|  |  |  |  |
| --- | --- | --- | --- |
| F:\BTS cours\portfolio\logoIMC.jpg | **BTS SIO**  **Services Informatiques aux Organisations** | | F:\BTS cours\portfolio\logolaposte.jpg |
| **Option** | **SISR** |
| **Session** | **2015** |

|  |  |  |
| --- | --- | --- |
| **Costes Antoine** | **Activité professionnelle N°** | **4** |

|  |  |
| --- | --- |
| **NATURE DE L'ACTIVITE** | Travaux pratique réalisé en formation : VLAN |
| **Contexte** | Dans une entreprise, il y a souvent plusieurs services (ex : comptabilité, ressource humaine) il peut être utile de regrouper ces services dans des « réseaux » propres afin de renforcer la sécurité. |
| **Objectifs** | Mise en place de groupe de travail, sécurité des échanges. |
| **Lieu de réalisation** | Centre de formation |

|  |
| --- |
| **SOLUTIONS ENVISAGEABLES** |
| VLAN, réseau local virtuel |

|  |  |
| --- | --- |
| **DESCRIPTION DE LA SOLUTION RETENUE** | |
| **Conditions initiales** | Un réseau sans VLAN, sans groupe de travail à sécurité moindre |
| **Conditions finales** | Mise en place de VLAN |
| **Outils utilisés** | Cisco Packet Tracer, switch, machine, repertoire de commandes CISCO |

|  |  |
| --- | --- |
| **CONDITIONS DE REALISATION** | |
| **Matériels** | Machines, switch |
| **Logiciels** | Cisco Packet Tracer |
| **Durée** | 3 fois 2 heures |
| **Contraintes** | Respect des commandes CISCO |

|  |  |
| --- | --- |
| **COMPETENCES MISES EN OEUVRE POUR CETTE ACTIVITE PROFESSIONNELLE** | |
| A5.2.4  A3.3.1  A3.2.1  A3.1.3  A3.1.1  A3.1.2  A2.3.2  A2.3.1  A1.2.4 | Étude d’une technologie, d'un composant, d'un outil ou d'une méthode  Administration sur site ou à distance des éléments d'un réseau, de serveurs, …  Installation et configuration d'éléments d'infrastructure  Prise en compte du niveau de sécurité nécessaire à une infrastructure  Proposition d'une solution d'infrastructure  Maquettage et prototypage d'une solution d'infrastructure  Proposition d'amélioration d'un service  Identification, qualification et évaluation d'un problème  Détermination des tests nécessaires à la validation d'un service |

