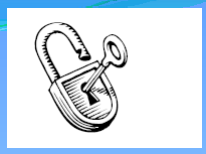
Université Abou Bakr Belkaid
Faculté des sciences / Département d'Informatique



Sécurité Informatique
Chapitre 3

Les Réseaux Locaux Virtuels VLAN Et les Réseaux Privés Virtuels VPN

Présenté par Mme Labraoui N.

Master 1 Réseaux et systèmes distribués

2019-2020

Introduction

- Beaucoup de compagnies qui veulent mettre à jour leur méthode de communication avec leurs employés créent un réseau; mais ce réseau doit être sécurisé pour prévenir des accès non autorisé et des attaques malicieuses.
- C'est pour cette raison que les compagnies exigent un **VLAN** ou un **VPN** comme mécanisme de sécurité pour contrecarrer toute menace sur le système.

Introduction

Les réseaux privés:

- utilisés dans les entreprises
- les réseaux privés entreposent souvent des données confidentielles à l'intérieur de l'entreprise
- On appelle alors ces réseaux privés « **intranet** »
- Pour garantir cette confidentialité, le réseau privé **est coupé logiquement du réseau internet**.
- En général, les machines se trouvant à l'extérieur du réseau privé ne peut accéder à celui-ci. L'inverse n'étant pas forcément vrai.
- L'utilisateur au sein d'un réseau privé pourra accéder au réseau internet.

INTRODUCTION

- **Réseau privé virtuel/**
- Le but d'un vpn est de « fournir aux utilisateurs et administrateurs du système d'information des conditions d'exploitation, d'utilisation et de sécurité à travers un réseau public identiques à celles disponibles sur un réseau privée ».
- En d'autre terme, on veut regrouper des réseaux privés, séparé par un réseau public (internet) en donnant l'illusion pour l'utilisateur qu'ils ne sont pas séparés, et toute en gardant l'aspect sécurisé qui était assuré par de la coupure logique au réseau internet.

INTRODUCTION

Cas d'utilisation des VPN:

- **Le Télétravail**. Il existe des entreprises sans locaux, ou les employés travaillent chez eux. Quand ce type de travail est possible, pourquoi dépenser plus pour des locaux, des problèmes de transport, etc ... ?
- Le VPN apporte la possibilité pour tous ses employés de travailler sur un même réseau privé virtuel.
- Il doit alors évidement disposer d'une connexion internet qui lui permet de travailler à distance, et d'utiliser les différents services du réseau, et même exploiter des outils de travail collaboratif.

INTRODUCTION

Cas d'utilisation des VPN:

- **Connexion de sites distants**.:
- Pour en entreprise possédant plusieurs sites, il est parfois avantageux de les relier.
- Une première solution serait d'utiliser une LS.(ligne spécialisée)
- Mais cette solution à un coup, et le VPN ne coûte pas plus que 2 connexion d'accès à internet.

Distinctions entre VLAN et VPN

- **VLAN est une sous-catégorie du VPN**
- VPN est utilisé pour communiquer d'une manière sécurisé dans un endroit qui n'est pas considéré sure
- VLAN permet la communication distante dans des groupes qui ne se trouvent pas au même endroit, alors qu'un VPN crée un tunnel virtuel crypté pour le transfert des données
- Toutes données sont sécurisées par le VPN contre tout accès non autorisé, que ce soit des regards indiscrets ou des hackers dont l'intention est de voler les droits à la propriété intellectuelle ou des informations sensibles qu'ils peuvent utiliser pour leur fins criminels
- VLAN n'utilise pas des techniques de cryptage pour la sécurité parce que c'est seulement utilisé pour diviser le réseau dans des parties différentes pour une gestion plus facile et pour des raisons de sécurité

Partie 1

Les Réseaux Locaux Virtuels

Introduction

Domaine de diffusion:

- Un LAN est défini par un domaine de diffusion.
- Tous les hôtes d'un LAN reçoivent les messages de diffusion émis par n'importe quel autre hôte de ce réseau.
- Par définition, un réseau local est délimité par des équipements fonctionnant au niveau 3 du modèle OSI : la couche réseau.

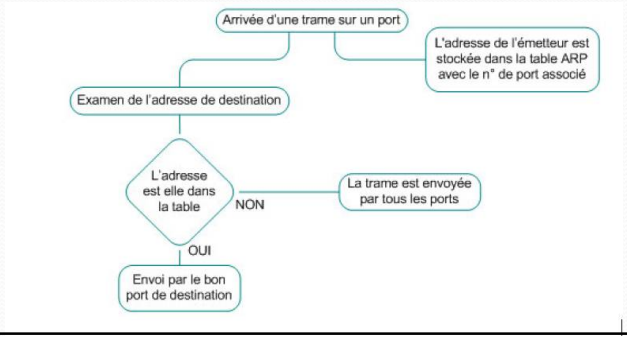
Rappel : Commutateur

- Mémorisation des trames
- Table Port/adresse MAC
- Remplie à l'aide des premiers paquets
- Les trames ne sont réemises que vers la destination
- Plus de collisions, fonctionne en full-duplex

Rappel: Fonctionnement d'un Commutateur

Limitations:

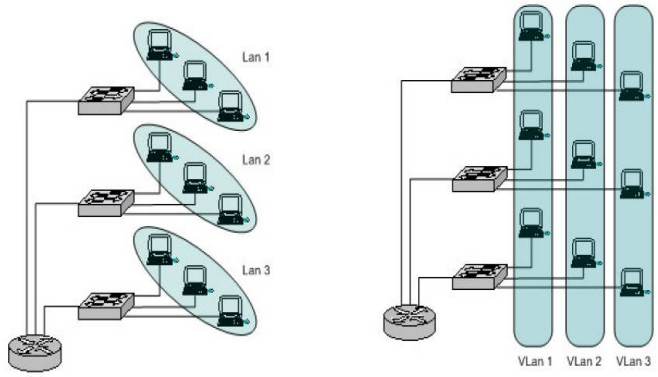
- Pas de limitation du champs de broadcast
- Pas de partage en sous-réseaux
- Pas de sécurité entre utilisateurs



LES VLAN

- Un réseau local virtuel (VLAN) est un LAN distribué sur des équipements fonctionnant au niveau 2 du modèle OSI : la couche liaison.
- À priori, il n'est donc plus nécessaire d'avoir recours à un équipement de niveau 3 pour «borner» le réseau local.

