur l'interface interne de R1, spécifiez l'activation du NAT IP interieur.
3. Créez une liste d'accès 10 qui identifie tout trafic avec la commande :

```
access-list 10 permit any
```

4. À l'aide d'une seule commande, configurez le NAT IP intérieur pour utiliser la liste 10 comme source, et l'interface de sortie de R1. Utilisez l'option `overload` pour permettre au NAT de faire correspondre plusieurs adresses à son adresse publique.
5. H1 et H2 peuvent-ils joindre R2 ?
6. Qu'observez-vous à l'aide de la commande *show ip nat translation* ?

Pour vérifier le comportement du NAT, vous allez effectuer une capture sur l'interface de R2. Vous auriez pu rajouter un hôte et utiliser Wireshark, mais cela permet d'économiser du matériel et de vous faire tester de nouvelles commandes.

7. Créez un buffer de capture et associez-le à une interface à l'aide des commandes suivantes :

```
ip access-list extended FILTER
  permit ip any any
monitor capture buffer BUF size 2048 max-size 1518 linear
monitor capture buffer BUF filter access-list FILTER
monitor capture point ip cef POINT gi0/0/0 both
monitor capture point associate POINT BUF
```

8. Sur R2, en mode enable, lancez une capture de paquet avec la commande `monitor capture start`.
9. Lancez un ping de H1 vers R2, puis coupez la capture avec la commande `monitor capture stop`.
10. Qu'observez-vous avec la commande `show monitor capture BUF buffer brief` ?

3 Troisième Partie : Syslog

Vous avez configuré votre passerelle pour que vos hôtes puissent accéder à un réseau public. Afin de superviser les actions des hôtes, et de pouvoir analyser en cas d'attaque, vous allez mettre en place des messages Syslog. Toute attribution d'adresse et toute translation sera enregistrée.

1. Vérifiez la configuration du serveur Rsyslog dans le fichier `/etc/rsyslog.conf`
2. Sur HS, vérifiez que votre serveur Rsyslog est lancé à l'aide de la commande `sudo systemctl status rsyslog`.
3. Sur R1, réglez l'horloge à l'aide de la commande `clock`.
4. À l'aide de la commande `logging`, configurez HS comme hôte de réception des alertes Syslog.
5. Utilisez la commande `logging trap debugging` pour que les alarmes de niveau débug (7) soient envoyées via Syslog.
6. Le routeur est maintenant configuré pour émettre des messages Syslog vers HS. Activez les messages DHCP en mode `enable` à l'aide de la commande `debug ip dhcp server events`.
7. Renouvelez le bail DHCP sur H1 et H2, et consultez le serveur Syslog.
8. Activez les messages NAT à l'aide de la commande `ip nat log translations syslog`
9. Effectuez des requêtes depuis H1 et H2 vers R2, et consultez le serveur Syslog. Dans un premier temps, regardez les messages Syslog à l'aide de Wireshark. On pourrait configurer le serveur pour inscrire les messages dans différents fichiers.
10. À l'aide du serveur Syslog, comment détectez vous si un hôte indésirable s'est connecté à votre LAN ?
11. À l'aide du serveur Syslog, comment détectez vous si l'un des hôtes de votre réseau est à l'origine d'une attaque (volontairement ou pas) ?

4 Partie Bonus : NTP

Vous l'avez vu dans la partie précédente, l'horodatage des évènement est capital à leur analyse. Afin de synchroniser les horloges de tout le réseau, il existe le Network Time Protocol (NTP - RFC 5905). En pratique l'un des éléments de votre réseau doit faire office de serveur NTP, autrement dit un élément doit être la référence. Cet élément fait partie de votre réseau. Dans ce TP, pour éviter de vous faire refaire une topologie, nous allons utiliser R2 comme serveur NTP.

1. Sur R2, configurez l'horloge au premier Janvier 2021 à minuit.
2. Configurez R2 comme maître NTP.
3. Sur R1, déclarez l'adresse de R2 comme serveur. Utilisez également la commande `ntp update-calendar`
4. Vérifiez votre configuration à l'aide des commandes `show clock` et `show ntp associations`.

POLYTECH NANCY

5 Nettoyage

Sur tous vos ordinateurs :

- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

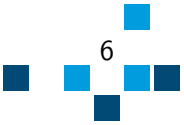
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

- Tapez la commande `vtp mode transparent`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:vlan.dat`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos firewall ASA ou PIX :

- Effacez la configuration courante à l'aide de la commande `clear config all`
- Effacez la configuration de démarrage à l'aide de la commande `write erase`
- Rangez les câbles et posez les équipement en bout de paillasse



Travaux pratiques - Contrôle d'accès

TP - Le contrôle d'accès avec les ACL

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

Éléments de cours

La RFC 4949 défini les Access Control List comme suit : c'est un mécanisme qui contrôle l'accès à une ressource, désignant les entités reconnues et les modes d'accès associés. En Réseaux, une ACL sur un pare-feu ou un routeur, est une liste d'adresses ou de ports autorisés ou interdits.

Les Access Control List sont divisés en deux grandes catégories, l'ACL standard et l'ACL étendue. Basiquement, l'ACL standard ne contrôle que l'adresse source, alors que l'ACL étendue peut également contrôler l'adresse de destination, le type de protocole (TCP, UDP, ICMP, IGRP, IGMP, etc.), le port source et destination, les flux TCP, IP TOS (Type of service) ainsi que les priorités IP.

Les ACL conviennent bien à des protocoles dont les ports sont statiques et connus à l'avance, comme pour des protocoles classiques (FTP, HTTP, SMTP...), mais ne suffisent pas toujours, comme pour des logiciels où les ports peuvent varier (P2P par exemple).

Une ACL est constituée d'Access Control Entries (ACE) qui définissent chacune une autorisation ou une interdiction pour un critère donné. L'ordre des ACE au sein de l'ACL est primordial, car l'équipement filtrant appliquera ces règles dans l'ordre à chaque paquet jusqu'à ce qu'un critère corresponde à la règle. L'autorisation ou l'interdiction liée à cette ACE est alors appliquée, sans consulter le reste de l'ACL.

Une bonne pratique est de définir les règles les plus spécifiques d'abord, et de définir ensuite les règles de plus en plus générales.

Matériel nécessaire

- 1 routeur CISCO
- 2 PC sous Windows ou Ubuntu
- 1 câble console (à paires inversées) pour connecter le port série du PC aux ports console

Partie préliminaire : Topologie

Si et seulement si vous disposez de l'équipement adapté, ou que vous travaillez sous Packet Tracer, utilisez la topologie suivante Figure 19 pour vous simplifier la vie. Sinon, passez à la page suivante et utilisez les topologies des Figures 20, 21 et 22.

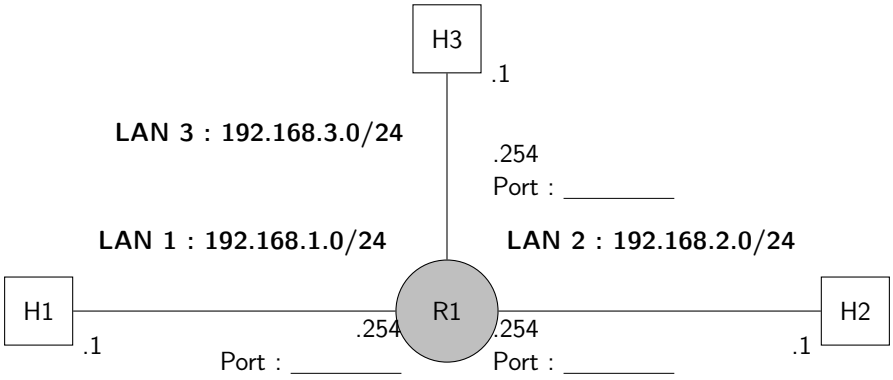


FIGURE 19 – Topologie complète du réseau

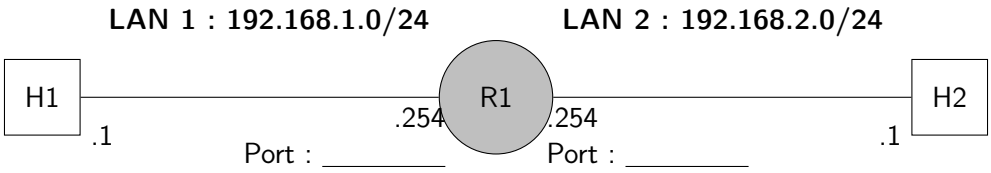


FIGURE 20 – Première topologie du réseau

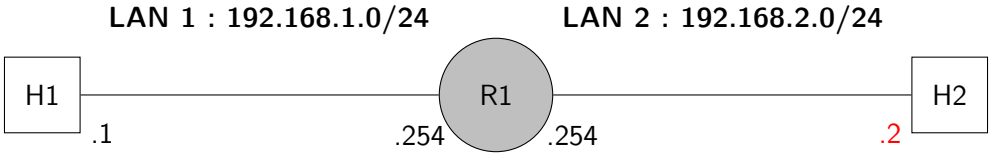


FIGURE 21 – Deuxième topologie du réseau

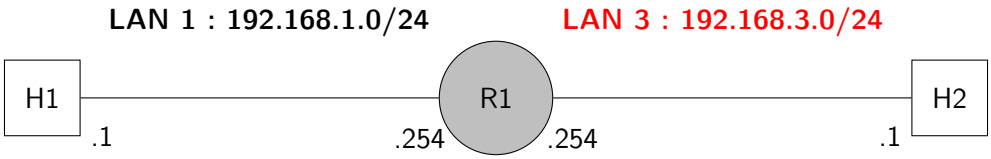


FIGURE 22 – Troisième topologie du réseau

Dans un premier temps, déployez la première topologie présentée dans la figure 20. Au cours du TP, vous aurez à la modifier au niveau de l'adressage, comme présenté aux figures 21 et 22. Notez les ports utilisés sur le schéma, ils seront indispensables pour décrire les réalisations de ce TP.

Configurez un accès Telnet sur le routeurs R1 (mots de passe `polytech` et `poly`) :

```
#configure terminal
(config)#enable password polytech
(config)#line vty 0 2
(config-line)#transport input telnet
(config-line)#password poly
(config-line)#login
```

1 Première Partie : ACL Standard

Dans cette première partie, seules les ACL dites standards seront utilisées.

1. Configurez sur R1 une ACL 10 bloquant uniquement l'adresse de l'hôte H1, en entrée sur le port LAN 1. Toutes les autres adresses sources doivent-être autorisées.
   a. Quelles ACE allez-vous utiliser dans votre ACL ?
   b. Quelles commandes utilisez vous pour définir l'ACL ? Et pour l'appliquer à une interface ?
   c. H1 peut-il contacter la passerelle ?
   d. H1 peut-il contacter H2 ?
2. Retirez l'ACL et appliquez l'ACL 10 en sortie sur le port LAN 2 de votre routeur R1. Cette fois-ci, à quoi l'hôte H1 a-t-il accès ?
3. Supprimez l'ACL 10.
4. Créez une nouvelle ACL 20 sur R1. Cette ACL doit permettre uniquement à l'adresse 192.168.2.1 d'accéder au LAN 1.
   a. Comment allez-vous définir votre ACL ?
   b. À quelle interface de R1 allez-vous l'attribuer, et dans quel sens ?
   Rappelez-vous que le sens est toujours relatif à l'équipement qui porte l'ACL.
   c. Déployez cette ACL et testez-la sur la topologie Fig. 20 puis sur la topologie Fig. 21.
5. Supprimez l'ACL 20.
6. Créez une nouvelle ACL 30 sur R1. Cette ACL doit permettre à tout le LAN 2 d'accéder au LAN 1. Cette ACL doit donc faire en sorte que tout autre réseau, par exemple le réseau 192.168.3.0/24, ne doit pas pouvoir contacter le LAN 1. Mais on ne veut pas d'une ACL à rallonge qui bloque tous les réseaux existants.
   a. Comment allez-vous définir votre ACL ?
   b. À quelle interface allez-vous l'attribuer, et dans quel sens ?
   c. Déployez cette ACL et testez-la sur la topologie Fig. 20 puis sur la topologie Fig. 22.
7. Supprimez l'ACL 30.
8. Rétablissez la topologie Fig. 20.
9. Imaginez que vous voulez restreindre l'accès FTP vers votre hôte H2 pour des raisons de sécurité, par exemple s'il s'agissait d'un serveur de dépôt de fichier pour les employés d'une entreprise. Mais vous voulez autoriser d'autres types de trafic vers votre réseau interne.
   a. Quelle ACL standard permettrait uniquement à l'hôte H1 de contacter H2 ?
   b. À quelle interface faudrait-il l'attribuer, et dans quel sens ?
   c. Pourquoi cela poserait-t-il problème ?

2 Deuxième Partie : ACL étendues

Nous avons pu remarquer précédemment les limitations des ACL standards, nous allons donc étudier ici plus en détail les ACL étendues.

1. Assurez-vous d'avoir supprimé toutes les ACLs standards précédentes.
2. Les ACL étendues permettent un filtrage par adresse de destination. Créez une nouvelle ACL 110 sur R1. Cette ACL doit bloquer toute communication à destination de H1.
   a. Comment allez-vous définir votre ACL ?
   b. À quelle interface allez-vous l'attribuer, et dans quel sens ?
   c. Déployez cette ACL et testez-la.
3. Supprimez l'ACL 110.
4. Imaginons un scénario où, pour des raisons de sécurité, vous voulez empêcher certains types de trafic. Par exemple, vous souhaitez bloquer le trafic ICMP. Créez une nouvelle ACL 120 sur R1. Cette ACL doit bloquer tout trafic ICMP à destination de H1.
   a. Comment allez-vous définir votre ACL ?
   b. À quelle interface allez-vous l'attribuer, et dans quel sens ?
   c. Déployez cette ACL et testez-la. Testez que d'autres protocoles fonctionnent, par exemple avec une connexion Telnet vers R1.
5. Supprimez l'ACL 120.
6. Quels autres protocoles pouvez-vous filtrer à l'aide des ACL étendues ?

3 Troisième Partie : ACL pour connexion distante

Les lignes TTY (TeleTYpe) sont les connexions aux terminaux physique, tels que le port console. En configuration, il apparaît sous "line con 0". Les VTY (Virtual Terminal Lines) sont une sorte de TTY implémentées en logiciel, et donc virtuelles. Elles servent pour les connexions à distance de type Telnet ou encore SSH. En configuration, elles apparaissent sous la forme "line vty 0 4", ce qui signifie que les lignes 0 à 4 sont définies. On peut changer le nombre de sessions virtuelles, contrairement aux connexions physiques qui sont limitées par les ports de l'équipement.

1. Assurez-vous d'avoir supprimé toutes les ACL standards précédentes sur R1.
2. Assurez-vous d'avoir permis uniquement 2 sessions Telnet sur le routeur R1. Pour cela, définissez une ACL 50 qui bloque tout trafic, et appliquez-la dans les VTY 2 à 4.
3. À l'aide d'une ACL 51, faites en sorte que la VTY 1 soit toujours réservée à votre hôte H1.
4. N'appliquez aucune ACL à la VTY 0.
5. Connectez-vous en Telnet avec H2. Maintenez la connexion ouverte.
6. Pouvez-vous ouvrir une autre connexion depuis H2 (sur Packet Tracer utilisez H3) ? Pourquoi ?
7. Pouvez-vous ouvrir une autre connexion depuis H1 ? Pourquoi ?

POLYTECH NANCY

4 Nettoyage

Sur tous vos ordinateurs :

- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

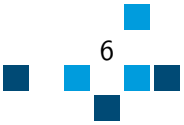
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

- Tapez la commande `vtp mode transparent`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:vlan.dat`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos firewall ASA ou PIX :

- Effacez la configuration courante à l'aide de la commande `clear config all`
- Effacez la configuration de démarrage à l'aide de la commande `write erase`
- Rangez les câbles et posez les équipement en bout de paillasse



Travaux pratiques - Contrôle d'accès

TP - Firewall

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

Éléments de cours

Un firewall est un élément de surveillance et de filtrage de trafic. Il peut s'agir d'un équipement physique dédié, d'une partie d'un équipement réseau, ou d'un logiciel déporté. Suivant les classifications, on distingue plusieurs types de firewalls. On résumera les types de fonctionnement des firewalls de la manière suivante :

- Filtrage de paquet : les règles de filtrage sont appliquées à chaque paquet indépendamment, en se basant sur l'en-tête réseau du paquet. On parle alors d'inspection superficielle, ou de Shallow Packet Inspection (SPI). Parfois, l'en-tête UDP/TCP peut également être observée.
- Filtrage à état ou stateful : le firewall a une mémoire des connexions en cours (comme une session TCP par exemple), toujours en se basant sur du SPI.
- Filtrage niveau application : le firewall peut identifier les applications et vérifier la conformité des paquets. Il accède à des informations de couche 7 en effectuant du Deep Packet Inspection (DPI), c'est-à-dire que le filtrage inspecte la donnée, la payload d'un paquet.

Vous lirez et entendrez souvent que les firewalls permettent de faire plus de choses : tunneling, chiffrement, serveur mandataire (proxy)... En réalité, le firewall est simplement l'élément de filtrage d'un équipement, mais il est rare qu'un tel équipement de sécurité possède une seule fonctionnalité. L'amalgame vient de la réalité pratique, où le rôle de l'équipement dit "firewall" est souvent multiple, comme c'est le cas des PIX et des ASA.

Les Cisco Private Internet eXchange (PIX) et Adaptive Security Appliance (ASA) sont des équipements de sécurité Cisco aux multiples fonctionnalités. On a tendance à les appeler à tort des "firewalls" (pare-feux). En réalité, les PIX et ASA combinent -entre autres- des fonctionnalités de firewall, antivirus, VPN, et détection d'intrusion. Les PIX ne sont plus commercialisés, mais les ASA perpétuent la gamme, avec un fonctionnement et des configurations similaires.

Dans le cadre de ce TP, nous nous intéresserons donc à l'élément définissant un firewall : le filtrage.

Un mot d'avertissement : jusqu'ici, vous avez travaillé avec des routeurs ou des commutateurs. Dans d'autres environnements, vous avez peut-être entendu parler de commutateurs de niveau 3, qui embarquent des fonctionnalités de routage inter-VLAN. Les PIX ou ASA sont un type d'équipement similaire. Capable de commutation et de routage (même du routage WAN), il sont néanmoins plus limités physiquement. L'objectif est de fournir un portail de sécurité, il sont donc moins performant qu'un routeur pour du routage, et moins performant qu'un commutateur pour de la commutation.

Matériel nécessaire

- 1 routeur CISCO
- 1 commutateur CISCO
- 1 équipement PIX ou ASA 5505 CISCO (le 5506 est un peu différent)
- 3 PC sous Windows ou Ubuntu
- 1 câble console (à paires inversées) pour connecter le port série du PC aux ports console

1 Première Partie : Filtrage de paquet avec les ACL

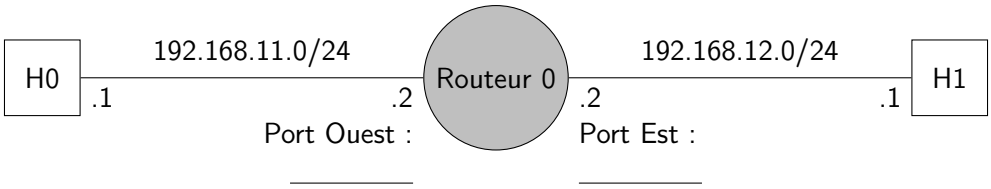


FIGURE 23 – Topologie à déployer

Les ACL (Access Control List) sont un mécanisme de contrôle d'accès à une ressource, désignant une liste d'adresses ou de ports autorisés ou interdits. Elles sont étudiées plus en détail dans le TP dédié, mais il s'agit du premier élément de filtrage à votre disposition. Souvent, les routeurs sont capables d'appliquer des ACL.

1. Déployez la topologie présentée dans la figure 23.
2. L'hôte H0 peut-il pinger l'hôte H1 ?
3. Définissez une ACL standard 10 pour bloquer tous les paquets. Appliquez là dans le sens **entrant** sur l'interface Est. Utilisez les commandes suivantes :

```
access-list 10 deny any
interface Fa0/1
  ip access-group 10 in
```

4. L'hôte H0 peut-il pinger l'hôte H1 ?
5. Lancez un ping de l'hôte H0 vers H1. Qu'observez-vous sur le trajet de la requête ? Observez avec Wireshark, ou l'outil simulation si vous travaillez sur Packet Tracer.
6. Supprimez votre ACL 10.
7. Définissez une ACL standard 20 pour bloquer tous les paquets **entrant** dans l'interface Est, sauf si le paquet provient de H1. Votre ACL doit avoir deux entrées :

```
access-list 20 permit 192.168.12.1 0.0.0.0
access-list 20 deny any
```

8. L'hôte H0 peut-il pinger l'hôte H1 ?
9. Supprimez votre ACL 20.

Le même système d'ACL est disponible sur les PIX ou ASA comme nous le verrons plus loin.

