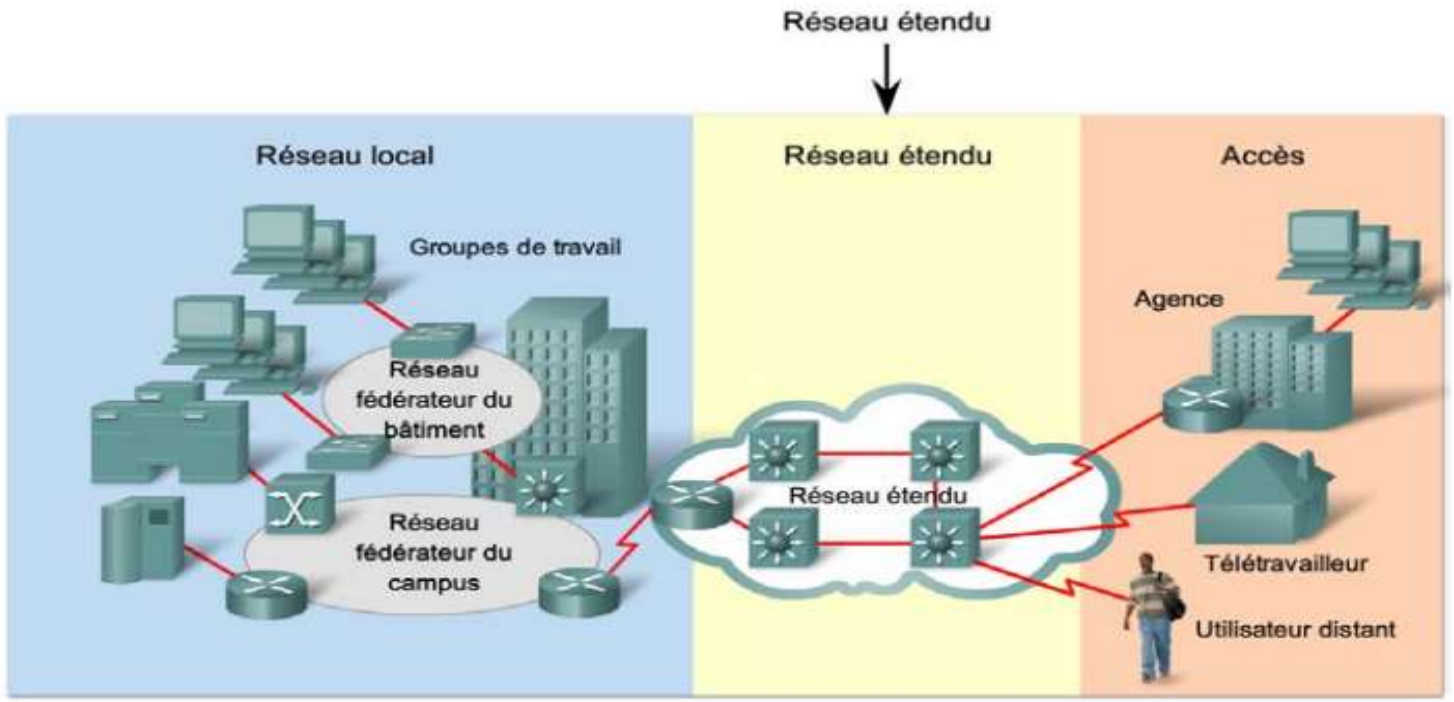
Les Réseaux étendus

Administration avancée

1

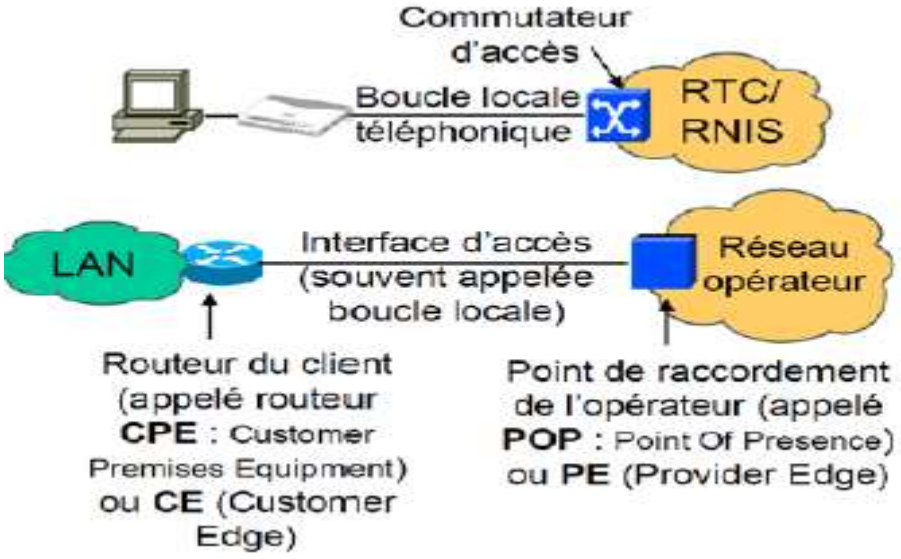
INTRODUCTION

- Un réseau WAN est un réseau de communication de données qui fonctionne au-delà de la portée géographique d'un réseau LAN.
- Exemple des réseaux WAN: FAI

