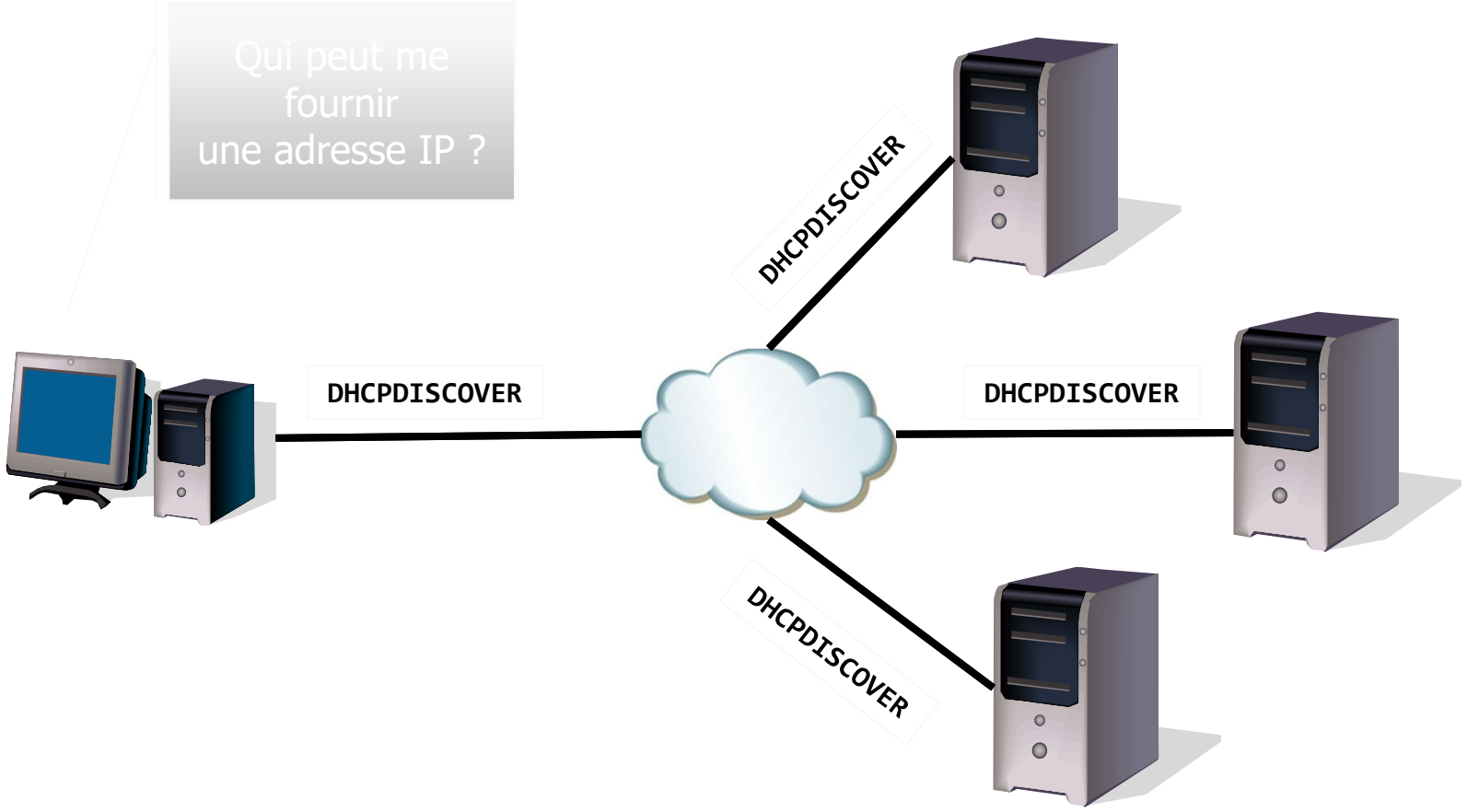
4. Translations d'adresses et architectures sécurisées

