Concevoir un réseau informatique multi-sites

Contexte Général

- Etude et fourniture de l'architecture de deux entreprises dans l'e-commerce : UC Exchange et ABC Conseil
- Les deux entreprises sont présentes dans l'Est de la France : Strasbourg, Nancy et Metz.
- Toutes les succursales ont le même gabarit :
- Le siège social comptera 4 services : service informatique, la direction, service financier et salle des serveurs (DNS, DHCP, Web/DNS secondaire, mail, AD)

Besoin Architectural

- Les autres sites compteront 4 services dont une la salle des serveurs (DHCP, AD)
- Tous les sites doivent être équipés informatiquement
  - L'adressage IP LAN fourni est la suivante :
  - UC exchange : 10.242.xy.0/17
  - ABC Conseil : 10.252.xy.0/18

Où “x” représente le numéro du site et “y” le numéro de Vlan dans le site “x”

Besoin Architectural

- En tant qu'Architecte réseaux :
  - Proposer des solutions en adéquation avec les besoins de l'entreprise : services, ressources, etc.
  - Proposer les bonnes solutions réseaux pour dimensionner l'usage des réseaux : réseaux inter-sites

Prérequis

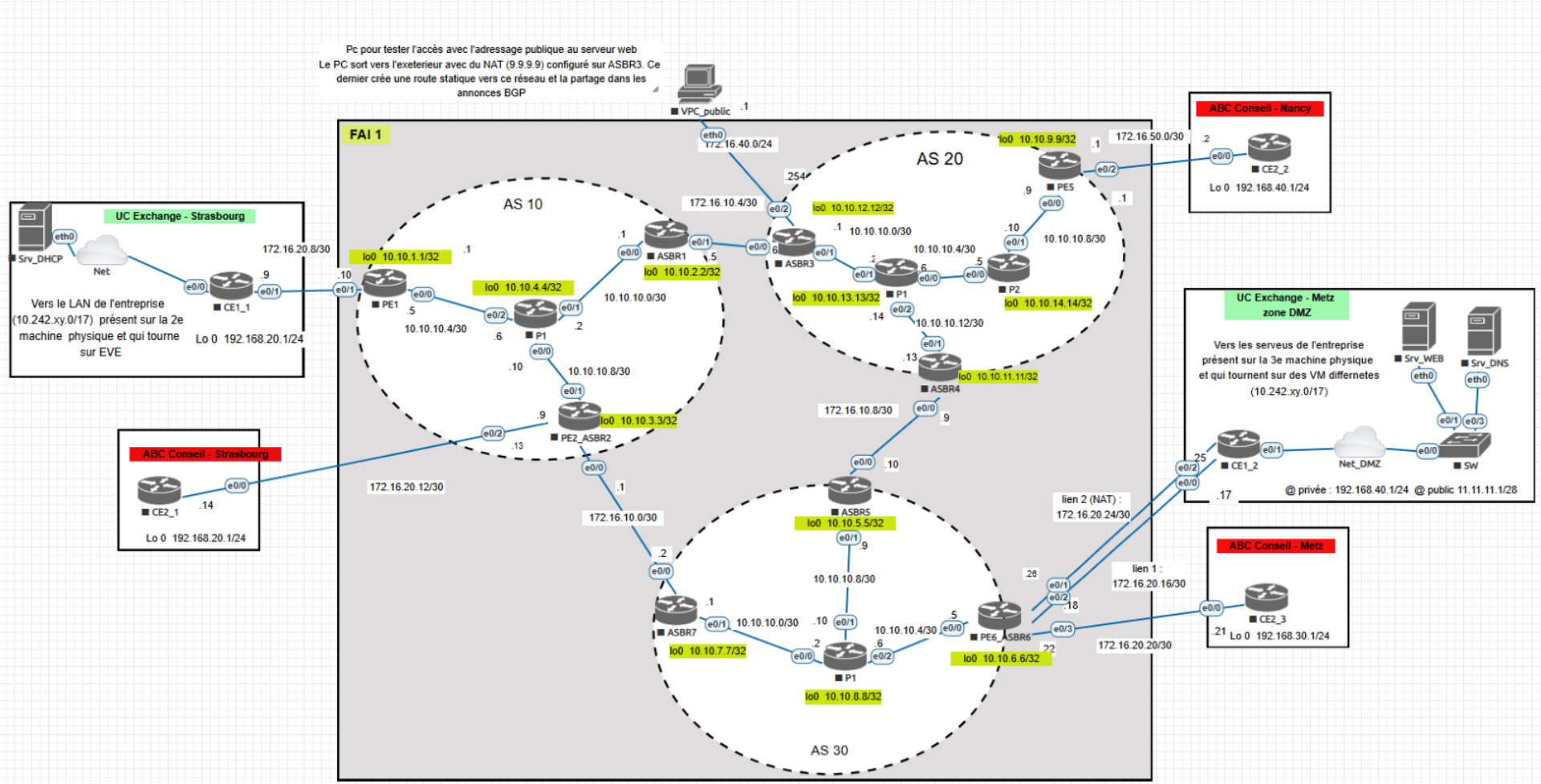
Compétences à valider :

- **R3.01 | Réseaux de campus**
- **R3.02 | Réseaux opérateurs**
- **R3.03 | Services réseaux avancés**
- **R3.04 | Services d'annuaires**
- R3.11 | Anglais professionnel 1
- R3.12 | Expression-Culture-Communication professionnelles : Savoir collaborer
- R3.13 | Projet Personnel et Professionnel