2 Deuxième Partie : Filtrage stateful

Nous avons vu dans la partie précédente que l'utilisation d'ACL ne permet pas de garder en mémoire des échanges en cours. Nous allons maintenant déployer un PIX/ASA et observer du filtrage stateful.

2.1 Déploiement du Firewall

Vous allez devoir modifier la configuration par défaut du Firewall. Il possède un CLI très proche de celui de l'IOS, qu'on trouve sur les routeurs et commutateurs Cisco.

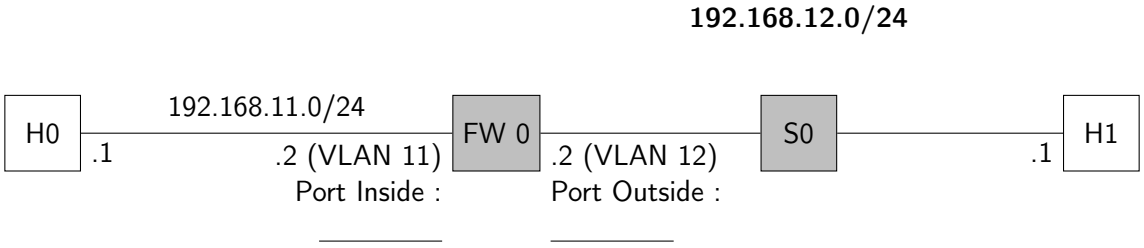


FIGURE 24 – Topologie à déployer

1. Déployez uniquement le câblage de la topologie présentée dans la figure 24. Configurez les adresses IP des hôtes.
2. Que ce soit sur un PIX ou un ASA, le mot de passe "enable" par défaut est **vide**.
   Changez-le pour `polytech`.
3. Vérifiez l'absence de toute configuration serveur et client DHCP. Les équipements plus récents comme les ASA proposent un fonction serveur DHCP par défaut. D'après vous, pourquoi ?
4. Les configurations IP des PIX et des ASA sont un peu différentes, car l'ASA se base sur des interfaces VLAN plutôt que directement sur les interfaces physiques. Néanmoins, le fonctionnement et la configuration de la partie Firewall à proprement parler sont les mêmes. Reportez-vous à la partie ci-dessous suivant le support que vous utilisez.

   Configuration sur un PIX :

   a. À l'aide de la commande `nameif`, configurez l'interface dirigée vers H0, nommez-là "inside" et attribuez-lui un niveau de sécurité 100. Sur ces vieux modèles, il n'y a pas de mode de configuration d'interface comme un routeur.

   b. À l'aide de la commande `ip address inside` attribuez une adresse à l'interface que vous venez de nommer, conformément à la Fig. 24.

   c. Activez l'interface avec la commande `interface ethernet0 auto`. Encore une fois, ces vieux modèles ne se comportent pas comme IOS...

   d. Configurez l'interface dirigée vers S0 "outside", niveau de sécurité 0 et affectez-lui son adresse IP.

   e. Pour des réseaux plus complets, il faudrait définir une route par défaut. Définissez une route par défaut sur l'interface "outside". La commande est un peu différente de celle d'un routeur :

```
route outside 0.0.0.0 0.0.0.0 192.168.12.1
```

f. Le NAT n'est pas nécessaire au PIX dans cette partie, mais on s'en servira plus tard. Utilisez les lignes suivantes :

```
global (outside) 1 192.168.12.4-192.168.12.254
nat (inside) 1 192.168.11.0 255.255.255.0
```

Configuration sur un ASA :

a. Créez une interface VLAN 11, nommez-là "inside", attribuez-lui un niveau de sécurité 100. Enfin, définissez l'adresse IP conformément au schéma.

b. Créez une interface VLAN 12, nommez-là "outside", attribuez-lui un niveau de sécurité 0. Enfin, définissez l'adresse IP conformément au schéma.

c. Attribuez à chacune des interfaces physique le VLAN 11 ou 12, suivant la figure 24, à l'aide de la commande `switchport`. N'oubliez pas d'activer les interfaces.

d. Pour des réseaux plus complets, il faudrait définir une route par défaut. Définissez une route par défaut sur l'interface "outside". La commande est un peu différente de celle d'un routeur :

```
route outside 0.0.0.0 0.0.0.0 192.168.12.1
```

e. L'ASA requiert l'utilisation de NAT pour fonctionner. La configuration est un peu différente de celle d'un routeur. Vous allez devoir utiliser la commande `object` qui n'apparaît pas dans les aides " ?" ou "Tab". Utilisez les lignes suivantes :

```
object network outside
  network-object 192.168.12.0 255.255.255.0
  global (outside) 1 192.168.12.4-192.168.12.254
object network inside
  network-object 192.168.11.0 255.255.255.0
  nat (inside) 1 192.168.11.0 255.255.255.0
```

5. L'hôte H0 peut-il pinger l'adresse de l'interface "inside" ?
6. L'hôte H0 peut-il pinger l'adresse de l'interface "outside" ?
7. L'hôte H0 peut-il pinger l'hôte H1 ?
8. À quelle étape le paquet est-il abandonné ? Observez le trafic sur les interfaces des hôtes.
9. L'hôte H1 peut-il pinger l'hôte H0 ?
10. À quelle étape le paquet est-il abandonné ?
11. Observez la table de routage. Selon vous, pourquoi le ping ne fonctionne-t-il pas ? Autrement dit, quel est le comportement par défaut du Firewall ? Souvenez-vous que vous avez défini des niveaux de sécurité différent.

2.2 Class-map et Policy-map : filtrage et actions

Comme vous l'avez vu en début de TP, si on définit une ACL qui bloque tous les paquets entrant dans l'interface extérieure, l'hôte H0 ne peut pas pinger l'hôte H1 car la réponse ne peut pas lui parvenir.

Nous allons maintenant exploiter les possibilité du Firewall pour définir des politiques d'inspections. Il s'agit de définir des règles de filtrage, d'inspection et d'actions. On peut les voir comme l'évolution des ACL.

12. Définissez une politique d'inspection ICMP à l'aide des commandes suivantes. Par défaut, l'inspection d'un trafic permet le transport (comme une ACL "permit").

```
class-map inspection_default
 match default-inspection-traffic
 exit
policy-map global_policy
 class inspection_default
  inspect icmp
```

13. Appliquez la politique d'inspection à l'interface `inside`.

```
no service-policy global_policy global
service-policy global_policy interface inside
```

14. L'hôte H0 peut-il pinger l'hôte H1 ? Qu'observez-vous comme différence avec les ACLs ? Qu'en déduisez-vous sur le filtrage par politique d'inspection ?

3 Troisième Partie : Placement du firewall

3.1 Sortie de réseau

Dans les parties précédentes, vous avez vu comment utiliser et configurer un firewall. Chaque réseau a ses propres besoins en sécurité, et il faudra adapter la configuration en conséquence. Nous allons maintenant évoquer le placement des firewalls dans les réseaux. De manière similaire, ce placement dépend des usages, mais il existe des conception courantes.

Généralement, le firewall est placé à la limite entre votre réseau, que vous considérez sécurisé, et le réseau extérieur, que vous **devez** considérer comme dangereux, car vous ne le maîtrisez pas.

Le firewall peut-être placé avant ou après l'équipement passerelle entre votre réseau et le réseau extérieur. Traditionnellement, on les place avant, comme illustré sur la figure 25. La passerelle utilise -entre autres- des protocoles de routages WAN et doit pouvoir communiquer avec celui-ci. Néanmoins, suivant la configuration du firewall, il est parfaitement possible de le placer avant, comme sur la figure 26. Si le firewall est transparent aux protocoles nécessaires, la passerelle assure toujours son rôle, et elle est plus sécurisée.

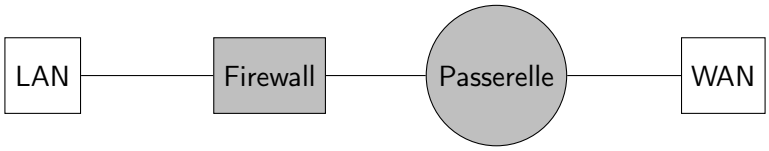


FIGURE 25 – Placement du firewall avant passerelle

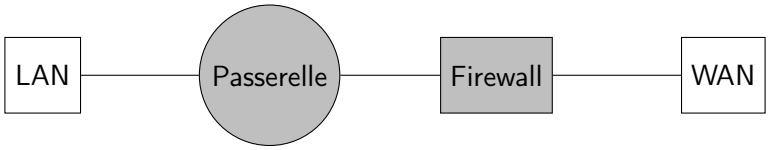


FIGURE 26 – Placement du firewall après passerelle

3.2 Notion de DMZ

Parfois, vous voulez sécuriser votre réseau, mais laisser accessibles certains services au réseau extérieur. Par exemple, votre entreprise possède un réseau pour ses employés, mais souhaite héberger son site Web : il faut donc un accès entrant à Internet sur un serveur, mais pas nécessairement sur toutes les machines. Vous avez alors besoin de la notion de Zone Démilitarisée (DMZ).

Une DMZ est un sous-réseau physique ou logique qui expose une partie des ressources au réseau externe non-sécurisé. L'objectif est de restreindre l'accessibilité au strict nécessaire, en créant une zone tampon moins sécurisée. On trouve généralement des conceptions à un ou deux firewall.

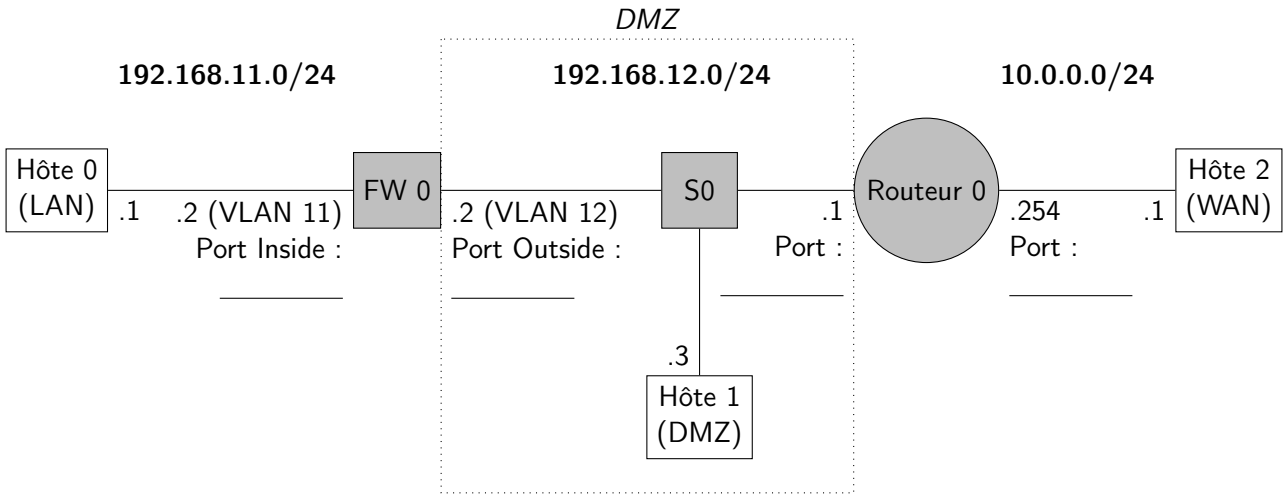


FIGURE 27 – DMZ à un seul firewall

1. Déployez le réseau illustré par la figure 27.
2. Dans la partie précédente, vous avez déjà configuré le NAT sur le Firewall, et définit une route par défaut vers R0.
3. Conservez l'inspection ICMP.
4. Vérifiez le comportement du ping depuis l'hôte 0 vers 2, puis de 2 vers 0.
5. Sachant que le Firewall applique du NAT, expliquez ce que vous avez observé.
6. Faites de même entre l'hôte 0 et l'hôte 1.
7. L'hôte 2 peut-il contacter l'hôte 1 ?
8. L'hôte 1 est-il sécurisé ?

Le type de topologie présenté dans la figure 28 est également possible. Il demande des configurations plus complexes et expose votre firewall aux requêtes extérieures, mais permet de créer un niveau de sécurité minimal pour la DMZ. Par exemple, vous pouvez attribuer à l'hôte 1 un niveau de sécurité de 50, entre l'intérieur et l'extérieur. Il est ainsi joignable par l'hôte 0, mais pas par l'hôte 2. Et il ne peut pas lui même contacter l'hôte 0. On le protège, sans lui faire confiance.

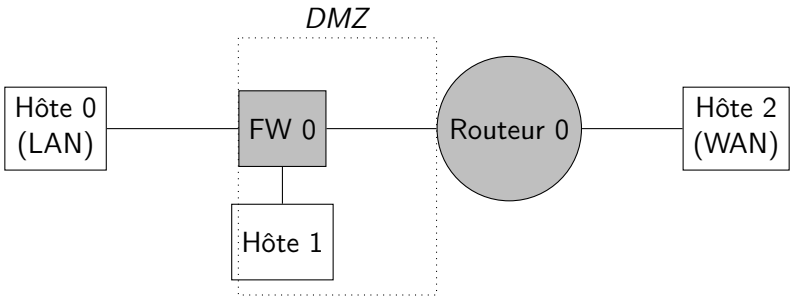


FIGURE 28 – DMZ à un seul firewall

Vous pouvez également déployer deux firewalls, comme illustré dans la figure 29. L'objectif est de protéger à la fois votre réseau intérieur, votre DMZ et votre routeur passerelle. Le premier firewall a un niveau de sécurité moins élevé que le second. Il est également courant d'utiliser deux firewalls de constructeurs différents, pour se protéger contre des failles systèmes qui pourraient apparaître sur une même gamme.

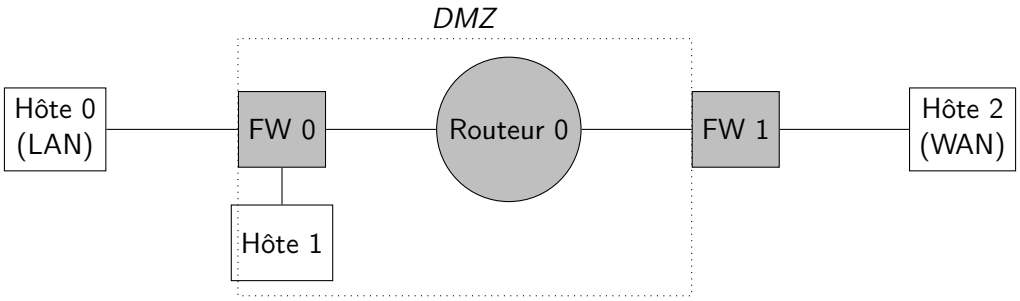


FIGURE 29 – DMZ à deux firewalls

4 Quatrième Partie : Filtrage niveau application - Deep Packet Inspection

Vous ne pourrez pas réaliser cette partie sur Packet Tracer, puisque les couches application n'y sont pas modélisées.

Vous avez normalement compris dans la partie sur le filtrage stateful que le comportement par défaut du Firewall est d'interdire les communications d'un niveau de sécurité vers un niveau plus haut. Grâce aux ACLs, vous pouvez créer des exceptions à ce comportement en autorisant certains trafics entrants.

1. Autorisez le trafic ICMP vers le "inside", à l'aide d'une ACL 120 sur l'interface "inside" en "out", et validez son comportement. Contrairement à un routeur, pour affecter une ACL sur un ASA ou un PIX, il ne faut pas aller dans le mode de configuration d'interface, mais directement en mode de configuration globale avec la commande `access-group`, puis spécifier dans la commande l'interface où elle doit être appliquée. Où avez-vous placé cette ACL ?
2. Supprimez l'ACL 120.

Grâce au DPI, vous pouvez explorer le contenu des paquets et prendre des décisions avancées sur le trafic. Dans cet exemple, nous allons utiliser le protocole FTP. Nous allons utiliser la même topologie que précédemment. L'hôte H0 fera office de serveur FTP.

3. Créez une ACL 130 autorisant le trafic FTP entrant sur l'interface *outside* de toute source à destination de H1.
4. Déployez un serveur FTP sur l'hôte H0. Sur Ubuntu, utilisez *vsftpd*. Pensez à autoriser les opérations en écriture dans la configuration. Sur Windows, vous pouvez utiliser la version serveur de Filezilla.
5. Effectuez une requête PUT depuis l'hôte H1 pour placer un fichier sur l'hôte H0.
6. Effectuez une requête DELETE pour supprimer ce fichier.

Vous allez maintenant ajoutez le DPI pour bloquer les opérations DELETE :

7. Retirez la politique d'inspection de l'interface outside.
8. Retirez le FTP du mode d'inspection global.

```
policy-map global_policy
  class inspection_default
    no inspect ftp
```

9. Puis configurez une `class-map` et une politique d'inspection spécifique (il n'est pas nécessaire de définir.

```
class-map type inspect ftp match-any nodeleteclass
  match request-command DELE
    exit
policy-map type inspect ftp nodeletepolicy
  class nodeleteclass
    reset log
    exit
  exit
policy-map global_policy
  class inspection_default
    inspect ftp strict nodeletepolicy
    exit
  exit
```

10. Appliquez la politique d'inspection de manière globale.

```
service-policy global_policy global
```

11. Effectuez à nouveau une requête PUT puis une requête DELETE. Qu'observez-vous ?

POLYTECH NANCY

5 Nettoyage

Sur tous vos ordinateurs :

- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

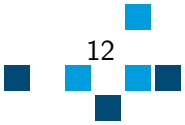
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

- Tapez la commande `vtp mode transparent`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:vlan.dat`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos firewall ASA ou PIX :

- Effacez la configuration courante à l'aide de la commande `clear config all`
- Effacez la configuration de démarrage à l'aide de la commande `write erase`
- Rangez les câbles et posez les équipement en bout de paillasse



Travaux pratiques - Contrôle d'accès

TP - VPN et Proxy

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

Éléments de cours

Un Virtual Private Network (VPN) est -comme son nom l'indique- un réseau privé virtuel, c'est-à-dire un réseau privé géographiquement étendu à travers un autre réseau. Un VPN permet ainsi aux équipements connectés d'échanger comme s'ils se trouvaient sur un même sous-réseau, aux performances physique près. Le VPN est un concept, qui peut s'implémenter de différentes manières. Les VLANs créent des VPN sur une technologie niveau 2. Vous pouvez bien isoler différents sous-réseaux et relier des éléments physiquement séparés. Plus généralement, on utilisera des VPN sur des topologies niveau 3. Pour cela, on utilise une technologie de Tunneling.

Le Tunneling permet d'encapsuler des données dans un protocole de transport, afin de conserver toute en-tête protocolaire même si le réseau de transport ne supporte pas le protocole encapsulé. Par exemple, une entreprise utilise de l'IPv6 pour connecter ses machines entre elles sur deux sites, alors que son fournisseur d'accès Internet n'utilise que de l'IPv4. L'entreprise peut encapsuler son trafic IPv6 dans un tunnel IPv4 au niveau des passerelles pour connecter ses deux sites de manière transparente.

Par défaut, un tunnel permet simplement d'encapsuler des données. Il est possible d'appliquer à un tunnel du chiffrement, afin de garantir la confidentialité des données. Ce sont bien deux concepts distincts. Dans ce TP, vous verrez deux techniques de tunneling, avec et sans chiffrement.

On distingue globalement trois types d'utilisation des VPN : les Site-to-site, les Point-to-point et les Point-to-site. Techniquement, il s'agit toujours des mêmes tunnels, ce sont les cas d'usages dans une architecture globale qui diffère. Les architectures VPN Site-to-site ont pour but d'interconnecter plusieurs sites possédant chacun plusieurs machines. On trouve généralement les points de tunneling au niveau des passerelles ou sur un serveur de rebond interne. Les architectures VPN Point-to-point sont eux portés par des tunnels connectant directement les machines. Les architecture VPN Point-to-site connectent une machine à un réseau distant. Cette solution est privilégiée pour les utilisateurs mobiles, par exemple pour le télétravail.

On retrouve souvent la notion de VPN associée à la notion de Proxy ou serveur mandataire. Un Proxy est un élément qui va relayer les requêtes d'un hôte avec sa propre identité. C'est un intermédiaire, un substitut à l'hôte pour tous ses échanges. Il a littéralement un "mandat" de l'hôte. Il permet d'assurer la confidentialité de l'hôte, ainsi que son intégrité. En cas d'attaque, c'est le Proxy qui subira les effets.

Ce que l'on trouve régulièrement appelé "VPN" sur le marché est en réalité un abus de langage. Il s'agit généralement d'une architecture VPN point-to-point vers un serveur Proxy, basée sur un tunnel chiffré.