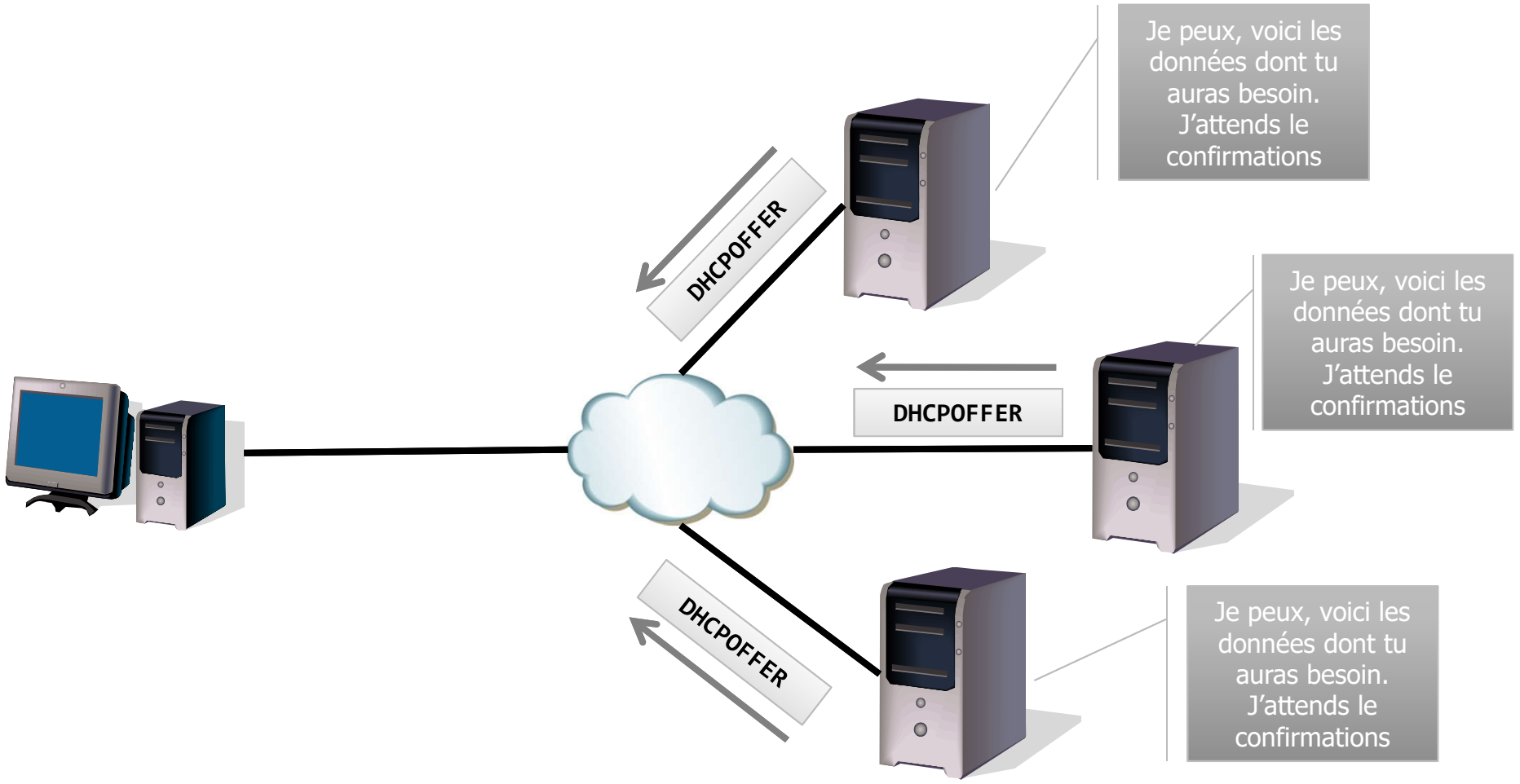
Rappel DHCP

- Dynamic Host Configuration Protocol
- Protocole permettant d'attribuer dynamiquement des @IP et d'autres paramètres de configuration IP tels que :
  - Adresse IP
  - Passerelle par défaut
  - Masque
  - Serveur DNS
  - Durée du bail, Etc.
- Serveurs → @IP fixe, Station → @IP dynamique
- Utilise les ports UDP 67 et 68
- Les routeurs peuvent jouer le rôle de serveur DHCP pour des clients

