Nom : **LAGUERRE**
Prénom : **Rithler**
Université : **UNITECH**
Concentration : **CyberSecurity**
Cours : **Architecture des Réseaux**
Enseignante : **Judith Soulamite Nouho Noutat**

TD/TP 3

Exercice 1 (Approfondissement des notions vues en cours)

Explication des notions et services suivantes :

1. **Commutation de niveau 2**

La commutation de niveau 2 fonctionne au niveau de la couche liaison de données du modèle OSI. Elle utilise les adresses MAC pour acheminer les trames entre les dispositifs au sein d'un même réseau local. Les commutateurs de niveau 2 construisent et maintiennent une table d'adresses MAC (table CAM) associant ces adresses aux ports physiques, permettant ainsi une transmission efficace des trames sans diffusion inutile.

2. **Commutation de niveau 3**

La commutation de niveau 3 combine les fonctionnalités d'un routeur et d'un commutateur. Elle opère au niveau réseau du modèle OSI en utilisant les adresses IP pour prendre des décisions de routage. Contrairement à la commutation de niveau 2, elle permet la communication entre différents réseaux en examinant l'adresse IP de destination et en déterminant le meilleur chemin via des tables de routage.

- Services de la couche accès du modèle de conception hiérarchique :

3. **Adressage de réseau à valeur ajoutée**

Ce service fournit des mécanismes d'attribution d'adresses IP aux dispositifs d'extrémité (via DHCP), incluant des informations supplémentaires comme les serveurs DNS, les passerelles par défaut et autres paramètres réseau. Il simplifie la configuration des équipements tout en assurant une allocation cohérente des ressources d'adressage dans l'organisation.

4. **Segmentation de réseau**

La segmentation divise un réseau en sous-réseaux logiques distincts pour améliorer les performances et la sécurité. À la couche d'accès, elle s'effectue généralement via des VLANs qui isolent le trafic entre groupes de travail ou départements, réduisant

ainsi les domaines de collision et de diffusion, tout en permettant une application plus granulaire des politiques de sécurité.

5. **Diffusion broadcast et diffusion multicast**

La diffusion broadcast permet d'envoyer des données à tous les hôtes d'un réseau, tandis que le multicast cible un groupe spécifique d'hôtes. La couche d'accès gère ces types de trafic en définissant leur portée, en filtrant les broadcasts excessifs et en implémentant des protocoles comme IGMP pour optimiser la distribution du multicast, réduisant ainsi la consommation inutile de bande passante.

6. **Services de noms, de proxy et de cache local**

Ces services améliorent les performances réseau en localisant les ressources de résolution de noms (DNS) et les caches web au niveau de la couche d'accès. Les serveurs proxy interceptent les requêtes des utilisateurs pour les servir localement quand possible, réduisant ainsi la latence et économisant la bande passante du réseau fédérateur, tout en offrant un contrôle d'accès additionnel.

7. **Sécurité de l'accès au média**

Ce service comprend les mécanismes contrôlant l'accès physique et logique aux ressources réseau, tels que l'authentification 802.1X, le filtrage MAC, la sécurisation des ports de commutation (port-security) et les VLANs dynamiques. Ces mesures protègent contre les accès non autorisés et assurent que seuls les utilisateurs légitimes peuvent se connecter au réseau.

8. **Découverte de routeurs**

La découverte de routeurs permet aux périphériques d'identifier automatiquement les routeurs disponibles sur leur réseau local. Des protocoles comme ICMP Router Discovery Protocol (IRDP) ou Neighbor Discovery Protocol (NDP) dans IPv6 permettent aux hôtes de localiser leur passerelle par défaut sans configuration manuelle, facilitant ainsi leur connexion à d'autres réseaux.

- <u>Services de la couche distribution:</u>

9. **Gestion de la bande passante du réseau fédérateur**

Ce service implique l'implémentation de mécanismes de Quality of Service (QoS) et de contrôle de flux pour garantir une utilisation optimale des liens vers la couche centrale. La couche distribution priorise le trafic critique, façonne le débit des applications gourmandes en bande passante et agrège les connexions de la couche d'accès pour maximiser l'efficacité du réseau fédérateur.

10. **Filtrage de zones et de services**

Le filtrage à la couche distribution établit des frontières de sécurité entre les différentes zones du réseau en implémentant des listes de contrôle d'accès (ACLs) et des règles de pare-feu. Ce service contrôle le trafic autorisé entre les segments, filtre les protocoles indésirables et isole les ressources sensibles, formant ainsi une deuxième ligne de défense après la couche d'accès.

