RÉSEAU INTERNET

Pour déployer un réseau Internet performant pour le parc informatique tout en respectant les contraintes spécifiées dans le projet M2L, voici une méthode structurée :

Étape 1 : Établir une connexion principale à Internet

1. **Choix du fournisseur d'accès à Internet (FAI) :**

   Optez pour un fournisseur proposant une connexion fibre optique professionnelle (SLA, garantie de temps de rétablissement, débit symétrique).
   Débit recommandé : **1 Gbps symétrique** pour 150 utilisateurs, extensible en fonction de la croissance.
2. **Point d'entrée principal :**

   Installation du routeur principal dans le bâtiment principal (centre névralgique du réseau).
   Reliez ce routeur à une baie de brassage équipée d'un switch principal managé.

Étape 2 : Interconnexion entre les bâtiments

1. **Connexion par fibre optique :**

   Reliez les bâtiments secondaires (ailes Est et Ouest) au bâtiment principal via des liens **fibre optique multimode**.
   Utilisation des modules SFP+ sur les switches des baies de brassage pour connecter la fibre.
2. **Sécurité et redondance :**

   Installation d'un second lien en fibre comme connexion de secours (spare) pour éviter les interruptions.
   Activation des protocoles comme **Spanning Tree Protocol** (Protocole réseau qui construit une topologie logique sans boucle**)** pour éviter les boucles.

Étape 3: Réseau interne filaire

1. **Distribution des connexions :**

   Mise en place des switches managés dans chaque baie de brassage pour distribuer les connexions.
   Préférez des switches avec **PoE+** (Le Power over Ethernet ou l’alimentation électrique par câble Ethernet) pour alimenter les équipements réseau tels que les bornes Wi-Fi.

2. **Câblage réseau :**

   Utilisation du **câble Cat 6a** pour toutes les connexions RJ45 dans les bureaux.
   Répartition des prises réseau en fonction des plans d'aménagement (open-space ou cloisonné).
3. **Configuration des VLAN(connexion virtualisée qui relie plusieurs périphérique :**

   Création des VLAN pour séparer les différents types de trafic :
   - VLAN 10 : Administration.
   - VLAN 20 : Invités.
   - VLAN 30 : IoT (si applicable).

Étape 4 : Réseau Wi-Fi

1. **Bornes Wi-Fi :**

   Installation des bornes compatibles **Wi-Fi 6** dans chaque bâtiment.
   Placez une borne tous les 15 à 20 mètres dans les espaces ouverts, ou plus densément si le béton affecte le signal.
2. **Gestion centralisée :**

   Configuration d'un **contrôleur Wi-Fi** pour gérer les bornes (Ubiquiti, Cisco ou Aruba).
   Optimisez les canaux pour réduire les interférences (2,4 GHz et 5 GHz).
3. **Accès sécurisé :**

   Configuration d'un portail captif pour les visiteurs avec authentification.
   Utilisez **WPA3** et, si possible, une **authentification 802.1X** pour les connexions filaires et Wi-Fi des administrateurs.

Étape 5 : Sécurité du réseau

1. **Pare-feu principal :**

   Installation d'un pare-feu matériel (Fortinet, Cisco ASA, ou Sophos).
   Configuration des règles strictes pour protéger les VLAN et bloquer les attaques externes.
2. **Détection et prévention :**

   Activation des fonctionnalités IDS/IPS (Intrusion Detection and Prevention System).
3. **DNS sécurisé :**

   Utilisation des services DNS filtrants pour protéger les utilisateurs (ex. Quad9, Cloudflare DNS).

Étape 6 : Monitoring et gestion

1. **Outils de supervision :**

   Installation d'un logiciel de gestion réseau tel que **Zabbix**, **PRTG** ou **Nagios** pour surveiller l'état des équipements.
   Configuration des alertes pour les défaillances ou saturations.
2. **Documentation :**

   Nominations des équipements et des prises selon la **RFC 1178**.
   Créez une documentation claire avec :
   - Schémas réseau.
   - Configurations VLAN.
   - Inventaire des équipements.

Étape 7 : Test et déploiement

1. **Validation en laboratoire :**

   Simulation de la configuration avec **Packet Tracer** pour vérifier la topologie logique.
2. **Déploiement progressif :**

   Configuration du bâtiment principal, puis des bâtiments secondaires.
   Test de chaque connexion (filaire et Wi-Fi) avec des outils comme **iPerf**.
3. **Plan de secours :**

   Préparation d'un plan pour revenir à une configuration stable en cas d'échec.

Étape 8 : Gestion des serveurs et infrastructure associée

1. **Hébergement des serveurs**

   Installation d'une salle dédiée dans le bâtiment principal, équipée de climatisation, onduleurs pour l'alimentation, et contrôle d'accès sécurisé.

2. **Connectivité des serveurs**

   Reliez les serveurs via un switch managé configuré en **VLAN** dédié, avec une connexion fibre ou Ethernet à haut débit.

3. **Sécurisation des serveurs**

   Installation des serveurs derrière le pare-feu principal et utilisation d'une **DMZ**(réseau périmétrique qui protège et ajoute une couche de sécurité supplémentaire au réseau local interne) pour les services accessibles depuis Internet.

4. **Sauvegarde et redondance**

Mise en place des sauvegardes régulières et configuration des disques en **RAID** c'est-à- dire répartir des données sur plusieurs disques pour assurer la sécurité(en cas de perte) et la continuité des données critiques.

Simulation Packet Tracer