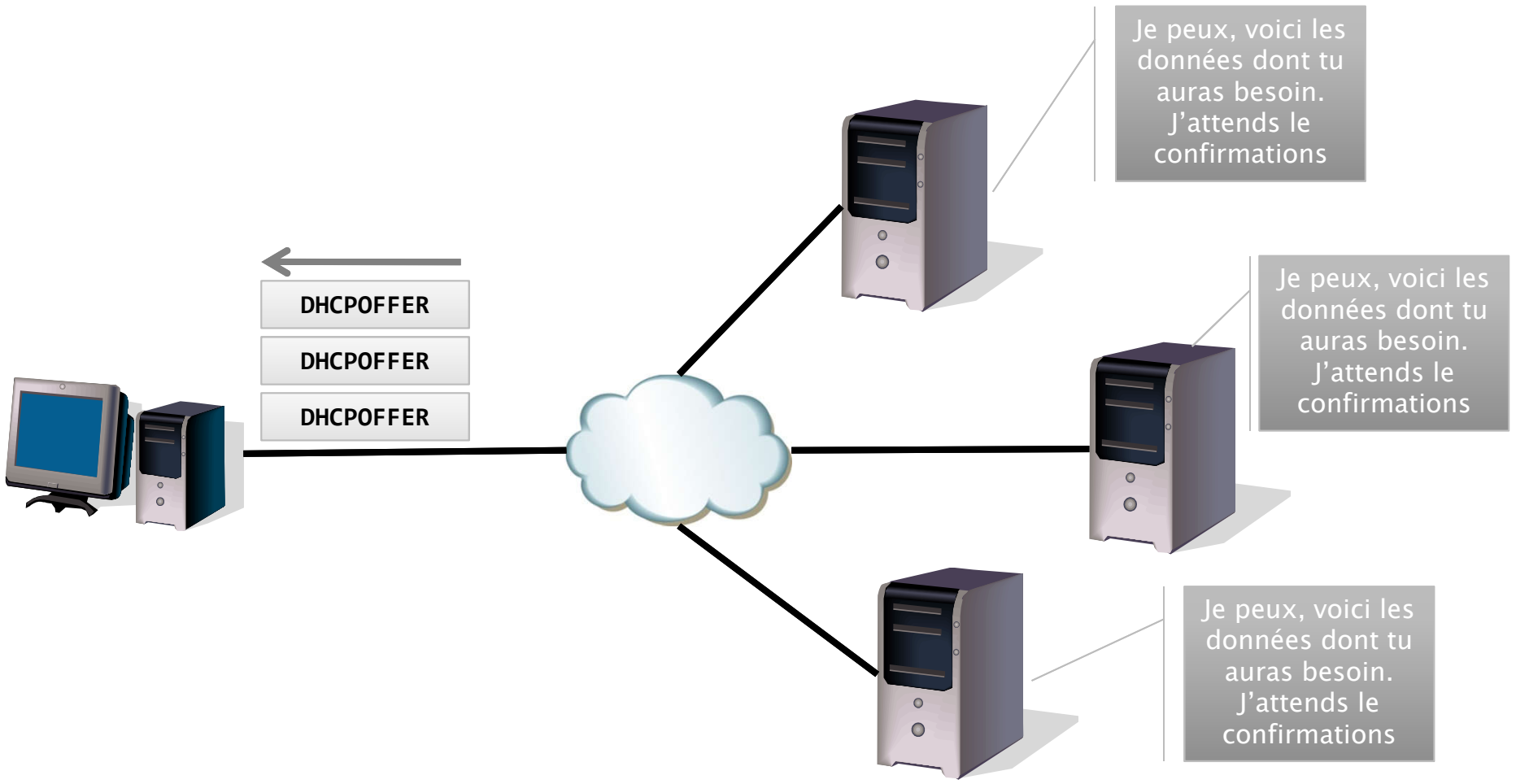
Fonctionnement de DHCP



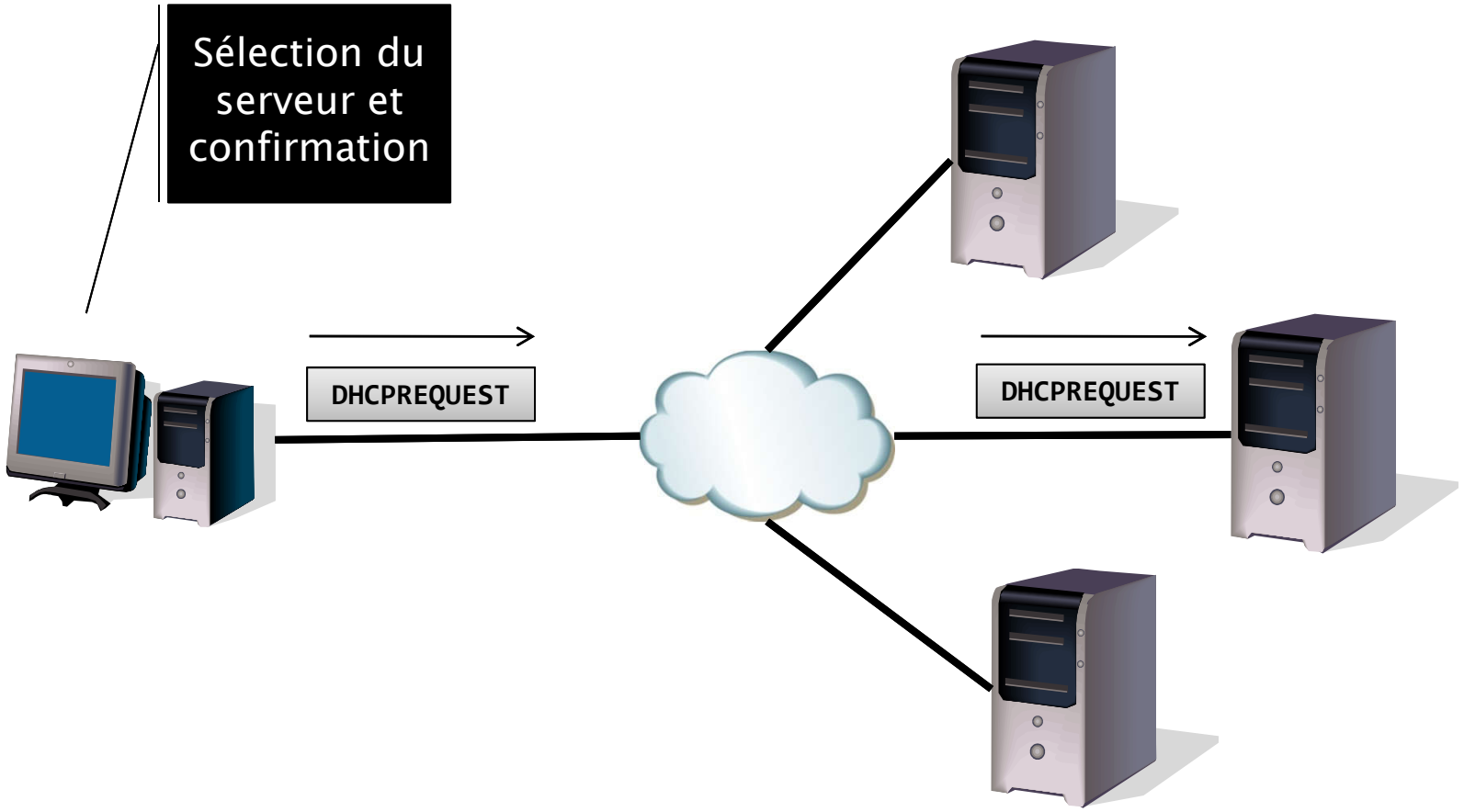
Fonctionnement de DHCP



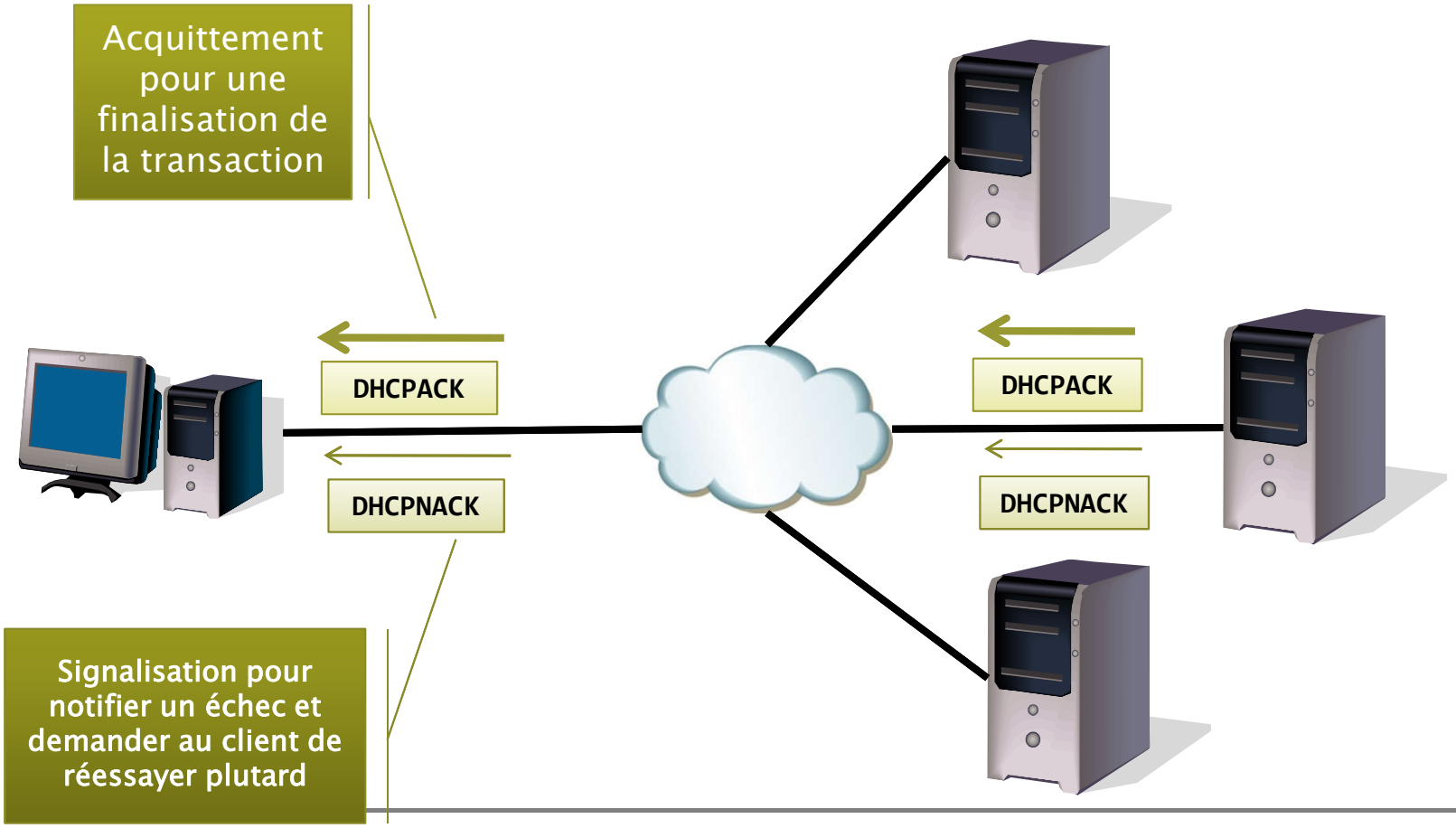
Fonctionnement de DHCP



Fonctionnement de DHCP



Fonctionnement de DHCP

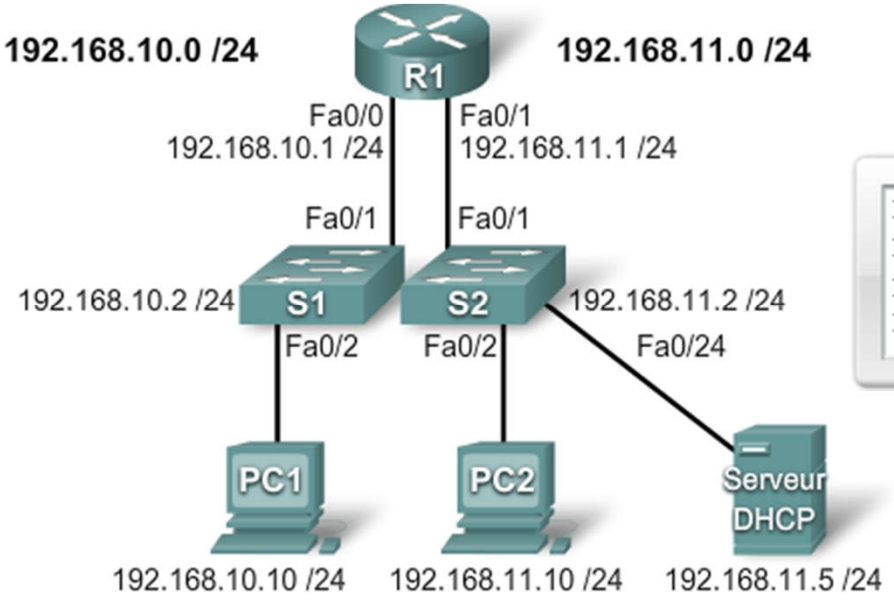


Allocations d'@IP par DHCP

- Il existe trois mécanismes d'allocation d'@IP
  - **Allocation statique** : l'administrateur attribue une adresse IP préallouée au client et le protocole DHCP communique uniquement l'adresse IP au périphérique.
  - **Allocation automatique** : le protocole DHCP attribue de façon automatique et permanente une adresse IP statique à un périphérique. Il n'y a pas de bail et l'adresse est attribuée de façon permanente au périphérique.
  - **Allocation dynamique** : le protocole DHCP attribue, ou loue, de façon automatique et dynamique une adresse IP pour une durée limitée.

Relais DHCP

- Les routeurs bloquent les diffusions
  - Les requêtes DHCP ne sont pas diffusées
- Nécessité de configurer un relais DHCP
  - Les routeurs peuvent transférer les diffusions DHCP à des serveurs situés sur d'autres réseaux IP




