

INSA

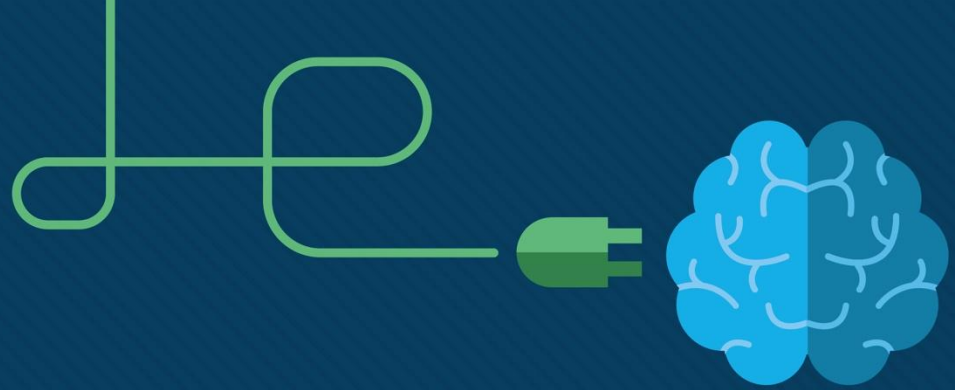
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
HAUTS-DE-FRANCE



