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

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

|  |  |
| --- | --- |
| **NATURE DE L'ACTIVITE** | Travaux pratiques réalisé en stage |
| **Contexte** | Renouvellement infrastructure du système d’information |
| **Objectifs** | Mise en place d’une borne WiFi pour le personnel de l’entreprise (châteaux en  bordeaux) et d’un deuxième SSID pour des clients de passage.  Un deuxième TP sur la liaison entre SSID et VLAN est présent dans cette fiche. |
| **Lieu de réalisation** | Bordeaux, Chateaux en Bordeaux et le centre de formation (IMC) |

|  |
| --- |
| **SOLUTIONS ENVISAGEABLES** |
| 3G, 4G, liaisons filaires |

|  |  |
| --- | --- |
| **DESCRIPTION DE LA SOLUTION RETENUE** | |
| **Conditions initiales** |  |
| **Conditions finales** |  |
| **Outils utilisés** | Putty, navigateur web |

|  |  |
| --- | --- |
| **CONDITIONS DE REALISATION** | |
| **Matériels** | Machines, switch, borne Wifi CISCO |
| **Durée** | 3 heures |
| **Contraintes** | Respect des commandes CISCO |

|  |  |  |
| --- | --- | --- |
| **COMPETENCES MISES EN OEUVRE POUR CETTE ACTIVITE PROFESSIONNELLE** | | |
| A1.1.1  A1.1.2  A1.2.2  A1.2.3  A1.3.4  A1.4.1  A1.4.2  A2.3.2  A3.1.1  A3.1.3  A3.2.1 | Analyse du cahier des charges d'un service à produire  Étude de l'impact de l'intégration d'un service sur le système informatique  Rédaction des spécifications techniques de la solution retenue  Évaluation des risques liés à l'utilisation d'un service  Déploiement d'un service  Participation à un projet  Évaluation des indicateurs de suivi d'un projet et justification des écarts  Proposition d'amélioration d'un service  Proposition d'une solution d'infrastructure  Prise en compte du niveau de sécurité nécessaire à une infrastructure  Installation et configuration d'éléments d'infrastructure | |
| **DEROULEMENT DE L'ACTIVITE** | |
| **Notion réseaux Wi-Fi :**  Le réseau Wi-Fi est un réseau distribué, c’est-à-dire qu’il partage la bande passante entre tous les postes intégré au réseau. Chaque poste s’intègre dans le réseau par une procédure négociation avec le contrôleur Wi-Fi.  **Normalisation techniques :**  La norme IEEE 802.11, est un standard règlementé par 3 organismes internationaux, WIFI c’est juste une marque déposé :   * IEEE : institut electronical electronics engineer (802.11 ; 802.11a ; 802.11b …) * WECA: wireless Ethernet compability alliance (interopérabilité entre les équipements répondant aux normes ci-dessus). * ETSI : europeen telecomunication standards institut (standards offrant les débits 10/20mbits ou 54mbits).   **Les normes 802.11 :**   * IEEE 802.11a : Bande de fréquences de 5 GHz et permet des débits allant jusqu’à 54 Mbits/s avec une plage de distance allant jusqu’à 25 mètres. Elle possède une zone de couverture plus petite et est moins efficace pour pénétrer des structures de bâtiments. Il n’y a pas d’interopérabilité entre les périphériques fonctionnant sous cette norme, 802.11b et 802.11g. * IEEE 802.11b : Bande de fréquences de 2,4 GHz et permet des débits allant jusqu’à 11 Mbits/s avec une plage de distance allant jusqu’à 35 mètres. Les périphériques mettant en oeuvre cette norme ont une portée plus longue et sont davantage capables de pénétrer les structures de bâtiments que les périphériques basés sur la norme 802.11a. * IEEE 802,11g : Bande de fréquences de 2,4 GHz et permet des débits allant jusqu’à 54 Mbits/s avec une plage de distance allant jusqu’à 25 mètres. Les périphériques mettant en oeuvre cette norme fonctionnent aux mêmes portées et radiofréquence que la norme 802.11b mais avec la bande passante de la norme 802.11a. * IEEE 802.11n : La norme IEEE 802.11n est actuellement à l’étude. La norme proposée définit la fréquence de 2,4 GHz ou 5 GHz. Les débits de données types attendus théoriques égales 300 Mbits/s avec une plage de distance allant jusqu’à 300 mètres.   Les autres services pris en charge par les réseaux 802.11 sont :   * + l’authentification (RADIUS voir doc)   + l’association (connectivité à un périphérique sans fil : SSID)   + la confidentialité (chiffrement : WAP, WEP, certificat,..)   Le sans fils WIFI utilise les ondes radio électriques, plusieurs technologies existe selon la fréquence d’émission, le débit et la portée des transmissions :   * Bande ISM 2.4Ghz pour une bande passante max de 84 Mhz * Bande U-NII 5.4Ghz pour une bande passante de 300 Mhz   **Procédure d’accès au réseau :**  Un réseau radio est un réseau partagé, il y a donc plusieurs machines. Afin d'éviter des conflits d’accès il y a une procédure d’accès au réseau radio.  Un réseau radio est identifié par plusieurs paramètre : fréquence de travail (canaux de transmissions), la bande utilisé (ISM ou Unii) et le nom du réseau (SSID) et enfin le mode de sécurisation (WiFi Protected Access). Cette procédure se passe en trois étapes :   * Processus de sondage (poste mobile se synchronise avec le contrôle WiFi. * Processus d'identification (mdp plus demande d'acceptation). * Procédure d'association récupération des paramètres réseau et entré dans la trames WiFi.   **Sécurité des réseaux sans fil :**  Un réseau sans fil est facile à implémenter mais vulnérable s'il n'est pas correctement configuré, etant donné que le signal sans fil traverse les murs, il est accessible depuis l'extérieur des locaux de l'entreprise. Les méthodes ci-après permettent de sécuriser un réseau sans fil :   * Filtrage d'adresse MAC: Empêche les ordinateurs indésirables de se connecter à votre réseau en imposant une restriction sur les adresses MAC. Toutefois, comme il est possible de cloner une adresse MAC, d'autres mesures de sécurité doivent être implémentées en plus du filtrage d'adresse MAC. * WEP: L'algorithme Wired Equivalent Privacy assure la sécurité des données par le chiffrement des données qui sont envoyées entre les nœuds sans fil. Il utilise une clé hexadécimale prépartagée de 64, 128 ou 256 bits pour chiffrer les données. Il existe de nombreux outils de déverrouillage WEP accessibles sur Internet. Le protocole WEP doit être réservé aux équipements anciens qui ne prennent pas en charge les protocoles de sécurité sans fil plus récents. * WPA : Wifi Protected Accessest un protocole de chiffrement sans fil plus récent qui utilise un algorithme de chiffrement amélioré appelé le protocole TKIP (Temporal Key Integrity Protocol). Le protocole TKIP génère une clé unique pour chaque client et fait tourner les clés de sécurité à un intervalle configurable. Le protocole WPA offre un mécanisme d'authentification réciproque. Étant donné que le client et le point d'accès possèdent tous deux la clé, celle-ci n'est jamais transmise. * WPA2: Wifi Protected Access 2 est une version améliorée et plus récente du protocole WPA. Il utilise la technologie de chiffrement AES (Advanced Encryption Standard), plus sécurisée. Il offre de nouvelles fonctionnalités de sécurité telles que le « Key Caching » qui permet a l’utilisateur de conserver la clé PMK, cela signifie qu’un utilisateur mobile n’a besoin de s’identifier qu’une seule fois avec un point d’accès spécifique.   **Configuration d’une borne Wi-Fi Cisco MR12 en interface graphique :**   * Décompactage * Adressage IP * Création du réseau * Création de deux SSID (utilisateurs et inviter) avec leurs paramétrage respectif (WPA2 personnel et WPA2 entreprise ; mode par défaut et d’authentification bridge)   SSID Public  SSID Personnel  Internet  Réseau Privé  VLAN Personnel  VLAN Public  Switch Cisco  2950  Routeur 2611XM  Cisco        La solution prototypée devra comporter :   * La création des sous réseaux SSID WIFI avec l’application des consignes de base de sécurité sur ces sous réseaux, * une séparation des deux réseaux Wifi en VLAN, * la gestion de l'accès internet. Le public et personnel M2L accèdent à Internet (filtrage), * la mise en place du service de DHCP par le point d’accès pour les 2 sous réseaux, * Isolation des 2 réseaux par le biais d’une sécurisation (Filtrage local ou authentification Radius). Seuls les personnels M2L et Ligues peuvent accéder au réseau interne privé.   **Atelier Scriba Bordeaux : Configuration de base Wi-Fi Cisco MR12 en interface graphique**   * Décompactage * Adressage IP * Création du réseau * Création de deux SSID (utilisateurs et inviter) avec leurs paramétrage respectif (WPA2 personnel et WPA2 entreprise ; mode par défaut et d’authentification bridge)   **Configuration  borne CISCO en TP au cours de la deuxième année**   1. **Branchement:**  * Matériel : switch, routeur, point d’accée wifi, * Câbles Ethernets PA-switch (fa0/1) ; PC-switch (fa0/2) ; switch-routeur  1. **Point d’accès (SSID, VLAN, Sécurité cryptage et clé wifi, config dhcp) :**  * Sur interface web, express security : configuration des SSID PERSONNEL et PUBLIC, activer le mode diffusion sur le SSID PUBLIC (pour qu’il soit visible et non le SSID PERSONNEL pour plus de sécurité). * Ensuite dans le menu security, il configurer le mode d’encryptions de la communication, activer le mode cipher AES CCMP\*. * Ouvrir le SSID manager et configurer les mode de clé, la clé utiliser pour la wifi PERSONNEL\* * Toujours dans la l’interface graphique de configuration de la borne WIFI, configuration des 2 étendues (172.16.101.0 /28 et 172.16.100.0/24 ; DNS-server 172.16.2.61)  1. **Configuration du switch (VLAN, trunk routeur-switch) :**  * Création des VLANs (100) PUBLIC et (101)PERSONNEL, * Affectation d’une adresse IP au VLANs ensuite il faut affecter les port au VLANs, * Activer le trunk switch-routeur et switch-PA. * Vérifier les configuration avec un show vlan ( ou show conf)  1. **Configuration routeur : encapsulation ; acl ; (étendu) ; OSPF (routage des 2 vlans) :**  * Affectation des adresse ip au sous interfaces pour les VLANs ainsi que le mode d’encapsulation fa0/1.100 et fa0/1.101 (faire un nom logique de la sous interface avec lID du VLAN). * Routage dynamique des deux VLANs avec OSPF | |

|  |
| --- |
| **CONCLUSION** |
| La Wi-Fi est de plus en plus utilisé, j’ai remarqué qu’il est très souvent utilisé dans les salles de réunion pour avoir un accès à internet en dehors de son bureau ou pour des connections de personne externe à l’entreprise. |

|  |
| --- |
| **EVOLUTION POSSIBLE** |
|  |