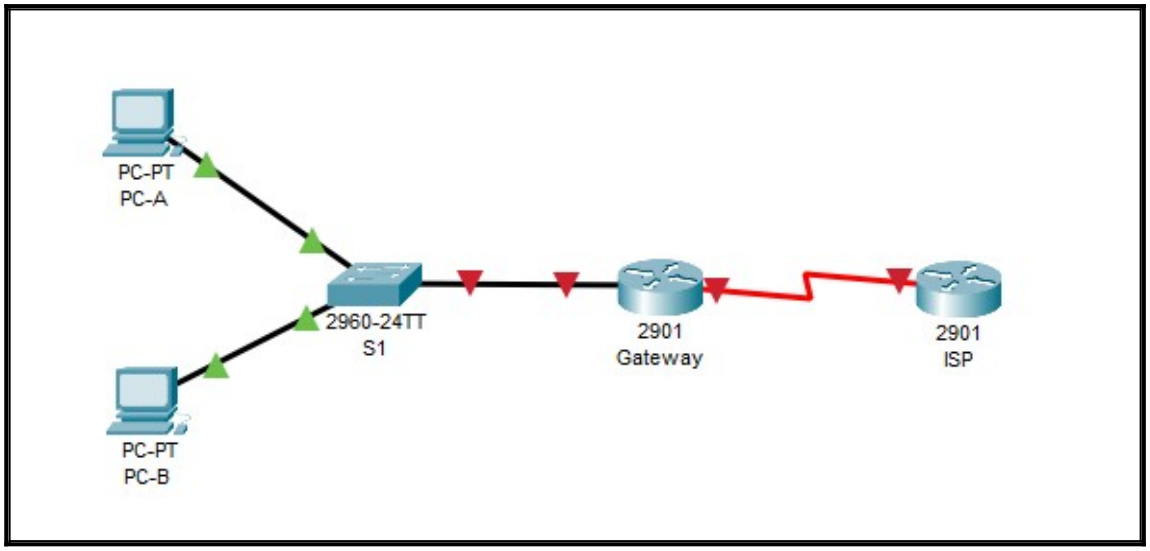
Travaux pratiques : configuration de la fonction NAT dynamique et statique (11.2.2.6).

Sommaire :

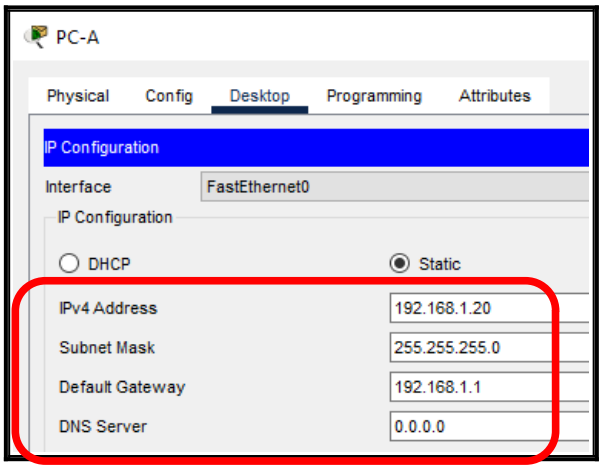
Partie 1: Création du réseau et vérification de la connectivité :

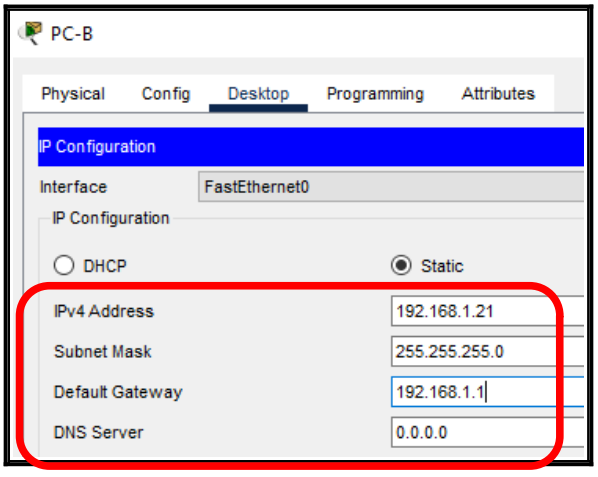
- Étape 1: Câblez le réseau conformément à la topologie.



