

# **02 Le protocole NAT**

## **Network Address Translation**

Module 146

Reprise du Module 129\_05\_01\_NAT.ppt

# Chapitres :

1. Qu'est-ce que le NAT?
2. Rappel important
3. Les types principaux de NAT:
  1. NAT statique
  2. NAT dynamique
  3. NAT-PAT

# **Qu'est-ce que le NAT?**

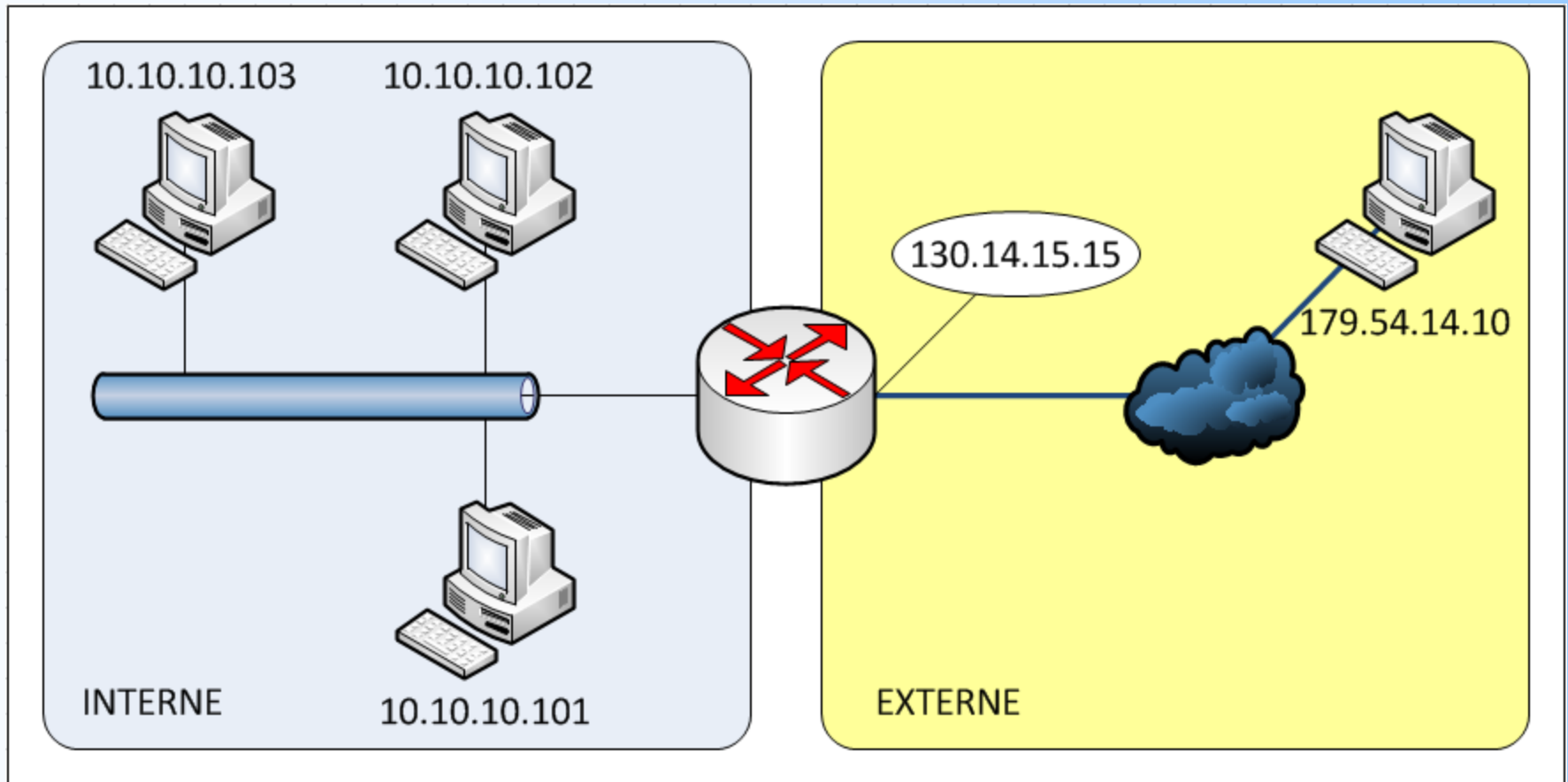
## **Qu'est-ce que le NAT? Network Address Translation**

- Translation d'Adresse Réseau
- L'objectif du NAT est de changer une adresse IP par une autre

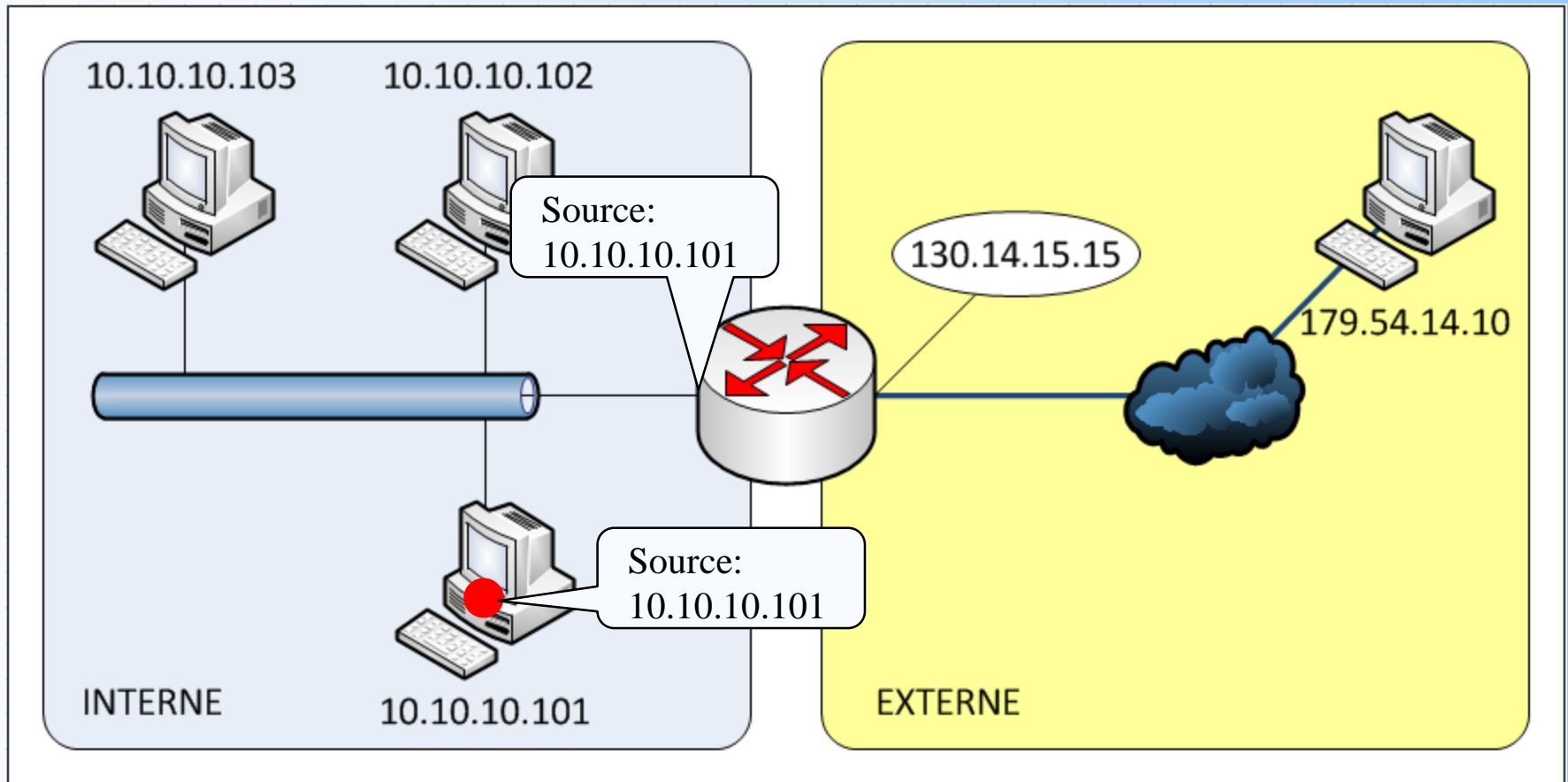
## **Pour quelle raison changer une adresse IP?**

- ☐ Les adresses privées ne sont pas routables sur internet
- ☐ En IPv4: pour pallier au manque d'adresse IP
- ☐ NAT est utilisé pour traduire les IP privées (de classe A/B/C) en une IP publique connue par le FAI
- ☐ NAT est aussi utilisé pour des questions de sécurité (pas d'adresse interne qui est connue à l'extérieur)

