

Routage IP

Préambule

Ce cours vous présente le principe du routage dans les réseaux IP. Il aborde également les protocoles de routage dynamique (intérieur et extérieur) ainsi que le principe du routage inter-vlan.

Pour mettre en œuvre le routage, je vous invite à faire les exercices et tutoriels proposés.

Introduction

Internet résulte de l'interconnexion de différents réseaux physiques par des machines appelées routeurs. Chaque réseau, contenant un ensemble d'hôtes, peut être connecté, éventuellement à un routeur.

Le routage peut s'effectuer via un élément de type routeur (cas général), switch (dans le cadre du routage intervlan), serveur (pour des tests)

La décision du routage se prend grâce aux informations situées dans la table de routage.

Le routage indique à un hôte réseau par où passer pour aller vers un autre réseau IP. Le travail du réseau consiste à trouver le bon chemin pour acheminer les paquets d'une source vers une destination.

On peut trouver une analogie avec un véhicule qui part de Paris vers Brest et qui à chaque intersection cherche à prendre la meilleure route, qui peut être la plus courte, la plus économique ou la plus rapide. Quand on voyage, on s'intéresse d'abord aux grandes villes que l'on doit traverser (toutes directions) et plus on se rapproche, plus les indications vont être précises.

Dans le cadre d'un réseau, c'est quasiment équivalent à la différence près que ce n'est pas le paquet qui décide du chemin mais le réseau.

Routage minimal

Un réseau complètement isolé d'autres réseaux requiert uniquement un routage minimal qui est mis en place dès que l'interface est configurée. Cette table permet à une station de connaître son réseau et son adresse IP.

Exemple : une machine d'adresse 192.168.1.2/24 retrouvera ces informations dans la table de routage avec les lignes :

```
(@)192.168.1.2 (MASK)255.255.255.255 – (GW)192.168.1.2  
(INT)192.168.1.2 (indiquant sa propre adresse IP)  
(@)192.168.1.0 (MASK)255.255.255.0 – (GW)192.168.1.2 (INT)192.168.1.2  
(indiquant son propre réseau)
```

Routage static

Un réseau doté d'un nombre limité de routeurs vers d'autres réseaux IP peut être configuré en routage statique. L'administrateur crée manuellement une table de routage statique.

Les tables de routage statiques ne s'adaptent pas aux modifications apportées au réseau (pannes, ajouts de routeurs)

Les routeurs permettent de déterminer l'adresse physique de destinataire et de faire circuler les paquets à travers différents réseaux interconnectés.

Table de routage : c'est une mémoire qui possède l'adresse IP pour chaque numéro de réseau à atteindre. Elle peut également contenir une adresse de route par défaut.

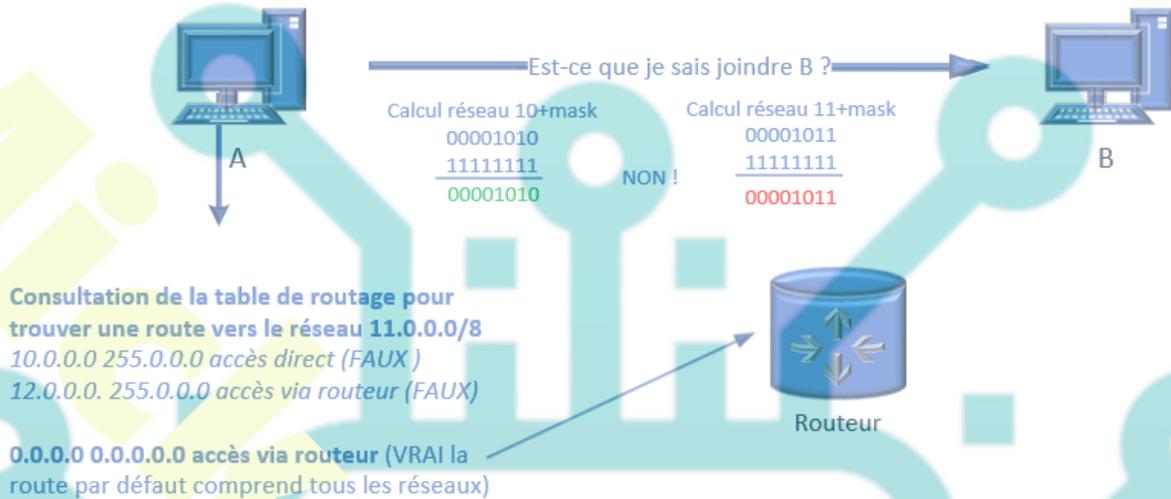
Les adresses IP sont traitées par des routeurs qui effectuent le routage en se basant sur le numéro de réseau. Un routeur relié à plusieurs réseaux aura plusieurs adresses IP.

