

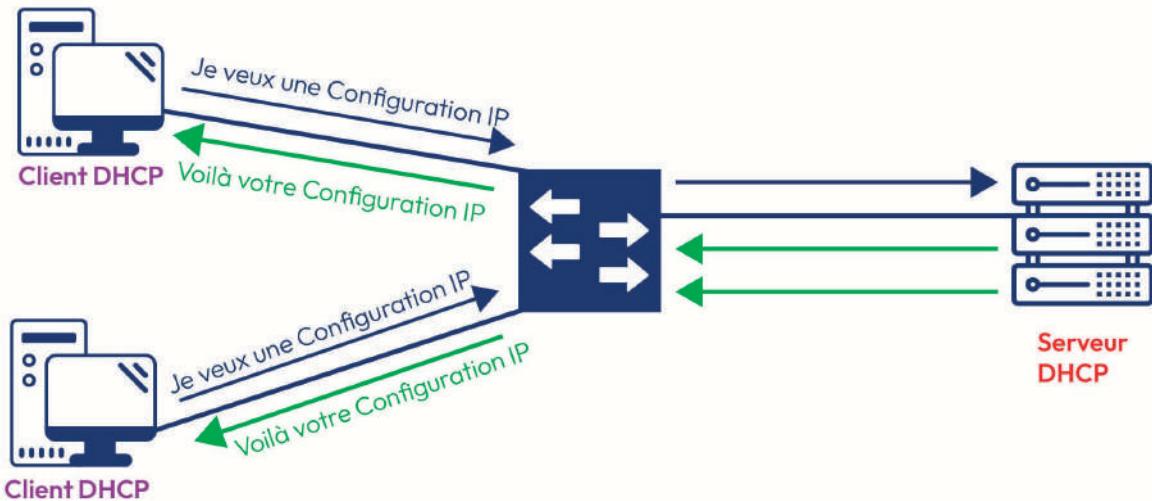
10

LES SERVICES IP

10.1. Le service DHCP pour IPv4

10.1.1. Définition :

Le protocole DHCP (Dynamic Host Configuration Protocol) permet d'attribuer une configuration IP d'une manière dynamique aux hôtes du réseau.



Le protocole DHCP assure la communication entre :

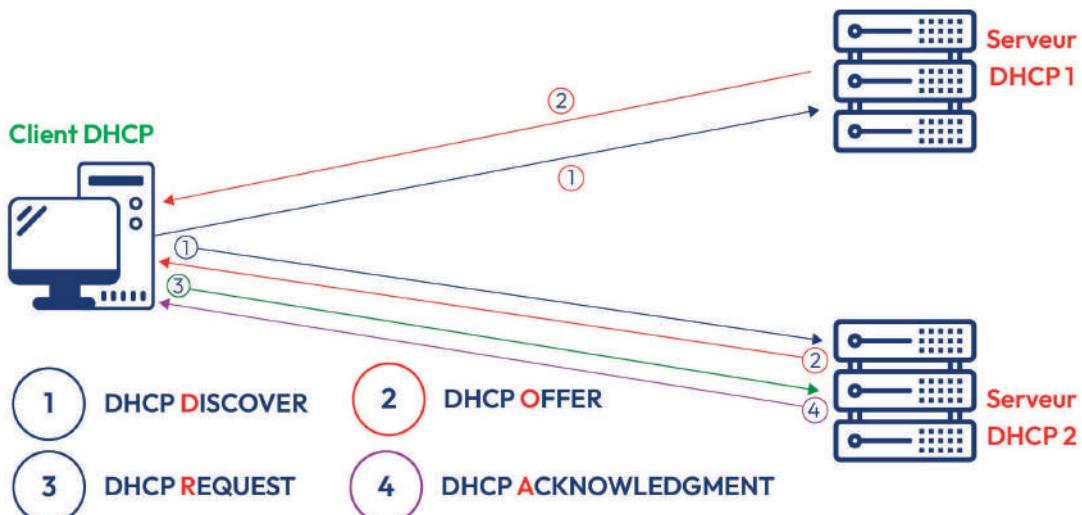
- ⌚ **Les clients DHCP**, qui demandent une configuration IP (Adresse IP, Masque de sous-réseau, Passerelle par défaut, Adresses des serveurs DNS, etc.)
- ⌚ **Un serveur DHCP**, qui fournit une configuration IP comme réponse aux requêtes des clients DHCP.

10.1.2. Avantages liés à l'utilisation du DHCP

AVEC DHCP	SANS DHCP
Les adresses sont fournies automatiquement	Les adresses sont configurées manuellement
L'exactitude des informations de configuration est garantie	Risque d'erreur de saisie d'une configuration IP
La configuration des clients est mise à jour automatiquement	La configuration doit être mise à jour manuellement
La tâche de configuration ne demande aucune intervention après la configuration du serveur DHCP	La tâche de configuration est délicate surtout si le nombre des machines est très élevé

10.1.3. Fonctionnement DHCP :

PREMIÈRE CONNEXION DU CLIENT DHCP



DHCP DISCOVER :

DESCRIPTION	Premier message envoyé par le client DHCP pour détecter la présence d'un serveur DHCP
MAC SOURCE	MAC du client DHCP
MAC DESTINATION	FF:FF:FF:FF:FF:FF
IP SOURCE	0.0.0.0
IP DESTINATION	255.255.255.255
PORT SOURCE	UDP 68
PORT DESTINATION	UDP 67

DHCP OFFER :

DESCRIPTION	Le serveur propose une configuration IP en envoyant DHCP OFFER
MAC SOURCE	MAC du serveur DHCP
MAC DESTINATION	FF:FF:FF:FF:FF:FF
IP SOURCE	IP du serveur DHCP
IP DESTINATION	255.255.255.255
PORT SOURCE	UDP 67
PORT DESTINATION	UDP 68

Remarque :

Si plusieurs serveurs DHCP existent, plusieurs offres peuvent être reçues par le client DHCP.

DHCP REQUEST :

DESCRIPTION	Le client retient une des offres reçues et diffuse sur le réseau un message DHCP REQUEST
MAC SOURCE	MAC du client DHCP
MAC DESTINATION	FF:FF:FF:FF:FF:FF
IP SOURCE	0.0.0.0
IP DESTINATION	255.255.255.255
PORT SOURCE	UDP 68
PORT DESTINATION	UDP 67

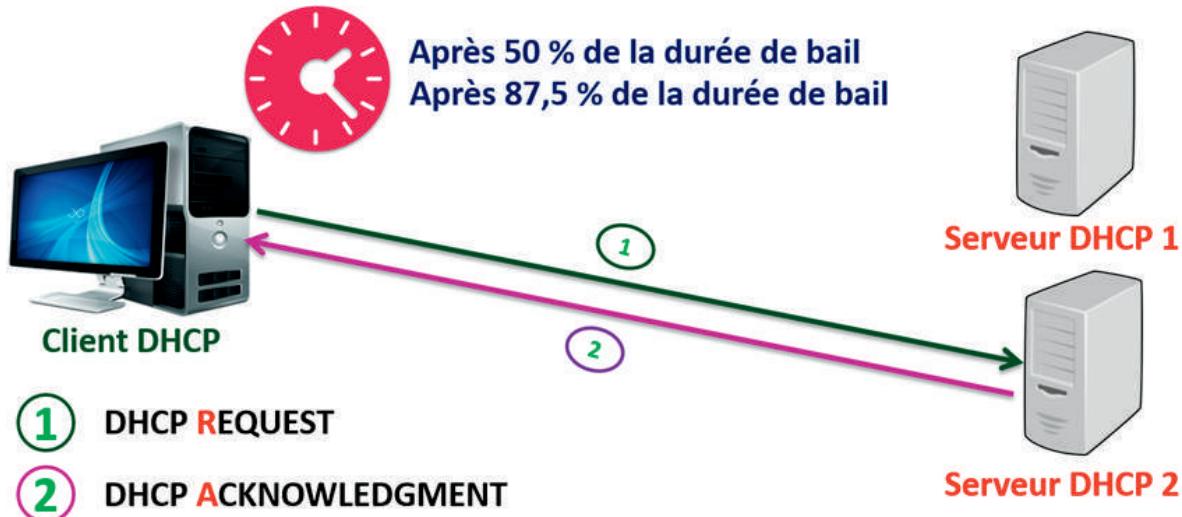
DHCP ACK

DESCRIPTION	Le serveur DHCP valide l'attribution de la configuration IP au client
MAC SOURCE	MAC du serveur DHCP
MAC DESTINATION	FF:FF:FF:FF:FF:FF
IP SOURCE	IP du serveur DHCP
IP DESTINATION	255.255.255.255
PORT SOURCE	UDP 67
PORT DESTINATION	UDP 68

Après la réception du dernier paquet DHCP ACK, le client obtient une configuration IP :

- ⌚ Adresse IP
- ⌚ Masque de sous-réseau
- ⌚ Passerelle par défaut
- ⌚ Adresses des serveurs DNS
- ⌚ Adresse du serveur DHCP (qui a fourni la configuration au client)
- ⌚ Durée de bail : la durée de validité de la configuration IP

RENOUVELLEMENT DE BAIL DHCP

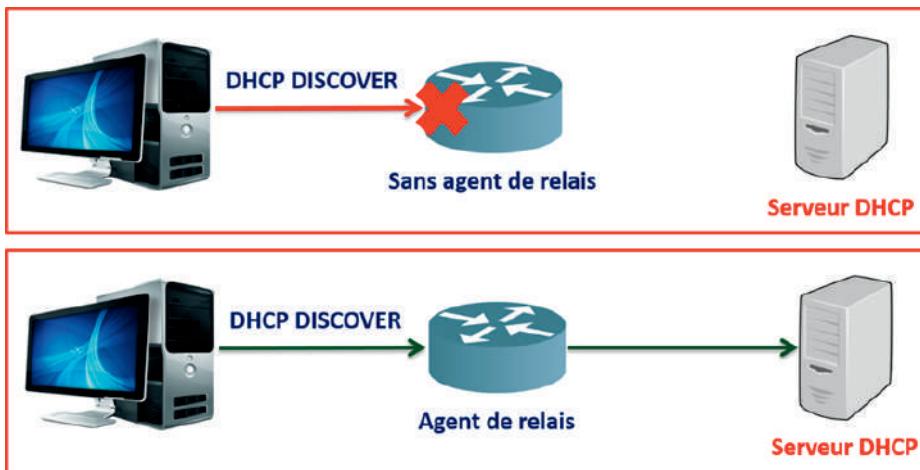


Quand la durée de bail arrive à 50%, le client DHCP envoie une requête DHCP REQUEST pour la renouveler.

S'il ne reçoit aucune réponse, il attend jusqu'à 87,5% de la durée de bail.

S'il ne reçoit aucune réponse, il envoie un DHCP DISCOVER pour chercher d'autres serveurs DHCP.

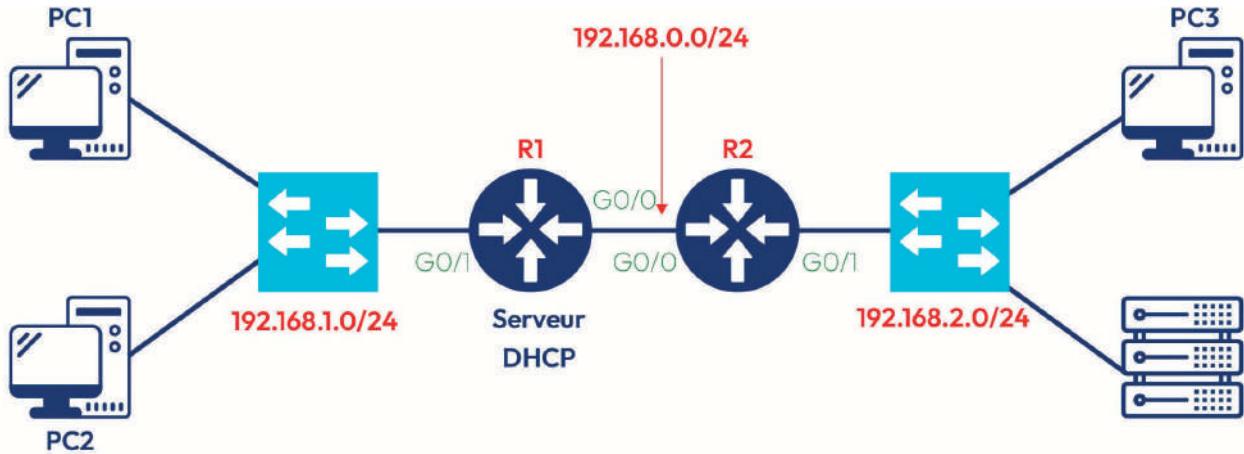
10.1.4. Agent de relais DHCP :



Le message DHCP DISCOVER est envoyé en broadcast (diffusion).