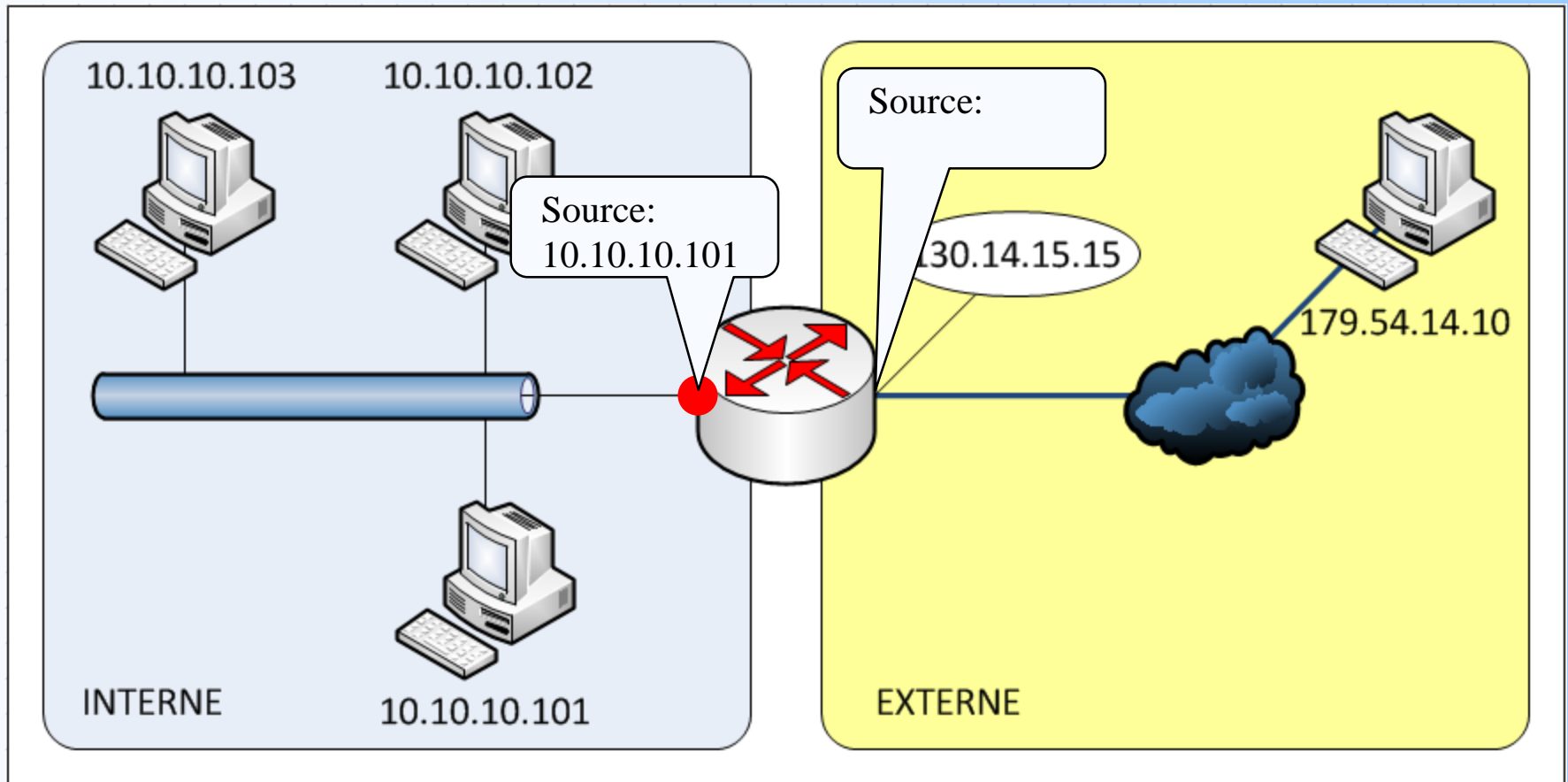
# Qu'est-ce que le NAT? - Illustration



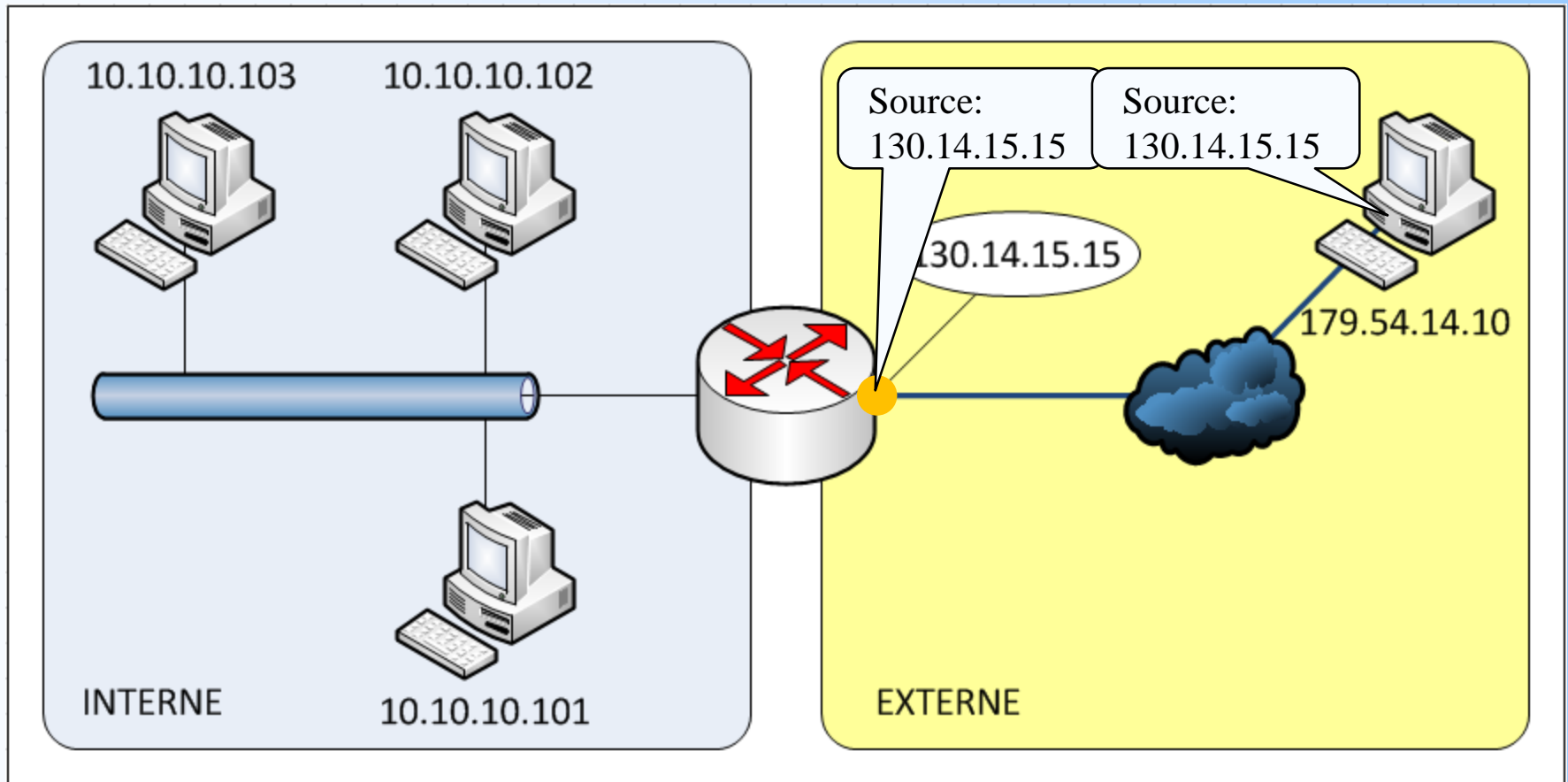
# Qu'est-ce que le NAT? - Illustration



# Qu'est-ce que le NAT? - Illustration



# Qu'est-ce que le NAT? - Illustration



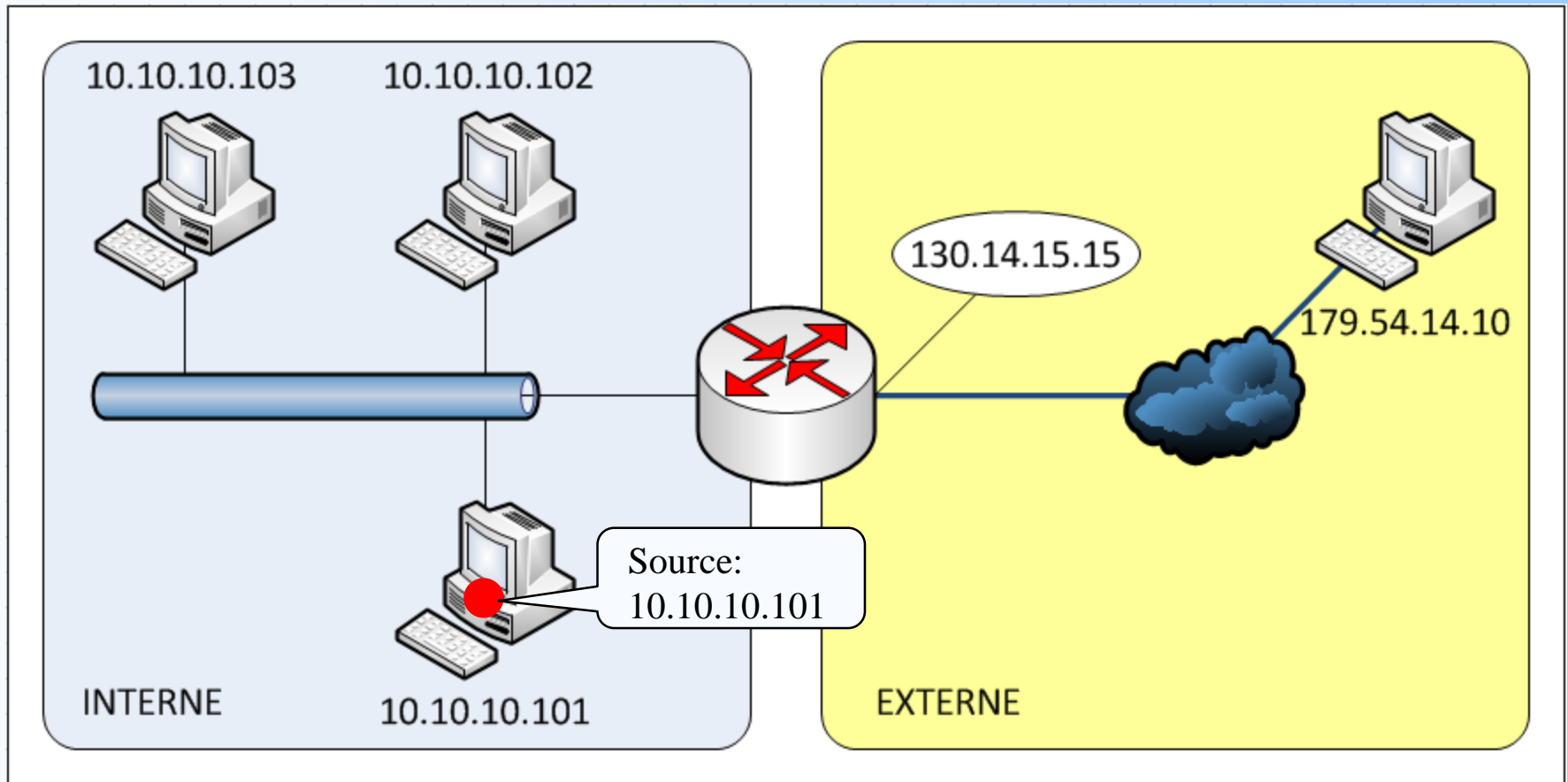
# Qu'est-ce que le NAT?