Matériel nécessaire

- 3 routeurs CISCO 2901 ou 4321
- 1 commutateurs CISCO
- 3 PC sous Ubuntu
  - H1 disposant d'un client VPN (OpenVPN Connect)
  - H2 disposant d'un serveur Web mininal
  - H3 disposant d'un serveur VPN (OpenVPN Access Server) et d'un proxy HTTP (Tinyproxy)

Partie préliminaire : Topologie

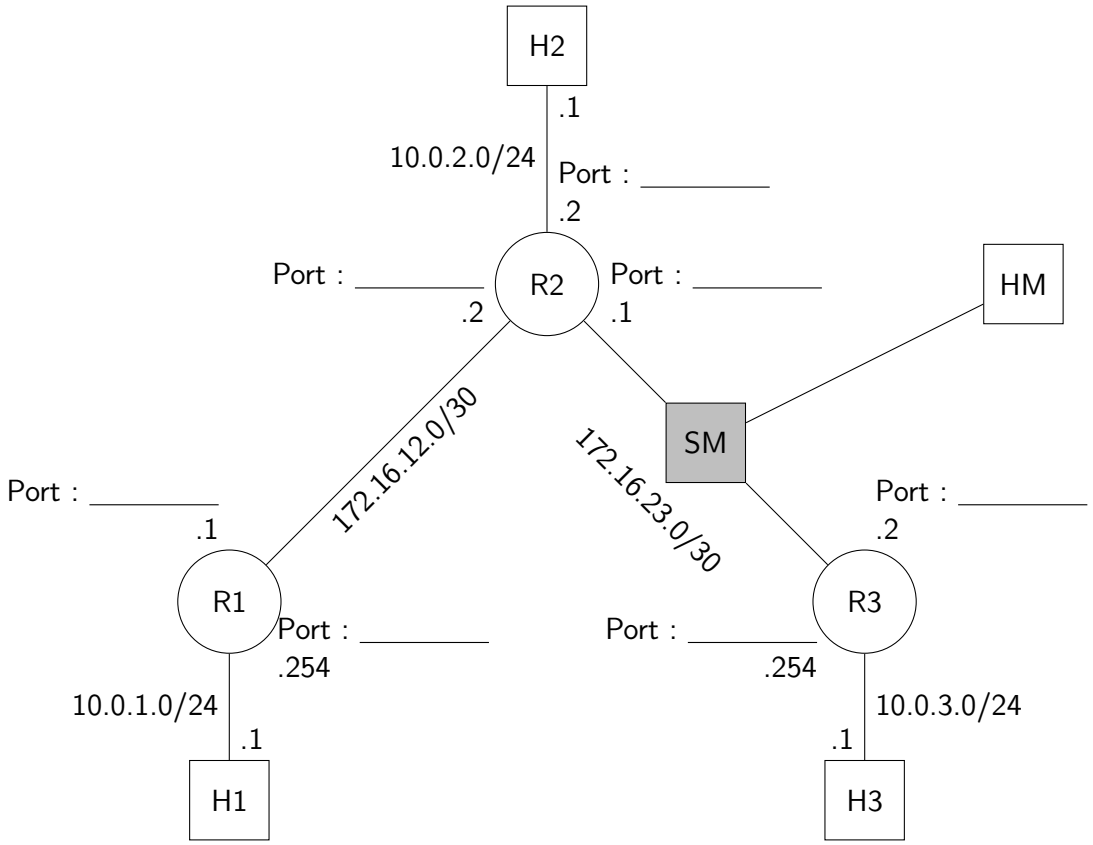


FIGURE 30 – Topologie du réseau

L'hôte HM est présent uniquement pour observer le trafic et ne nécessite pas de configuration.

1. Complétez le plan avec les ports que vous allez utiliser. Si nécessaire, utilisez une liaison série entre les routeurs R1 et R2. Pensez à configurer le *clockrate* sur l'interface série maître.
2. Déployez le réseau présenté en Fig. 30.
3. Sur R1, R2 et R3, créez un routage OSPF avec un numéro d'instance 1, en y déclarant uniquement les réseaux entre R1 et R2, et R2 et R3. Vérifiez la connectivité entre les trois routeurs R1, R2 et R3.
4. Pour l'instant, vérifiez simplement que H1, H2 et H3 parviennent à contacter les ports des routeurs. Pourquoi les hôtes ne peuvent-ils pas se contacter entre eux d'après notre configuration ?
5. Sur SM, configurez un port-mirroring du port connecté à R2 vers le port connecté vers HM. Vous aurez besoin des commandes suivantes. L'argument `both` permet de copier le trafic entrant et sortant.

```
Switch(config)#monitor session 1 source interface fa 0/1 both
Switch(config)#monitor session 1 destination interface fa0/2
```

6. Vérifiez que votre mirroring est bien configuré avec la commande `show monitor session 1`.
7. Vérifiez que le mirroring fonctionne en effectuant un ping entre R2 et R3. Que devriez-vous observez ?

1 Première partie : VPN

1.1 Tunneling Site-to-site

Generic Routing Encapsulation (GRE) est un protocole de tunneling sur réseaux IP défini par la RFC 2784. GRE ne propose pas de chiffrement mais il est possible d'activer IPsec, qui nécessite la licence Cisco "security" (version d'évaluation disponible sur Packet Tracer).

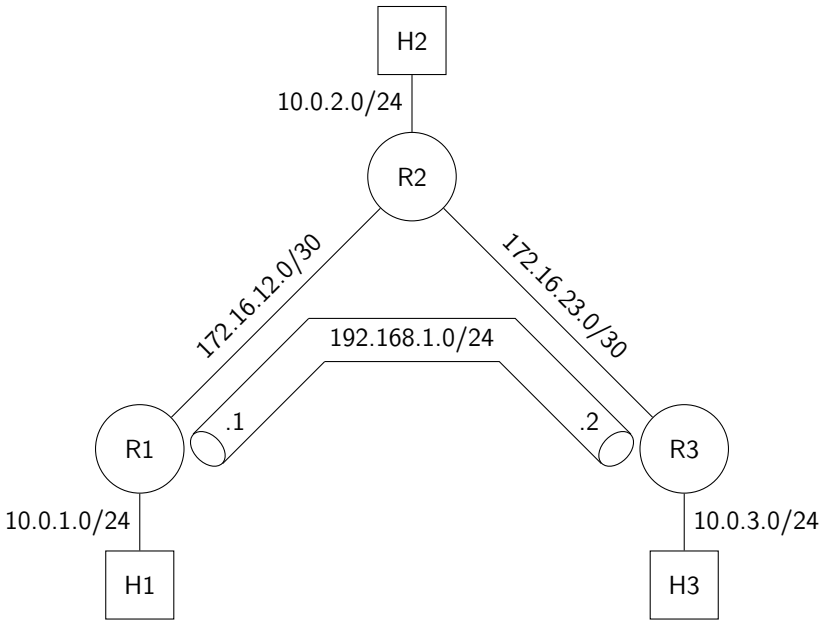


FIGURE 31 – VPN Site-to-site

1. Conservez toute votre configuration, le schéma a été simplifié pour faciliter la lecture.
2. Configurez les extrémités du tunnel GRE sur R1 et R3 en créant une interface "tunnel 0". Attribuez-leur une adresse IP conformément au schéma.
3. Dans chaque interface de type "tunnel", spécifiez l'interface source, autrement dit le port sortant vers le WAN. Configurez la destination en utilisant l'adresse de l'interface WAN du routeur distant.
4. Qu'observez-vous avec la commande "`show ip interface brief`" sur R1, R2 et R3 ?
5. À l'aide de la commande "`show interfaces tunnel 0`", déterminez les paramètres du tunnel établi.
6. Depuis R1, pouvez-vous pinger l'adresse de l'interface du tunnel sur R3 ?
7. Depuis R1, qu'indique la commande "`traceroute`" vers l'adresse de l'interface du tunnel sur R3 ?
8. Depuis R1, qu'indique la commande "`traceroute`" vers l'adresse de l'interface physique sur R3 ?
9. Sur R1 et R3, créez un routage OSPF avec un numéro d'instance 2, en y déclarant uniquement le réseau local et le réseau du VPN.
10. Depuis H1, pouvez-vous pinger H3 ?
11. Depuis H1, pouvez-vous pinger H2 ?
12. Depuis H1, qu'indique la commande "`traceroute`" vers H3 ?
13. Qu'observez vous sur l'hôte miroir ?

1.2 Tunneling Point-to-point

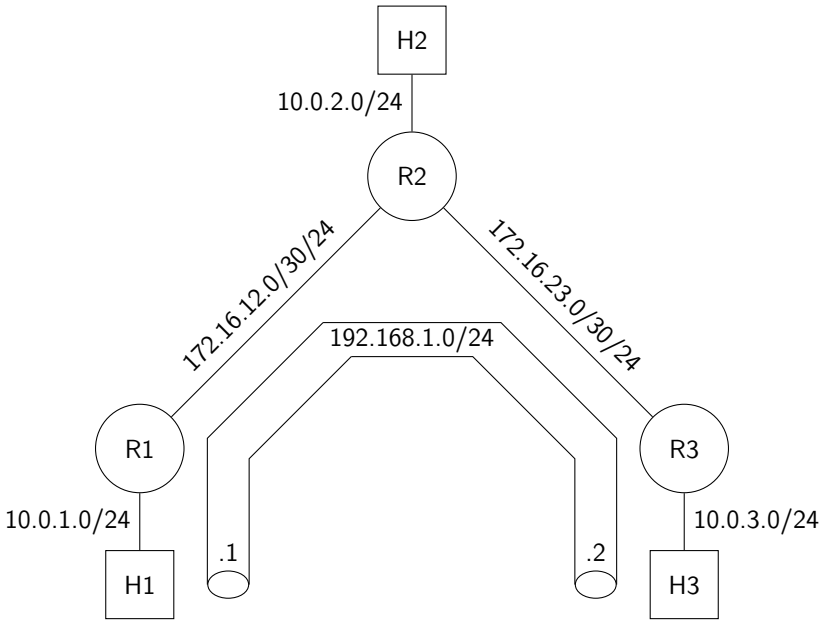


FIGURE 32 – VPN Point-to-point

1. Supprimez votre instance OSPF 2 et votre tunnel GRE.
2. Sur R1, R2 et R3, ajoutez le réseau local à la configuration de l'instance OSPF 1.
3. Vérifiez la connectivité entre les hôtes.
4. Sur H3, démarrez le serveur OpenVPN Access Server à l'aide de la commande `sudo systemctl start openvpnas.service`
5. Sur H3, accédez en HTTPS à l'interface de gestion d'OpenVPN Access Server avec les identifiants (openvpn, polytech) à l'adresse `https://127.0.0.1:943/admin`
6. Dans la configuration réseau "Network Settings", spécifiez l'adresse d'interface native de H3. Assurez-vous d'être en mode UDP uniquement.
7. Dans la configuration "VPN Settings", utiliser les adresses spécifiées en Fig. 32.
8. Vérifiez dans la configuration avancée que vous autorisez les communications entre les clients du VPN.
9. Créez une configuration client (polytech1,polytech) qui n'a pas les droits d'administration.
10. Dans le menu "Status", stoppez et relancez le serveur VPN.

11. Sur H1 utilisez les identifiants créés pour vous connecter via navigateur à l'URL du serveur OpenVPN sur le port 943 en HTTPS. Vous aurez alors la possibilité de télécharger un fichier `.ovpn` (lien en bas de page) qui vous servira à vous connecter en tant que client du VPN.
12. Ouvrez ce fichier avec un éditeur de texte, et vérifiez que l'adresse du serveur est bien une adresse routée dans le réseau.
13. Dans la configuration réseaux, créez une connexion VPN en important le fichier téléchargé. Toute la configuration client est incluse dans ce fichier.
14. Observez la configuration IP de l'hôte H1, à l'aide de la commande "`ip a`" sur Linux ou "`ipconfig`" sur Windows.
15. Observez sur l'interface de gestion du serveur que l'hôte H1 est bien connecté.
16. Observez la configuration IP de l'hôte H3, à l'aide de la commande "`ip a`".
17. H1 peut-il pinger l'adresse d'interface native de H3 ?
18. H1 peut-il pinger l'adresse d'interface VPN de H3 ?
19. Qu'observez-vous sur l'hôte miroir ?

2 Deuxième partie : Proxy

1. Conservez la configuration VPN Point-to-point précédente.
2. Vérifiez que le serveur HTTP sur H2 est actif en effectuant une requête depuis H3 (Par défaut sur l'adresse IP de H2 sans port).
3. Effectuez des requêtes HTTP de H1 vers H2. D'après vos observations sur l'hôte miroir, par où passent les échanges ?
4. Activez maintenant le proxy HTTP sur H3.

```
sudo /etc/init.d/tinyproxy start
```

5. Relevez le port d'écoute du proxy dans le fichier de configuration qui se trouve dans `/etc/tinyproxy/tinyproxy.conf`
6. Configurez H1 pour qu'il soit client du proxy (serveur mandataire).
7. Effectuez à nouveau des requêtes HTTP de H1 vers H2. Par où passent les échanges cette fois-ci ?

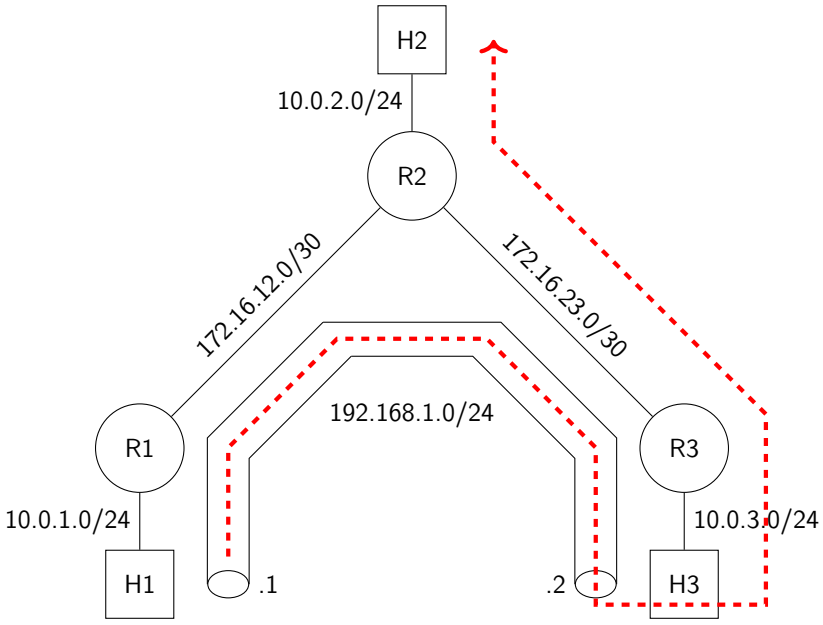


FIGURE 33 – Architecture VPN + Proxy

POLYTECH NANCY

3 Nettoyage

Sur tous vos ordinateurs :

- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

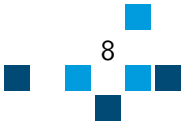
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

- Tapez la commande `vtp mode transparent`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:vlan.dat`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos firewall ASA ou PIX :

- Effacez la configuration courante à l'aide de la commande `clear config all`
- Effacez la configuration de démarrage à l'aide de la commande `write erase`
- Rangez les câbles et posez les équipement en bout de paillasse



Travaux pratiques - Infrastructures et réseaux opérateur

TP - Diffusion audiovisuelle : RTP et Multicast

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

Matériel nécessaire

- 2 routeurs CISCO
- 3 PC sous Windows ou Ubuntu
- 1 câble console

Partie préliminaire : Topologie

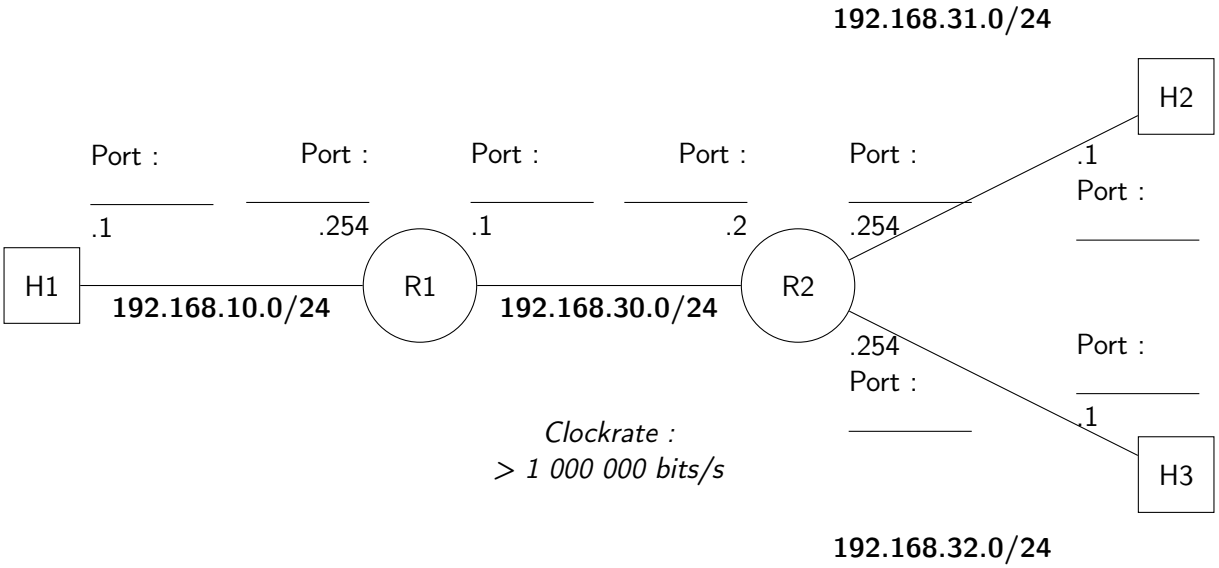


FIGURE 34 – Topologie du réseau

Mettez en place le réseau présenté sur le schéma avec un routage statique. Utilisez-les adresses présentes sur le schéma. Complétez le schéma avec les ports que vous utiliserez.

Vous allez transporter un flux vidéo, il vous faut donc une vitesse de communication suffisante.

Si vous utilisez une liaison série entre R1 et R2, vous devez augmenter suffisamment le *clockrate* de la liaison série. Essayez d'être au bien delà de 1 000 000 bits/s (1 Mbit/s). Il se peut qu'un de vos routeurs soit physiquement limitant. Essayez de changer le sens du câble. Si vous ne dépassez pas 1 Mbit/s, vous aurez peut-être besoin de changer de routeur.

1 Première Partie : Real-Time Protocol (RTP)

Dans un premier temps, nous allons travailler en Unicast pour comprendre le protocole RTP défini dans la RFC 3550. Le protocole RTP est un protocole de couche application, dont le but est de transporter des flux audio et vidéo sur un réseau IP. Il peut s'agir de vidéos, de téléphonie... Il est généralement basé sur le protocole de couche transport UDP. En effet, TCP est orienté sur la fiabilité du transport plutôt que son aspect temps réel. Dans cette première partie, vous allez utiliser le protocole RTP pour diffuser un flux audiovisuel d'une machine à une autre.

1. Créez un fichier vidéo. Si votre bande-passante n'est pas supérieure à 1 Mbit/s, votre vidéo doit être au mieux en résolution 480p.
2. Sur la machine H1, utilisez VLC pour créer un flux à partir d'un fichier vidéo :
   a. Média > Flux... > Ajoutez un fichier
   b. Puis cliquez sur Diffuser > Suivant > Sélectionnez Profil RTP/MPEG et cliquez sur "Ajouter"
   c. Renseignez l'adresse du destinataire et le port d'écoute : 192.168.31.1 :16384
   d. Puis cliquez sur "Suivant"
   e. Activez le transcodage et sélectionnez un profil "Video - H.264 + MP3 (MP4)"
   f. Puis cliquez sur "Suivant" et complétez la ligne avec un champ "vb=1000". On limite ainsi le débit du flux à 1 Mbps. Votre ligne complète devrait être la suivante :
   `:sout=#transcode{vcodec=h264,vb=1000,scale=Automatique,acodec=mpga, ab=128,channels=2,samplerate=44100}:rtp{dst=192.168.31.1,port=16384, mux=ts} :sout-keep`
   g. Enfin cliquez sur "Flux"
3. Sur la machine H2, utilisez VLC pour recevoir le flux vidéo :
   a. Média > Ouvrir un flux réseau
   b. Renseignez l'adresse du flux : `rtp://192.168.31.1:16384`
   c. Enfin cliquez sur "Lire"
4. Observez la réception du flux sur H2.
5. Confirmez à l'aide d'une capture Wireshark. Assurez-vous que le décodage de protocole RTP est activé dans le menu "Analyser>Protocoles activés".
6. Wireshark affiche des paquets UDP. Pour observer les paquets dans le contexte du protocole RTP : Clic droit > Decode as > RTP.
7. Diminuez progressivement la bande-passante, soit avec la commande "speed", soit en diminuant le *clockrate* de la liaison série. Observez la vidéo sur H2 et le champ RTP "Sequence" des paquets sur votre capture. Que remarquez-vous ?

2 Deuxième Partie : Multidiffusion - Multicast

La multidiffusion est un procédé consistant à diffuser un flux vers plusieurs destinataires. Les techniques de multidiffusion diffèrent de multiples diffusion, car elles répliquent le trafic pour économiser de la bande-passante. C'est pourquoi elles sont souvent utilisées pour la diffusion de contenu audiovisuel.

Nous allons maintenant diffuser le flux vers les deux hôtes H2 et H3.