LES VLAN



Segmentation traditionnelle a Segmentation avec VLAN

Différence entre commutation traditionnelle et les VLAN

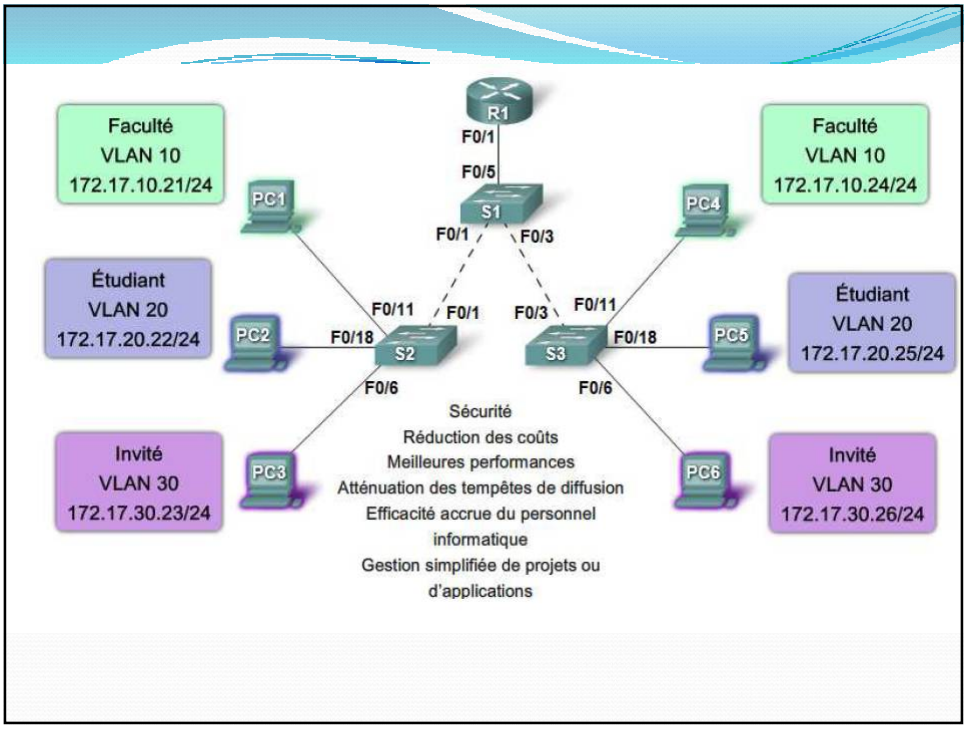
- Les VLAN fonctionnent au niveau des couches 2 et 3 du modèle OSI
- La communication inter VLAN est assurée par le routage de couche 3
- Les VLAN fournissent une méthode de contrôle des broadcasts
- Les VLAN permettent d'effectuer une segmentation selon certains critères
  - Des collègues travaillant dans le même service
  - Une équipe partageant le même applicatif
- Les VLAN peuvent assurer la sécurité des réseaux en définissant quels nœuds réseaux peuvent communiquer entre eux

Il est alors possible de segmenter le réseau en plusieurs domaines de broadcast afin d'en améliorer les performances.

La communication inter VLANS est assurée par des routeurs

But des VLAN

- Découper un réseau local physique en plusieurs réseaux virtuels
- Les réseaux virtuels sont isolés les uns des autres
- Limite les domaines de diffusion: les trames en broadcast sont Isolées
- Possible seulement avec un commutateur

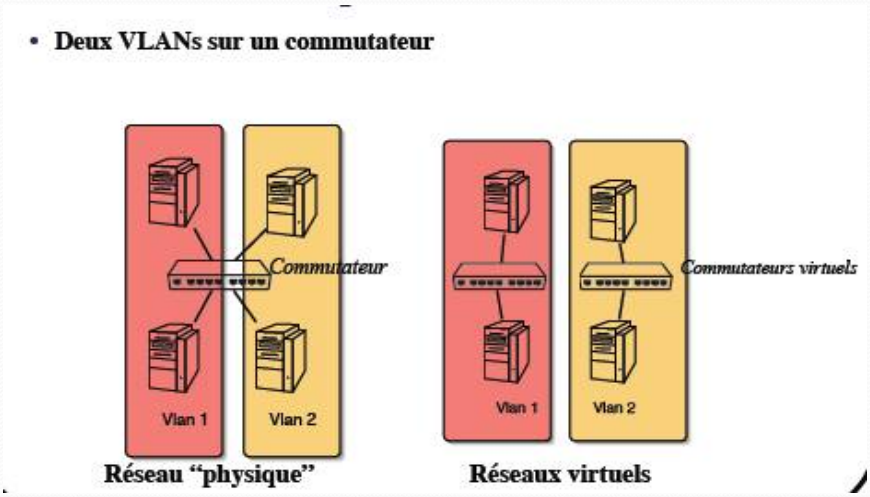


Intérêt des VLANs

- Mettre en place plusieurs réseaux locaux virtuels sur un seul LAN Physique
- Mise en œuvre simple et souple contrairement à du vrai câblage
- Isolation des VLANS : sécurité, confidentialité
- Administration plus aisée qu'une administration de niveau 3 (routage)

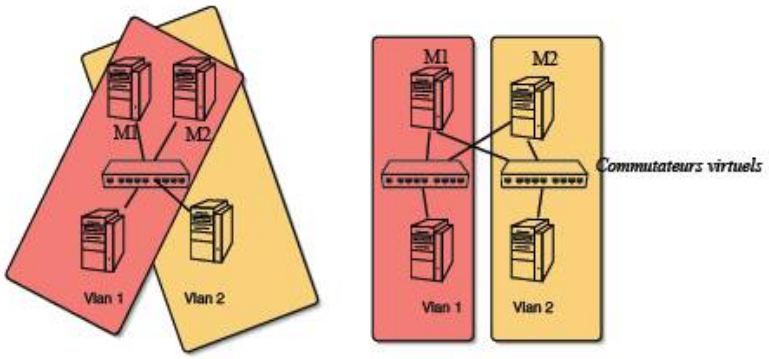
Exemple de VLAN

- **Deux VLANs sur un commutateur**



Exemple de VLAN

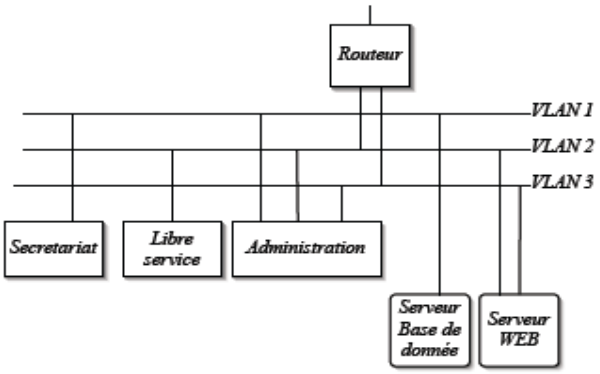
- Une machine peut appartenir à plusieurs VLANs