**OK !! Mais 2 hôtes internes peuvent-ils utiliser la même IP publique ?**

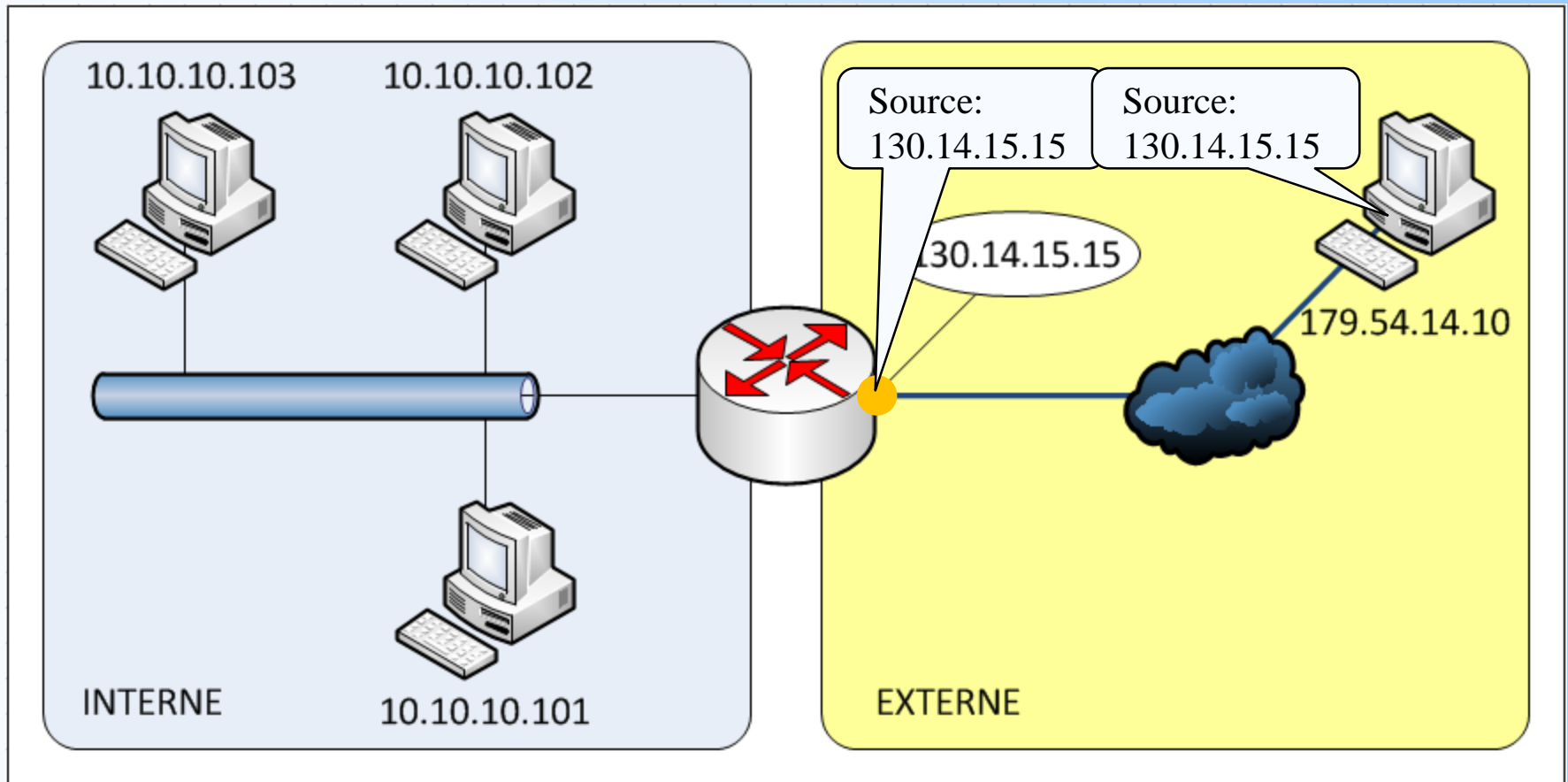
- Lors de la translation au niveau du routeur, le problème ne se pose pas à l'émission: en effet il est capable de traduire plusieurs IP locales.
- Le problème se pose au retour du paquet: si plusieurs IP locales ont été traduites avec la même IP publique, comment le routeur fait-il pour retrouver le bon hôte à qui faire suivre la réponse ?  
Il doit être capable de retrouver le PC émetteur.