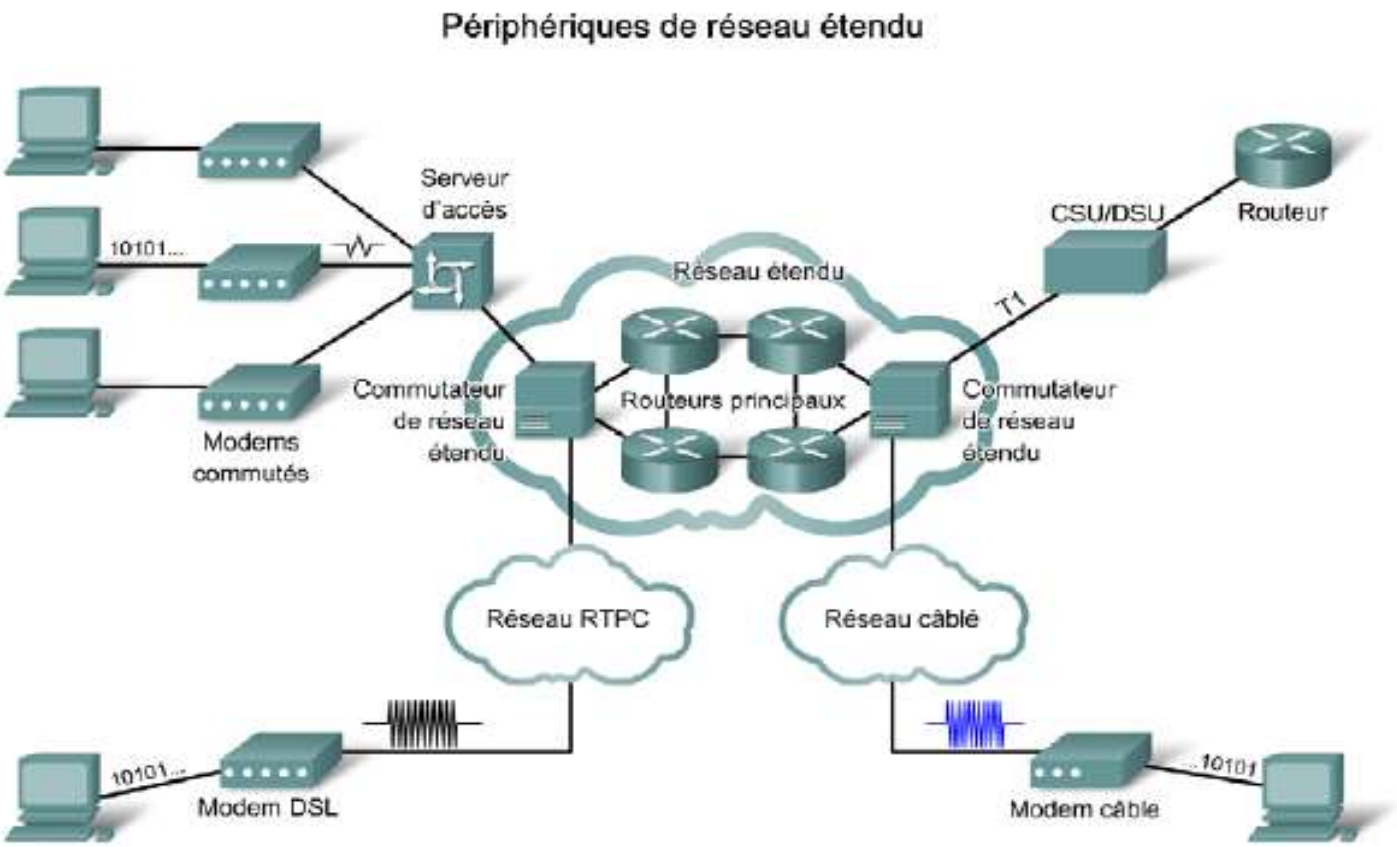


CARACTÉRISTIQUES

- Connecte des périphériques séparés par une zone géographique plus étendu que ne peut couvrir un réseau local;
- Utilise les services d'opérateurs, tels que des compagnies de téléphone ou de câble ou fournisseurs de réseaux;
- Utilise des connexions série pour l'accès aux réseaux



TOPOLOGIES DES RÉSEAUX WANS



- Commutation de circuit : RNIS
- Commutation de paquets : FR, ATM, MPLS => PVC ou SVC

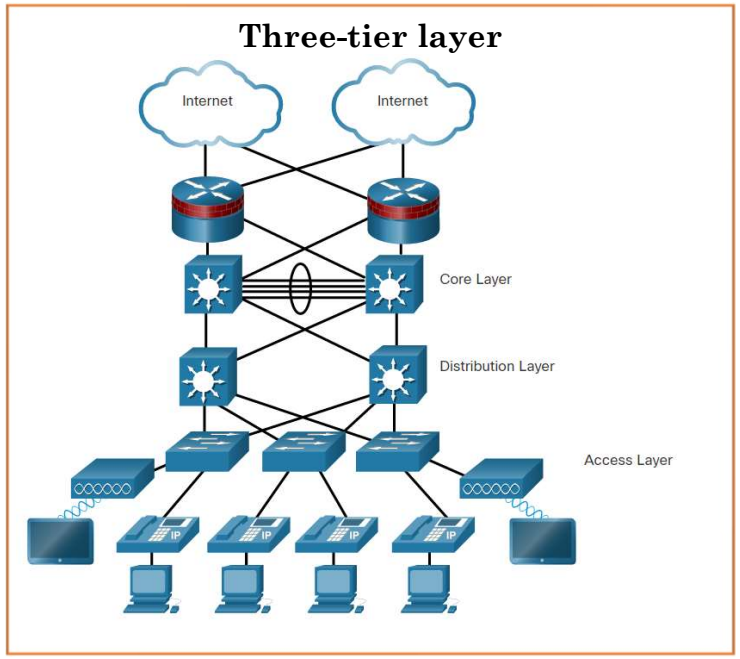
Conception des réseaux

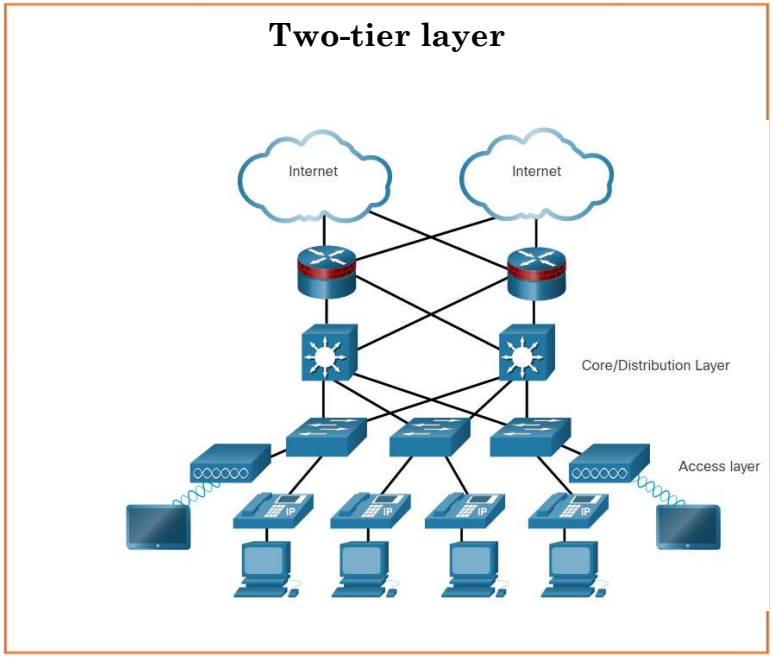
Besoin d'étendre le réseau

- L'utilisation des infrastructures réseau pour des services essentiels
- Besoin des réseaux capables de s'étendre et de s'adapter :
  - Trafic réseau convergent
  - Applications critiques : BdD, Transactionnel
  - Contrôle administratif centralisé
- Modèle de Réseau Hiérarchique : plus simple à gérer et à développer
- La conception de réseau devient modulaire, ce qui facilite l'évolutivité et les performances.

