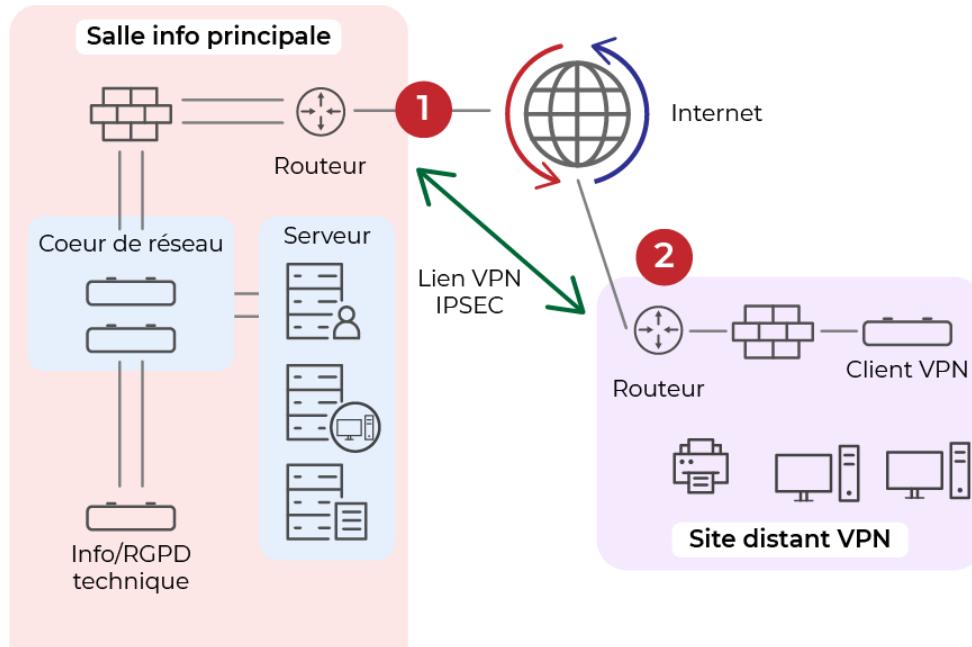


Réalisez les premières configurations des routeurs de votre réseau

(Re)Découvrez ce qu'est un routeur

Dans le cours [Concevez votre réseau TCP/IP](#), vous avez appris que le **routeur** est l'**équipement d'interconnexion** qui relie plusieurs **réseaux ensemble**. Vous allez donc vous intéresser à cet équipement dans ce chapitre. Combien de routeurs seront présents dans le schéma final ?

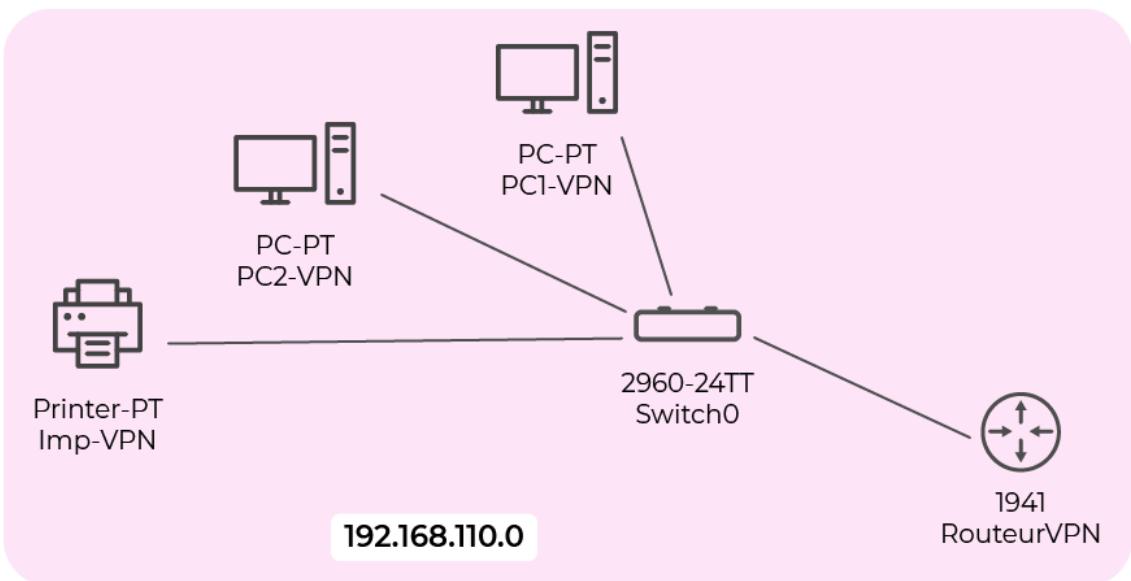
Si vous reprenez le schéma de réseau, vous trouverez **deux** routeurs :