1. Rétablissez le clockrate pour assurer le bon fonctionnement du flux
2. Supprimez le flux Unicast créé précédemment

2.1 PIM et IGMP

Pour diffuser en Multicast, nous allons utiliser les protocoles PIM et IGMP.

PIM (Protocol-Independent Multicast - RFC 7761) est un protocole de niveau 3 permettant le transport de flux en Multicast sur la partie WAN d'un réseau. C'est lui qui construit les arbres de multidiffusion suivant le protocole de routage sous-jacent, la source et les destinations. PIM dispose de différents modes (Dense et Sparse), mais nous n'entrerons pas dans le détail.

IGMP (Internet Group Management Protocol - RFC 4605) est également un protocole de niveau 3, utilisé dans la partie LAN. Il sert, comme son nom l'indique, à gérer les groupes d'abonnement à des flux multicast.

IGMP gère les différents abonnements sur un LAN, et signale sur le routeur passerelle si le LAN doit être alimenté par certains flux multicast. Á partir de ces informations, PIM raccorde le routeur passerelle aux arbres de diffusions associés aux flux demandés.

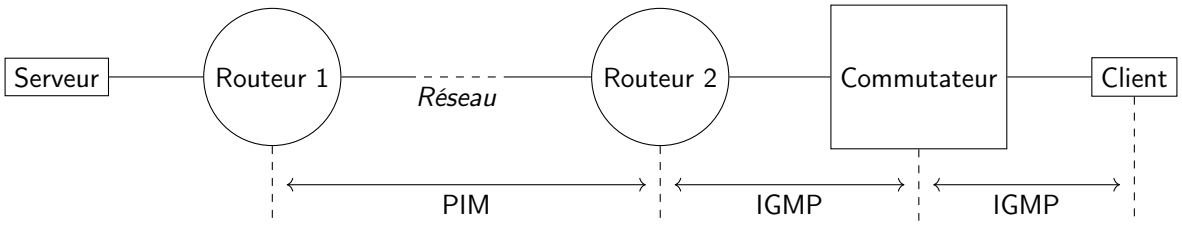


FIGURE 35 – Principe d'architecture multicast exploitant PIM et IGMP

Par défaut, chez Cisco, l'activation de PIM sur une interface active également IGMP par défaut.

1. Activez le routage multicast sur les routeurs avec la commande `ip multicast-routing`
2. Activez le protocole PIM sur toutes les interfaces avec la commande `ip pim sparse-dense-mode`
3. Configurez VLC sur l'hôte H1 pour émettre un flux en multidiffusion, suivant la démarche précédente. Utilisez l'adresse 224.0.1.1 comme destination du flux. Il s'agit de l'adresse du groupe Multicast. **Attention**, par défaut sur VLC, le TTL de la multidiffusion est de 1. Le paquet va être détruit en arrivant au premier routeur. Rajoutez un champ "ttl=100" dans les options "rtp" de la ligne de commande VLC avant de valider le flux.
4. Configurez les deux hôtes H2 et H3 pour recevoir le flux
5. Vérifiez que vous observez bien la vidéo sur les deux hôtes
6. Observez les routes multicast sur les routeurs à l'aide de la commande `show ip mroute`

2.2 Client unique par LAN

1. Observez les messages IGMP sur l'un des hôtes. Décrivez le comportement observé.
2. En capturant les messages IGMP, stoppez la réception sur H3. Décrivez le comportement observé.
3. Relancez la réception du flux sur l'hôte H3. Décrivez le comportement observé.
4. Stoppez la réception du flux sur les hôtes H2 et H3. Décrivez le comportement observé.
5. Observez les routes multicast actives sur les routeurs à l'aide de la commande `show ip mroute active`. Que remarquez-vous ?
6. Relancez la réception du flux sur les hôtes H2 et H3.
7. Diminuez progressivement le clockrate de la liaison série. Observez la vidéo sur les hôtes H2 et H3. Que remarquez-vous ?

2.3 Clients multiples par LAN

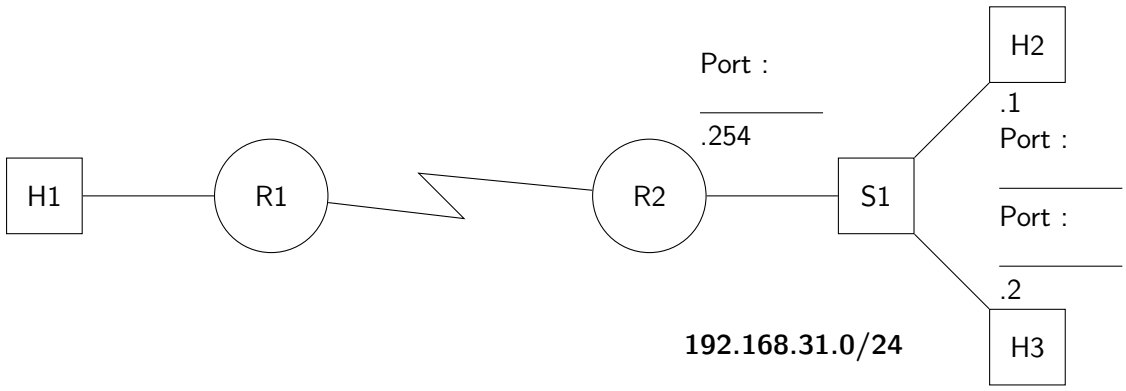


FIGURE 36 – Topologie du réseau

1. Modifiez votre topologie pour insérer un commutateur S1 après R2, de sorte à ce que vos deux hôtes soient dans le même LAN
2. Sur le commutateur S1, désactivez l'IGMP-snooping.
3. Configurez les deux hôtes H2 et H3 pour recevoir le flux.
4. Vérifiez que vous observez bien la vidéo sur les deux hôtes.
5. Laissez le flux connecté sur H2.
6. Stoppez la réception du flux sur l'hôtes H3. Observez l'interface de H3 avec Wireshark. Que remarquez-vous ?
7. Coupez maintenant le flux sur H2. Que remarquez-vous ?

Pour améliorer la situation, vous allez avoir besoin de la fonction appelée "IGMP-snooping". Cette fonction écoute les requêtes IGMP et bloque le flux sur les interfaces du commutateurs qui n'ont pas émis de demande d'abonnement au flux ou qui ont mis fin à l'abonnement.

8. Activez l'IGMP-snooping sur le commutateur S1. Abonnez-vous au flux sur H3, puis coupez-le. Qu'observez-vous dans Wireshark ?

Il existe aujourd'hui d'autres protocoles pour la diffusion multicast, et différentes combinaisons de protocoles, généralement regroupées sous l'appellation "MVPN".

POLYTECH NANCY

3 Nettoyage

Sur tous vos ordinateurs :

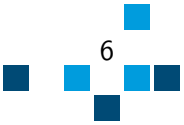
- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

- Tapez la commande `vtp mode transparent`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:vlan.dat`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse



Travaux pratiques - Infrastructures et réseaux opérateur

TP - BGP

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

Éléments de cours

Vous connaissez déjà des protocoles de routage classiques comme OSPF ou RIP. Ce genre de protocoles étaient à l'origine des réseaux, mais avec l'agrandissement d'Internet le nombre de route a explosé. Une nouvelle architecture à été mise en place : les Autonomous Systems (AS).

Un AS est un ensemble de réseaux informatiques intégrés à Internet. Les ISP (Internet Service Provider) sont un exemple typique d'AS. Les AS possèdent un plan de routage interne, qui peut être implémenté via différents protocoles qu'on nomme Interior Gateway Protocol. Il peut s'agir d'OSPF, RIP, IS-IS... Et ils permettent la communication au sein d'un AS. Les AS sont identifiés par un nombre, et portent des préfixes IP, correspondant aux sous-réseau qu'ils contiennent.

Pour interconnecter les AS, et ainsi connecter l'Internet, le Border Gateway Protocol (BGP) a été créé. C'est un protocole de couche 4 d'échange d'informations de routage. Il ne dispose pas de mécanisme d'annonce et de découverte de voisins, comme c'est le cas par exemple dans OSPF. Il faut déclarer tous les voisins manuellement en configuration. On parle généralement de "Peer", car le terme voisin est un peu trompeur : des peers BGP n'ont pas besoin d'être directement connectés.

Une fois un voisinage déclaré, les peers s'échangent une seule fois un ensemble de route. On peut configurer BGP pour échanger les routes connectées, les routes apprises par un protocole donné, des préfixes spécifiques ou l'intégralité de la Routing Information Base (RIB). Les peers BGP au sein d'un AS ne propagent pas les routes apprises, contrairement aux voisinages inter-AS.

Lorsque les peers BGP ont échangé les routes souhaitées, ils ne procèdent ensuite que par mise-à-jour. À moins de recharger le peering, les tables complètes ne sont jamais réémises pour économiser l'overhead de communication.

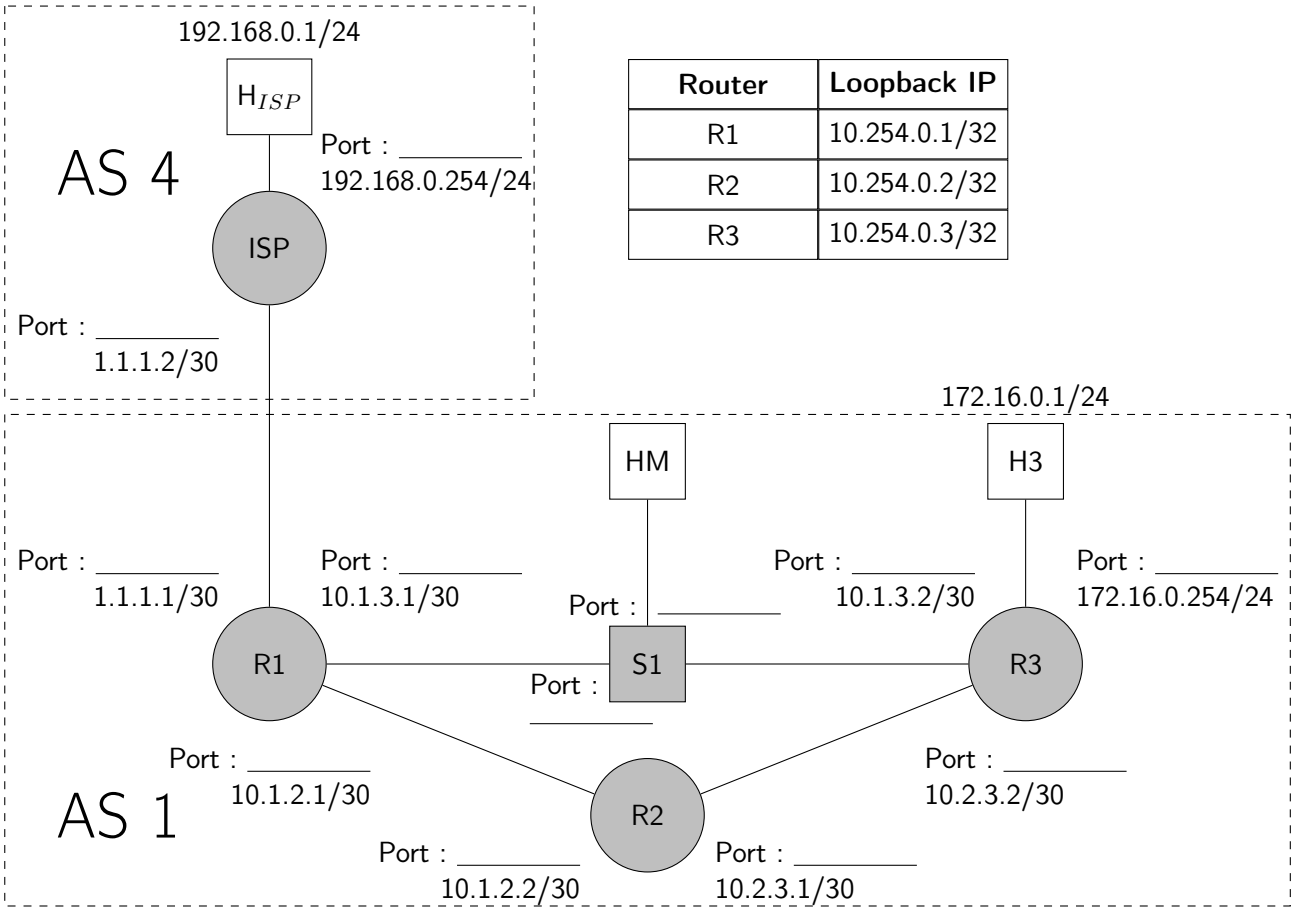
BGP est un protocole dit "Path Vector", c'est-à-dire qu'il propage l'intégralité du détail d'une route (Path), et non pas juste le prochain saut (Vecteur de distance) ou une vision de la topologie (État de lien).

Le routeur utilisant le protocole BGP possède une RIB complète, avec plusieurs routes possibles, mais n'utilise que la meilleure pour chaque réseau dans sa table de routage. La route considérée la meilleure est celle traversant le moins d'AS possible. On parle de "Shortest-AS Path".

Matériel nécessaire

- 4 routeurs CISCO (dont 2 possédant au moins 3 ports)
- 1 commutateur CISCO
- 3 PC sous Windows ou Ubuntu
- 1 câble console (à paires inversées) pour connecter le port série du PC aux ports console

Partie préliminaire : Topologie



Router	Loopback IP
R1	10.254.0.1/32
R2	10.254.0.2/32
R3	10.254.0.3/32

FIGURE 37 – Topologie du réseau

1. Complétez le plan présenté en Fig. 37 avec les ports que vous allez utilisé. Déployez le réseau en n'oubliant pas de configurer les interfaces de Loopback suivant les adresse indiquées dans le tableau.
2. Si vous utilisez des interfaces séries, pensez à définir un clock rate.
3. Mettez en place un routage OSPF uniquement pour les sous-réseaux du 10.0.0.0/8 et le réseau 172.16.0.0/24 de l'AS 1. Cela inclut également les adresses de Loopback. **Ne routez pas le réseau de l'AS 4 ni le réseau d'interconnexion, car ils sont extérieurs à l'AS 1.** Pour rappel, déclarez les réseaux connectés participant au protocole OSPF. Par exemple, la configuration de R3 sera :

```
ip routing
router ospf 1
    network 10.1.3.0 0.0.0.3 area 1
    network 10.2.3.0 0.0.0.3 area 1
    network 172.16.0.0 0.0.0.255 area 1
    network 10.254.0.3 0.0.0.0 area 1
```

4. Vérifiez la connectivité au sein de chaque AS.
5. Sur S1, configurez un port-mirroring du port connecté à R1 vers le port connecté vers HM. Vous aurez besoin des commandes suivantes. L'argument `both` permet de copier le trafic entrant et sortant.

```
Switch(config)#monitor session 1 source interface fa0/1 both
Switch(config)#monitor session 1 destination interface fa0/2
```

6. Vérifiez que votre mirroring est bien configuré avec la commande `show monitor session 1`.
7. Vérifiez que le mirroring fonctionne en effectuant un ping entre R1 et R3. Que devriez-vous observez sur HM ?

1 Première Partie : eBGP

On parle de eBGP (exterior BGP) lorsqu'on interconnecte différents AS. C'est typiquement ce qu'on retrouve entre les différents acteurs de l'Internet. Dans cette partie, nous allons faire en sorte que l'AS 1 et l'AS 4 établissent un voisinage BGP et échangent des routes.

Note : dans la réalité, on ne propagerait pas des routes vers des réseaux privés. On mettrait en place le protocole NAT, mais pour simplifier l'exercice nous allons en faire abstraction.

1.1 Établissement d'un voisinage

1. Dans un premier temps vous allez configurer R1.
2. Rentrez en mode de configuration BGP avec la commande `router bgp 1` pour l'AS 1.
3. Pour voir les interactions BGP dans la console, activez `bgp log-neighbor-changes`
4. Déclarez ensuite que vous travaillez dans une famille d'adresse en IPv4 unicast.
5. Déclarez enfin le voisin BGP `neighbor` par l'adresse de son interface directement connectée à R1, et son numéro d'AS 4.
6. Connectez-vous maintenant sur ISP, et effectuez la configuration symétrique.
7. À l'aide de la commande `show bgp ipv4 unicast neighbors` ou `show ip bgp neighbors`, observez le voisinage établi entre R1 et ISP.

1.2 Redistribution de routes

1. R1 peut-il contacter H_{ISP} ?
2. Observez les routes connues via BGP avec la commande `show bgp all summary`
3. Sur ISP, ajoutez à la configuration l'option `redistribute connected`. Quel est l'effet de cette commande ?
4. Observez à nouveau les routes connues via BGP sur R1 est ISP.
5. R1 peut-il contacter H_{ISP} ?
6. Configurez maintenant R1 pour qu'il redistribue les routes apprises via OSPF. Qu'observez-vous dans la RIB de ISP ?

2 Deuxième Partie : iBGP

2.1 Voisinage BGP

1. Lancez une capture sur HM.
2. À l'aide des mêmes commandes que pour l'eBGP, établissez des voisinages BGP R1-R2, R1-R3 et R2-R3. Utilisez les adresses des interfaces correspondant aux liaisons.
3. Vérifiez que les sessions sont bien établies et que les routes sont propagées.
4. H_{ISP} et H3 peuvent-ils se contacter ?
5. Du point de vue de R3, quel est le prochain saut pour contacter le réseau de H_{ISP} ?
6. Sur R1, dans la configuration de famille d'adresse IPv4 unicast, utilisez la commande l'option `next-hop-self` pour le voisin R3. Quel est maintenant le prochain saut de R3 vers H_{ISP} ? H_{ISP} et H3 peuvent-ils se contacter ?
7. Observez les paquets échangés par R1 et R3 sur votre capture. Quels paquets intéressants relevez-vous ? Quels champs utiles identifiez-vous ?

2.2 Utilisation des Loopbacks

1. Coupez maintenant la liaison entre S1 et R3.
2. H_{ISP} et H3 peuvent-ils se contacter ?
3. Que pouvez-vous dire de l'état du BGP sur R3 ?
4. Modifiez votre configuration BGP sur R1 et R3 pour utiliser les adresses de Loopback pour définir le voisin.
5. H_{ISP} et H3 peuvent-ils se contacter ?
6. Que pouvez-vous dire de l'état du BGP sur R3 ?
7. Quel est alors l'intérêt d'utiliser les adresses de Loopback comme adresse de voisin BGP ?
8. Reconnectez la liaison entre S1 et R3.

2.3 Route reflector

1. Supprimez le voisinage BGP entre R1 et R3.
2. H_{ISP} et H3 peuvent-ils se contacter ?
3. Configurez R2 pour être route-reflector pour R1 et R3.
4. Quelles routes sont maintenant apprises sur R1, R2 et R3 ?
5. H_{ISP} et H3 peuvent-ils se contacter ?
6. Observez votre miroir. Par où passent les échanges BGP ?
7. Dans un réseau d'une dizaine de routeurs, combien de voisinages BGP sont nécessaires sans et avec route-reflector ?
8. Quel est l'intérêt d'un route reflector ?

POLYTECH NANCY

3 Nettoyage

Sur tous vos ordinateurs :

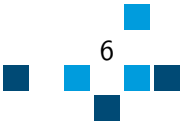
- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

- Tapez la commande `vtp mode transparent`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:vlan.dat`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse



Travaux pratiques - Infrastructures et réseaux opérateur

TP - IPv6

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

Éléments de cours

L'IPv6 est le remplaçant logique de l'IPv4, développé de longue date en prévision du manque d'adresses inévitable. Outre le fait que l'adressage IPv6 offre un bien plus grand nombre d'adresses, il inclut également des changements utiles, et implique des évolutions des protocoles de niveau 3. En effet, IPv6 et IPv4 ne sont pas intéropérables.

Les adresses IPv6 utilisent 128 bits (au lieu de 32 en IPv4), et sont généralement écrites sous la forme suivante : 8 groupes de 4 chiffres hexadécimaux [1]. Par exemple :

`2001:0db8:0000:0000:0000:ff00:0042:8329`

Afin d'en faciliter l'écriture et la lecture, deux règles existent : les zéros au début d'un groupe sont retirés, et **la plus longue** section constituée d'au moins 2 blocs de zéros est abrégée en "::". Pour reprendre l'exemple précédent :

`2001:db8::ff00:42:8329`

La notion de masque existe comme en IPv4, un "/X" correspondant à X bits réservés.

Les blocs d'adresses les plus courants sont :

Blocs d'adresses	Utilisation
::/0	Route par défaut
::1/128	Adresse de rebouclage locale
fc00::/7	Adresses des réseaux privés
fe80::/10	Adresses *link-local*
2000::/3	Adresses globales (Internet)
ff00::/8	Adresses de multidiffusion
ff02::1/128	Adresse de multidiffusion à tous les noeuds (diffusion)

À noter, certains des blocs du tableau sont des sous-blocs d'autres.

La seule nouveauté pour vous est la notion d'adresse *link-local*. Il s'agit simplement d'une adresse réservée à un lien, pour les communications entre voisins connectés par un même domaine de diffusion. Ces adresses ne sont pas routées, et servent essentiellement dans des protocoles de découverte de voisin et d'échange de routes. Par défaut, une adresse link-local est générée pour toute interface.