Réseaux "virtuels"

Exemple d'administration

- Suivant le type d'utilisateur, de l'accès aux serveurs et à l'extérieur



Identification des VLAN

- Chaque VLAN est identifié par un numéro qui l'identifie:
- VLAN n°20, VLAN n°30
- Le numéro du VLAN est codé sur 12 bits
- Théoriquement, on peut créer 4096 VLAN

Définitions de VLANs

Plusieurs techniques pour définir un VLAN:

VLAN STATIQUE:

– Ports physiques des commutateurs

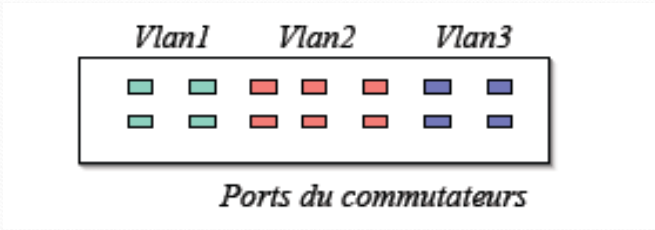
VLAN DYNAMIQUE

– Adresse MAC des ordinateurs
– Adresse IP des ordinateurs
– Protocole Réseaux

- **Dans tous les cas : cela définit l'appartenance de chaque port du**
- commutateur à un ou plusieurs VLANs (table dans le commutateur)
- **A la réception d'une trame sur un port, la trame n'est reémise que**
- sur le (ou les) port associé à l'adresse MAC destination qui appartient au même VLAN
- **Dans le cas d'une adresse destination broadcast, la trame est reémise** sur tous les ports appartenant au même VLAN

Définition de VLANs A l'aide des ports du commutateur (1)

- On associe un numéro de VLAN à chacun des ports du commutateur
- Effectué par **l'administrateur** sur le commutateur
- Le plus simple et le plus sûr mais "statique"
- La définition du VLAN ne dépend que de la configuration du commutateur (un utilisateur ne peut pas la changer)

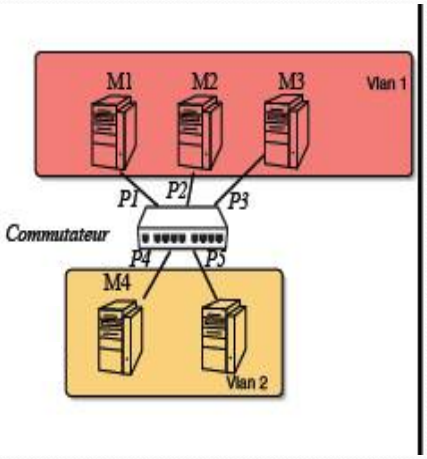


Exemple de configuration de VLANs A l'aide des ports du commutateur (2)

- Dans le commutateur
  - **Port VLAN**
  - **P1 1**
  - **P2 1**
  - **P3 1**
  - **P4 2**
  - **P5 2**
- **Sur M1 : ping M4**

Paquet ARP request diffusé seulement sur VLAN1

Donc pas de réponse



Définition de VLANs
Par les adresses MAC (1)

- Dans le commutateur il faut remplir une table (Adresse Mac, VLAN)
  - L'association (port,VLAN) se fait à l'aide des 1er paquets portant l'adresse MAC source
- **Plus souple** (nouveaux utilisateurs, portables, changement des branchements)
  - On peut changer la liaison ordinateur/commutateur et appartenir toujours au même VLAN
- Moins sûr:
  - L'utilisateur peut changer de VLAN puisque l'on peut changer une adresse MAC sur une machine !
- Plus lourd : connaissance des adresses MAC par l'administrateur

Définition de VLANs
Par les adresses IP

- Dans le commutateur il faut remplir une table (Adresse IP réseau, VLAN)
  - L'association (port, VLAN) se fait à l'aide des 1er paquets portant l'adresse IP source
- Moins sûr:
  - l'utilisateur peut changer d'adresse IP
- Moins performant:
  - Analyse des entêtes IP
- Plus simple pour l'administrateur :
  - Peut se faire à partir du plan d'adressage IP

Définition de VLANs
Par le protocole réseau

- Dans le cas où plusieurs protocole réseau sont utilisés (IPX, IP, Apple Talk ...)
- On associe un VLAN suivant le protocole Réseau

Principe de fonctionnement des VLAN

- On distingue 2 méthodes pour regrouper les utilisateurs en VLAN:

1. Le filtrage de trame
2. L'identification des trames

Principe de fonctionnement des VLAN

- Le filtrage de trames
  - Un examen de chaque trame permet d'élaborer pour chaque commutateur une table de filtrage afin de permettre de prendre les décisions appropriées.
  - Cela suppose une table de filtrage par commutateurs, donc des temps de mise à jour lents ainsi que des problèmes d'évolutivité

Principe de fonctionnement des VLAN

- L'identification des trames
  - Chaque trame dispose d'un code d'identification VLAN (TCI = Tag Control Information) définit par la norme IEEE 802.1q
  - L'identificateur est utilisé lors du transfert des paquets sur le réseau
  - Il est enlevé lorsque le paquet quitte le réseau pour atteindre les hôtes ou les routeurs.

Cette dernière méthode est la plus couramment utilisée. Elle est identifiée de manière claire au niveau des commutateurs par le support de cette norme.

