Architecture de réseaux

Enseignante: Judith Soulamite Nouho Noutat, Msc en Informatique

Chapitre 5: Conception de réseaux LAN commutés

Rack /Baie/
Coffret de brassage

Topologies des petits réseaux

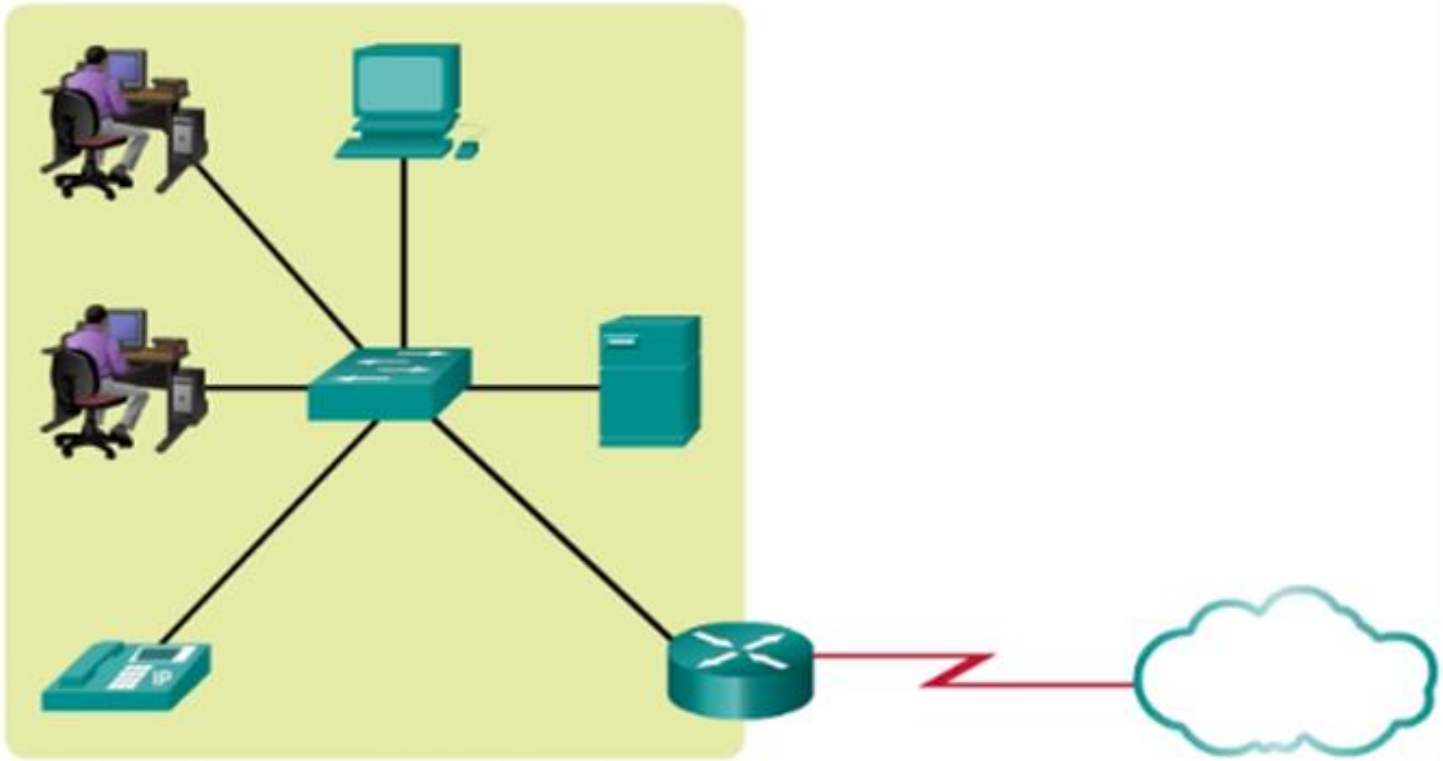
- La majorité des entreprises sont petites → la majorité des réseaux d'entreprises sont également petits.

- Une petite conception de réseau est généralement simple.
  - Le nombre et les types de périphériques inclus sont largement réduits par rapport à un réseau plus étendu.

- Les topologies des réseaux de petite taille exigent généralement un seul routeur et un ou plusieurs commutateurs. Les réseaux de petite taille peuvent également comporter des points d'accès sans fil (éventuellement intégrés au routeur) et des téléphones IP.

- En terme de connexion à Internet, les réseaux de petite taille comportent généralement une seule connexion de réseau étendu par DSL, le câble ou une connexion Ethernet.

Topologies des petits réseaux



Choix des périphériques d'un réseau de petite taille

- Pour répondre aux besoins des utilisateurs, même les réseaux de petite taille doivent faire l'objet d'une planification et d'une conception.
  - La planification garantit que tous les besoins, les facteurs de coûts et les options de déploiement sont pris en compte.

- Plusieurs facteurs déterminent le choix des périphériques intermédiaires:
  - **Coût**: équipements, câblage, maintenance, redondance, alimentation
  - **Vitesse et types de port/d'interface** : Nombre de ports, ports en cuivre, ports à fibre optique
  - **Évolutivité**: configurations physiques fixes ou modulaires
  - **Fonctions et services du système d'exploitation**: Sécurité, QoS, VoIP, commutation de couche 3, NAT, DHCP, fibre optique

Adressage IP d'un réseau de petite taille

- Chacun des types de périphériques doit être alloué à un bloc d'adresses logique dans la plage d'adresses du réseau.

- Le schéma d'adressage IP doit être planifié, documenté et mis à jour en fonction du type de périphérique recevant l'adresse.

- Exemples de différents types de périphériques qui détermineront le modèle IP :
  - Périphériques finaux pour les utilisateurs
  - Serveurs et périphériques
  - Hôtes accessibles depuis Internet
  - Périphériques intermédiaires

Redondance dans un petit réseau

- Un autre aspect important de la conception d'un réseau est la fiabilité.
  - Même dans les petites entreprises, le réseau joue un rôle déterminant.
  - La moindre panne du réseau peut coûter très cher.

- Pour assurer un niveau de fiabilité élevé, la redondance doit être pensée dans la conception du réseau.
  - La redondance permet d'éliminer les points de défaillance uniques.
  - Il existe plusieurs moyens d'assurer la redondance d'un réseau.
  - Elle peut passer par l'installation d'équipements en double, mais elle peut également être assurée par le doublement des liaisons réseau dans les zones critiques.

