TP - M1IF15 Réseau par la pratique

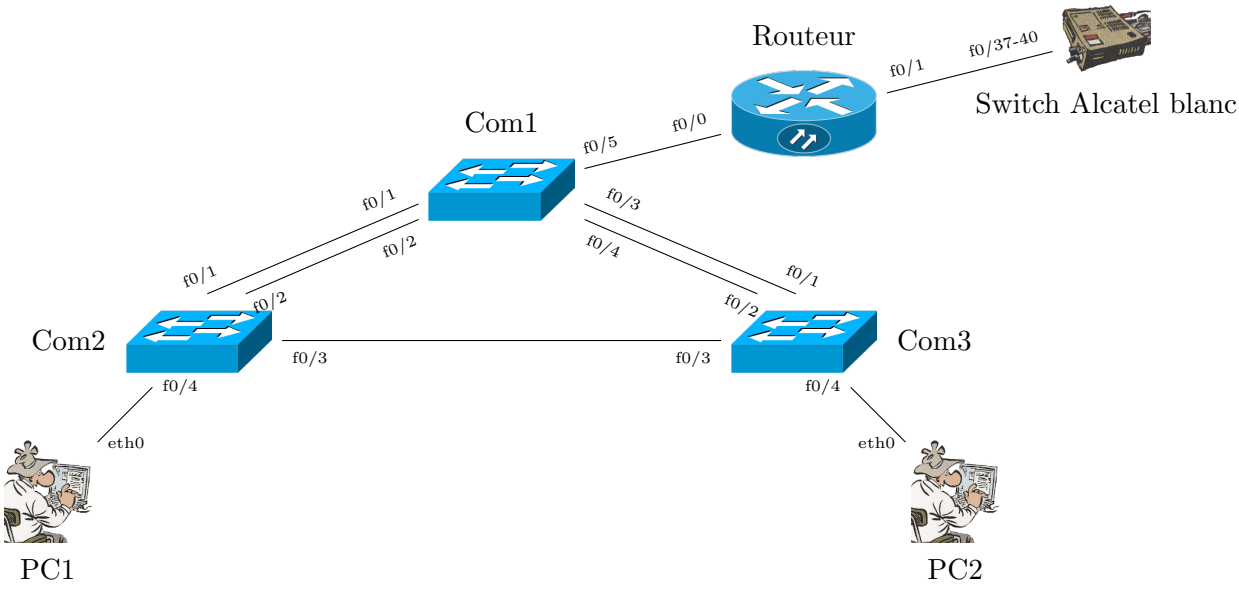
Spanning Tree DHCP et début des ACL

23 mai 2018

Objectifs

- Spanning Tree (utilisation, modification de l'arbre, ...)
- Agrégation de liens
- Mise en place d'un serveur DNS
- Premières ACLs

I Description du réseau



II Scénario

Chaque groupe aura une plage d'adresse réseau propre. Pour cela, vous devez définir un numéro X différent de celui des autres groupes. Utilisez votre numéro de plot N et une valeur M différente de celle des autre groupes sur le même plot :

$$X = N * 10 + M$$

Par exemple le groupe 1 du plot 3 utilise X = 31.

Vous allez configurer 1 réseau : `192.168.X.0/24`

II.1 Adresses

Les attributions sont celles du tableau suivant :

Appareil	Interface	Adresse IP	Masque	Passerelle
Routeur	Fa0/0	`192.168.X.254`	`255.255.255.0`	N/D
	Fa0/1	`192.168.0.X`	`255.255.255.0`	192.168.0.254
Com1	VLAN1	`192.168.X.1`	`255.255.255.0`	N/D
Com2	VLAN1	`192.168.X.2`	`255.255.255.0`	N/D
Com3	VLAN1	`192.168.X.3`	`255.255.255.0`	N/D
PC1	eth0	`192.168.X.11`	`255.255.255.0`	192.168.X.254
PC2	eth0	`192.168.X.12`	`255.255.255.0`	192.168.X.254

III Travail à faire

III.1 Préparer le réseau

Q.III.1) - Câblez le réseau comme montré dans le diagramme.

Q.III.2) - Effacez les configurations existantes (startup-config et vlan.dat).