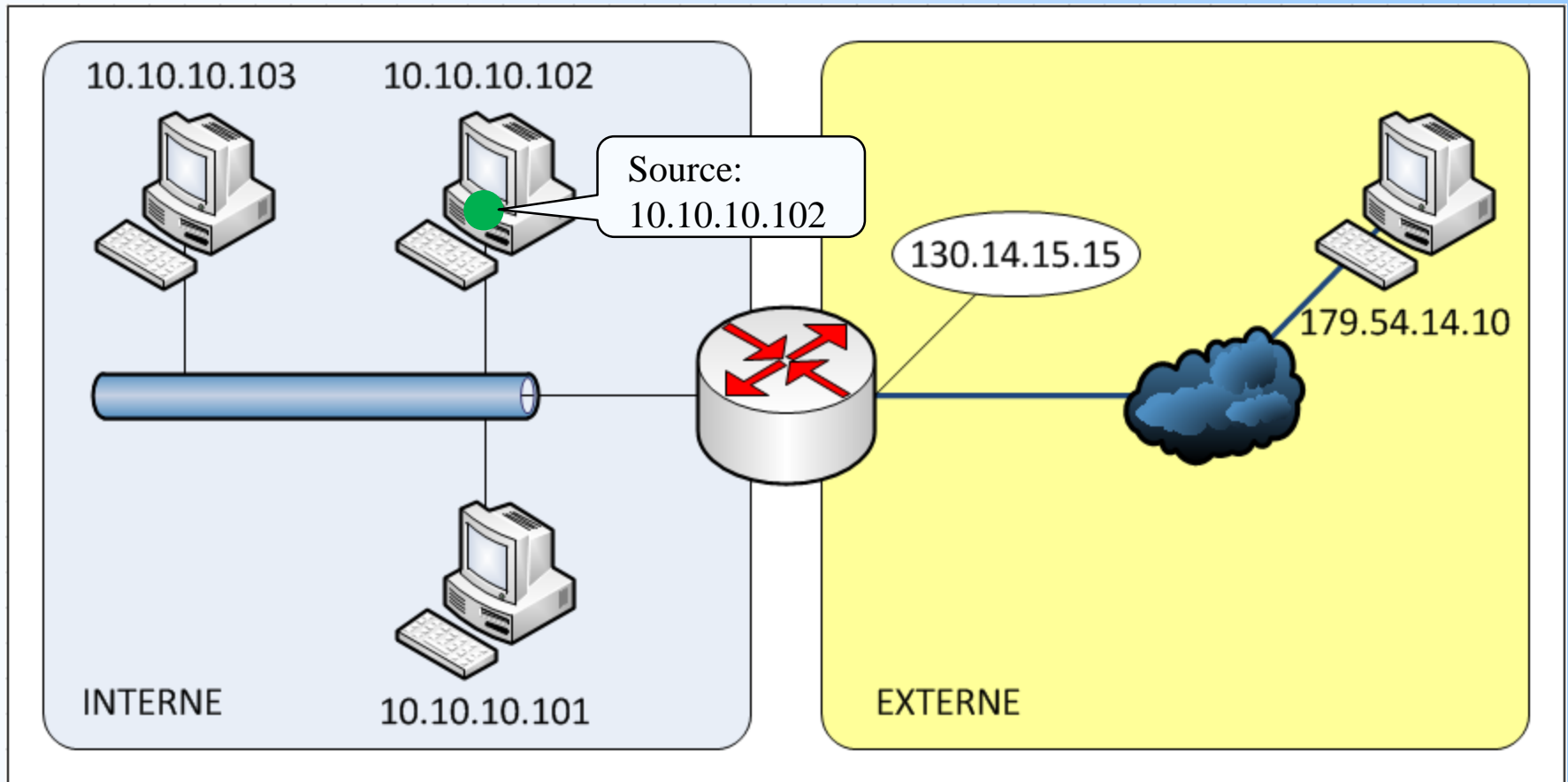
# Qu'est-ce que le NAT? - Illustration



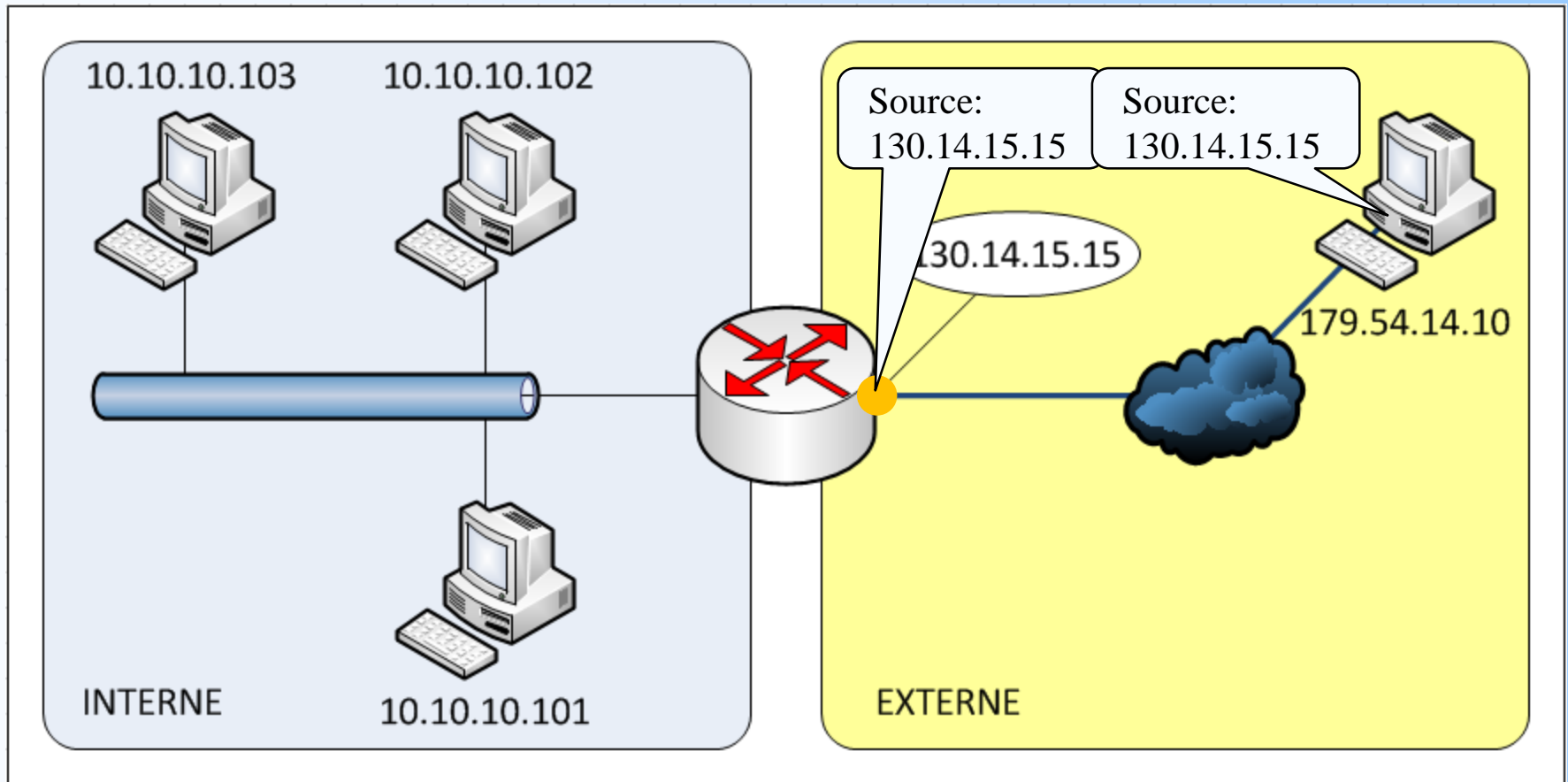
# Qu'est-ce que le NAT? - Illustration



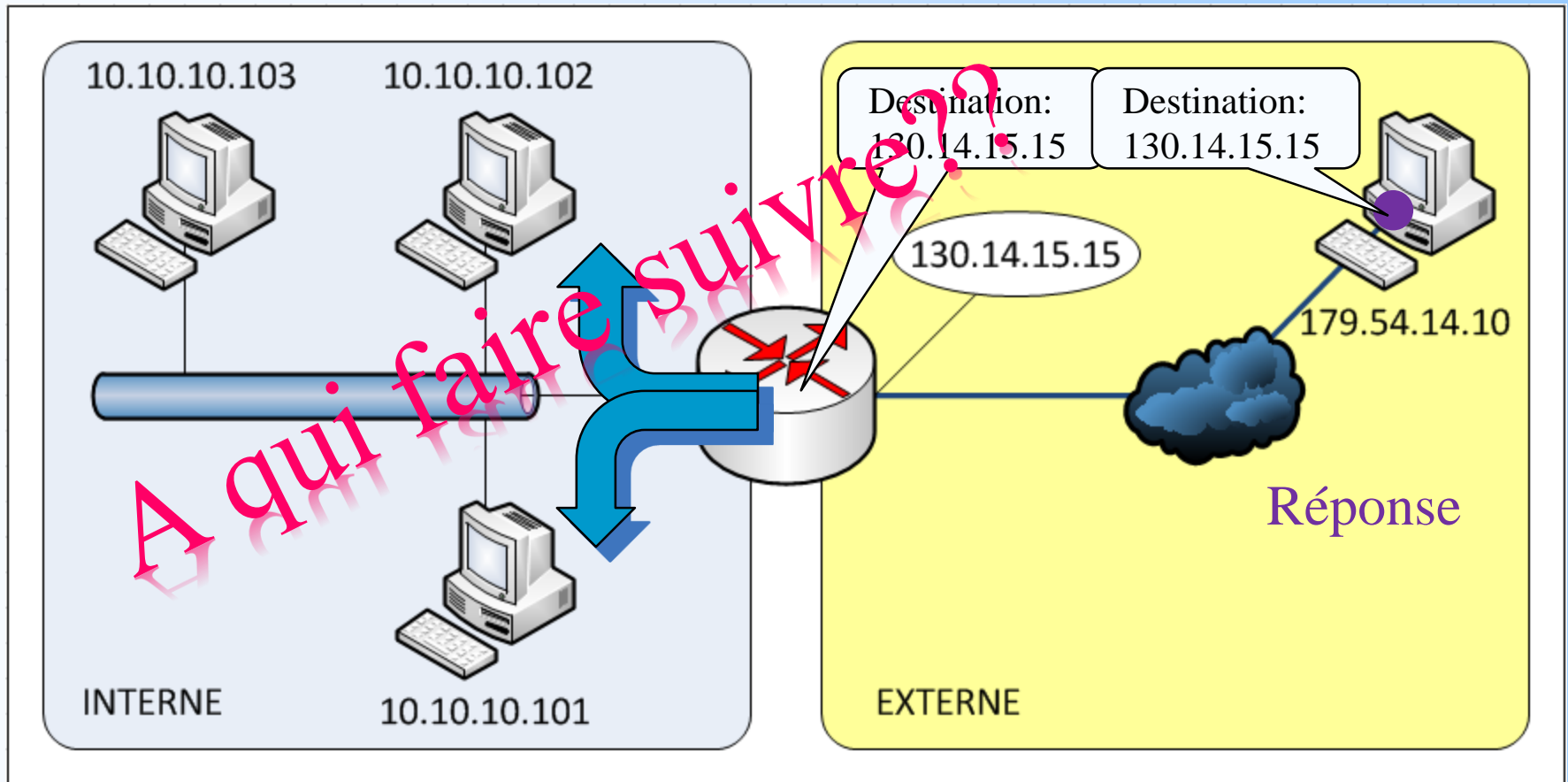
# Qu'est-ce que le NAT? - Illustration



# Qu'est-ce que le NAT? - Illustration



# Qu'est-ce que le NAT? - Illustration



# Rappel important

socket = ????????????

# Rappel important

socket = adresse + port

- On peut jouer sur l'adresse et/ou sur le port pour créer des sockets différents
- Le routeur mémorise à quel hôte interne est associé un socket

# **Les types principaux de NAT:**

1. NAT statique
2. NAT dynamique
3. NAT-PAT (Port Address Translation)



# NAT statique

## Comment ça marche?

- on associe 1 adresse interne avec 1 adresse externe

## Avantages?

- on ne touche pas au port
- on peut joindre la machine depuis l'extérieur

## Inconvénient?

- il faut autant d'adresses externes que de machines qui doivent « sortir » :
- impossible dès que l'on dépasse quelques machines

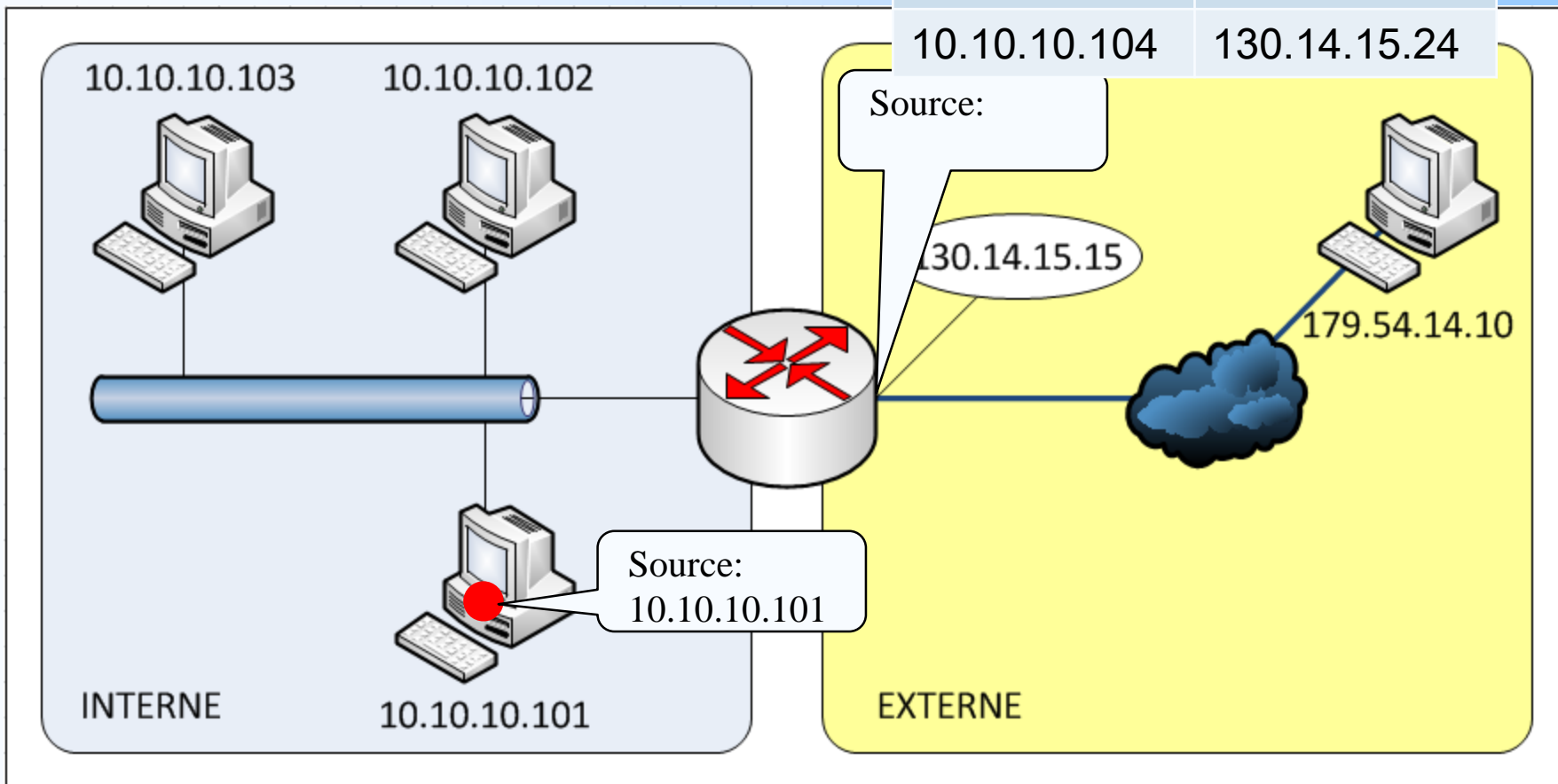
## Utilisation?

- technique encore utilisée pour certains serveurs web

Autre nom? avec certains pare-feu: MIP - Mapped IP

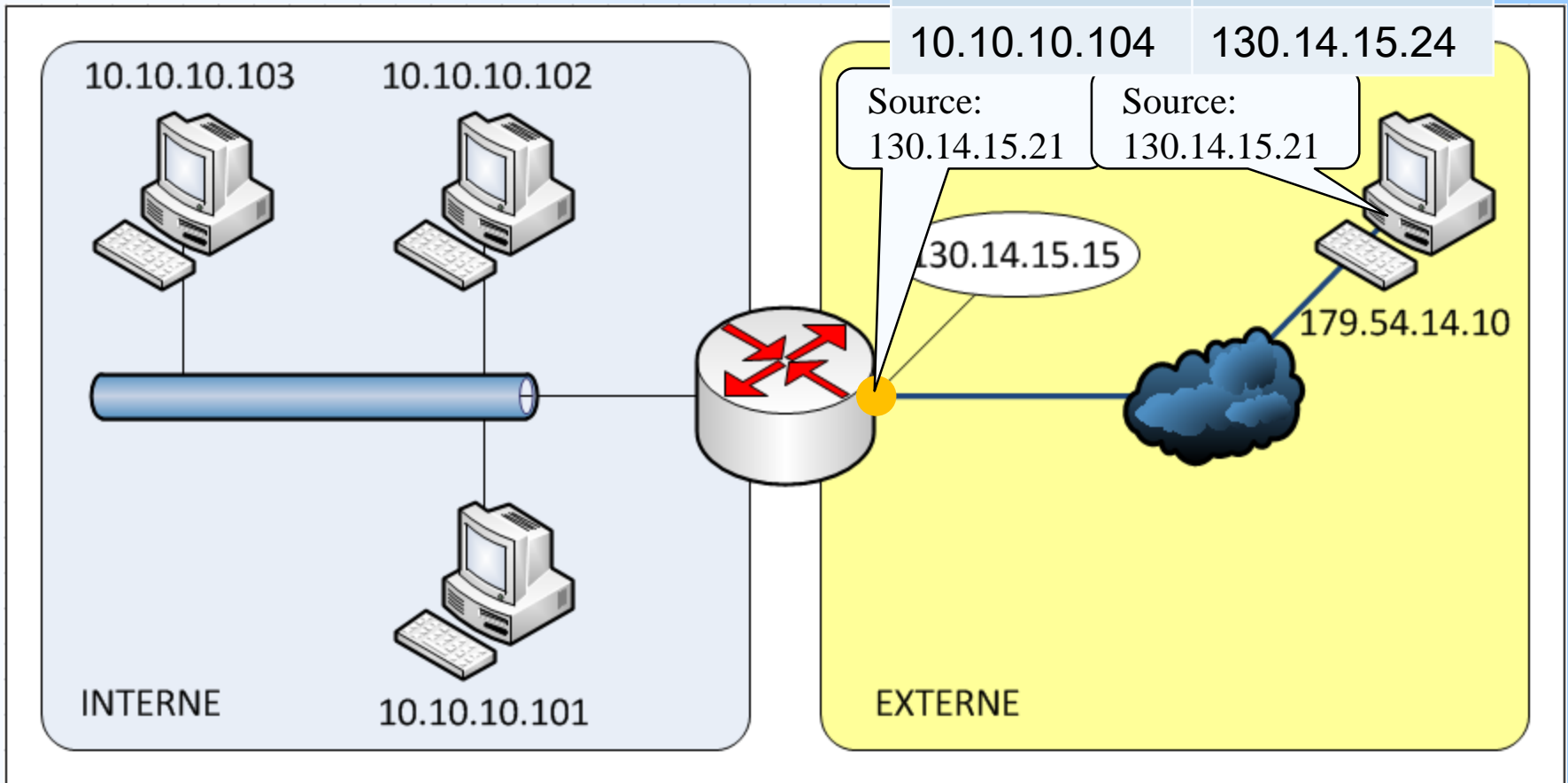
# NAT statique - Illustration

interne	externe
10.10.10.101	130.14.15.21
10.10.10.102	130.14.15.22
10.10.10.103	130.14.15.23
10.10.10.104	130.14.15.24



