

## SOMMAIRE

1. Partie 1 : Configuration de la topologie et initialisation des périphériques.....	2
2. Partie 2 : Configuration des périphériques et vérification de la connectivité.....	2
Étape 2 : Configuration du routeur.....	3
Étape 3 : Vérifiez la connectivité du réseau.....	5
Étape 4 : Configurez le routeur pour l'accès SSH.....	6
3. Partie 3 : Affichage des informations du routeur.....	8
Étape 3 : Affichez la configuration initiale.....	10

## 1. Partie 1 : Configuration de la topologie et initialisation des périphériques

Je fais le câblage conformément à la topologie et je mets sous tension tout les périphériques

## 2. Partie 2 : Configuration des périphériques et vérification de la connectivité

Configuration de PC A :



Configuration de PC B :

Adresse IP : **192.168.0.3**

Masque : **255.255.255.0**

Passerelle par défaut : **192.168.0.1**

## Étape 2 : Configuration du routeur

Sur le routeur je passe en mode privilégié avec la commande **enable** puis en mode de configuration avec la commande **conf t** pour attribuer un nom au routeur pour le nommer **R1**

```
Routeur (config)#hostname R1
R1 (config)#
```

Je désactive la recherche DNS en tapant la commande **no ip domain-lookup** pour éviter une recherche DNS si une commande est mal taper

```
R1 (config)#no ip domain-lookup
R1 (config)#
```

La commande **security passwords min-length 10** permet de saisir un mot de passe avec un minimum de 10 caractères

```
R1 (config)#security passwords min-length 10
R1 (config)#
```

J'attribue le mot de passe **ciscoenpass** comme mot de passe chiffréS

```
R1 (config)#enable secret ciscoenpass
R1 (config)#
```

Je tape la commande **line con 0** et j'attribue le mot de passe **ciscovtypass** et je mets un délai d'attente

```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#login
R1(config-line)#exec-timeout 5 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#
```

Je chiffre tout les mot de passe avec la commande **service password-encryption**

```
R1(config)#service password-encryption
R1(config)#
```

Je créer une bannière MOTD pour indiquer que la configuration du routeur a été modifiée

```
R1(config)#banner motd #Configuration modifiée#
R1(config)#
```

j entre dans l'interface g0/0 avec la commande **int g0/0** j'ajoute une description et j'entre l'adresse IP et je fais la même chose pour l'interface **g0/1S**

```
R1(config)#int g0/0
R1(config-if)#description Connexion a PC-B
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#int g0/1
R1(config-if)#description Connexion a S1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

Je fais un **no shut** pour passer le **status en up**

J'enregistre la configuration actuelle avec la commande **copy run start**

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

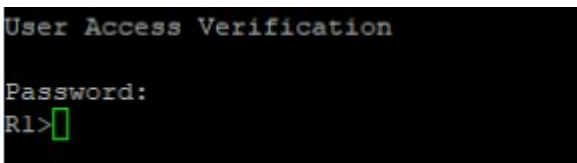
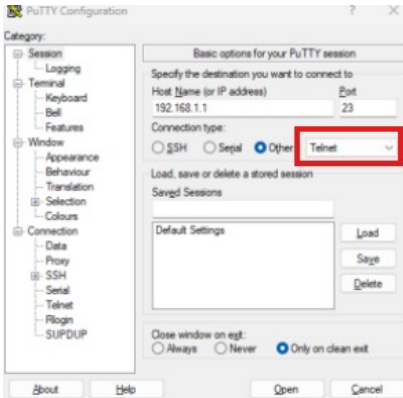
### Étape 3 : Vérifiez la connectivité du réseau

Depuis PC A je ping PC B pour vérifier la connectivité réseau

```
Envoi d'une requête 'Ping' 192.168.0.1 avec 32 octets de données :
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=255
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=255
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=255
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=255

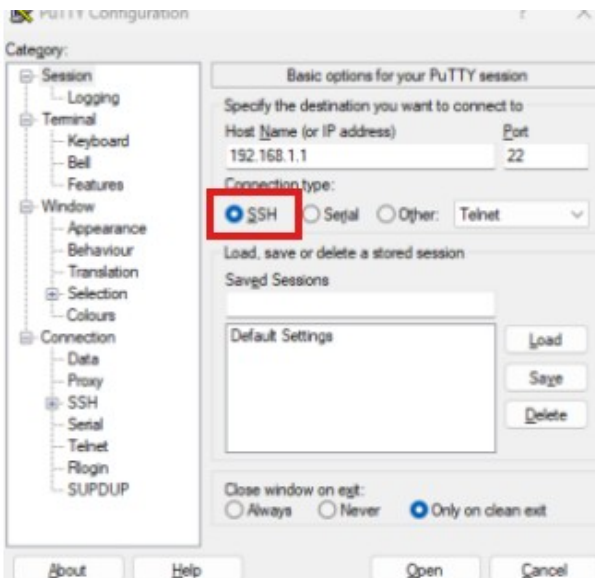
Statistiques Ping pour 192.168.0.1:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
  Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

J'accède à distance à R1 depuis PC A à l'aide du client Telnet de Putty



#### Étape 4 :Configurez le routeur pour l'accès SSH

Cette fois-ci j'accède à distance au routeur R1 à partir de PC A via le client SSH