```
R1# config t
R1(config)# interface Fa0/0
R1(config-if)# ip helper-address 192.168.11.5
R1(config-if)# end
```

Adressage Internet

- Adresses IP publiques enregistrées auprès d'organismes ou des FAI
- Adressage privé en interne
  - Pas besoin des les acheter
  - Réutilisables
  - Cependant adresses non routables sur Internet

- Mécanisme de traduction de ces adresses privées en adresses publiques afin d'être routées sur Internet
  - La traduction d'adresse de réseau (NAT)
  - Mécanisme de sécurité très utilisé pour masquer des ressources internes à un réseau

Introduction NAT

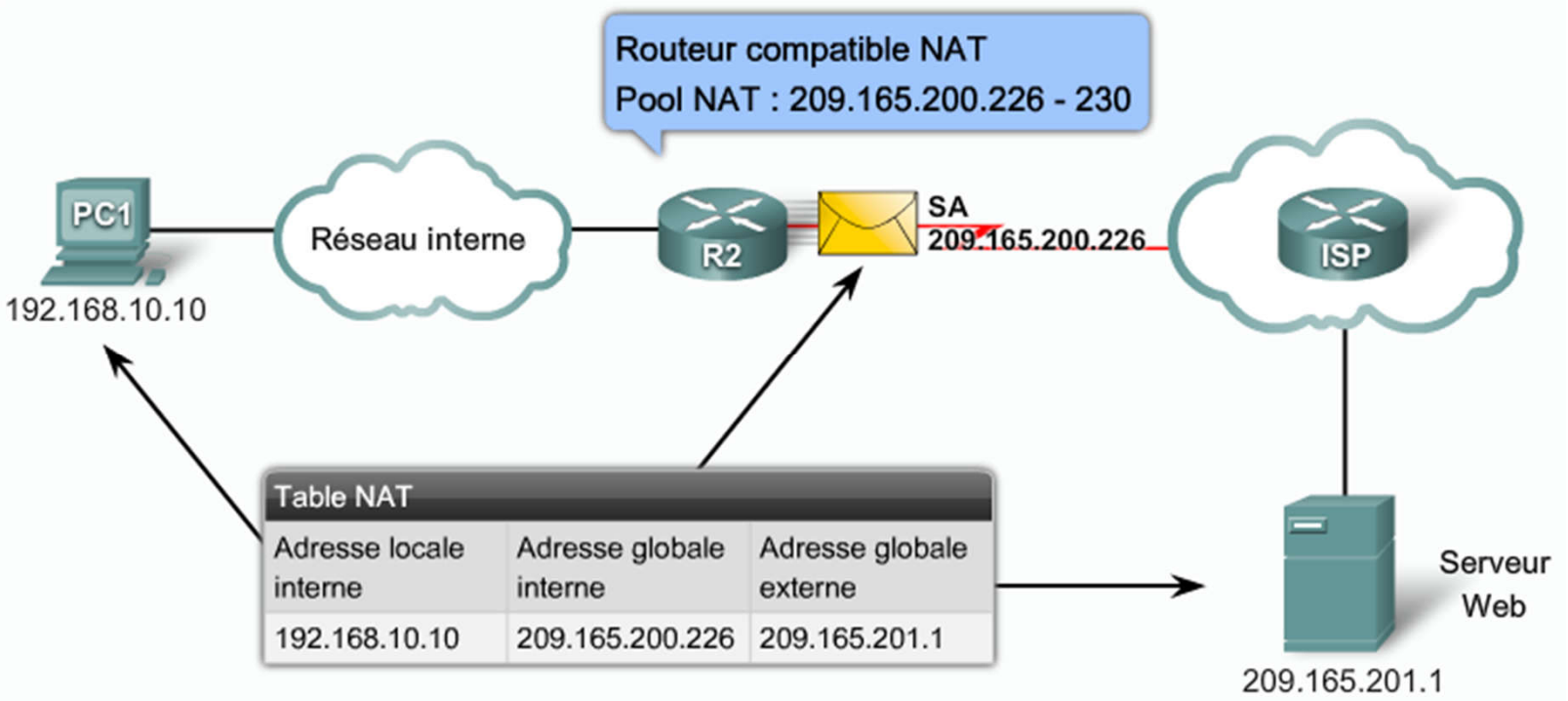
- Adresse IP publique
  - Nécessaires pour le routage sur Internet
  - Les adresses IP publiques sont de moins en moins disponibles et doivent être achetées
  - On ne peut attribuer à chaque station d'un LAN une adresse IP publique → **Solution NAT**
- NAT (Network Address Translation)
  - Remplacer un grand nombres d'adresses privées par un plus petit nombre d'adresses publiques
- Un routeur du LAN gère la NAT
  - Il effectue les translations d'adresses dans le sens sortant et entrant