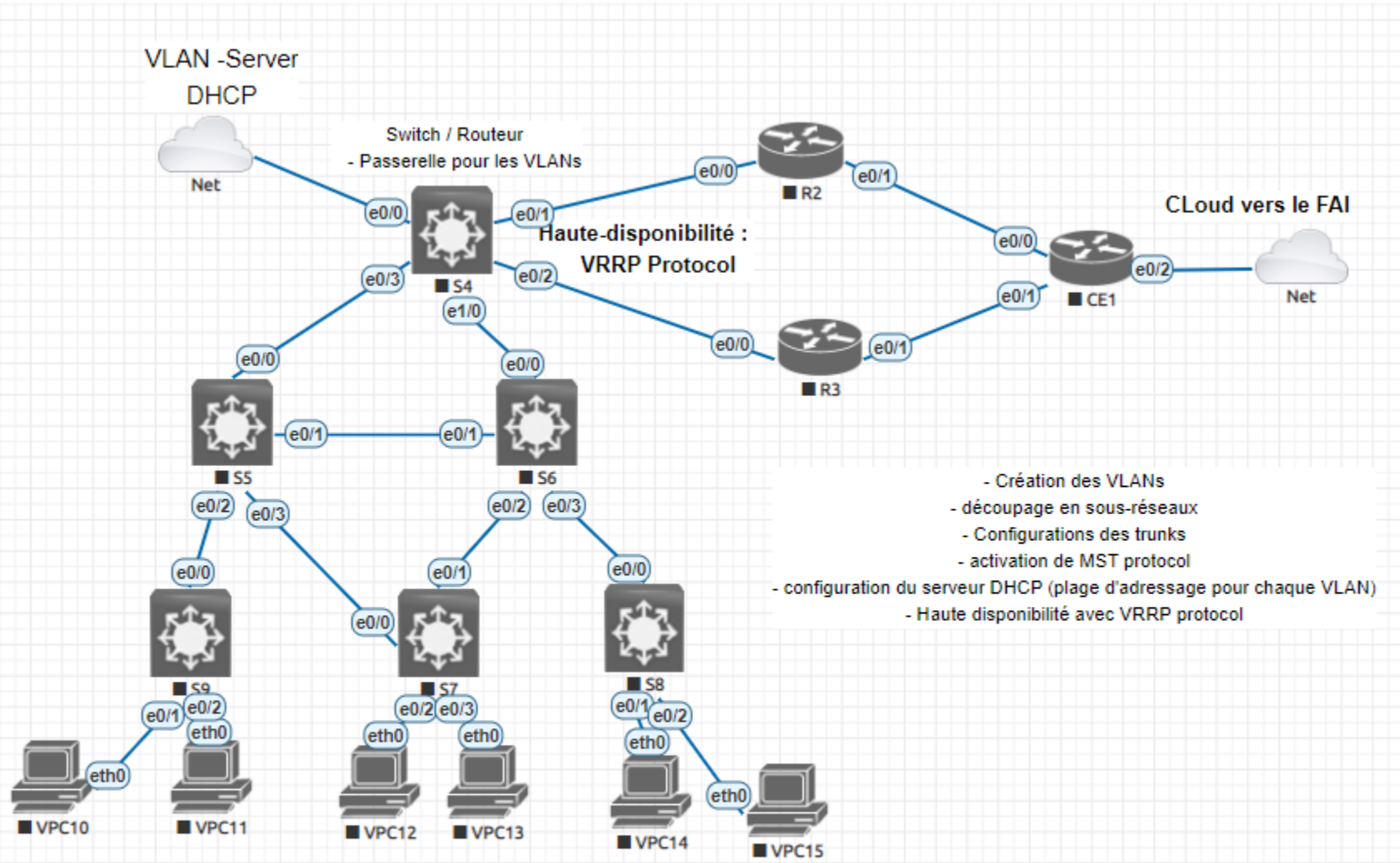
Contexte Précis

- Groupes de Trois étudiant(e)s
- Etude de l'architecture globale
- Définir les besoins de chaque entreprise
- Valider les compétences

Architecture des sites



Architecture LAN

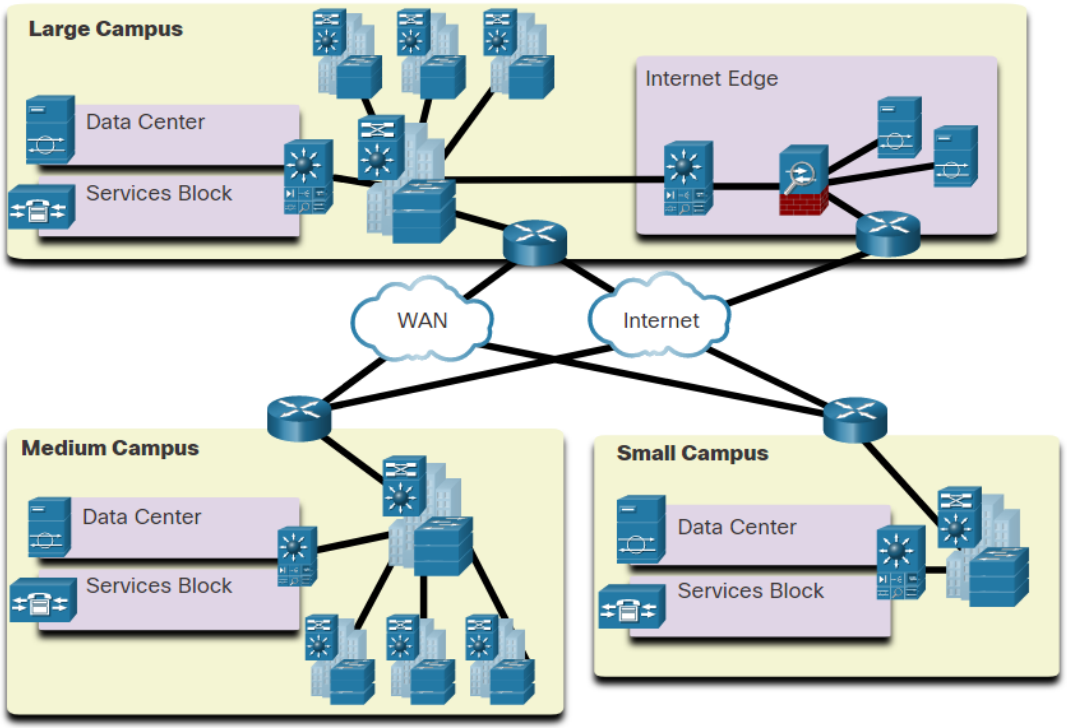


Validation de l'infrastructure

- Le rendu en trois partie :
  - Partie LAN
  - Partie mise œuvre des services réseau
  - Partie réseau opérateur