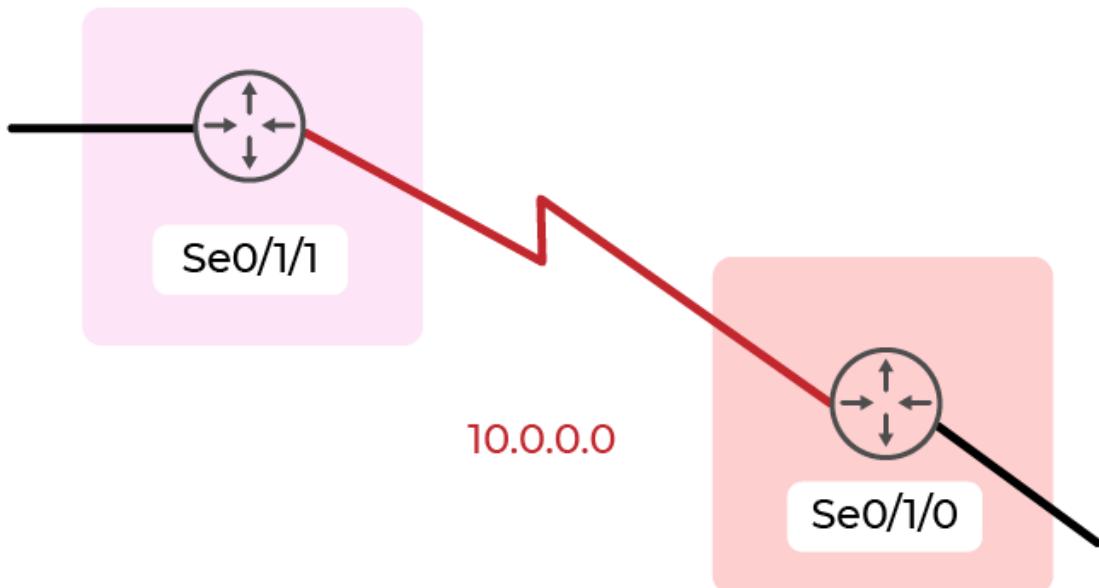
Les deux routeurs dans notre schéma du réseau

Le routeur présent dans l'entreprise est déjà dans notre réseau sous Cisco Packet Tracer. Vous allez **ajouter** maintenant le routeur pour les **clients VPN** dans Cisco Packet Tracer. Pour cela, vous allez ajouter le **sous-réseau VPN** (routeur et périphériques finaux).

Avec un peu de couleur, voici notre **sous-réseau VPN** sous Cisco Packet Tracer :



Le sous-réseau VPN est ajouté
Intéressons-nous un instant à cette [connexion série](#) :



Connexion en série des routeurs

Tout d'abord, vous remarquerez que le lien entre les deux routeurs est un **éclair**. C'est cette représentation graphique qui est utilisée lorsque l'on veut représenter une [connexion WAN](#) longue distance ; vous retrouverez fréquemment ce type de connexion dans les schémas de réseau. En général, cela représente des connexions **point-à-point VPN** entre **sites distants**.

Ensuite, vous avez ajouté une carte [WIC-2T](#) qui est une carte qui présente deux ports série. Cela permet de réaliser justement des connexions de type WAN. On utilisera un **câble DTE/DCE** pour

relier les routeurs ensemble, ils sont également de couleur **bleue** comme les câbles console, mais sont d'un bleu plus prononcé.



Câble DCE/DTE utilisé pour réaliser des connexions WAN

Il est important de souligner qu'un troisième routeur est présent dans l'entreprise. Alors ce n'est pas un routeur en tant que tel, mais il fait office de routage : c'est le commutateur de niveau 3 !

Le **sous-réseau VPN** se situant à l'**extérieur** de l'entreprise, le commutateur sera laissé dans son état d'origine sans aucune configuration.

Par contre, il faut penser à configurer les **adresses IP** des **2 ordinateurs** et de l'**imprimante** ! Cependant, ces 3 périphériques finaux seront sur le sous-réseau **192.168.110.0/24**, nous ne mettrons donc pas l'imprimante sur le sous-réseau **Impression**.

Peu de postes sont présents dans le VLAN DMZ, il n'y a donc pas d'utilité à mettre en place des VLAN dans la DMZ, nous verrons plus tard dans le cours dans quel cas de figure il est intéressant de mettre des VLAN.

Voici le **plan d'adressage du sous-réseau VPN** :

PC1-VPN	PC2-VPN	Imp-VPN	Passerelle
192.168.110.1/24	192.168.110.2/24	192.168.110.3/24	192.168.110.254

Configurez votre routeur pour le sécuriser

Vous allez configurer les paramètres de base du routeur avec comme objectif premier la **sécurité** ! Ces configurations doivent être systématiques sur les équipements réseau et il faut prendre les bonnes habitudes dès le début, même si ces opérations sont fastidieuses. Vous l'avez déjà fait pour le commutateur, je vous donne la configuration pour l'accès sécurisé.