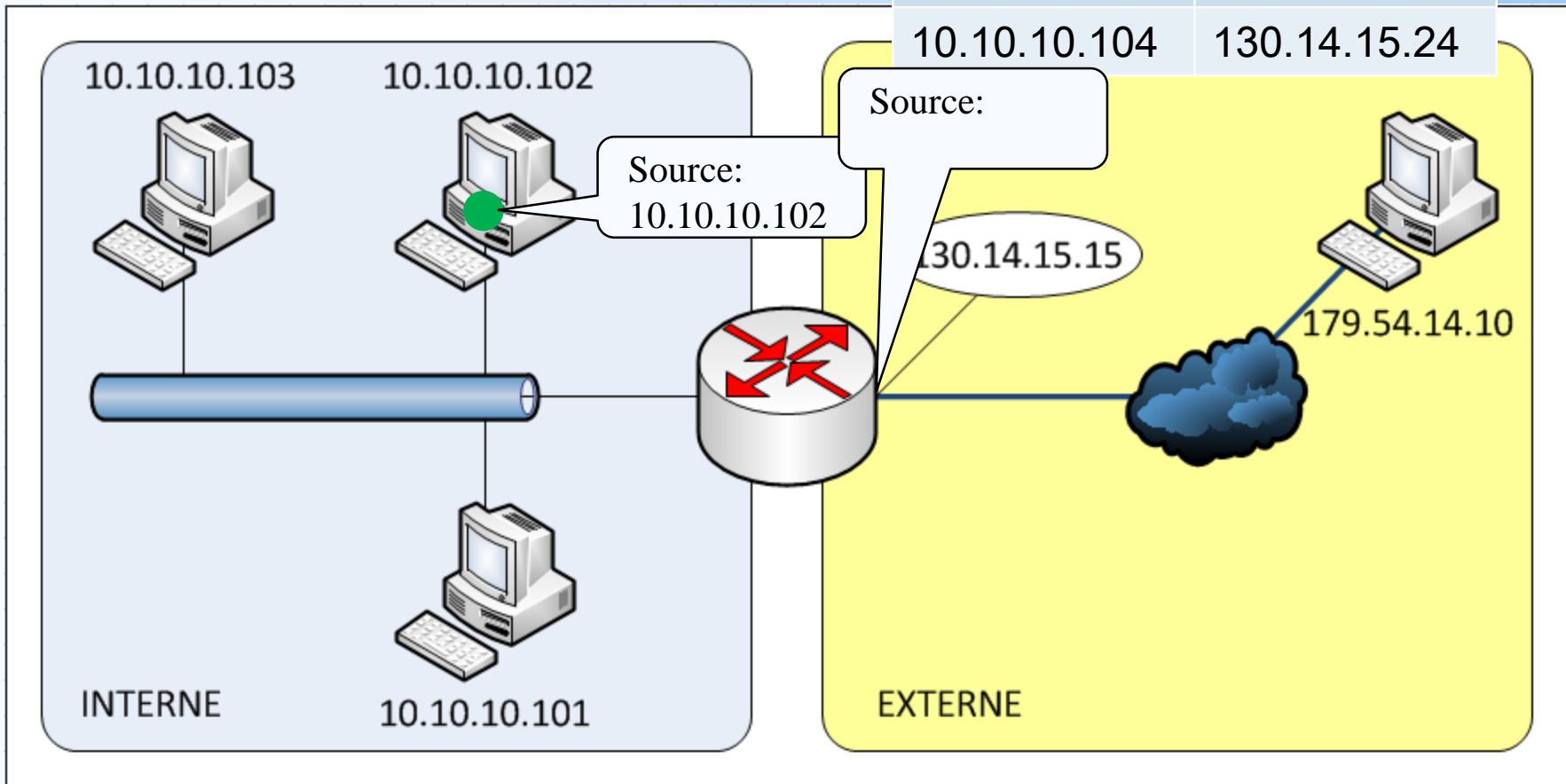
# NAT statique - Illustration

interne	externe
10.10.10.101	130.14.15.21
10.10.10.102	130.14.15.22
10.10.10.103	130.14.15.23
10.10.10.104	130.14.15.24



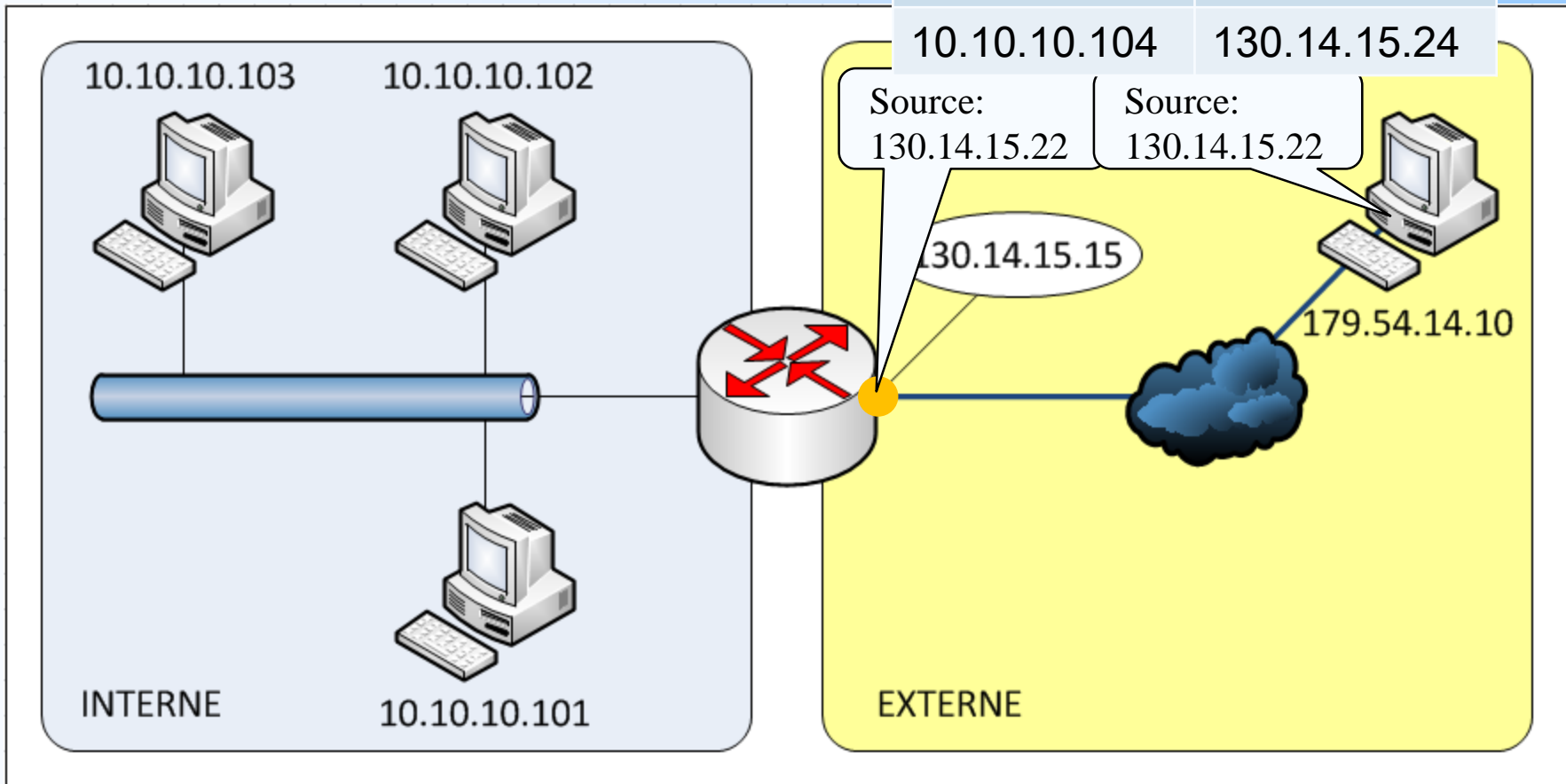
# NAT statique - Illustration

interne	externe
10.10.10.101	130.14.15.21
10.10.10.102	130.14.15.22
10.10.10.103	130.14.15.23
10.10.10.104	130.14.15.24