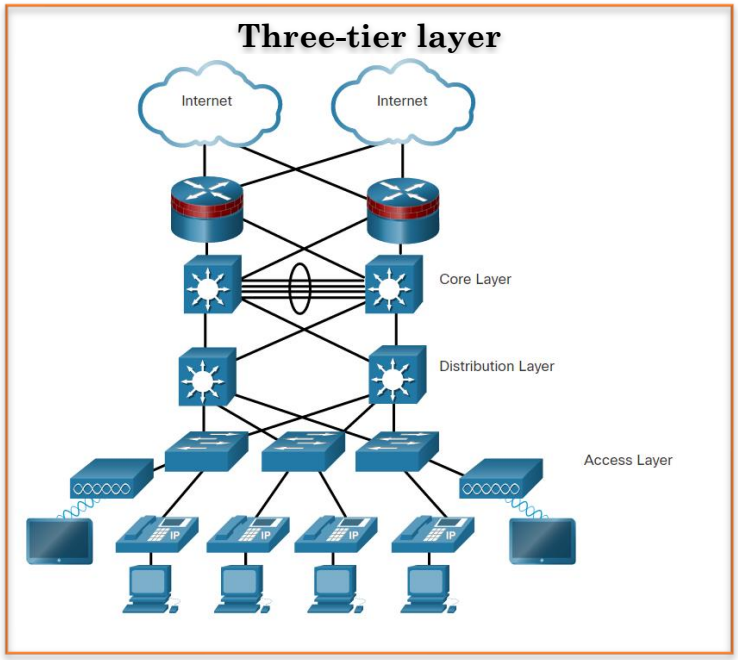
Partie LAN : Architecture Hiérarchique

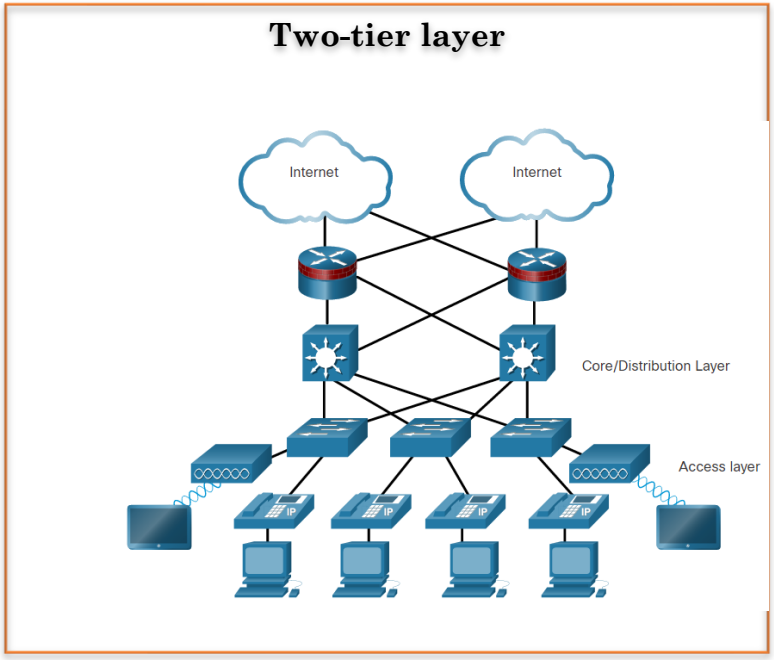
- Modèle de Réseau Hiérarchique : plus simple à gérer et à développer
- La conception de réseau devient modulaire, ce qui facilite l'évolutivité et les performances.



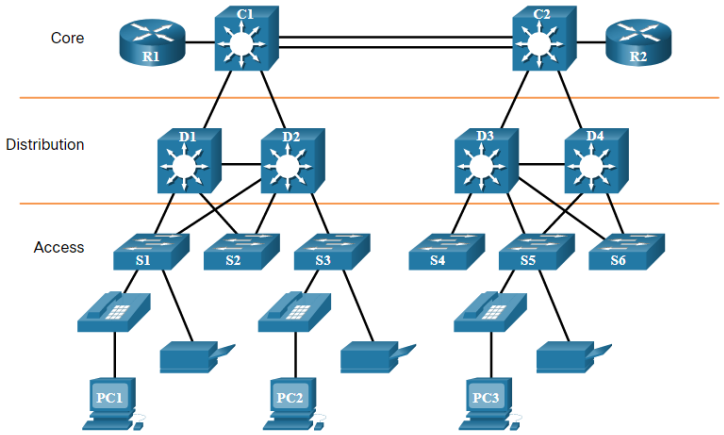
Conception des réseaux hiérarchiques

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





Rôle des Switch



- Les réseaux ont fondamentalement changé, passant d'un réseau plat à des réseaux commutés dans un réseau hiérarchique.
- Un réseau local commuté offre davantage de flexibilité, de gestion du trafic, de qualité de service et de sécurité.
- Un réseau local commuté peut également prendre en charge les réseaux sans fil et d'autres technologies telles que la téléphonie IP et les services de mobilité

Évolutivité - Scalability

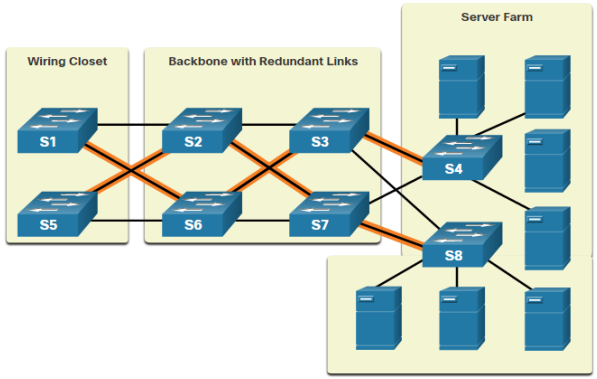
- L'évolutivité (facteur d'échelle) est le terme qui désigne un réseau qui peut se développer sans perdre en disponibilité et en fiabilité.