Université
Polytechnique
HAUTS-DE-FRANCE

Les VLANs

Réseaux informatique

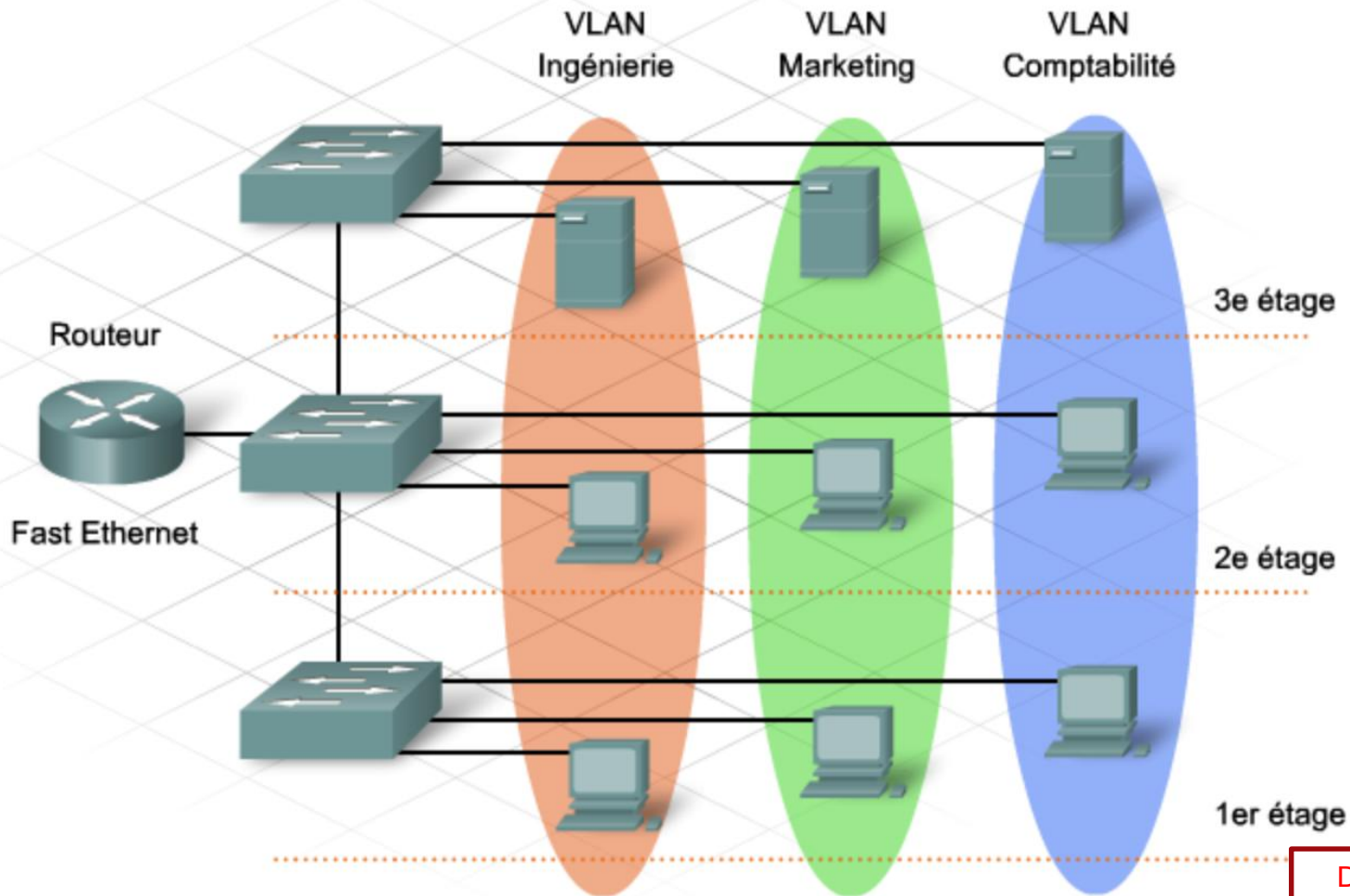


Présentation avantages/inconvénients

Les VLAN

Présentation

- Un VLAN (Virtual Local Area Network - Réseau Local Virtuel) est un regroupement logique de machines formant ainsi un LAN. Il est qualifié de virtuel car elles ne sont pas physiquement reliées.
- Ce « regroupement » se fait par des commutateurs manageables, qui sont configurés par les administrateurs réseaux.
- Les objectifs : Améliorer la sécurité, la performance et la gestion du réseau.



Avantages en Sécurité et Performance

- Sécurité renforcée par la segmentation réseau et l'isolation des groupes



- Réduction des congestions réseau grâce à la limitation des domaines de diffusion, améliorant ainsi les performances globales.



Robert Tomczak

Diapo 5

Flexibilité et Efficacité de la Gestion

- Regroupement d'utilisateurs par fonction, pas par localisation, simplifiant la gestion.
- Allocation dynamique des ressources et facilité de déploiement des politiques de réseau, offrant une meilleure utilisation des ressources.
- .



Isolation et simplification

- Isolation et contrôle du trafic pour une qualité de service optimale.
- Simplification des opérations réseau, menant à une meilleure efficacité globale.
- Les VLAN offrent une solution puissante pour répondre aux besoins complexes des réseaux d'entreprise.



Les inconvénients

- **Complexité de configuration et de gestion**
- **Besoins en matériel spécifique**
- **Problèmes de performance inter-VLAN**
- **Limitation du nombre de VLAN**
- **Sécurité inter-VLAN**

Les différents types de VLAN

Les VLAN

1. VLAN basé sur les ports (Port-Based VLAN)

- Type de VLAN le plus courant.
- L'appartenance à un VLAN déterminée par le port du commutateur.
- Nécessité de changer la configuration de port pour déplacer un dispositif d'un VLAN à un autre.

2. VLAN basé sur les adresses MAC (MAC-Based VLAN)

- Détermination de l'appartenance au VLAN basée sur l'adresse MAC du dispositif
- Indépendance vis-à-vis du port du commutateur auquel le dispositif est connecté
- Suivi de la politique de VLAN basé sur l'adresse MAC du dispositif, offrant une flexibilité de connexion

3. VLAN basé sur les adresses IP (IP Subnet VLAN)

- L'appartenance à un VLAN est déterminée par l'adresse IP du dispositif.
- Cela permet une segmentation logique qui est souvent alignée avec la structure de sous-réseau IP de l'organisation,
- facilitant la gestion des politiques de réseau et de sécurité.