- Le routeur bloque les diffusions y compris le message DHCP
- On configure le routeur comme agent de relais DHCP afin de pouvoir contacter le serveur DHCP

10.1.5. Configuration du DHCP sur un routeur :



On va configurer :

- ➊ R1 comme serveur DHCP pour les deux sous-réseaux : 192.168.1.0/24 et 192.168.2.0/24.
- ➋ R2 comme agent de relais DHCP pour relayer les requêtes DHCP DISCOVER à partir du réseau 192.168.2.0/24

CONFIGURATION DES ADRESSES IP DES INTERFACES DES ROUTEURS :

Routeur R1:

```
R1(config)#interface G0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface G0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

Routeur R2:

```
R2(config)#interface G0/0
R2(config-if)#ip address 192.168.0.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface G0/1
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
```

CONFIGURATION DU SERVEUR DHCP :

NOM DU POOL DHCP	SR1	SR2
ADRESSES EXCLUES	192.168.1.1	192.168.2.1 – 192.168.2.10
RÉSEAU	192.168.1.0	192.168.2.0
MASQUE	/24	/24
PASSERELLE PAR DÉFAUT	192.168.1.1	192.168.2.1
ADRESSE DNS	192.168.1.1	192.168.1.1
NOM DU DOMAINE	Formip.com	Formip.com

Pool SR1 :

```
R1(config)#ip dhcp excluded-address 192.168.1.1
R1(config)#ip dhcp pool SR1
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#dns-server 192.168.1.1
R1(dhcp-config)#domain-name Formip.com
R1(dhcp-config)#exit
```

Pool SR2 :

```
R1(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
R1(config)#ip dhcp pool SR2
R1(dhcp-config)#network 192.168.2.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.2.1
R1(dhcp-config)#dns-server 192.168.1.1
R1(dhcp-config)#domain-name Formip.com
R1(dhcp-config)#exit
```

ATTRIBUTION DES ADRESSES IP AUX MACHINES :

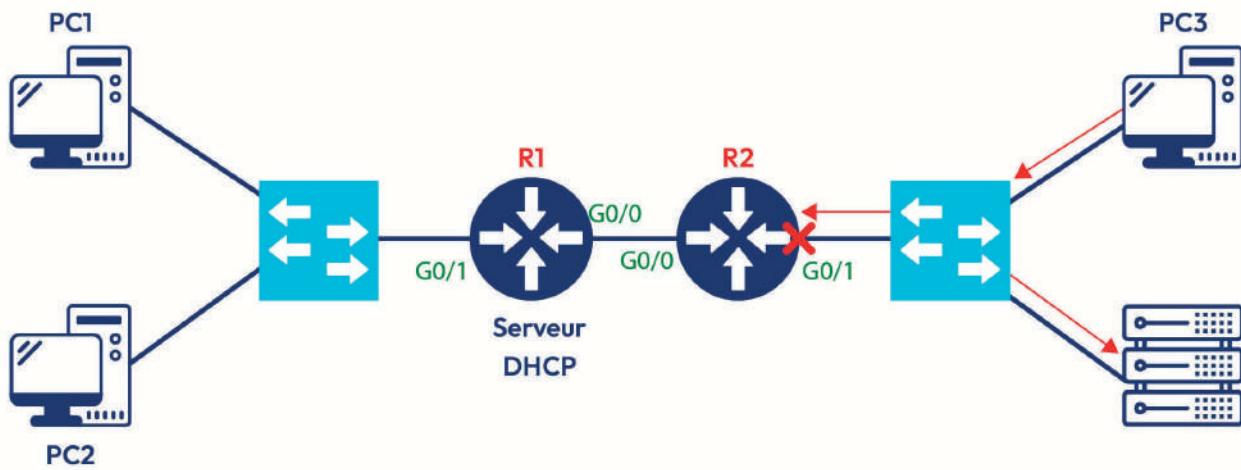
PC1 et PC2 vont recevoir la configuration IP

IP Configuration

DHCP Static DHCP request successful.

IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	192.168.1.1

Pour PC3 et le serveur, ils ne peuvent pas contacter le serveur DHCP



Et ils vont utiliser des adresses APIPA :

IP Configuration

DHCP Static DHCP failed. APIPA is being used.

IPv4 Address	169.254.179.193
Subnet Mask	255.255.0.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

Pour rappel : L'adresse IP APIPA (Automatic Private IP Addressing) est une fonctionnalité qui permet à un ordinateur sous Windows de configurer automatiquement une adresse IP privée dans un réseau local lorsque aucun serveur DHCP n'est disponible pour l'attribuer.

CONFIGURATION D'UN AGENT DE RELAIS DHCP

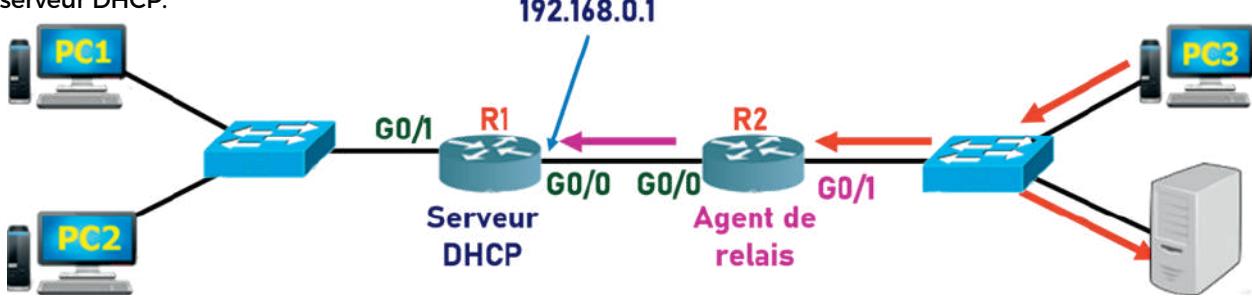
Définition :

Un agent de relais DHCP est un logiciel ou un périphérique qui permet aux clients DHCP de différents sous-réseaux de communiquer avec un serveur DHCP unique, en transmettant les demandes de clients à un serveur DHCP et en acheminant les réponses du serveur DHCP aux clients.

Il agit donc comme une passerelle pour les paquets DHCP entre les différents sous-réseaux et le serveur DHCP central.

En effet, cela permet aux administrateurs réseau de déployer des serveurs DHCP sur des sous-réseaux distants, tout en maintenant un seul point central de gestion des paramètres DHCP.

L'agent de relais permet de convertir le paquet « DHCP DISCOVER » en un paquet en monodiffusion destiné au serveur DHCP.



Configuration :

```
R2(config)#interface G0/1
R2(config-if)#ip helper-address 192.168.0.1
R2(config-if)#exit
```

Vérification de l'attribution des adresses IP

IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	192.168.2.16
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	192.168.1.1

AUTRES COMMANDES DHCP :

Affichage de la configuration DHCP :

```
R1#show running-config | section dhcp
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.2.1 192.168.2.10
ip dhcp pool SR1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 192.168.1.1
domain-name Formip.com
ip dhcp pool SR2
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
dns-server 192.168.1.1
domain-name Formip.com
```

Affichage des adresses attribuées aux clients DHCP :

IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.1.2	0002.162C.3C41	--	Automatic
192.168.2.11	0060.3E25.B3C1	--	Automatic

Configuration d'une interface d'un routeur comme client DHCP :

```
R2(config)#interface G0/0
R2(config-if)#ip address dhcp
R2(config-if)#exit
```

Affichage de la configuration IP d'une interface :

```
R1#show ip interface G0/2
```

Affichage de la configuration IP d'une carte réseau Windows :

```
PC> ipconfig
ou
PC> ipconfig /all
```

Libération de l'adresse IP d'une machine Windows :

```
PC> ipconfig /release
```

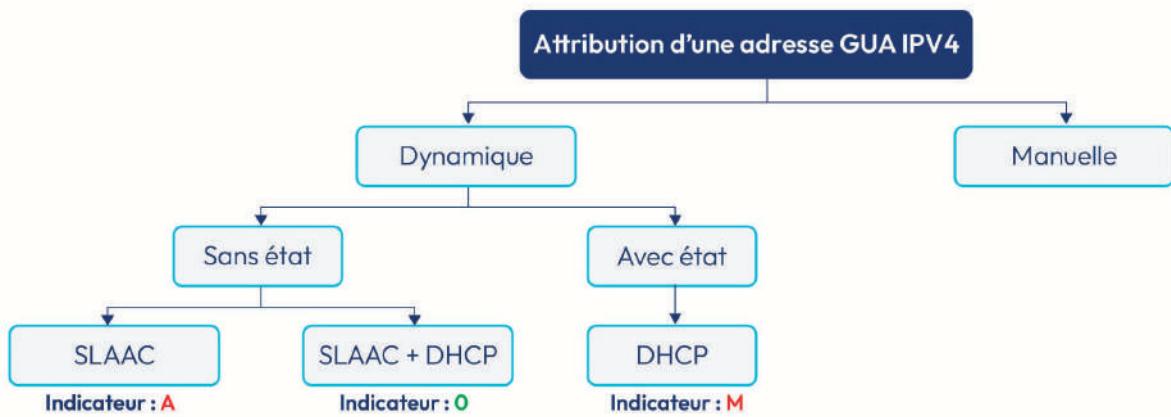
Renouvellement de bail DHCP d'une machine Windows :