Routage par défaut

Ce principe est utilisé pour indiquer à une machine ou un routeur la façon de communiquer avec les réseaux qu'il ne connaît pas. Il envoie alors la requête vers cette route par défaut.

Les routes par défaut peuvent être indiquées en utilisant la notation 0.0.0.0

Exemple : que se passe t'il lorsqu'une machine A située dans le réseau 10.0.0.0/8 veut communiquer avec une machine B située elle dans le réseau 11.0.0.0/8 ?



1. la machine A va comparer son adresse avec l'adresse destination en utilisant le ET entre l'adresse réseau et le masque.
2. Si la machine A obtient un résultat différent, cela veut indiquer que la machine B est dans un réseau différent du sien.
3. La machine A va consulter sa table de routage pour savoir s'il lui est possible d'atteindre le réseau demandé et s'il elle ne trouve pas la réponse, elle va chercher s'il existe une route par défaut.

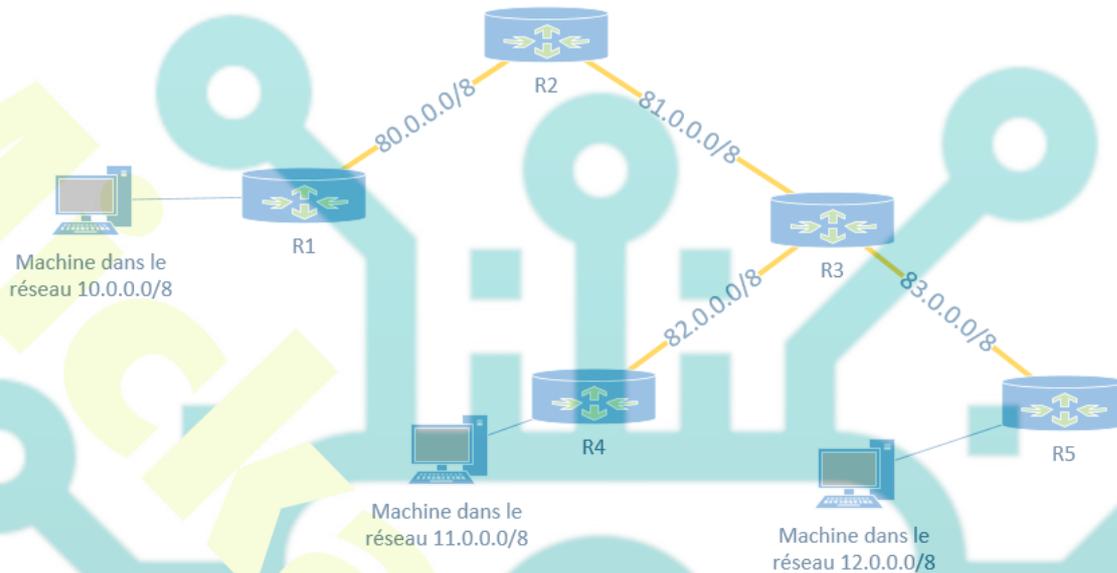
Routage direct

Consiste à rattacher x réseaux au même routeur.

Routage indirect

C'est le routage le plus complexe car il consiste à envoyer les messages de routeur à routeur jusqu'au destinataire en se servant des tables de routage.

Comment concevoir ses routes?