CONCEPTION DES RÉSEAUX HIÉRARCHIQUES

- Les réseaux hiérarchiques utilisent une conception à plusieurs niveaux
- chaque couche jouant un rôle bien défini dans le réseau du campus.





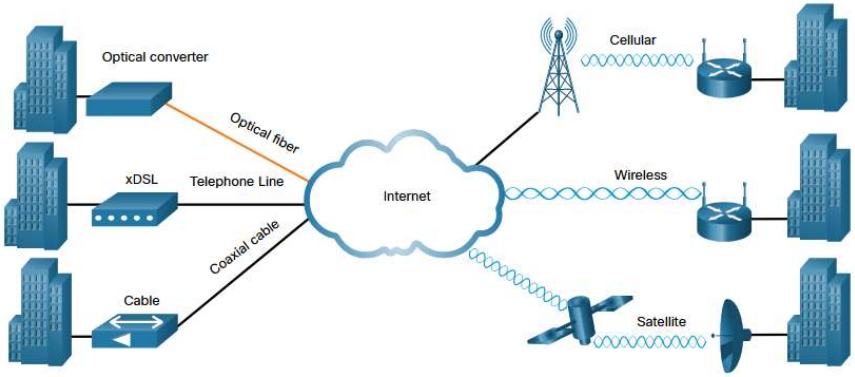
- Recommandation : construire une topologie à étoile étendue à partir d'un bâtiment centralisé.

Conception des réseaux hiérarchiques

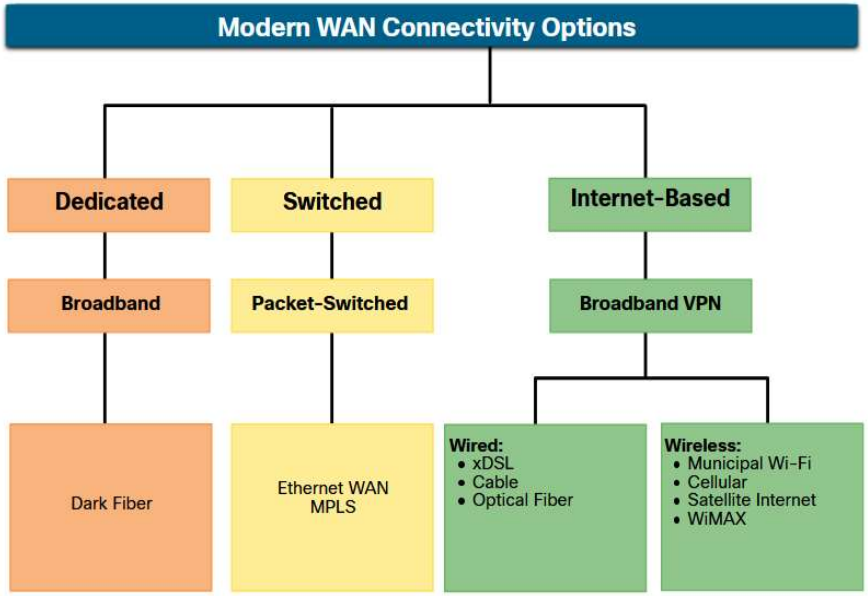
- Couche d'Accès :
  - Fournit un réseau d'accès aux utilisateurs
- Couche de Distribution
  - Implémente les politiques de communications : routage, QoS, Sécurité, gestion de Vlans, etc.
  - Supporte les liens d'agrégation, de la redondance et délimite le domaine de Broadcast
- Couche Backbone (cœur de réseau)
  - Connecte tout le réseau d'entreprise
  - Fournit des connexions à haut-débits
  - Gère facilement les pannes réseaux

Nouvelles Architectures de Connexions

- Actuellement, les entreprises souhaitent avoir des connectivités rapides et flexibles



- Options de connectivités



Routage OSPF

ROUTAGE OSPF : PRINCIPES

- Chaque routeur détient une configuration locale
- Chaque routeur se base sur une métrique (coût) :

$$\text{coût} = [\ 10^{8}\ /\ \text{bande passante en Bit/s}\ ]$$

- Routeur construit son message et le diffuse vers l 'ensemble des routeurs

Un mécanisme de numérotation de l'information limite la propagation des messages et évite la formation des boucles

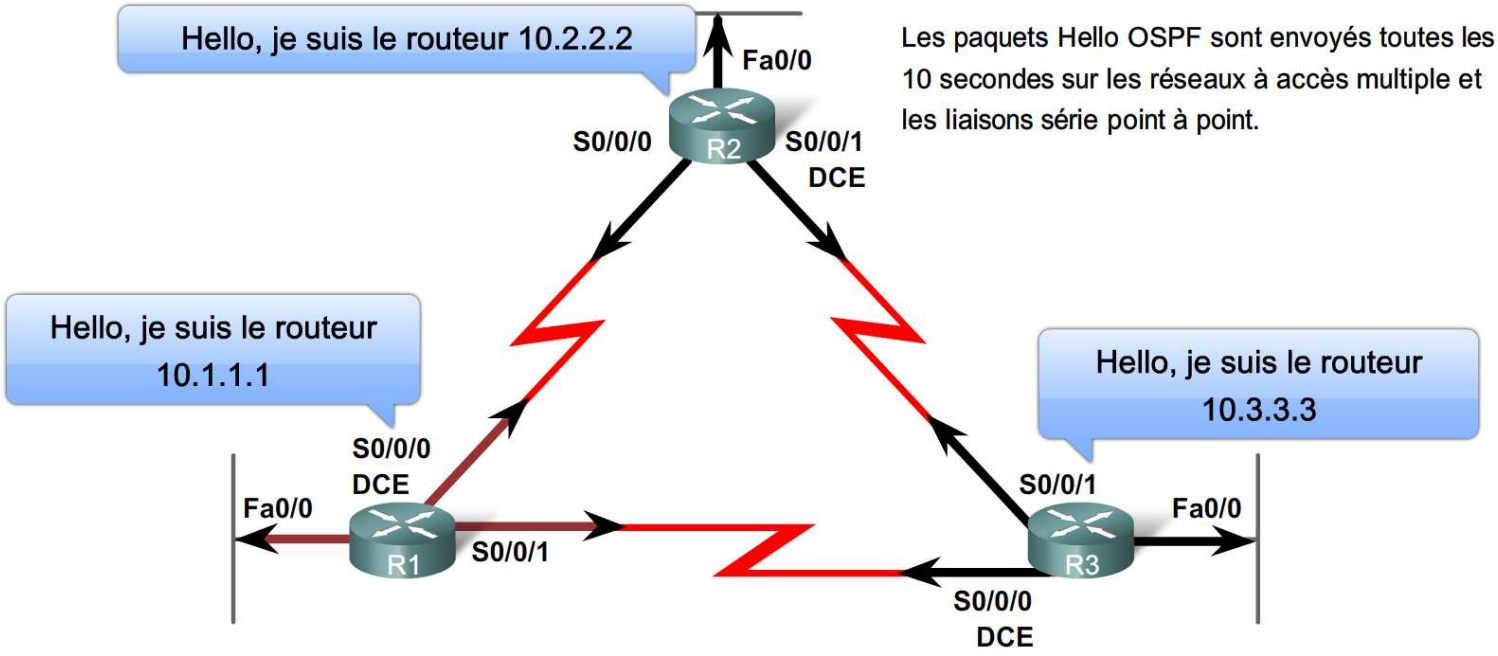
- Routeurs disposent tous des mêmes informations, calculent la route vers l 'ensemble du réseau : algorithme Dijkstra