Redondance dans un petit réseau

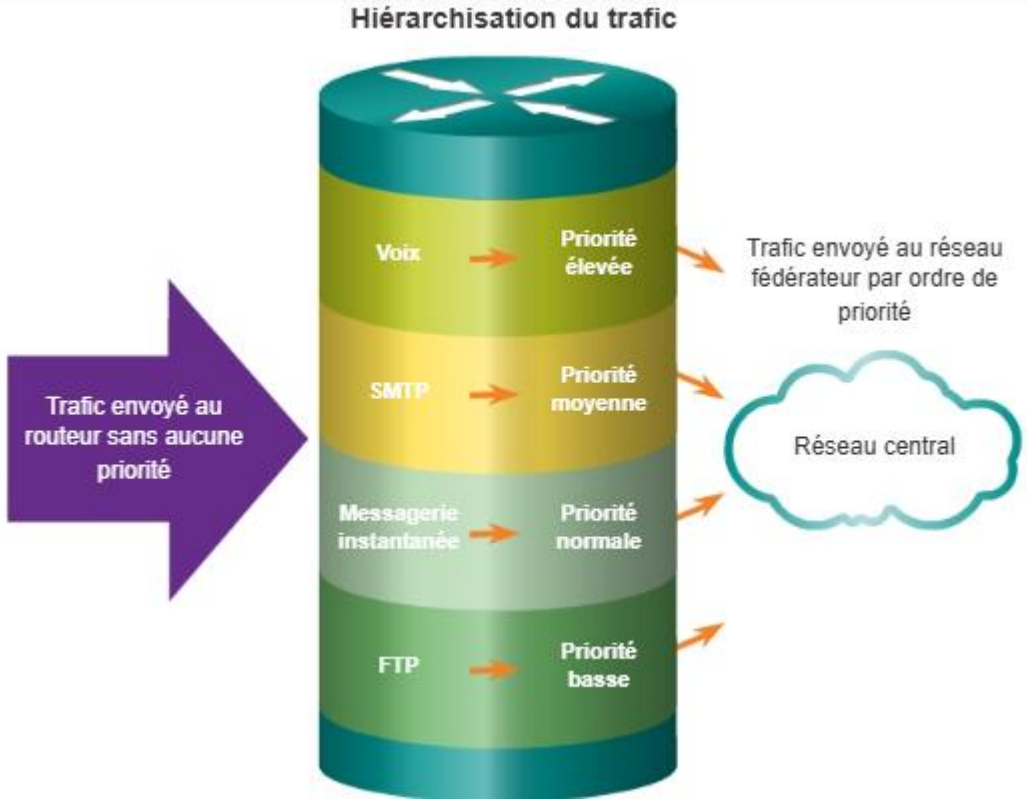
- Dans un réseau de petite taille, les serveurs sont généralement déployés en tant que serveurs Web, serveurs de fichiers ou serveurs de messagerie.
  - Ils offrent en général un seul point de sortie vers Internet via une ou plusieurs passerelles par défaut.
  - Il est conseillé aux petites entreprises de prendre une option à moindre coût chez un second fournisseur d'accès par mesure de sécurité.

Considérations liées à la conception d'un petit réseau

- L'administrateur réseau doit tenir compte des différents types de trafic et de leur traitement dans la conception du réseau.

- Dans un réseau de petite taille, les routeurs et les commutateurs doivent être configurés pour prendre en charge le trafic en temps réel, comme la voix et la vidéo, et ce, séparément du trafic des autres données.

- Dans une conception de réseau bien pensée, le trafic est classifié de manière précise en fonction des priorité



Protocoles courants d'un petit réseau

- Les protocoles réseau prennent en charge les services et applications utilisés par les employés d'un petit réseau.

- Protocoles réseau les plus courants :
  - DNS
  - Telnet
  - IMAP, SMTP, POP (e-mail)
  - DHCP
  - HTTP
  - FTP

Applications en temps réel pour un petit réseau

- Pour prendre en charge les applications en temps réel existantes et prévues, l'infrastructure doit être compatible avec les caractéristiques de chaque type de trafic.

- **VoIP**
  - La voix sur IP (VoIP) est mise en œuvre dans les entreprises qui utilisent encore des téléphones traditionnels.
  - La VoIP fait appel à des routeurs compatibles avec les services de voix

- **Téléphonie IP**
  - Les téléphones IP utilisent un serveur dédié pour le contrôle des appels et la signalisation.

- **Applications en temps réel**
  - Pour transporter efficacement des flux multimédias en continu, le réseau doit être en mesure de prendre en charge les applications sensibles aux retards d'acheminement.
  - Les protocoles RTP (Real-Time Transport Protocol) et RTCP (Real-Time Transport Control Protocol) répondent tous deux à cette exigence.

Sécurité dans un petit réseau

- La sécurité du réseau passe par la protection des périphériques réels, y compris les périphériques finaux et intermédiaires, tels que les périphériques réseau.

- Voici quelques étapes simples qu'il convient d'effectuer sur la plupart des systèmes d'exploitation :
  - Changement immédiat des noms d'utilisateur et des mots de passe par défaut.
  - Accès aux ressources du système limité strictement aux personnes autorisées à utiliser ces ressources.
  - Désactivation des services et applications qui ne sont pas nécessaires et désinstallation dans la mesure du possible.

