M2-ESECURE Rezo TP1: Switch

Pierre Blondeau Pierre.Blondeau@unicaen.fr

19/09/2010

1 Introduction

Ce TP a pour but de découvrir l'utilisation de marionnet et la configuration de switchs, avec pour objectifs d'être autonome dans la création de réseaux virtuels dans marionnet, de manipuler un langage de commandes de switch et d'en étudier certaines fonctionnalités.

2 Contexte

Dans le cadre du cours de réseaux en ESECURE, vous aurez à effectuer de nombreux TPs cette année. La salle 409 a été spécialement équipée dans ce but. Chaque machine possède deux cartes réseaux : une reliée au département d'informatique et l'autre sur le réseau de TP. Le réseau de TP se compose de quelques switches réformés du CRISI et de la société Intrinsec.

Une documentation papier des switchs est mise à votre disposition pendant le TP ou à consulter ici : http://www.cisco.com/en/US/docs/switches/lan/catalyst2900xl_3500xl/release12.0_5_wc16/ol256212.html

3 Matériel

Rappel : Liaison série, câble coaxial, câble à paire torsadée (droit/croisé), fibre optique, convertisseur de média, répéteur (hub), commutateur(switch), routeur.

4 Marionnet

Démonstration. Créer le réseau suivant :



FIGURE 1 – Schema

4.1 Avec l'interface

Dans un premier temps, configurez les adresses IP des machines grâce à l'interface de marionnet et vérifiez la connectivité entre vos machines (ping et ssh).

4.2 Sans l'interface

Dans un deuxième temps, déconfigurez les adresses IP des machines dans l'interface de marionnet. Démarrez les machines et utilisez le fichier /etc/network/interfaces. Vérifiez la connectivité entre vos machines. Que se passe t'il en cas de redémarrage des machines, pourquoi?

5 Utilisation et configuration des switchs

Mettez en place les liaisons physiques comme définies au tableau.

5.1 Configuration minimale

Les switchs ont été entièrement réinitialisés. Il faut leur donner un nom, une adresse IP, un mot de passe et permettre les connexions telnet pour l'administration à distance. Attention : telnet est un protocole non sécurisé à éviter en environnement de production lorsque c'est possible.

Pour cela, vous allez utiliser le port série. Il existe de nombreux logiciels dont les plus connus sont Hyper-Terminal pour windows et minicom pour linux. Nous allons utiliser gtkterm.

Si les switchs n'ont pas été réinitialisés, voici les commandes de bases : enable # mdp tprezo erase nvram : delete flash :vlan.dat reload

5.1.1 Commandes de base

Notez que la complétion automatique de commande fonctionne sous IOS.

?	Liste les commandes ou les arguments utilisables
enable	Passer en mode administrateur
config terminal	Passer en mode configuration
\mathbf{exit}	Retour au mode précédent
end	Quitte le mode en cours
show running-config	Affiche la configuration en cours
write	Sauvegarde la configuration

5.1.2 Nom du switch

Passez en mode configuration et : hostname NAME

5.1.3 Adresse IP

Passez en mode configuration puis :

interface vlan 1	Entrez dans le contexte du vlan 1
ip address IP MASQUE	Configurez l'adresse IP et le MASQUE
ip default-gateway IP	Configurez la route par défaut (falcutatif)

Rappel : Vous configurez des switchs, pas des routeurs. L'adresse IP n'est là que pour les administrer.

Vous configurez le vlan1 car c'est le vlan d'administration par défaut chez Cisco. Il permet la configuration des switchs. La route par défaut permettrait de joindre les switchs si il était dans une classe ip différente de la machine qui administre. Il est également possible de rensigner les adresses IP des switchs dans un serveur DNS pour les joindre avec un nom plutôt qu'une IP.

Testez la connexion avec un ping depuis une des machines m1 de ce switch.

5.1.4 Mots de passe

Pour pouvoir vous connecter en telnet sur les switchs, il faut configurer des mots de passe.

Passez en mode configuration puis :

line vty 0 15Entrez dans le contexte du vty 1password PASSWORDConfigurez le mot de passe avec tprezo

Essayez de vous connecter sur les switchs depuis la machines m1 : **telnet 192.168.128.10X** (X est numéro du switch). Essayez de passer en mode administrateur. Que se passe t-il? Pour la configuration du mot de passe enable, passez en mode configuration puis :

enable password PASSWORD Configurez le mot de passe avec tprezo

Vérifiez la configuration du switch. Que remarquez vous au sujet des mots de passe? Re-testez la connection telnet depuis m1.

5.2 Configuration des vlans

Pour la configuration des vlans, voici quelques commandes utiles. Trouvez à quoi elles servent et ou elles peuvent / doivent être utilisées.

```
switchport access vlan 10
switchport trunk allowed vlan 1,10,1002-1005
switchport trunk encapsulation dot1q
switchport mode trunk
switchport priority default 5
```

5.3 Vèrrouillage des adresses MAC

Voici quelques commandes utiles pour activer le vèrrouillage des ports des switchs sur une adresse mac.

```
port security
port security max-mac-count 1
port security action shutdown
mac-address-table secure 0204.0600.0016 FastEthernet0/5 vlan 1
mac-address-table secure 0204.0600.0624 FastEthernet0/3 vlan 5
```

5.4 Pour les plus rapides

Les systèmes d'exploitation peuvent également gérer les vlans. Vous pouvez donc mettre en "trunk" la prise de votre machine et gérer les vlans sur votre machine virtuelle m1.

6 Pour aller plus loin

6.1 Virtualisation

Il existe de nombreuses solutions de virtualisation. Je vous conseille de jeter un coup d'œil du côté de Xen, KVM, VirtualBox, etc ...

6.2 Switchs

Les nouvelles générations de switchs possèdent d'autres fonctionnalités intéréssantes :

- connexion ssh
- interface web
- cluster de switchs
- supervision snmp
- agrégation de liens
- authentification des clients 802.1x

- ...