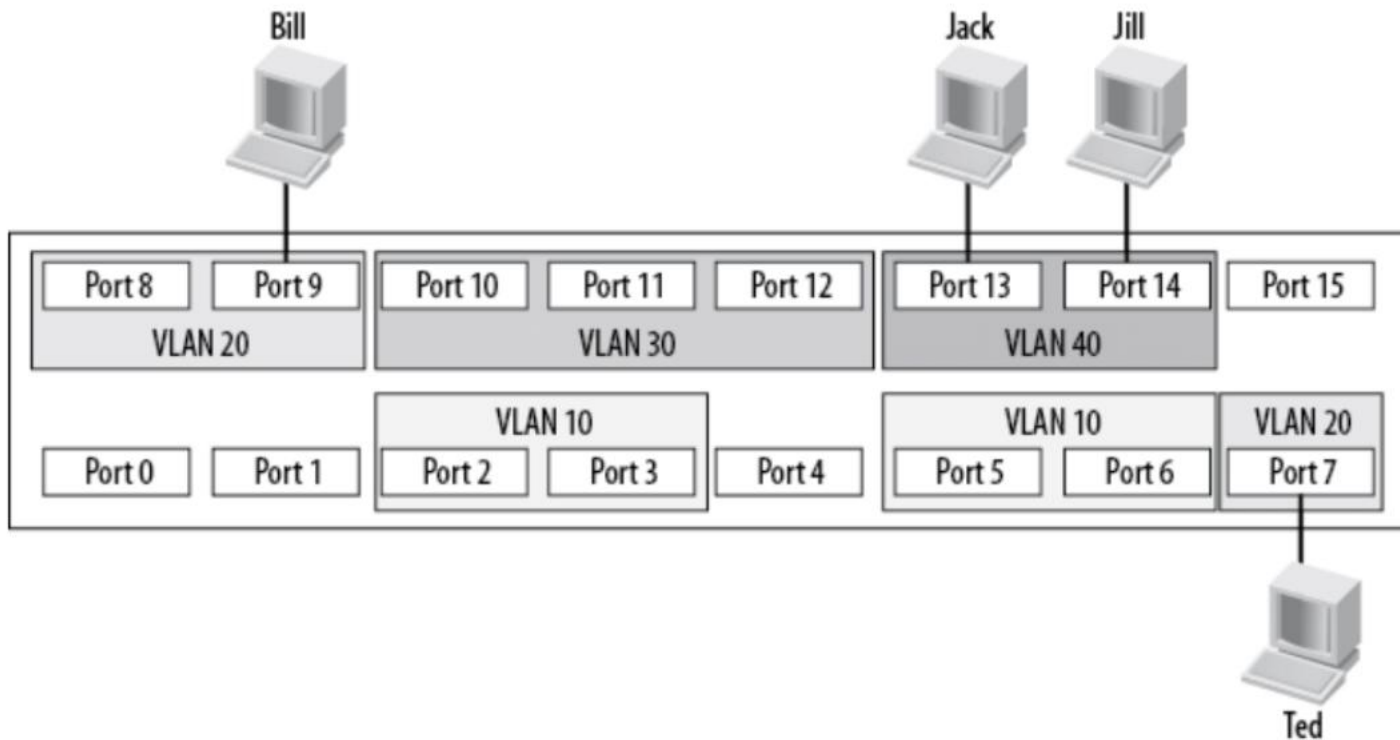
4. VLAN basé sur le protocole (Protocol-Based VLAN)

- Ce type de VLAN segmente le trafic en fonction du protocole
- Cela peut être utile pour séparer les types de trafic pour des raisons de performance ou de sécurité.