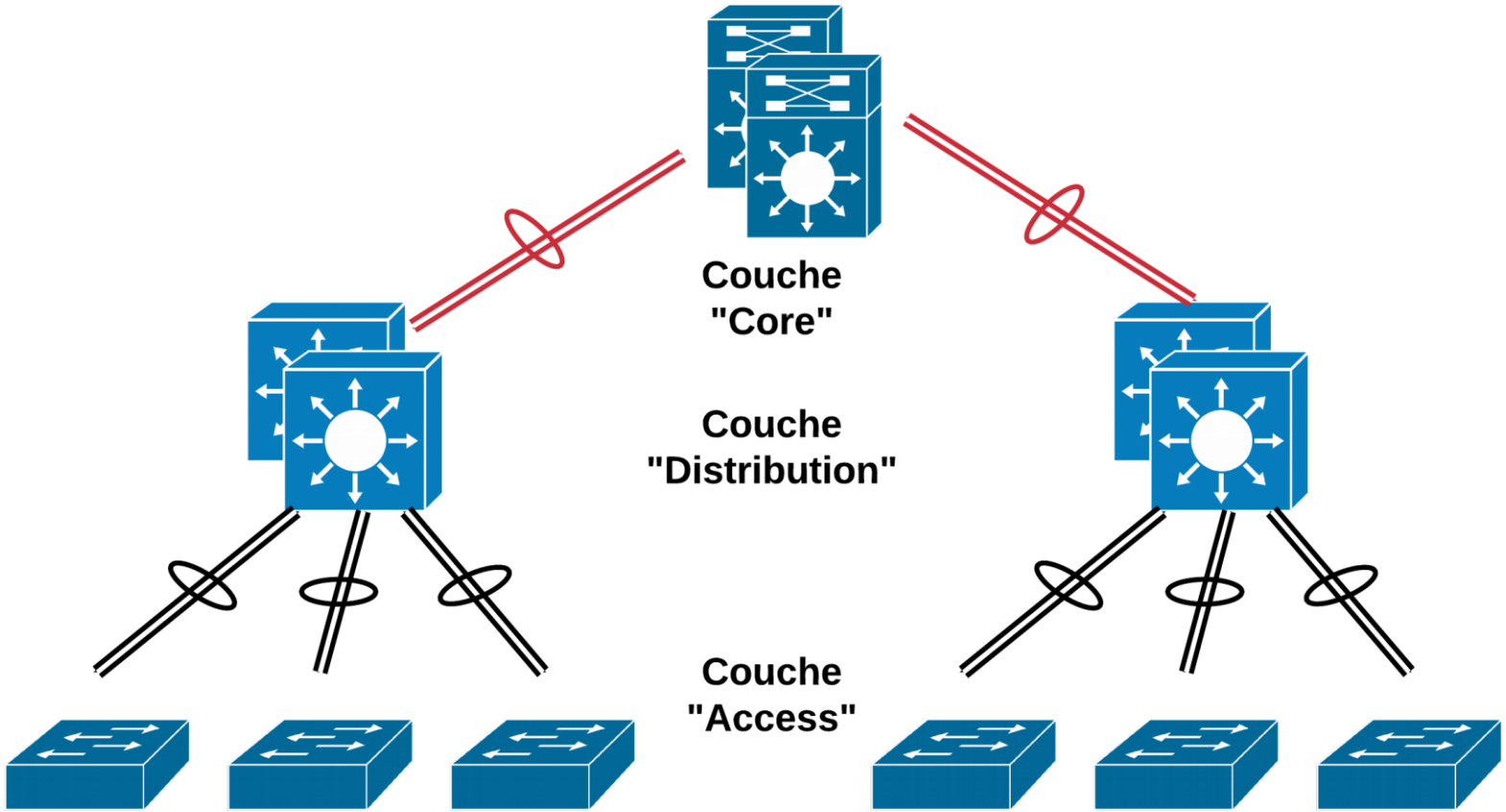
Principes de conception LAN commuté

- Les principes de conception des réseaux LAN (LAN Design) sont popularisés par Cisco Systems dans un modèle de conception hiérarchique et modulaire à trois couches : Access, Distribution et Core.

- L'infrastructure devrait répondre à plusieurs critères.
  - Elle est documentée et basée sur un modèle de conception.
  - Elle est robuste avec une redondance L1, L2 et L3.
  - Elle est évolutive avec une possibilité de déployer une architecture VLAN.
  - Elle est sécurisée, documentée et dispose de mécanismes d'authentification forte

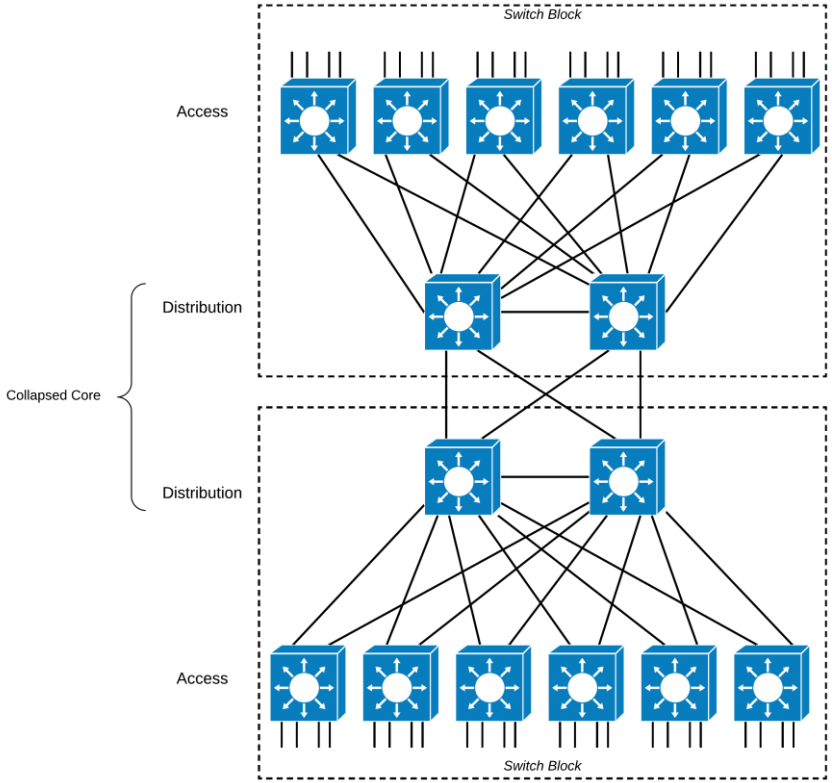
Modèle hiérarchique à trois couches / 3 Tier

- Dans une modèle de conception 3 Tier on trouve trois couches d'agrégation du trafic.



Collapsed Core / 2 Tier

- Toutes les situations ne nécessitent pas une couche Core dédiée.
  - Dans ce cas, on peut simplifier la topologie en “Collapsed Core” en réduisant le nombre de couches de trois à deux selon un modèle 2 Tier.