ROUTAGE OSPF : TYPES DE RÉSEAU

- Le protocole OSPF définit cinq types de réseau :
  - point à point ;
  - accès multiple avec diffusion ;
  - accès NBMA (No-Broadcast Multi-Access);
  - point-à-multipoint ;
  - liaisons virtuelles.

ROUTAGE OSPF: CONTIGUÏTÉ

- Avant la diffusion des tables de routage, OSPF doit d'abord déterminer s'il existe d'autres voisins OSPF sur une de ses liaisons.
- les paquets Hello OSPF sont utilisés (non seulement à ce type de mission).
- Les HELLO contiennent l'ID routeur OSPF du routeur qui envoie le paquet Hello
- La réception d'un paquet Hello OSPF confirme à un routeur qu'il existe un autre routeur OSPF sur la liaison.
- OSPF établit ainsi des ***contiguïtés*** avec le voisin.



Les paquets Hello OSPF sont envoyés toutes les 10 secondes sur les réseaux à accès multiple et les liaisons série point à point.

Mise en correspondance des valeurs d'interface des deux routeurs afin de créer une contiguïté

Intervalle Hello	=	Intervalle Hello
Intervalle Dead		Intervalle Dead
Type de réseau		Type de réseau

PROCESSUS D'ÉLECTION

- Le routeur désigné va permettre une réduction du nombre d'échange nécessaires pour que les bases de données soient à jour sur chacun des routeurs d'un réseau.

- Le Protocole d'élection se base sur les éléments suivante :

  - La priorité la plus grande sur le réseau physique
  -

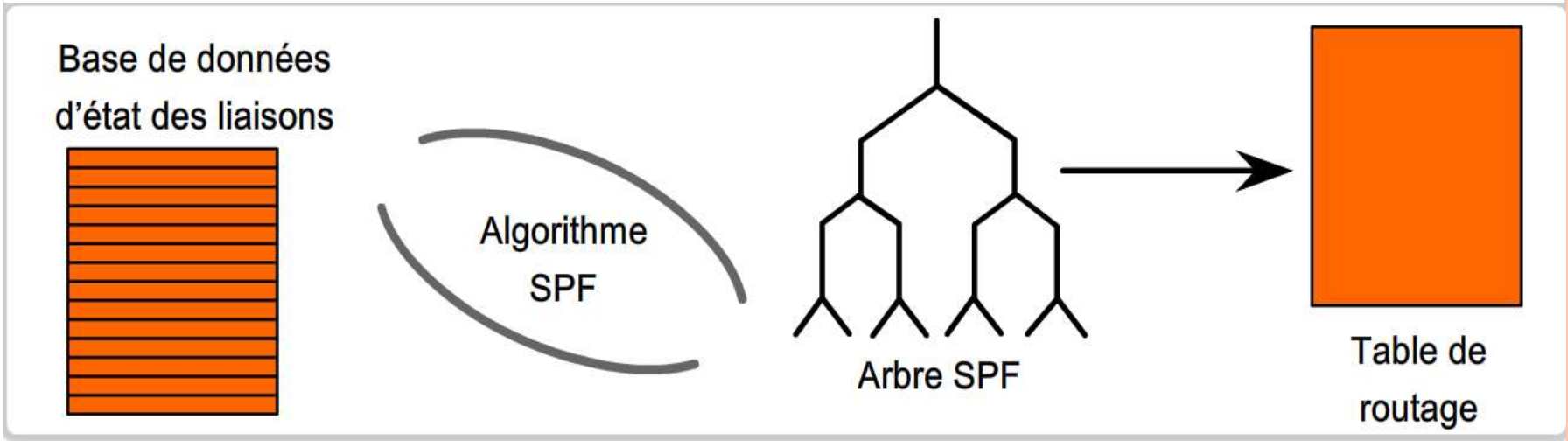
- Le retour qui démarre, émet le paquet Hello avec le champ routeur désigné et de secours à 0

- Chaque routeur recherche sa propre adresse dans les paquets Hello émis par les autres routeurs pour s'assurer du bon fonctionnement du réseau : communication Symétrique.

- Le routeur peut ensuite mettre à jour sa base de données en interrogeant le routeur désigné.

ALGORITHME OSPF

- Chaque routeur OSPF conserve une base de données d'état des liaisons contenant les LSA (Link State Advertisement)) reçues de tous les autres routeurs.