- Les concepteurs de réseaux doivent développer des stratégies pour permettre au réseau d'être disponible et de s'étendre efficacement et facilement.
- Ceci est accompli en utilisant :
  - La redondance
  - Utilisation des liens multiples
  - Protocole de routage évolutif

Administration Avancée

- spanning tree
- Haute disponibilité
- NAT

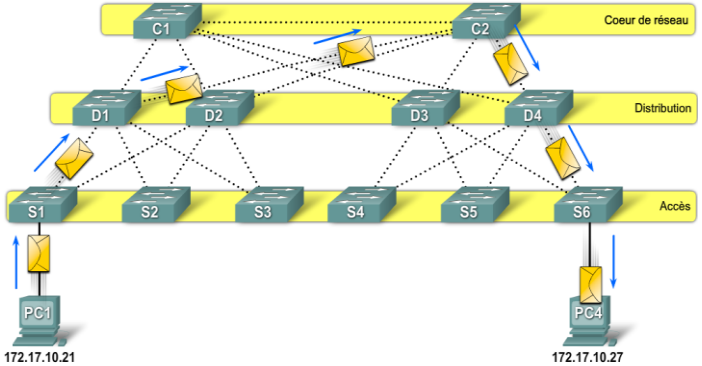
La Rodondance



- La redondance peut empêcher l'interruption des services du réseau en minimisant la possibilité d'un point de défaillance unique :
  - Installant des équipements en double
  - Fournissant des services de basculement pour les dispositifs critiques
- Les chemins redondants offrent des chemins physiques alternatifs pour que les données traversent le réseau, ce qui favorise la haute disponibilité.
  - Les chemins redondants dans un réseau Ethernet peuvent provoquer des boucles logiques de couche 2.
  - C'est pourquoi le protocole STP (Spanning Tree Protocol) est nécessaire.

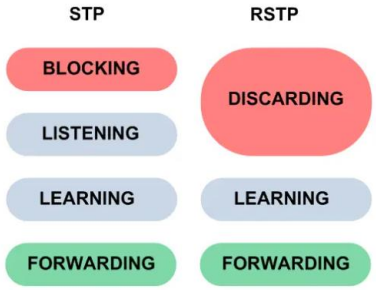
SPANNING-TREE

- Dans une conception hiérarchique, la redondance est assurée au niveau de la couche distribution et de la couche cœur de réseau via des chemins de substitution.



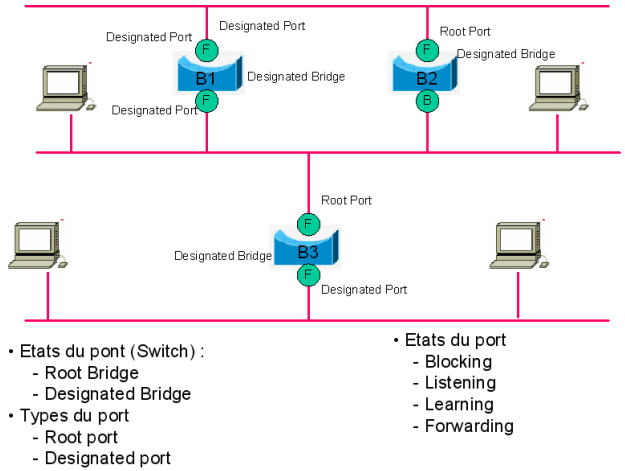
- La redondance offre une grande liberté de choix des chemins dans un réseau ; elle permet d'assurer la transmission des données même si un chemin ou un périphérique est défaillant dans la couche de distribution ou la couche cœur de réseau.

SPANNING-TREE : RPVST & MST PROTOCOLS

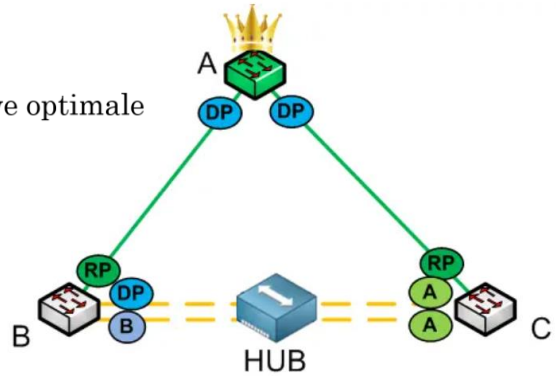


- STP protocol : Rappel
- RSTP (IEEE 802.1w)

  Rapid Spanning Tree Protocol
  - STP : problème de convergence en cas de panne – 50 secondes
- RSTP – Améliorations :
  - Temps de convergence est de **6 secondes**
  - Apparition de nouvelles terminologies :
    - **Alternate Port :** Remplace le Root Port en cas de panne
    - **Backup Port :** Remplace le Designated Port en cas de panne



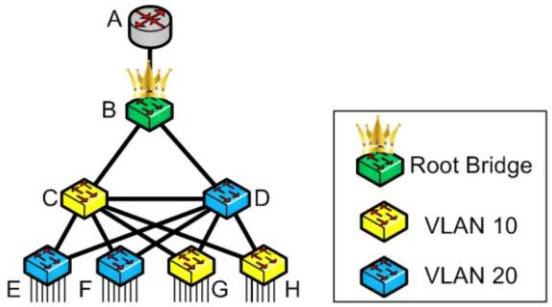
- Le but chercher une route alternative optimale en cas de panne du Root Port



RPVST Protocol

- RPVST : Rapid Per Vlan STP
- Basé sur le protocole RSTP et le protocole PVST+ :