Principes d’un modèle de conception

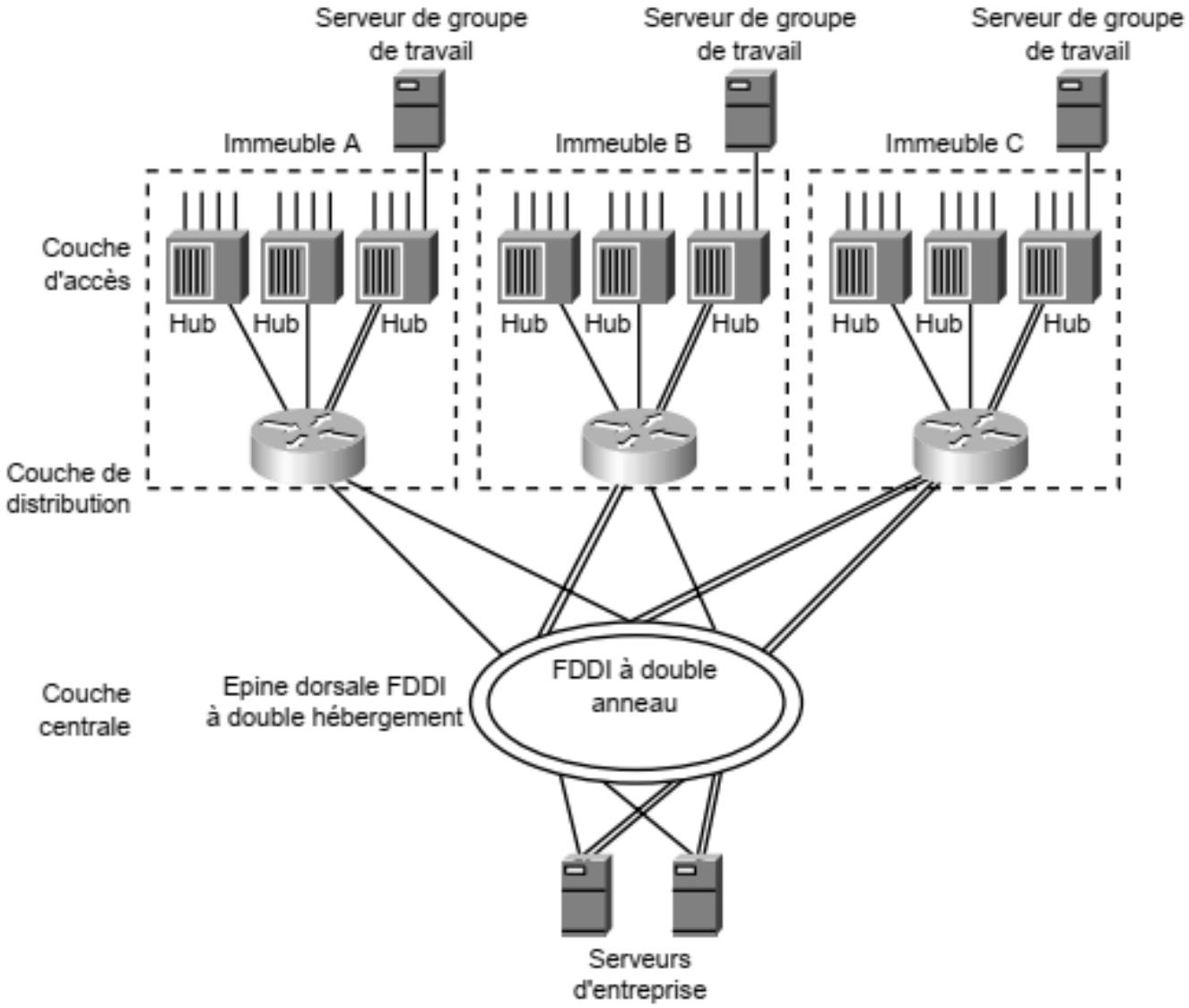
- **Hiérarchie** : le modèle offre des niveaux fonctionnels : Core/Distribution/Access
- **Modularité** : il supporte facilement la croissance et les changements; faire évoluer le réseau est facilité par l’ajout de nouveaux modules au lieu redessiner entièrement l’architecture du réseau.
- **Résilience** : il supporte la haute disponibilité (HA) proche des 100 % de disponibilité
- **Flexibilité** : les changements dans l’entreprise peuvent être adaptés au réseau rapidement selon les besoins
- **Sécurité** : la sécurité est intégrée au niveau de chaque couche

Composants du modèle de réseau commuté

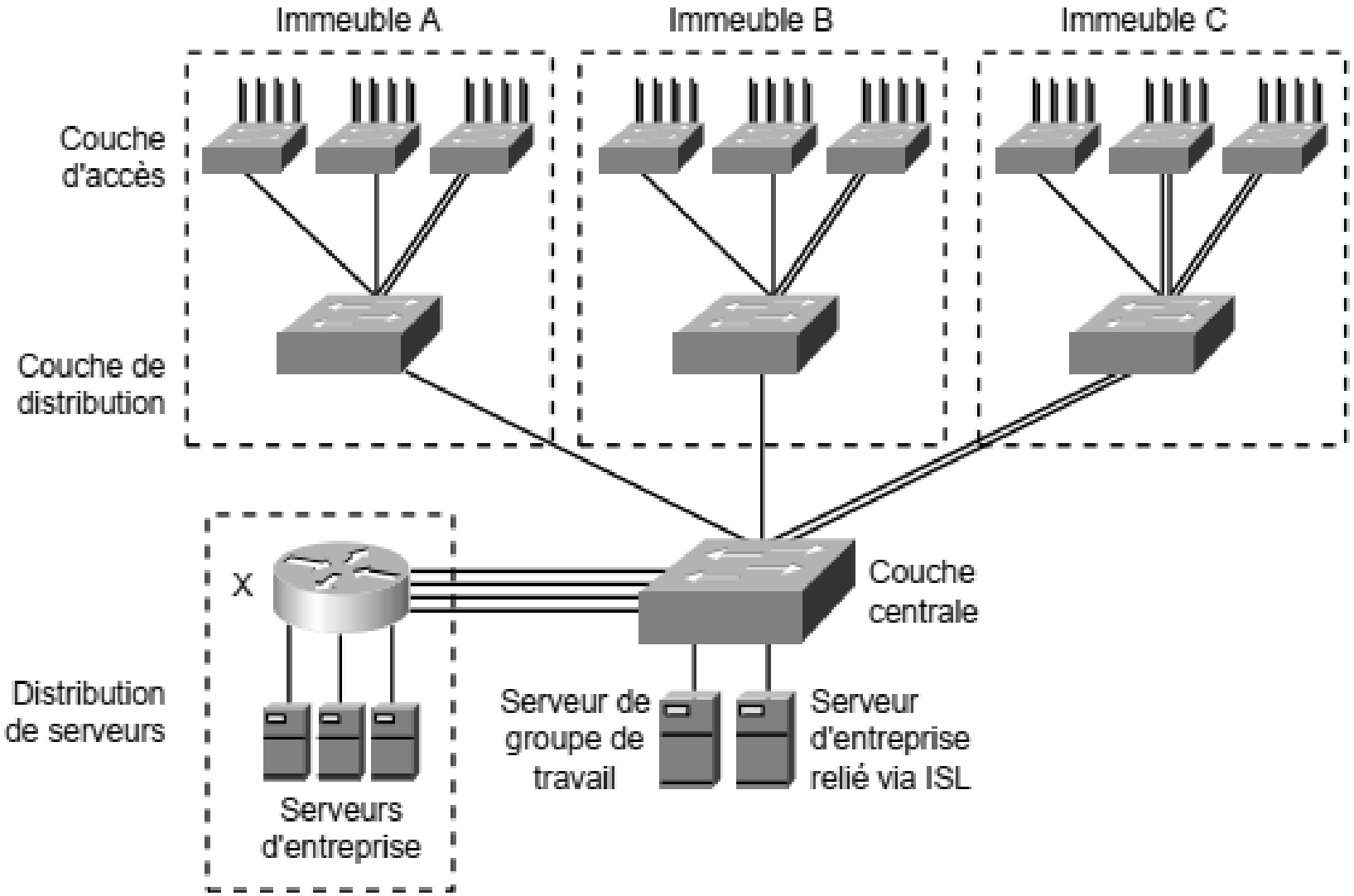
- Un réseau commuté englobe les trois composants de base suivants :
  - **Des plates-formes de commutation physiques**:
    - commutateur ATM, commutateur LAN / multicouche, routeur de commutation.
  - **Une infrastructure logicielle commune:**
    - Sa fonction est d'unifier la diversité des plates-formes de commutation physique.
    - Elle devrait permettre de réaliser les tâches suivantes :
      - surveillance de la topologie logique du réseau ;
      - routage et reroutage logique du trafic ;
      - gestion et contrôle du trafic sensible ;
      - fourniture de systèmes pare-feu, de passerelles, du filtrage et de la traduction de protocoles.
  - **Des outils et des applications d'administration de réseau:**
    - les applications d'administration sont nécessaires à la surveillance, à la configuration, à la planification et à l'analyse des équipements et des services