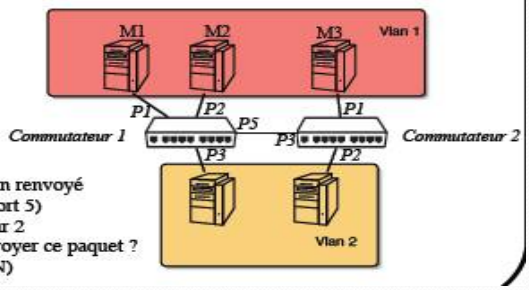
Exemple de configuration de VLANs statiques

- Dans le commutateur 1:

PORT	VLAN
P1	1
P2	1
P3	2
P5	1, 2

Dans le commutateur 2:

PORT	VLAN
P1	1
P2	2
P3	1, 2



- Problème :
  - Sur M1: ping M3
  - Le paquet ARP request est bien renvoyé sur le commutateur 2 (par le port 5)
  - Mais comment le commutateur 2 peut il savoir sur quel port renvoyer ce paquet ? (P3 est associé aux deux VLAN)

Etiquetage des trames

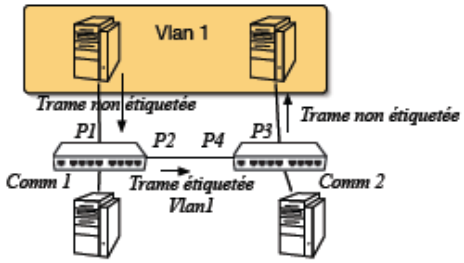
- Dans le cas précédent on peut résoudre le problème
  - en ajoutant l'association (Adresse MAC, VLAN) dans les commutateurs
  - le commutateur 2 peut savoir ainsi à quel VLAN doit être renvoyé une trame à l'aide de l'adresse MAC source incluse dans l'entête du paquet
  - l'association VLAN/Ports et VLAN/Adresse MAC à faire sur tous les commutateurs devient laborieuse
- On peut aussi mettre deux liaisons physiques entre les deux commutateurs et associés leurs deux ports à un seul des deux VLANs

Trunk Link

- Idée d'amélioration : il faut que le paquet porte le numéro de VLAN dans son entête
- On parle alors de VLAN "étiqueté" (tagged) ou "informé"

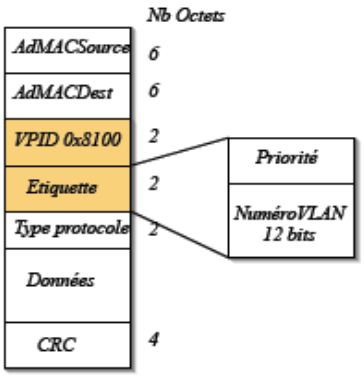
Exemple de VLAN étiqueté

- L'étiquetage des trames indiquant le numéro de VLAN auquel elle appartient peut se faire
  - Dans les machines (carte Ethernet compatible 802.1Q)
  - Seulement dans les commutateurs le cas écheant
- Exemple d'étiquetage des trames dans les commutateurs



Format trame 802.1Q

- VPID : identifie une trame 802.1Q
- VID(VLAN Identifier): numéro de VLAN
- Gestion de priorités (ou COS Class Of services) : 3 bits possible : norme 802.1p (indépendant des VLAN)



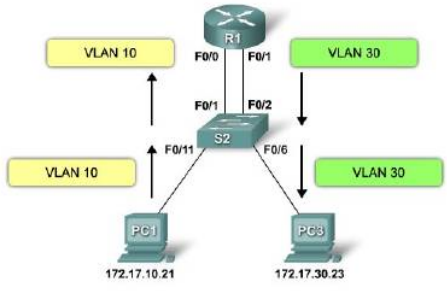
Routage inter-VLAN

Le principe des VLAN est de limiter la diffusion des informations entre VLAN. Ce qui rend imperméable la communication entre 2 machines situées sur des VLAN différents.

Les ports d'interconnexion entre commutateurs supportant les VLAN sont dénommés Port "TRUNK". Cette dénomination permet de prendre en compte de façon particulière la communication inter commutateurs. Cette communication maintien l'isolement entre les VLAN.

La seule solution technique permettant de partager des ressources ou d'échanger des données est soit de passer par un routeur qui assurera la communication à l'aide de ses tables de routage, soit de rendre disponible les ressources aux 2 VLAN

Routage inter-VLAN



Le routage entre VLAN basé sur routeur est un processus d'acheminement du trafic réseau d'un VLAN à un autre à l'aide d'un routeur.

- Les hôtes appartenant à des VLANs diérents ne peuvent pas communiquer entre eux
- La communication inter-VLAN nécessite un dispositif de niveau 3

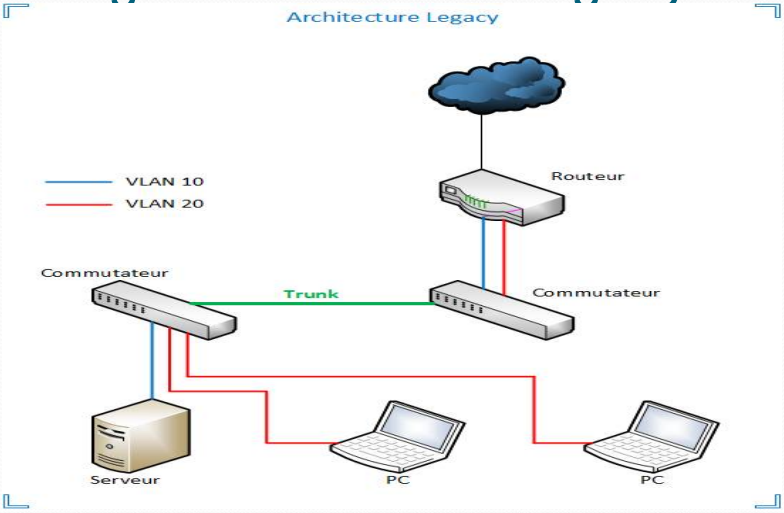
Routage inter VLAN

- Il existe 3 types d'architectures possibles dans le cadre de routage inter-VLANs.
- Les architectures présentées sont :
  1. Legacy,
  2. Router-on-a-stick,
  3. Multilayer Switch.