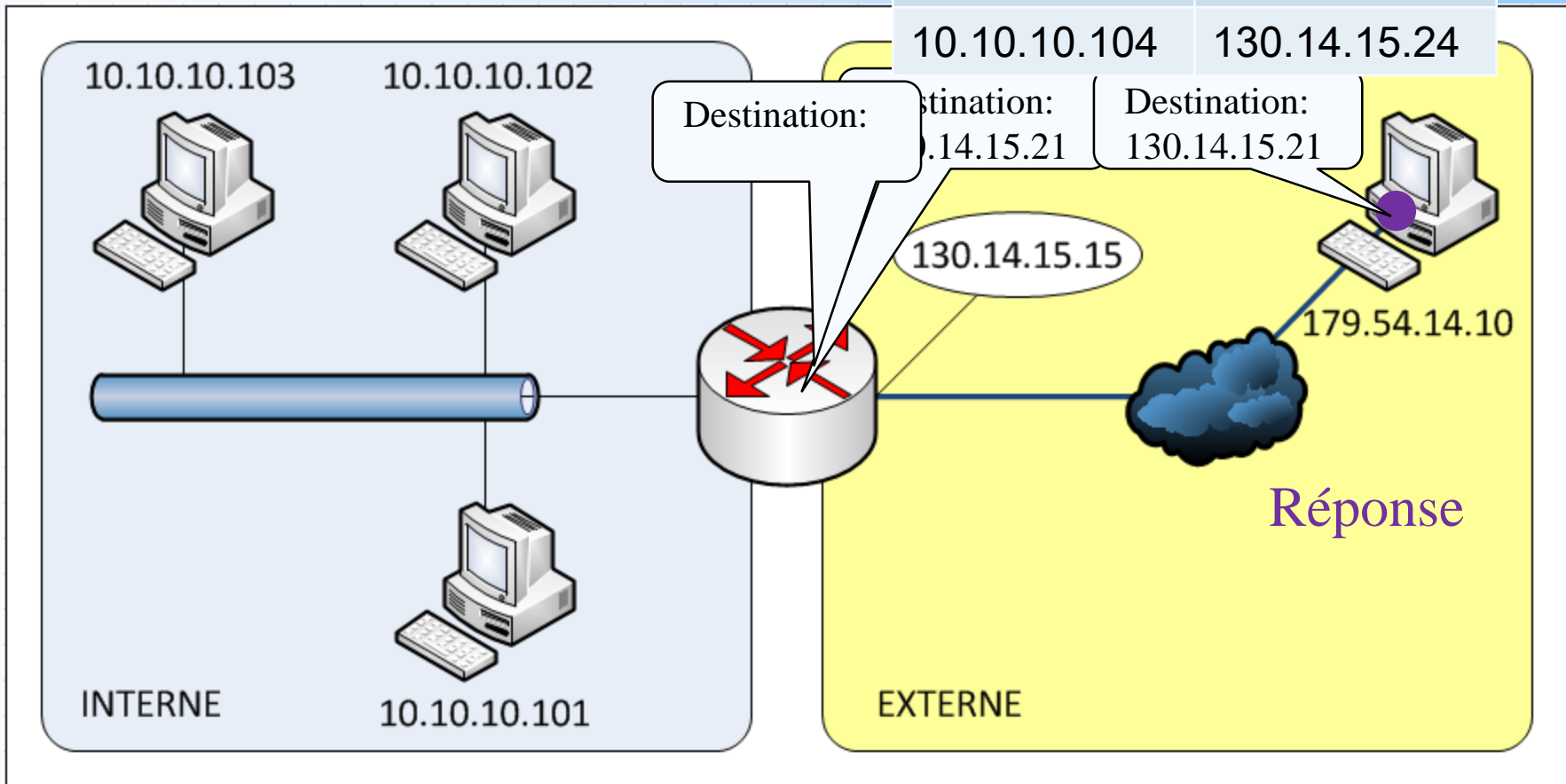
# NAT statique - Illustration

interne	externe
10.10.10.101	130.14.15.21
10.10.10.102	130.14.15.22
10.10.10.103	130.14.15.23
10.10.10.104	130.14.15.24



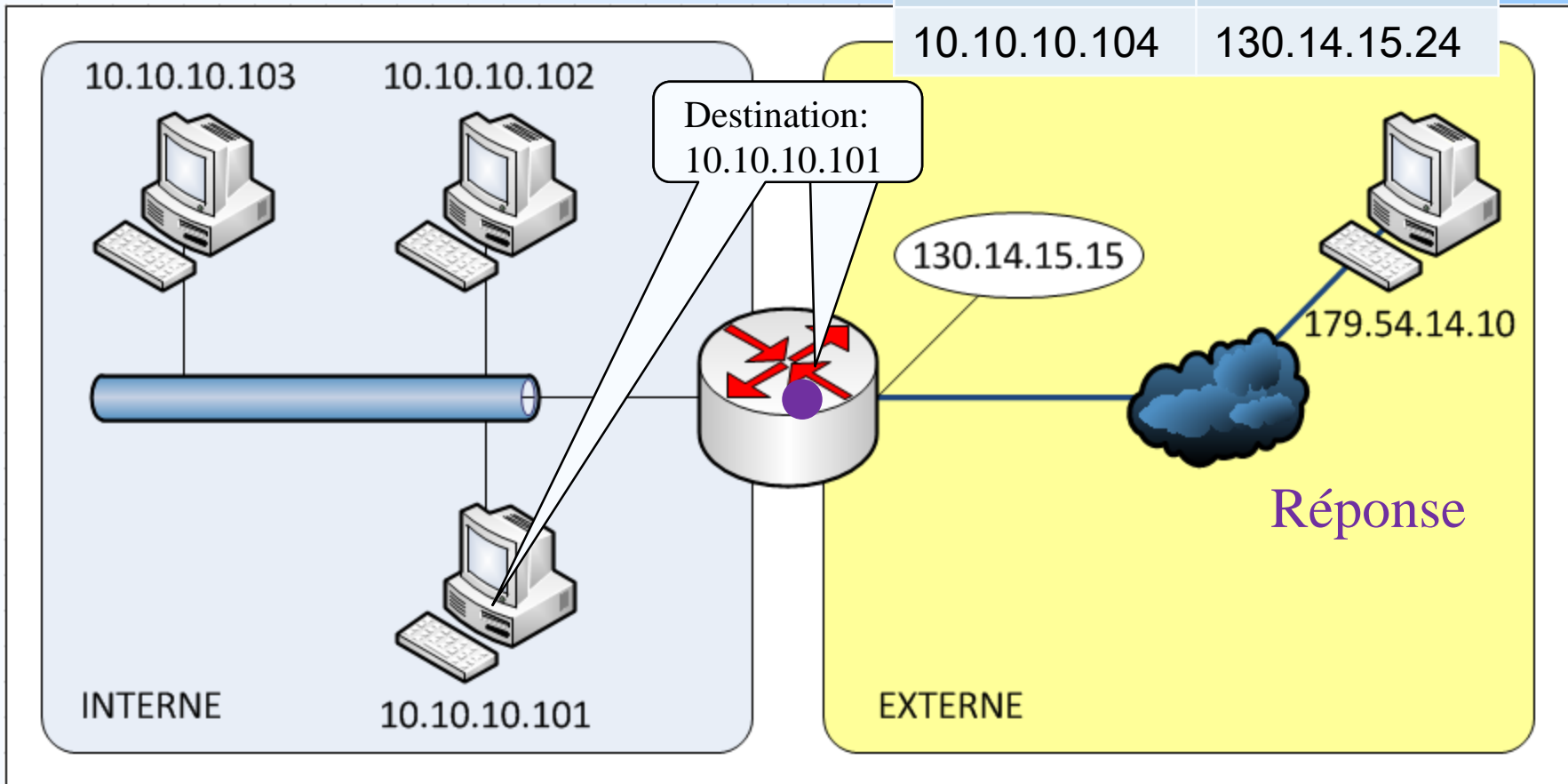
# NAT statique - Illustration

interne	externe
10.10.10.101	130.14.15.21
10.10.10.102	130.14.15.22
10.10.10.103	130.14.15.23
10.10.10.104	130.14.15.24



# NAT statique - Illustration

interne	externe
10.10.10.101	130.14.15.21
10.10.10.102	130.14.15.22
10.10.10.103	130.14.15.23
10.10.10.104	130.14.15.24



# NAT dynamique

## Comment ça marche?

- on dispose d'un pool d'adresses externes: on associe 1 adresse interne à 1 adresse du pool seulement quand c'est nécessaire et pour un temps limité. Le routeur conserve la correspondance dans une table

## Avantage?

- on utilise un minimum d'adresses externes

## Inconvénients?

- on doit limiter le nombre d'accès simultanés à l'extérieur
- la correspondance change (on ne peut pas joindre une machine interne de l'extérieur facilement)



# NAT-PAT (Port Address Translation)

## Comment ça marche?

- on utilise 1 ou plusieurs adresses extérieures et l'on remplace l'adresse interne ET le port interne par une adresse extérieure et un port externe libre. Le routeur conserve la correspondance dans une table

## Avantage?

- moins de limitations

## Inconvénients?

- la correspondance change (on ne peut pas joindre une machine interne de l'extérieure facilement)
- plus de calculs au niveau du routeur

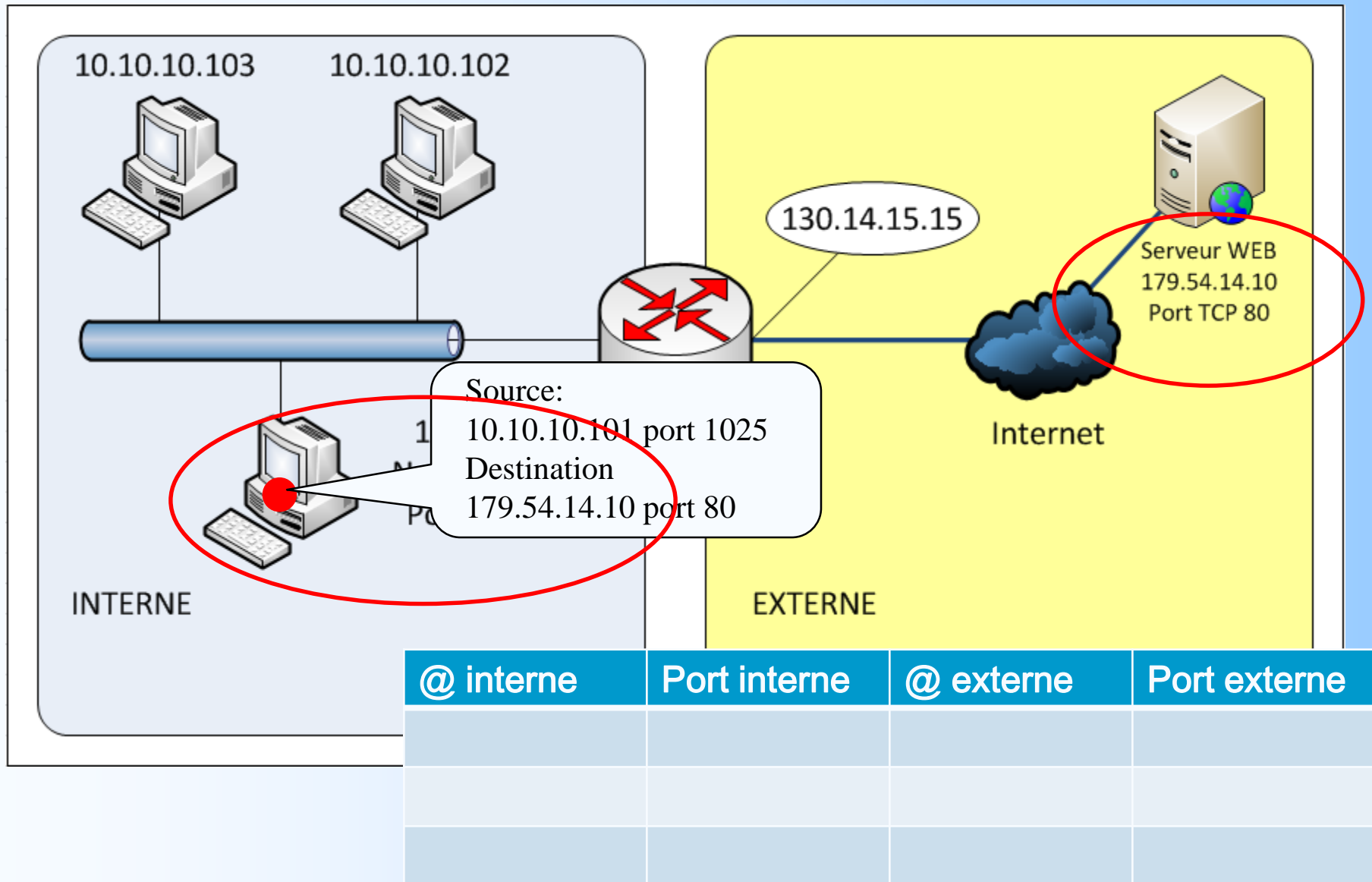
Autre nom: NAT dynamique avec surcharge  
(NAT overload)