Conception de réseaux LAN commutés

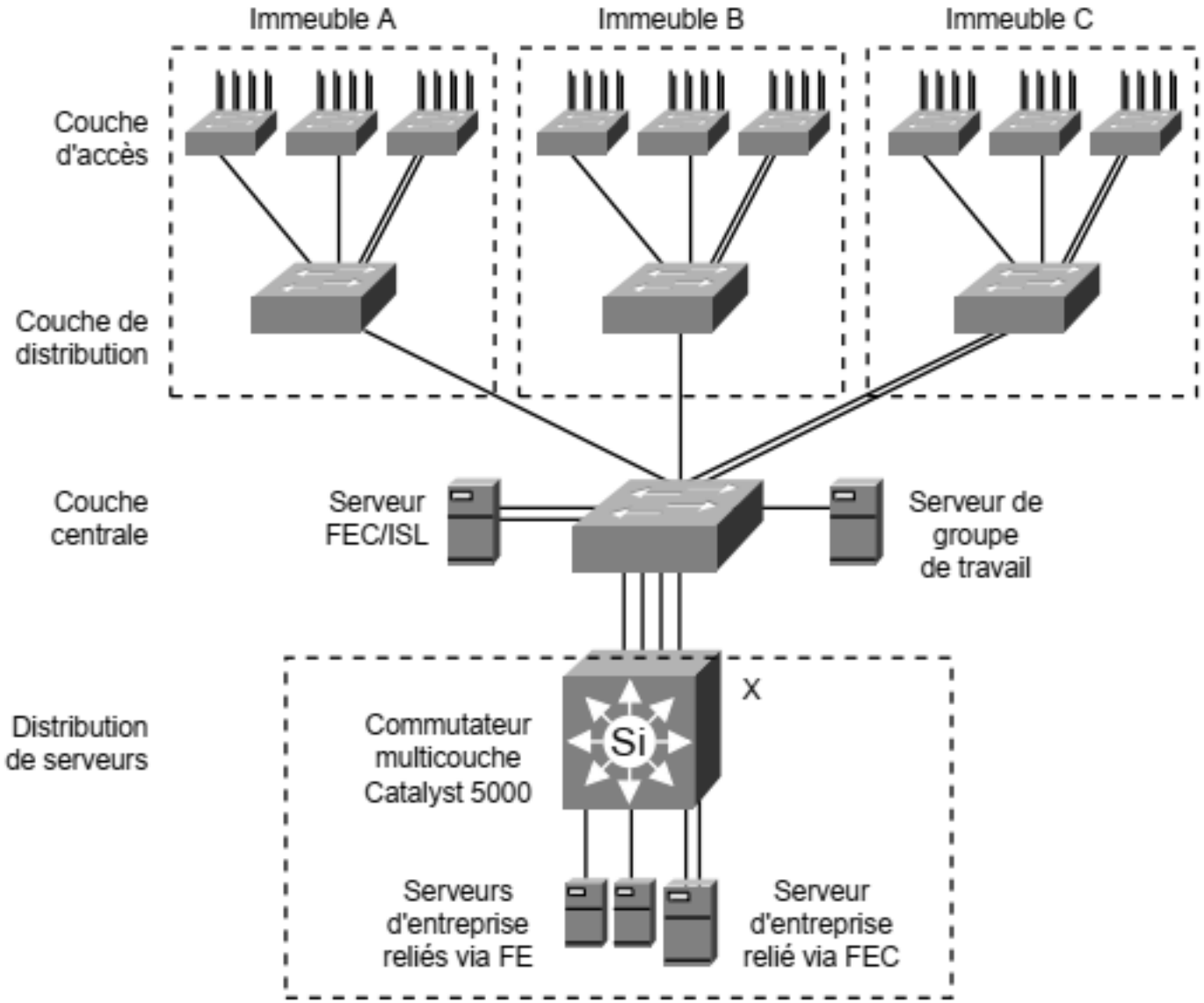
Modèle hub et routeur



Modèle de VLAN de campus



Modèle de VLAN de campus

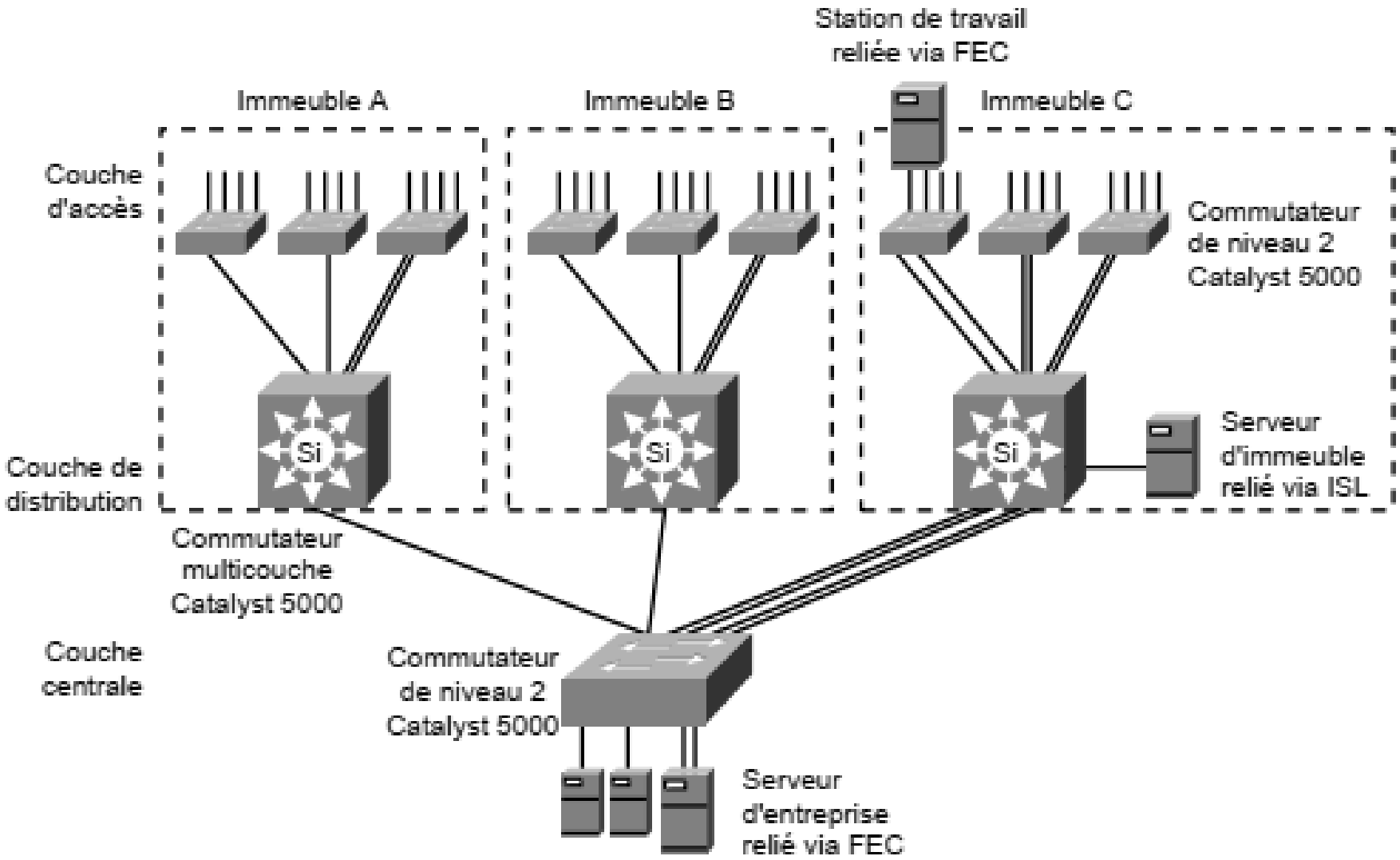


Modèle multicouche

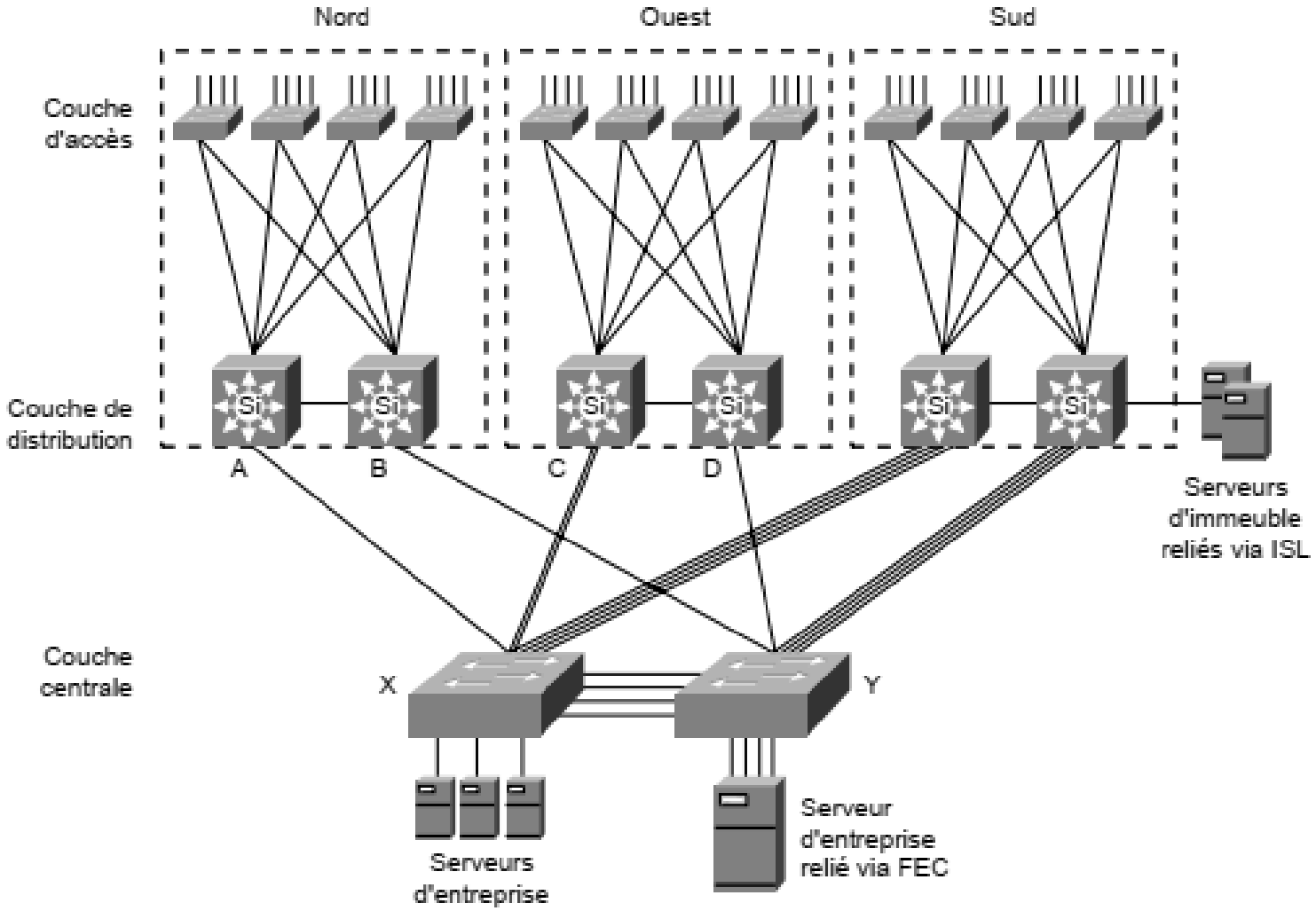
- Règle 80/20
  - Avec le modèle de VLAN de campus, le groupe de travail logique est réparti à travers le réseau, mais demeure organisé de façon que 80 % du trafic soient maintenus dans les limites du VLAN.
  - Les 20 % de trafic restants quittent le réseau ou sous-réseau par l'intermédiaire d'un routeur.

- De nombreuses applications, nouvelles ou existantes, s'orientent vers le Web distribué pour le stockage et l'extraction de données.
  - En conséquence, le modèle de trafic évolue maintenant vers une règle 20/80, c'est-à-dire que 20% seulement du trafic sont réservés au groupe de travail LAN et que les 80% restants quittent le réseau.