Routage inter VLAN :Legacy

- Dans l'approche Legacy, le routage inter-VLAN est effectué en connectant différentes interfaces physiques du routeur sur différentes interfaces physiques du commutateur.
- Les ports du commutateur connectés au routeur ne sont pas en mode trunk mais en mode accès (***access***) chaque interface physique est assignée à un VLAN différent.
- autant d'interfaces physiques que vous avez de VLANs (génant !)
- Cette méthode n'est plus implémentée

Routage inter VLAN :Legacy

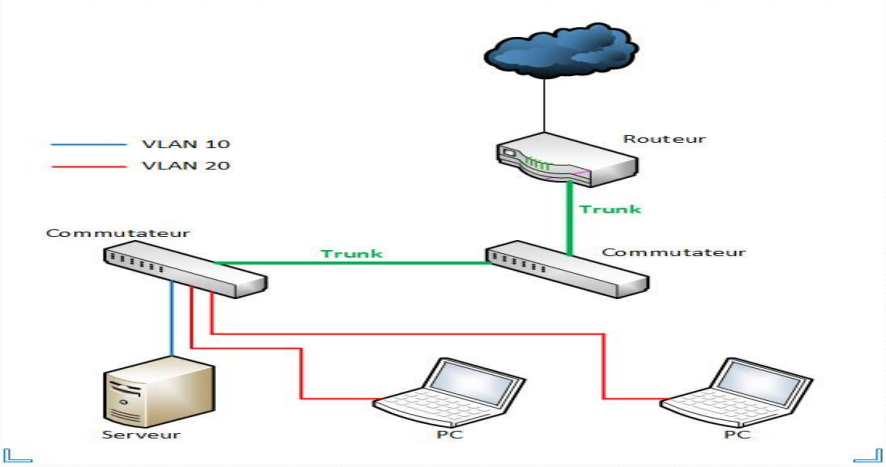


Vous remarquerez qu'il y a 2 VLANs, le VLAN 10 et le VLAN 20 chacun dispose de son propre lien dédié entre le routeur et le commutateur. Entre les deux commutateurs on trouve un lien trunk pour tagguer les trames Ethernet.

Routage inter VLAN: **Router-on-a-stick**

- une évolution de l'architecture Legacy, notamment au niveau du lien commutateur – routeur
- puisqu'au lieu d'avoir un lien par VLAN, un seul lien suffira. Le lien entre le routeur et le commutateur est désormais un lien **trunk**.
- sur l'interface du routeur connectée au commutateur, il faudra créer une **sous-interface virtuelle** pour chaque VLAN en activant l'encapsulation 802.1Q pour le VLAN pour que le tagguage des trames Ethernet opère correctement.
- Chaque sous-interface sera la passerelle des postes du VLAN, il faudra donc penser à attribuer une adresse IP à ces interfaces virtuelles et à les rendre active (*no shutdown*).

Routage inter VLAN: **Router-on-a-stick**



Les liens trunk agissent comme des tuyaux capables de transporter le flux de données de chacun des VLANs autorisés.

Trunk

- Un *trunk* est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels.
- Les trames qui traversent le *trunk* sont complétées avec un identificateur de réseau local virtuel (VLAN id).
- Grâce à cette identification, les trames sont conservées dans un même VLAN (ou domaine de diffusion).

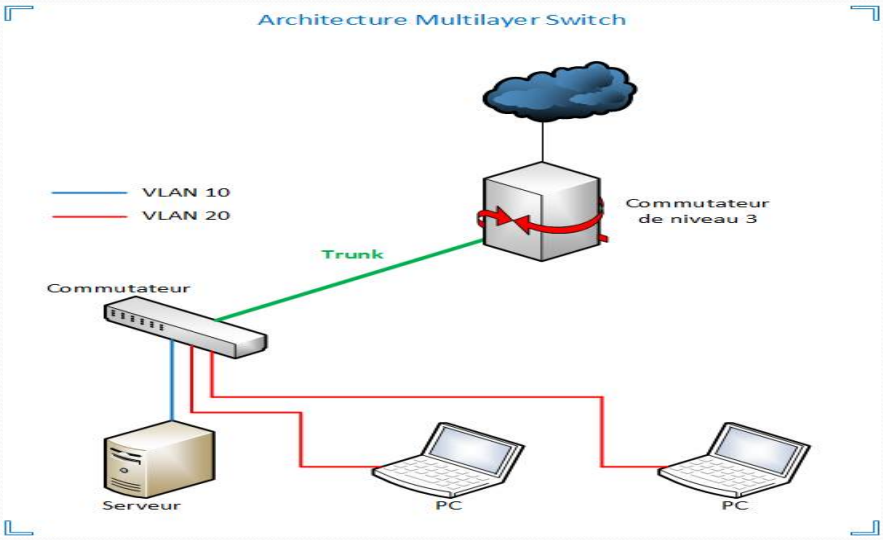
Trunk

- Les *trunks* peuvent être utilisés :
- entre deux commutateurs C'est le mode de distribution des réseaux locaux le plus courant.
- entre un commutateur et un hôte C'est le mode de fonctionnement à surveiller étroitement. Un hôte qui supporte le *trunking* a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels.
- entre un commutateur et un routeur C'est le mode fonctionnement qui permet d'accéder aux fonctions de routage ; donc à l'interconnexion des réseaux virtuels par routage inter-VLAN. La mise en œuvre de ce type de routage est l'objet de ce document.
- Enfin, il ne faut pas oublier que tous les VLANs véhiculés dans le même *trunk* partagent la bande passante du média utilisé. Si un *trunk* utilise un lien 100Mbps Full-Duplex, la bande passante de tous les VLANs associés est limitée à ces 100Mbps Full-Duplex.

Routage inter VLAN :**Multilayer Switch**

- pas de routeur pour effectuer le routage.
- La fonctionnalité de routage est assurée par un **commutateur de niveau 3** et donc avec des fonctions de niveau 3 comme le routage.
- ces *mutlilayer switch* sont capables d'assurer les fonctions de niveau 2 et de niveau 3.
- Le commutateur qui effectue le routage doit avoir l'**ip routing** d'activé pour que cela fonctionne. Il effectuera le routage directement en interne.
- Ce type d'architecture est plus évolutif que les autres architectures car les routeurs ont un nombre limité d'interfaces alors que les commutateurs en ont beaucoup plus

Routage inter VLAN :Multilayer Switch



Mise en œuvre des VLANs

- Nous allons dans ce TP mettre en œuvre des VLANS de **niveau 1**, c'est à dire que chaque VLAN se verra attribuer un ou plusieurs ports physiques du commutateur.