Ces adresses link-local sont particulièrement utiles, car l'IPv6 autorise l'attribution de plusieurs adresses IP à une même interface. Seule l'adresse link-locale est unique par interface, les autres adresses n'ont même pas besoin d'appartenir au même LAN des deux côtés d'une liaison. Soyez vigilants en tapant vos commandes, si vous attribuez une adresse IP à une interface, elle s'ajoutera à la liste au lieu de remplacer l'ancienne.

1. Pour rappel, les chiffres hexadécimaux sont 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f

Matériel nécessaire

- 2 routeurs CISCO 2901
- 2 commutateurs CISCO 2960 Plus
- 3 PC sous Windows ou Ubuntu
- 1 câble console

1 Première Partie : mise en place du réseau en configuration manuelle

Dans un premier temps, câblez le réseau de la Figure 38.

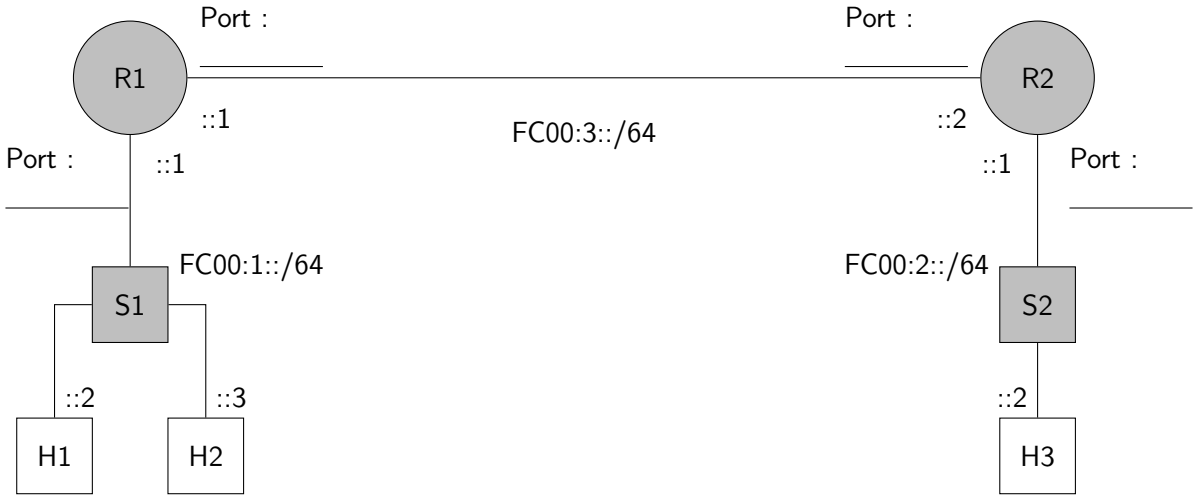


FIGURE 38 – Topologie du réseau

1.1 Configuration des hôtes

Assurez-vous d'avoir activé la prise en charge de l'IPv6 sur la carte réseau des hôtes, et attribuez les adresses conformément à la Figure 38, et spécifiez une adresse de passerelle.

1.2 Configuration des commutateurs

1. Nommez les commutateurs.
2. Activez la commutation IPv6 sur les commutateurs en modifiant le gestionnaire de base de données de commutation (SDM) de la manière suivante :

```
Switch# configure terminal
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# end
Switch1# reload
```

3. Vérifiez la connectivité entre H1 et H2.

1.3 Configuration des routeurs

Utilisez un câble console pour configurer vos équipements. Nous activerons Telnet plus tard, après avoir configuré le plan d'adressage IPv6.

1. Nommez les routeurs
2. Activez le routage IPv6 à l'aide des commande suivantes :

```
Router> enable
Router# configure terminal
Router(config)# ip routing
Router(config)# ipv6 unicast-routing
```

3. Attribuez les adresses IPv6 sur les différentes interfaces de vos routeurs en respectant le schéma d'adressage de la Figure 38. Vous pouvez également attribuer une adresse link-local à chaque interface de vos routeurs, mais ce n'est pas nécessaire.

```
Router(config)# interface g0/0
Router(config-if)# ipv6 address FC00:1::1/64
Router(config-if)# no shutdown
```

4. Vérifiez la connectivité entre les différents éléments.

Vous observerez que beaucoup de commandes sont similaires à celles en IPv4 en y rajoutant "`ipv6`".

2 Deuxième Partie : routage

2.1 Configuration du routage statique

1. Ajoutez des routes statiques sur les routeurs (utilisez bien l'adresse de prochain saut, pas l'interface) :

```
Router(config)# ipv6 route network/mask next-hop
```

2. Effectuez des pings ICMP pour valider la connectivité entre H1, H2 et H3.

2.2 Routage dynamique : OSPFv3

Retirez les routes statiques. Vous allez utiliser le protocole OSPFv3 spécifié dans la RFC 5340. L'une des différences majeures avec OSPFv2 est qu'il ne fonctionne pas par sous-réseau, mais par interface.

1. Pour chaque routeur, activez le routage OSPF dans le mode de configuration globale IPv6. Utilisez le numéro d'instance 100.
2. Dans la configuration OSPF, définissez un `router-id` sous la forme d'un adresse IPv4. Il s'agit simplement d'un identifiant au sein du protocole, il n'y a pas de conflit avec le plan d'adressage IPv6. Utilisez les `router-id` 1.1.1.1 et 2.2.2.2.
3. Dans chacune des interfaces, activez OSPF en IPv6 pour le numéro d'instance 100, dans l'aire 1.
4. Vérifiez le fonctionnement du routage à l'aide de pings ICMP.
5. Affichez l'état et la configuration OSPFv3 à l'aide d'une commande `show`.
6. Observez la table de routage IPv6.

3 Troisième Partie : Attribution des adresses hôtes en IPv6

Il existe plusieurs moyens d'attribuer des adresses aux hôtes en IPv6 :

- Manuellement, de manière similaire à ce que vous avez fait dans la première partie ;
- Par DHCP, de manière similaire à l'IPv4, autrement appelé DHCPv6 ou Stateful (car le serveur DHCP conserve l'"état" de l'adresse, le bail) ;
- Par autoconfiguration, les hôtes s'attribuent eux-même une adresse à partir de messages émis par la passerelle du réseau local. On parle d'attribution SLAAC (StateLess Address AutoConfiguration).

3.1 Configuration des adresses avec DHCPv6

Dans cette partie, vous allez déployer un DHCP sur R1, pour que les hôtes H1 et H2 puissent obtenir des adresses. Notez qu'on aurait également pu utiliser le commutateur S1 comme DHCP.

1. Désactivez la configuration manuelle IPv6 sur les hôtes H1 et H2 et activez la configuration automatique.
2. Désactivez l'interface de R1 vers les hôtes avec un "shutdown".
3. En mode de configuration globale, créez un pool d'adresses ipv6 pour le DHCP "ipv6poolA". Définissez "ipv6.com" comme nom de domaine, le préfixe FC00:1::/64 pour les adresses à distribuer. Attention, la commande à utiliser est mal renseignée dans la documentation Cisco, il faut utiliser `address prefix FC00:1::/64`.
4. Définissez l'interface R1 vers les hôtes comme serveur DHCP utilisant le pool "ipv6poolA". Utilisez également la commande suivante, pour vous assurer que les hôtes du LAN connecté n'accepteront qu'une configuration par DHCPv6 :

```
R1(config-if)# ipv6 nd managed-config-flag
```

5. Vérifiez que les paramètres ont bien été pris en compte avec "show ipv6 interface".
6. Lancez la capture Wireshark sur l'interface Ethernet de H1.
7. Réactivez l'interface G0/0 de R1.
8. Si besoin, réinitialisez la configuration réseau sur les hôtes, et vérifiez qu'ils ont bien reçu une adresse.
9. Appliquez un filtre DHCPv6 sur Wireshark pour simplifier l'observation et trouvez le paquet correspondant à un échange d'information DHCPv6. Vous devriez trouver l'adresse IPv6 qui a été attribuée, l'adresse du serveur DNS et le nom de domaine. Notez ces informations.
10. Vérifiez sur R1 le fonctionnement du DHCPv6 à l'aide des commandes : "show ipv6 dhcp binding" et "show ipv6 dhcp pool". Combien de clients actifs observez vous ? Combien d'adresses ont été distribuées ?
11. Vérifiez la connectivité des hôtes H1 et H2 avec le LAN connecté à R2.
12. De quel type est l'adresse de passerelle définie sur les hôtes ? Étant donné qu'en DHCPv6 il est impossible d'émettre une adresse de passerelle, comment les hôtes en ont ils obtenu une ?

3.2 Configuration automatique des adresses sans état SLAAC

Dans cette partie, nous allons faire en sorte que le commutateur S2 annonce sur son LAN que la configuration d'adresse est en mode SLAAC.

1. Désactivez la configuration manuelle IPv6 sur l'hôte H3 et activez la configuration automatique.
2. Désactivez l'interface G0/0 de R2.
3. Configurez l'interface `"vlan 1"` de S2 de manière à déclarer l'autoconfiguration des adresses IPv6. Rappelez-vous que le VLAN 1 est le VLAN par défaut, et il correspond donc à tout le LAN dans ce cas.
4. Lancez la capture Wireshark sur l'interface Ethernet de H3.
5. Réactivez l'interface G0/0 de R2.
6. Si besoin, réinitialisez la configuration réseau sur les hôtes, et vérifiez qu'ils ont bien une adresse IPv6 calculée automatiquement.
7. Appliquez un filtre ICMPv6 sur Wireshark pour simplifier l'observation et trouvez un paquet correspondant à l'annonce du routeur R1. Analysez la couche du protocole ICMPv6. Observez les valeurs qui montrent que l'autoconfiguration est activée. Quelles sont les adresses sources et destination du paquet ?
8. Vérifiez la connectivité de l'hôte H3 avec le LAN connecté à R1.

3.3 Configuration des adresses avec DHCPv6 et SLAAC

Dans certains cas, il peut être nécessaire de combiner les deux approches précédentes. Par exemple, pour diffuser l'adresse du DNS, SLAAC est insuffisant.

Dans cette partie, vous allez déployer un DHCP sur R2, pour que l'hôte H3 puisse obtenir l'adresse du DNS, mais se configure toujours seul.

1. Désactivez l'interface G0/0 de R2.
2. En mode de configuration globale, créez un pool d'adresses ipv6 pour le DHCP "ipv6poolB". Définissez 2001:DB8:CAFE:1::ABCD comme adresse du serveur DNS.
3. Définissez l'interface G0/0 de R2 comme serveur DHCP utilisant le pool "ipv6poolB". Utilisez également la commande suivante, pour vous assurer que les hôtes du LAN connecté acceptent les informations DHCP, mais configurent bien leur IP en SLAAC :

```
R1(config-if)# ipv6 nd other-config-flag
```

4. Vérifiez que les paramètres ont bien été pris en compte à l'aide de la commande "show ipv6 interface".
5. Lancez la capture Wireshark sur l'interface Ethernet de H3.
6. Réactivez l'interface G0/0 de R2.
7. Si besoin, réinitialisez la configuration réseau sur l'hôte, et vérifiez qu'il a bien reçu l'adresse du DNS.
8. Appliquez un filtre ICMPv6 sur Wireshark pour simplifier l'observation et trouvez un paquet correspondant à l'annonce du routeur R2. Analysez la couche du protocole ICMPv6. Observez les valeurs qui montrent que l'adresse n'a pas été configurée via DHCP.
9. Appliquez un filtre DHCPv6 sur Wireshark pour simplifier l'observation et trouvez le paquet correspondant à un échange d'information DHCPv6. Vous devriez retrouver l'adresse du serveur DNS.
10. Vérifiez sur R2 le fonctionnement du DHCPv6 à l'aide des commandes : "show ipv6 dhcp binding" et "show ipv6 dhcp pool". Combien de clients actifs observez vous ? Combien d'adresses ont été distribuées ?
11. Vérifiez la connectivité des hôtes H1 et H2 avec le LAN connecté à R2.
12. Quelle est l'adresse du serveur DNS définie sur les hôtes ?

POLYTECH NANCY

4 Nettoyage

Sur tous vos ordinateurs :

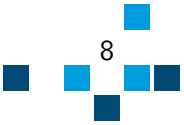
- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

- Tapez la commande `vtp mode transparent`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:vlan.dat`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse



Travaux pratiques - Infrastructures et réseau opérateur

TP - Management de réseau

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

Note : Ce TP n'est pas réalisable sur Packet Tracer

Matériel nécessaire

- 2 routeurs CISCO
- 1 commutateurs CISCO
- 2 PC sous Windows ou Ubuntu
  - Un gérant et un agent SNMP installés sur les hôtes (sur Linux `snmp` et `snmpd`)
  - Un explorateur de MIB (sur Linux `qtmib`) installé sur un hôte
  - Un serveur Zabbix installé sur un hôte
- 1 câble console

Partie préliminaire : Topologie

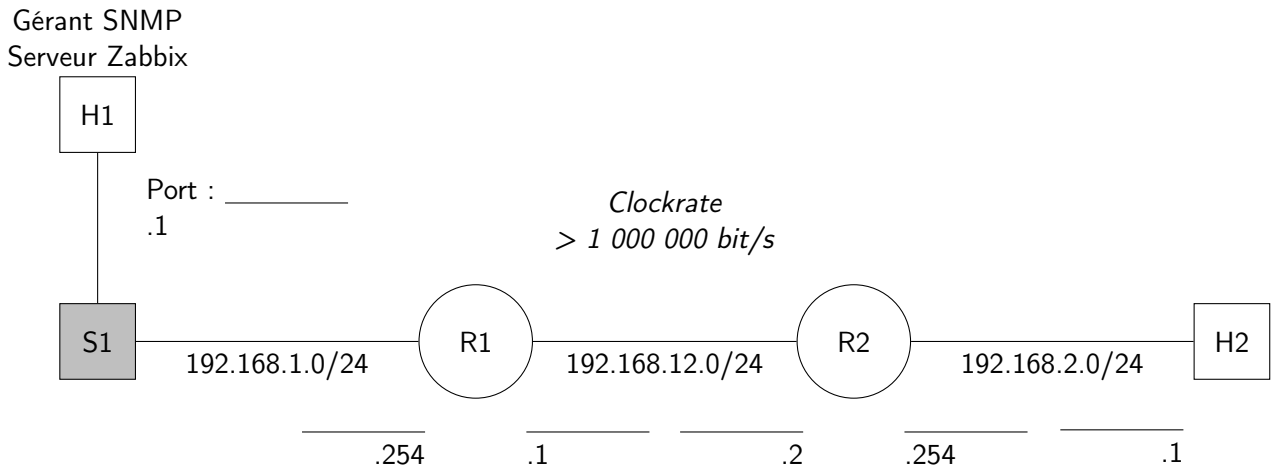


FIGURE 39 – Topologie du réseau

Mettez en place le réseau présenté sur le schéma avec un routage statique. Utilisez-les adresses présentes sur le schéma. Complétez le schéma avec les ports que vous utiliserez.

Vous devez configurer une adresse sur le VLAN 1 de S1. Il s'agit d'une adresse de gestion, qui permet de le contrôler à distance. Le switch n'est pas pour autant capable de routage, mais il est joignable en IP.

Si vous utilisez une liaison série entre R1 et R2, vous devez augmenter suffisamment le *clockrate* de la liaison série. Essayez d'être au bien delà de 1 000 000 bits/s (1 Mbit/s). Il se peut qu'un de vos routeurs soit physiquement limitant. Essayez de changer le sens du câble. Si vous ne dépassez pas 1 Mbit/s, vous aurez peut-être besoin de changer de routeur.

1 Première Partie : SNMP

Le protocole SNMP (Simple Network Management Protocol) est défini dans la RFC 3416 comme un protocole d'échange d'informations (configurations et mesures) utilisées pour gérer un réseau. Il s'agit d'un protocole de couche application basé sur IP/UDP. On peut résumer le protocole SNMP en trois aspects :

- Collecte d'information : un manager peut interroger des équipements pour obtenir des informations sur sa configuration, sur l'état des protocoles, sur le statut des ports, sur des compteurs...
- Configuration d'équipements : bien que peu utilisé, SNMP permet également à un manager de configurer des équipements.
- Alertes (ou Traps) : les équipements réseau peuvent générer des alertes appelés "Traps SNMP" pour signaler un évènement particulier, une panne, un dégradation de service...

On peut noter qu'il existe d'autres protocoles aux capacités similaires tels que Netconf, qui est notamment plus pratique pour ses fonctions de configuration, basées sur du XML ou du JSON.

Le protocole SNMP est basé sur un modèle "Manager-Agent". Le manager est l'entité qui s'exécute sur le poste de supervision, qui envoie des requêtes de lecture (GET) ou d'écriture (SET). L'agent est le processus qui s'exécute sur un nœud du réseau qu'on souhaite gérer. L'agent est capable de répondre au requêtes du manager, et peut émettre des Traps.

Le protocole SNMP se base sur des MIB : Management Information Base. Une MIB est un ensemble d'informations organisée de manière hiérarchique. Les MIBs sont accessibles par d'autres protocoles que SNMP. Certaines sont spécifiques suivant les constructeurs et d'autres, sont des standards, comme la MIB-II, définie dans la RFC 1213. Les données d'une MIB sont identifiées par un OID unique (Object IDentifier). Un OID est formé par une suite de nombre séparés par un point, et on y retrouve la hiérarchie des données.

La MIB-II se place dans la hierarchie standard de la manière suivante : iso.org.dod.internet.mgmt.1, ou 1.3.6.1.2.1. en nombre. La MIB-II est divisée en différents sous-groupes, dont le nom est assez explicite :

Nom	OID	Description
system	1.3.6.1.2.1.1	Objets associés au système : nom, temps de fonctionnement...
interfaces	1.3.6.1.2.1.2	Objets associés aux interfaces : état, octets transmis, erreurs...
at	1.3.6.1.2.1.3	Champs associés à la translation d'adresse (déprécié).
ip	1.3.6.1.2.1.4	Objets associés au protocole IP : adresse, routage...
icmp	1.3.6.1.2.1.5	Objets associés au protocole ICMP : réceptions, erreurs...
tcp	1.3.6.1.2.1.6	Objets associés au protocole TCP : état des connexions...
udp	1.3.6.1.2.1.7	Objets associés au protocole UDP : statistiques...
egp	1.3.6.1.2.1.8	Objets associés au protocole EGP (aujourd'hui déprécié).
transmission	1.3.6.1.2.1.10	Utilisé pour contenir d'autres sous-arbres, dépendants du média.
snmp	1.3.6.1.2.1.11	Objets associés au protocole SNMP : statistiques...

TABLE 1 – Sous-arbres de la MIB-II

Par exemple, la variable associée au temps de fonctionnement d'un équipement est stockée dans `"sysUpTime"` correspondant à l'OID 1.3.6.1.2.1.1.3, dans le sous-arbre système. On peut aussi écrire "mib2.system.3".

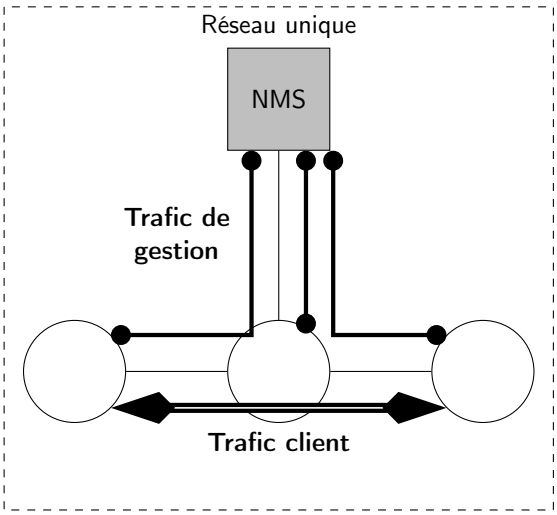
Dans cette partie, vous allez découvrir le fonctionnement du protocole SNMP et observer comment il peut servir à gérer un équipement.

1. Activez les agents SNMPv2 sur tous les équipements, en lecture sur la communauté "public".
   - Il devrait être activé sur les hôtes, assurez-vous que l'agent écoute sur toutes les adresses IP. Sur Linux, le fichier de configuration se trouve dans `/etc/snmp/snmpd.conf`
   - Sur les switches en particulier, vous aurez besoin d'une adresse de gestion. En mode de configuration, accédez à **l'interface** vlan 1, et attribuez-lui une adresse IP.
   - Sur les switches et les routeurs utilisez la commande `snmp-server community public ro`.
2. Depuis H1, à l'aide de la commande `snmpget`, relevez le temps d'activité `sysUpTime` (OID 1.3.6.1.2.1.1.3.0) de chacun des équipements S1, R1 et H2.
3. À l'aide de Wireshark, capturez l'échange de trames SNMP. Quels champs intéressants identifiez-vous ?
4. À l'aide de la commande `snmpwalk`, observez les champs possibles de la MIB-II.
5. Utilisez maintenant un explorateur de MIB (par exemple `qtmib` sur Linux) pour trouver l'OID correspondant au nombre d'octets transmis par l'interface de H2. Effectuez une requête GET.
6. Effectuez un ping entre H1 et H2, puis observez à nouveau le compteur de l'interface de H2.
7. Essayez à l'aide de la commande `snmpset` de modifier l'adresse de l'interface de H2 depuis H1.