Principe

1. Les routeurs connaissent déjà les réseaux sur lesquels ils sont connectés.
 2. On doit leur indiquer quels sont les réseaux distants et par quel routeur voisin passer, où utiliser une route par défaut (ce qui veut dire que le routeur n'a qu'un seul voisin possible).
 3. Il n'est pas utile d'indiquer les réseaux ne contenant pas de machines à joindre (réseaux intermédiaires)
- Dans le schéma ci-dessus, le R1 peut utiliser la route par défaut puisque pour joindre n'importe quel réseau il devra forcément passer par R2 (seul voisin possible). On indiquera à R1 le réseau suivant **0.0.0.0** puis le masque associé **0.0.0.0** et enfin par quel routeur passer **@ip de R2** (coté 80.0.0.0)

Réseau destination	Masque	Passerelle
0.0.0.0	0.0.0.0	80.0.0.2

Table de routage de R1

- Le R2 lui ne peut pas utiliser la route par défaut car il a 2 voisins (R1 et R3), on doit donc lui préciser quel routeur utiliser en fonction des réseaux à joindre. On indiquera la route **10.0.0.0** puis le **masque associé 255.0.0.0** et enfin par quel routeur passer **@ip de R1** (coté 80.0.0.0). Puis on indiquera la route **11.0.0.0** puis le masque associé **255.0.0.0** et enfin par quel routeur passer **@ip de R3** (coté 81.0.0.0). Enfin, on indiquera la route **12.0.0.0** puis le masque associé **255.0.0.0** et via **@ip de R3** (coté 81.0.0.0)

Réseau destination	Masque	Passerelle
10.0.0.0	255.0.0.0	80.0.0.1
11.0.0.0	255.0.0.0	81.0.0.3
12.0.0.0	255.0.0.0	81.0.0.3

Table de routage de R2

- Le R3 lui ne peut pas utiliser la route par défaut car il a 3 voisins (R2,R4 et R5), on doit donc lui préciser quel routeur utiliser en fonction des réseaux à joindre. On indiquera la route **10.0.0.0** puis le **masque associé 255.0.0.0** et enfin par quel routeur passer **@ip de R2** (coté 81.0.0.0). Puis on indiquera la route **11.0.0.0** puis le masque associé **255.0.0.0** et enfin par quel routeur passer **@ip de R4** (coté 82.0.0.0). Enfin, on indiquera la route **12.0.0.0** puis le masque associé **255.0.0.0** et via **@ip de R5** (coté 83.0.0.0).

Réseau destination	Masque	Passerelle
10.0.0.0	255.0.0.0	81.0.0.2
11.0.0.0	255.0.0.0	82.0.0.4
12.0.0.0	255.0.0.0	83.0.0.5

Table de routage de R3

- Le R4 peut utiliser la route par défaut puisque pour joindre n'importe quel réseau il devra forcément passer par R3 (seul voisin possible). On indiquera à R4 le réseau suivant **0.0.0.0** puis le masque associé **0.0.0.0** et enfin par quel routeur passer **@ip de R3** (coté réseau 82.0.0.0)

Réseau destination	Masque	Passerelle
0.0.0.0	0.0.0.0	82.0.0.3

Table de routage de R4

Le R5 peut utiliser la route par défaut puisque pour joindre n'importe quel réseau il devra forcément passer par R3 (seul voisin possible). On indiquera à R5 le réseau suivant **0.0.0.0** puis le masque associé **0.0.0.0** et enfin par quel routeur passer **@ip de R3** (coté réseau 83.0.0.0).

Réseau destination	Masque	Passerelle
0.0.0.0	0.0.0.0	83.0.0.3

Table de routage de R5

<http://en.dnstools.ch/visual-traceroute.html>

Trace route visuel

La translation d'adresses – NAT

Le NAT est une technique qui permet de traduire une adresse privée non routable en une adresse publique routable.

En effet, les adresses privées ne sont pas routables sur Internet du fait qu'il existe des milliards d'adresses privées partagées par les particuliers et les entreprises et que les routeurs d'internet ne pourraient aiguiller dans leur table de routage.