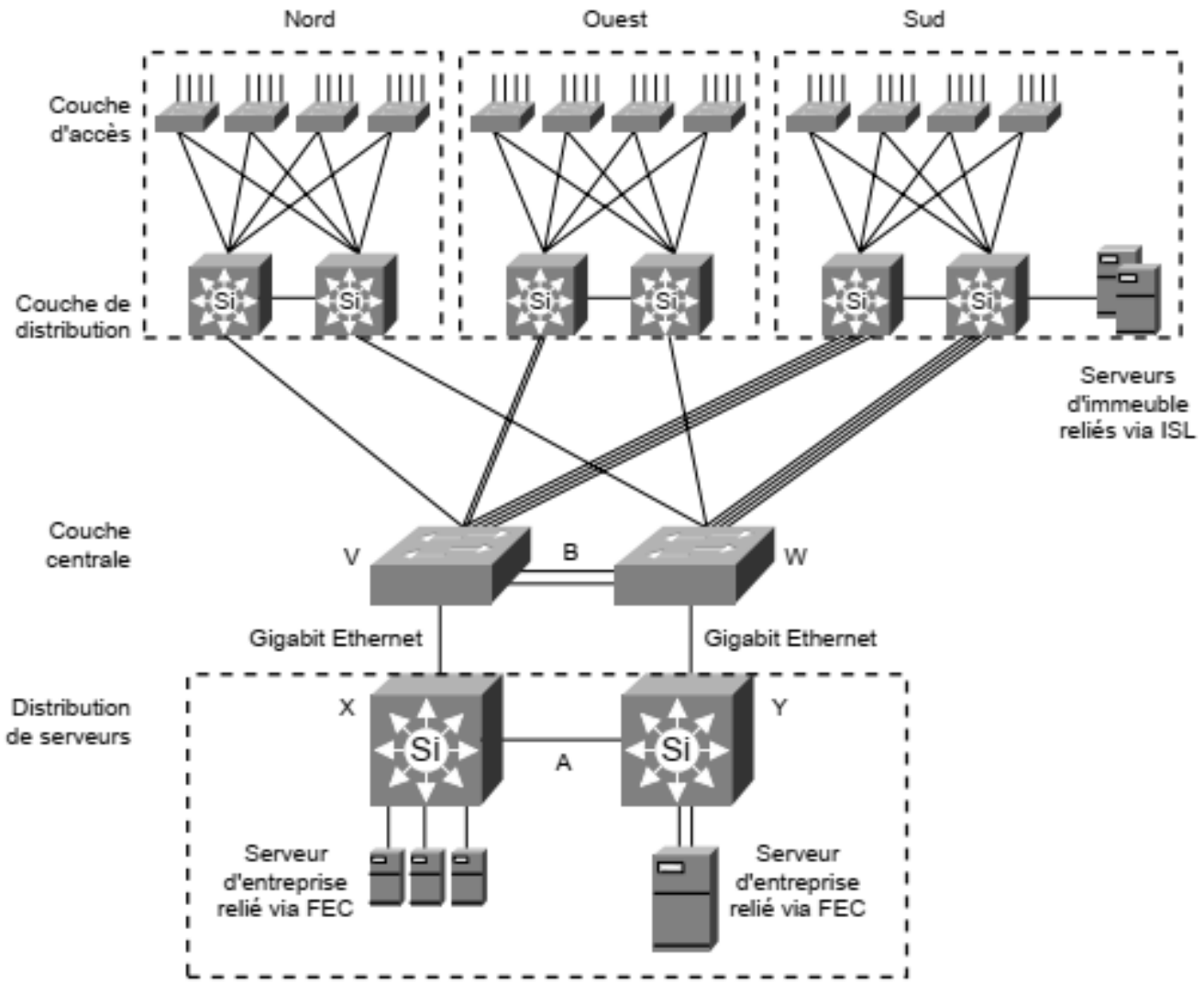
Composants du modèle multicouche



Campus multicouche redondante.



Modèle multicouche avec une ferme de serveurs



Sécurité dans le modèle multicouche

- Les listes de contrôle d'accès sont supportées par la commutation multicouche, sans entraîner de dégradation des performances.
  - Etant donné que tout le trafic transite par la **couche de distribution**, c'est l'endroit idéal pour implémenter une stratégie de sécurité fondée sur des listes de contrôle d'accès.
  - Celles-ci peuvent également être utilisées dans le cadre de la sécurité globale du réseau afin de limiter l'accès aux commutateurs eux-mêmes.
  - De plus, les protocoles TACACS+ et RADIUS assurent un contrôle centralisé de l'accès aux commutateurs.
  - Le système Cisco IOS fournit également plusieurs niveaux d'autorisation avec cryptage des mots de passe.