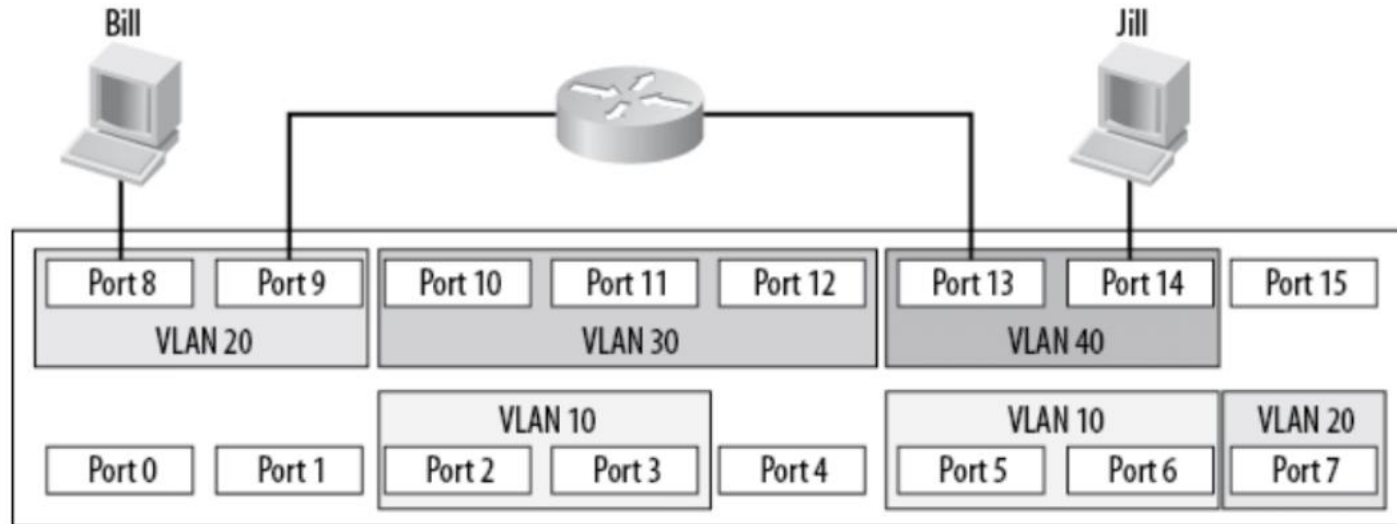
Et d'autres

Connecter les VLANs

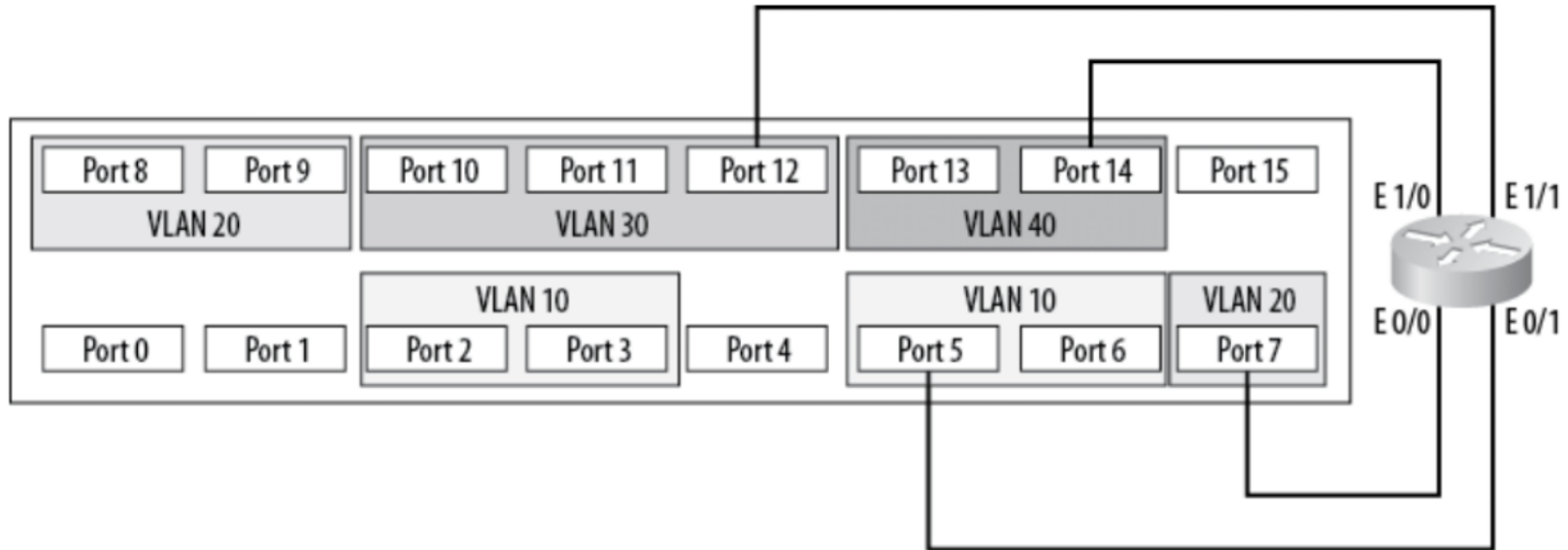
VLAN sur un seul switch



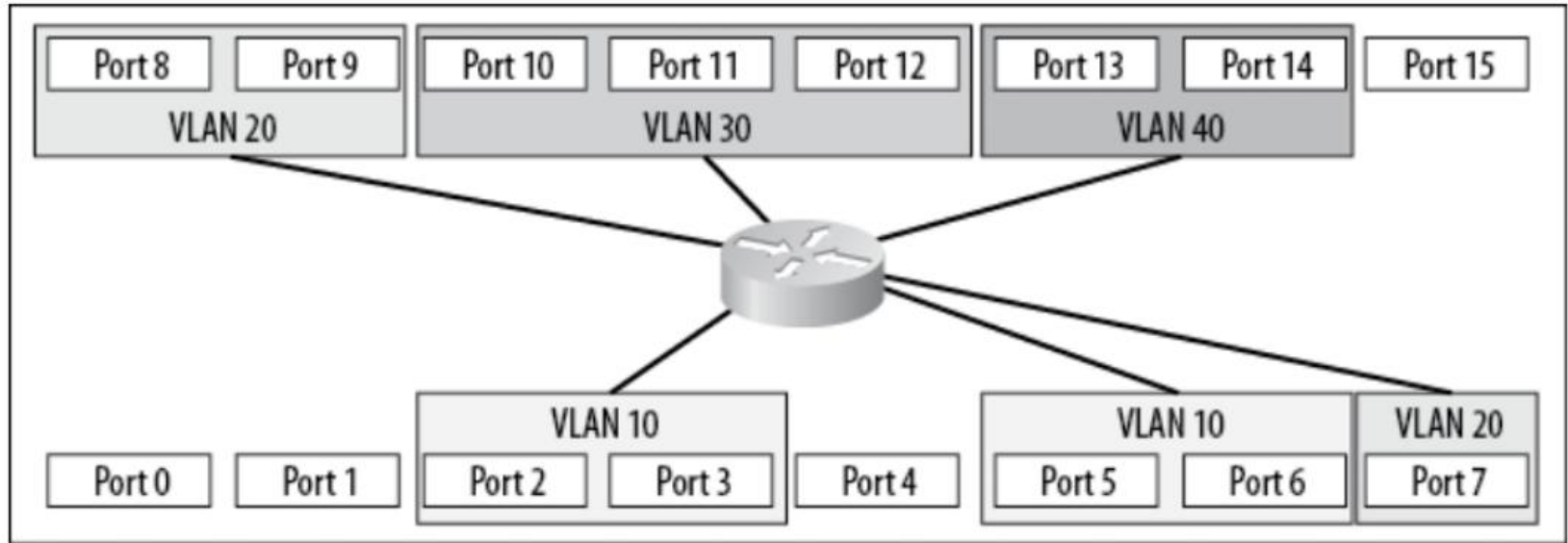
Routage



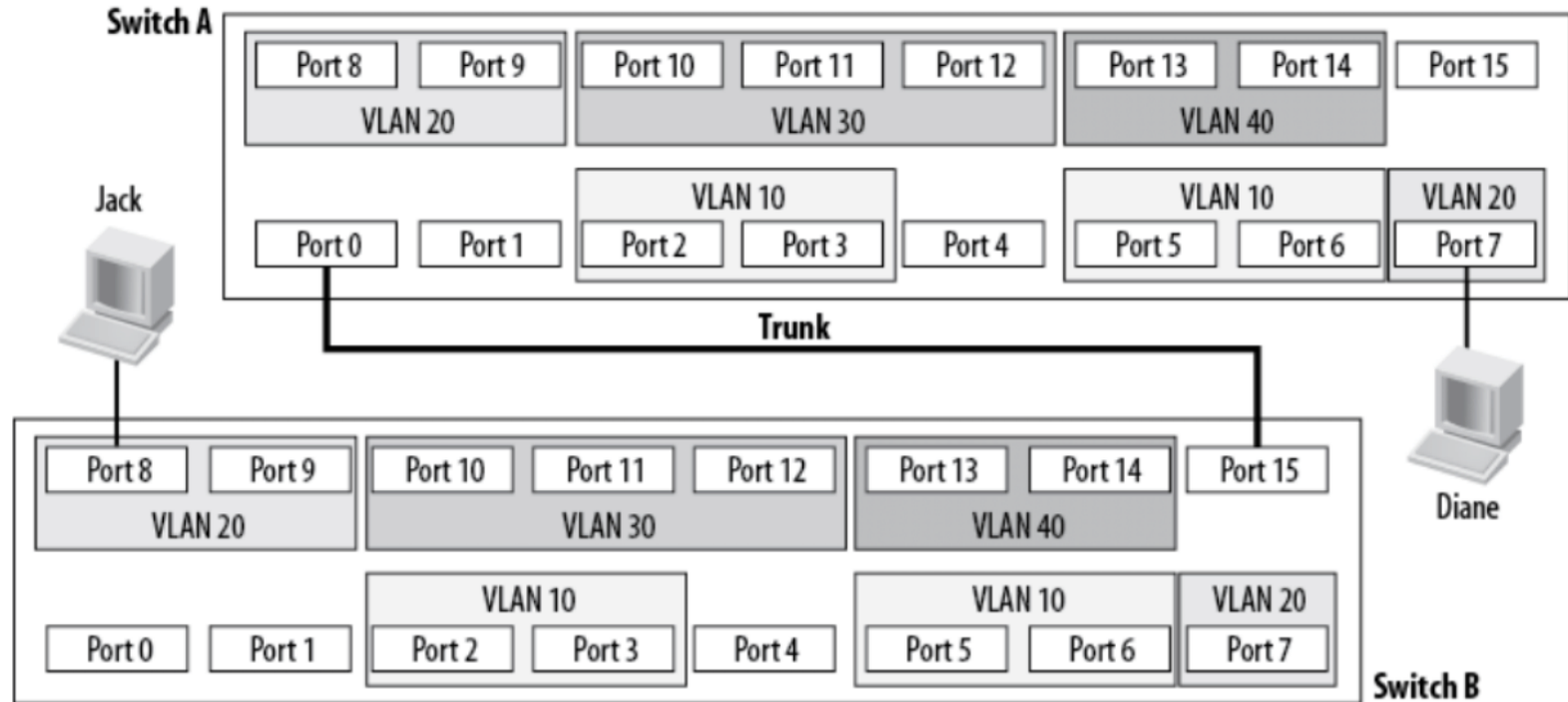
Routage



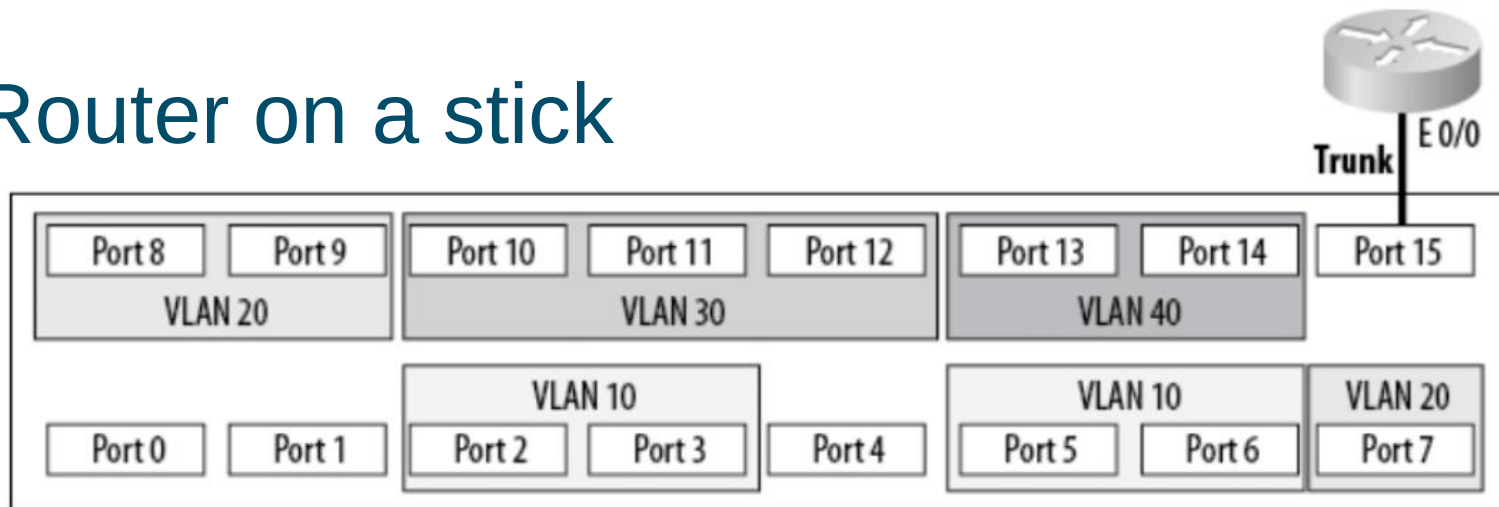
Switch niveau 3



2 switch connectés à l'aide de Trunk



Router on a stick



un seul port physique