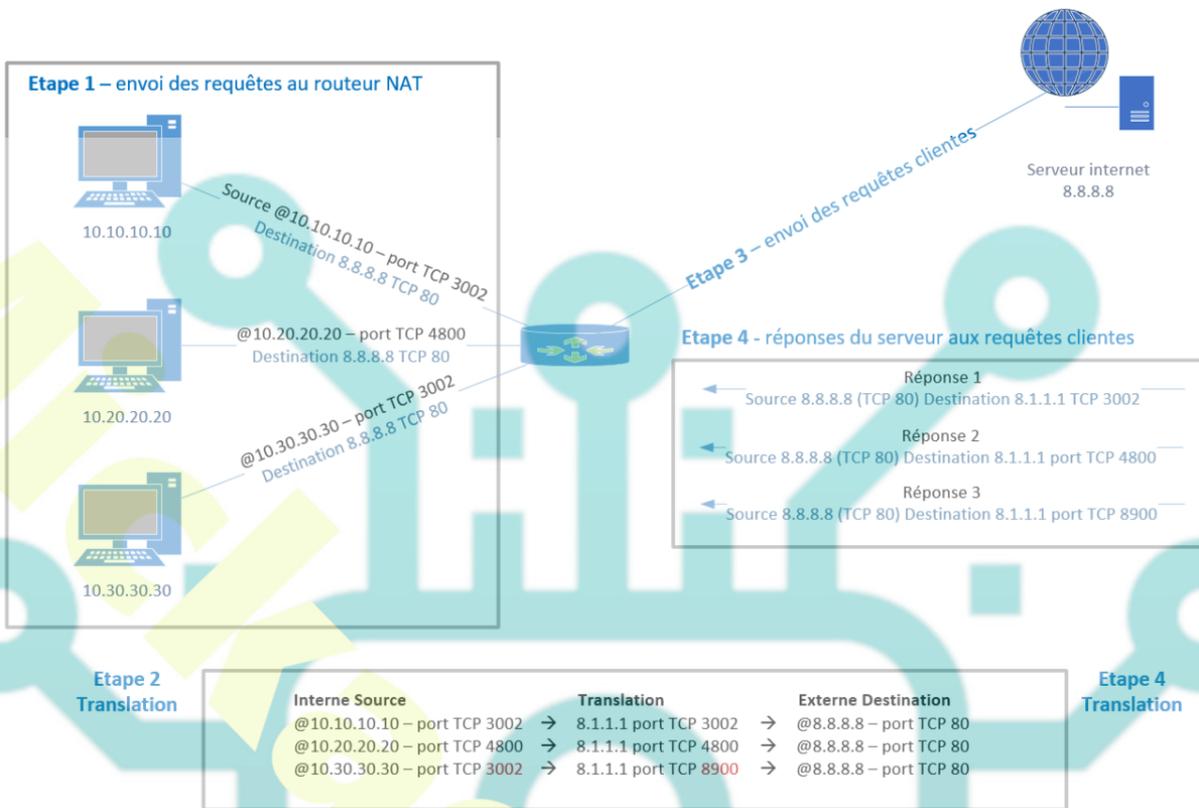
Le principe du NAT consiste donc à utiliser une passerelle de connexion entre le réseau privé et internet. Cette passerelle possède au moins une interface réseau connectée sur le réseau privé et au moins une interface réseau connectée à Internet.

Le NAT de base est statique et attribue de façon unique et automatique une adresse IP publique à une adresse IP privée. Cependant, si nous avons 500 PC cela oblige à avoir le même nombre d'IP publiques que d'IP privées, soit 500 adresses publiques, ce qui n'est pas possible.

Le NATP ou NAT/PAT

Le NAT associé au PAT (translation de ports) va permettre de résoudre le problème en associant adresse et port de connexion pour pouvoir identifier les flux de façon certaine.

Cette opération reste transparente pour la machine locale (privée) puisque cela est effectué au niveau du NAT qui rétablit ensuite les paramètres initiaux pour cette machine comme dans l'exemple suivant.