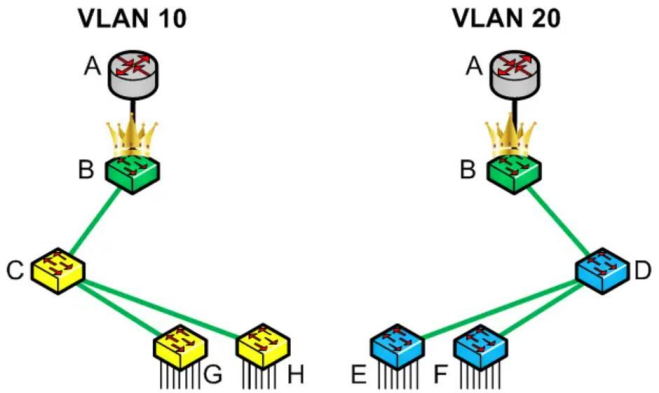
  Un Vlan = Une instance Spanning Tree



Architecture logique :

Echange de messages BPDU

Dans chaque instance



CONFIGURATION

- Création des VLANs et configuration des Trunks entre les Switchs

- Activer le mode RPVST:

  spanning-tree mode rapid-pvst

- Choisir un switch « Root Bridge »

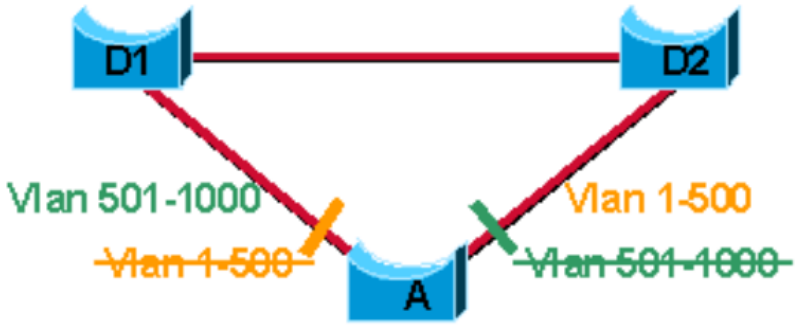
  spanning-tree vlan x,y root primary

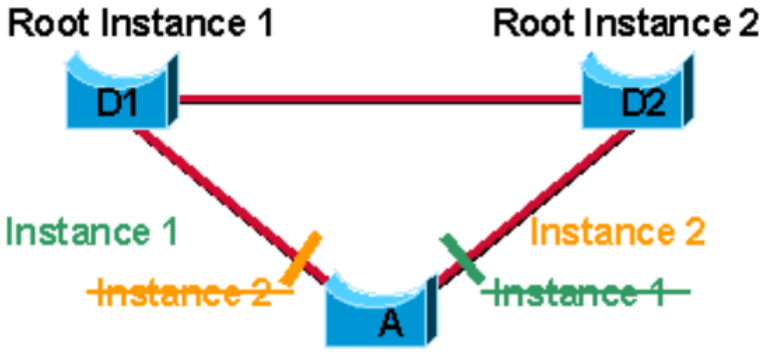
  spanning-tree vlan x,y priority Z

Z : représente une valeur qui est un multiple de **4096**

Multiple Spanning Tree (MST)Protocole

- Basé sur le protocole RSTP
- Permet à plusieurs VLANs d'être mappé sur une seule instance de Spanning-Tree
  - Réduction du nombre d'instances, Root Bridges, root ports
  - Réduction des messages de contrôle : BPDU dans le réseau

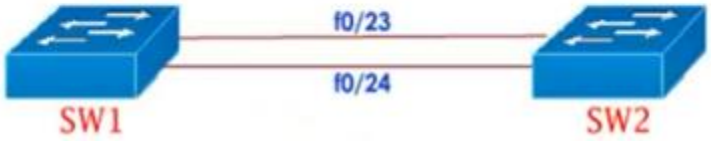




CONFIGURATION

SW1 /SW2

```
SWx(config)#spanning-tree mode mst
SWx(config)# spanning-tree mst configuration
SWx(config-mst)# revision 1
SWx(config-mst)# name CCIE
SWx(config-mst)# instance 1 vlan 10,20
SWx(config-mst)# instance 2 vlan 30,40
SWx(config-mst)# exit
```



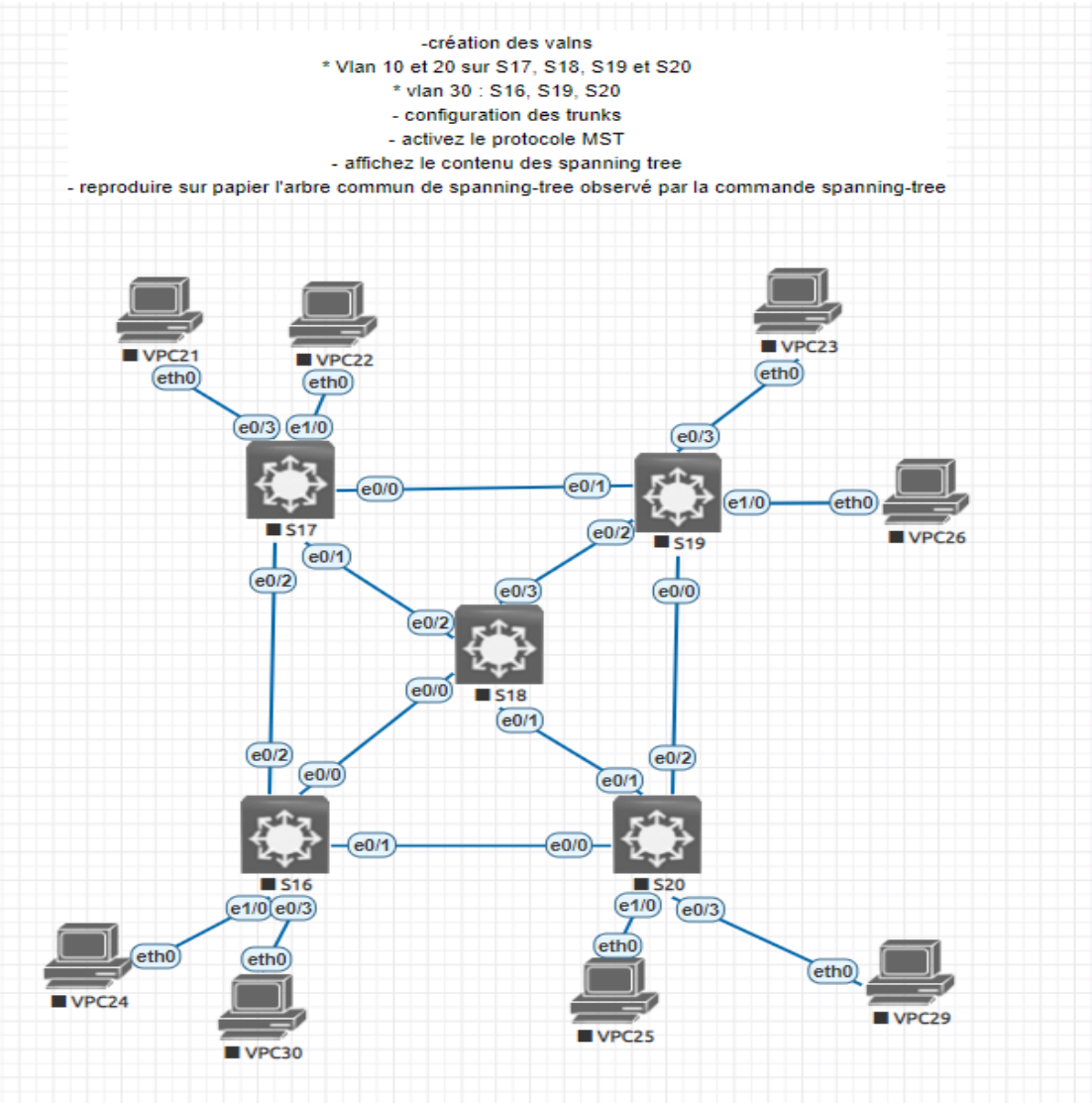

```
SW1(config)#spanning-tree mst 1 root primary
SW1(config)#spanning-tree mst 2 root secondary

SW2 (config)#spanning-tree mst 2 root primary
SW2 (config)#spanning-tree mst 1 root secondary
```

