TD 10 : Projet - Réseau (2)

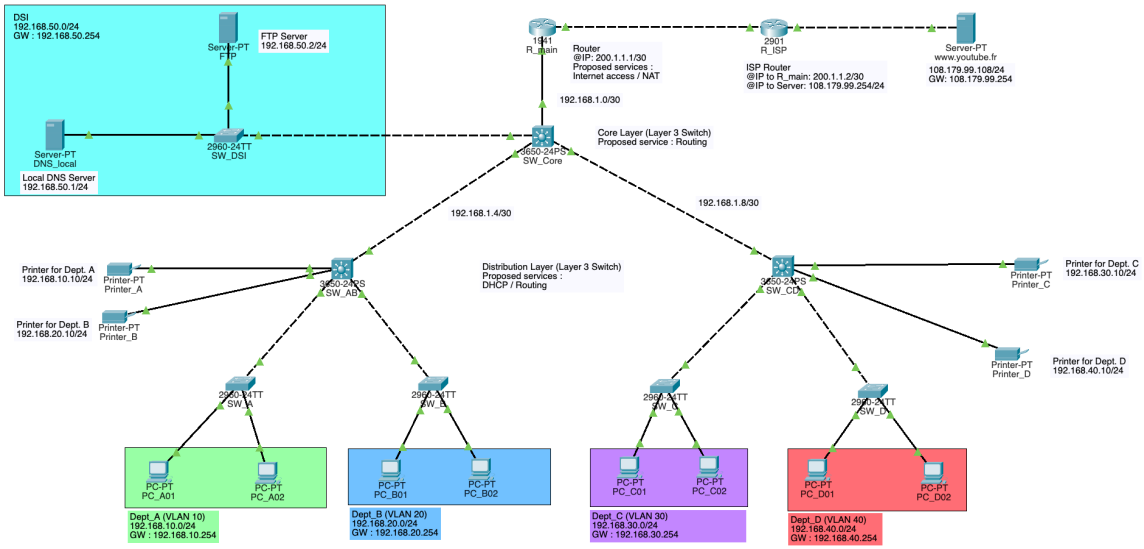
Équipe pédagogique : Zhiyi ZHANG, Saeed ALSABBAGH

Objectifs pédagogiques

- Mettre en place l'authentification des ports dot1x
- Configurer les ACL
- Comprendre le fonctionnement du DHCP snooping et BPDU Guard

N'oubliez pas de modifier le nom des équipements.

1) Topologie



On va poursuivre les configurations de la séance précédente.

2) Authentification au niveau de ports

Dans un réseau Ethernet classique, tout équipement branché sur un port du commutateur peut immédiatement accéder au réseau. Dans un contexte d'entreprise, cette situation représente un risque de sécurité. L'authentification au niveau du port permet de contrôler l'accès au réseau en s'assurant que seuls les utilisateurs autorisés peuvent se connecter.

Grâce à ce mécanisme d'authentification, le port de commutateur d'accès reste bloqué par défaut, et ne devient actif qu'après une authentification réussie.

On va configurer le premier port de chaque commutateur de la couche d'accès comme un port nécessitant une authentification. Cela signifie que les ordinateurs A01, B01, C01 et D01 devront saisir un nom d'utilisateur et un mot de passe afin de pouvoir établir une connexion réseau avec le commutateur.

IEEE 802.1X est un standard largement utilisé pour implémenter l'authentification dans les réseaux filaires et sans fil. Par exemple, sans IEEE 802.1X, l'eduroam est impossible. Si l'architecture d'eduroam vous intéresse : https://www.eduroam.fr/specif_tecnik. Il y a trois rôles principaux dans IEEE 802.1X :

- Supplicant (Client) : PC client ou équipement sans fil
- Authenticator : équipement de la couche d'accès (commutateur ou point d'accès)
- Serveur d'authentification : généralement, un serveur RADIUS

Le serveur d'authentification se trouve dans la DSI. Dans le réseau DSI, ajoutez un serveur et configurez son adresse IP : 192.168.50.3/24, avec la passerelle par défaut : 192.168.50.254.

Afin de permettre aux commutateurs de la couche d'accès (authenticator) d'échanger avec le serveur d'authentification, il est nécessaire de configurer une adresse IP sur l'interface VLAN de SW_A, SW_B, SW_C et SW_D. Un commutateur classique est un équipement de couche 2, il ne possède pas de table de routage et donc pas de notion de route par défaut au sens du routage IP. Cependant, afin de permettre l'émission de paquets IP (gestion, 802.1X ...), il faut configurer une passerelle par défaut à l'aide de la commande : *ip dafault-gateway*, pointant vers la passerelle par défaut du VLAN local.

Par exemple, on fait sur le SW_A :
SW_A(config)# interface vlan 10
SW_A(config-if)# ip address 192.168.10.253 255.255.255.0
SW_A(config)# ip default-gateway 192.168.10.254
et sur le SW_AB : *SW_AB(config)# ip dhcp excluded-address 192.168.10.253*

Vérifiez la connectivité depuis chaque commutateur d'accès vers le serveur d'authentification 192.168.50.3.