11. **Distribution stratégique**

La distribution stratégique implique la répartition intelligente du trafic réseau selon des politiques précises tenant compte des besoins de l'entreprise. Elle utilise des protocoles de routage avancés pour diriger les flux de données vers les ressources appropriées, applique des règles de routage basées sur l'application ou l'utilisateur, et optimise les chemins selon la nature du trafic.

12. **Services de passerelle**

Ces services assurent l'interconnexion entre différents types de réseaux en traduisant les protocoles et formats de données. Les passerelles à la couche distribution peuvent connecter les segments LAN aux réseaux WAN, traduire entre IPv4 et IPv6, ou intégrer des systèmes de communication distincts, tout en appliquant les politiques de sécurité appropriées aux points de transition.

13. **Redistribution de routes interprotocoles**

Ce mécanisme permet l'échange d'informations de routage entre différents protocoles (comme OSPF, EIGRP ou BGP). La couche distribution assure que les routes découvertes par un protocole soient accessibles aux routeurs utilisant d'autres protocoles, permettant ainsi une connectivité homogène à travers des environnements réseau hétérogènes tout en contrôlant la propagation des informations de routage.

14.**Traduction du format de trame**

Ce service convertit les formats de trames entre différentes technologies réseau (par exemple, Ethernet vers MPLS ou ATM). La couche distribution adapte les en-têtes, tailles et formats des trames pour permettre la communication entre des infrastructures réseau différentes, tout en préservant l'intégrité des données transportées à travers ces transitions technologiques.

Services de la couche centrale

15. **Optimisation du chemin**

Ce service utilise des algorithmes de routage avancés pour déterminer les chemins les plus efficaces à travers le réseau central. Il s'appuie sur des protocoles comme OSPF

ou IS-IS qui prennent en compte la bande passante, la latence et d'autres métriques pour calculer dynamiquement les meilleures routes, réduisant ainsi les délais de transmission et maximisant le débit global.

16. **Priorité du trafic**

La gestion de priorité à la couche centrale implémente des mécanismes QoS avancés pour traiter différemment les flux selon leur importance. Ce service identifie et marque les paquets critiques (voix, vidéo, données sensibles), leur alloue les ressources nécessaires et leur garantit un traitement préférentiel durant les périodes de congestion, assurant ainsi la performance des applications essentielles.

17. **Équilibrage de charge**

Ce service distribue équitablement le trafic entre plusieurs chemins ou ressources disponibles pour éviter la surcharge de certains liens. La couche centrale implémente des techniques comme Equal-Cost Multi-Path (ECMP) ou des algorithmes de répartition de charge plus sophistiqués pour maximiser l'utilisation des ressources réseau tout en améliorant la résilience face aux pics de trafic.

18. **Chemins alternatifs**

La gestion des chemins alternatifs assure la continuité de service en cas de défaillance d'un lien ou d'un équipement. La couche centrale maintient des routes de secours préétablies et peut rapidement basculer le trafic vers ces chemins alternatifs grâce à des protocoles comme Fast Reroute, minimisant ainsi l'impact des pannes sur les communications critiques de l'entreprise.

19. **Accès commuté**

Ce service fournit des connexions à la demande pour les utilisateurs ou sites distants. Au niveau de la couche centrale, il s'agit généralement de gérer les interconnexions avec les fournisseurs d'accès, les connexions VPN concentrées ou les liaisons WAN redondantes, permettant l'établissement dynamique de connexions selon les besoins tout en maintenant la sécurité et la qualité de service.