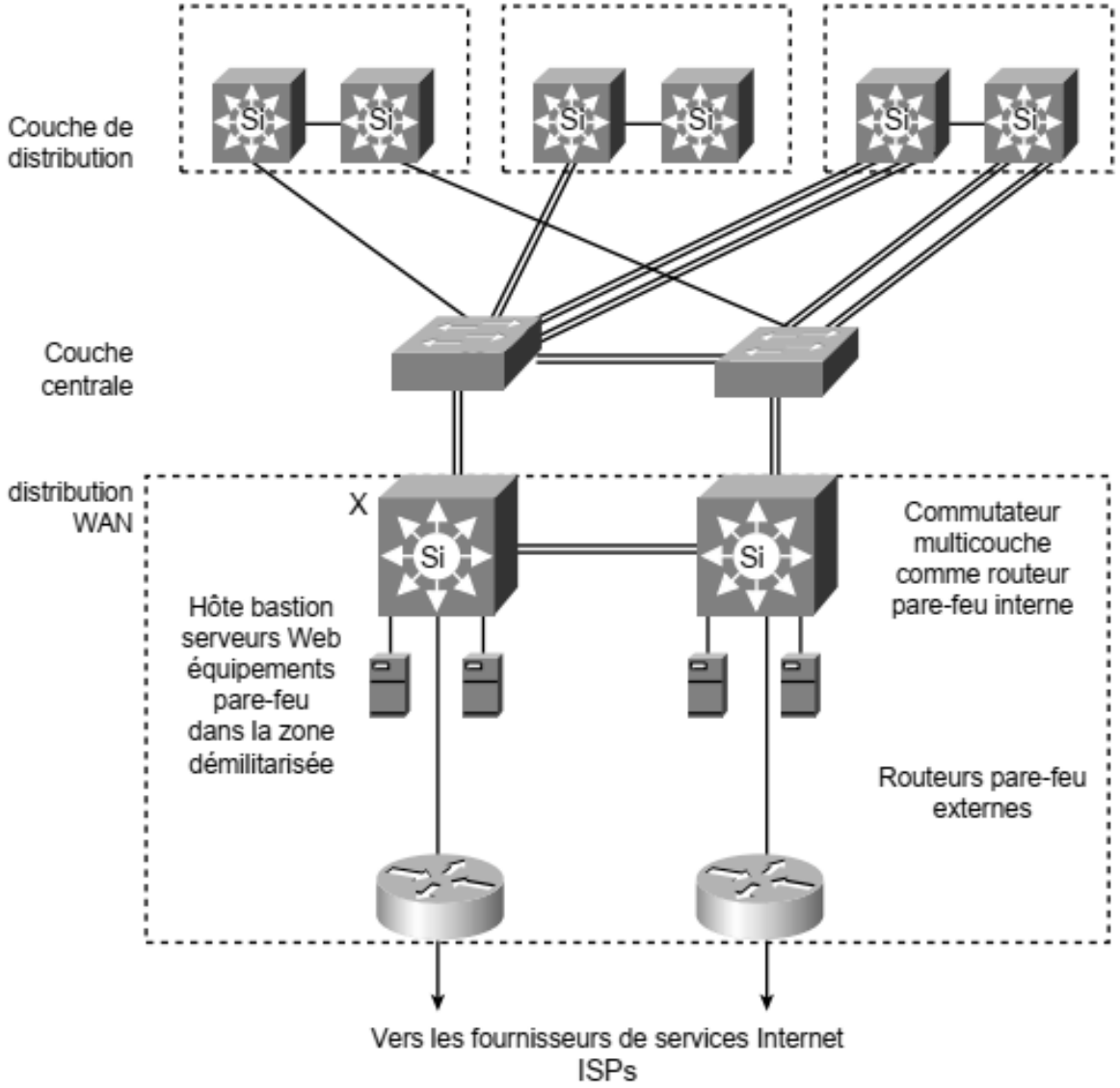
Sécurité dans le modèle multicouche

- L'implémentation de la commutation de niveau 2 sur la couche d'accès et sur la ferme de serveurs présente des avantages immédiats en matière de sécurité.
  - Sur un média partagé, tous les paquets sont visibles par tous les utilisateurs du réseau logique.
  - Un utilisateur a ainsi la possibilité de visualiser des mots de passe ou des fichiers en clair.
  - Sur un réseau commuté, les conversations sont accessibles uniquement à l'émetteur et au récepteur ; avec une ferme de serveurs, tout le trafic interserveur est maintenu en dehors de l'épine dorsale.

Sécurité dans le modèle multicouche

- La sécurité WAN est implémentée au moyen de systèmes pare-feu.
  - Un pare-feu est constitué d'un ou de plusieurs routeurs et de systèmes hôtes bastion placés sur un réseau spécial, appelé zone démilitarisée (DMZ, Demilitarized Zone).
  - Des serveurs de caches Web ainsi que d'autres équipements parefeu peuvent être reliés à la zone démilitarisée.
  - Les routeurs pare-feu internes sont rattachés à l'épine dorsale de campus au niveau de ce que l'on pourrait appeler une couche de distribution WAN.

Modèle multicouche sécurisé



Régles de Conception

1. Chaque couche devrait contenir au moins une paire de commutateurs.

2. Connecter chaque commutateur à la couche supérieure avec deux liens pour la redondance.

3. Connecter chaque paire de commutateurs de couche Distribution avec au moins un lien, mais ne jamais connecter les commutateurs Access entre eux!

4. Ne pas étendre les VLANs au-delà de la couche Distribution

5. Prendre avantage du Stacking de châssis.

Modèles de commutateurs Cisco Campus LAN couche Access

- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9200 Series Switches
- Cisco Catalyst 1300 Series Switches
- Cisco Catalyst 1200 Series Switches
- Cisco Catalyst 1000 Series Switches
- Cisco Catalyst 2960-X and 2960-XR Series Switches
- Cisco Catalyst 9400
- Cisco Meraki gérés dans le cloud

Modèle C2960-XR

Modèles de commutateurs Cisco Campus LAN couche Distribution

- Cisco Catalyst 6880-X Series Switches
- Cisco Catalyst 4500-X Series Switches
- Cisco Catalyst 4500E Series Switches
- Cisco Catalyst 9600 Series Switches
- Cisco Catalyst 9500 Series Switches

Modèles de commutateurs Cisco Campus LAN couche Core

- Cisco Nexus 7700 Series Switches with Supervisor 2E
- Cisco Catalyst 6807-XL Switches
- Cisco Catalyst 6500 Supervisor Engine 6T
- Cisco Nexus 7000 Series Switches

Modèle C6807XL

Etude de cas: Conception et Déploiement d'une Infrastructure Réseau de Campus

Une compagnie commerciale projette de transférer son siège vers un nouveau local. Le nouveau siège est un campus (Un bâtiment) d'une superficie importante et comprend trois étages. Le staff de la compagnie avoisine les 600 employés.

Il vous y demandé de concevoir l'infrastructure réseau du campus.

L'infrastructure doit répondre aux besoins et exigences du business actuel et des services futures.

Les différents départements et les utilisateurs de l'infrastructure sont réparties comme suit :

- Le premier étage héberge deux départements. Le département commercial et marketing de 150 employés et le département ressources humaines de 105 employés .
- Le deuxième étage héberge deux département aussi. Le département finance et comptabilité 110 employés et le département des relations extérieurs et prospection de 90 employés.
- Le troisième étage est réservée au Data Center (DC) et le personnel de l'IT qui avoisine le nombre de 140.

Etude cas: Instructions

- Pour la conception et le déploiement de la solution, on utilise le logiciel Packet Tracer de CISCO.
- Utiliser le modèle hiérarchique (3-Tiers) pour assurer la haute disponibilité dans chaque couche.
- La redondance des équipements réseau est indispensable, on aura besoin de deux routeurs et deux MLS switchs.
- Les deux routeurs vont constituer la couche cœur et les deux MLS la couche distribution.
- Le business de la compagnie nécessite une connexion Internet fiable et permanente.
- Le réseau doit être connecté à deux ISPs (Internet service provider).
- Tous les départements et les structures doivent été connectés à Internet.
- Chaque routeur du cœur doit être connecté aux deux routeurs des ISPs.
- Les employés de chaque département doivent disposer d'une connexion Wifi.

Etude cas: Instructions

- Le plan d'adressage du réseau se base sur l'adresse IP de base 172.16.0.0
- Le réseau est connecté aux ISPs via les adresses publiques statiques : 195.136.17.0/30, 195.136.17.4/30, 195.136.17.8/30, 195.136.17.12/30
- L'OSPF est utilisé pour le routage entre les équipements L3.
- Le personnel des différents département peuvent communiquer entre eux, sauf ceux du département finance et comptabilité qui ne doivent communiquer qu'avec le DC.
- L'assignation des adresses IP aux différents équipements (devices) se fait dynamiquement via un serveur DHCP hébergé dans le DC.
- Evidemment, L'attribution des adresses IP aux équipements hébergés dans DC doit se faire d'une manière statique.
- L'accès et la connexion à tous les équipement réseaux, en vu de leurs administration, n'est possible qu'à travers ssh.
- Effectuer les configuration de base des équipements: hostname, console password, enable password, banner message, disable IP domain lookup, ..