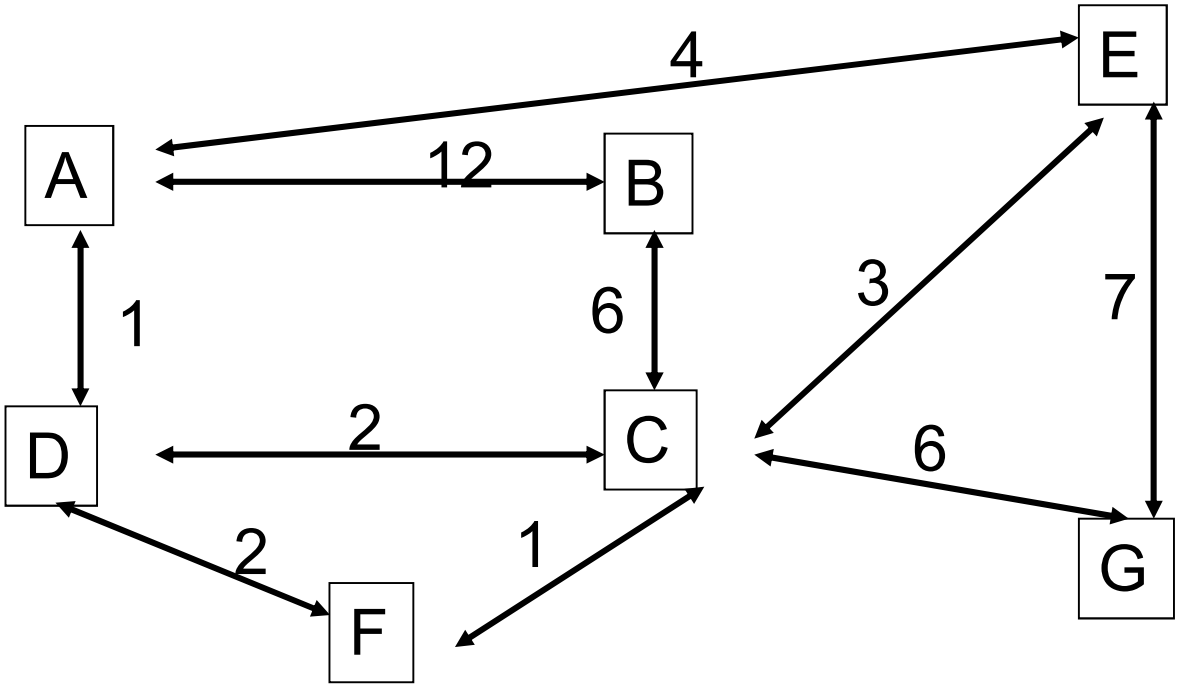


- À partir de l'arbre des plus court chemins, les routeurs construisent la table de routage.

Comme les routeurs ne démarrent pas au même instant, ils ont besoins des informations sur le réseau global.

-Le routeur qui démarre à besoin :

- d'identifier ses voisins immédiats,
- de trouver parmi ses voisins le « designated router » et celui de secours « backup designated router » qui sont élu sur chaque réseau
- de dialoguer avec le routeur désigné pour acquérir sa base de données



CONFIGURATION DE OSPF

- Activer le processus OSPF

R(config)#router ospf X
R(config-router)# network zzzz netmask_wilcard area N°

- Les commandes de dépannage OSPF :
  - ***show ip protocols***
  - ***show ip ospf***
  - ***show ip ospf interface***

ACCESS-LIST

Introduction

Une liste de contrôle d'accès est un ensemble séquentiel d'instructions d'autorisation ou de refus, qui s'appliquent aux adresses ou aux protocoles de couche supérieure.

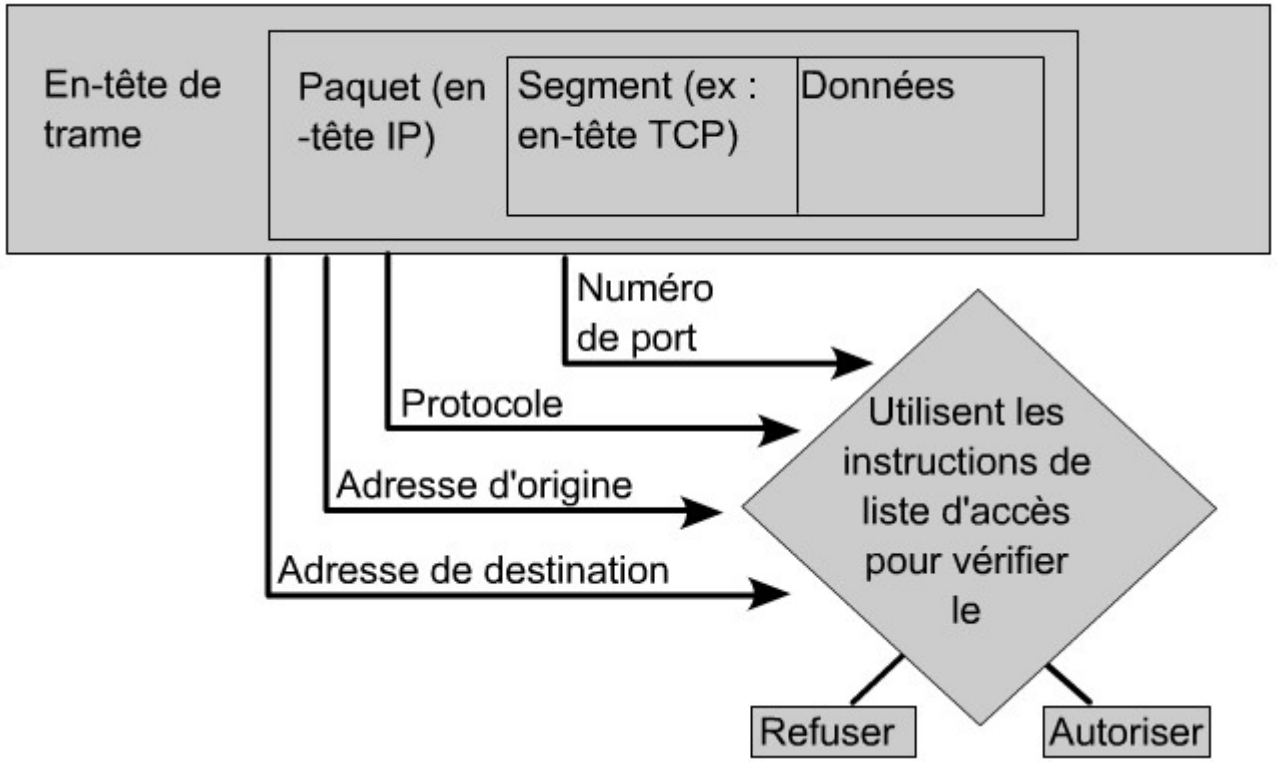
Une liste d'accès définit les conditions pour qu'un paquet puisse franchir un routeur. Les informations contenues dans ces listes portent :

- sur le numéro du protocole de niveau 3, les N° de port, …
- d'autres informations dans le paquet comme les drapeaux TCP;
- le type de la règle : autoriser ou refuser l'interaction

Les listes d'accès filtrent le trafic réseau en commandant aux interfaces d'un routeur d'acheminer ou de bloquer des paquets routés.

Le routeur examine chaque paquet afin de déterminer s'il doit l'acheminer ou le rejeter en fonction des conditions précisées dans la liste de contrôle d'accès

Introduction



Les listes de contrôle d'accès doivent être définies en fonction d'un protocole, d'une direction ou d'une interface.

Pour contrôler le flux du trafic sur une interface, une ACL doit être définie pour chaque protocole activé sur l'interface. Les ACL contrôlent le trafic dans une seule direction à la fois sur une interface

Introduction

Voici les principales raisons justifiant la création de listes de contrôle d'accès :

- Limiter le trafic réseau et accroître les performances réseau.
- Déterminer le type de trafic qui sera acheminé, ou bloqué, au niveau des interfaces de routeur.
- Autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.
- Filtrer certains hôtes afin de leur accorder, ou de leur refuser, l'accès à une section de réseau.
- Accorder, ou refuser, aux utilisateurs la permission d'accéder à certains types de fichiers ou services, tels que FTP ou HTTP.