Q.III.3) - Redémarrez les commutateurs.

III.2 Configuration de base

Configurer les 3 commutateurs :

Q.III.4) - Configurez le nom

Q.III.5) - Désactivez la recherche DNS .

Q.III.6) - Ajoutez le nom de domaine groupX.org (remplacer X par la valeur)

Q.III.7) - Configurez un mot de passe d'exécution privilégié « class ».

Q.III.8) - Configurez les logs synchrones.

Q.III.9) - Ajoutez un utilisateur local root avec droit d'administration et « cisco » comme mot de passe.

Q.III.10) - Configurez ssh et limiter l'accès distant à ssh.

IV Configuration des Pcs et vérification de la table MAC

Q.IV.1) - Affichez la table d'adresse MAC sur COM2 et COM3, videz là.

Q.IV.2) - Configurez les adresses des Pcs et vérifiez l'accès ssh depuis PC1, vers les commutateurs COM1, COM2 et COM3.

Q.IV.3) - Ré-affichez la table d'adresse MAC et expliquez les différences, pourquoi y-a-t'il plusieurs adresse mac associés à certains ports ?

V Configuration du protocole Spanning Tree

V.1 Examen de la configuration par défaut du protocole STP802.1D

Sur chaque commutateur, affichez la table Spanning Tree pour le vlan1. Recopiez le résultat dans la suite. Ensuite répondez aux questions suivantes à partir des résultats :

Q.V.1) - Quelle est la priorité de l'ID de pont pour les commutateurs Comm1, Comm2 et Comm3 sur le VLAN 1 ?

1(a) - COM1 :

1(b) - COM2 :

1(c) - COM3 :

Q.V.2) - Quel commutateur représente la racine Spanning Tree du VLAN 1 ?

Q.V.3) - Sur le VLAN 1, quels sont les ports Spanning Tree à l'état de blocage sur le commutateur racine ?

Q.V.4) - Sur le VLAN 1, quels sont les ports Spanning Tree à l'état de blocage sur les commutateurs non-racine ?

Q.V.5) - Comment le commutateur racine est-il choisi via STP ?

Q.V.6) - Étant donné que les priorités de pont sont toutes identiques, quel autre élément le commutateur utilise-t-il pour déterminer la racine ?

Q.V.7) - Faites le shema du réseau en tenant compte des ports bloqués, le chemin est-il toujours optimal pour des paquets partant des PC et allant vers le routeur ? Et des paquets entre les PC eux mêmes ? Quelle racine devrait-on utiliser ?

V.2 optimisation du protocole STP

Vous devez modifier les priorités de manière à ce que la racine soit COM1. Faites en sorte que la racine secondaire soit COM2.

Q.V.8) - Quel commutateur correspond à la racine du VLAN 1 ?

Q.V.9) - Sur le VLAN 1, quels sont les ports Spanning Tree à l'état de blocage sur le nouveau commutateur racine ?

Q.V.10) - Refaites le shema du réseau en tenant compte des ports bloqués.

VI observation de la réponse à une modification de la topologie STP 802.1D

Pour observer une continuité sur le réseau local lors d'une modification de la topologie, lancer un ping de PC1 vers PC2 ou inversement.

Placez Com2 et Com3 en mode de débogage des événements Spanning Tree pour contrôler les modifications lors du changement topologique (debug spanning−tree events)

Q.VI.1) - Coupez la liaison permettant d'aller de COM2 à COM3 et observer les événements relatifs au calcul du spanning tree. Quelles interfaces changent d'état ? Par quels états passent-elles ? Quel est la topologie finale ? Combien de temps dure la coupure sur le ping ?

VII Configuration du protocole Spanning Tree rapide PVST

Attention, tous les commutateurs ne sont pas capables de faire du Rapid-PVST, vérifiez que cela est possible avant de faire cette tâche. Sinon, sauter à la section suivante.

Q.VII.1) - Configurez les 3 commutateurs afin qu'ils utilisent le protocole Rapid-PVST.

Q.VII.2) - Configurer tous les ports qui ne sont pas reliés à des commutateurs avec l'option portfast.

Q.VII.3) - Exécutez la commande show spanning−tree summary pour vérifier que RSTP est activé.