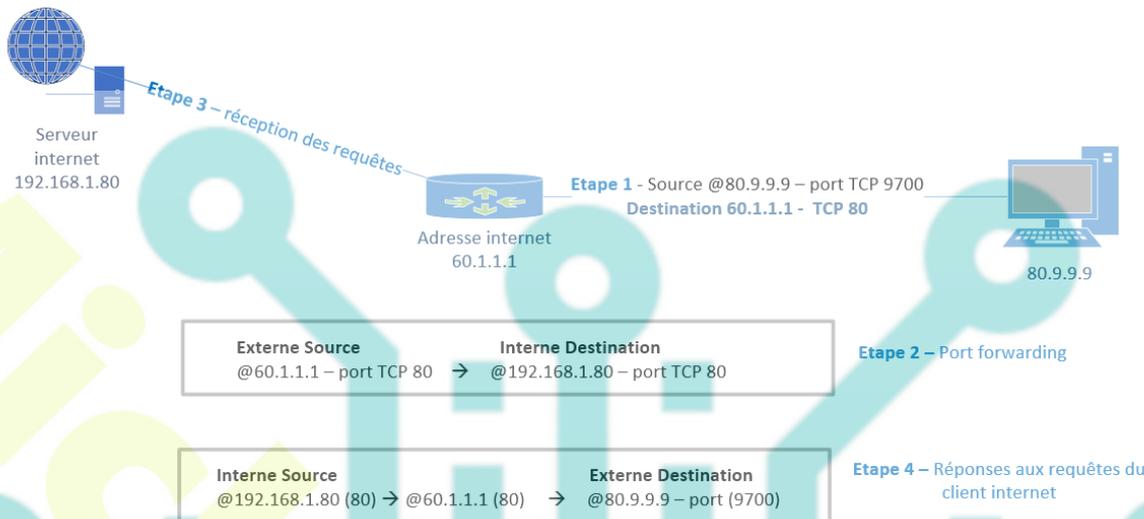


Le NAT Redirect/Port Forwarding

Il est identique au précédent sauf qu'il présente des services additionnels de redirection des flux entrants ou sortants.

Le Port Forwarding permet aux machines situées à l'extérieur d'accéder à un service (serveur WEB ou autre) qui est en fait basé sur une machine de réseau privé.

La machine distante pense alors communiquer directement avec la machine hébergeant le NAT alors qu'en fait celui-ci redirige le flux vers la machine correspondant réellement à ce service.



Redondance routeur

VRRP (Virtual Router Redundancy Protocol)

Ce protocole utilise la notion de routeur virtuel, auquel est associée une adresse IP virtuelle ainsi qu'une adresse MAC virtuelle.

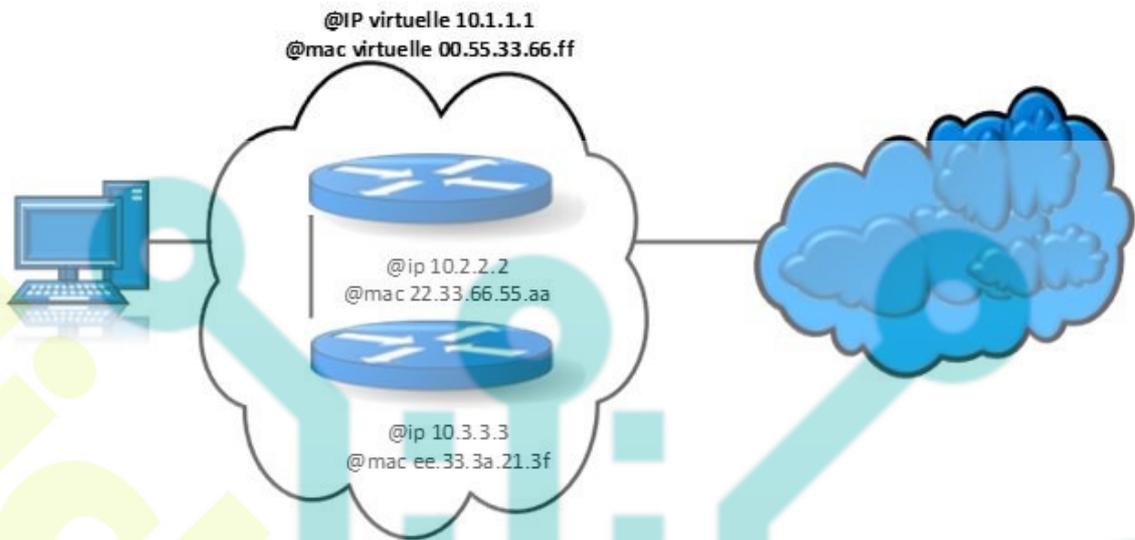
Parmi un groupe de routeurs participant à VRRP, le protocole va élire un maître, qui va répondre aux requêtes ARP pour l'adresse IP virtuelle, ainsi qu'un ou plusieurs routeurs de secours, qui reprendront l'adresse IP virtuelle en cas de défaillance du routeur maître.