Dénomination des adresses

- Adresse locale interne
  - C'est l'adresse IP privée dans le LAN qui désire transmettre des informations sur Internet
- Adresse globale interne
  - C'est l'adresse IP publique obtenue après avoir effectuée une translation d'adresse
  - Le routeur remplace l'**adresse source locale** par cette nouvelle **adresse globale interne**
  - Il fera l'opération inverse en cas de réponse
- Adresse globale externe
  - C'est l'adresse IP publique de destination.
- Exemple transparent suivant.

NAT

- Traduction des adresses non routables, privées et internes en adresses routables publiques
- Empêche les réseaux externes de voir les adresses IP internes



Fonctionnement du NAT

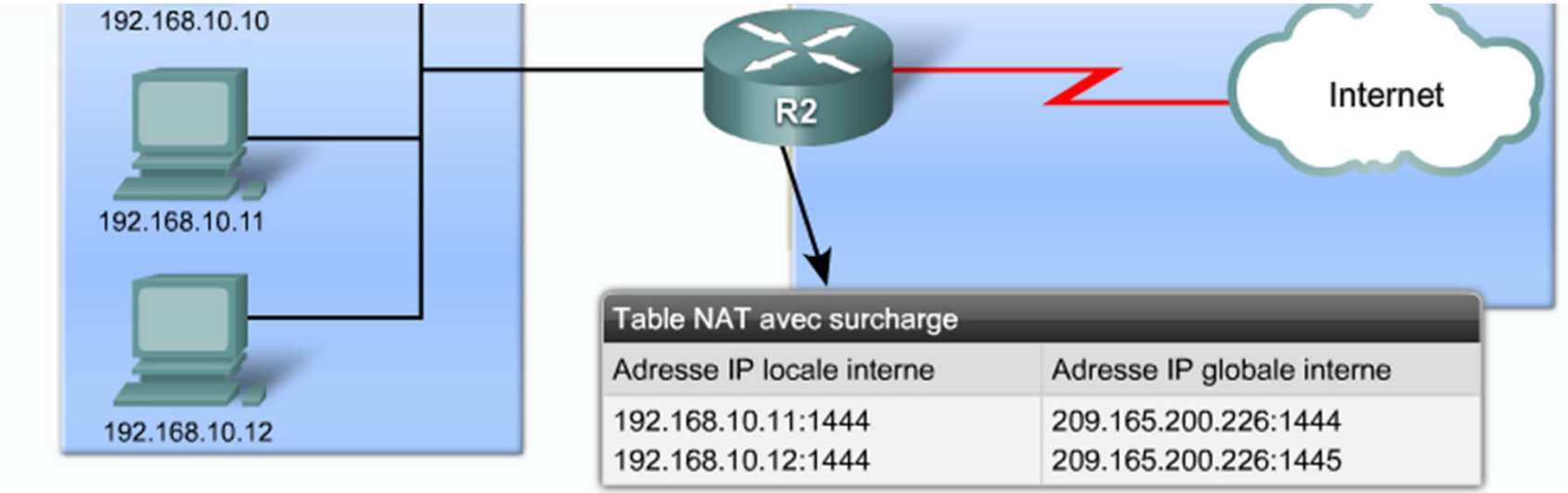
- Exemple de fonctionnement
  - PC1 → R2 (@IP source = 192.168.10.10)
  - R2 lit l'@IP de destination et vérifie si la NAT est autorisé pour ce paquet (**ACL spécifique**)
  - Traduit l'adresse locale interne **192.168.10.10** en adresse IP globale interne **209.165.200.226**.
  - Stocke cette traduction dans la table NAT
  - Réponse du serveur à l'@IP 209.165.200.226
  - Consultation de sa table NAT
  - Retraduction inverse de l'@IP globale interne 209.165.200.226 en @IP locale interne 192.168.10.10 et envoi des données vers PC1

Mappage des adresses

- Mappage statique (NAT statique)
  - Association fixe et prédéfinie d'un @IP interne à une @IP publique
  - Utile pour des serveurs Web devant disposer d'une adresse permanente atteignable depuis l'extérieur
- Mappage dynamique (NAT dynamique)
  - Utilise un pool d'adresses publiques
  - Premier arrivé, premier servi
  - Affectation d'une @IP publique non utilisée par un autre hôte
- Les fonctions NAT statique et dynamique
  - Nécessitent un nombre suffisants d'@IP publiques