## NAT-PAT : Illustration

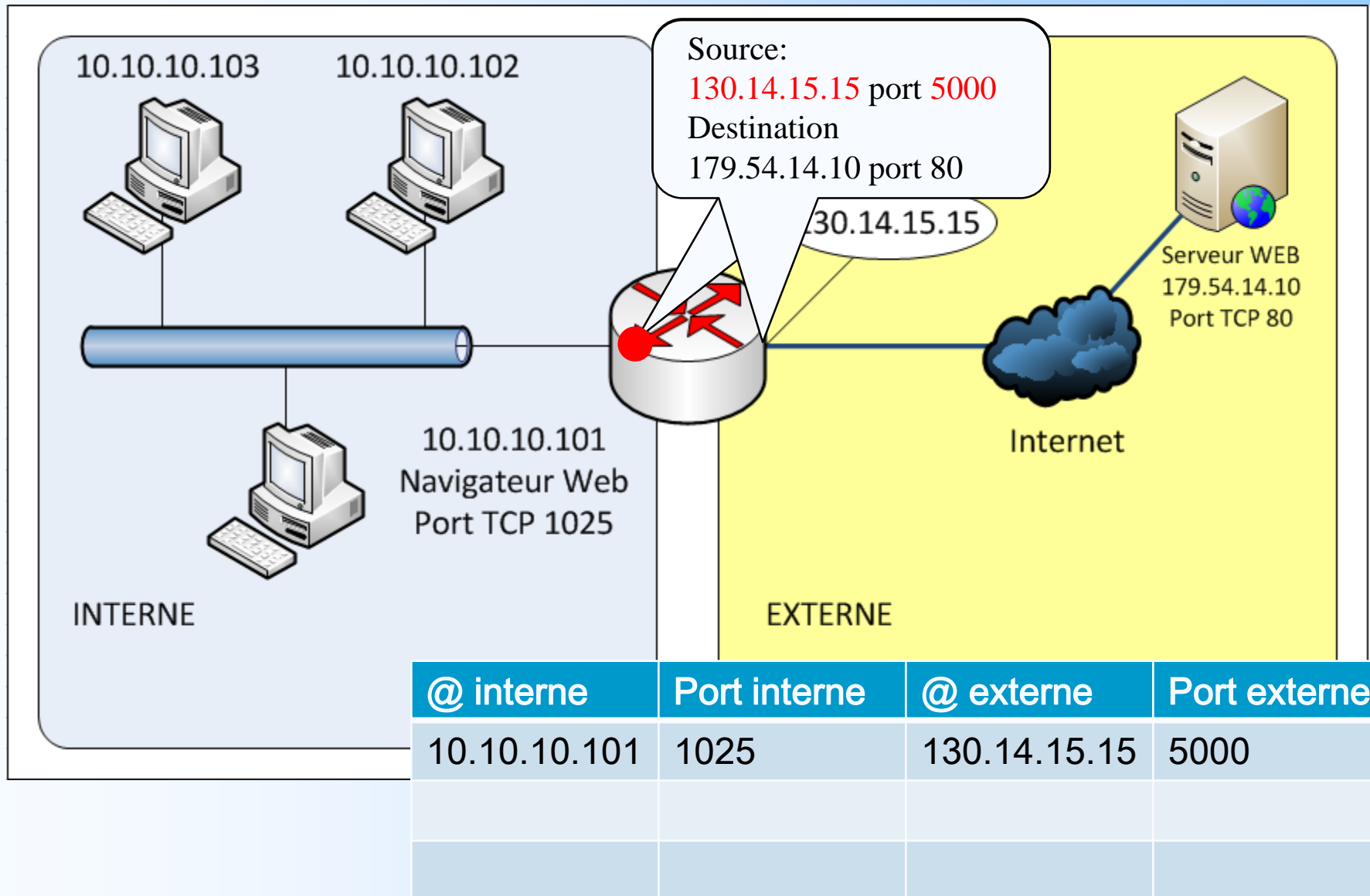
- Cette technique peut être utilisée avec une ou plusieurs adresses externes.
- Typiquement, on l'utilise quand on connecte une PME à l'internet avec un routeur basique, ou bien à la maison (où vous avez plusieurs équipements qui se connectent à internet, mais une seule adresse externe).
- La table du routeur contiendra les informations suivantes:

@ interne	Port interne	@ externe	Port externe

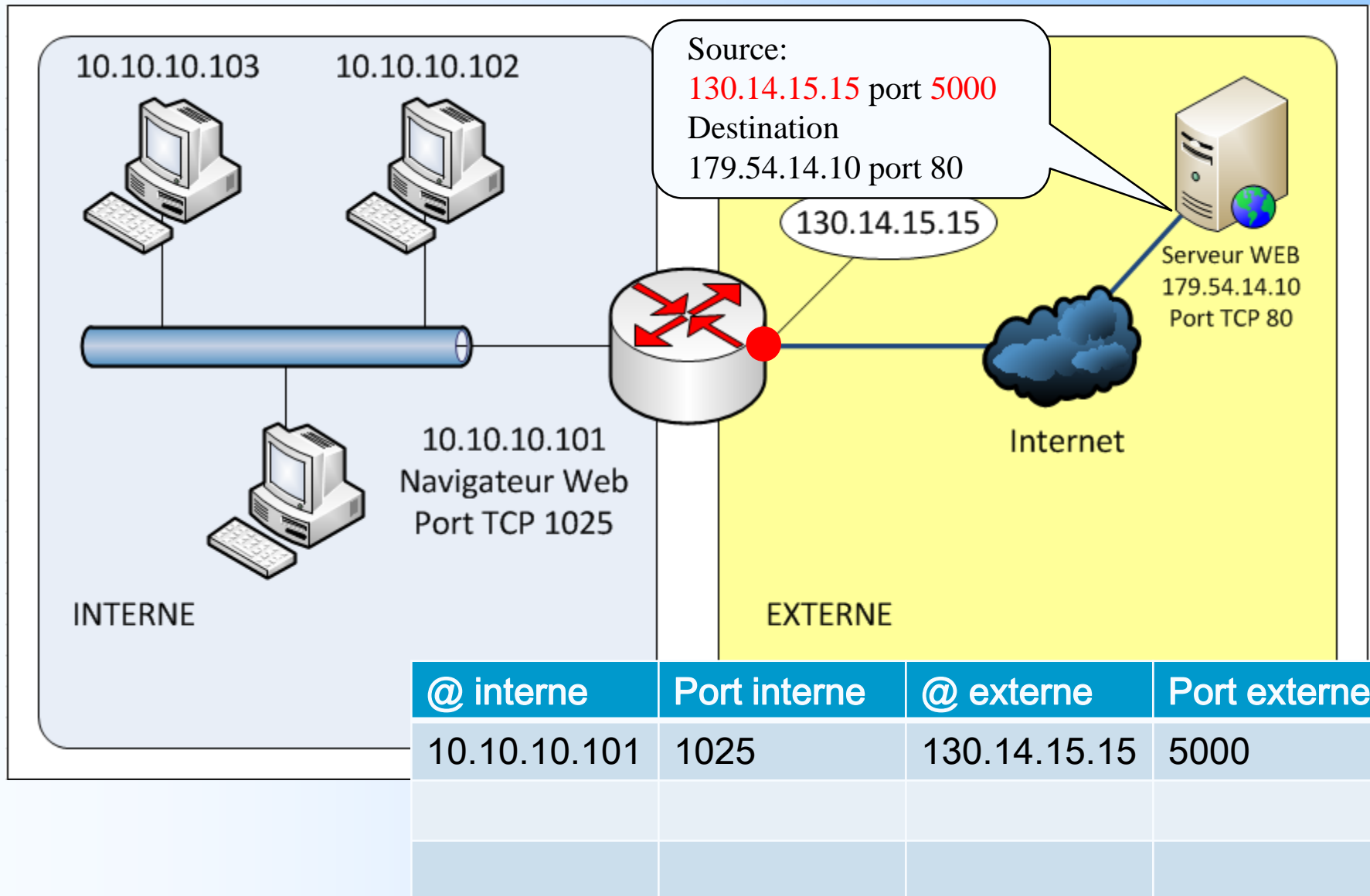
# NAT-PAT : Exemple – accès à un serveur web avec 1 adresse externe