```
PC> ipconfig /renew
```

10.2. SLAAC et DHCPv6 pour IPv6 :

10.2.1. Attribution des adresses GUA IPv6 :

MÉTHODES D'ATTRIBUTION DES ADRESSES GUA IPV6 :



Une adresse **Global Unicast Address (GUA)** est une adresse IPv6 unique qui peut être utilisée pour identifier un hôte sur Internet.

Généralement, cette dernière est utilisée dans le but d'identifier les hôtes finaux (par exemple, les ordinateurs, les téléphones, les serveurs, etc.), mais elle peut également être utilisée pour identifier d'autres équipements de réseau, tels que les routeurs et les commutateurs.

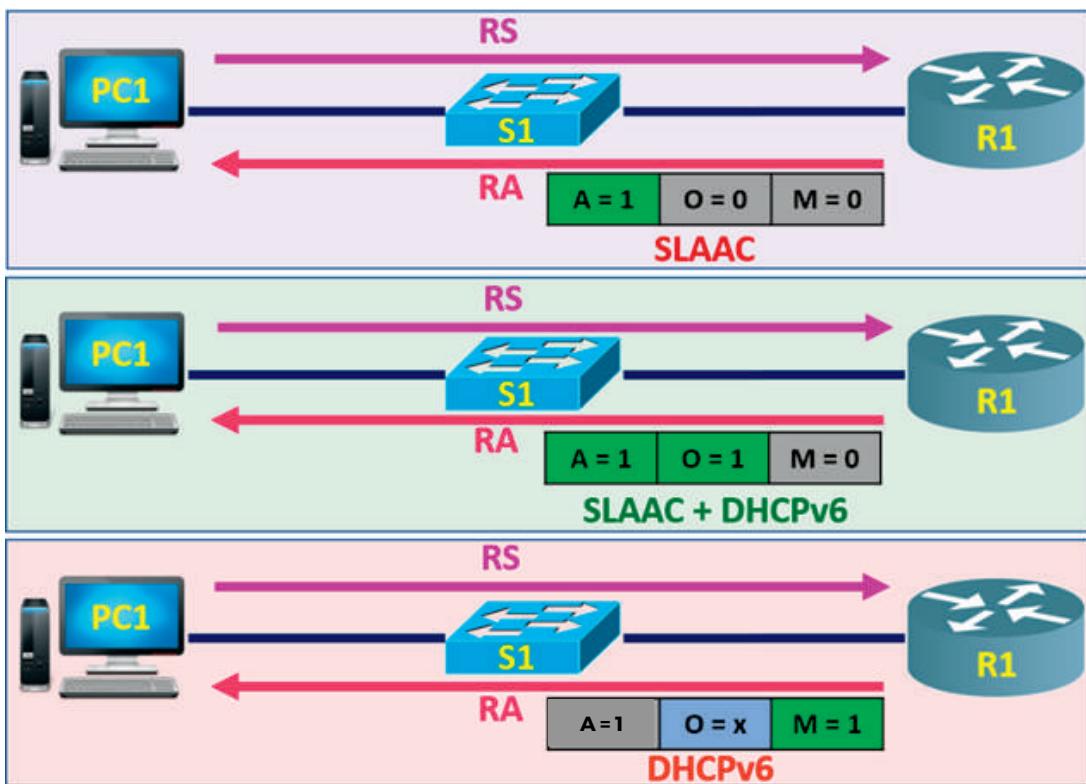
Les adresses GUA sont généralement assignées par un fournisseur de services Internet (ISP) ou un administrateur de réseau et sont utilisées afin de permettre à un hôte de communiquer avec d'autres hôtes sur Internet.

CHOIX DE LA MÉTHODE D'ATTRIBUTION PAR LES HÔTES :

L'ordinateur envoie un message de demande de sollicitation du routeur (RS)

Le routeur répond par un message d'annonce du routeur (RA) avec 3 possibilités :

- ➊ Indicateur A = 1, O = 0 et M = 0 → L'hôte utilise la méthode SLAAC seulement
- ➋ Indicateur A = 1, O = 1 et M = 0 → L'hôte utilise la méthode SLAAC et DHCPv6
- ➌ Indicateur A = 1, (O = 0 ou O = 1) et M = 1 → L'hôte utilise DHCPv6 seulement



10.2.2. SLAAC (Stateless Automatic Auto Configuration) :

SLAAC (Stateless Automatic Auto Configuration) est un protocole qui permet aux dispositifs réseau de configurer automatiquement leur adresse IP en utilisant les informations d'annonce "Router advertisement" qui sont diffusées par les routeurs sur un réseau local.

Il n'y a pas de mécanisme de demande d'adresse comme DHCP, les dispositifs utilisent plutôt des informations fournies par les routeurs pour configurer leur adresse IP automatiquement.

Cela rend SLAAC plus simple à mettre en place et à gérer, car il n'y a pas besoin de serveur DHCP. Néanmoins, il n'offre pas les mêmes fonctionnalités avancées que DHCP (attribution d'adresse en fonction de l'utilisateur ou du temps, gestion des réservations d'adresses, etc.).

SLAAC est souvent utilisé conjointement avec DHCPv6 pour fournir des fonctionnalités supplémentaires telles que la gestion des noms d'hôtes et la configuration d'autres paramètres réseau, comme les serveurs DNS.

En utilisant SLAAC, les dispositifs peuvent obtenir une adresse IP unique pour une plage d'adresses définie par les routeurs et cette dernière sera ainsi automatiquement configurée sur les dispositifs, sans besoin d'intervention manuelle.

Cela permet également aux adresses IP d'être utilisées de manière efficace, car elles sont attribuées en fonction de la disponibilité et non pas selon un ordre prédéfini.

Il est important de noter que SLAAC est un protocole de configuration d'adresse dit "stateless", cela signifie qu'il n'y a pas de mécanisme de "suivi" de l'utilisation des adresses IP attribuées.

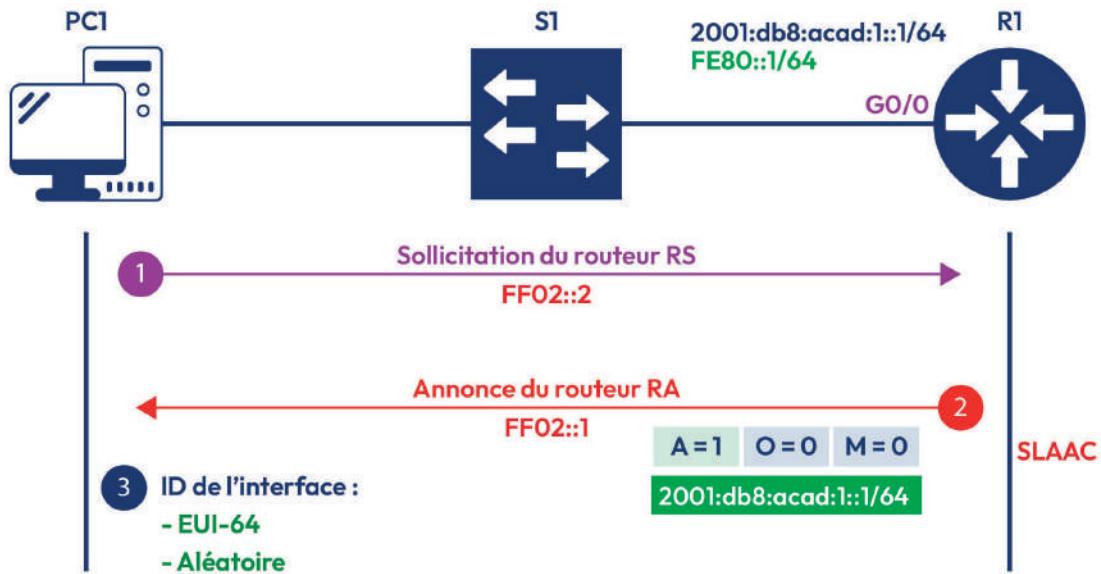
FONCTIONNEMENT SLAAC :

Les messages **Router Advertisement (RA)** et **Router Solicitation (RS)** sont utilisés dans les protocoles de configuration d'adresse IPv6 pour configurer automatiquement les adresses IP sur les dispositifs réseau.

- Les messages **Router Advertisement (RA)** sont utilisés par les routeurs pour annoncer leur présence sur le réseau et pour fournir des informations sur la configuration réseau aux dispositifs clients. Les informations fournies dans un message RA peuvent inclure des informations sur les plages d'adresses disponibles pour la configuration automatique, des informations sur les paramètres réseau tels que les serveurs DNS et des informations de sécurité pour les communications sur le réseau.
- Les messages **Router Solicitation (RS)** sont utilisés par les dispositifs clients pour demander des informations de configuration à un routeur sur le réseau. Lorsqu'un dispositif client envoie un message RS, les routeurs du réseau répondent en envoyant des messages RA avec les informations de configuration nécessaires. Cela permet aux dispositifs de configurer automatiquement leur adresse IP et d'autres paramètres réseau en utilisant les informations fournies par les routeurs.

En résumé, **les messages RA** permettent aux routeurs de fournir des informations de configuration aux dispositifs clients et **les messages RS** permettent aux dispositifs de demander ces informations à un routeur.

Ces deux types de message sont utilisés en conjonction pour configurer automatiquement les adresses IP et les paramètres réseau sur les dispositifs réseau.



- PC1 envoie un message **RS** à l'adresse de multidiffusion attribuer à tous les routeurs **FF02::2**
- R1 répond au message RS par un message **RA** et l'envoie à l'adresse de multidiffusion attribuée à tous les nœuds **FF02::1**: ce message RA contient le préfixe réseau **2001:DB8:ACAD:1:/64**
- PC1 génère l'ID de l'interface **aléatoirement** ou en utilisant la méthode **EUI-64**

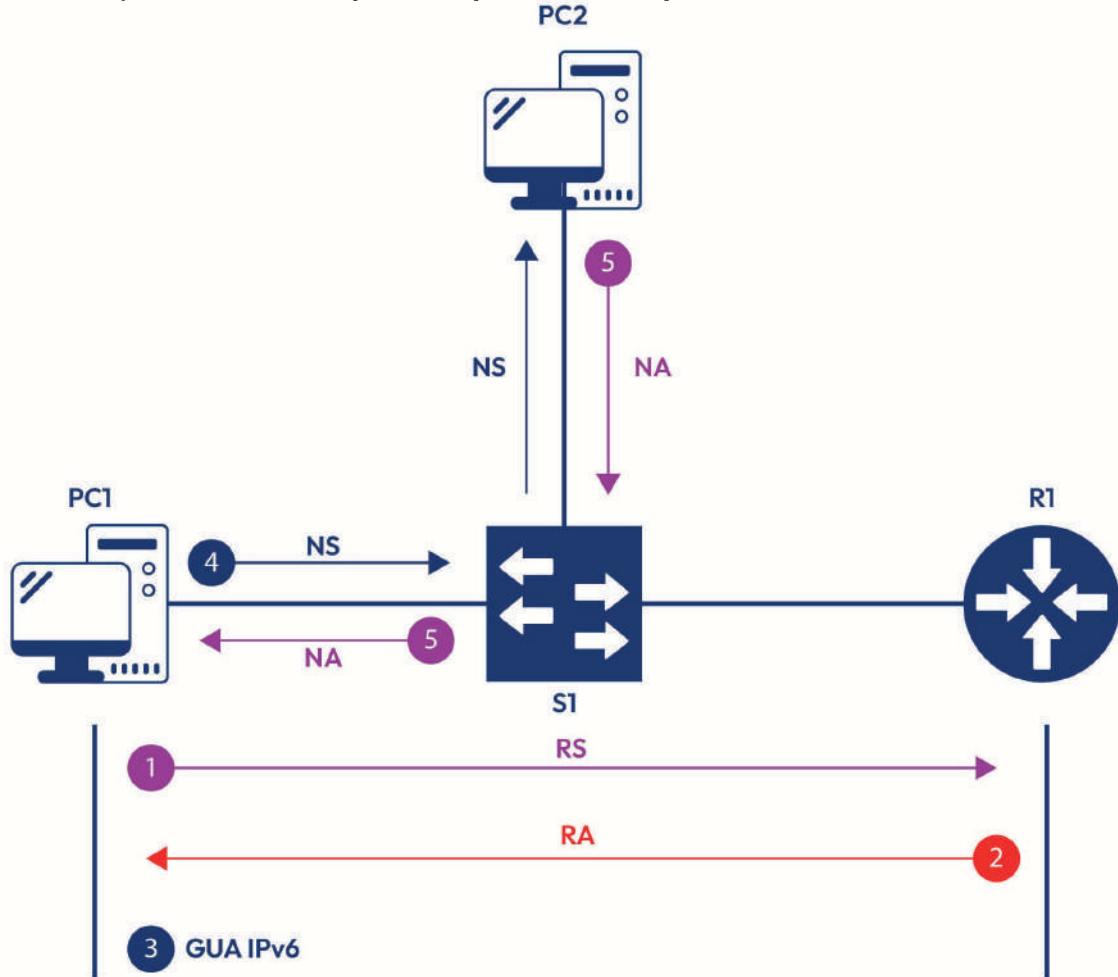
Le routeur envoie des messages **RA** chaque **200 secondes** à tous les nœuds IPv6 ou suite à la réception d'un message RS

SLAAC est le protocole qui permet aux dispositifs réseau de configurer automatiquement leur adresse IP en utilisant les informations d'annonce **Router advertisement** (RA) diffusées par les routeurs sur un réseau local.

DÉTECTION DES ADRESSES DUPLIQUÉES (DAD) :

Avec la méthode SLAAC, PC1 n'a aucune garantie que l'adresse n'est pas dupliquée. Alors, le processus **DAD** (Duplicate Address Detection) est lancé.

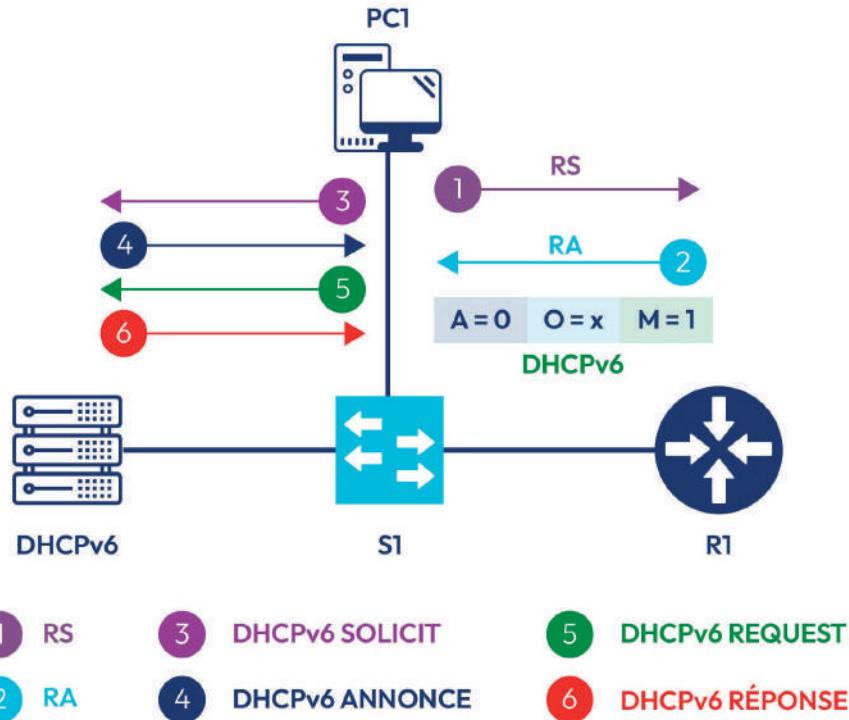
La détection des adresses dupliquées (DAD) est un processus utilisé dans le but de vérifier **si une adresse IP configurée sur un dispositif réseau est déjà utilisée par un autre dispositif** sur le même réseau.



- PC1 envoie un message de sollicitation du voisin **NS** (Neighbor Sollicitation) à l'adresse du nœud sollicité.
 - Si PC2 répond par un message d'annonce du voisin **NA** (Neighbor Advertisement), alors l'adresse n'est pas unique. → Le système génère un nouvel ID de l'interface.
 - Si aucun hôte ne répond avec le message **NA**, alors l'adresse est unique.

10.2.3. DHCP avec état

Avec la méthode DHCP avec état, les hôtes obtiennent toute la configuration à partir du serveur DHCP.

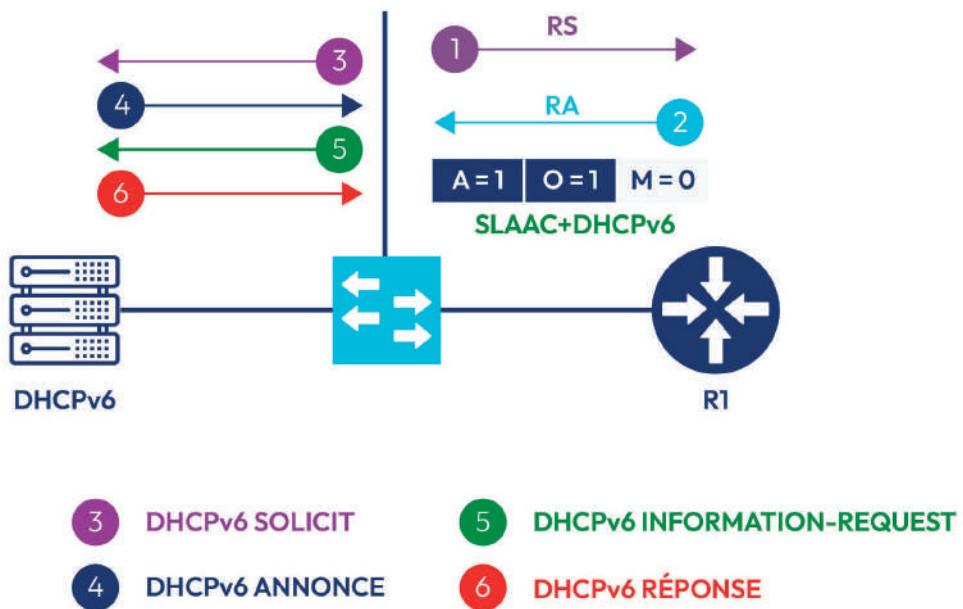


- ➊ PC1 envoie un message RS.
- ➋ PC reçoit une réponse RA lui indiquant qu'il doit contacter un serveur DHCP.
- ➌ PC1 envoie un message de sollicitation DHCP à l'adresse de multidiffusion attribué aux serveurs DHCP **FF02::1:2**.
- ➍ Le serveur DHCP répond par un message d'annonce indiquant qu'il est disponible.
- ➎ PC1 envoie une requête demandant tous les paramètres de configuration IPv6.
- ➏ Le serveur DHCP envoie une réponse contenant toute la configuration IPv6.

10.2.4. DHCP sans état (SLAAC et DHCPv6)

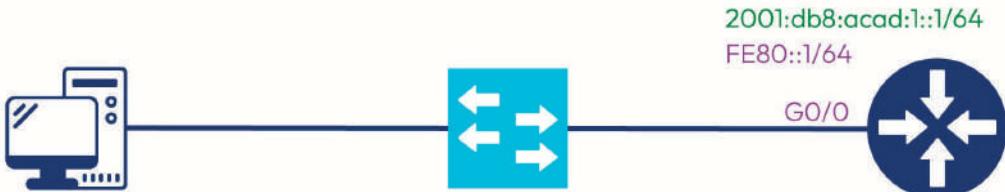
Pour la méthode DHCP sans état, l'hôte obtient la configuration IPv6 à partir du :

- ➊ **Routeur** : L'hôte obtient le **préfixe réseau** envoyé dans le **message RA** et génère l'ID de l'interface pour créer une **adresse IPv6**
- ➋ **Serveur DHCP** : paramètres de configuration supplémentaires (**Adresse DNS**, etc.)



10.2.5. Configuration du routeur :

CONFIGURATION SLAAC :



Configuration de l'interface du routeur G0/0 :