Vous allez configurer :

1. Le nom d'hôte.

2. Un mot de passe pour le mode privilégié.
3. La configuration du SSH pour une version 2, la création d'un utilisateur **admin** et la création d'une clé SSH avec l'insertion dans un nom de domaine.
4. Un mot de passe pour l'accès sur le port console.
5. Un mot de passe pour les lignes VTY pour l'accès en SSH.
6. Le cryptage des mots de passe.
7. L'affichage d'une bannière pour fournir une notification légale d'accès non autorisé.
8. La copie de la configuration dans la mémoire non volatile.

```

Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)# hostname RouteurVPN
RouteurVPN(config)# enable secret 1234-MetroPole:1234
RouteurVPN(config)# ip ssh version 2
RouteurVPN(config)# ip domain-name metropolecg.com
RouteurVPN(config)# username admin secret
1234-MetroPole:1234
RouteurVPN(config)# crypto key generate rsa
The name for the keys will be: RouteurVPN.metropolecg.com
Choose the size of the key modulus in the range of 360 to
2048 for your
General Purpose Keys. Choosing a key modulus greater than
512 may take
a few minutes.

```

```

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be
non-exportable...[OK]

```

```

RouteurVPN(config)# line console 0
RouteurVPN(config-line)# password 1234-MetroPole:1234
RouteurVPN(config-line)# login
RouteurVPN(config-line)# exit
RouteurVPN(config)# line vty 0 15
RouteurVPN(config-line)# transport input ssh
RouteurVPN(config-line)# login local
RouteurVPN(config-line)# exit
RouteurVPN(config)# service password-encryption
RouteurVPN(config)# banner motd #Acces aux Personnes
Autorisees Seulement !#

```

```
RouteurVPN(config)# exit
RouteurVPN#
%SYS-5-CONFIG_I: Configured from console by console

RouteurVPN# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RouteurVPN#
N'oubliez pas de faire la même configuration sur le routeur de l'entreprise, le nom d'hôte sera
RouteurCG.
```

En résumé

Vous avez vu dans ce chapitre :

- L'ajout d'un routeur Cisco ainsi que la connexion WAN réalisée par une liaison série entre les deux retours.
- La configuration de la sécurisation de vos 2 routeurs, sensiblement équivalente à un commutateur.

Configurez les interfaces de votre routeur

Les routeurs sont compatibles avec les **LAN** et les **WAN**, ils peuvent interconnecter **differents types de réseaux**, ils prennent donc en charge **plusieurs types d'interfaces**. Pour être disponible, une interface doit :

- Être **configurée avec au moins une adresse IP** : Utilisez les commandes de configuration de l'interface **ip address Adresse_IPMasque_Sous_Réseau** et **ipv6 address Adresse_IP_v6/Préfixe**.
- Être **activée** : Par défaut, les interfaces LAN et WAN ne sont pas activées (**shutdown**). Pour activer une interface, il faut l'activer à l'aide de la commande **no shutdown** (pas d'arrêt). Cela revient à mettre l'interface sous tension. L'interface doit également être connectée à un autre périphérique (concentrateur, commutateur ou autre routeur) pour que la couche physique soit active.
- **Avoir une description** : En option, l'interface peut également être configurée avec une courte description de **240 caractères maximum**. Il est recommandé de configurer une description sur chaque interface. Sur les réseaux de production, les avantages des descriptions d'interface sont rapidement réalisés car elles sont utiles pour le dépannage, et pour identifier une connexion et des coordonnées de tiers.

Configurez le routeur VPN

Configurez le Routeur VPN comme ceci :

```
RouteurVPN(config)# interface GigabitEthernet0/0
RouteurVPN(config-if)# ip address 192.168.110.254
255.255.255.0
RouteurVPN(config-if)# ipv6 address
2001:db8:acad:110::254/64
RouteurVPN(config-if)# description Lien Sous-Reseau VPN
RouteurVPN(config-if)# no shutdown
RouteurVPN(config-if)# exit
RouteurVPN(config)# interface Serial0/1/1
RouteurVPN(config-if)# ip address 10.0.0.2 255.255.255.0
RouteurVPN(config-if)# ipv6 address
2001:db8:acad:1001::2/64
RouteurVPN(config-if)# description Lien
RouteurVPN-RouteurCG
RouteurVPN(config-if)# no shutdown
RouteurVPN(config-if)# exit
```

N'oubliez pas de faire la même configuration sur le routeur de l'entreprise (**RouteurCG**) :

- Le nom de l'interface **Série** sera **Serial0/1/0**, l'adresse **IPv4** sera **10.0.0.1/24** et l'adresse **IPv6** sera **2001:db8:acad:1001::1/64**.