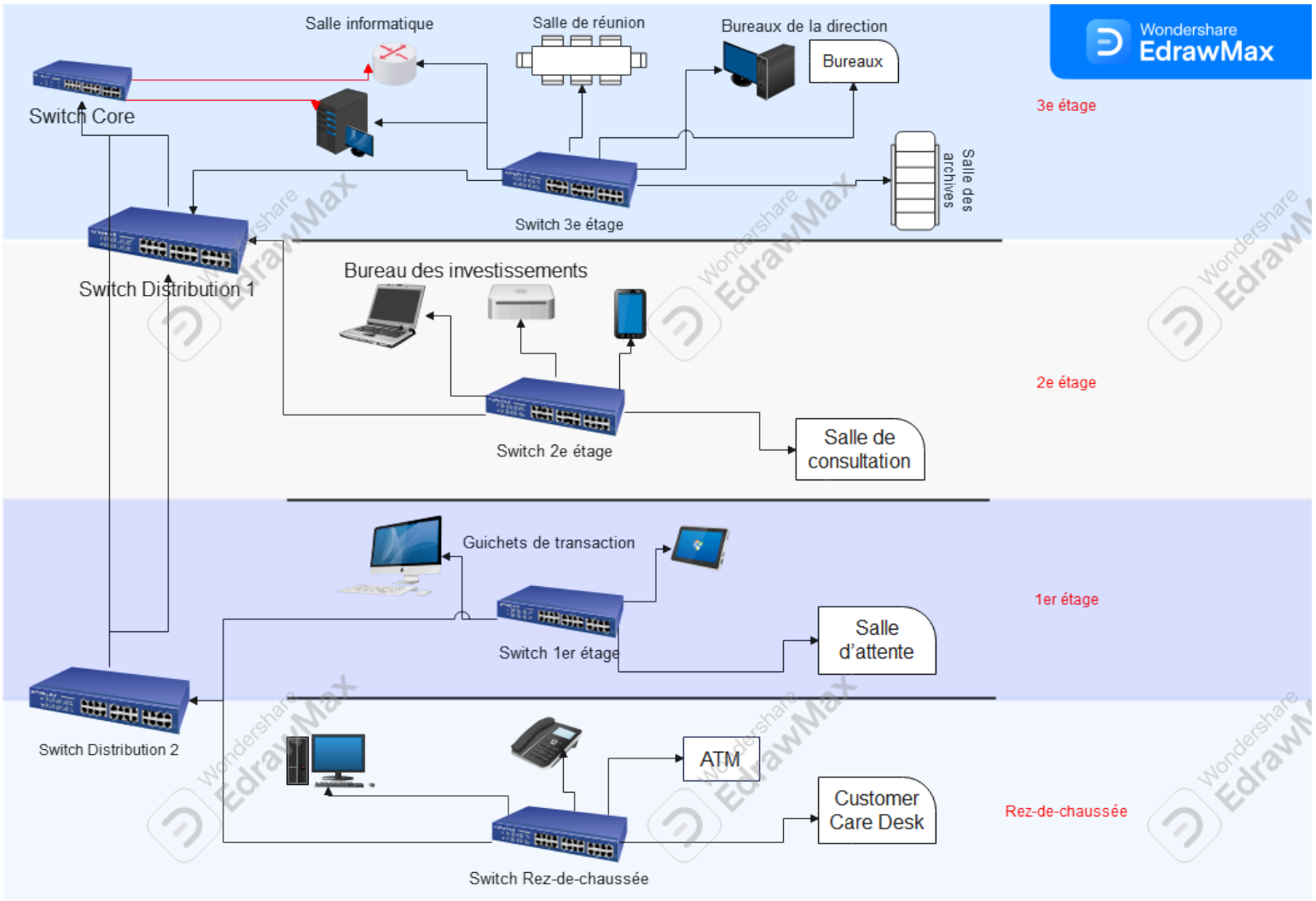
20. **Encapsulation (mise en œuvre d'un tunnel)**

L'encapsulation consiste à envelopper un protocole dans un autre pour permettre son transport à travers des réseaux qui ne le supportent pas nativement. À la couche centrale, cette technique est utilisée pour implémenter des VPNs, transporter IPv6 sur IPv4, ou créer des réseaux virtuels overlay. Les tunnels ainsi créés traversent le réseau central tout en isolant et protégeant le trafic encapsulé.

Exercice 2 (Conception et utilisation d'EdrawMax pour dessiner une architecture de réseau de campus pour une banque)

L'architecture réseau que je propose pour la banque suit le modèle hiérarchique à trois couches, reconnu comme une pratique standard dans la conception de réseaux d'entreprise. Cette approche modulaire permet d'obtenir un réseau robuste, évolutif et facile à gérer, tout en répondant aux exigences spécifiques d'une institution financière.

Schéma de l'architecture :



NB : Ce schéma montre une vue d'ensemble de l'architecture, avec les couches d'accès, de distribution et coeur.

Cette conception divise le réseau en trois couches distinctes, chacune avec des fonctions spécifiques:

Couche d'accès : Fournit une connectivité réseau aux utilisateurs finaux et aux appareils.

Couche de distribution : Aggrège les connexions de la couche d'accès et fournit une connectivité basée sur des politiques.