```
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ipv6 address 2001:0DB8:ACAD:1::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shutdown
```

Vérification de la configuration de l'interface G0/0 :

```
R1#show ipv6 interface G0/0
GigabitEthernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
Joined group address(es):
FF02::1
FF02::1:FF00:1
(Résultats Omis)
```

L'adresse FF02::1 est l'adresse de multidiffusion attribuée à tous les nœuds IPv6.

Activation du routage en monodiffusion IPv6 :

```
R1(config)#ipv6 unicast-routing
```

Vérification de l'activation SLAAC :

```
R1#show ipv6 interface G0/0
GigabitEthernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF00:1
```

L'adresse FF02::2 est l'adresse de multidiffusion attribuée aux routeurs IPv6.

SLAAC est activé par défaut après l'activation du routage en monodiffusion IPv6.

Si la configuration par défaut est modifiée, on peut y revenir à l'aide des commandes suivantes :

```
R1(config)#interface GigabitEthernet0/0
R1(config-if)#no ipv6 nd other-config-flag
R1(config-if)#no ipv6 nd managed-config-flag
```

Les deux commandes mettent les deux indicateurs O et M à zéro.

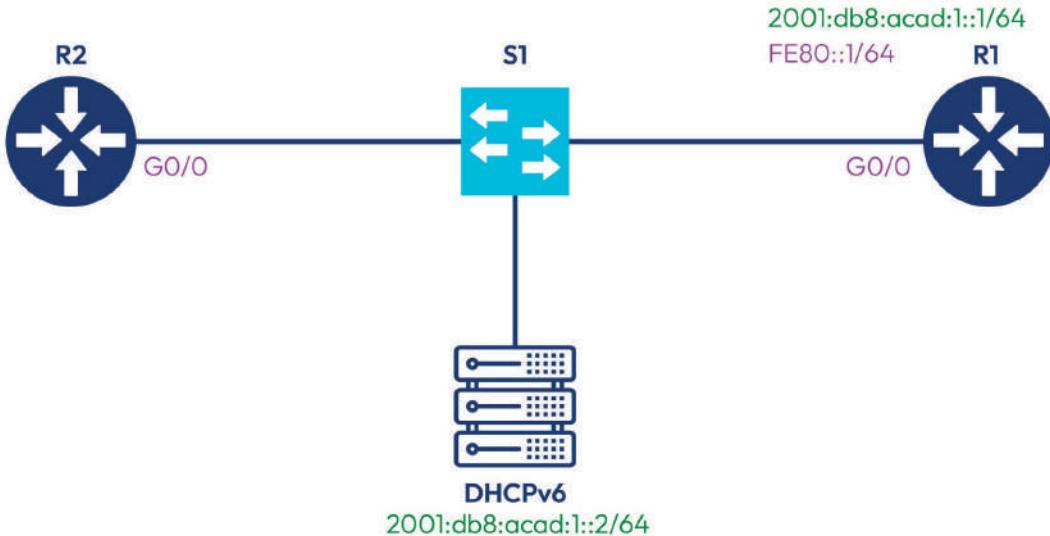
Vérification au niveau du PC1 :

```
C:\>ipconfig

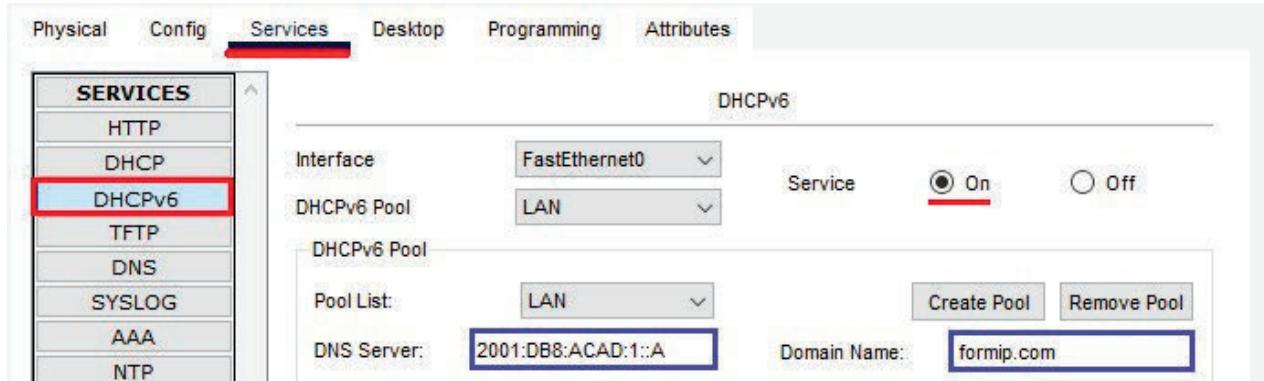
FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::260:3EFF:FE14:B029
IPv6 Address.....: 2001:DB8:ACAD:1:260:3EFF:FE14:B029
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: FE80::1
0.0.0.0
```

CONFIGURATION DHCP SANS ÉTAT :



Configuration du serveur DHCP :



Activation du DHCP sans état au niveau de l'interface G0/0 :

```
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ipv6 nd other-config-flag
R1(config-if)#no ipv6 nd managed-config-flag
```

- ⌚ La première commande met à 1 l'indicateur O
- ⌚ La deuxième commande met à 0 l'indicateur M

Configuration de l'autoconfiguration du routeur R2 :

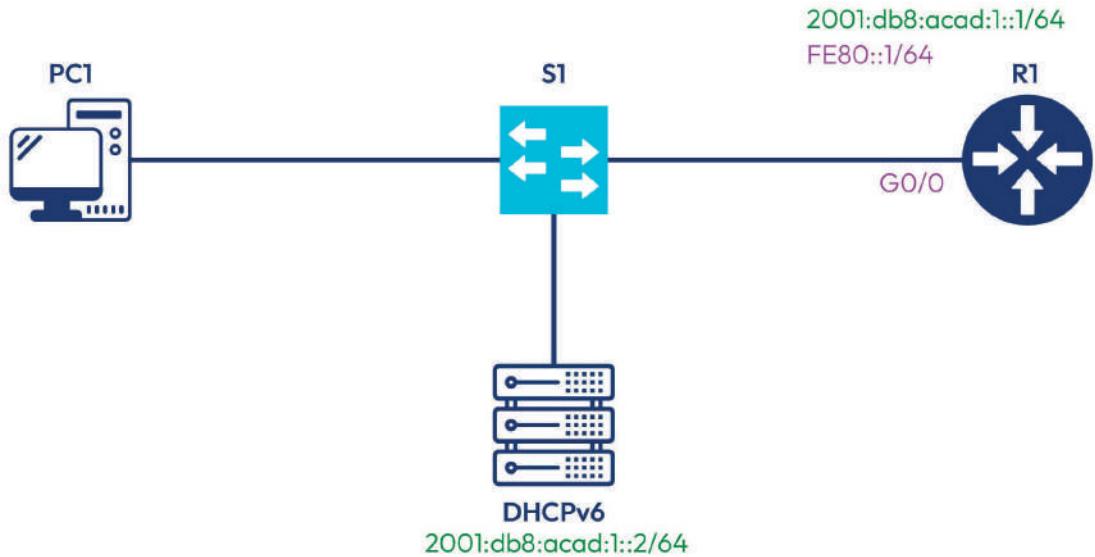
```
R2(config)#interface G0/0
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 address autoconfig
R2(config-if)#no shutdown
```

Vérification de la configuration de l'interface de R2 :

```
R2#show running-config | include ip name-server
ip name-server 2001:DB8:ACAD:1::A
R2#show ipv6 interface brief
GigabitEthernet0/0      [up/up]
  FE80::2E0:B0FF:FEB7:6E01
  2001:DB8:ACAD:1:2E0:B0FF:FEB7:6E01
(Résultats omis)
```

Pour les hôtes sur Packet Tracer, le DHCP sans état n'est pas disponible.

10.2.6. DHCP avec état :



Configuration du serveur DHCP :

Prefix	Prefix Length	Valid Lifetime	Preferred Lifetime
2001:DB8:ACAD:1::	64	2592000	604800

Activation du DHCP avec état au niveau de l'interface G0/0 :

```
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ipv6 nd managed-config-flag
```

Vérification de l'activation du DHCP avec état :

```
R1#show ipv6 interface G0/0
(Résultats omis)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use DHCP to obtain routable addresses.
```

Vérification de la configuration au niveau du PC1 :

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..: formip.com
Physical Address.....: 0060.3E14.B029
Link-local IPv6 Address.....: FE80::260:3EFF:FE14:B029
IPv6 Address.....: 2001:DB8:ACAD:1:AB77:47EB:F2F0:D6DC
(Résultats omis)
Default Gateway.....: FE80::202:4AFF:FE66:3413
(Résultats omis)
DNS Servers.....: 2001:DB8:ACAD:1::A
0.0.0.0
```

On peut configurer un routeur comme client DHCP avec état à l'aide des commandes suivantes :

```
R2(config)#interface G0/0
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 address dhcp
R2(config-if)#no shutdown
```

En résumé :

DHCPv6 avec état permet une gestion centralisée de l'adressage, mais nécessite un serveur DHCPv6 pour gérer les états.

DHCPv6 sans état permet une configuration réseau plus autonome, mais nécessite une gestion de l'adressage plus complexe.