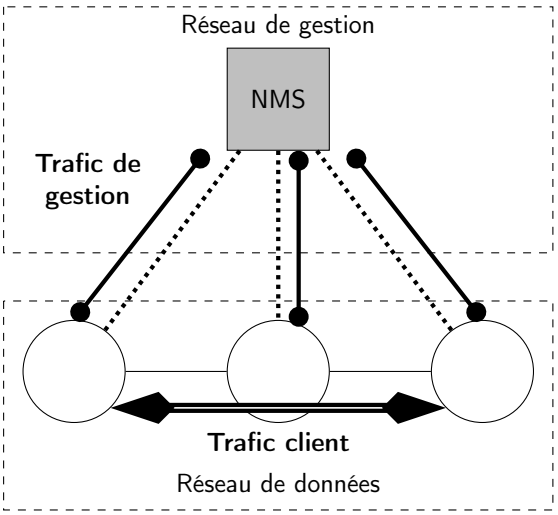
2 Deuxième Partie : NMS

Un NMS (Network Management Software) est un logiciel permettant la gestion d'un réseau informatique. On l'associe généralement aux fonctions suivantes (entre autres) : surveillance (monitoring), ingénierie de trafic (provisionning), configuration, gestion des licences...

Les NMS utilisent généralement des protocoles comme SNMP pour interagir avec le réseau. On définit deux manières de placer le NMS dans un réseau, suivant le réseau qu'il utilise pour joindre les équipements. Si le NMS est placé dans le réseau et suit le même plan de routage que le trafic, on parle de gestion Intrabande (Inband management). Si le NMS utilise un réseau de contrôle, indépendant du réseau du trafic client, alors on parle de gestion Extrabande (Outband management).



(a) Inband Management



(b) Outband Management

Dans ce TP vous allez utiliser le NMS Open Source Zabbix avec le protocole SNMP, déployé en Inband.

2.1 Ajouter des équipements au NMS

1. Utilisez le serveur Zabbix sur H1 avec la commande :

```
# service zabbix-server start
```

2. Accédez à l'interface à l'URL `127.0.0.1/zabbix`, les identifiants sont par défaut (`Admin, zabbix`)
3. Configurez les équipements pour être gérés par le serveur :
   a. Dans le menu Configuration > Hosts, cliquez sur "Create Host"
   b. Définissez un hostname, associez l'hôte au groupe "Discovered Host", renseignez l'adresse IP de l'hôte dans les champs "SNMP", supprimez l'adresse du champ "Agent".
   c. Dans l'onglet "Template", sélectionnez un modèle "Generic SNMPv2" pour les hôtes ou "Net Cisco IOS SNMPv2" pour les routeurs et le switch, cliquez sur "Add".
   d. Dans l'onglet "Trigger", quelles alarmes ont été créées ? Avec quelle niveau de gravité ?
4. Coupez la liaison entre R2 et H2, et observez la remontée d'alarme dans la page Monitoring > Dashboard. Si nécessaire, rechargez la page.
5. Rétablissez la liaison, et vérifiez le fonctionnement avec un ping. Qu'observez-vous ?
6. Coupez maintenant la liaison entre S1 et R1. Qu'observez-vous si vous coupez à nouveau la liaison entre R2 et H2 ?
7. Que pouvez-vous dire de la méthode de gestion Inband ?

2.2 Surveillance de liaisons

Vous allez maintenant voir qu'il est possible de surveiller en détail les liaisons. Ce genre d'outil peut permettre une détection de problème, ou fournir des données pour une future ingénierie de trafic.

1. Dans le menu Configuration > Hosts, cliquez sur l'onglet "Graphs".
2. Créez un graphe observant le temps de réponse ICMP de H2.
3. Observez-le sur l'interface dans le menu Monitoring > Graphs.
4. Dans le menu Configuration > Hosts, cliquez sur l'onglet "Discovery rules".
5. Modifiez l'intervalle de détection de la règle "Network interfaces discovery" à 10s.
6. Créez un graphe observant la bande passante entre R1 et R2.
7. Observez-le sur l'interface dans le menu Monitoring > Graphs.
8. À l'aide de l'outil `iperf`, générez différents niveaux de trafic, et observez-les sur le graphe.

POLYTECH NANCY

3 Nettoyage

Sur tous vos ordinateurs :

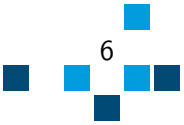
- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

- Tapez la commande `vtp mode transparent`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:vlan.dat`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse



Travaux pratiques - Infrastructures et réseaux opérateur

TP - QoS

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

Éléments de cours

Lors de la conception d'une architecture réseau, les caractéristiques de performance d'un réseau sont à prendre en compte. Certains services nécessitent une forte disponibilité, d'autres une faible latence, et très souvent plusieurs paramètres à la fois.

Le terme Qualité de Service (QoS) regroupe toutes les techniques et technologies qui permettent de gérer un trafic en termes de débit, d'amélioration et stabilisation de latence, réduction des pertes et augmentation de la disponibilité.

Une bonne utilisation des outils de QoS permet à un opérateur de prendre des engagements forts sur les services fournis, notamment dans des Service Level Agreement (SLA).

La QoS passe souvent par :

- la sélection de routes, par exemple en pondérant des protocoles de routage ;
- la mise en forme du trafic (Shaping), qui permet de limiter le débit de trafics identifiés ;
- l'ordonnancement des paquets, c'est-à-dire la gestion des files d'attentes internes aux cartes de commutation d'un équipement.

Matériel nécessaire

- 2 routeurs CISCO 2901 ou 4321
- 2 PC sous Windows ou Ubuntu
- 1 câble console (à paires inversées) pour connecter le port série du PC aux ports console

Partie préliminaire : Topologie

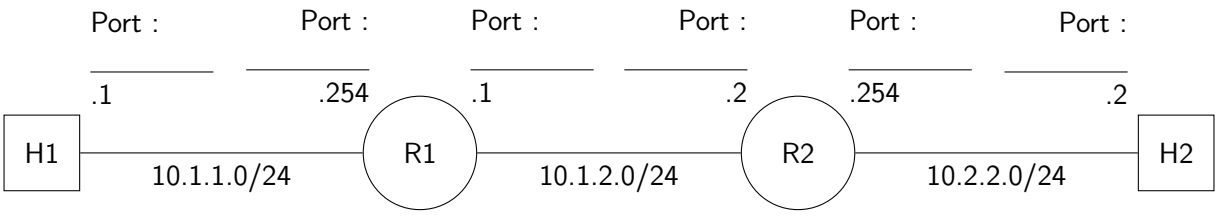


FIGURE 40 – Topologie du réseau

Mettez en place le réseau présenté sur le schéma avec un routage statique. Utilisez-les adresses présentes sur le schéma. Complétez le schéma avec les ports que vous utiliserez.

1 Première Partie : QoS - Marquage de trafic

- Sur R1, créez une ACL étendue 100 qui correspond au trafic UDP. Nous n'allons pas appliquer cet ACL comme Firewall, elle servira simplement à identifier du trafic. Vous aurez besoin de la commande : `access-list 100 permit udp any any`
- Sur R1, créez une ACL étendue 101 qui correspond au trafic TCP.

Les class-map sont des objets qui permettent au routeur de trier le trafic suivant différents critères.

- Sur R1, en mode de configuration globale, créez une class-map UDP qui doit correspondre à l'ACL 100.
- Quelle est la différence entre une class-map match-all et match-any ?
- Créez également une class-map TCP qui correspond à l'ACL 101.
- À l'aide de la commande `show class-map`, combien de class-map observez-vous ?
- Quels autres critères qu'une ACL peuvent utiliser les class-map ? (Pensez à utiliser le " ?")

Les policy-map sont des objets qui permettent au routeur d'appliquer différentes actions à du trafic classé par le routeur. Dans un premier temps, nous allons simplement marquer le trafic.

- Sur R1, créez une policy-map MARK, qui doit marquer le champ DSCP du trafic UDP à 0 (ou BE) et TCP à EF.
- Qu'est-ce que le champ DSCP ?
- L'objectif est de marquer le trafic entrant dans le réseau reliant R1 à R2. Imaginez qu'entre R1 et R2 se trouve votre réseau opérateur, sur lequel vous utilisez le trafic marqué pour gérer votre bande-passante. À quelle interface et dans quelle direction allez-vous appliquer la policy-map MARK ? Vous aurez besoin de la commande `service-policy`.
- À l'aide d'iperf, créez du trafic UDP et TCP simultané de H1 vers H2.
- À l'aide de Wireshark, observez les paquets qui arrivent sur H2. Que retrouvez-vous ?
- Quelle commande *show* vous permet d'observer le nombre de paquet ayant été traités par la policy-map ?

2 Deuxième Partie : QoS - Shaping de trafic

- À l'aide de la commande `speed`, limitez la liaison entre R1 et R2 à 100 Mbit/s.
- Utilisez iperf entre H1 et H2 pour valider la bande-passante totale dont vous disposez.
- À l'aide de la commande `show interfaces`, identifiez la méthode actuelle de gestion de file d'attente de l'interface de R1 vers R2.
- Sur R1, créez une class-map EF qui filtre les paquets marqués "EF", et une class-map BE.
- Sur R1, créez une policy-map SHAPE qui réserve 10% de bande-passante à la classe BE, et 89% à la classe EF.
- Appliquez cette policy-map en sortie de R1 vers R2.
- Quelle est maintenant la méthode de file d'attente de l'interface ?
- À l'aide d'iperf, créez 100 Mbits/s de trafic UDP et 100 Mbits/s de trafic TCP simultané de H1 vers H2.
- Que remarquez-vous ?

POLYTECH NANCY

3 Nettoyage

Sur tous vos ordinateurs :

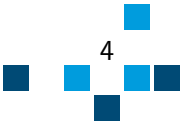
- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

- Tapez la commande `vtp mode transparent`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:vlan.dat`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse



Travaux pratiques - Sujets complémentaires

TP - Connectique WAN et LAN

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

L'objectif de ce TP est, dans un premier temps, de se familiariser avec les techniques de câblage et de test de validité des supports physiques des réseaux de communication de données, en particulier pour les câbles RJ45 et la fibre optique. Dans un second temps, vous aborderez la connectivité sans fil Wi-Fi.

Éléments de cours

L'architecture des réseaux de communication commence avec les lignes de transmission des éléments binaires qui relient les nœuds de transfert aux équipements terminaux des utilisateurs. Les câbles métalliques, la fibre optique et les ondes hertziennes en sont les principaux supports. A ces supports physiques s'ajoutent de nombreux équipements intermédiaires, tels que prise de connexion, coupleur, adaptateur, etc. Les équipements réseau (routeurs, switch) complètent la partie physique de l'architecture des réseaux. Enfin, différentes topologies permettent l'interconnexion des équipements utilisateurs et des nœuds du réseau.

La paire de fils torsadés

Elle est le support de transmission le plus simple (cf figure 41). Elle est formée de deux conducteurs mono ou multibrin, recouvert d'un isolant et torsadée l'un par rapport à l'autre. Ces fils métalliques sont particulièrement adaptés à la transmission d'information sur de courtes distances.

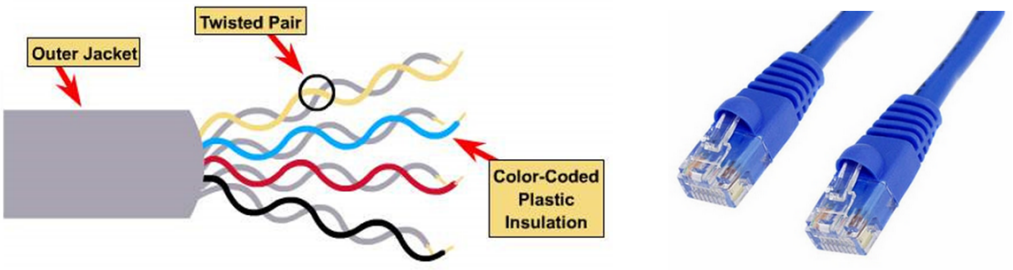


FIGURE 41 – Fils torsadés sans blindage

Le câble coaxial

Il est constitué d'un fil conducteur mono ou multi brin (âme), entouré d'un isolant, puis d'une tresse de blindage constituant le second conducteur (cf figure 42). L'isolant permet de limiter les perturbations dues au bruit externe. Bien qu'il perde du terrain par rapport à la fibre optique, ce support reste encore très utilisé.

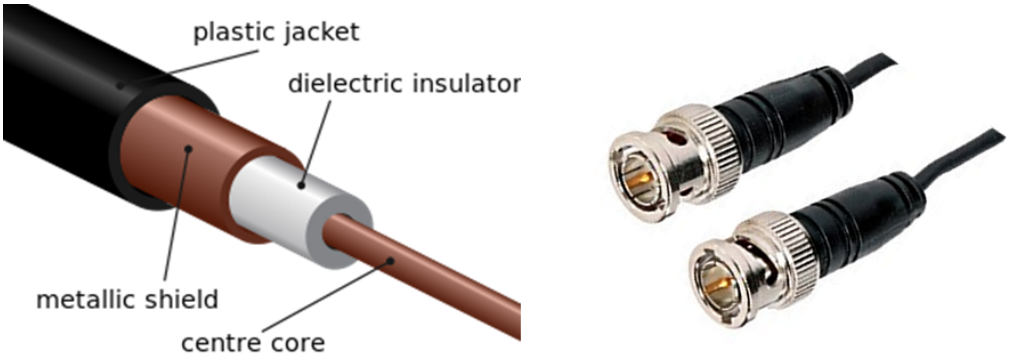


FIGURE 42 – Câble coaxial

La fibre optique

Dans les fils métalliques, les informations sont transmises par le biais d'un courant électrique modulé. Avec la fibre optique c'est un faisceau lumineux modulé qui est utilisé. Ainsi, une fibre optique est un guide d'onde créé dans un matériau transparent (cf figure 43). Deux matériaux sont utilisés : le verre ou le plastique. Les fibres en verre sont les plus performantes mais elles présentent un certain nombre d'inconvénients : difficulté de raccordement, fragilité, coût élevé. Les fibres en plastique sont plus faciles à mettre en œuvre car elles sont peu fragiles et leur diamètre important facilite les raccordements.

FIGURE 43 – Fibre optique

Les supports hertziens

Les supports hertziens exploitent les transmissions d'ondes radioélectriques. On distingue :

Les faisceaux hertziens qui utilisent des antennes directionnelles afin de relier deux points, sensibles aux obstacles, à la météo.

Les antennes de diffusion, comme les antennes-relais mobiles formant les réseaux cellulaires, une cellule étant une zone géographique dont tous les points peuvent être atteints à partir d'une même antenne.

1 Première partie : Câblage RJ45 (30 min)

Matériel nécessaire :

- Deux PCs sous Ubuntu contenant le package "eth-tools"
- Un câble RJ45 croisé et un câble droit
- L'appareil CableMeter et sa documentation

1. Comment identifier un câble droit et un câble croisé ?
2. Utilisez l'appareil "CableMeter" pour vérifier un câble droit et un câble croisé.
3. Sur les deux PC, désactivez la fonction "auto-MDI/MDI-X" et forcer le passage en MDI avec la commande "sudo ethtool –s <nom de l'interface> mdix off".
4. Configurez les deux PCs comme sur la figure 44.

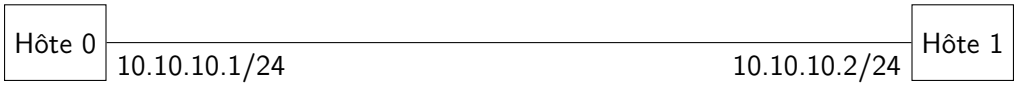


FIGURE 44 – Connexion directe

5. Utilisez le câble droit puis un câble croisé pour connecter deux PCs entre eux, en vérifiant la connectivité à l'aide d'un ping.
6. Connectez les PC à travers un Hub ou un Switch [2] en utilisant des câbles droits puis croisés comme illustré dans la figure 45

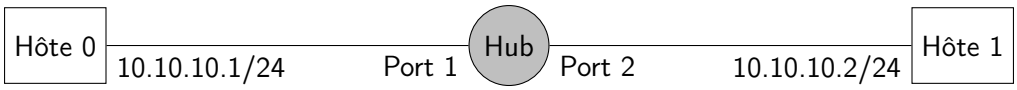


FIGURE 45 – Connexion à travers un Hub

7. Sur les deux PC, réactivez la fonction "auto-MDI/MDI-X" avec la commande "sudo ethtool –s <nom de l'interface> mdix auto". Reconnectez à nouveau directement les PC.
8. Qu'en concluez-vous sur l'utilisation des câbles droits et croisés ? Pour vous aider, utilisez la table suivante :

Equipement	**Configuration usuelle**
PC	MDI
Routeur	MDI
Commutateur (sauf ports mode Uplink)	MDI-X
Hub (sauf ports mode Uplink)	MDI-X

2. Sur un switch Cisco récent, il faut désactiver l'auto MDI-X dans l'interface : "no mdix auto". Pour l'activer et qu'il fonctionne, il faut également que le port soit en "duplex auto" et "speed auto".

2 Deuxième partie : Équipement optique (1h30)

Dans le monde des télécoms, il arrive souvent que les fibres que vous utilisez passent par l'intermédiaire d'un opérateur tiers, propriétaire de la ligne. Cela peut être Orange, SFR, EDF ou une société d'autoroute ; et chacun possède ses équipements et clients de fibre. L'objectif de cette partie est de comprendre les problématiques d'utilisation des fibres optiques sur les réseaux.

Matériel nécessaire :

- 2 Switchs Cisco
- 2 équipements ADVA
- Différentes fibres optiques
- Un testeur de niveau optique

2.1 Vérification du matériel

Les deux switchs sont prévus pour autoriser les échange entre les tous ports. Il faut vérifier pas à pas que tout fonctionne correctement.

1. Réalisez le montage présenté en figure 46.

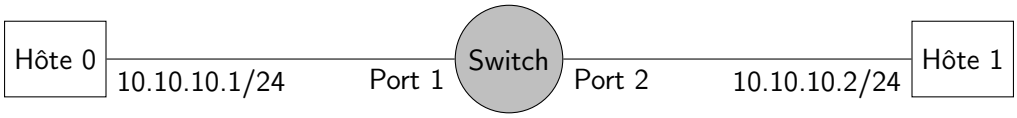


FIGURE 46 – Connexion à travers un Switch

2. Vérifiez la connectivité en mettant en place un `ping` continu.
3. Réalisez le montage présenté en figure 47. Utilisez les ports RJ45 du port combo à droite de l'équipement.

FIGURE 47 – Configuration des commutateurs

4. Vérifiez la connectivité.
5. Les équipements utilisent des SFP (Small Form-factor Pluggable). Quels sont leurs avantages par rapport aux ports intégrés aux châssis ?
6. Installer un SFP Cisco dans la cage SFP du port combo, et connecter les deux Switchs via une fibre multimode. Vérifier la connectivité.

2.2 Multiplexeurs optiques

Les deux équipements utilisés pour représenter l'opérateur tiers sont des multiplexeurs optiques CWDM de marque ADVA. Ils se composent de différentes cartes qui ont chacune leurs caractéristiques.

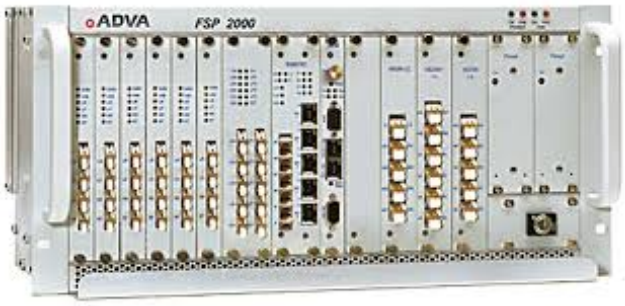


FIGURE 48 – Multiplexeur optique de marque ADVA

1. Se documenter sur le multiplexage optique et son intérêt. Proposer une façon simple de l'expliquer.
2. Quelle est simplement la différence entre le multiplexage CWDM et DWDM ?
3. Il y a à disposition différents types de fibres : monomode et multimode. Quelles sont les différences entre chaque type et dans quels cas préfère-t-on l'utilisation de la fibre monomode ?
4. Appelez l'enseignant avant de passer à la suite.

2.3 Intégration des équipements ADVA

Maintenant que notre infrastructure fonctionne il faut inclure l'opérateur tiers.

1. Repérez sur l'équipement les cartes présentées dans la figure 49. Les cartes passives multiplexent les ports inférieurs vers le port supérieur. Les cartes de droite et de gauche sont les deux parties des longueurs d'ondes du spectre CWDM. La carte centrale permet de multiplexer ces deux segments pour obtenir le spectre complet.