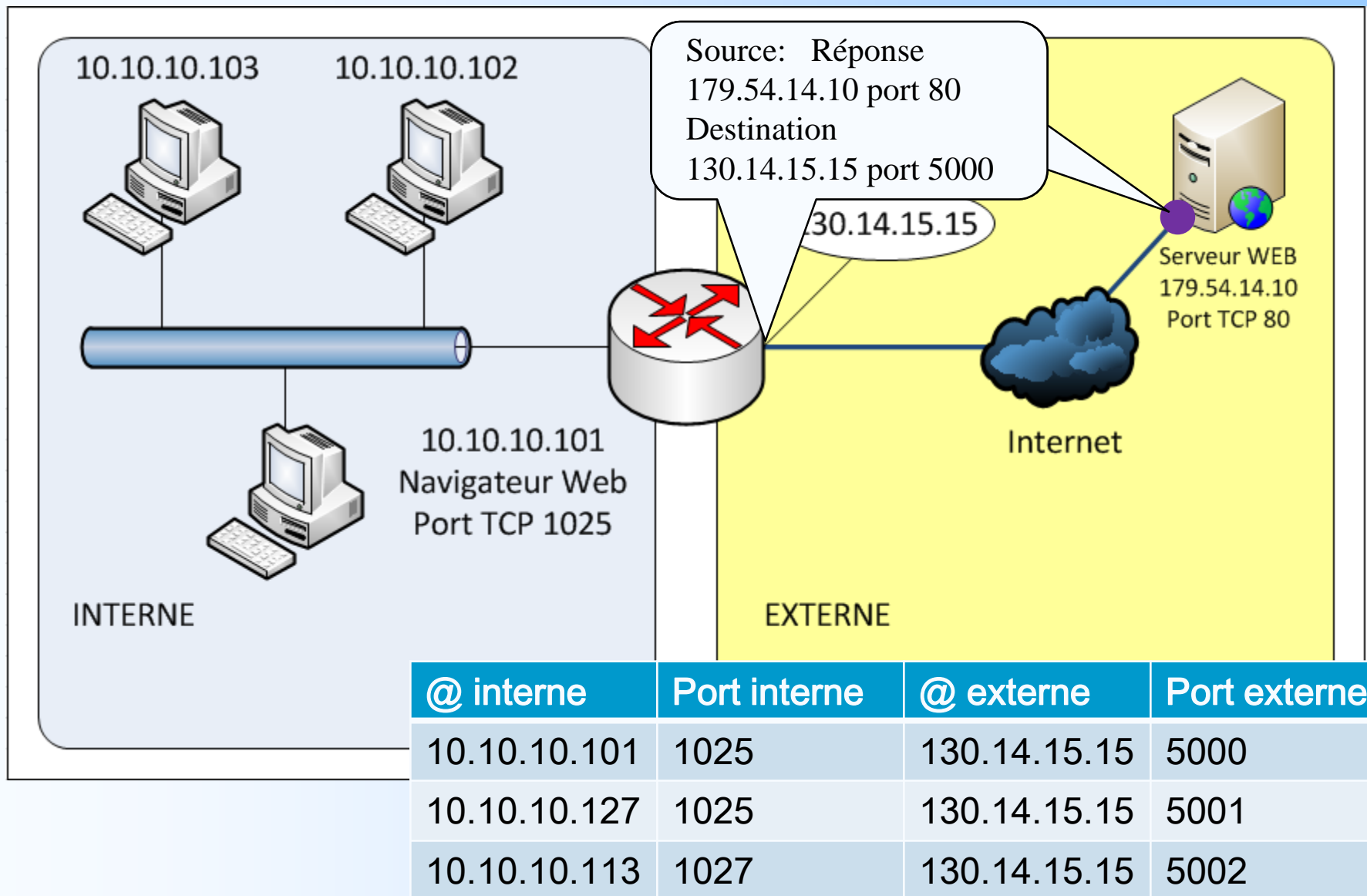
# NAT-PAT : Exemple – accès à un serveur web avec 1 adresse externe



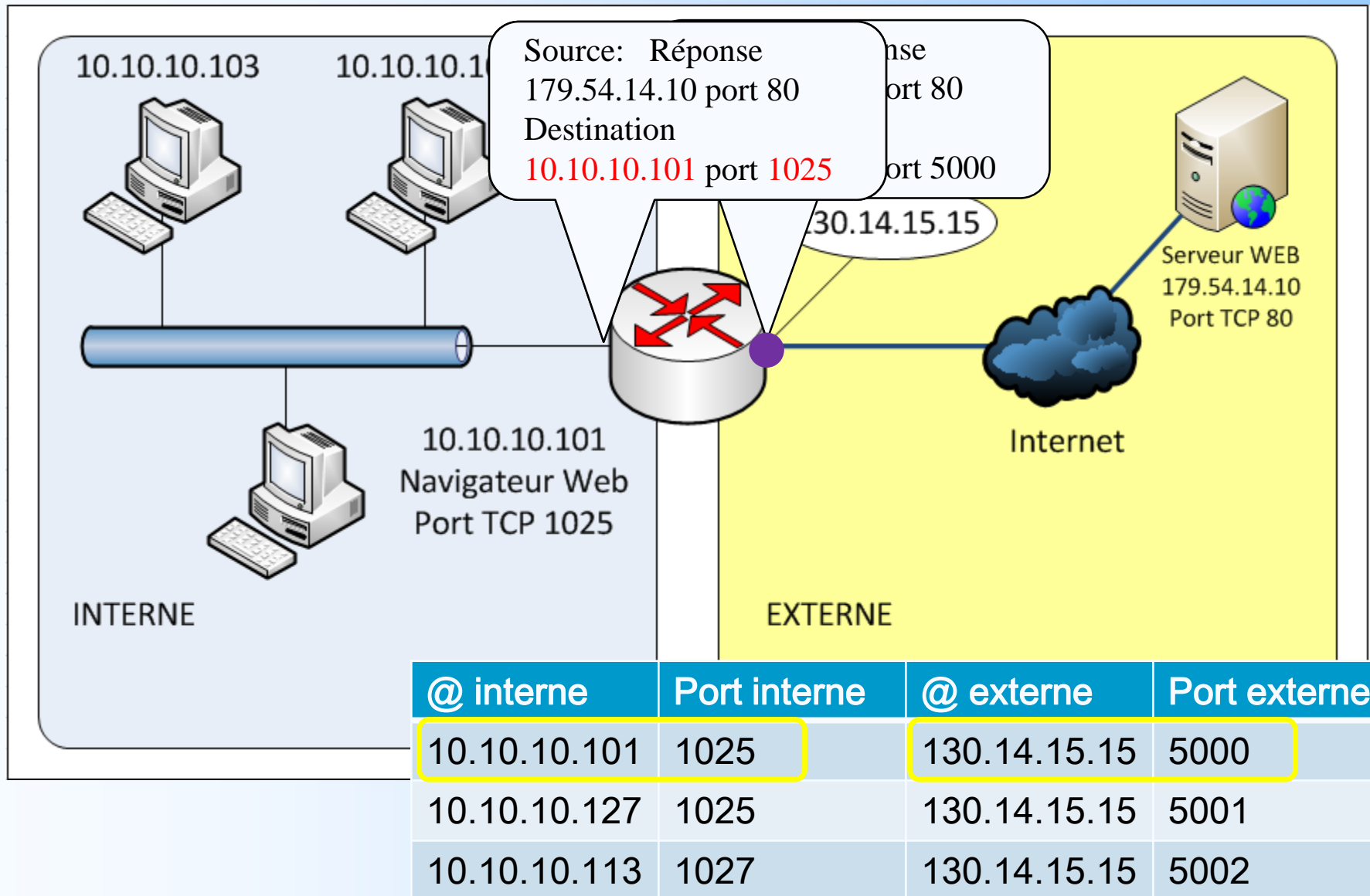
# NAT-PAT : Exemple – accès à un serveur web avec 1 adresse externe



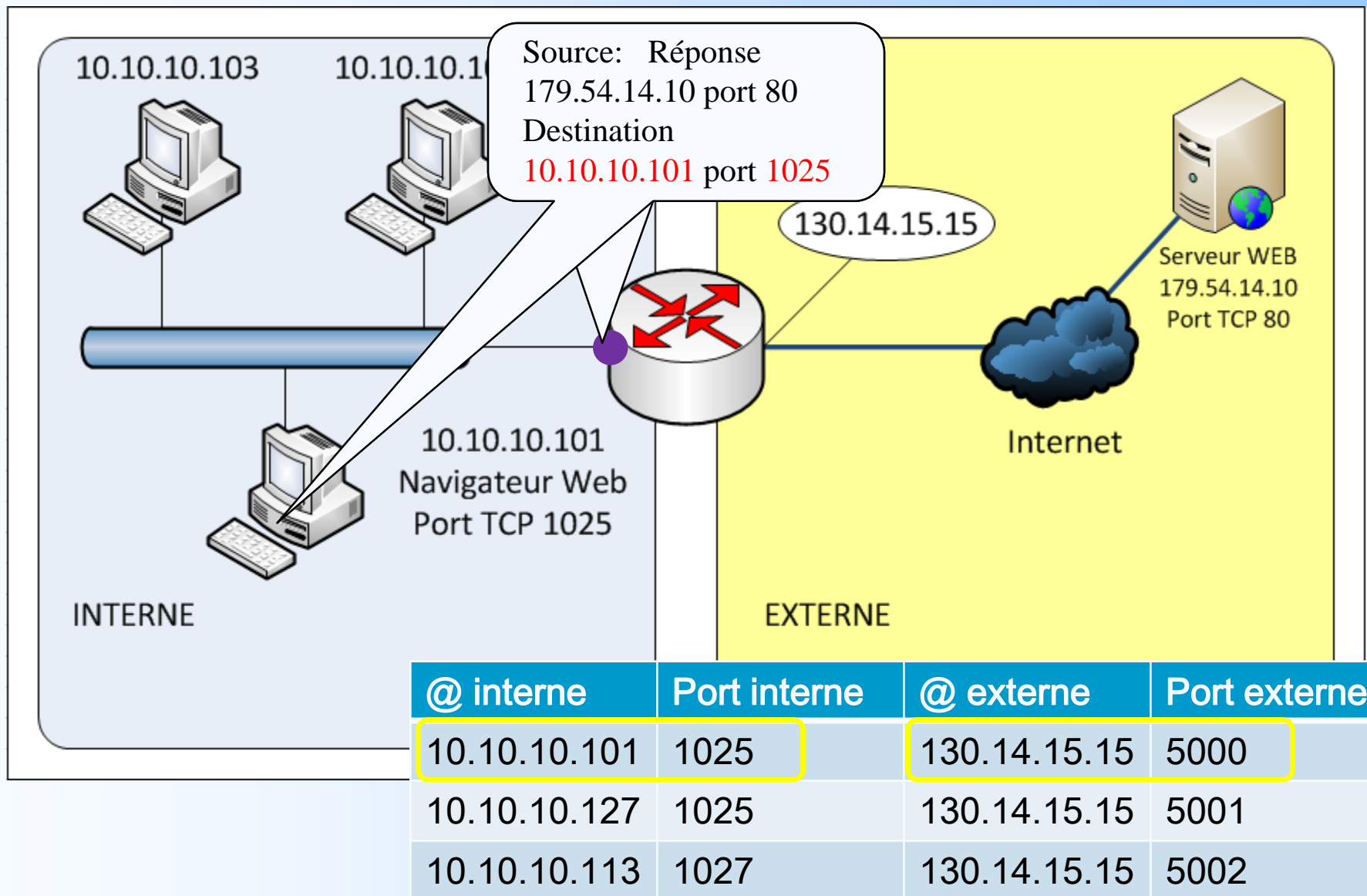
# NAT-PAT : Exemple – accès à un serveur web avec 1 adresse externe



# NAT-PAT : Exemple – accès à un serveur web avec 1 adresse externe



# NAT-PAT : Exemple – accès à un serveur web avec 1 adresse externe





## NAT - précisions

- Il existe d'autres scénarios plus complexes que nous n'aborderons pas dans ce module (qui font intervenir des modifications au niveau des serveurs DNS par exemple)
- On peut dans un réseau typique utiliser le NAT statique pour des serveurs accessibles depuis l'extérieur (extranet, webmail, site internet...) et du NAT-PAT pour les postes de travail.
- Au lieu du NAT statique on peut aussi utiliser du «port forwarding»: pour les paquets entrants on détermine l'hôte interne en se basant uniquement sur le port. Pour par exemple différencier le trafic vers le serveur web, le web mail, le vpn, le ftp ... Utile si on a 1 adresse seulement.