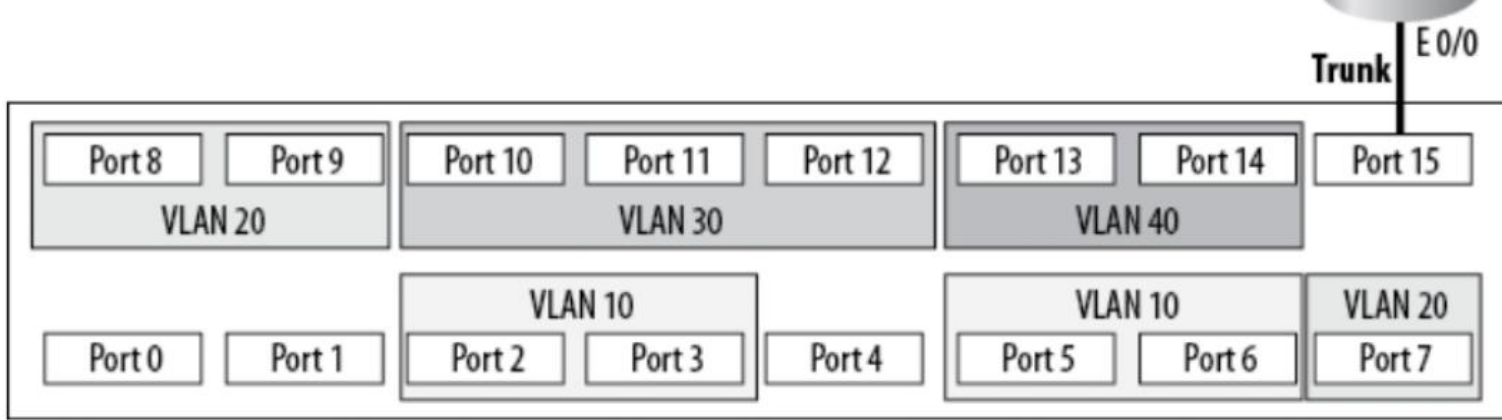
Subinterfaces

Routage inter-VLAN

Efficacité du réseau

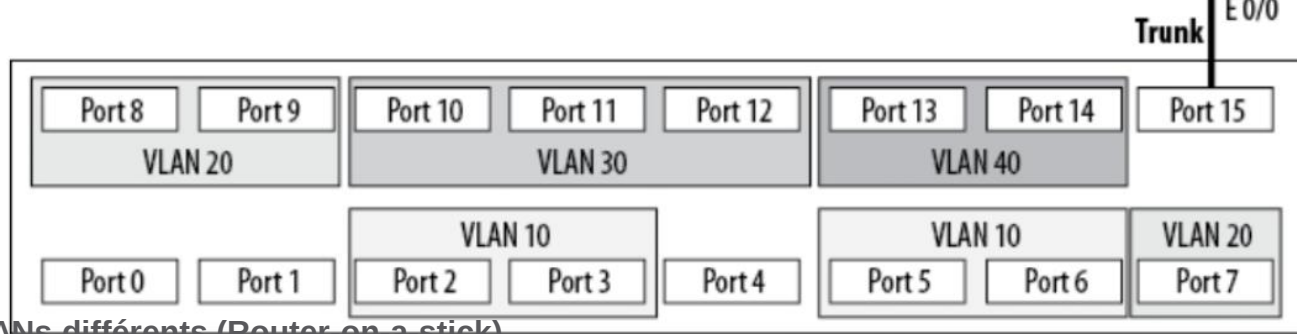
Configuration

Limitations



Communication entre hôtes du même VLAN

1. L'hôte A envoie une trame Ethernet à l'adresse MAC de l'hôte B (ou ARP si IP connue).
2. Le switch reçoit la trame sur un port access, la considère comme appartenant au VLAN X.