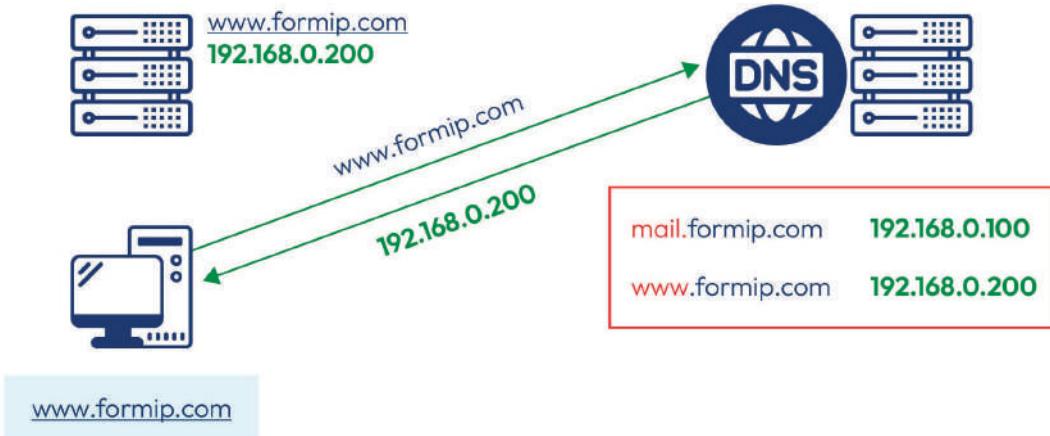
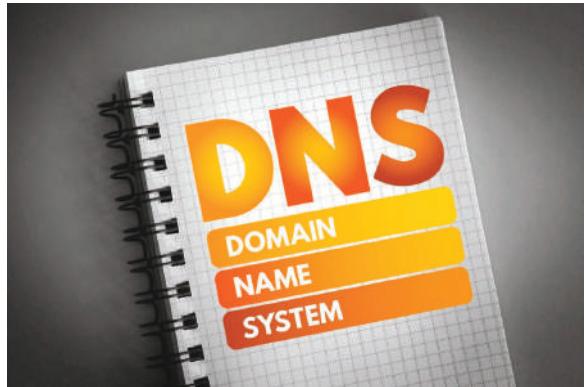
La choix dépend des besoins de la configuration réseau et des capacités des équipements.

10.3. Le service DNS

10.3.1. Définition :

Le protocole DNS (Domain Name System) permet de :

- ➊ Faire la résolution d'un nom d'hôte « **Hostname** » en adresse IP
- ➋ Faire la résolution d'une adresse IP en nom d'hôte
- ➌ Localiser des services réseau tels que les services d'annuaire Active Directory.

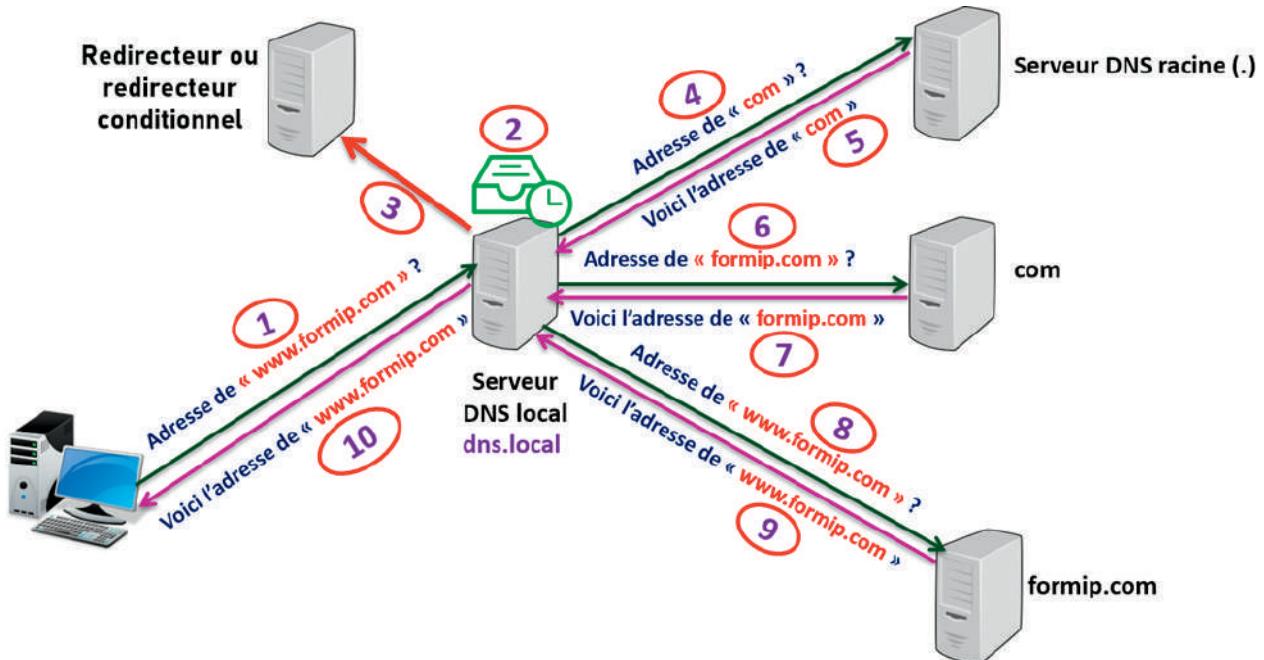


10.3.2. Types d'enregistrement DNS :

ENREGISTREMENT	DESCRIPTION
A	L'enregistrement principal qui résout un nom d'hôte en une adresse IP
CNAME	Un type d'enregistrement d'alias qui mappe un nom à un autre
MX	L'enregistrement MX est utilisé pour spécifier un serveur de messagerie électronique pour un domaine particulier

ENREGISTREMENT	DESCRIPTION
SRV	L'enregistrement SRV identifie un service qui est disponible dans le domaine.
NS	L'enregistrement NS identifie un serveur de noms pour un domaine.
SOA	L'enregistrement SOA identifie le serveur de noms principal pour une zone DNS, durée de vie TTL, etc.
PTR	L'enregistrement PTR est utilisé pour rechercher une adresse IP et la mapper à un nom de domaine

10.3.3. Étapes de résolution de noms d'hôtes :



10.3.4. Commandes utiles :

Affichage du cache DNS d'une machine Windows :

PC> **ipconfig /displaydns**

Suppression du cache DNS d'une machine Windows :

PC> **ipconfig /flushdns**

Lancement d'une résolution de noms d'hôtes manuellement :

PC> **nslookup**

```
C:\>nslookup
Serveur par défaut : [REDACTED]
Address: [REDACTED]

> www.formip.com
Serveur : [REDACTED]
Address : [REDACTED]

Réponse ne faisant pas autorité :
Nom : www.formip.com
Addresses: 2001:41d0:301::26
87.98.154.146
```

La commande affiche :

- ⌚ Le nom du serveur DNS
- ⌚ L'adresse du serveur DNS

Lorsqu'on saisit le nom d'hôte www.formip.com, le serveur DNS répond :

- ⌚ L'adresse IPv4, correspondant au nom d'hôte
- ⌚ L'adresse IPv6, si elle existe

Type de réponse : « Réponse ne faisant pas autorité » signifie que le serveur qui a donné la réponse n'est pas le serveur qui héberge l'enregistrement.

10.4. Le protocole SNMP

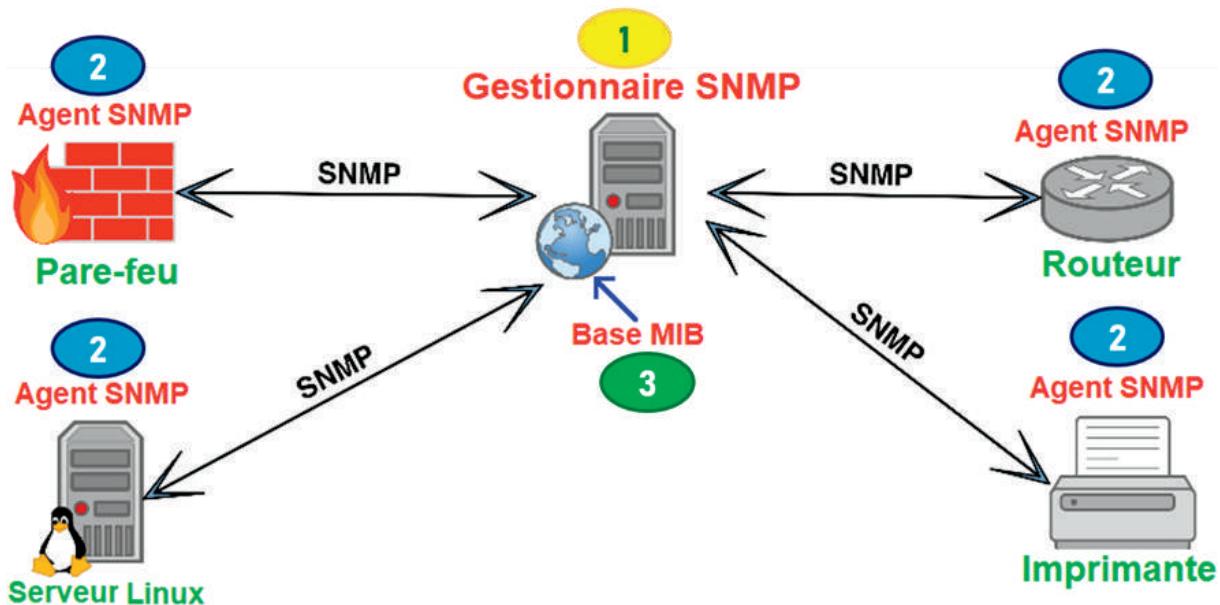
10.4.1. Définition :

Le protocole SNMP « Simple Network Management Protocol » est un protocole qui permet aux administrateurs de gérer des équipements réseau, tels que des serveurs, des stations de travail, des routeurs, des commutateurs et des appareils de sécurité sur un réseau IP.



Les composants SNMP :

- ➊ Gestionnaire SNMP : (Nagios, ...)
- ➋ Agents SNMP : Routeurs, commutateurs, ordinateurs, etc.
- ➌ La base de données MIB : elle contient toutes les variables à surveiller (Interfaces, nom des périphériques, protocoles de routage, etc.)



10.5. Les protocoles CDP et LLDP

Les protocoles CDP « Cisco Discovery Protocol » et LLDP « Link Layer Discovery Protocol » sont des protocoles de la couche 2 du modèle OSI et qui permettent la découverte des voisins directement connectés pour des raisons de diagnostic, de surveillance, de gestion et de configuration.

Affichage de la liste des voisins CDP :

R1#show cdp neighbors					
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone					
Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
Switch	Gig 0/1	141	S	2960	Fas 0/1
R2	Gig 0/0	141	R	C2900	Gig 0/0

Deux voisins CDP :

- ⌚ R2 : Routeur (R)
- ⌚ Switch : Commutateur (S)

Affichage de la liste des voisins LLDP :

R1#show lldp neighbors				
Capability codes:				
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other				
Device ID	Local Intf	Hold-time	Capability	Port ID
R2	Gig0/0	120	R	Gig0/0
Switch	Gig0/1	120	B	Fa0/1

Deux voisins LLDP :

- ⌚ R2 : Routeur (R)
- ⌚ Switch : Commutateur (B)

10.6. Le protocole NTP

NTP permet de synchroniser les horloges de plusieurs périphériques sur un réseau.



Vérification de la configuration NTP :

```
S1#show ntp status
Clock is synchronized, stratum 9, reference is 192.168.1.1
(Résultats omis)
```

10.7. La qualité de service QoS :

La QoS (Quality of Service, ou qualité de service en français) est un ensemble de techniques utilisées dans les réseaux informatiques afin de contrôler et gérer la façon dont les différents types de trafic réseau sont acheminés et priorisés.

En utilisant la QoS, il est ainsi possible de garantir un niveau de performance minimal pour certains types de trafic, tels que la voix sur IP ou la diffusion en direct de vidéos, afin de s'assurer que ces services fonctionnent de manière fiable et fluide, même lorsque le réseau est encombré.

La QoS peut être mise en œuvre à différents niveaux dans un réseau, tels que sur les routeurs et les commutateurs ou bien sur les hôtes finaux, tels que les ordinateurs et les téléphones.