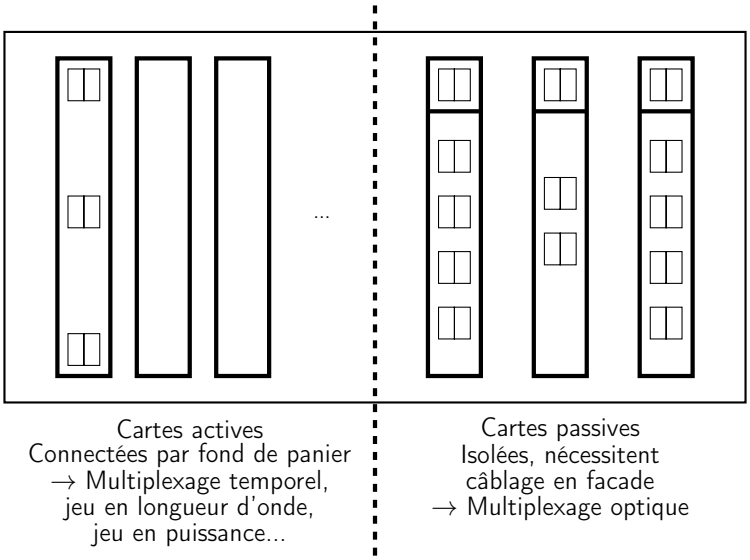


FIGURE 49 – Présentation des cartes des ADVA

2. Connecter les deux ADVA aux Switchs, comme illustré sur la figure 50. Ils vont faire office de liaison opérateur. Vous allez dans un premier temps convertir la longueur d'onde fournie par les Switches grâce à une seule carte active nécessitant des SFP, puis utiliser des fibres monomodes pour passer dans les cartes passives de multiplexage optique, et enfin relier les deux équipements.

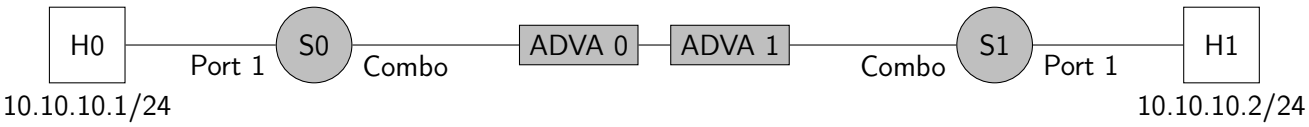


FIGURE 50 – Configuration des commutateurs

1. Une fois le montage fait, pensez à :
    a. Vérifier que les SFP du bon constructeur sont utilisés ;
    b. Vérifier que les longueurs d'ondes des différents SFP et des différents ports sont utilisés ;
    c. Vérifier que les câbles sont bien enfichés ;
    d. Suivre les chemins en transmission et réception.
2. Le ping entre les deux hôtes fonctionne-t-il ?
3. Utiliser l'équipement de mesure pour caractériser le tronçon entre les deux ADVA. Sachant que la plage de fonctionnement des SFP utilisés doit être en -5dBm et -23dBm, pourquoi est-ce que les ports ne montent pas ?
4. Mettre en place la connectique pour que les ports montent et que le ping fonctionne.

3 Troisième partie : Wi-Fi (2h)

3.1 Introduction

Le Wi-Fi est un ensemble de norme pour les réseaux locaux sans fil. Cette technologie suit la norme IEEE 802.11 et ses révisions qui définissent des éléments de débit, fréquence et autres fonctions associées au Wi-Fi : Roaming, QoS, sécurité, énergie, puissance... Le Wi-Fi utilise des bandes de fréquences normées pour ne pas interférer avec d'autres équipements sans-fil. On parle de canaux Wi-Fi.

Le mode le plus courant de mise en réseau utilisant des technologies Wi-Fi est le mode "Infrastructure". Un ensemble de bornes appelées "Point d'Accès" sont disposées et permettent aux équipements d'être interconnectés au sein d'un même réseau (à la manière d'un Hub).

FIGURE 51 – Point d'accès Aironet 1700

Les Points d'Accès doivent être configurés au préalable. Dans le cas de ce TP, un contrôleur permettra de configurer des Points d'Accès.

FIGURE 52 – Contrôleur Wi-Fi Cisco 2504

1. Qu'est-ce qu'un SSID ?
2. Qu'est-ce que le PoE ?
3. Quels sont les modes d'alimentation de l'Access Point ?

3.2 Mise en place

1. Connectez le contrôleur Wi-Fi (port 1 ou 2) et le PC au réseau de la salle. La figure 53 vous guidera pour cette partie.

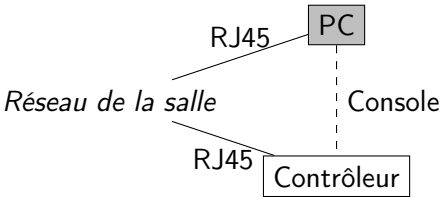


FIGURE 53 – Connexions partie Wi-Fi

2. Connectez-vous au contrôleur en console pour effectuer la configuration initiale. Le démarrage prend quelques minutes. Acceptez d'utiliser la configuration automatique. Pour le login et mot de passe utilisez **(polytech, polytech)**. D'autres paramètres vous seront demandés :

LAG	Non
Adresse de management	192.168.0.241/24
Gateway	192.168.0.254/24
VLAN	0
Port	Voir plus haut
DHCP	192.168.0.254/24
Virtual Gateway	1.1.1.1
IP Multicast	225.10.10.1
RF Group Name	PolyRFGrp
SSID	Poly5ATP
DHCP Bridging, Static IP, Radius, NTP, Configuration date	Non

3. Configurez l'horloge du contrôleur avec la commande "config time manual".
4. Rendez-vous à l'adresse IP de management via un navigateur Web. Connectez-vous.
5. Branchez un AP sur un port PoE d'un commutateur sur le même réseau local que le contrôleur. Vous pouvez utiliser le même commutateur qui connecte déjà le contrôleur et votre machine. Connectez-vous en console sur l'AP. Le démarrage peut-être un peu long. Utilisez les identifiants par défaut (Cisco, Cisco) pour vous connecter. Configurez l'horloge de l'AP avec la commande "clock set". Référez-vous à la figure 54

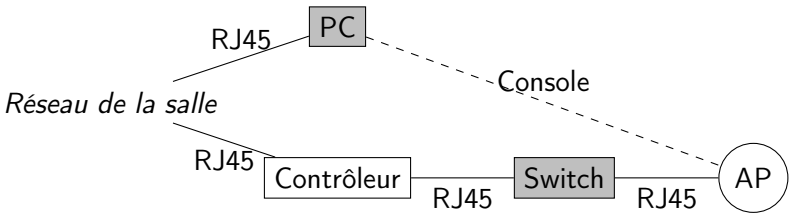


FIGURE 54 – Connexions partie Wi-Fi

6. Reconnectez-vous sur le contrôleur, et observez l'état de la connexion avec l'AP à l'aide de la commande "show ap join stats summary all"
7. Retournez sur l'interface Web de gestion. Vous devriez voir l'AP apparaître dans l'interface Web du contrôleur. Vous pouvez alors obtenir des informations : version d'OS, nombre de clients...

3.3 Configuration et essais

3.3.1 Création d'un réseau Wi-Fi

1. Assurez-vous que les interfaces soient activées : dans le menu du haut, onglet "Wireless", menu de gauche catégorie "802.11", "Network", assurez-vous que le statut soit "Enable".
2. Créez un réseau Wi-Fi non sécurisé et testez la connexion depuis un appareil de votre choix (PC portable, smartphone...) :
3. Notez votre adresse IP. Est-ce qu'un ping depuis le PC fixe vers cette IP doit fonctionner ? Pourquoi ?
4. Laissez l'appareil connecté pour la suite du TP. Lancez un ping ICMP continu du PC fixe vers son adresse IP.

3.3.2 Profilage

Activez les options de profilage client sur le contrôleur, et surfez pendant quelques minutes sur votre appareil connecté en Wi-Fi sur quelques sites différents (gardez en tête les conditions d'utilisation de la connexion de l'UL...). Regardez ensuite dans l'interface d'accueil du contrôleur, et expliquez ce que vous observez.

3.3.3 Partage de SSID sur plusieurs AP

Créez un second réseau Wi-Fi. Vous avez la possibilité de la propager sur un ou plusieurs APs. En effet, un AP peut servir d'émetteur à plusieurs réseaux sans fil.

3.3.4 Sécurisation

Déconnectez votre appareil du réseau Wi-Fi. A partir de l'interface du contrôleur, activez la sécurité WPA2 avec chiffrement AES et mot de passe sur l'un des réseaux. Tentez de vous reconnecter.

POLYTECH NANCY

4 Nettoyage

Sur tous vos ordinateurs :

- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

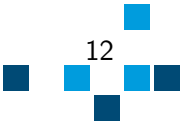
- Tapez la commande `vtp mode transparent`
- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:/vlan.dat`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos contrôleurs Wi-Fi :

- Entrez en console la commande `reset system`
- N'enregistrez pas la configuration
- Attendez que le système redémarre
- Lorsque l'invite vous demandera un "username", rentrez `recover-config`
- Attendez à nouveau que le système redémarre, et vérifiez que le dialogue de configuration initiale démarre
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos AP Wi-Fi :

- Entrez en console la commande `erase nvram:`
- Si vous avez configuré une IP statique, entrez la commande `write default-config`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse



Travaux pratiques - Sujets complémentaires

TP - OAM IP et Ethernet

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

Note : Ce TP n'est pas réalisable sur Packet Tracer

Éléments de cours

Que ce soit suite à des plaintes d'utilisateurs ou pour superviser l'état de votre réseau, vous aurez besoin d'outils pour surveiller les performances de votre réseau. La recommandation ITU-T Y.1563 définit ces paramètres de performance. En particulier :

- La latence, "delay" ou "latency" : c'est le temps mis par une trame pour transiter de sa source à sa destination. On utilise souvent le terme RTT "Round-trip Time" qui correspond à la latence d'un aller-retour d'une trame. C'est typiquement ce que l'on observe à l'aide d'un ping ICMP. On parle de FTD ("Frame Transfer Delay") lorsqu'on ignore les différents calculs de routage ou encore d'encapsulation dans le transport total.
- La gigue ou "jitter" : c'est la variation de la latence au cours du temps. La gigue est exprimée dans la même unité que la latence. Certaines confusions peuvent exister avec le domaine électronique, où la gigue a une définition différente. La gigue se calcule de deux manières : par rapport à un temps de référence minimal (2-Point Frame Delay Variation) ou entre deux trames identiques consécutives (Inter-Frame Delay Variation). On notera que ces deux définitions donnent une même moyenne de variation, à la valeur de référence près. Il faudra être vigilant sur la définition utilisée suivant le test utilisé.
- Le taux de pertes de trames ou "Frame Loss Ratio" : c'est le rapport du nombre de trames perdues et du nombre de trames émises. On le différencie du "Frame Loss Rate" qui est le nombre de trames perdues par unité de temps, ou encore du "Frame Error Ratio" qui est définit comme le nombre de trames abandonnées suite à une erreur dans la trame.

L'acronyme OAM "Operation, Administration and Maintenance" désigne un ensemble d'outils et de protocoles qui permettent la détection de panne et/ou la mesure de performance d'un réseau. Vous connaissez déjà l'un de ces outils : le ping ICMP. On s'en sert généralement pour tester une connectivité, ou mesurer grossièrement latence, gigue et aux de pertes. Vous allez voir que des outils dédiés et plus précis existent parmi les OAM. Il existe différentes normes définissant différents outils, qu'on peut synthétiser comme suit : Ces outils ont été définis pour les trois premières couches du modèle OSI (Physique, Liaison de données et Réseau). On décompose parfois les outils OAM suivant leur portée et leur usage :

- OAM Réseau : surveillance bout-en-bout d'un service client ou d'un sous-réseau, généralement en couche Réseau (MEF 30 et 35)
- OAM Liaison : surveillance des liens au sein du réseau, généralement en couche Liaison de données (IEEE802.3ah, MEF 20 et 21, ITU-T Y.1731/ IEEE 802.1ag)

Dans ce cadre, le ping ICMP est un OAM Réseau, puisqu'il teste la connectivité à travers un ou plusieurs sous-réseaux IP.

Matériel nécessaire

- 2 routeurs CISCO 2901 ou 4321
  IMPORTANT : prenez les équipements étiquetés TP OAM, et vérifiez que la commande `"show ip sla application"` est disponible.
- 1 commutateur CISCO
- 1 PC sous Windows ou Ubuntu
- 1 câble console (à paires inversées) pour connecter le port série du PC aux ports console

Partie préliminaire : Topologie

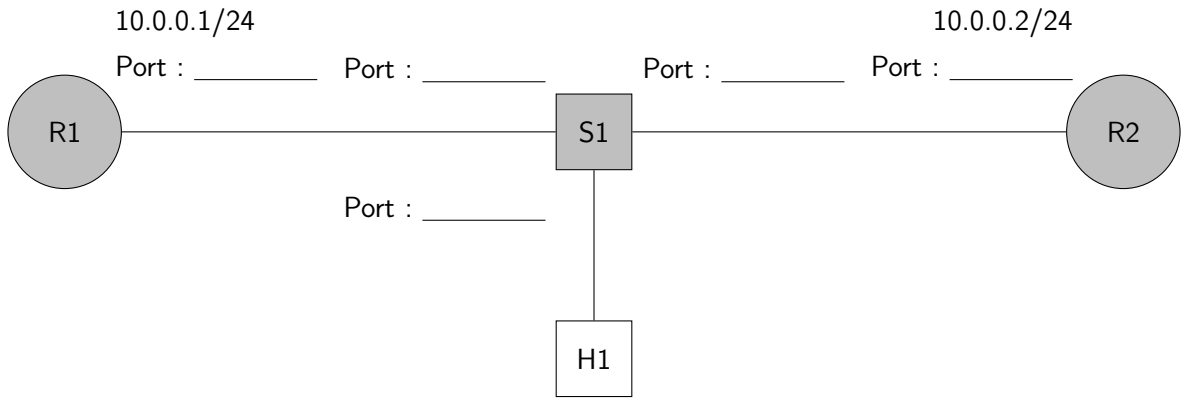


FIGURE 55 – Topologie du réseau

1. Complétez le plan avec les ports que vous allez utiliser.
2. Déployez le réseau présenté en Fig. 55.
3. Vérifiez la connectivité entre les routeurs R1 et R2.
4. Sur S1, configurez un port-mirroring du port connecté à R1 vers le port connecté vers H1. Vous aurez besoin des commandes suivantes. L'argument `both` permet de copier le trafic entrant et sortant.

```
Switch(config)#monitor session 1 source interface fa 0/1 both
Switch(config)#monitor session 1 destination interface fa0/2
```

5. Vérifiez que votre mirroring est bien configuré avec la commande `show monitor session 1`.
6. Vérifiez que le mirroring fonctionne en effectuant un ping entre R1 et R2. Que devriez-vous observez sur H1 ?

1 Première Partie : IP SLA

La fonctionnalité IP SLA est un outil propriétaire Cisco, qui offre des outils OAM de niveau 2 à 4. Certains de ces tests sont standards, d'autres diffèrent des normes. En particulier, IP SLA permet de mettre en place des tests de manière simplifiée, car l'infrastructure logique des points de mesures est déployée automatiquement, contrairement aux standards que nous verrons par la suite.

Dans IOS, ce sont les "schedulers" IP SLA qui contrôlent les tests, leur type, leur fréquence...

1.1 Déployer un test IP SLA

1. Créez un test IP SLA 10 de type icmp-echo, se répétant toutes les 5 secondes. Quelles commandes utilisez-vous ?
2. À l'aide de la commande `ip sla schedule`, lancez votre test en continu. Quelles options utilisez-vous ?
3. Quelles sont les autres options de cette commande ?
4. Observez les résultats du test à l'aide de la commande `show ip sla statistics`. Décrivez.
5. Observez les trames de test à l'aide du mirroring sur H1. Quels champs y retrouvez-vous ?
6. Testez un autre type de test.

2 Deuxième Partie : OAM Ethernet Standards

Parmi les OAM Liaison, on s'intéressera notamment aux outils dédiés au protocole Ethernet. Les OAM Ethernet sont définis dans la recommandation ITU-T Y.1731, conjointe à IEEE 802.1ag.

Dans IOS, ce sont les "schedulers" IP SLA qui permettent de contrôler les OAM Ethernet, mais ces tests particuliers nécessitent la mise en place d'une infrastructure logique.

2.1 Architecture OAM

Un MEP (Maintenance End Point) est une entité OAM active capable de générer des trames OAM de sollicitation ou de traiter les réponses. Un MIP (Maintenance Intermediary Point) est une entité OAM capable de réagir à certaines trames. Les MEP et les MIP sont placés sur les interfaces des différents noeuds du réseau, donc en couche 2 du modèle OSI.

Une ME (Maintenance Entity) est une relation logique entre exactement deux MEP.

Un MEG (Maintenance Entity Group) est un ensemble logique de MEP appartenant aux mêmes ME au sein d'un même domaine OAM. Vous verrez parfois les termes Maintenance Association, Association ou encore Service.

Un domaine OAM définit une partie logique d'un réseau dans lequel on peut déployer des entités OAM et y appliquer différents tests. Un domaine possède un niveau qui permet de définir différents éléments sur un même équipement, sans que ces éléments puissent interagir. Cela permet par exemple de mettre en place des éléments OAM indépendants pour l'opérateur et pour le client sur un équipement fournisseur. Retenez qu'il y a une hiérarchie dans les domaines, mais qu'il faut généralement éviter que des domaines se recouvrent partiellement. Vous trouverez parfois l'abréviation MD (Maintenance Domain).

En résumé, une architecture OAM consiste en un ensemble de MEP capables d'émettre des tests, chacun au sein de leur ME, MEG et domaine. Souvent, le ME et MEG sont confondus pour des raisons pratiques.

- Complétez le schéma de la Figure 56 à l'aide de ce que vous avez compris de l'architecture OAM.

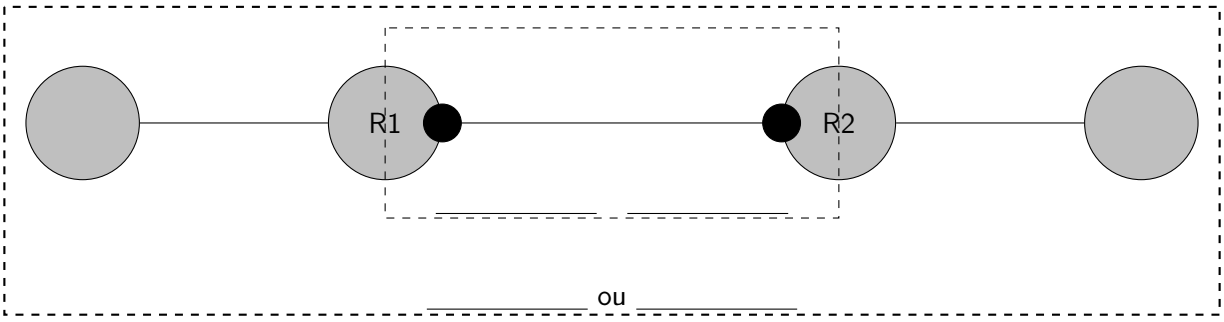


FIGURE 56 – Exemple d'architecture OAM

2.2 Mise en place d'une infrastructure OAM

1. Conservez la topologie de la Figure 55. Supprimez les tests IP SLA précédents.
2. Activez l'utilisation des OAM Ethernet avec les commandes suivantes :

```
ethernet cfm ieee
ethernet cfm global
```

3. Activez les logs console avec la commande `ethernet cfm logging`
4. Déployez une infrastructure OAM Ethernet entre R1 et R2.
   - Sur R1 et R2, un domaine `ethernet cfm` de niveau 1 "MD1" et un service 12 de type "port", avec un nom ICC-based "abcde".
   - Un MEP 1 sur l'interface Est de R1, en spécifiant un remote-mep `rmep mpid 2`.
   - Un MEP 2 sur l'interface Ouest de R2, en spécifiant un remote-mep `rmep mpid 1`.
5. Quelles commandes avez-vous utilisé ?
6. Vérifiez votre configuration avec les commandes suivantes :

```
show ethernet cfm maintenance-points local
show ethernet cfm maintenance-points remote
show ethernet cfm maintenance-points remote static
```

   Qu'observez-vous ?
7. Sur R1, lancez la commande `show ip interface brief`. Vous devez observez l'interface vers S1 "UP/UP".
8. Coupez la liaison entre S1 et R2.
9. Observez-vous des messages de log CFM ?

10. Observez à nouveau l'état de l'interface de R1. Notez le pour plus tard.
11. Rétablissez la liaison S1-R2.
12. Observez-vous des messages de log CFM ?