Si le *ping* fonctionne, on revient sur le serveur d'authentification et on active le service ***AAA***. Dans la configuration client, le champ *Client Name* doit correspondre au nom du commutateur de la couche d'accès, par exemple SW_A. Le champ *Client IP* correspond à l'adresse IP configurée sur l'interface VLAN du commutateur. Il est nécessaire de définir une clé RADIUS partagée aussi (le champ *Secret*), puis on va utiliser la même clé sur le commutateur. Ensuite, configurez les identifiants des utilisateurs (nom d'utilisateur et mot de passe). Ces identifiants seront utilisés lors de l'authentification côté client (PC).

Dans le service ***Radius EAP***, activez EAP-MD5.

Sur les commutateurs de la couche d'accès, activez AAA et IEEE 802.11X, configurez l'authentification via RADIUS et renseignez les informations du serveur RADIUS. Par exemple :
SW_A(config)# aaa new-model
SW_A(config)# dot1x system-auth-control
SW_A(config)# aaa authentication dot1x default group radius
SW_A(config)# radius-server host 192.168.50.3 auth-port 1645 key <Clé_Radius >

Ensuite, activez l'authentification 802.1X sur le port reliant le PC.
SW_A(config-if)# authentication port-control auto
SW_A(config-if)# dot1x pae authenticator

Après la configuration de l'authentification au niveau du port, l'état de port devient orange, ce qui sinifie que la connexion réseau est bloquée en attente d'authentification. Sur le PC, dans les paramètres IP, activez l'authentification 802.1X et saisissez le nom d'utilisateur et le mot de passe configurés sur le serveur.

Après quelques instants, l'état du port repasse au vert, indiquant que l'authentification a réussi. Vérifiez que le service DHCP fonctionne toujours.

3) Configuration des ACL

La présence de plusieurs imprimantes accessibles sur le réseau peut rapidement entraîner de la confusion pour les utilisateurs. Alors, on souhaite que chaque imprimante soit réservée à son département respectif, en interdisant l'accès aux imprimantes des autres départements. Autrement dit, l'accès aux imprimantes doit être limité au réseau de leur propre VLAN.

Une fois les ACL configurées, vérifiez leur bon fonctionnement à l'aide de tests de connectivité.

4) Protection contre un serveur DHCP illégal

Le département utilise le service DHCP, et le serveur DHCP légitime est fourni par la couche de distribution. Cependant, un utilisateur peut connecter un serveur DHCP non autorisé au réseau par erreur, ce qui peut provoquer une mauvaise attribution des adresses IP, une fausse passerelle par défaut, et une perte de connectivité.

Dans le département D (SW_D), ajoutez un nouveau serveur configuré comme serveur DHCP. Configurez ce serveur avec un pool DHCP pour le réseau : 10.10.10.0/24, une passerelle par défaut : 10.10.10.1.

Renouvelez l'adresse IP d'un poste client du département D. Est-il encore possible d'obtenir l'adresse correcte ?

Le DHCP snooping est un mécanisme de sécurité destiné à protéger le réseau contre les attaques liées au protocole DHCP, telles que la présence de serveurs DHCP non autorisés.

Sur le SW_D, configurez le mécanisme DHCP snooping :

- Activez DHCP snooping au niveau global
  SW_D(config)# ip dhcp snooping
- Précisez le VLAN
  SW_D(config)# ip dhcp snooping vlan <N°_vlan >
- Désactivez l'insertion de l'option 82 (en environnement Packet Tracer)
  SW_D(config)# no ip dhcp snooping information option
- Configurez l'interface montante vers la couche de distribution comme port de confiance (trusted)
  SW_D(config-if)# ip dhcp snooping trust

Renouvelez l'adresse IP du poste client du département D. Vérifiez que le client obtient une adresse IP correcte, et seul le serveur DHCP légitime est autorisé à répondre.

5) Configuration de BPDU Guard

Sur les commutateurs de la couche d'accès, les ports connectés aux postes clients sont généralement configurés en mode *PortFast*, afin de permettre aux équipements d'accéder rapidement au réseau en passant directement à l'état Forwarding. Cependant, il est important de ne pas connecter de commutateurs, ou d'autres équipements d'interconnexion

sur ces ports, car cela pourrait entraîner la création de boucles de couche 2 sur une courte période.

C'est pourquoi on active généralement le mécanisme BPDU Guard sur les ports *edge*. Ainsi, si un port configuré en *PortFast* reçoit un BPDU, le port est immédiatement mis en état *err-disabled*, ce qui permet de protéger le réseau contre les boucles de couche 2.

Pour activer BPDU Guard sur des ports *edge* :
SW_X(config)# spanning-tree portfast bpduguard default
Pour configurer les ports en mode *PortFast* :
SW_X(config)# interface range FastEthernet 0/1-24
SW_X(config-if-range)# spanning-tree portfast

Que se passe-t-il si on connecte un autre commutateur sur un port d'un commutateur d'accès ?