|  |
| --- |
| **DEROULEMENT DE L'ACTIVITE** |
| **VLAN de niveau 1,2 et 3 :**  Un VLAN (Virtual Local Area Network : réseau local virtuel) permet de créer des domaines de diffusion indépendant gérés par les commutateurs de manière logique.  **Méthodes**: Il existe 3 méthodes pour créer des VLAN :   * VLAN niveau 1 : par port réseaux virtuel en relation avec les ports du commutateur. * VLAN niveau 2 : par adresses MAC (niveau 2) en fonction de l’adresse MAC de la machine (VLAN beaucoup plus souple en gestion). * VLAN niveau 3 : par adresse IP (niveau 3) selon l’IP source des datagrammes (solution de grande souplesse) ou VLAN par protocole.   **Protocole 802.1q :** un commutateur peut gérer plusieurs vlans et un vlan être géré par plusieurs commutateurs. Pour cela l’appartenance à un vlan est déterminé par un « marquage » de la trame (tag). Ce protocole modifie l’en-tête MAC de la trame en y ajoutant un identifiant vlan. Le vlan associe ensuite la trame au vlan indiquer.  Dans un vlan il y a 3 types de trame :   * Non étiqueté (sans info sur l’appartenance à un vlan) * Etiqueté (par un tag de la trame) * Etiqueté par une priorité   **Avantage du VLAN :** Un VLAN forme un réseau de manière logique au-dessus d’un réseaux physique. Il présente donc une grande souplesse d’administration, un gain de sécurité car les informations sont encapsulée et ainsi une réduction de la diffusion des trafics.  **Affectation de ports aux VLANs :**   * Un port Trunk véhicule un trafic agrégé c'est-à-dire provenant de plusieurs sources de Vlan. Un trunk ne peut être raccordé qu’à un autre port Trunk (switch, routeur ou passerelle). * Un port access véhicule un trafic ne provenant que d’une seule source VLAN, c’est pourquoi il ne peut être connecté qu’à un poste terminal (poste, serveur, imprimante).   **Ports agrégé :** un port agrégé est une liaison entre le commutateur et un autre périphérique réseau. Les agrégations transportent le trafic provenant de plusieurs réseaux locaux virtuels via une liaison unique divisé en sous interface et permettant à chaque réseau local virtuel d’atteindre l’intégralité du réseau.  Les ports agrégé sont nécessaire à l’acheminement entre des périphéries de trafique provenant de plusieurs VLAN.  **TP  VLAN niveau 1 :**    On remarque que les PC peuvent communiquer entre eux. Pour commencer, en mode commande on doit créer les vlans à l’aide des commandes suivantes :  *switch> en switch# vlan data switch(vlan)# vlan 10 name Comptabilite switch(vlan)# vlan 20 name Informatique switch(vlan)# exit*  Puis on assigne les ports où les PC sont connectés aux vlans correspondant :  *switch# conf t*  *switch (config)# int fast 0/1*  *switch (config-if)# switchport mode access*  *switch (config-if)# switchport access vlan 10*  *switch (config-if)# end*  *switch # exit*  *switch# conf t*  *switch (config)# int fast 0/2*  *switch (config-if)# switchport mode access*  *switch (config-if)# switchport access vlan 20*  *switch (config-if)# end*  *switch # exit*    Après cette manipulation, on fait un test ping du PC B vers PC A, on remarque que les PC ne peuvent plus communiquer, donc on en déduit que les deux PC sont bien dans deux VLAN différents.  Une fois que les VLANs sont configurés, on peut sauvegarder la configuration du switch de la manière suivante :  *switch# copy running-config startup-config*  **TP VLAN niveau 2 :**  **Quelques commandes :**  Configuration en cours : show running config  Version du commutateur : show version  A partir de la console, on peut configurer des paramètres de vitesse : conf t / interface fastethernet / speed 100 / duplex full  **Gestion de la table MAC :** On commence par déterminer les adresse MAC des pc relié au switch (en commande ipconfig /all), il est possible d’observer certaine configuration avec la commande show mac-adress-table. On peut aussi supprimer les adresses MAC déjà existante avec clear mac-address-table dynamic.  La sécurisation d’un port peut s’effectuer par filtrage MAC. Seule la ou les adresses MAC configurées ne sont pas filtrées. 3 méthodes sont possibles :  Fixer en dur l’adresse MAC sur le port  *Switch(config-if)# switchport port-security mac-address 0123.4567.1423.7890*  Ou par apprentissage de l'adresse MAC de la 1ère trame qui traversera le port  *Switch(config-if)#switchport port-security mac-address sticky*  Limiter le nombre de Postes possibles par ports  *Switch(config-if)#switchport port-security maximum 2* Seuls 2 postes peuvent se connecter sur ce port  Conserver définitivement l’@MAC apprise dynamiquement  *Switch(config-if)#switchport port-security mac-address sticky*  Configurer le port pour se désactiver en cas de violation de sécurité sur ce port  *Switch(config-if)#switchport port-security violation shutdown*  **TP VLAN de niveau 3 :**  Configurer les sous interfaces du commutateur:  *Router(config)#interface fa0/0.1* 🡪 positionnement sur une sous-interface  *Router(config-subif)#ip add 192.168.10.254 255.255.255.0* 🡪attribuer @IP et masque  *Router(config-subif)#descr \*\*VLAN1*\*\* 🡪 description de l'interface  *Router(config-subif)#encap dot1q 10*  *Router(config-subif)#exit*  Router#write 🡪on enrengistre la configuration  <http://www-igm.univ-mlv.fr/~dr/XPOSE2004/rlataix/index.php?rub=201>  **VLAN trunk :**  Principe de base du mode trunk : Rajoute de l’information dans la trame. Le mode Trunk consiste a lié des vlan correspondant entre eux et donc cloisonne les différents vlan (trunker les switchs). Le mode Trunk par défaut laisse passer tous les vlan, possibilité d’interdire des passages.  Pour établir une communication entre VLAN, il faut établir une encapsulation en mode "trunk". Ce fonctionnement permet la communication entre les stations de 2 VLAN différents sur un même Switch et/ou entre les stations d'un même VLAN sur des Switches différents. Il s'agit d'un processus intervenant à la couche 2 du modèle OSI.  Taper les commandes suivantes :  SW01#conf t  SW01(config)#int fa 0/1  SW01(config-if)#switchport mode trunk  Switch(config-if)# switchport trunk encapsulation dot1q    Pour mettre l'interface en mode nonegociate afin de désactiver l'envoi de packets DTP (Dynamic Trunking Protocol) :  Switch(config-if)# switchport nonegociate  Test ping pour vérifier la communication entre les PC des différents VLAN. |

|  |
| --- |
| **CONCLUSION** |
| Les VLANs apportent un allègement de l’administration (architecture modifiable par paramétrage des commutateurs), gain de sécurité et une réduction du trafic sur le réseau. |