2.3 Test CC - Continuity-Check

1. Sur R1, activez le Continuity-Check dans le service :

```
Router(config-ecfm-srv)#continuity-check
Router(config-ecfm-srv)#continuity-check interval 1s
```

2. Dans l'interface, dans le MEP, activez également le Continuity-Check à destination des MEP distants statiques.
3. Vérifiez l'envoi de trames Continuity-Check Messages avec la commande suivante :

```
show ethernet cfm statistics
```

4. Activez le même test depuis R2.
5. Observez les trames de test CCM à l'aide du mirroring sur H1. Quels champs y retrouvez-vous ?
6. Sur R1, lancez la commande `show ip interface brief`. Vous devez observez l'interface vers S1 "UP/UP".
7. Coupez la liaison entre S1 et R2.
8. Observez-vous des messages de log CFM ?
9. À l'aide du mirroring, observez-vous toujours des trames sur le port de S1 connecté à R1 ?
10. Observez à nouveau l'état de l'interface de R1. Que remarquez-vous ? Cela correspond-il aux messages de log observés ?
11. Rétablissez la liaison S1-R2.
12. Observez-vous des messages de log CFM ?
13. À quoi sert le test CC ?

Sur nos équipements, les tests de la norme Y1731 ne fonctionnent pas sur une liaison native. Le TP n'est pas réalisable à partir de ce point.

2.4 Test SLM - Synthetic Loss Measurement

1. À l'aide d'IP SLA, déployez un test SLM (Y1731 loss LMM) entre R1 et R2. Quelle configuration utilisez-vous ?
2. Vérifiez l'envoi de Loss Measurement Messages (LMM) avec :

   ```
   show ethernet cfm statistics
   ```

   Qu'observez-vous ?
3. Observez les résultats d'un test à l'aide de la commande suivante :

   ```
   show ip sla history interval-statistics
   ```

   Qu'observez-vous ?
4. Observez les trames de test SLM à l'aide du mirroring sur H1. Quels champs y retrouvez-vous ?
5. À l'aide de la documentation et de vos observations, décrivez comment fonctionne le test SLM et son intérêt.

2.5 Test DM - Delay Measurement

1. À l'aide d'IP SLA, déployez un test DM (Y1731 delay DMM) entre R1 et R2. Quelle configuration utilisez-vous ?
2. Vérifiez l'envoi de Delay Measurement Messages (DMM) avec :

   ```
   show ethernet cfm statistics
   ```

   Qu'observez-vous ?
3. Observez les résultats d'un test à l'aide de la commande suivante :

   ```
   show ip sla history interval-statistics
   ```

   Qu'observez-vous ?
4. Observez les DMM à l'aide du mirroring sur H1. Quels champs y retrouvez-vous ?
5. À l'aide de la documentation et de vos observations, décrivez comment fonctionne le test DM et son intérêt.

3 Nettoyage

Sur tous vos ordinateurs :

- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées

Sur tous vos routeurs :

- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Si vous avez perdu le mot de passe du routeur (généralement "polytech", "poly", "cisco", ou "class"), vous allez devoir le redémarrer et l'interrompre pendant le boot. Depuis PuTTy, clic droit sur le bandeau de l'application, "Special Command", "Break". Vous accédez alors au mode ROMMON. Tapez `confreg 0x2142`, puis `reset`. Une fois redémarré, appliquez la commande `copy run start`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos commutateurs :

- Tapez la commande `vtp mode transparent`
- Listez les fichiers sur la carte flash avec la commande `dir`
- Effacez le fichier de configuration de VLAN avec la commande `delete flash:/vlan.dat`
- Effacez la configuration de démarrage à l'aide de la commande `write erase` ou `erase startup-config` suivant les versions
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos contrôleurs Wi-Fi :

- Entrez en console la commande `reset system`
- N'enregistrez pas la configuration
- Attendez que le système redémarre
- Lorsque l'invite vous demandera un "username", rentrez `recover-config`
- Attendez à nouveau que le système redémarre, et vérifiez que le dialogue de configuration initiale démarre
- Rangez les câbles et posez les équipement en bout de paillasse

Sur tous vos AP Wi-Fi :

- Entrez en console la commande `erase nvram:`
- Si vous avez configuré une IP statique, entrez la commande `write default-config`
- Redémarrez à l'aide de la commande `reload` et vérifiez que la configuration est vierge
- Rangez les câbles et posez les équipement en bout de paillasse

Travaux pratiques - Sujets complémentaires

TP - Utilisation élémentaire de Linux

C. Colombo

L'objectif de ce TP est d'appréhender des commandes élémentaires sur Linux.

Matériel nécessaire

- 1 PC ou une VM sous Ubuntu 18 ou plus, version Server ou Desktop
- Une connexion Internet

1 Première Partie : Shell, la console Linux

Dans un premier temps, vous allez apprendre à vous diriger dans un système Linux sans interface graphique.

1. Si votre système dispose d'une interface graphique, passez en mode console avec la commande `Ctl+Alt+F2`

Lorsque vous entrez dans une console (ou terminal ou Shell), une invite de commande ("prompt" en anglais) doit s'afficher. Il s'agit en général du nom d'utilisateur et du dossier courant, suivi du symbole $ ou #.

2. Tapez la commande `ls` (pour "**l**i**s**t"). Cette commande affiche le contenu du dossier courant.
3. Toutes les commandes peuvent s'accompagner d'options ajoutée avec un tiret. Tapez la commande `ls -l`. Vous voyez maintenant le contenu du dossier sous forme de liste contenant plus de détails.
4. Essayez maintenant de taper la commande `man ls`. Cette commande vous affiche toute la documentation (le **man**uel).
5. Découvrez maintenant la commande `cd`, qui permet de changer de dossier (pour "**c**hange **d**irectory").
6. Créez un dossier "testfolder" avec la commande `mkdir` (pour "**m**a**k**e **dir**ectory").
7. Rendez vous dans ce dossier.
8. Les chemins Linux peuvent se définir de manière absolue ou relative. Quel est le chemin absolu de votre dossier ?
9. Le chemin relatif qui désigne le dossier courant s'écrit "./". Quel est le chemin relatif qui désigne le dossier parent ?
10. Créez un fichier "testfile.txt" avec la commande `touch`
11. Copiez ce fichier avec le nom "testfile2.txt" avec la commande `cp` (pour "**c**o**p**y").
12. Déplacez le fichier "testfile2.txt" dans le dossier parent avec la commande `mv` (pour "**m**o**v**e").
13. Supprimez le fichier "testfile2.txt" avec la commande `rm` (pour "**r**e**m**ove").

Sachez que ces commandes sont également utilisables dans les terminaux Mac, et qu'il existe des équivalents dans les systèmes Windows.

2 Deuxième Partie : Lire et écrire

Par défaut, vous allez voir comment utiliser l'éditeur `nano`. Il en existe d'autres, plus ou moins complets, complexes, beaux... L'éditeur `nano` est léger, relativement simple, et présent sur les distributions Ubuntu. Commandes utiles sur `nano` :

- Ctl+x : Quitter
- Ctl+o : Sauver
- Ctl+w : Chercher
- Alt+r : Chercher et remplacer

1. Éditez le fichier "testfile.txt" à l'aide de la commande `nano testfile.txt`
2. Écrivez chaque lettre de l'alphabet sur une ligne.
3. Sauvegardez et quittez.
4. Affichez le contenu du fichier avec la commande `cat`
5. Affichez uniquement les 10 dernières lignes avec la commande `tail`

3 Troisième Partie : Propriété et permissions

Les fichiers et les dossiers Linux sont soumis à un système de permission. Pour un objet donné, on distingue trois types d'utilisateurs : le propriétaire, le groupe autorisé, les autres ; et trois types de droits : la lecture (r pour "**r**ead"), l'écriture (w pour "**w**rite"), l'exécution (x pour "e**x**ecute"). On a donc un système à 9 paramètres, 3 droits ou interdictions pour 3 catégories d'utilisateur.

On les représente généralement sous la forme d'une chaîne de 10 caractères. Le premier indique s'il s'agit d'un fichier "-" ou d'un dossier "d". Les 9 suivants indiquent un droit avec le caractère associé "r", "w" ou "x" ou un tiret "-" pour une interdiction. Par exemple :
`-rwxr-xr- polytech guest`
Signifie que l'objet est un fichier. Son propriétaire "polytech" peut le lire, le modifier, l'éxécuter. Les membres du groupe "guest" peuvent lire et exécuter le fichier. Tous les autres utilisateurs peuvent uniquement lire le fichier.

1. À l'aide de la commande `ls`, affichez les permissions du fichier "testfile.txt".
2. Modifiez vos droits en écriture sur le fichier à l'aide de la commande `chown`.
3. Que se passe-t-il lorsque vous essayez d'éditer le fichier avec `nano` ?

La commande sudo (pour "super**u**ser **do**") permet d'élever temporairement les privilèges de l'utilisateur pour accéder à des fichiers ou des commandes en tant qu'administrateur.

4. Essayez maintenant d'éditer le fichier "testfile.txt" avec la commande `sudo nano`
5. Supprimez le fichier.

POLYTECH NANCY

4 Quatrième Partie : Scripting

Généralement, on cherche à automatiser les tâches récurrentes sur une machine. Pour cela, on écrit des scripts. Le langage par défaut sur les systèmes Linux est le `bash`. Il correspond au Shell, et sa syntaxe est sensiblement la même que la ligne de commande.

1. Créez un fichier "testscript.sh"
2. Éditez-le pour afficher régulièrement "Hello". Vous aurez besoin de la commande `echo`
3. Vérifiez que vous avez bien les droits d'exécution sur le fichier.
4. Lancez le script avec la commande `./testscript.sh`

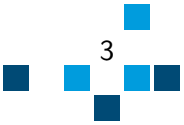
Il existe également un système qu'on appelle le Cron, qui permet de lancer des commandes ou des scripts régulièrement, ou à des heures données. C'est un processus qui tourne en tâche de fond.

5 Cinquième Partie : Configuration réseau

Nous allons maintenant faire en sorte que notre système ait accès à Internet. Il a probablement déjà une configuration automatique en DHCP.

1. Vérifiez la configuration actuelle avec les commandes `ip a` (ou `ifconfig` sur des vieux systèmes) et `ip route`
2. Pour modifier la configuration sur des systèmes récents :
   a. Éditez le fichier "/etc/netplan/01-network-manager-all.yaml"
   b. Validez la configuration avec la commande `sudo netplan try`
   c. Appliquez la configuration avec la commande `sudo netplan apply`
3. Pour modifier la configuration sur des systèmes plus anciens (mais encore nombreux en production) :
   a. Éditez le fichier "/etc/network/interfaces"
   b. Appliquez la configuration avec la commande `systemctl restart networking`

Sur un système avec interface graphique, il est généralement plus simple et plus fiable de passer par les menus de configuration. Il peut arriver que le système observe un conflit entre la configuration par fichier et la configuration graphique (c'est généralement la configuration préférée), il faut alors corriger le problème.



POLYTECH NANCY

6 Sixième Partie : Packages

Installer Emacs

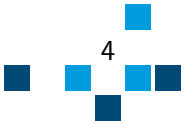
7 Septième Partie : Interface graphique

Ctl+Alt+F1 et Emacs graphique

8 Nettoyage

Sur tous vos ordinateurs :

- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées



Travaux pratiques - Sujets complémentaires

TP - Installation de Linux

C. Colombo

À la fin de la séance de TP, il vous est demandé de faire parvenir à l'enseignant un rapport de 2 à 6 pages. Étant donné le format court, inutile de faire une page de garde et un sommaire.

Vous devez faire apparaître votre nom, la date, numéroter les pages, et l'envoyer au format PDF. La mise en forme du document ainsi que l'orthographe ont leur importance. Votre interlocuteur vous pardonnera facilement quelques erreurs si la majorité du document est irréprochable. À l'inverse, si votre document est illisible, la moindre erreur sera plus fortement pénalisée.

Le rapport doit présenter le but du TP, ce que vous avez fait, comment s'est déroulé le TP, ce que vous avez observé et les conclusions que vous en avez tiré. L'idée c'est que vous puissiez le relire lors des TPs suivants et vous remémorer rapidement ce qui est nécessaire, sans relire le sujet. Par exemple : la topologie, les commandes utiles, les problèmes que vous avez pu rencontrer et comment vous les avez résolus...

Évidemment, l'objectif est toujours que le TP se passe sans accroc, mais vous n'êtes pas pénalisé si vous expliquez que vous avez fait une erreur dans le TP. Bien au contraire : si vous relevez votre erreur, et expliquez comment vous vous en êtes sortis, on verra d'autant plus votre compréhension.

Vous avez accès à toutes les ressources de votre choix : le support de cours, les TP précédents et vos compte-rendus, ainsi qu'Internet. L'objectif du TP est de vous faire comprendre des notions par la pratique, et de vous apprendre à les utiliser. Si vous trouvez par ailleurs des explications qui vous aident à comprendre ou de la documentation utile, n'hésitez pas à les intégrer à votre rapport.

L'objectif de ce TP est dans un premier temps d'apprendre à installer et administrer un serveur Linux. Une seconde partie vise à appréhender des outils et langages usuels.

Matériel nécessaire

- 2 PC connectés à Internet
- Un CD ou clé USB d'installation de la distribution choisie

1 Première Partie : Mise en place d'un serveur

Il s'agit dans un premier temps d'installer Linux sur une des machines à votre disposition. La machine Linux servira de serveur et l'autre machine de client.

1. Assurez-vous que les machines sont bien reliées au réseau de la salle
2. Assurez-vous que les machines sont bien reliées à Internet
3. Installez la distribution sur l'une des machines
4. Au démarrage de la machine, accédez au BIOS avec "F12"
5. Détectez le clavier. Vous devez arriver au "fr :oss"
6. Définissez le login "polytech", mdp "polytech"
7. Ne chiffrez pas le dossier
8. Patientez pendant quelques minutes la détection de timezone
9. Sélectionnez "Démonter partitions existantes : Assisté - utiliser un disque (SANS LVM)"
10. Ne sélectionnez pas de mandataire HTTP
11. Pas de mise-à-jour auto
12. Installer GRUB sur le disque dur (PAS SUR LA CLEF USB)
13. Pendant l'installation, faites quelques recherches sur la seconde machine :
    a. Qu'est-ce qu'une distribution Linux ?
    b. Qu'est-ce qu'un paquet Linux ?
    c. A quoi correspond l'utilitaire "apt-get" ?
    d. A quoi sert la commande "sudo" ?

2 Deuxième Partie : Découverte de Linux

Note : si vous avez déjà utilisé Linux, passez directement à la partie suivante.

Vous venez d'installer une distribution Linux, mais pas d'interface graphique. Vous allez donc devoir utiliser la console. Cette partie va vous faire découvrir quelques commandes élémentaires de la console, qui vous permettront de naviguer simplement dans les systèmes Linux sans interface graphique. Vous verrez plus tard que, même avec une interface graphique, certains outils Linux ne sont disponibles qu'en ligne de commande.

Lorsque vous entrez dans une console (ou terminal), une invite de commande ("prompt" en anglais) doit s'afficher. Il s'agit en général du nom d'utilisateur et du dossier courant, suivi du symbole $ ou #.

1. Tapez la commande `ls`. Cette commande affiche le contenu du dossier courant.
2. Toutes les commandes peuvent s'accompagner d'options ajoutée avec un tiret. Tapez la commande `ls -l`. Vous voyez maintenant le contenu du dossier sous forme de liste contenant plus de détails.
3. Essayez maintenant de taper la commande `man ls`. Cette commande vous affiche toutes les options disponibles pour la commande `ls`.
4. Découvrez maintenant la commande `cd`, qui permet de changer de dossier.
5. Créez un fichier avec la commande `touch`.
6. Copiez un fichier avec la commande `cp`.
7. Déplacez un fichier avec la commande `mv`.

Sachez que ces commandes sont également utilisables dans les terminaux Mac, et qu'il existe des équivalents dans les systèmes Windows.

3 Troisième Partie : Administration du serveur

3.1 Configuration réseau

1. Attribuez une IP fixe au serveur (utilisez la cheat sheet Nano en annexe)
   a. Sur la machine client, utilisez des ping pour trouver une adresse non-utilisée sur le réseau de la salle.
   b. Recherchez le fichier "/etc/network/interfaces"
   c. Modifiez le avec l'aide de la commande "sudo nano interfaces"
   d. Créez l'interface "eno1" (référez-vous à la documentation pour la syntaxe)
   e. Utilisez le DNS 193.50.27.66
2. Redémarrez le service réseau (si nécessaire, débranchez puis rebranchez le câble RJ45)
3. Vérifiez la prise en compte des changements avec "ifconfig"
4. Vérifiez que les paquets "ssh" et "openssh-server" sont bien installés
5. Depuis le client, prenez la main en SSH sur le serveur (pour Windows, utilisez le logiciel PuTTY)
6. Observez les ports actifs sur le serveur à l'aide de la commande "nmap". Pensez à utiliser l'adresse de loopback
7. Observez les connexions actives sur le serveur à l'aide de la commande "netstat -a"

Note : dans les nouvelles releases Linux, pour des raisons de sécurité il est impossible de se connecter en tant que "root". Utilisez les logins définis à l'installation du serveur.

3.2 Serveur Web

1. Installez le paquet apache2
2. Depuis le navigateur de la machine client allez sur l'adresse affectée au serveur
3. Modifiez le fichier /var/www/html/index.html (utilisez la cheat sheet Nano en annexe)
4. Rechargez la page
5. Observez les ports actifs sur le serveur à l'aide de la commande "nmap". Pensez à utiliser l'adresse de loopback
6. Qu'est-ce que LAMP ?

3.3 Configuration DNS et DHCP

1. Installez le paquet "dnsmasq" sur la machine serveur
2. Connectez ensuite directement votre machine client avec votre serveur à l'aide d'un câble RJ45
3. Configurez une adresse IP statique 192.168.10.254/24 sur le serveur
4. Assurez-vous que la machine client soit configurée pour obtenir une adresse IP automatiquement depuis le serveur
5. Dans le fichier "/etc/dnsmasq.conf" assurez-vous que les lignes suivantes soient présentes :
   - `dhcp-range=192.168.10.1,192.168.10.10,12h` qui défini le range d'adresses distribuées
   - `dhcp-option=1,255.255.255.0` qui défini le masque du réseau
   - `dhcp-option=3,192.168.10.254` qui distribue une adresse de passerelle
6. Dans le fichier "/etc/hosts", assurez-vous que la ligne "192.168.10.254 polyserver" soit présente
7. Redémarrez le service dnsmasq avec la commande "/etc/init.d/dnsmasq restart"
8. Depuis la machine client, vérifiez que vous avez obtenu une IP dans l'intervalle défini
9. Lancez un ping vers l'adresse du serveur
10. Lancez maintenant un ping vers "polyserver". Qu'observez-vous ?
11. Vérifiez que le serveur Web mis en place précédemment fonctionne toujours
12. Observez les ports actifs sur le serveur à l'aide de la commande "nmap". Pensez à utiliser l'adresse de loopback

3.4 Configuration d'un serveur FTP

1. Installez un serveur FTP sur votre machine serveur.
2. Installer un client FTP (ex : Filezilla) sur votre machine client.
3. Transférez un fichier texte quelconque vers le serveur.
4. Observez les ports actifs sur le serveur à l'aide de la commande "nmap". Pensez à utiliser l'adresse de loopback
5. Quelle est la différence entre FTP et TFTP ?

4 Quatrième Partie : Découverte des langages de scripts

Les scripts sont des outils utiles pour l'administrateur d'un serveur, car ils permettent de mettre en place rapidement des systèmes simples. Il existe de nombreux langages adaptés à la création de scripts, notamment perl, bash ou python (2.7 ou 3.x).
En utilisant au choix Bash, Perl ou Python, réalisez les scripts suivants :

- Une boucle "for" sur un intervalle de 1 à 10 n'affichant que les nombres pairs.
- Lancez la commande "ifconfig" toutes les 10 secondes.
- Analysez le résultat de la commande et affichez uniquement le nombre de paquets transmis "TX Packets" (utilisez une regex !).

5 Partie Bonus : Interface graphique

Cette partie est optionnelle et peut être longue.
Sur un serveur, pour des raisons de performance, on installe rarement une interface graphique.

1. Installez le paquet emacs
2. Installez le paquet ubuntu-desktop
3. Redémarrez la machine
4. Lancez le programme emacs
5. Basculez vers le mode console avec la combinaison "Ctl + Alt + F1"
6. Lancez la commande emacs
7. Vous pouvez rebasculer vers l'interface graphique avec "Ctl + Alt + F7"

Annexe : Cheat sheets

Commandes utiles sur Nano :

- Ctl-x – Quitter
- Ctl-o – Sauver
- Ctl-w – Chercher
- Alt-r - Chercher et remplacer

Commandes utiles sur Emacs :

- Ctl-x Ctl-c – Quitter
- Ctl-x Ctl-s – Sauver
- Ctl-s – Chercher
- Shift-Alt-% - Chercher et remplacer

6 Nettoyage

Sur tous vos ordinateurs :

- Effacez toutes les configurations IP de vos machines, et configurez-les en DHCP
- Assurez-vous qu'elles soient reliées au réseau de la salle via la baie de brassage
- Vérifiez qu'une adresse a été attribuée aux machines
- Laissez les machines connectées