HSRP (Hot Standby Router Protocol)

Protocole Cisco utilisé pour assurer la disponibilité de la passerelle par défaut dans un sous-réseau en dépit d'une panne d'un routeur.

Parmi un groupe de routeurs participant à HSRP, un routeur actif est élu (celui possédant la priorité la plus élevée), les autres routeurs sont en standby et écoutent les messages émis par le routeur actif.

Périodiquement, les routeurs du groupe échangent des messages Hello pour s'assurer que les routeurs du groupe sont encore joignables. Par défaut, les messages Hello sont envoyés toutes les 3 secondes. Un délai de 10 secondes sans message Hello venant du routeur actif entraîne la promotion du routeur Standby en routeur actif.



Les routeurs physiques forment un routeur virtuel. Un des routeurs est en état « **Actif** » et transmet les échanges alors que l'autre est en « **Passif** » et reste à l'écoute de l'état du routeur « **Actif** », prêt à prendre la relève. En réalité, le routeur que voient les utilisateurs est un routeur virtuel composé de plusieurs routeurs qui travaillent via le protocole **HSRP**. Formant un groupe, un routeur sera désigné comme le routeur actif qui travaillera réellement et le ou les autres se tiendront prêt à prendre la relève si besoin.

L'élection des routeurs

L'élection des routeurs sert à déterminer lequel sera primaire (actif) et lequel sera secondaire (passif). Le processus d'élection se met en place dès l'installation des liens et des routeurs dans un groupe. Le routeur qui aura la plus haute priorité (ou « **priority** ») sera le routeur primaire du groupe **HSRP**. Si aucune modification des priorités n'est faite (valeur par défaut 100), c'est le routeur qui aura **PIP** la plus haute qui sera désigné comme routeur primaire. Le groupe **HSRP** est alors sûr de trouver un routeur primaire parmi l'ensemble des routeurs qui le compose.

Une fois l'élection effectuée, seul le routeur principal enverra des paquets pour avvertir les autres de son état.

Ceux-ci seront envoyés en **multicast** sur l'IP 224.0.0.2 via UDP. Les routeurs passifs, attentifs à la réception de ces paquets, prendront le relais (après une réélection) s'ils ne reçoivent pas de paquets « Hello » pendant un certain délai.

Proxy ARP

C'est un serveur qui répond aux requêtes ARP concernant une ou plusieurs adresses IP qui ne sont pas présentes sur ce réseau. Le mandataire ARP connaît lui la véritable adresse de l'équipement destinataire du datagramme IP.

Fonctionnement

Lorsque que le mandataire reçoit une demande à destination de l'élément pour lequel il travaille, il répond aux requêtes ARP avec sa propre @mac et se charge de les communiquer à l'emplacement réel de l'équipement à qui elles étaient destinées, le plus souvent à travers un tunnel réseau.