Création de listes de contrôle d'accès : ACL

Les ACL sont créées en mode de configuration globale. Il existe différents types de listes de contrôle d'accès : standard, étendues, IPX et AppleTalk.

Au moment de configurer les listes de contrôle d'accès d'un routeur, vous devez identifier chaque liste en lui attribuant un numéro unique.

Ce numéro identifie le type de liste d'accès créé et doit être compris dans la plage de numéros valide pour ce type

Protocole	Plage
IP standard	1-99, 1300-1999
IP étendu	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
IPX étendu	900-999
Protocole IPX Service Advertising	1000-1099

Les règles de base suivantes doivent être respectées lors de la création et de l'application des listes d'accès :

- Une liste d'accès par direction et par protocole.

- Les listes d'accès standard doivent être appliquées le plus près possible de la destination.

- Les listes d'accès étendues doivent être appliquées le plus près possible de la source.

- Pour faire référence à une interface d'entrée ou de sortie, placez-vous à l'intérieur du routeur en regardant l'interface en question.

- Les instructions sont traitées dans l'ordre depuis le début de la liste
- jusqu'à la fin jusqu'à ce qu'une correspondance soit trouvée. Si aucune correspondance n'est détectée, le paquet est refusé.

- Il existe un refus implicite deny any à la fin de toutes les listes de contrôle d'accès. Cela n'apparaît pas dans la liste de configuration.

Création de listes de contrôle d'accès : ACL standard

Les commandes pour utiliser les ACLs sont :

- access-list {N° de la liste}
- deny
- permit
- {protocole} access-groupe {N°de la liste} (in ou out)

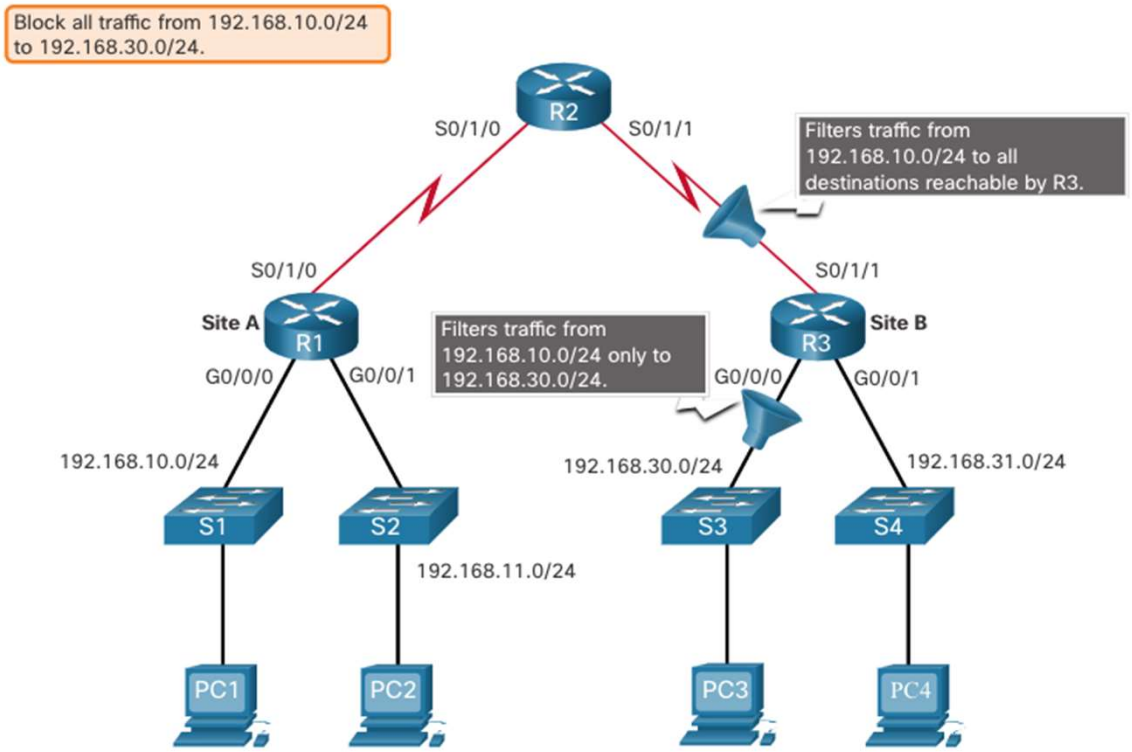
```
Router(config)#access-list 2 deny 172.16.1.1
Router(config)#access-list 2 permit 172.16.1.0 0.0.0.255
Router(config)#access-list 2 deny 172.16.0.0 0.0.255.255
Router(config)#access-list 2 permit 172.0.0.0
0.255.255.255
Router(config)#interface e0
Router(config-if)#ip access-group 2 in
```

- access-list n° de la list (deny ou permit) @IP **~masque**

-access-list 1 permit 0.0.0.0 255.255.255.255 (masque générique)
ou access-list 1 permit any

ACL Standard : Exemple

- on souhaite refuser tout le trafic depuis le réseaux 192.168.10.0/24 vers le réseau 192.168.30.0/24 de R3




```
access-list 2 deny 192.168.10.0 0.0.0.255
```

Création de listes de contrôle d'accès : ACL étendue

Les listes d'accès étendues sont utilisées plus souvent que les listes d'accès standard car elles fournissent une plus grande gamme de contrôle.

Les listes d'accès étendues vérifient les adresses d'origine et de destination du paquet, mais peuvent aussi vérifier les protocoles et les numéros de port