- Une instance doit avoir le même nom et numéro de révision
- Dans le cas contraire, elle sera considérée comme une instance différente même si elle détient les mêmes VLANs

Exercice Pratique

-création des valns
* Vlan 10 et 20 sur S17, S18, S19 et S20
* vlan 30 : S16, S19, S20
- configuration des trunks
- activez le protocole MST
- affichez le contenu des spanning tree
- reproduire sur papier l'arbre commun de spanning-tree observé par la commande spanning-tree



Haute Disponibilité – Tolérance aux Pannes

- Assurer la continuité de service
- Plusieurs Protocoles utilisés des les LANS
  - HSRP : Hot Standby Redundancy Protocol (Cisco)
  - VRRP : Virtual Router Redundancy Protocol
  - CARP : Aommon Address Redundancy Protocol

- Protocoles de Failover – permettent l'utilisation d'un second équipement en cas de panne du premier
- Fonctionnement : mode **Actif/Passif**

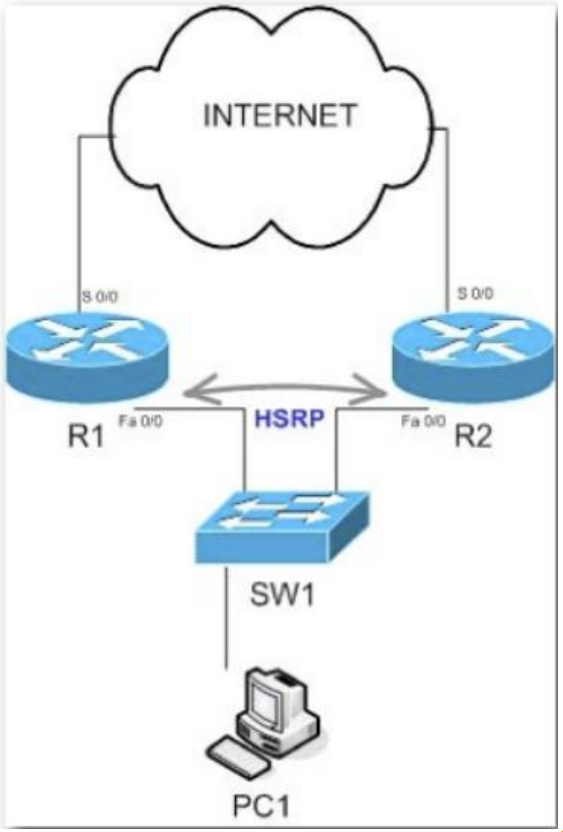
PROTOCOLE HSRP

Configuration du routeur 1

```
R1(config)#interface Fastethernet 0/0
R1(config-if)# ip address 192.168.0.2 255.255.255.0
R1(config-if)#standby 1 ip 192.168.0.1
R1(config-if)#standby 1 priority 105
R1(config-if)#standby 1 preempt
```

Configuration du routeur 2

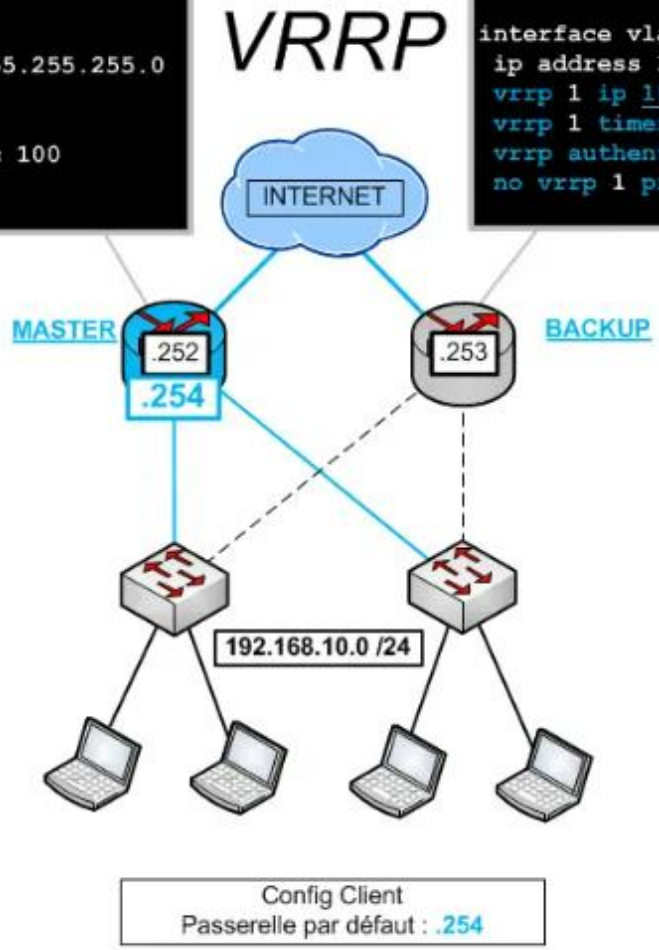
```
R2(config)#interface Fastethernet 0/0
R2(config-if)# ip address 192.168.0.3 255.255.255.0
R2(config-if)#standby 1 ip 192.168.0.1
R2(config-if)#standby 1 preempt
```