- Le nom de l'interface **GibabitEthernet** sera **GibabitEthernet0/0**, l'adresse **IPv4** sera **192.168.10.1/24** et l'adresse **IPv6** sera **2001:db8:acad:10::1/64**.

Configurez l'adresse de bouclage de votre routeur

Une autre configuration courante des routeurs Cisco IOS consiste à activer une **interface de bouclage**. L'interface de bouclage est une interface **logique interne** au routeur. Elle n'est pas attribuée à un port physique et ne peut jamais être connectée à un autre appareil. Elle est considérée comme une interface logicielle qui est automatiquement placée en état “**up**” (interface dite *active*) tant que le routeur fonctionne.

L'interface de bouclage est utile en cas de test et de gestion d'un périphérique Cisco IOS, car elle garantit qu'au moins une interface est toujours disponible. Vous utiliserez souvent une interface de bouclage pour simuler Internet. L'activation et l'attribution d'une interface de bouclage se font ainsi :

```
RouteurVPN(config)# interface loopback 0
RouteurVPN(config)#
%LINK-5-CHANGED: Interface Loopback0, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Loopback0, changed state to up
RouteurVPN(config-if)# ip address 192.168.200.2
255.255.255.0
RouteurVPN(config-if)# exit
```

Plusieurs interfaces de bouclage peuvent être activées sur un routeur, cependant, l'adresse IPv4 de chaque interface de bouclage doit être **unique** et **inutilisée** par toute autre interface ; vous utiliserez l'adresse IP **192.168.200.1/24** pour l'adresse IP de bouclage du routeur de l'entreprise (**routeur CG**).

En résumé

Vous avez vu dans ce chapitre :

- La configuration de base d'un routeur afin de le sécuriser (nom d'hôte, mot de passe pour le mode privilégié, accès SSH, cryptage des mots de passe, bannière et copie de la configuration dans la mémoire non volatile).
- La configuration des interfaces d'un routeur (adresse IPv4, adresse IPv6 et description).
- La configuration d'une adresse de bouclage pour simuler Internet.

Configurez le routage de votre routeur

Comprenez le fonctionnement d'un routeur

Pour éviter qu'un routeur ne transfère un paquet n'importe où, il doit déterminer le **meilleur chemin** (la route) pour le paquet à prendre. À l'inverse d'un commutateur (sauf le commutateur de niveau 3 qui fait office de routeur), un routeur relie **plusieurs réseaux** entre eux. Il dispose donc de **plusieurs interfaces** appartenant chacune à un **sous-réseau différent**.

Un routeur a au moins deux interfaces disponibles pour relier et interconnecter au moins deux réseaux (ou sous-réseaux) différents.

Lorsqu'un routeur reçoit un paquet sur une interface, il détermine quelle interface il doit utiliser pour transférer le paquet vers sa destination. L'interface qu'utilise le routeur pour transférer le paquet peut être :

- la destination finale (on parle alors de **routeur d'extrémité**) ;
- mais aussi un réseau connecté à un autre routeur utilisé pour atteindre le réseau de destination.

Les principales fonctions d'un routeur consistent à déterminer le **meilleur chemin** d'acheminement des paquets en fonction des informations contenues dans sa **table de routage**, et à **transférer** les paquets vers leur destination.

Le meilleur chemin dans la table de routage sera la correspondance la plus longue. Il vous suffit donc de prendre le préfixe le plus long :

Entrées de route	Longueur du préfixe	Adresse en notation binaire
1	172.16.0.0/12	10101100.00010000.00000000.00001010
2	172.16.0.0/18	10101100.00010000.00000000.00001010
3	172.16.0.0/26	10101100.00010000.00000000.00001010

Ici, la correspondance la plus longue étant la 3e entrée, le routeur privilégiera celle-ci.

Il en sera de même avec les routes en IPv6. Si un paquet arrive en 2001:db8:c000::99, le routeur a comme table de routage :

Entrées de route	Longueur du préfixe	Correspondance
1	2001:db8:c000::/40	Correspond à 40 bits
2	2001:db8:c000::/48	Correspond à 48 bits
3	2001:db8:c000:5555::/64	Bien que 64 bits, ne correspond pas à cause du sous-réseau

Les tables de routage se remplissent de plusieurs manières :