PAT ou surcharge NAT

- Translation d'adresse par port
  - Généralement un seule @IP publique
  - Chaque adresse IP privée est associé à un port
  - Plusieurs sessions TCP/IP sont donc distinguées par les numéros de ports utilisées pour la PAT
  - Fonctionne comme la NAT avec des différences



Différences entre NAT et PAT

- Principales différences
  - NAT association @IP privée → @IP publique
  - NAT nécessite au moins pour chaque @IP privée une @IP publique
  - PAT une seule adresse publique mais des numéros de ports différents pour chaque @IP privée
  - PAT nécessite au moins une @IP publique pour environ des milliers d'@IP privées (Numéros de ports codés sur 16 bits donc en théorie 65536 possibilités)
  - En pratique environ 4000 possibilités
  - Les ports déjà utilisés par d'autre services ne sont pas attribués pour les translations PAT

Avantages et inconvénients

- Avantages
  - Économie des adresses publiques et avec la PAT une seule adresse est partagée entre plusieurs hôtes
  - Sécurité car masque les @IP privées internes
- Inconvénients
  - Performances
  - Fonctionnalité de bout en bout affecté
  - Délai supplémentaire ajouté ce qui peut gêner les applications de types VoIP
  - Traçabilité IP de bout en bout perdue
- IPv6 abandonne le concept de NAT et PAT au profit des adresses de monodiffusion globale

Configuration NAT-PAT

- Elle se fait en 4 étapes
  - **Étape 1** : Définition du groupe d'adresses IP publiques utilisables
  - **Étape 2** : Définition d'une liste de contrôle d'accès correspondant aux adresses IP privées internes
  - **Étape 3** : Définition la traduction NAT de la liste interne vers le groupe d'adresses IP externes
  - **Étape 4** : Définition des interfaces actives sur le routeur en tant qu'interfaces internes ou externes par rapport à la NAT

Configuration NAT

- Adresses globales internes disponibles
  - **Router(config)#ip nat pool extern 199.12.1.1 199.12.1.20 netmask 255.255.255.0**
- ACL des adresses locales internes autorisées
  - **Router(config)#access-list 1 permit 10.0.0.0 0.255.255.255**
- Mise en place de la NAT dynamique
  - **Router(config)#ip nat inside source list 1 pool extern**
- Interface inside et outside
  - **Router(config-if)#ip nat [inside | outside]**
- **Mise en place NAT statique**
  - **Router(config#ip nat inside source static 10.0.0.1 199.12.1.1**

Configuration PAT

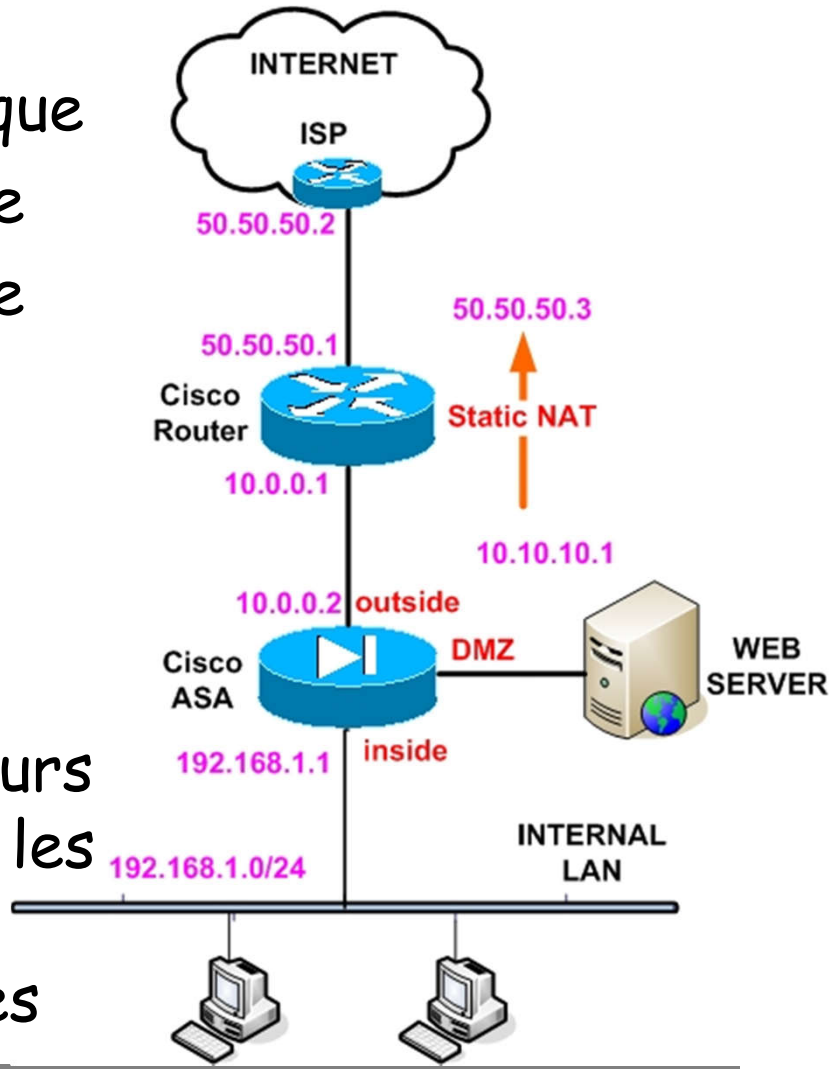
- ACL des adresses locales internes autorisées
  - Router(config)#access-list 1 permit 10.0.0.0 0.255.255.255
- Mise en place de la PAT
  - Router(config)#ip nat inside source list 1 interface serial 0/0 overload
- Interface inside et outside
  - Router(config-if)#ip nat [inside | outside]
- Possibilité de définir une plage d'adresses si une seule adresse est insuffisante pour la PAT
  - Router(config)#ip nat pool extern 199.12.1.1 199.12.1.5 netmask 255.255.255.0
  - Router(config)#ip nat inside source list 1 pool extern overload

Architecture de réseau sécurisée

- Architectures modulaire à trois niveaux
- **Niveau 1 : Le LAN**
  - C'est le réseau interne de la société. Il doit avoir une protection maximale vis-à-vis de l'extérieur.
  - Ne doit pas être accessible depuis l'extérieur
- **Niveau 2 : L'extérieur**
  - Généralement l'Internet. Doit être accessible depuis le LAN pour les ressources externes
- **Niveau 3 : La DMZ**
  - Zone permettant de stocker les serveurs publics de la société. Doit avoir un niveau de sécurité élevé
  - Doit être accessible de l'extérieur et du LAN