VII.1 Observation du délai de convergence de RSTP

Commencez par restaurer les liens que vous avez déconnectées dans la Tâche VII, si ce n'est déjà fait. Suivez ensuite les étapes de la Tâche VII :

Q.VII.4) - Définissez le PC2 pour envoyer des requêtes ping continues sur le réseau.

Q.VII.5) - Activez le débogage des événements Spanning Tree sur les commutateurs.

Q.VII.6) - Déconnectez les câbles connectés.

Q.VII.7) - Observez le délai nécessaire au rétablissement d'un Spanning Tree stable.

VIII Agrégation de lien (au sens cisco)

Q.VIII.1) - Configurer les liens doubles COM1/COM2 et COM1/COM3 de manière à les agréger (protocole LaCP).

Q.VIII.2) - Vérifier le fonctionnement des liaisons.

Q.VIII.3) - Cela change-t-il le résulat du spanning-tree ? Pourquoi ?

IX Configuration du routeur

Configurez le routeur :

Q.IX.1) - Configurez le nom

Q.IX.2) - Désactivez la recherche DNS .

Q.IX.3) - Ajoutez le nom de domaine groupX.org (remplacer X par la valeur)

Q.IX.4) - Configurez un mot de passe d'exécution privilégié « class ».

Q.IX.5) - Configurez les logs synchrones.

Q.IX.6) - Ajoutez un utilisateur local root avec droit d'administration et « cisco » comme mot de passe.

Q.IX.7) - Configurez ssh et limiter l'accès distant à ssh.

Q.IX.8) - Configurez les 2 interfaces Gigabit 0/0 et Gigabit 0/1

X ACL

Vous allez utiliser des ACL pour protéger les accès à votre réseau.

Q.X.1) - Créez une acl standard pour protéger l'accès au serveur ssh du routeur. Elle ne doit autoriser l'accès que depuis le réseau interne mais pas des commutateurs.

1(a) - Quel numéro d'ACL allez-vous utiliser ?

1(b) - Donnez la définition de l'ACL ?

1(c) - Où la placer pour quelle assure la protection ?

Q.X.2) - Créez une acl étendue pour qu'elle ne laisse entrer dans le réseau que les paquets qui sont une question vers le serveur web sur pc2 ou les paquets dns.

2(a) - Comment reconnait-on un paquet à destination d'un serveur web ?

2(b) - Donnez la définition de l'ACL

2(c) - Où la placez-vous ?

Q.X.3) - Testez les ACLs (après avoir installé un serveur web sur pc2).

3(a) - Pouvez-vous accéder à pc1 et pc2 depuis votre réseau ?

3(b) - Depuis le réseau d'un autre groupe ?

3(c) - S'il le faut corrigez l'ACL pour que les site web soient utilisables.

XI Un premier service DNS

Vous allez installer le logiciel `dnsmasq` qui est une implémentation simple d'un serveur : DHCP, DNS et TFTP. Ce logiciel est très utilisé pour créer des serveurs de *boot-on-lan* ou gérer les réseau des machines virtuelles. Il est aussi utilisé pour gérer les requêtes DNS par l'application `NetworkManager` sous ubuntu.

Pour le serveur DNS, ce logiciel utilise les fichiers de résolution de nom classiques afin répondre aux requètes : `/etc/resolv.conf` est utilisé pour savoir à qui transmettre les requêtes auxquelles il ne peut pas répondre. Et `/etc/hosts` est utilisé pour trouver les noms de machines du réseau local.

Q.XI.1) - Modifiez le fichier `/etc/resolv.conf` pour que le serveur dns principale de la machine devienne `192.168.0.254`

Q.XI.2) - Modifiez `/etc/hosts` pour ajouter les machines `pc1.groupX.org`, `pc2.groupX.org`, et `pc3.groupX.org`

Q.XI.3) - Installez `dnsmasq` et modifier le fichier `/etc/dnsmasq.conf` pour lui signaler que le le réseau local est `groupX.org` (c'est l'option `local=` dans le fichier).

Q.XI.4) - Testez de nouveau l'accès au site mais en utilisant le nom dns.

XII Remise en état

Supprimez les configurations et rechargez les configurations par défaut pour les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).