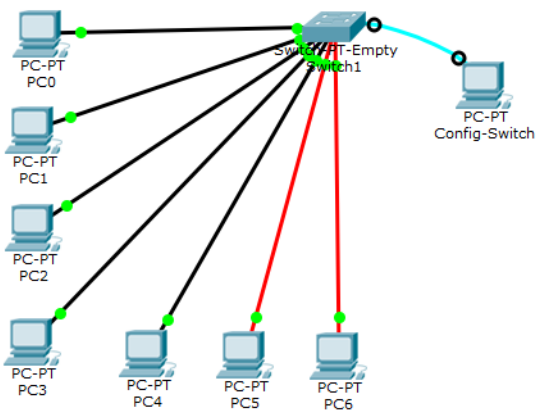
ACTIVITE 2
Sécurisation d'un switch

L'objectif de cette activité est de vous familiariser avec les commandes CISCO qui permettent la configuration des mots de passe, le chiffrage et l'ajout d'une bannière.

Pour paramétrer le switch, vous utiliserez la fiche "Fiche SWITCH - Commandes CISCO.pdf**".**
Elle propose une description des principales commandes utilisées pour la configuration d'un switch.

1 – Rappels activité 1 (SWITCH)

☞ 1 - Saisissez le schéma ci-dessous sous Packet tracer.



Modèle du switch utilisé : **switch-PT-Empty**.
Equipement : 6 modules "**PT-SWITCH-NM-1CGE**"

ATTENTION
Le câble rouge symbolise de la fibre optique. Il faut adapter les connecteurs du coté ordinateur et du coté switch pour pouvoir connecter une fibre optique.

☞ 2 - Configurez les postes PC0 à PC6 en respectant les caractéristiques suivantes :

- Changer la carte réseaux des postes PC5 et PC6 par une carte réseau fibre optique.
- Configurez les postes PC0, PC1, PC2, PC3, PC4, PC5 et PC6 (onglet **config**) en **Mode automatique** (full duplex – 1 Gbits/s).

☞ 3 - Configurez les adresses IP des postes PC0 à PC6 en respectant les caractéristiques suivantes :

- Nom du réseau : 192.168.1.0
- Masque de sous réseau : 255.255.255.0

Attention : le **PC-ConfigSwitch** ne doit pas être connecté au switch à l'aide d'un câble Ethernet. Par mesure de sécurité, ce PC est isolé du réseau.

☞ 4 - Testez la connectivité des hôtes (ping) et résolvez les problèmes de connectique.

☞ 5 – Connectez-vous au switch avec l'outil terminal.

✍ 6 – Changez le nom du switch. Nouveau nom : "TP_Switch2"
Commande CISCO :

La sécurisation d'un switch consiste à sécuriser les accès au switch
- Accès console : mot de passe, cryptage des mots de passe. - Accès réseau (line VTY) : Bannière d'avertissement, utilisateurs avec des niveaux d'accréditations différents (niveau 15 le plus haut), mot de passe, chiffrage (SSH), chiffrage des mots de passe, …

La première étape consiste à informer les utilisateurs que le switch est la propriété de telle entreprise ou telle organisation, que les personnes non autorisées ne doivent pas se connecter et effectuer des modifications. Il peut également encourager les utilisateurs à contacter le support technique pour obtenir des informations complémentaires.

✍ 7 – Ajoutez une bannière au switch. Message : " Ce switch est la propriete du BTS CIEL de Lorgues, connexion et modification interdites à toutes personnes non autorisees" (ne pas utiliser de caractères accentués).

Commande CISCO :

Sécurisation de l'accès "console"

La deuxième étape consiste à sécuriser l'accès console. Il faut définir un mot de passe qui validera l'accès du terminal (PuTTY par exemple) au port console du switch.

✍ 8 – Définissez un mot de passe pour l'accès Terminal / Console.

Commandes CISCO :

☞ 9 – Fermez le terminal puis reconnectez-vous au switch avec l'outil terminal. Cette fois-ci, on doit vous demandez le mot de passe. Entrez-le puis validez.

Sécurisation du switch

L'étape suivante consiste à vérifier si la personne qui se connecte au mode privilège est bien autorisé.