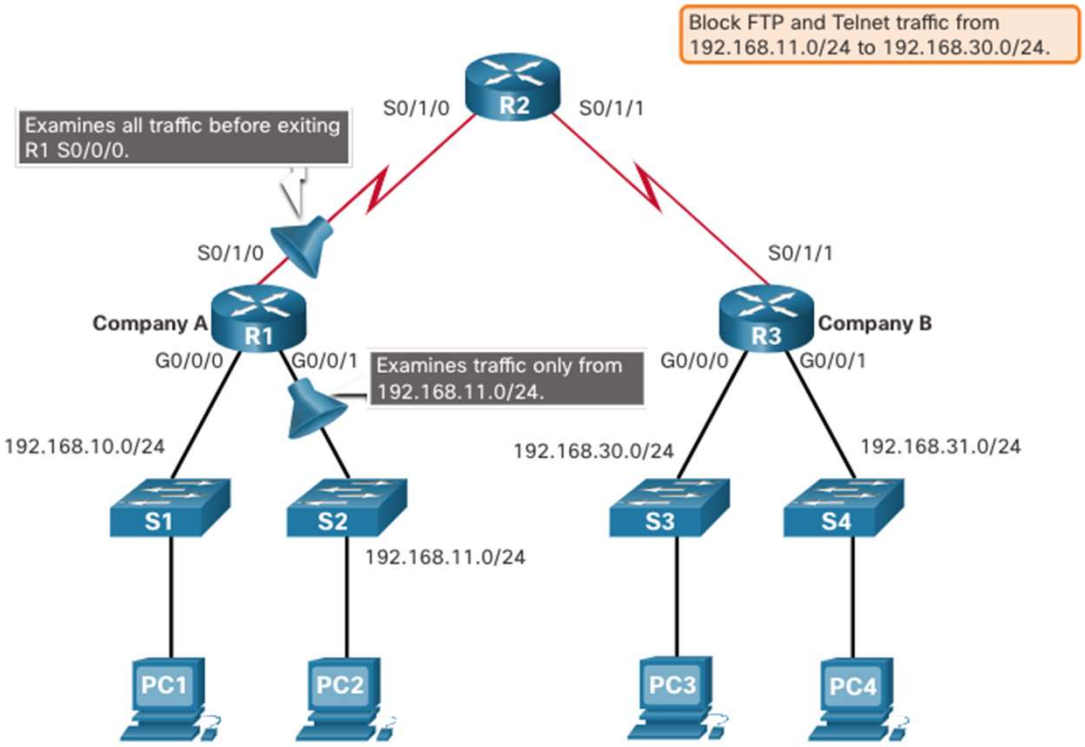
Pour une même liste de contrôle d'accès, plusieurs instructions peuvent être configurées. Chacune de ces instructions doit contenir le même numéro de liste d'accès pour que toutes les instructions soient associées à la même liste de contrôle d'accès

```
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data
```

- Les plages de numéros de liste d'accès 100-199 et 2000 - 2699
- Adresse IP de destination source
- Numéro de protocole de couche 4
- Application au port le plus proche de l'hôte source

ACL Etendue : Exemple

- on souhaite refuser le trafic « telnet » depuis le réseaux 192.168.11.0/24 vers le réseau 192.168.30.0/24 de R3




```
access-list 110 deny 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 eq 23
```

EXEMPLES – ACLS ÉTENDUES

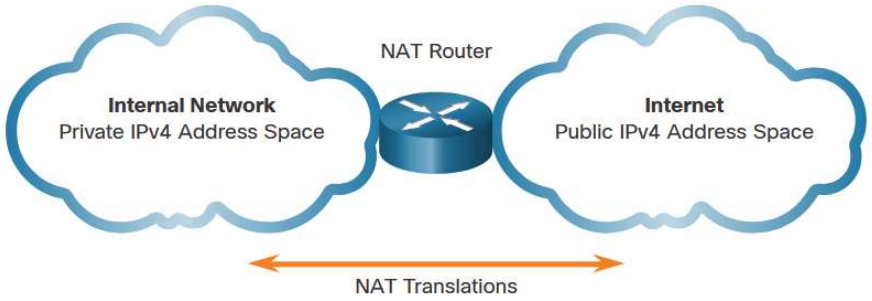
- ACL **PERMIT-PC1** permet à PC1 (192.168.10.10) un accés TCP : FTP, SSH, Telnet, DNS , HTTP et HTTPS.
- ACL **REPLY-PC1** permet le retour du trafic au PC1.
- ACL **PERMIT-PC1** est appliquée en entrée, par contre l'ACL **REPLY-PC1** est sur l'outbound de l'interface G0/0/0 du routeur.

```
R1(config)# ip access-list extended PERMIT-PC1
R1(config-ext-nacl)# Remark Permit PC1 TCP access to internet
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 20
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 21
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 22
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 23
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 53
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 80
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 443
R1(config-ext-nacl)# deny ip 192.168.10.0 0.0.0.255 any
R1(config-ext-nacl)# exit
R1(config)#
R1(config)# ip access-list extended REPLY-PC1
R1(config-ext-nacl)# Remark Only permit returning traffic to PC1
R1(config-ext-nacl)# permit tcp any host 192.168.10.10 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0/0
R1(config-if)# ip access-group PERMIT-PC1 in
R1(config-if)# ip access-group REPLY-PC1 out
R1(config-if)# end
R1#
```

Configuration NAT : Network Address Translation

INTRODUCTION

- Réseaux d'entreprise utilisent les réseaux IPv4 privés.
- Réseaux non routable sur internet
- NAT permet la translation d'adresse privée en adresse publique



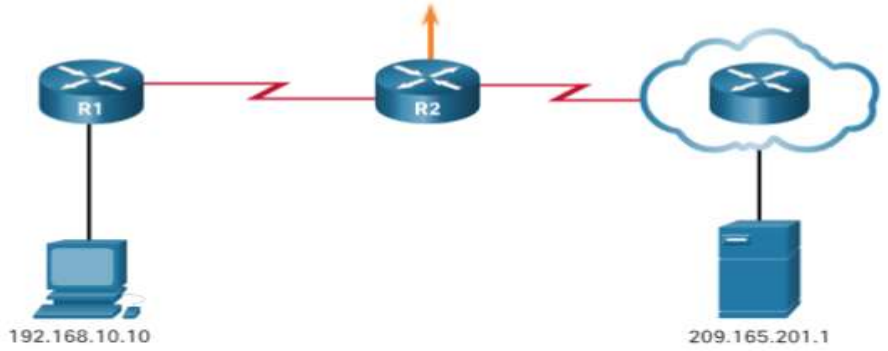
Class	Activity Type	Activity Name
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

NAT - FONCTIONNEMENT

- Besoin de la table NAT
- Terminologie :
  - Inside local address : adresse source, qui sera translatée
  - Inside Global address: adresse publique pour translater
  - Outside Local address : adresse de destination vue depuis l'intérieur du réseau
  - Outside Global addresse : adresse de destination vue depuis l'extérieur du réseau

NAT Table

Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



TYPES DE NAT

- types de méthodes de NAT:

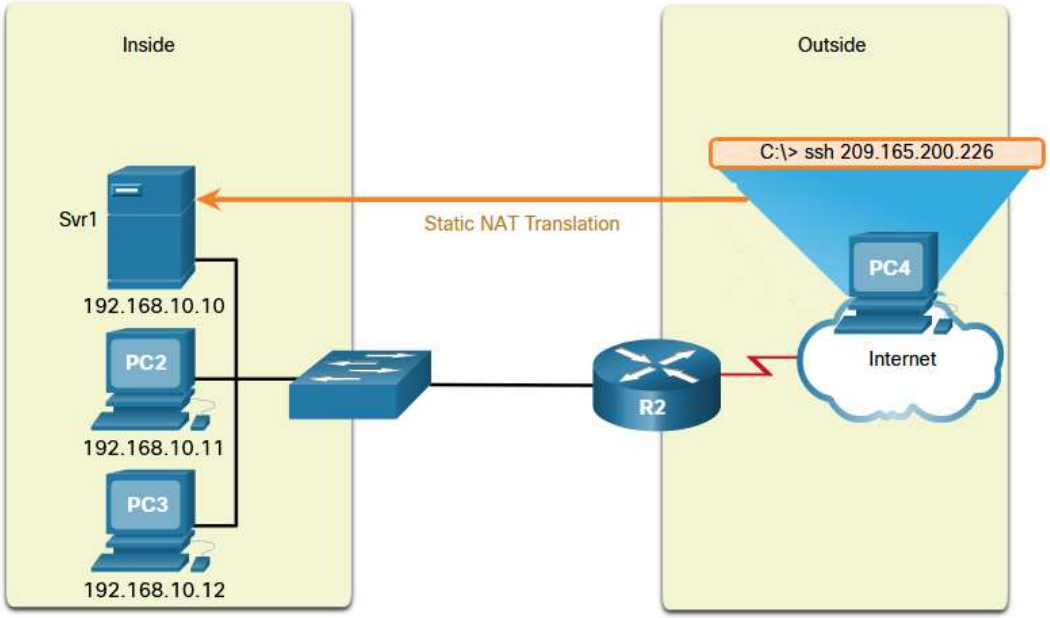
  - Translation dynamique NAT: Translate les adresses sources du réseau privé en un ensemble d'adresses publiques (pool)

  - Translation PAT: (Many-to-one translation), toutes les dresses du réseau privé sont représenté par une seule adresse publique. La plupart de temps on utilise l'interface « *outside* »

  - Translation NAT statique: fournit une adresse permanente de type one-to-one. Il permet au réseau public par exemple internet d'accéder au ressource interne comme un serveur web.

NAT STATIQUE

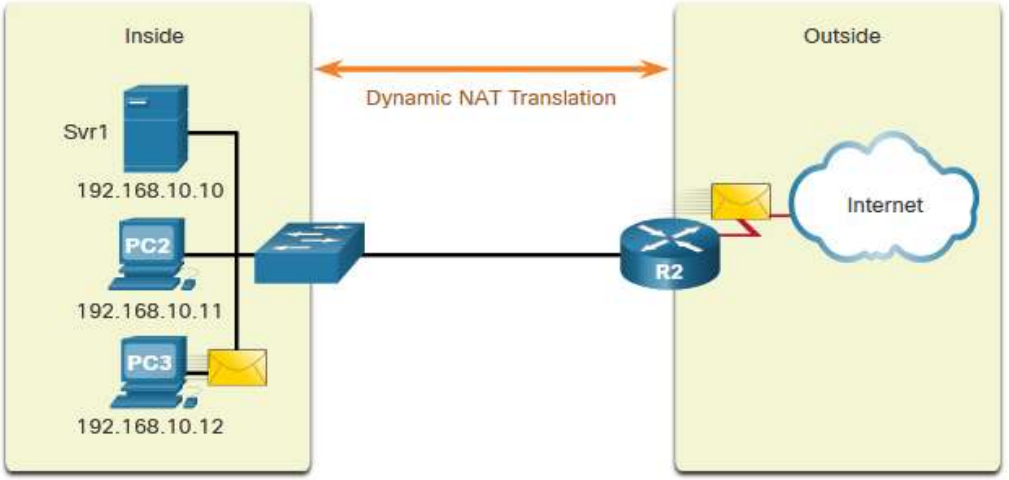
- Utilise un mappage one-to-one pour accéder une ressource inaccessible depuis l'internet
- La configuration reste permanente toute la durée de vie du routeur ou firewall



Static NAT Table	
Inside Local Address	**Inside Global Address - Addresses reachable via R2**
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

NAT Dynamique

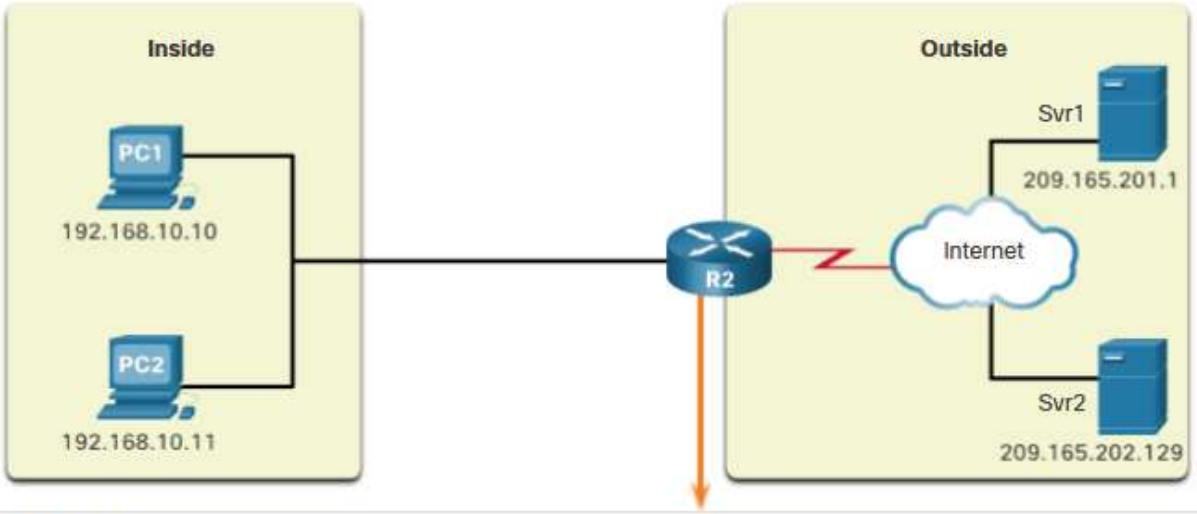
- NAT dynamique utilise un pool d'adresses IP publiques assignées à chaque réception d'adresse IP privée par le routeur



IPv4 NAT Pool	
Inside Local Address	**Inside Global Address Pool - Addresses reachable via R2**
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230

PAT – Port Address Translation

- PAT appelé aussi NAT overload utilise un mappage many-to-one (multiple adresses privées mappées en une seule adresse publique)



NAT Table with Overload

Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global IP Address
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80