- Les **réseaux directement connectés** sont des réseaux configurés sur les interfaces actives d'un routeur. Un réseau directement connecté est ajouté à la table de routage lorsqu'une interface est configurée avec une adresse IP et un masque de sous-réseau (longueur du préfixe) et lorsqu'elle est active (up).
- Les **réseaux distants** sont des réseaux qui ne sont pas directement connectés au routeur, le routeur apprend des réseaux distants de deux manières différentes :
 - **Routes statiques** : Ajoutées à la table de routage lorsqu'une route est configurée **manuellement**.
 - **Protocoles de routage dynamique** : Ajoutés à la table de routage lorsque les protocoles apprennent dynamiquement sur le réseau distant. Les protocoles de routage dynamiques comprennent **OSPF (Open Shortest Path First)** et **EIGRP (Enhanced Interior Gateway Routing Protocol)**, ainsi que plusieurs autres.
- Une **route par défaut** spécifie un routeur de **tronçon suivant** à utiliser lorsque la table de routage **ne contient pas de route** spécifique correspondant à l'adresse IP de destination. La route par défaut peut être saisie manuellement sous la forme de **route statique**, ou apprise **automatiquement** à partir d'un protocole de routage dynamique.

Dans ce cours, vous ne configurerez que des routes statiques dans les différents routeurs, et vous configurerez également des routes par défaut.

Configurez les routes de votre routeur

Maintenant que vous savez comment fonctionnent les routeurs, vous allez configurer les tables de routage de vos routeurs. Pour vous aider, j'ai schématisé nos 3 routeurs.

Trois routeurs ?

Eh oui, n'oubliez pas votre commutateur de niveau 3 qui fera office de routeur :

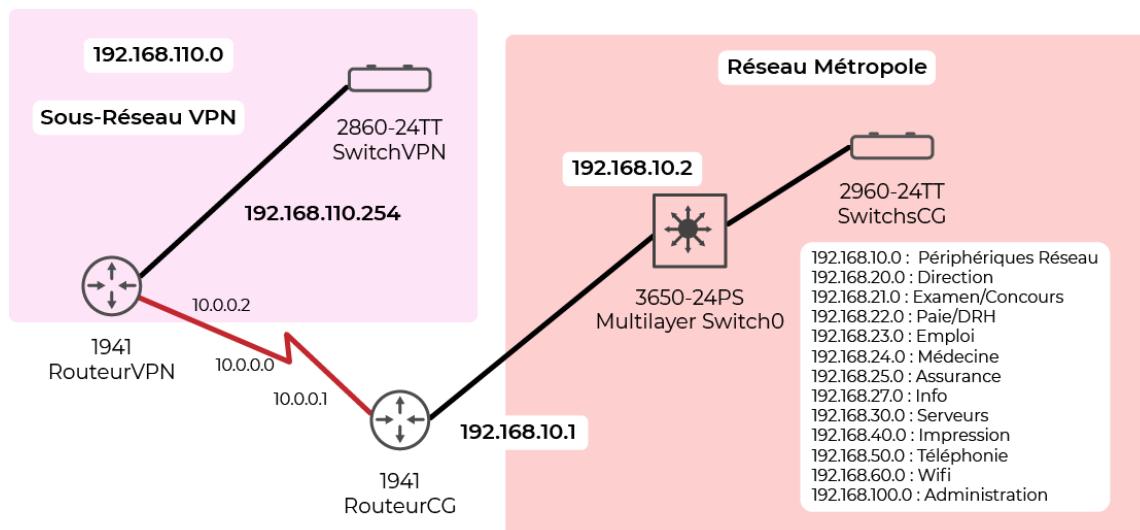


Schéma réseau du routage de l'entreprise

Bon, vous avez donc 3 tables de routage à remplir, et nous allons les remplir manuellement.

Si besoin, aidez-vous du cours [Concevez votre réseau TCP/IP](#) pour comprendre le fonctionnement des tables de routage.

Voici comment vous allez les remplir, mais commencez par la table de routage du routeur VPN :

Réseau destination	Masque de sous-réseau	Passerelle
0.0.0.0	0.0.0.0	10.0.0.1

Wow, mais c'est super simple 😊 !

En effet, vous avez utilisé une **route par défaut** car votre routeur est situé à l'extrémité du réseau. Donc pour aller ailleurs que sur votre sous-réseau (**192.168.110.0/24**), vous êtes obligé de passer par la passerelle d'adresse IP **10.0.0.1** !

Bon, vous remarquerez également que vous n'avez pas besoin de spécifier les réseaux directement connectés, car le routeur les connaît déjà !

Allez, je vous montre comment configurer une **route par défaut** : il suffit de taper la commande suivante :

```
RouteurVPN(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.1
```

Vous n'êtes pas obligé de spécifier les interfaces de sortie dans les tables de routage avec les routeurs Cisco, cela simplifie grandement la configuration des tables de routage !