1ère étape : Nous câblons le réseau conformément à la topologie.

- Étape 2: Configurez les hôtes de PC.





1ère étape : Configuration IP des PC.

- *Étape 4: Configurez les paramètres de base pour chaque routeur.*

```
GATEWAY$sh run
Building configuration...

Current configuration : 953 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname GATEWAY
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeC
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2901/K9 sn FTX152441GO-
!
!
!
!
!
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 shutdown
```

```
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 ip address 209.165.201.18 255.255.255.252
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
 password cisco
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 password cisco
 logging synchronous
 login
!
!
!
end
```

1ère étape : Configuration du routeur nommé **GATEWAY**.

```
ISP#sh run
Building configuration...

Current configuration : 986 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ISP
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.Z
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2901/K9 sn FTX152429Q
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Loopback0
 ip address 192.31.7.1 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 209.165.201.17 255.255.255.252
 clock rate 128000
 shutdown
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
 password cisco
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 password cisco
 logging synchronous
 login
!
!
!
end
```

2ème étape : Configuration du routeur **ISP**.

- Étape 6: Configurez le routage statique.

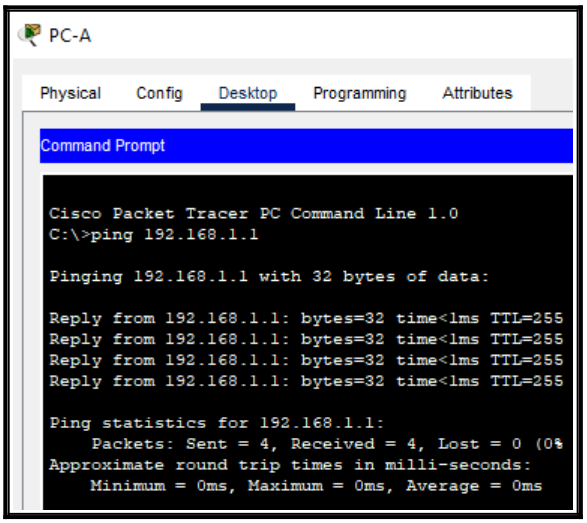
```
ISP(config)#ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

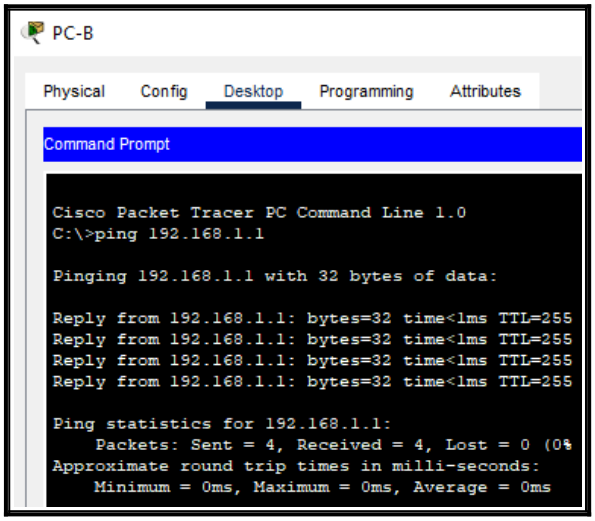
1ère étape : Création d'une **route statique** depuis le routeur **ISP** jusqu'au routeur **GATEWAY** en utilisant la **plage d'adresses réseau publiques** 209.165.200.224/27 attribuée.

```
GATEWAY(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

2ème étape : Création d'une **route par défaut** sur le routeur **GATEWAY** vers le routeur **ISP**.

- Étape 8: Vérifiez la connectivité du réseau.