10.7.1. Concepts de base de la qualité de service :

Il y a quatre critères à prendre en considération lors de l'implémentation de la qualité de service :

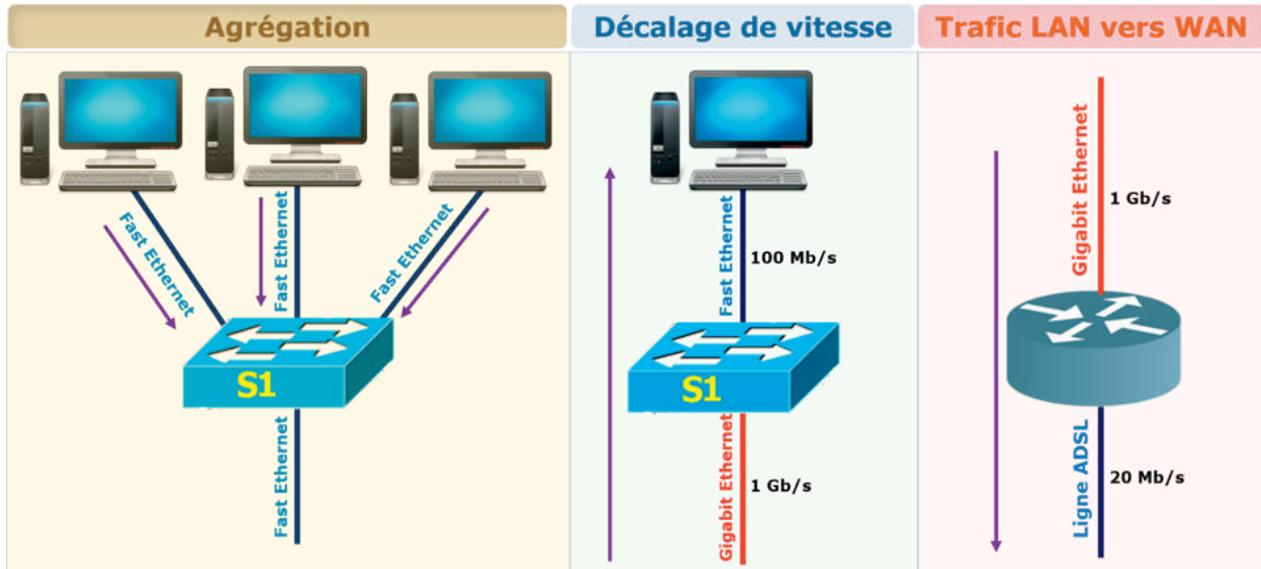
- ➊ La bande passante,
- ➋ la latence,
- ➌ la gigue
- ➍ et le pourcentage de perte toléré.

LA CONGESTION OU L'ENCOMBREMENT :

La congestion ou l'encombrement est un état provoqué quand le volume du trafic reçu est supérieur au volume pouvant être pris en charge par une interface.

La qualité de service est implémentée uniquement en cas de congestion.

Les points de congestion :



En cas de congestion, si aucun mécanisme de qualité de service n'est implémenté, les paquets seront perdus.

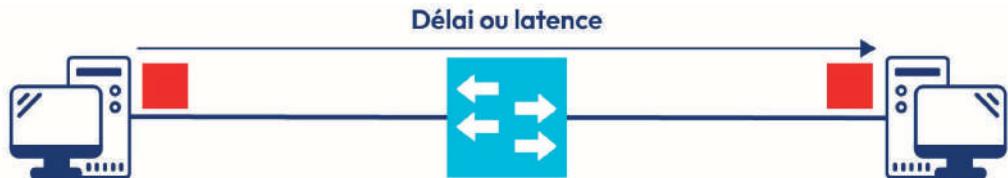
LA BANDE PASSANTE OU LE DÉBIT :

La bande passante est le nombre de bits pouvant être transmis en une seconde et elle est mesurée en Bit par seconde (Bit/s)

INTERFACE	BANDE PASSANTE OU DÉBIT
Ethernet	10 Mbps
Fast Ethernet	100 Mbps
Gigabit Ethernet	1 Gb/s

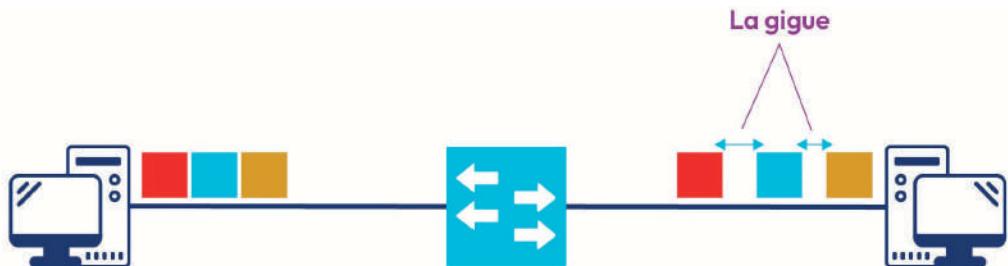
LE DÉLAI OU LA LATENCE :

Le délai ou la latence désigne le temps nécessaire à un paquet pour passer de la source à la destination.



LA GIGUE :

La gigue est la variation de délai entre les paquets reçus



10.7.2. Les caractéristiques du trafic réseau :

Données	Voix	Vidéo
<p>Insensitive aux pertes Insensitive aux retards Retransmission TCP</p>	<p>Latence ≤ 150ms Gigue ≤ 30ms Perte ≤ 1% Bande passante (30-128Kbit/s)</p>	<p>Latence ≤ 200-400 ms Gigue ≤ 30-50 ms Perte ≤ 0.1 - 1% Bande passante (384kbps-20 Mbps)</p>

La qualité de l'expérience QoE est importante à prendre en considération avec le trafic de données.

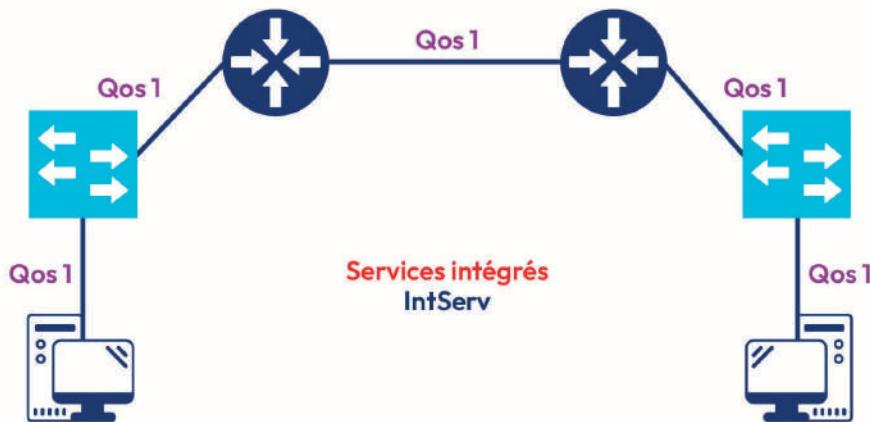
Si les données sont essentielles et proviennent d'une application interactive, on cherche un délai de réponse de 1 à 2 secondes.

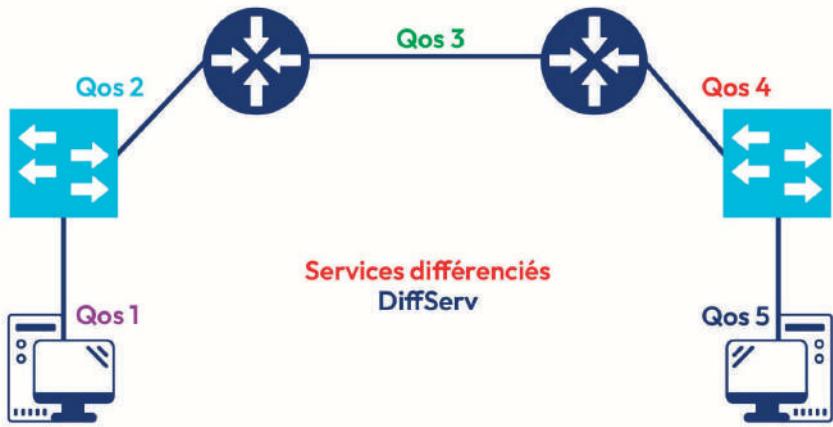
10.7.3. Modèles de qualité de service :

Il existe 3 modèles de qualité de service :

- ➲ Remise au mieux (Best Effort)
- ➲ Services intégrés (IntServ)
- ➲ Services différenciés (DiffServ)

	BEST EFFORT	INTSERV	DIFFSERV
QOS	Pas de qualité de service	QoS bout en bout	QoS saut par saut
GARANTIE DE LIVRAISON	Non	Oui	Non
ÉVOLUTIVITÉ	Le plus évolutif	Moins évolutif	QoS saut par saut
FLEXIBILITÉ	Pas de flexibilité	Pas de flexibilité	Plus flexible
PERFORMANCES	Pas de ressources	Plus de ressources	Moins de ressources





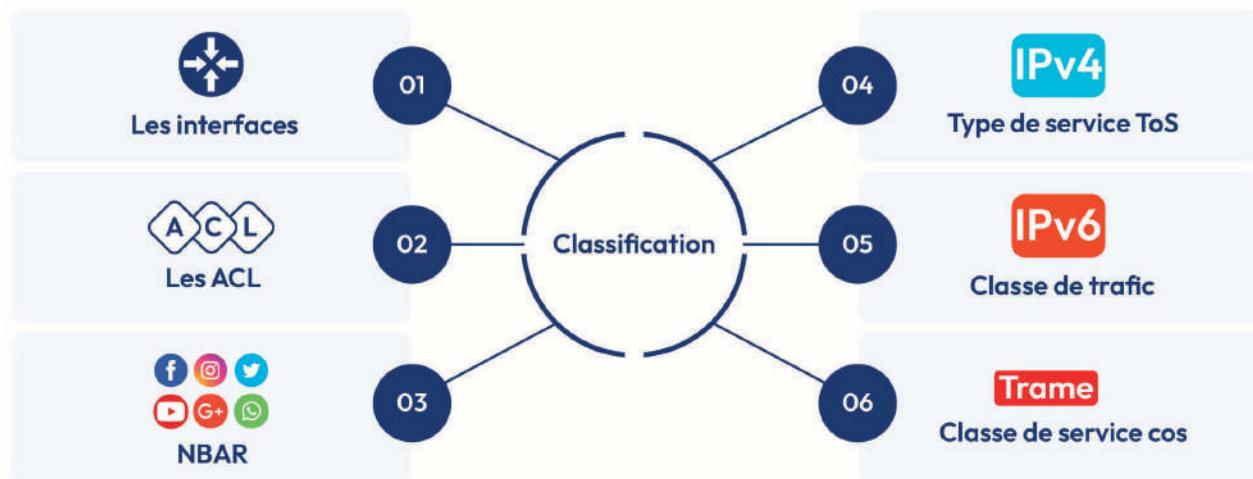
10.7.4.Outils de la qualité de service :

CLASSIFICATION ET DE MARQUAGE :

La classification :

La classification est l'opération qui consiste à examiner les paquets pour pouvoir prendre des décisions en termes de la qualité de service QoS.

Critères de classification



Le marquage :

Le marquage est l'opération qui consiste à modifier certains champs des paquets ou des trames pour les prioriser par rapport aux autres.

Marquage	
Couche 2	IPv4 Type de service Tos
	IPv6 Classe de trafic
Couche 3	Trame Classe de service cos

Le marquage d'un paquet IPv4 :

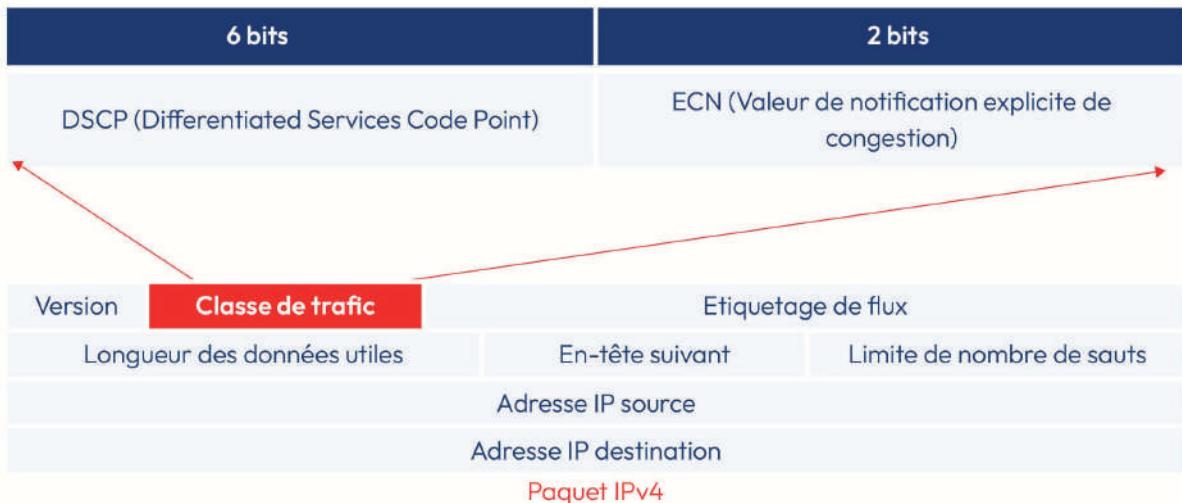
6 bits		2 bits
DSCP (Differentiated Services Code Point)		ECN (Valeur de notification explicite de congestion)
Version	Longueur d'entête	Type de service ToS (Service différenciés)
		Longueur totale
Identification	Indicateurs	Décalage du fragment
TTL	Protocole	Somme de contrôle de l'entête
	Adresse IP source	
	Adresse IP destination	
Options		Remplissage

Paquet IPv4

Le champ **DSCP** est utilisé afin de définir les priorités aux différentes classes de trafic.

Le champ **ECN** est utilisé pour empêcher l'abandon des paquets pendant les périodes d'encombrement (Il marque les paquets au lieu de les abandonner).