Architecture sécurisée : Exemple

- Adressage
  - Internet → adressage publique
  - DMZ → adressage privée
  - LAN → adressage privée
- Translations d'adresses
  - DMZ → NAT statique
  - LAN → PAT
- **Architecture évolutive**
  - DMZ externe pour les serveurs publics - DMZ internet pour les serveurs du LAN – DMZ extranet pour les partenaires



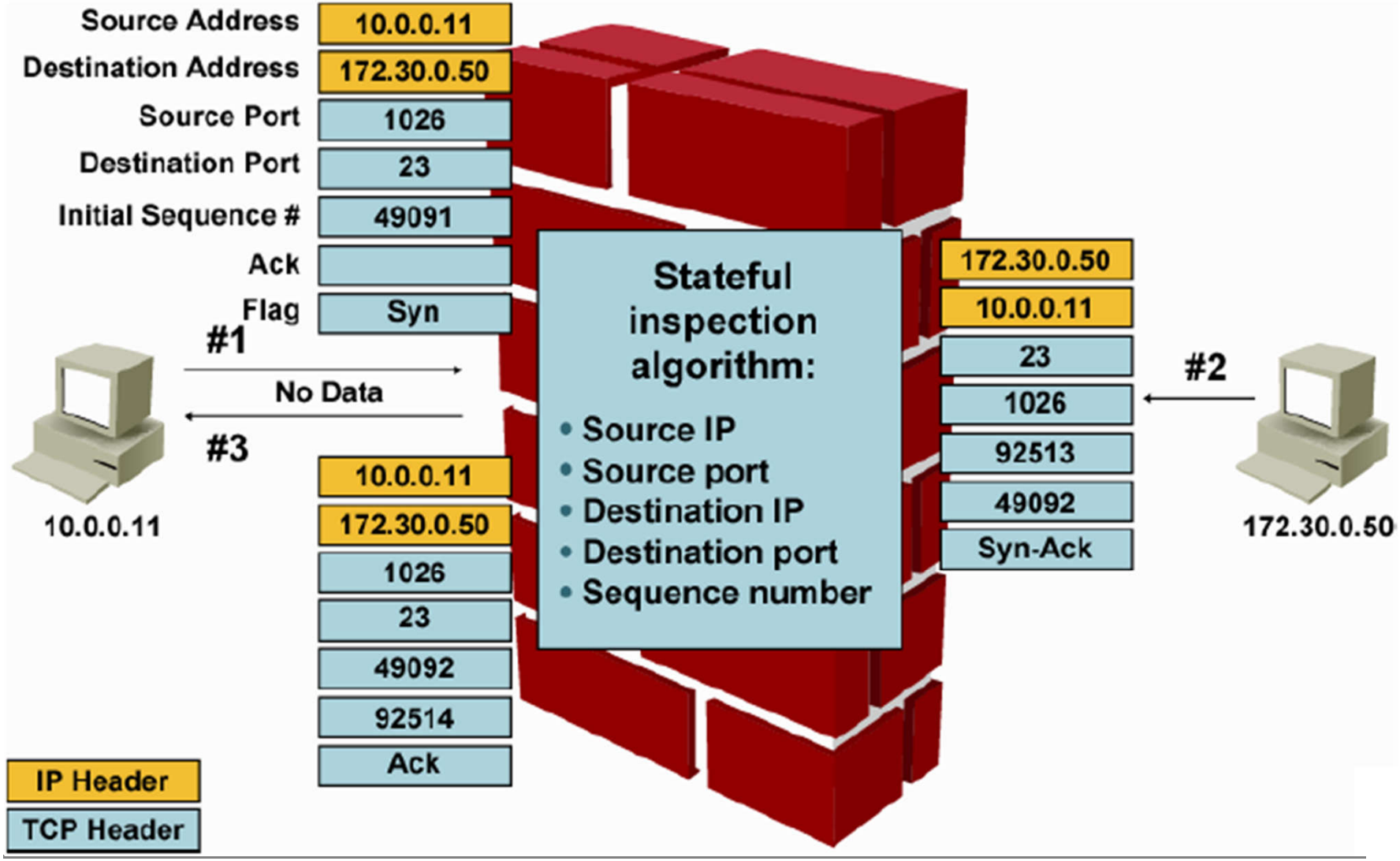
Règles de sécurité globale

- DMZ : Zone tampon entre l'extérieur et le LAN
  - Sous réseau abritant les serveurs publics appelés également **bastions** d'une société qui doivent être accessibles depuis l'Internet
- DMZ interne (Plus grande sécurité dans le LAN)
- **Politique de sécurité globale**
  - Extérieur vers DMZ → **autorisé**
  - Extérieur vers LAN → **interdit**
  - LAN vers DMZ → **autorisé**
  - LAN vers extérieur → **autorisé**
  - DMZ vers LAN → **interdit**
  - DMZ vers extérieur → **interdit**