1ère étape : Depuis **PC-A** et **PC-B** nous effectuons un **ping** vers l'**interface g0/1** de routeur **GATEWAY**.

```
GATEWAY#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.201.17 to network 0.0.0.0

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.16/30 is directly connected, Serial0/0/1
L       209.165.201.18/32 is directly connected, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.165.201.17
```

```
ISP#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.31.7.0/32 is subnetted, 1 subnets
C       192.31.7.1/32 is directly connected, Loopback0
S       209.165.200.224/27 [1/0] via 209.165.201.18
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
L       209.165.201.17/32 is directly connected, Serial0/0/0
```

2ème étape : Sur les deux routeurs nous affichons la **table de routage** afin de vérifier que les **routes statiques** figurent dans cette table et qu'elles sont configurées correctement sur les deux routeurs.

Partie 2: Configuration et vérification de la fonction NAT statique :

- Étape 1: Configurez un mappage statique.

```
GATEWAY(config)#ip nat inside source static 192.168.1.20 209.165.200.225
```

1ère étape : Configuration d'un **mappage statique**. Cela permet à un utilisateur d'accéder à **PC-A** depuis **Internet**. PC-A simule un serveur ou un périphérique avec une adresse constante qui est accessible depuis Internet.

- Étape 2: Indiquez les interfaces.

```
GATEWAY(config)#int g0/1
GATEWAY(config-if)#ip nat inside
GATEWAY(config-if)#int s0/0/1
GATEWAY(config-if)#ip nat outside
```

1ère étape : Nous indiquons si les **interfaces** sont **inside** ou **outside**.

- Étape 3: Testez la configuration.

```
GATEWAY#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.168.200.225   192.168.1.20       ---                ---
```

1ère étape : Nous affichons la **table NAT statique** sur le routeur **GATEWAY**.

```
C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=12ms TTL=254
Reply from 192.31.7.1: bytes=32 time=7ms TTL=254
Reply from 192.31.7.1: bytes=32 time=7ms TTL=254
Reply from 192.31.7.1: bytes=32 time=8ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 12ms, Average = 8ms
```

2ème étape : Depuis **PC-A** nous effectuons un **ping** vers l'interface **Lo0** sur le routeur **ISP**.

```
GATEWAY#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:36192.168.1.20:36    192.31.7.1:36      192.31.7.1:36
icmp 209.165.200.225:37192.168.1.20:37    192.31.7.1:37      192.31.7.1:37
icmp 209.165.200.225:38192.168.1.20:38    192.31.7.1:38      192.31.7.1:38
icmp 209.165.200.225:39192.168.1.20:39    192.31.7.1:39      192.31.7.1:39
---  209.165.200.225   192.168.1.20       ---                ---
```

3ème étape : Nous vérifions qu'une entrée **NAT** à été ajoutée à la table **NAT statique** du routeur **GATEWAY**.

```
C:\>telnet 192.31.7.1
Trying 192.31.7.1 ...Open


User Access Verification

Password:
ISP>
```

4ème étape : Depuis **PC-A** nous testons une connexion **telnet** vers **l'interface Lo0** du routeur **ISP**.

```
GATEWAY#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.225   192.168.1.20       ---                ---
---  209.168.200.225   192.168.1.20       ---                ---
tcp 209.165.200.225:1025192.168.1.20:1025  192.31.7.1:23      192.31.7.1:23
```

5ème étape : Nous affichons de nouveau la **table NAT** afin de vérifier que l'entrée avec le **protcole tcp** pour la connexion **telnet** est présente.

```
ISP#ping 209.165.200.225

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/6 ms
```

6ème étape : Nous effectuons un **ping** depuis le routeur **ISP vers PC-A**.

```
GATEWAY#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:10192.168.1.20:10    209.165.201.17:10  209.165.201.17:10
icmp 209.165.200.225:6 192.168.1.20:6     209.165.201.17:6   209.165.201.17:6
icmp 209.165.200.225:7 192.168.1.20:7     209.165.201.17:7   209.165.201.17:7
icmp 209.165.200.225:8 192.168.1.20:8     209.165.201.17:8   209.165.201.17:8
icmp 209.165.200.225:9 192.168.1.20:9     209.165.201.17:9   209.165.201.17:9
---  209.165.200.225   192.168.1.20       ---                ---
```

7ème étape : Nous affichons la **table NAT** du routeur **GATEWAY** et observons les changements.