Couche core (cœur) : Constitue l'épine dorsale du réseau, assurant un transport rapide et fiable des données.

Description détaillée de l'architecture proposée

1. Couche d'accès

Cette couche constitue le point d'entrée du réseau pour tous les utilisateurs et équipements de la banque. Elle est composée de:

Switch Rez-de-chaussée : Connecte les postes du hall d'accueil, les guichets ATM et le service client (Customer Care Desk).

Switch 1er étage : Dessert les guichets de transaction et la salle d'attente.

Switch 2e étage : Relie le bureau des investissements (avec postes fixes, portables et appareils mobiles) et la salle de consultation.

Switch 3e étage : Connecte les bureaux de la direction, la salle de réunion et la salle des archives.

Ces commutateurs d'accès assurent plusieurs fonctions essentielles:

Authentification des utilisateurs.

Application des politiques de sécurité.

Gestion du trafic local.

Point de connexion pour tous les équipements terminaux.

2. Couche de distribution

Cette couche intermédiaire joue un rôle crucial de liaison et de contrôle:

- Switch Distribution 1 et Switch Distribution 2: Placés de manière redondante pour assurer la haute disponibilité du réseau.

Ces équipements remplissent plusieurs fonctions clés:

- Agrégation du trafic provenant des différents switches d'accès.
- Filtrage et segmentation du trafic (mise en place de VLANs).
- Application des politiques de qualité de service.
- Routage entre les différents sous-réseaux.
- Redondance des passerelles par défaut.

3. Couche core (cœur)

Située dans la salle informatique du 3e étage, cette couche constitue l'épine dorsale du réseau bancaire:

- Switch Core: Commutateur haute performance qui forme le cœur du réseau.

Ce switch core remplit des fonctions critiques:

- Transport rapide et fiable des données entre les différentes parties du réseau.
- Connexion avec les serveurs bancaires critiques.
- Liaison avec le routeur pour la connectivité externe.
- Optimisation des performances globales du réseau.

Justification du matériel utilisé

Commutateurs d'accès (Layer 2)

Pour chaque étage, nous utilisons des commutateurs d'accès Ethernet avec un nombre de ports adapté aux besoins de l'étage correspondant:

- Commutateurs 48 ports PoE+: Ces équipements offrent:
    - Capacité suffisante pour connecter tous les postes clients, téléphones IP et autres équipements.
    - Alimentation via Ethernet (PoE+) pour les téléphones IP et éventuels points d'accès sans fil.
    - Support des VLANs pour la segmentation du trafic.
    - Sécurité de niveau 2 (filtrage MAC, port security).

Justification: Le choix de commutateurs PoE+ permet de simplifier le câblage en alimentant les téléphones et autres équipements directement via le câble réseau, réduisant ainsi les coûts d'infrastructure et facilitant l'installation.

Commutateurs de distribution (Layer 2/3)

Deux commutateurs multicouches redondants assurent la couche de distribution:

- Commutateurs Layer 3 avec redondance: Ces équipements fournissent:
    - Routage inter-VLAN à haute vitesse.
    - Agrégation de liens (Link Aggregation) pour augmenter la bande passante.

    - Support des protocoles de redondance (HSRP/VRRP).
    - Filtrage avancé et capacités ACL.

Justification: La redondance à ce niveau est cruciale pour assurer la haute disponibilité du réseau bancaire. L'utilisation de deux commutateurs de distribution permet d'éviter tout point unique de défaillance et garantit la continuité des services même en cas de panne d'un équipement.

Commutateur core (Layer 3)

Le cœur du réseau repose sur un commutateur haute performance:

- Commutateur core hautes performances: Cet équipement offre:
    - Grande capacité de commutation (backplane).
    - Ports haute vitesse (10G/40G).
    - Haute disponibilité avec redondance interne.
    - Faible latence pour des performances optimales.

Justification: Le commutateur core doit être dimensionné pour gérer l'ensemble du trafic réseau sans congestion, tout en offrant des performances et une fiabilité maximales. Son placement dans la salle informatique permet une sécurisation physique optimale.

Équipements additionnels

- Serveurs dans la salle informatique: Hébergent les applications bancaires, bases de données client, systèmes de traitement des transactions.
- Routeur Internet: Assure la connectivité sécurisée vers l'extérieur (siège social, autres agences, Internet).
- Équipements de téléphonie IP: Intégrés au réseau pour les communications internes et externes.