CBAC

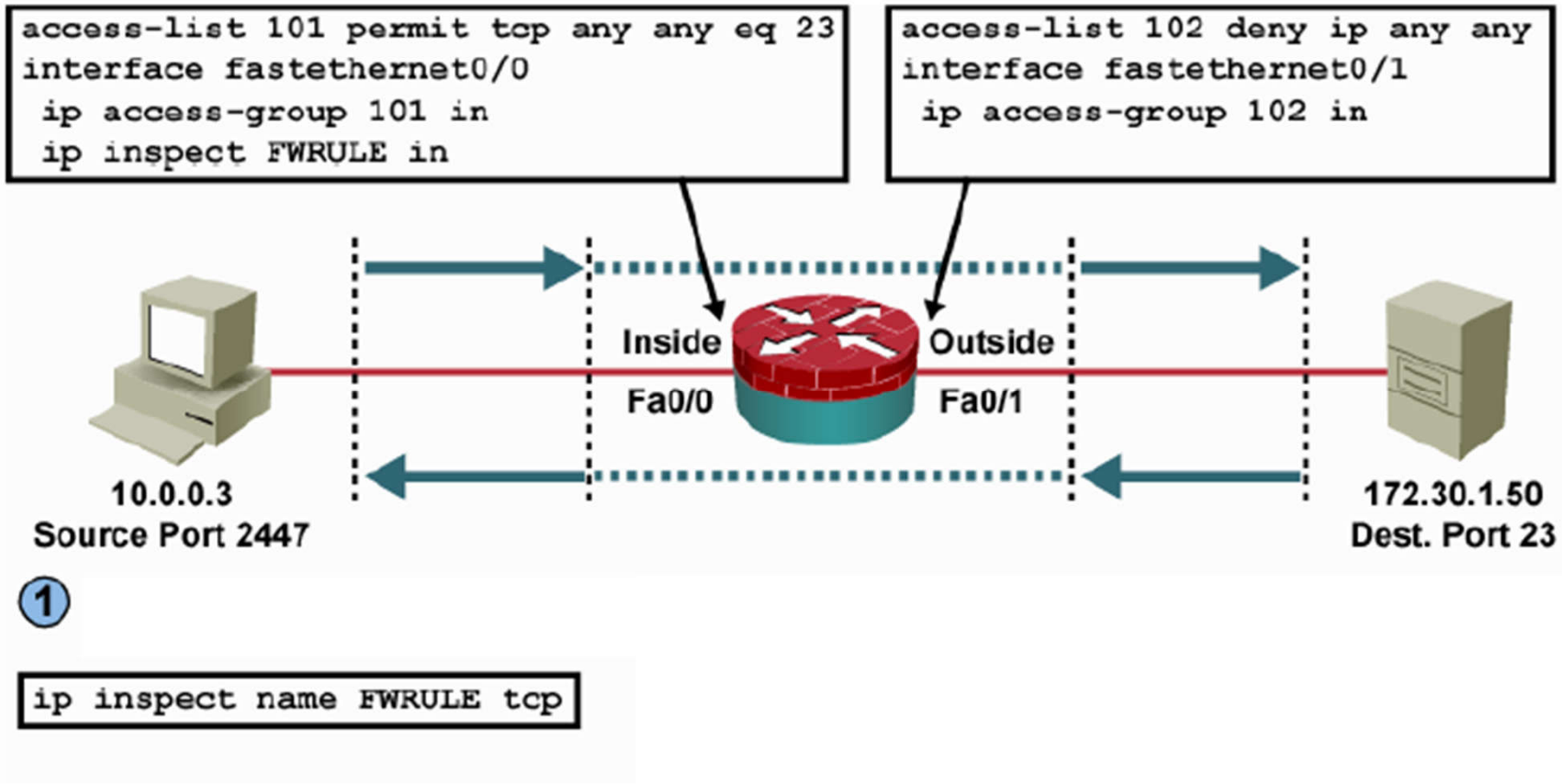
- **C**ontext-**B**ased **A**ccess **C**ontrol
- Mécanisme de filtrage plus évolué que les ACL
  - Filtrage basé sur l'état des connexions
  - Examine la **couche application** pour apprendre et inspecter l'état des sessions TCP et UDP
  - Maintenance, pour chaque connexion, des informations d'état dans des structures de données
- Ce mécanisme permet de supplanter temporairement des instructions d'interdictions présentes dans des ACL
- Utile pour autoriser les connexions LAN → Exterieur ou LAN → DMZ malgré les interdictions des ACL dans le sens contraire.

Principe CBAC



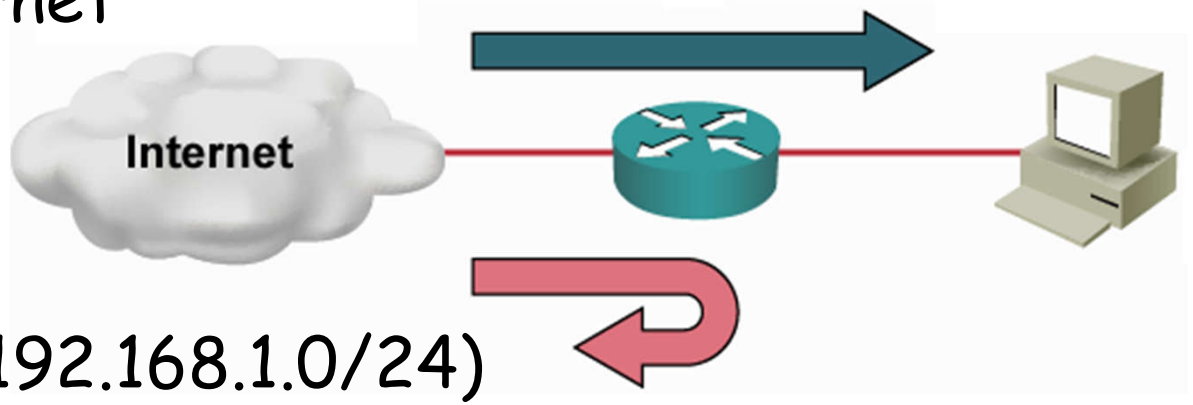
Exemple 1

- Autoriser les connexions Telnet du LAN vers l'extérieur uniquement



Exemple 2

- 1. Empêcher les connexions d'Internet vers le LAN
- 2. Autoriser le ping, le web et le telnet depuis le LAN vers Internet



- Solution (LAN 192.168.1.0/24)
  - ACL 1 . **deny ip any 192.168.1.0 0.255.255.255**
  - **Inconvénient** : cette ACL **devrait bloquer** même le trafic de réponse pour une connexion initié par PC1
  - Solution : **CBAC** →inspecter le trafic de PC1 et permettre les réponses de l'Internet vers PC1
  - Rappel de **l'état** d'une connexion (**stateful**)

Configuration CBAC

- Empêcher les connexions Internet LAN
  - R(config)#acces-list 101 deny ip any 192.168.1.0 0.255.255.255
  - R(config-if)#ip access group 101 in
- CBAC pour le trafic de PC1 vers l'Internet
  - R(config)# ip inspect name lan_internet icmp
  - R(config)# ip inspect name lan_internet http
  - R(config)# ip inspect name lan_internet telnet
- Appliquer cette cbac à l'interface interne
  - R(config-if)#ip inspect lan_internet in
- Le trafic http, telnet et icmp peuvent à partir du LAN contourner l'ACL 101
  - R#show ip inspect sessions
  - R(config)#ip inspect name lan_internet http timeout 5