Bon, c'est super, mais vous allez aller un petit peu plus loin, avec la configuration d'une table de routage en IPv6 🤯 ! Ne vous inquiétez pas, je vous montre comment faire. Mais il faut d'abord **activer le routage IPv6 et spécifier la route par défaut** !

```
RouteurVPN(config)# ipv6 unicast-routing
```

```
RouteurVPN(config)# ipv6 route ::/0 2001:db8:acad:1001::1
```

La seule différence, en plus du fait d'utiliser **ipv6** à la place d'**ip**, est le format de la route par défaut : **::/0**.

Bon maintenant, vous allez configurer le routeur de l'entreprise et c'est (un tout petit) plus compliqué car ce n'est plus un routeur d'extrémité. Il faut donc spécifier plusieurs routes.

Allez, je vous laisse chercher un peu ce que sera la table de routage du routeur de la métropole.

Vous avez terminé ? (En IPv4, bien sûr 😊) :

Réseau destination	Masque de sous-réseau	Passerelle
192.168.110.0	255.255.255.0	10.0.0.2
0.0.0.0	0.0.0.0	192.168.10.2

Facile, non ? En utilisant une route par défaut, vous n'avez besoin que de rajouter le réseau distant et c'est tout !

Prenez l'habitude d'utiliser une route par défaut pour les tables de routage qui ont le plus d'adresses de destination sur une même interface. Cela permet d'avoir des tables de routage condensé !

Bon allez, voici la configuration avec les commandes :

```
RouteurVPN(config)# ip route 192.168.110.0 255.255.255.0
10.0.0.2
RouteurVPN(config)# ip route 0.0.0.0 0.0.0.0 192.168.10.2
RouteurVPN(config)# ipv6 unicast-routing
RouteurVPN(config)# ipv6 route 2001:db8:acad:110::0/64
2001:db8:acad:1001::2
RouteurVPN(config)# ipv6 route ::/0 2001:db8:acad:10::2
```

Je vous conseille d'utiliser les mêmes identifiants pour vos sous-réseaux en IPv4 et en IPv6, cela vous permet de vérifier d'éventuelles erreurs de frappe 😊 !

Allez, maintenant, il faut configurer le commutateur de niveau 3 sauf que vous ne l'avez pas encore touché ! Pour information, il faut respecter les 3 étapes suivantes pour configurer convenablement un routeur (ou un commutateur de niveau 3) :

1. Donner un nom d'hôte.
2. Configurer les interfaces.
3. Configurer la table de routage.

Pour vous aider, je vous propose le schéma précédent précisant désormais le nom des interfaces :

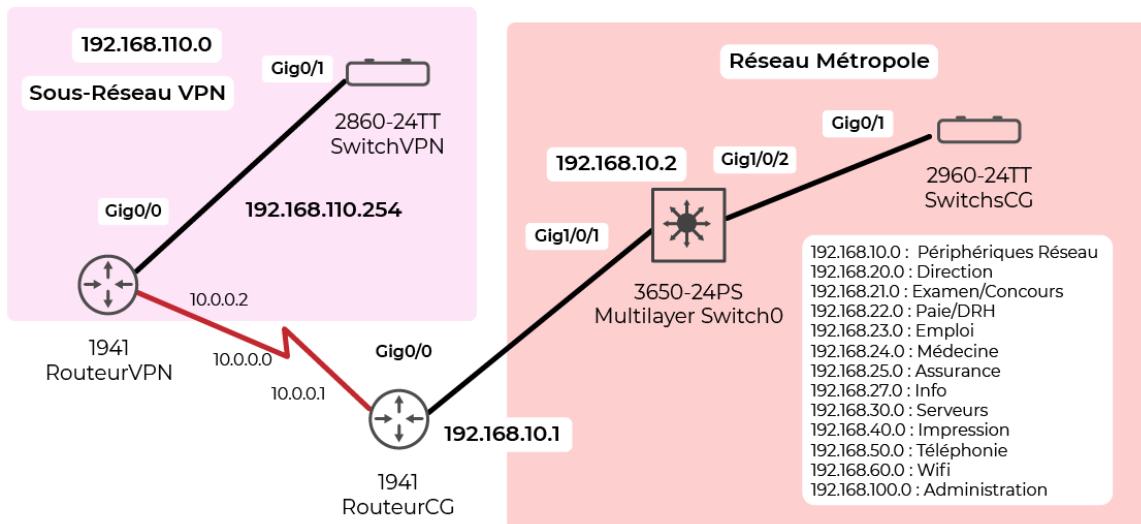


Schéma réseau du routage de l'entreprise avec le nom des interfaces

On peut considérer, à juste titre, que le commutateur de niveau 3 est un routeur d'extrémité car il se situe en bout du réseau. Le routage avec les différents sous-réseaux de l'entreprise sera assuré grâce au routage inter-VLAN.