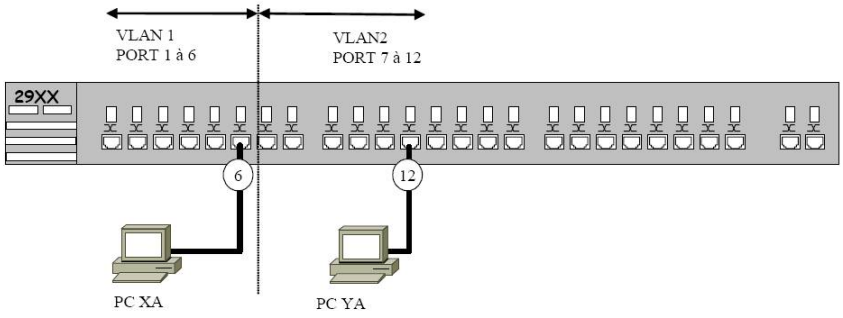


Figure 1

PARTIE 2
Les Réseaux Privés Virtuels
VPN

VPN

Réseau ('network')

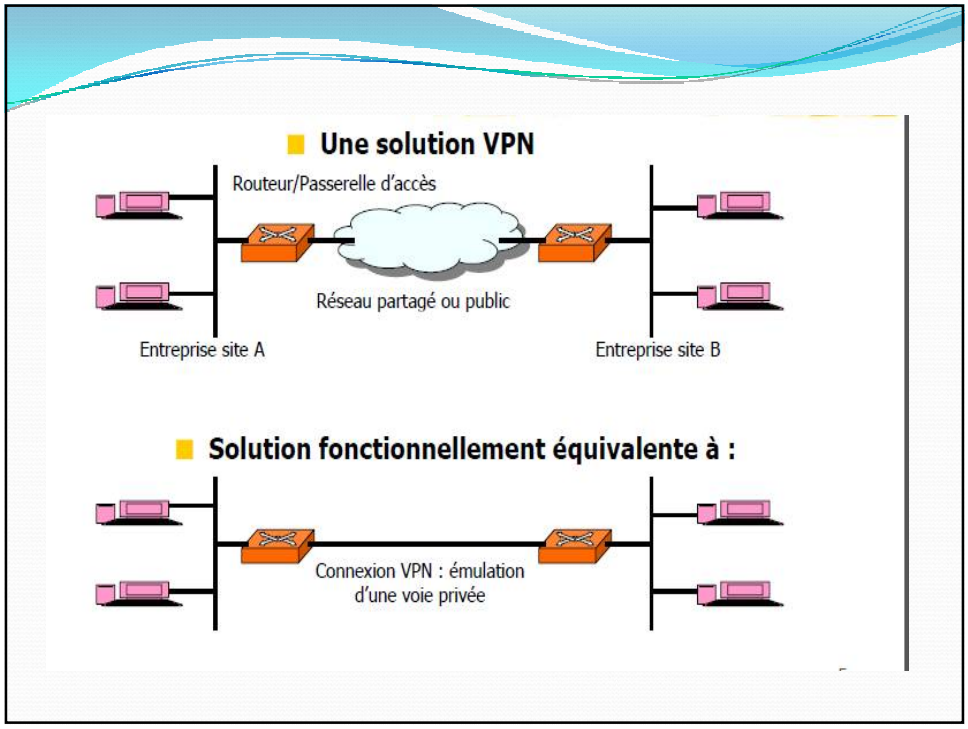
- Interconnecter un ensemble de **systèmes informatiques dispersés.**
- Résoudre des **problèmes de commutation/routage (niveau 2/3).**

Privé ('private')

- **Transporter des flots de messages d'une communauté 'privée' de** façon indépendante de ceux d'autres usagers.
- Les usagers doivent recevoir une **garantie de sécurité (confidentialité, intégrité ou protection) sur leurs données.**
- Les usagers autorisés peuvent communiquer en utilisant des **adresses, une topologie, un routage privés.**

Virtuel ('virtual')

- **Le réseau physique ne correspond pas forcément au réseau visé.**
- **Le réseau privé est réalisé en partageant les ressources d'un** (ou de plusieurs) fournisseur d'accès.



Motivations pour les VPN:Objectifs

1. **Communications sécurisées sur une infrastructure partagée.**

- **Sécurité visée : mécanismes de protection**

=> implantation en modifiant des protocoles de réseaux classiques.

- **Solutions: adressage et routage privé offerts par des mécanismes de** protection garantis par un constructeur de routeur et un fournisseur d'accès.
- **Sécurité visée : mécanismes pour la confidentialité et l'intégrité**

=> protocoles de sécurité utilisant des techniques de cryptographie.

- **Solutions: authentification, chiffrement en confidentialité, signatures.**

2. **Economies de coûts en partageant des plates-formes de communication à haut débit.**