✍ 10 – Définissez un mot de passe pour activer le mode privilège. (Mot de passe = **MdpPrivilege**)

Commande CISCO :

☞ 11 – Revenez au mode utilisateur puis entrez la commande "enable" pour activer le mode privilège. Cette fois-ci, on doit vous demandez le mot de passe. Entrez-le puis validez.

✍ 12 – Affichez la configuration courante du switch (running-Config). Que constatez-vous au sujet des mots de passe console et privilège ?

Commande CISCO :

Constatation :

Il existe une solution pour masquer (chiffrer) le mot de passe privilège.

✍ 13 – Définissez un mot de passe pour activer le mode privilège en mode "secret".
(Mot de passe = **MdpSecret**)

Commande CISCO :

✍ 14 – Revenez au mode utilisateur puis entrez la commande "enable" pour activer le mode privilège. Quel mot de passe vous demande-t-on ?

✍ 15 – Affichez la configuration courante du switch (running-Config). Que constatez-vous au sujet des mots de passe console et privilège ?

☞ 16 – Faire une sauvegarde de la configuration courante dans celle de démarrage.

Sécurisation de l'accès réseau (ligne VTY)

La dernière étape consiste à sécuriser l'accès réseau. En effet, on peut configurer le switch en passant par un de ses ports. Il faut que le port concerné soit affecté au VLAN de configuration. Par défaut, lors de l'activation de ce VLAN, tous les ports lui sont affectés.

✍ 17 – Le VLAN de configuration est joignable à partir d'une adresse IP ou d'un nom de domaine (une URL). Sélectionnez l'avant dernière adresse IP disponible de votre réseau pour le VLAN et utilisez ce nom de domaine : "switch-bts.fr".
Adresse IP :

✍ 18 – Configurez le VLAN.
Commandes CISCO :

✍ 19 – Si l'on souhaite joindre le switch depuis un poste situé à l'extérieur du réseau, cela est possible mais il faut préciser au switch, l'adresse IP de la passerelle.
Commande CISCO :

Actuellement, notre réseau ne dispose pas de passerelle ni d'accès vers l'extérieur : il faudrait ajouter un routeur, mais cela fera l'objet d'une autre activité.

Maintenant que le VLAN de configuration est actif, vous allez sécuriser les lignes d'accès (line VTY) en mettant en place un mot de passe et en chiffrant les communications.
Une ligne VTY correspond à l'ouverture d'un accès réseau entre le switch et un de ses administrateurs. Comme plusieurs administrateurs peuvent accéder simultanément au switch, il faut définir plusieurs lignes. Il peut y avoir des niveaux d'accréditation différents entre les administrateurs (le niveau 15 étant le plus haut).

✍ 20– Ajoutez un mot de passe et activez l'accès à distance du switch pour 16 utilisateurs (line VTY 0 15)

Commandes CISCO :

✍ 21 – Créez un compte administrateur (admin1) avec un niveau d'accréditation 15 et "adminLorgues" comme mot de passe.

Commande CISCO :

La sécurisation de base de notre switch est terminée mais on peut aller plus loin. Et si on chiffrait nos communications ?

Commande CISCO : "**crypto key generate rsa** 512/1024" (voir fiche SWITCH pour avoir la séquence complète)
Cette commande permet de générer une paire de clés RSA sur un switch Cisco pour chiffrer les données en transit et empêcher des tiers d'intercepter et de lire les données sensibles. Le paramètre "512/1024" spécifie la longueur de la clé en bits. Si vous utilisez "512", une clé RSA de 512 bits sera générée.

✍ 22 – Implémentez sur votre switch une clé RSA (512 bits) associée au protocole SSH (version 1). L'accès au switch sera coupé après 60 secondes d'inactivité ou après trois échecs de connexion.
Rappel : le nom de domaine proposé est : "switch-bts.fr".

Commande CISCO :

✍ 23 – Affichez la configuration courante du switch (running-Config). Quels sont les mots de passes qui apparaissent en clair ?

✍ 24 – Proposez une solution pour chiffrer (encryption) les derniers mots de passe en clair.

Commande CSICO :

☞ 25 – Afficher la configuration courante et vérifier si tous les mots de passes sont cryptés.