3. Le switch regarde sa table MAC : si l'adresse MAC de B est connue, il envoie la trame uniquement sur le port correspondant (forwarding unicast). Si inconnue, il broadcast sur tous les ports du VLAN X.
4. B reçoit la trame ; la communication reste entièrement au niveau L2, sans intervention du routeur



2) Communication entre hôtes de VLANs différents (Router-on-a-stick)

Supposons A (VLAN 10, IP 192.168.10.10) veut joindre C (VLAN 20, IP 192.168.20.10) :

1. A envoie un paquet IP vers la gateway (192.168.10.1 — la sous-interface du routeur pour VLAN 10).
2. Le switch reçoit la trame sur un port access (VLAN 10) et la transmet sur le trunk vers le routeur. Sur le trunk, la trame est taggée .10 (802.1Q).
3. Le routeur reçoit la trame taggée, la dirige vers la sous-interface VLAN 10, effectue le routage IP (consulte sa table de routage) et détermine que la destination est sur VLAN 20.
4. Le routeur encapsule la trame de sortie : il met le tag 802.1Q .20 et renvoie la trame sur le trunk vers le switch.
5. Le switch, voyant le tag .20, forward la trame uniquement aux ports en access VLAN 20 (ou au port de destination si MAC connue).

6. Le switch reçoit le paquet ; la communication inter-VLAN a traversé le routeur (L3).