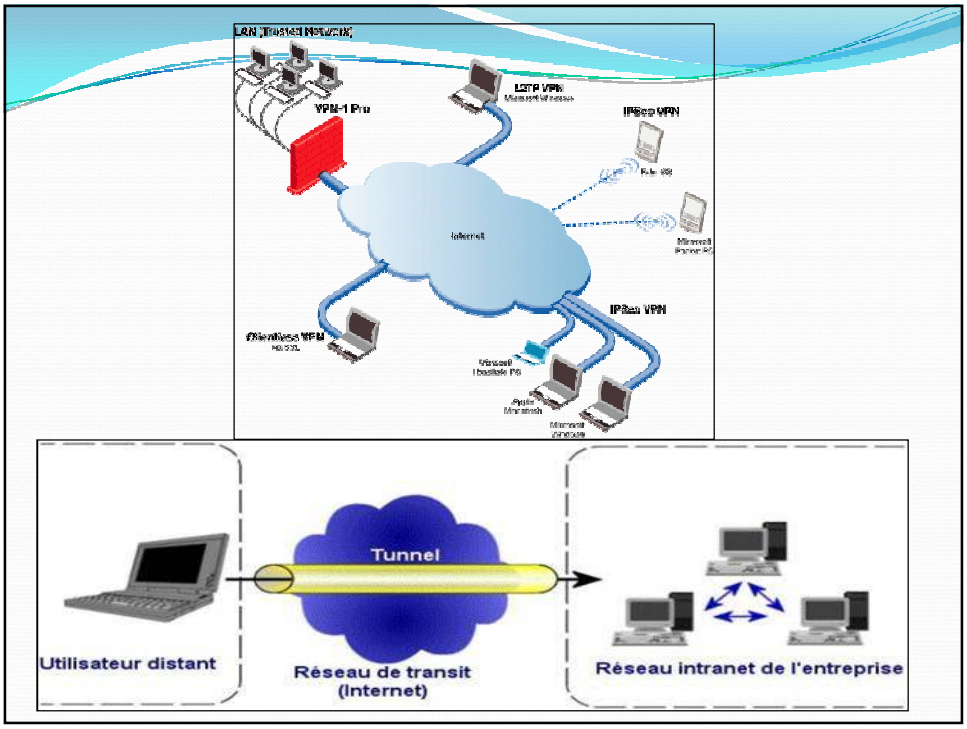
- **Efficacité du partage de voies physiques à haut débit: coût des** communications très réduit dans un réseau partagé (type l'Internet).
- **Solutions alternatives non VPN : construire sa propre infrastructure complètement privée en louant des liaisons spécialisées** ou des circuits => surcoûts de location, d'administration.

Motivations pour les VPN:Objectifs

3. **Communications fiables : sûres de fonctionnement 'dependable'.**
- **Critères : Disponibilité, fiabilité, sécurité ('safety'), maintenabilité.**
- Sûreté assurée par les redondances du réseau (maillage du réseau sous-jacent)
- => utilisation de protocoles de routage multi-chemin.

4. **Performances pour des infrastructures extensibles (qui passent à**
- **l'échelle, 'scalable').**
- **Critères : Temps de latence (temps jusqu'au commencement de la réponse à** une requête), **temps de réponse total , débit. Possibilité d'accroître la taille du réseau privé (extensibilité).**
- **Performances en VPN: souvent beaucoup de surcharges (protocoles** supplémentaires, algorithmes cryptographiques).

5. **Solutions pratiques ('flexible') : les VPN : sont souvent considérés comme difficiles à gérer.**
- **Facilité, simplicité d'établissement des connexions et de l'administration.**



VPN: Composants

- Réseau(x) local(aux) existant(s).
- Connexion à internet.
- Périphérique de périmètre (routeur, pare-feu ou switch).
- Logiciel de création et gestion du tunnel VPN.
- Télétravailleur (employé à distance) éventuellement.

VPN : types

- Il existe trois types de VPNs :

✓**VPN d'accès:** connexion d'un télétravailleur au réseau de l'organisation utilisant le VPN via internet.

✓**L'intranet VPN :** connexion de plusieurs intranets, géographiquement distants ,d'une même organisation.

✓**L'extranet VPN :** Ouverture du réseau local de l'organisation aux fournisseurs et clients. Ce type nécessite une forte authentification et traçabilité pour chaque accès.

VPN: avantages

- **Sécurité:** utilisation de protocoles de chiffrement et authentification protégeant les données.
- **Economie:** utilisation principale d'internet comme média de transport.
- **Evolutivité:** utilisation de l'infrastructure d'internet dans les FAIs, ce qui permet à l'infrastructure de l'organisation de rester presque la même en ajoutant des utilisateurs.

VPN: contraintes

- **Authentification:** seuls les utilisateurs autorisés peuvent avoir accès (se trouvant aux extrémités du tunnel VPN).
- **Cryptage:** les donnés doivent être chiffrées et cryptées afin d'assurer la confidentialité et l'intégrité de ces dernières lors du transport.
- **Multi-protocole:** les VPNs doivent supporter les protocoles les plus utilisés sur internet.

Classification des solutions VPN

A) Classification selon le niveau du modèle OSI.

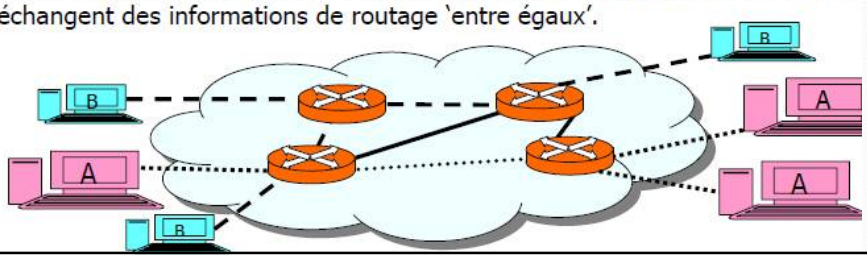
1. **VPN de niveau liaison**
2. **VPN de niveau réseau.**
3. VPN de niveau transport.
4. VPN de niveau application.

B) Classification selon l'approche de sécurité

- **Protection: Solutions de niveau 3 en routage pair à pair ('VPN Peer to** peer'), de niveau (1) ou 2 ou 3 en recouvrement (VPN 'overlay')
- **Authentification, Confidentialité, Intégrité : solutions de niveau** quelconque (2,3,4,7) basées sur l'utilisation de tunnels ('Secure VPN Tunnelling').

VPN de protection: Solution des VPN 'pair à pair' 'peer to peer'

- **1) Approche de VPN (niveau 3) basée sur le contrôle d'accès (routag**
  - On parle quelquefois de 'Trusted VPN', VPN de confiance.
  - Solution implantée essentiellement dans les **VPN MPLS: L3VPN.**
- **2) Construction de groupes fermés d'usagers** d'un réseau => VPN
  - Sur la figure groupe A rose, B bleu.
- **3) Un routage est défini pour chaque groupe (VPN)**
  - Sur la figure VPN A : routes en traits pointillés courts ou VPN B : traits pointillés lo
- **4) Idée de routage pair à pair :** Le routage dans un VPN pair à pair est ré comme dans les routages Internet classiques (RIP, OSPF,...): les routeurs voi échangent des informations de routage 'entre égaux'.



