Atelier - VLAN Natif et Sécurité

Présentation

Dans la continuité de l'atelier "VLAN et routage inter-VLAN", cet atelier vise à permettre aux PC du réseau SN_Tech de préparer la mise en place des accès à distance sur les équipements switch et routeurs, ainsi que de sécuriser la VLAN native.

Qu'entend-on par "accès à distance" ?

Un accès à distance est caractérisé par l'absence de nécessité d'un accès physique à l'équipement dans le cadre des opérations d'administration ou de maintenance. Deux protocoles notables permettent l'accès à distance : Telnet et SSH.

Telnet est un protocole ancien non sécurisé, les mots de passe y transitent en clair et n'importe quelle opération de traçage des trames sur le réseau permet de reconstruire les couples identifiants et mots de passe. Ce protocole est donc tombé en désuétude au profit de SSH.

Le protocole SSH (Secure SHell) est un protocole permettant la mise en place d'un tunnel sécurisé et chiffré avec une machine distante, pour notamment y opérer en ligne de commande. Dérivant du protocole RSH (Remote SHell), il est particulièrement indiqué pour la prise de contrôle à distance en ligne de commande.

Objectifs

Configuration des mots de passe console et exec

Il est temps de sécuriser les switchs et routeurs. La première étape consiste à ajouter un mot de passe pour l'accès à la console (associé à la ligne console), et un autre mot de passe pour l'activation du mode privilégié (exec).

1. **Configurez un mot de passe console de votre choix pour sécuriser l'accès à chaque équipement réseau (switch et routeur)**
2. **Configurez un mot de passe exec de votre choix pour sécuriser l'accès à chaque équipement réseau (switch et routeur)**

Nouveaux VLANs

On ajoutera deux VLAN à l'infrastructure :

- VLAN 999, sera utilisé en tant que VLAN native

- VLAN 998, sera utilisé pour les accès à distance sur les équipements switches et routeur, avec le nom SN_Equipements

VLAN 999 - Application du VLAN Natif

Le VLAN natif doit être configuré sur les divers équipements, et, pour plus de sécurité, le tagging des trames natives sur les liaisons trunk doit être forcé.

Sur SW_Acc_1 et SW_Acc_2 :

1. **Ajoutez le VLAN 999 avec comme nom “NATIF”**
2. **Spécifiez le VLAN 999 comme étant le VLAN natif**
3. **Forcez l’application du tag 802.1Q sur le trunk**

VLAN 998 - Accès distant aux équipements

La VLAN 998 nécessitera la mise en place de deux nouveaux sous-réseaux dédiés pour les accès à distance (oui, DEUX).

Nous sommes dans un cas particulier où un même numéro de VLAN peut être utilisé pour plusieurs sous-réseaux. Ceci est possible car la topologie actuelle ne permet pas aux trames de broadcast de traverser le routeur, qui agit ainsi comme une frontière entre plusieurs sous-réseaux, tout en ne permettant pas de diffuser un même sous-réseaux entre les deux plateaux (puisque le routeur refusera l’affectation d’un même sous-réseau sur deux interfaces ou sous-interfaces différentes).

Dans notre cas d’usage, chaque switch est d’un côté du routeur. Nous allons donc définir un réseau dédié aux accès distants pour le plateau 1 (Gi 0/0.998) et un réseau dédié aux accès distants pour le plateau 2 (GI 0/1.998) :

- **VLAN 998 sur le plateau 1 : 192.168.1.248/29**
- **VLAN 998 sur le plateau 2 : 192.168.2.248/29**

VLAN 998 - Plan d’adressage			
Equipement	Interface	IP	Passerelle
RT_Dis_1	Gi 0/0.998	192.168.1.254	-

VLAN 998 - Plan d'adressage			
RT_Dis_1	Gi 0/1.998	192.168.2.254	-
SW_Acc_1	Vlan 998	192.168.1.249	192.168.1.254
SW_Acc_2	Vlan 998	192.168.2.249	192.168.2.254

Vous remarquerez donc que les switch peuvent se voir attribuer une configuration IP sur une interface VLAN dédiée et c'est tout à fait normal et possible. En effet, les switch travaillent en layer 2 au sein de l'infrastructure mais peuvent tout à fait utiliser des protocoles layer 7 pour eux-même. Ils ne savent pas faire de routage mais peuvent tout à fait utiliser des adresses IP pour, notamment, permettre l'accès à distance.

Dès lors, les équipements du coeur de l'infrastructure ayant chacun une adresse IP dans la VLAN 998, celle-ci pourra être utilisée pour les accès à distance.

1. **Configurez SW_Acc_1 et SW_Acc_2 pour intégrer la VLAN 998**
    a. **Ajout de la VLAN 998 dans la base de données des VLAN**
    b. **Ajout de la VLAN 998 comme VLAN autorisée dans le trunk vers RT_Dis_1**
    c. **Ajout et configuration de l'interface virtuelle "vlan 998"**
    d. **Configuration de la passerelle par défaut (ip default-gateway …)**
2. **Réalisez les configurations nécessaires sur RT_Dis_1**
    a. **Configuration de l'interface gi 0/0.998**
    b. **Configuration de l'interface gi 0/1.998**
3. **Vérifiez la bonne application de vos configurations via ping**

(OPTIONNEL) Mise en place des accès SSH

Si vous voulez prendre de l'avance, recherchez la méthode permettant d'ajouter des utilisateurs aux équipements Cisco et mettez en place configuration d'accès via SSH sur le VLAN 998 pour chacun d'eux. Ceci fera l'objet d'un cours séparé, donc gardez bien en tête qu'il s'agit d'une tâche <u>optionnelle</u>