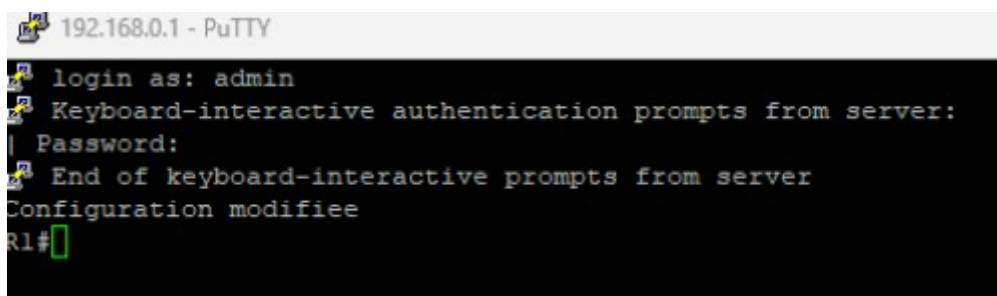
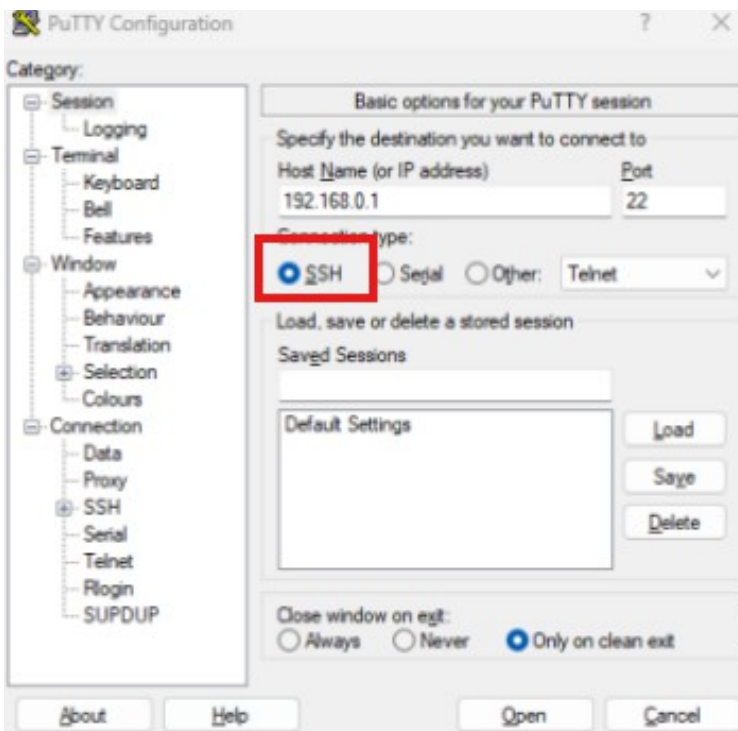
Je consulte la configuration du routeur à l'aide de la commande **show run**

```
R1#show run
Building configuration...

Current configuration : 1968 bytes
!
! Last configuration change at 06:30:48 UTC Wed Jan 21 2026
! NVRAM config last updated at 05:55:36 UTC Wed Jan 21 2026
! NVRAM config last updated at 05:55:36 UTC Wed Jan 21 2026
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 10
enable secret 4 pz9A9n/f8wxdG3eikEn8T6zR/eMGkCmgWdoDecKwgGA
enable password 7 082C485E
!
no aaa new-model
memory-size iomem 15
!
no ipv6 cef
ip source-route
ip cef
!
!
!
!
no ip domain lookup
ip domain name exupery.local
multilink bundle-name authenticated
!
!
crypto pki token default removal timeout 0
!
!
license udi pid CISCO2901/K9 sn FCZ1648C1EN
!
!
username admin privilege 15 secret 4 N8MfSN4ih5aPHwGKWri82fJTo5xdZQ/0.3PlqOUqRFk
!
```

### 3. Partie 3 :Affichage des informations du routeur

Depuis PC B j'ouvre une session SSH sur le routeur R1



```
R1#show version
```

```
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc1)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2012 by Cisco Systems, Inc.  
Compiled Tue 20-Mar-12 18:57 by prod_rel_team
```

```
ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
```

```
R1 uptime is 2 hours, 45 minutes  
System returned to ROM by power-on  
System restarted at 04:53:50 UTC Wed Jan 21 2026  
System image file is "flash0:c2900-universalk9-mz.SPA.151-4.M4.bin"  
Last reload type: Normal Reload
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:  
<http://www.cisco.com/w1/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to [export@cisco.com](mailto:export@cisco.com).

```
Cisco CISCO2901/K9 (revision 1.0) with 450560K/73728K bytes of memory.  
Processor board ID FCZ1648C1EN  
2 Gigabit Ethernet interfaces  
2 Serial(sync/async) interfaces  
1 terminal line  
DRAM configuration is 64 bits wide with parity enabled.  
255K bytes of non-volatile configuration memory.  
250880K bytes of ATA System CompactFlash 0 (Read/Write)
```

Quel est le nom de l'image IOS exécutée par le routeur ?

c2900-universalk9-mz.SPA.151-4.M4.bin

Quelle quantité de mémoire vive non volatile (NVRAM) le routeur possède-t-il ?

Il possède 255K de mémoire vive non volatile

Quelle quantité de mémoire Flash le routeur possède-t-il ?

Il possède 250880K de mémoire flash

Quel est le processus de démarrage du routeur lors du prochain redémarrage ?

Le processus de redémarrage du routeur lors du prochain redémarrage est 0x2102

### **Étape 3 : Affichez la configuration initiale.**

Comment les mots de passe sont-ils présentés dans les résultats ?

A faire

Quel est le résultat de l'exécution de cette commande ?

Le résultat de cette commande est :

```
line vty 0 4
```

```
exec-timeout 5 0
```

```
password 7 094F471A1A0A0106121C053939
```

```
logging synchronous login local
```

```
transport input ssh
```

```
!
```

```
scheduler allocate 20000 1000
```

```
end
```