PROTOCOLE VRRP

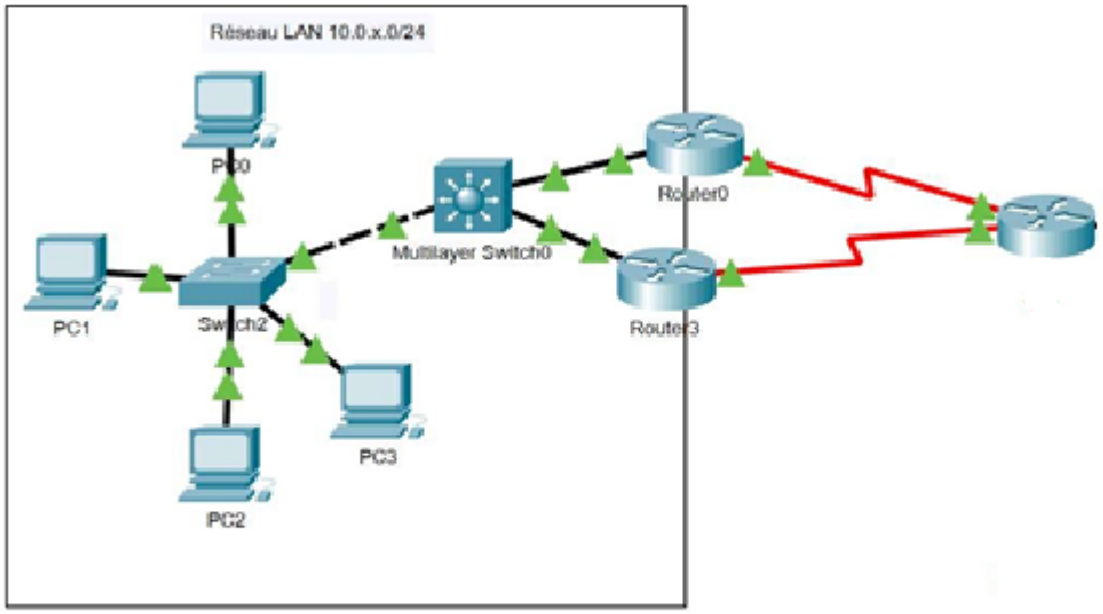
```
interface vlan 10
 ip address 192.168.10.252 255.255.255.0
 vrrp 1 ip 192.168.10.254
 vrrp 1 priority 110
 vrrp 1 timers advertise msec 100
 vrrp authentication Finger
```

```
interface vlan 10
 ip address 192.168.10.253 255.255.255.0
 vrrp 1 ip 192.168.10.254
 vrrp 1 timers learn
 vrrp authentication Finger
 no vrrp 1 preempt
```



Exercice Pratique

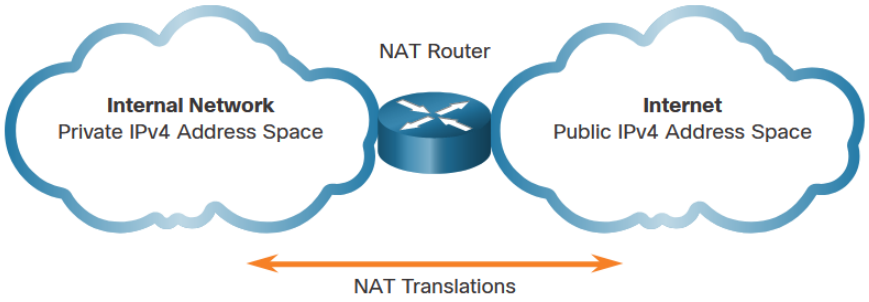
- Voir le TP – Haute disponibilité



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



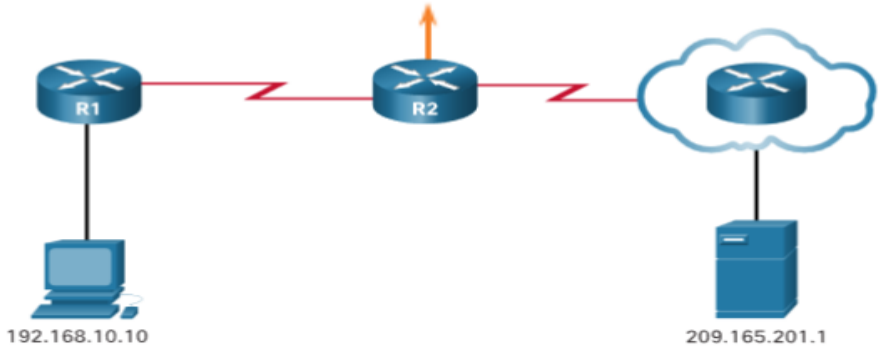
Class	Activity Type	Activity Name
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