Le marquage d'un paquet IPv6 :



Le champ DSCP est de 8 bits → 64 classes de services possibles

Les différentes valeurs possibles de DSCP :

0=000000	46=101110	XXXYY0	XXX000
Remise au mieux	Expédition rapide (Expedited Forwarding)	Expédition assurée (Assured Forwarding)	Sélecteur de classe (Class selector)



Données standards

Données à priorité élevée

Plus de détails pour AF (Assured Forwarding) :

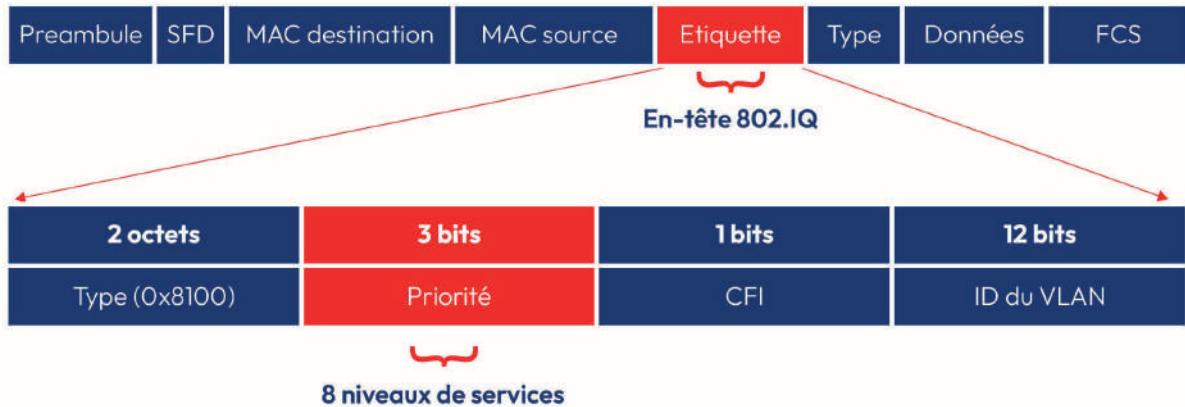
0=000000	46 = 101110	XXXYY0	XXX000
Remise au mieux	Expédition rapide (Expedited Forwarding)	Expédition assurée (Assured Forwarding)	Sélecteur de classe (Class Selector)
La probabilité d'abandon du paquet augmente →			
	Probabilité d'abandon faible	Probabilité d'abandon moyenne	Probabilité d'abandon élevée
Classe 4	AF41 = 100010	AF42 = 100100	AF43 = 100110
Classe 3	AF31 = 011010	AF32 = 011100	AF33 = 011110
Classe 2	AF21 = 010010	AF22 = 010100	AF23 = 010110
Classe 1	AF11 = 001010	AF12 = 001100	AF13 = 001110

Plus de détails pour CS (Class Selector)

Valeur DSCP	Valeur CS
CS0	000000 = 0
CS1	000000 = 8
CS2	000000 = 16
CS3	000000 = 24
CS4	000000 = 36
CS5	000000 = 40
CS6	000000 = 48
CS7	000000 = 56

← **Données standards**

Le marquage d'une trame 802.1Q :

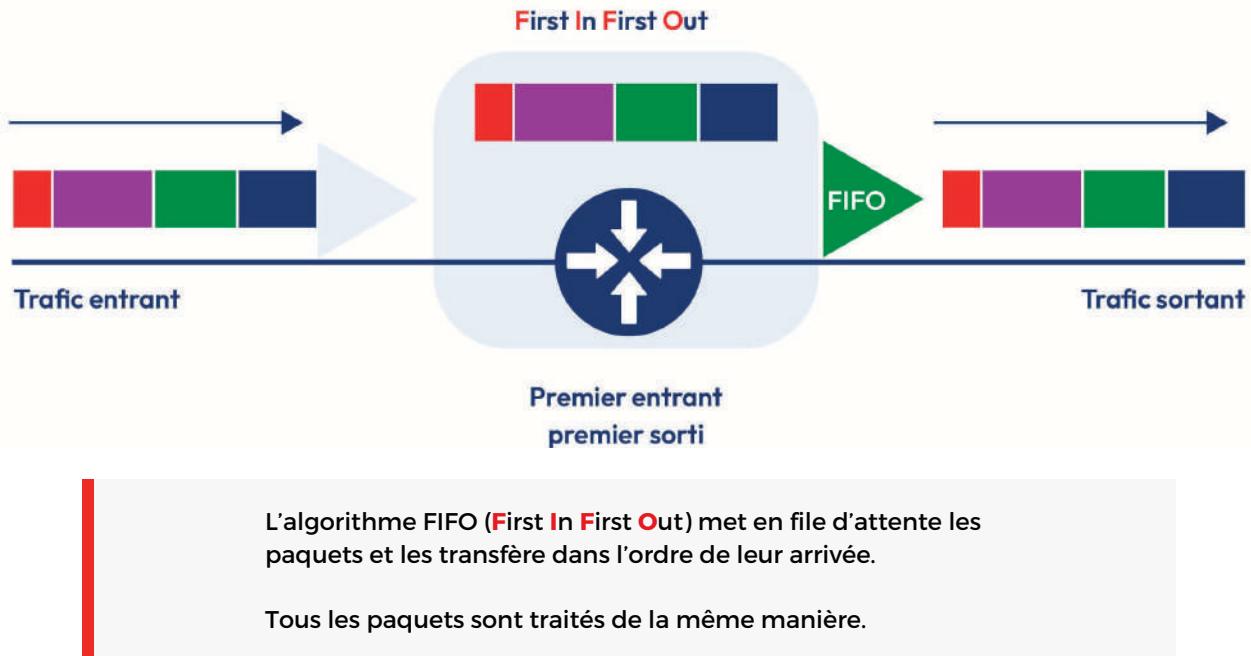


Les différentes valeurs CoS et leurs significations :

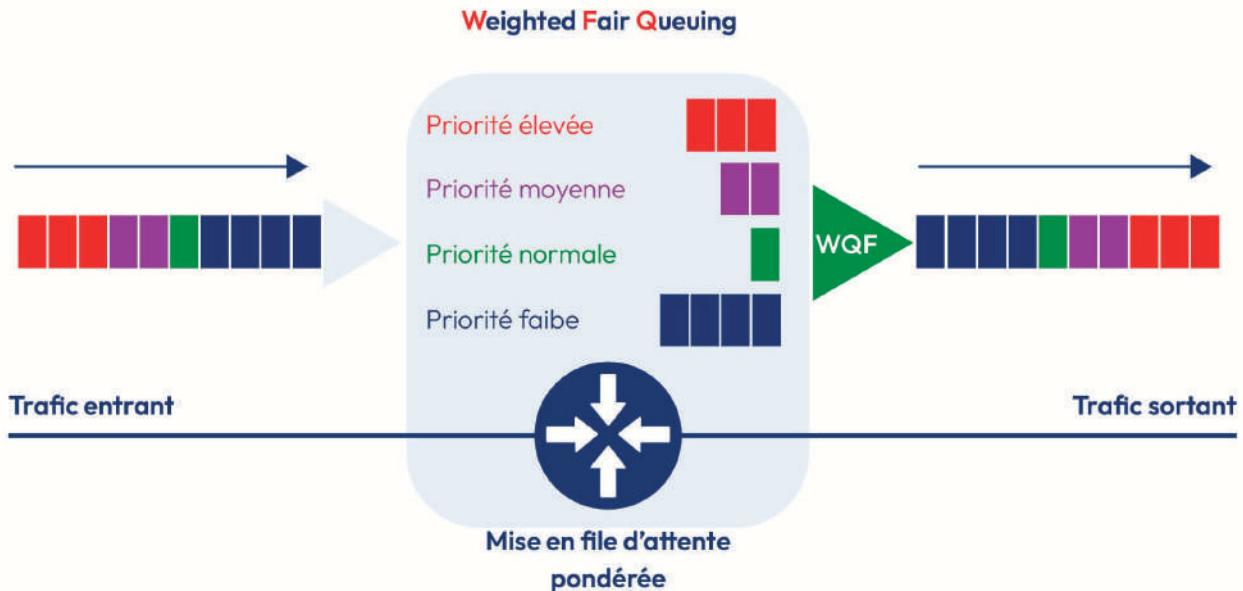
VALEUR COS	VALEUR COS BINAIRE	DESCRIPTION
0	000	Données de Remise au mieux
1	001	Données de priorité moyenne
2	010	Données de priorité forte
3	011	Signalisation d'appels
4	100	Vidéoconférence
5	101	Support voix (trafic voix)
6	110	Réservé
7	111	Réservé

MISE EN FILE D'ATTENTE

Le premier entrant est le premier sorti :



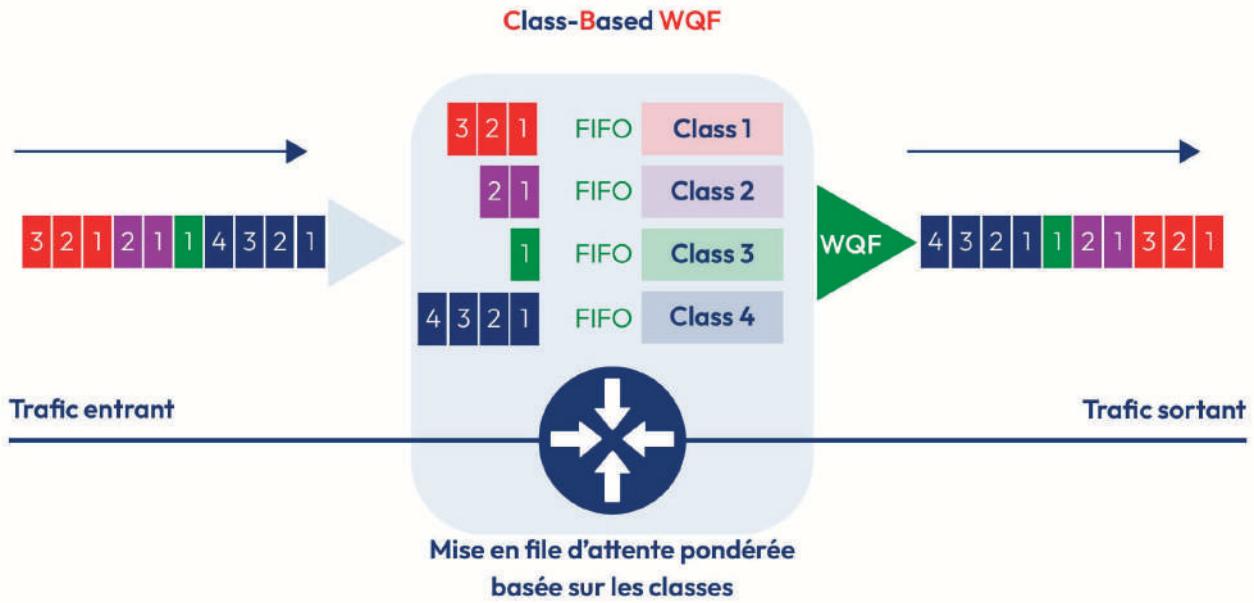
Mise en file d'attente pondérée



WFQ permet de classer le trafic en différents flux selon l'adressage des adresses IP source et de destination, les adresses MAC, les numéros de port, le protocole, et la valeur du type de service (ToS).

La méthode WFQ n'est pas prise en charge en cas de tunnelling et de chiffrement.

Mise en file d'attente pondérée basée sur les classes

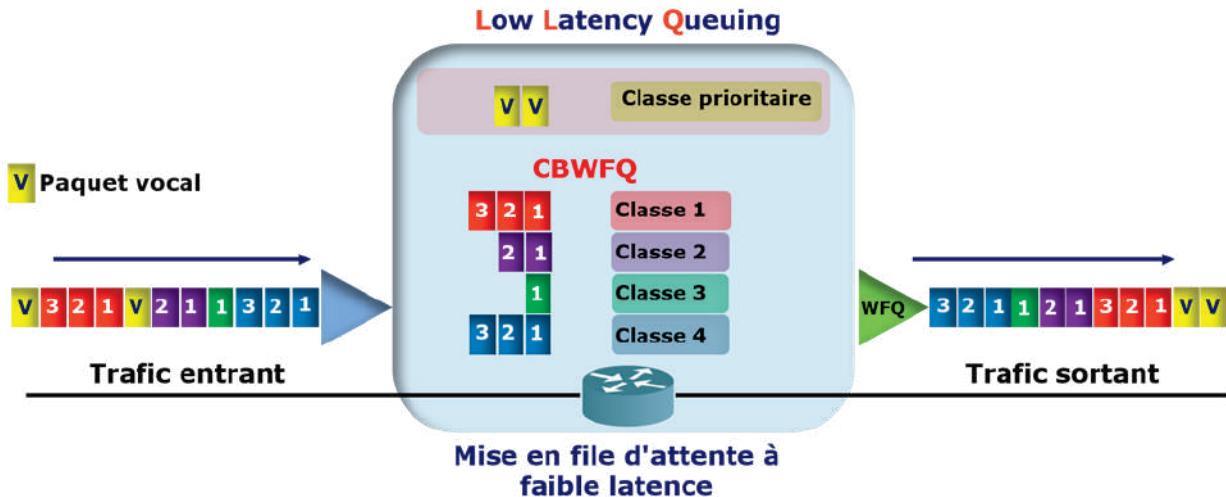


Les classes de trafic sont définies en fonction de critères de correspondance incluant les protocoles, les listes de contrôle d'accès (ACL) et les interfaces d'entrée.