2) Solution VPN en mode tunnel : Notion de tunnelage 'Tunneling'

- **Notion de tunnel :** utiliser un protocole pour acheminer des messages d'un autre protocole.
  - **Encapsulation des messages du protocole transporté** dans des messages du protocole transporteur.
  - **Solution fréquente en réseau.**
- **Architecture en couches des réseaux (OSI) :** encapsuler des messages de **niveau N+1** dans des messages de **niveau N** (inférieur).
- **Différence mode tunnel et modèle OSI:**

  Tunnel = encapsuler des messages **d'un niveau donné** dans des messages du **même niveau ou de niveaux supérieurs.**

12

VPN: protocoles de tuneling

- Tunnel reliant une source et une destination tous deux autorisées.
- Repose sur le protocole de «tuneling » .

✓ **Protocole de tuneling:**

permet de faire circuler les données de l'organisation d'un bout à l'autre du tunnel de façon sécurisée (chiffrement et cryptage) . Ainsi, les utilisateurs ont l'impression de se connecter directement sur le LAN de l'organisation.

VPN: protocoles de tunneling

Les protocoles de tunneling utilisés sont:

- protocoles de **couche 2** OSI : PPTP ou L2TP.
- protocoles de **couche 3** OSI : IPsec ou MPLS

- **PPTP** (Point to Point Tuneling Protocol) : son principe est de créer des trames sous le protocole PPP et de les encapsuler dans un paquet IP. Il permet de crypter les données et de les compresser.

  Remarque:

  Le protocole PPP (Point to Point Protocol) assure le transfert des données de bout en bout. Il garantit l'ordre d'arrivée des paquets.
- **IPsec** (IP security): il a intégré des techniques de protection des données communes aux protocoles IPv4 et IPv6. Il assure l'intégrité, le cryptage et l'authenticité.

IPSec

- « Protocole de sécurité au sein de la couche réseau. Ce protocole est développé pour fournir un service de sécurité à base de cryptographie, permettant de garantir l'authentification, l'intégrité, le contrôle d'accès et la confidentialité des données. »

- D'une manière plus commune : **IPSec = formatage de trame permettant le chiffrement des données au niveau IP.**

Services de sécurité fournis par IPsec

- **Confidentialité :**

  La capture des paquets ne doit pas permettre de savoir quelles sont les informations échangées.

  Seules les machines réceptrices et émettrices doivent pouvoir accéder à l'information.

- **Authentification:**

  Le récepteur doit être capable de vérifier si les données reçues proviennent bien de l'émetteur supposé.

Services de sécurité fournis par IPsec

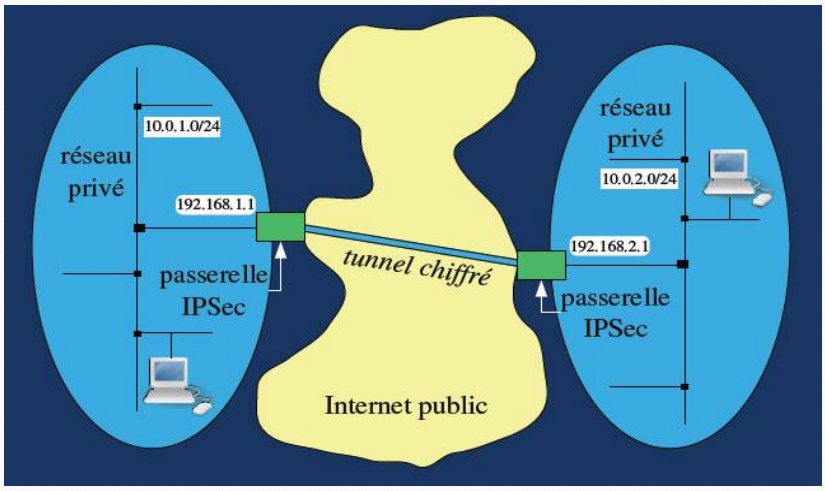
- **Intégrité :**

  Le récepteur doit être capable de vérifier si les données n'ont pas été modifiées lors de la transmission.

- **Protection contre le rejeu :**

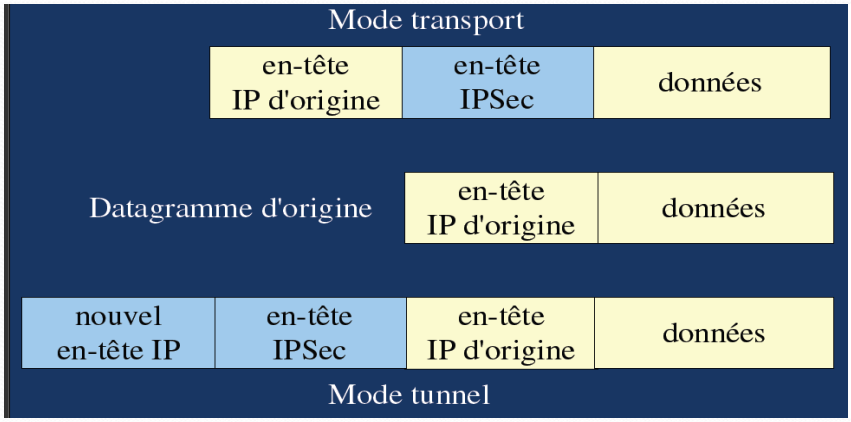
  Une personne qui intercepte un message d'une communication sécurisée entre deux machines ne pourra pas retransmettre ce message sans que cela soit détecté.

Fonctionnement d 'Ipsec



Les modes de fonctionnement d 'Ipsec

- *2 modes : mode tunnel et mode transport*



Les modes de fonctionnement d 'Ipsec

- En mode transport, seules les données des protocoles de niveau supérieur sont protégées. Le mode transport ne devrait être utilisé qu'entre des équipements connectés par une liaison point à point

- En mode tunnel, l'en-tête IP d'origine est protégé et est remplacé par un nouvel en-tête. En particulier, les adresses source et destination du datagramme original sont masquées. C'est le mode utilisé pour mettre en œuvre des VPN

09

Différence entre les 2 modes

- Dans le mode transport, l'en-tête extérieur est produite par la couche IP c'est-à-dire sans masquage d'adresse, alors que dans le mode tunnel l'encapsulation IPSec permet le masquage d'adresses.

- Le mode tunnel est utilisé entre deux passerelles de sécurité (routeur, firewall, ...) alors que le mode transport se situe entre deux hôtes.

IPSEC : illustration du mode tunnel