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

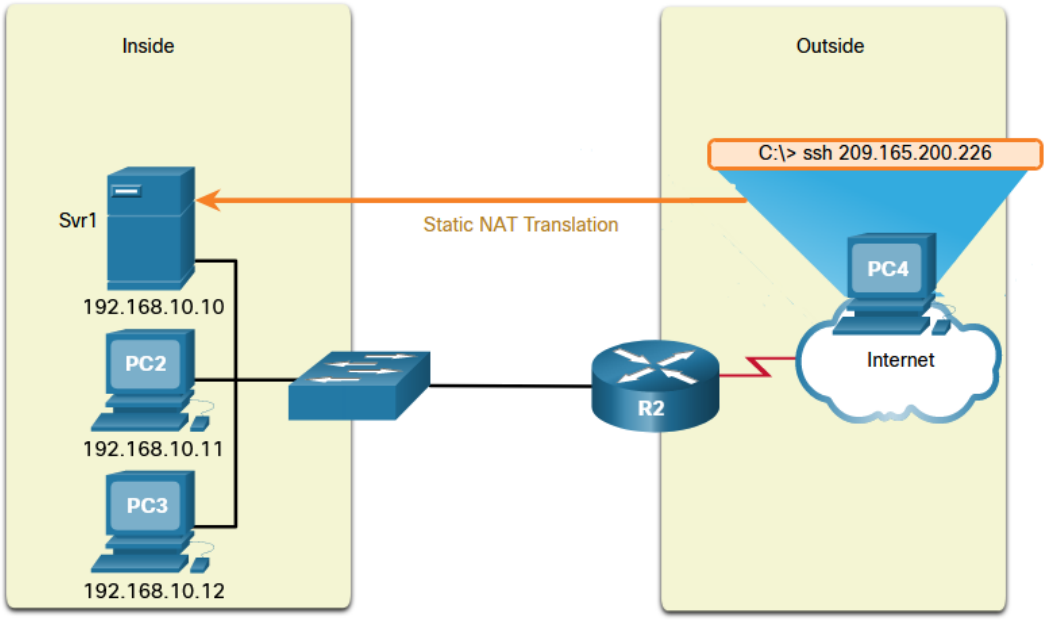


Types de NAT

- 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

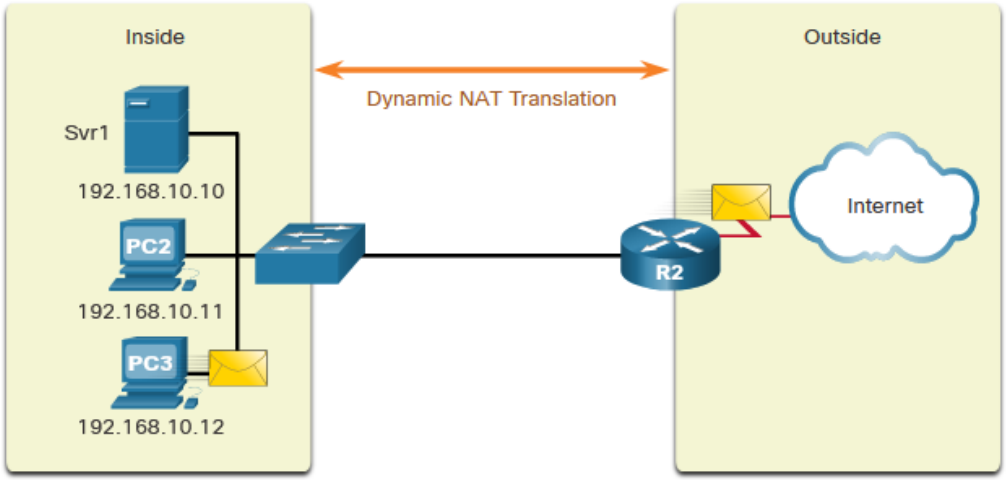
- Utilise un mappage one-to-one pour accéder une ressource inaccessible depuis l'internet
- La configuration reste permanente toute la durée de vie du routeur ou firewall



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

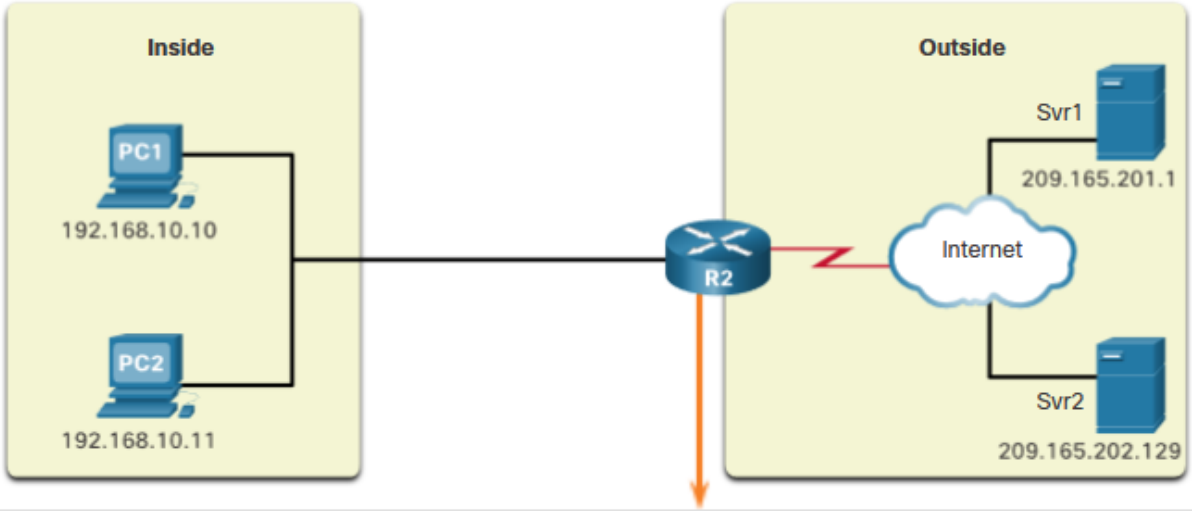
- NAT dynamique utilise un pool d'adresses IP publiques assignées à chaque réception d'adresse IP privée par le routeur



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