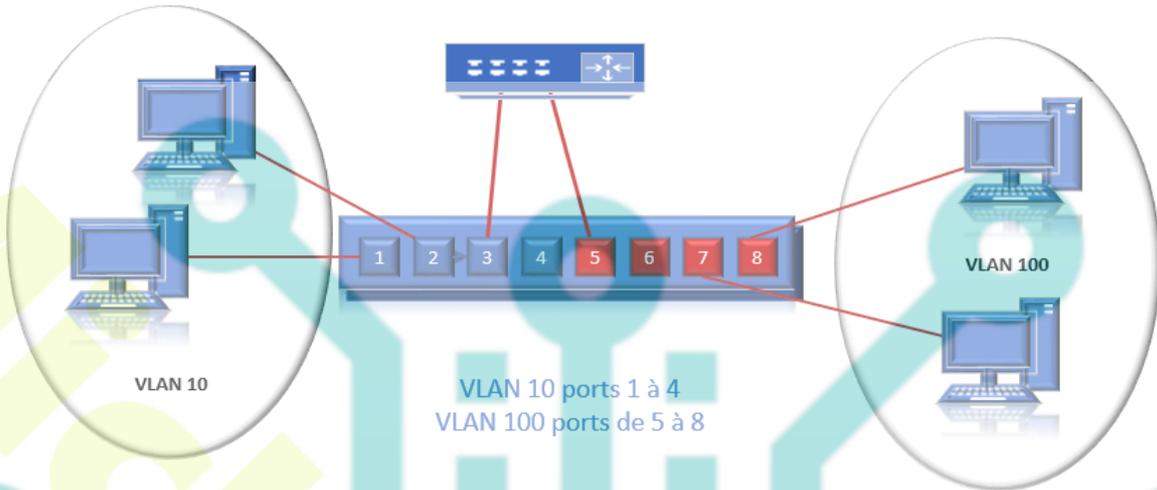
Le routage intervlan

Le routage intervlan permet d'interconnecter les messages entre plusieurs réseaux IP isolés dans des vlan.

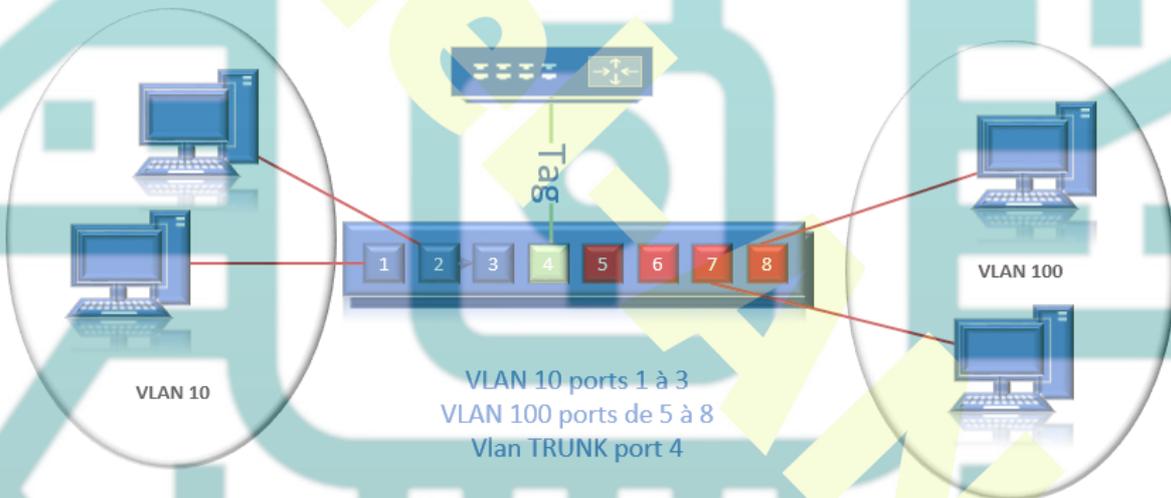
Ce routage peut être effectué par un routeur traditionnel ou par un switch de niveau 3 intégrant le service de routage.

- Un routeur avec une interface réseau dans chaque vlan. Cependant, cette technique n'est plus possible lorsqu'il y a de nombreux vlan.

Plusieurs techniques sont possibles



- Un routeur comprenant le tag (802.1q) Dans ce cas, une seule interface physique est nécessaire, on utilise la notion d'interface logique (1 par vlan)



- Un switch intégrant le routage. Cette solution est la plus efficace, cependant, ce type de commutateur est plus onéreux qu'un commutateur standard.