Partie 3: Configuration et vérification de la fonction NAT dynamique :

- Étape 1: Effacez les traductions NAT.

```
GATEWAY#clear ip nat translation *
```

1ère étape : Nous effaçons les **traductions NAT**.

- Étape 2: Définissez une liste de contrôle d'accès correspondant à la plage d'adresses IP privées du LAN.

```
GATEWAY(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

1ère étape : Nous définissons une **ACL** pour permettre la **traduction du réseau 192.168.1.0/24**.

- Étape 4: Définissez le pool d'adresses IP publiques utilisables.

```
GATEWAY(config)#ip nat pool public_access 209.165.200.242 209.165.200.254 netmask 255.255.255.224
```

1ère étape : Nous définissons le **pool d'adresses IP publiques utilisables**.

- Étape 5: Définissez la NAT à partir de la liste source interne vers le groupe externe.

```
GATEWAY(config)#ip nat inside source list 1 pool public_access
```

1ère étape : Nous définissons en **NAT** à partir de la **liste source interne vers le groupe externe**.

- *Étape 6: Testez la configuration.*

```
C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=11ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 3ms
```

1ère étape : Depuis **PC-B** nous effectuons un **ping** vers l'**interface Lo0** du routeur **ISP**.

```
GATEWAY#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.242:5 192.168.1.21:5     192.31.7.1:5       192.31.7.1:5
icmp 209.165.200.242:6 192.168.1.21:6     192.31.7.1:6       192.31.7.1:6
icmp 209.165.200.242:7 192.168.1.21:7     192.31.7.1:7       192.31.7.1:7
icmp 209.165.200.242:8 192.168.1.21:8     192.31.7.1:8       192.31.7.1:8
---  209.165.200.225   192.168.1.20       ---                ---
```

2ème étape : Nous vérifions à présent la **table NAT** du routeur **GATEWAY**.

```
GATEWAY#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.225   192.168.1.20       ---                ---
---  209.168.200.225   192.168.1.20       ---                ---
tcp 209.165.200.242:1025192.168.1.21:1025  192.31.7.1:80      192.31.7.1:80
```

3ème étape : Depuis **PC-B**, après avoir ouvert un navigateur et entré l'adresse IP du serveur Web simulé ISP (**Lo0**) nous affichons la table **NAT** du routeur **GATEWAY**.

- *Étape 7: Supprimez l'entrée NAT statique.*

```
GATEWAY(config)#no ip nat inside source static 192.168.1.20 209.165.200.225
```

1ère étape : Nous supprimons l'**entrée NAT statique**.

```
GATEWAY#clear ip nat translation *
```

2ème étape : Nous effaçons de nouveau les **traductions NAT**.

```
C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=11ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 3ms
```

3ème étape : Depuis les deux PC, nous effectuons un **ping** vers l'interface **Lo0** du routeur **ISP**. On constate alors que PC-A ne peux plus **ping** l'interface **Lo0** puisque l'**entrée NAT statique** à été supprimée mais **PC-B** peut toujours **communiqué** avec celle-ci.

```
GATEWAY#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.242:10192.168.1.21:10    192.31.7.1:10      192.31.7.1:10
icmp 209.165.200.242:11192.168.1.21:11    192.31.7.1:11      192.31.7.1:11
icmp 209.165.200.242:12192.168.1.21:12    192.31.7.1:12      192.31.7.1:12
icmp 209.165.200.242:9 192.168.1.21:9     192.31.7.1:9       192.31.7.1:9
```

4ème étape : Afin de vérifier que la communication avec **PC-B** et l'interface **Lo0** se fait correctement nous vérifions la **table NAT** du routeur **GATEWAY**.