La table de routage du commutateur de niveau 3 sera donc plutôt simple :

Réseau destination	Masque de sous-réseau	Passerelle
0.0.0.0	0.0.0.0	192.168.10.1

Voici les commandes à taper pour le commutateur de niveau 3 (la commande **ip routing** permet d'activer le routage IPv4 sur un commutateur de niveau 3) :

```
Switch(config)# hostname SwitchL3
SwitchL3(config)# interface g1/0/1
SwitchL3(config-if)# no switchport
SwitchL3(config-if)# ip address 192.168.10.2 255.255.255.0
SwitchL3(config-if)# ipv6 address 2001:db8:acad:10::2/64
SwitchL3(config-if)# exit
SwitchL3(config)# ip routing
SwitchL3(config)# ip route 0.0.0.0 0.0.0.0 192.168.10.1
SwitchL3(config)# ipv6 unicast-routing
SwitchL3(config)# ipv6 route ::/0 2001:db8:acad:10::1
```

En résumé

Vous avez vu dans ce chapitre :

- Un routeur permet de choisir le meilleur chemin pour qu'un paquet arrive à sa destination finale et ce, grâce à sa table de routage.
- La configuration et l'affichage de la table de routage d'un routeur.

Vérifiez l'état de votre routeur

Vérifiez l'état des interfaces et affichez les tables de routage

La sortie des commandes **show ip interface brief** et **show ipv6 interface brief** peut être utilisée pour révéler rapidement l'état de toutes les interfaces sur le routeur.

Vous pouvez vérifier que les interfaces sont actives et opérationnelles grâce à la mention “**up**” indiquée dans l'état et pour le protocole. Si vous avez un résultat différent, reprenez vos configurations.

```
RouteurVPN# show ip interface brief
Interface          IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0 192.168.110.254 YES manual up
    up
GigabitEthernet0/1 unassigned      YES unset
administratively
down   down
Serial0/1/0         unassigned      YES unset
administratively down  down
Serial0/1/1         10.0.0.2       YES manual up
up
Vlan1              unassigned      YES unset
administratively down  down
RouteurVPN#
```

```
RouteurVPN# show ipv6 interface brief
GigabitEthernet0/0 [up/up]
    FE80::260:3EFF:FE50:9101
    2001:DB8:ACAD:110::254
GigabitEthernet0/1 [administratively down/down]
    unassigned
Serial0/1/0         [administratively down/down]
    unassigned
Serial0/1/1         [up/up]
    FE80::260:3EFF:FE50:9101
    2001:DB8:ACAD:1001::2
Vlan1              [administratively down/down]
    unassigned
RouteurVPN#
```

Pour afficher les tables de routage, on utilisera les commandes **show ip route** et **show ipv6 route** :

```
RouteurVPN# 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 10.0.0.1 to network 0.0.0.0

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.0.0.0/24 is directly connected, Serial0/1/1
L      10.0.0.2/32 is directly connected, Serial0/1/1
192.168.110.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.110.0/24 is directly connected,
GigabitEthernet0/0
L      192.168.110.254/32 is directly connected,
GigabitEthernet0/0
S*    0.0.0.0/0 [1/0] via 10.0.0.1
```

RouteurVPN#

Si vous analysez cette table de routage, vous trouverez :

1. Les **réseaux connectés directement**, à savoir 10.0.0.0/24 et 192.168.110.0/24, le routeur les a donc rajoutés automatiquement :

```
C      10.0.0.0/24 is directly connected, Serial0/1/1
C      192.168.110.0/24 is directly connected,
GigabitEthernet0/0
```

2. Les deux entrées locales qui correspondent aux deux interfaces configurées :

```
L      10.0.0.2/32 is directly connected, Serial0/1/1
L      192.168.110.254/32 is directly connected,
GigabitEthernet0/0
```

3. La route par défaut que vous avez configurée :

```
S*    0.0.0.0/0 [1/0] via 10.0.0.1
```

Il en sera de même avec la **table de routage IPv6** :

```

RouteurVPN# show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
      ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr
      - Redirect
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP, EX - EIGRP external
S ::/0 [1/0]
  via 2001:DB8:ACAD:1001::1
C 2001:DB8:ACAD:110::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:110::254/128 [0/0]
  via GigabitEthernet0/0, receive
C 2001:DB8:ACAD:1001::/64 [0/0]
  via Serial0/1/1, directly connected
L 2001:DB8:ACAD:1001::2/128 [0/0]
  via Serial0/1/1, receive
L FF00::/8 [0/0]
  via Null0, receive
RouteurVPN#

```

Et si vous faisiez des petits tests ? C'est par ici avec moi :

Filtrez les résultats avec la commande Show

Les commandes qui génèrent plusieurs écrans de sortie sont, par défaut, mises en pause après **24 lignes**. À la fin de cette interruption, le texte **--More--** s'affiche. Appuyez sur **Entrée** pour afficher la ligne suivante, et appuyez sur la touche **Espace** pour afficher la série de lignes suivante.