Une file d'attente FIFO est réservée à chaque classe et le trafic appartenant à une classe est dirigé dans la file d'attente correspondant à cette classe.

Une classe peut être attribuée à des caractéristiques telles que la bande passante, le poids et la limite maximale de paquets.

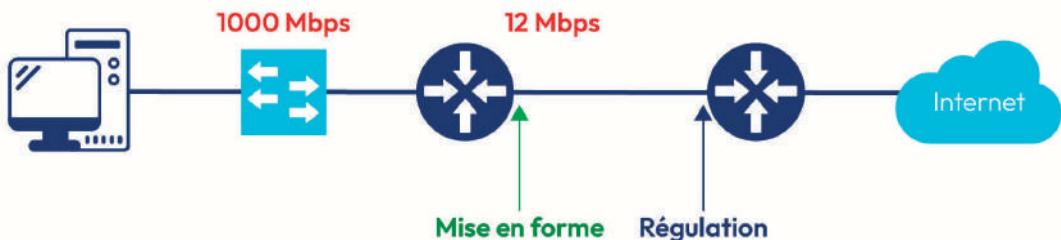
Mise en file d'attente à faible latence



La priorité stricte permet aux paquets soumis à des contraintes temporelles, par exemple la voix, d'être envoyées avant les paquets présents dans d'autres files d'attente

RÉGULATION ET MISE EN FORME :

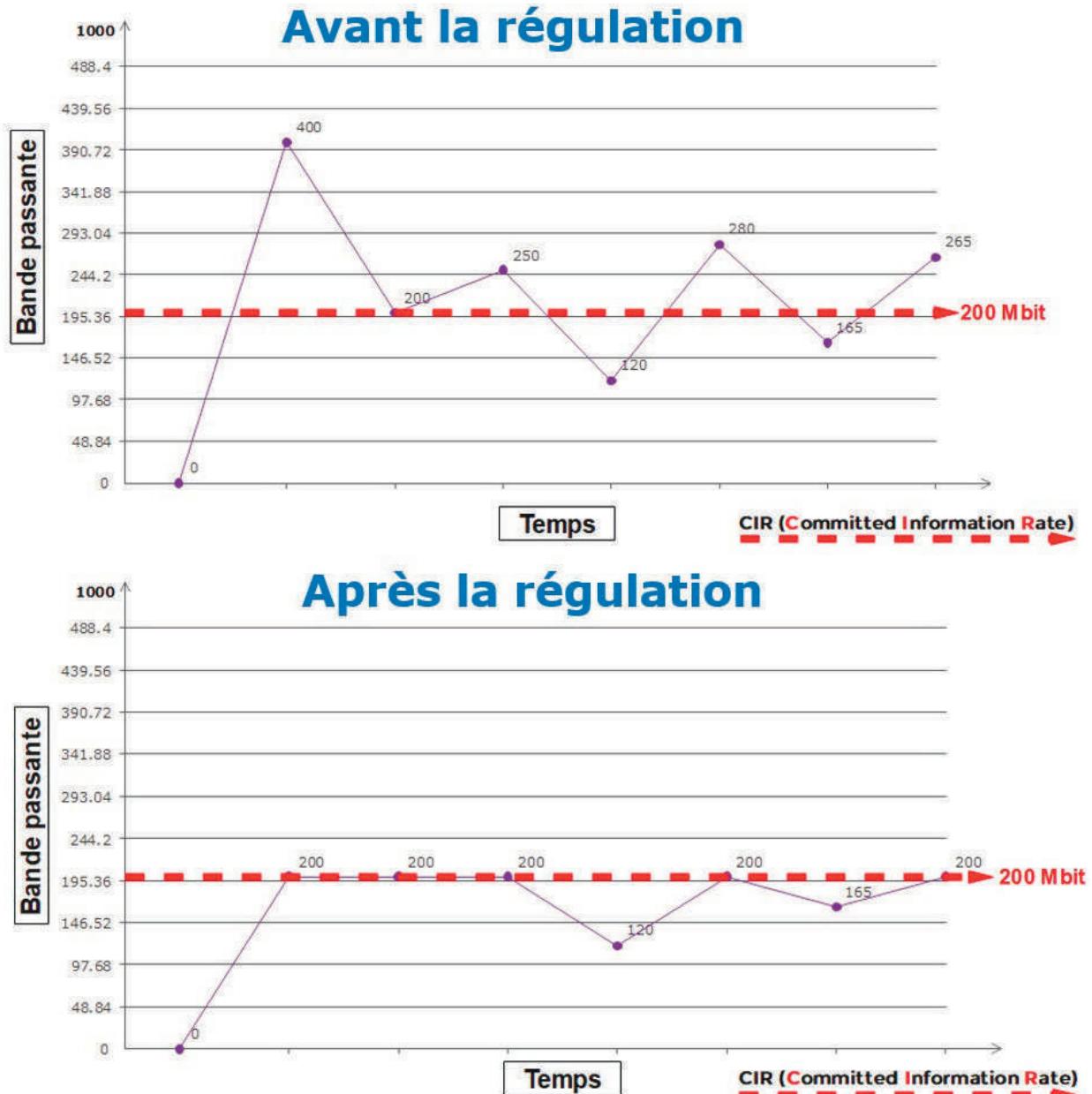
La régulation et la mise en forme sont deux outils QoS permettant de limiter le débit.



La régulation est utilisée généralement au niveau du fournisseur d'accès Internet

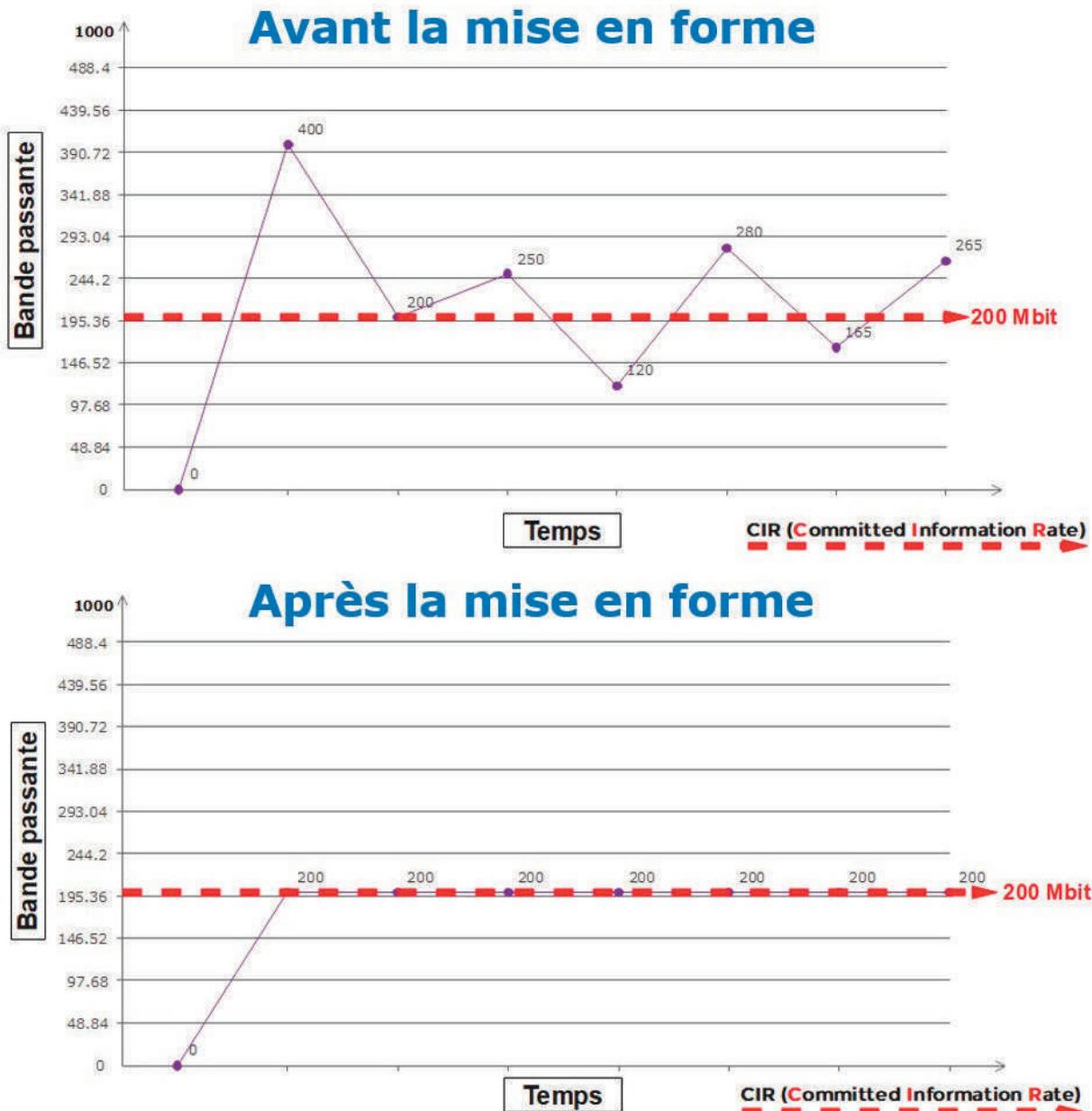
La mise en forme est utilisée au niveau de l'abonné aux services Internet

Principe de la régulation :



Le fournisseur d'accès Internet limite le débit en rejetant le trafic dépassant le débit garanti.

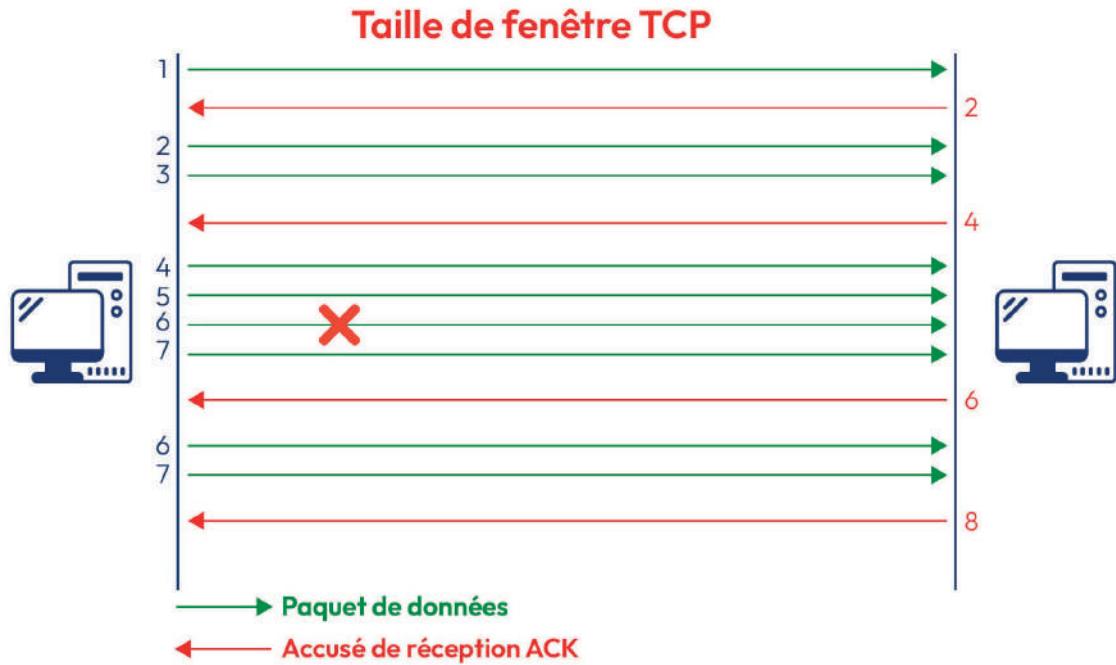
Principe de la mise en forme :



La mise en forme limite le trafic en le mettant dans des files d'attente pour ne pas dépasser le débit garanti.

PRÉVENTION DE LA CONGESTION : WRED ET TAILLE DE FENÊTRE TCP

La taille de fenêtre est le champ qui indique le nombre de paquets TCP à recevoir avant d'envoyer un accusé de réception.



Si aucun paquet TCP n'est perdu, la taille de fenêtre augmente en double.

Une fois qu'un paquet est perdu, la taille de fenêtre diminue de moitié et le paquet TCP est renvoyé de nouveau par l'émetteur ➔ En fait, ce processus permet d'éviter les congestions.

WRED permet de réguler le trafic de données TCP en utilisant efficacement la bande passante avant que des dépassements de file d'attente n'entraînent des abandons de paquets.

WRED est une méthode permettant d'éviter les engorgements en jetant aléatoirement les paquets lorsque la file d'attente atteint un certain niveau de congestion.

Il utilise également des poids pour prioriser certains types de trafic sur d'autres.