Une autre fonctionnalité très utile et qui améliore l'expérience de l'utilisateur dans le CLI est le filtrage des sorties **show**.

Les commandes de filtrage permettent d'afficher des sections de résultat spécifiques. Pour activer la commande de filtrage :

- tapez le symbole (**I**) après la commande **show** ;
- puis saisissez un paramètre de filtrage et une expression de filtrage.

Il existe quatre paramètres de filtrage qui peuvent être configurés après le **pipe** (= le caractère **|** dans votre commande) :

1. **section** : Montre la section entière qui commence par l'expression de filtrage.

```
RouteurVPN# show running-config | section
GigabitEthernet0/1
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
RouteurVPN#
```

2. **include** : Comprend toutes les lignes de sortie qui correspondent à l'expression de filtrage.

```
RouteurVPN# show ip interface brief | include up
GigabitEthernet0/0 192.168.110.254 YES manual up up
Serial0/1/1 10.0.0.2 YES manual up up
RouteurVPN#
```

3. **exclude** : Exclut toutes les lignes de sortie qui correspondent à l'expression de filtrage.

```
RouteurVPN# show ip interface brief | exclude unassigned
Interface IP-Address
OK? Method Status
Protocol
GigabitEthernet0/0 192.168.110.254 YES manual up up
Serial0/1/1 10.0.0.2 YES manual up up
RouteurVPN#
```

4. **begin** : Affiche toutes les lignes à partir d'un certain point, en commençant par la ligne qui correspond à l'expression de filtrage.

```
RouteurVPN# show ip route | begin Gateway
Gateway of last resort is 10.0.0.1 to network 0.0.0.0

 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.0.0.0/24 is directly connected, Serial0/1/1
L    10.0.0.2/32 is directly connected, Serial0/1/1
 192.168.110.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.110.0/24 is directly connected,
GigabitEthernet0/0
L    192.168.110.254/32 is directly connected,
GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.0.0.1
```

```
RouteurVPN#
```

Affichez vos anciennes commandes avec la commande History

La fonction d'historique des commandes est utile car elle stocke temporairement la liste des commandes exécutées à rappeler.

Pour rappeler des commandes dans la mémoire tampon, appuyez sur **Ctrl+P** ou sur la touche **Up Arrow** (↑). Le résultat de la commande commence par la commande la plus récente, et vous pouvez appuyer plusieurs fois sur la touche flèche pour rappeler des commandes plus anciennes.

Pour revenir à des commandes plus récentes dans la mémoire tampon de l'historique, appuyez sur **Ctrl+N** ou sur la touche **Down Arrow** (↓), et vous pouvez appuyer plusieurs fois sur cette touche pour rappeler des commandes plus récentes.

Par défaut, l'historique des commandes est activé, et le système enregistre les **10 dernières lignes de commande** dans sa mémoire tampon. Vous pouvez utiliser la commande **show history** pour afficher le contenu du tampon :

```
RouteurVPN# show history
  show history
  show ip interface brief
  show ipv6 interface brief
  show ip route
  show ipv6 route
  show running-config | section GigabitEthernet0/1
  show ip interface brief | include up
  show ip interface brief | exclude unassigned
  show ip route | begin Gateway
  show history
RouteurVPN#
```

Cette commande permet également d'augmenter le nombre de lignes de commande que l'historique enregistre uniquement au cours de la session de terminal en cours.

Vous pouvez utiliser la commande **terminal history size** pour augmenter ou réduire la taille de la mémoire tampon.

```
RouteurVPN# terminal history size 200
RouteurVPN# show history
  en
  conf t
  show history
  terminal history size
  terminal history size 200
  conf t
  show history
RouteurVPN# exit
RouteurVPN con0 is now available
```

Press RETURN to get started.

```
RouteurVPN> en
RouteurVPN# show history
  en
  show history
```

RouteurVPN#

Vous remarquerez que dans les tests effectués précédemment, si vous quittez la console et que vous vous reconnectez, la mémoire tampon s'est vidée ; faites donc attention à ne jamais quitter la console si vous voulez récupérer des anciennes commandes tapées précédemment !

En résumé

Vous avez appris dans ce chapitre :

- La vérification de l'état d'une interface.
- Le filtrage des résultats de commande avec show :
 - **section** ;
 - **include** ;
 - **exclude** ;
 - **begin** .
- Les fonctions d'historique de commande grâce à la commande **show history** qui permet d'afficher les 10 dernières commandes tapées.