Packet Tracer - Confirmation de dépannage - Utilisation de la documentation pour résoudre des problèmes (version de l'instructeur)

Remarque à l'intention de l'instructeur : le texte en rouge ou surligné en gris apparaît uniquement dans la version de l'instructeur.

Topologie

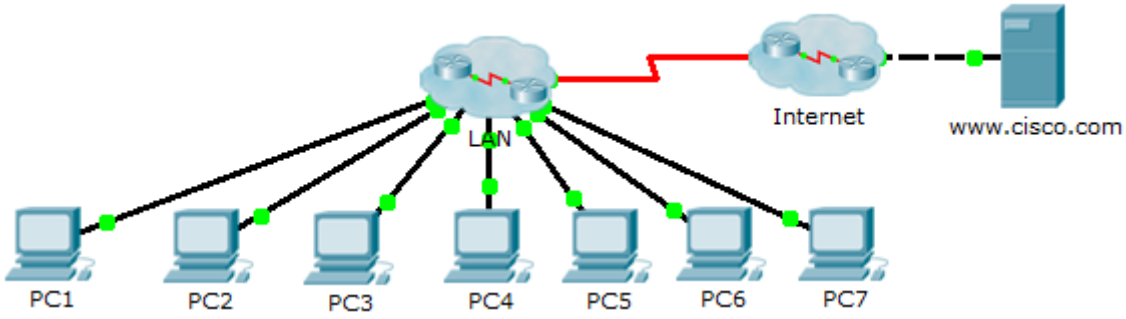

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
PC1	NIC	10.2.15.10	255.255.255.0	10.2.15.1
PC2	NIC	10.2.25.10	255.255.255.0	10.2.25.1
PC3	NIC	10.2.35.10	255.255.255.0	10.2.35.1
PC4	NIC	10.3.100.4	255.255.255.0	10.3.100.1
PC5	NIC	10.3.100.5	255.255.255.0	10.3.100.1
PC6	NIC	10.4.1.10	255.255.255.0	10.4.1.1
PC7	NIC	10.5.1.10	255.255.255.0	10.5.1.1
DNS Server	NIC	10.1.100.2	255.255.255.0	10.1.100.1
R1	S0/0/0	10.1.0.4	255.255.255.248	N/A
	G0/0	10.4.1.1	255.255.255.0	N/A
R2	S0/0/0	10.1.0.3	255.255.255.248	N/A
	G0/0.100	10.3.100.1	255.255.255.0	N/A
	G0/0.105	10.3.105.1	255.255.255.0	N/A
R3	S0/0/0	10.1.0.2	255.255.255.248	N/A
	G0/0.5	10.2.5.1	255.255.255.0	N/A
	G0/0.15	10.2.15.1	255.255.255.0	N/A
	G0/0.25	10.2.25.1	255.255.255.0	N/A
	G0/0.35	10.2.35.1	255.255.255.0	N/A
R4	S0/0/0	10.1.0.5	255.255.255.248	N/A
	G0/0	10.5.1.1	255.255.255.0	N/A
R5	S0/0/0	10.1.0.1	255.255.255.248	N/A
	S0/0/1	209.165.201.2	255.255.255.252	N/A
	G0/0	10.1.100.1	255.255.255.0	N/A
S1	None	None	None	None
S2	VLAN 105	10.3.105.21	255.255.255.0	10.3.105.1
S3	VLAN 105	10.3.105.22	255.255.255.0	10.3.105.1
S4	VLAN 5	10.2.5.21	255.255.255.0	10.2.5.1
S5	VLAN 5	10.2.5.23	255.255.255.0	10.2.5.1
S6	VLAN 5	10.2.5.22	255.255.255.0	10.2.5.1
S7	None	None	None	None

Objectifs

Partie 1 : collecte de documentation

Partie 2 : test de connectivité

Partie 3 : collecte de données et implémentation de solutions

Partie 4 : test de connectivité

Scénario

Cet exercice constitue la deuxième partie d'un exercice en deux parties. La Partie I est **Packet Tracer - Confirmation de dépannage - Documentation du réseau**, que vous devez avoir terminé précédemment dans ce chapitre. Dans la Partie II, vous allez utiliser vos compétences et documentation de dépannage de la partie I pour résoudre les problèmes de connectivité entre plusieurs ordinateurs.

Partie 1 : Collecte de documentation

Étape 1 : Récupérez la documentation réseau.

Pour effectuer cet exercice, vous aurez besoin de votre documentation relative à **Packet Tracer - Confirmation de dépannage - Documentation du réseau**, que vous avez effectué précédemment dans ce chapitre. Recherchez cette documentation maintenant.

Étape 2 : Exigences en matière de documentation

La documentation que vous avez effectuée dans l'exercice précédent doit disposer d'une table topologique et précise d'adressage. Si nécessaire, mettez à jour votre documentation pour refléter une représentation exacte d'une **réponse correcte de Packet Tracer - Confirmation de dépannage - Consignation d'informations sur l'activité du réseau**. Vous devrez peut-être consulter votre instructeur.

Remarque à l'intention de l'instructeur : l'étudiant doit avoir réalisé un schéma complet et précis du réseau de réponse de l'exercice précédent, à savoir **Packet Tracer - Confirmation de dépannage - Documentation du réseau**. Vous devrez vérifier que le travail antérieur de l'étudiant est correct ou fournir de la documentation détaillée.

Partie 2 : Test de connectivité

Étape 1 : Déterminez l'emplacement du problème de connectivité.

À la fin de cet exercice, vous devriez observer une connectivité complète de PC à PC et depuis les PC vers le serveur www.cisco.pka. Toutefois, vous devez maintenant déterminer où la connectivité échoue en envoyant une requête ping à partir de :

- Des PC au serveur **www.cisco.pka**
- De PC à PC
- Des PC à la passerelle par défaut

Étape 2 : Quelles requêtes ping ont abouti ?

Documentez à la fois les requêtes ping qui ont abouti et celles qui ont échoué.

Aucun PC ne peut envoyer de requête ping au serveur www.cisco.pka. PC1, PC2 et PC3 peuvent s'envoyer mutuellement des requêtes ping. PC4 et PC5 peuvent s'envoyer mutuellement des requêtes ping. Tous les PC peuvent envoyer des requêtes ping à leurs passerelles par défaut respectives.

Partie 3 : Collecte de données et implémentation de solutions

Étape 1 : Choisissez un PC pour commencer à collecter des données.

Choisissez un PC et commencez à collecter des données en vérifiant la connectivité avec la passerelle par défaut. Vous pouvez également utiliser la commande **traceroute** pour déterminer où la connectivité est interrompue.

Étape 2 : Établissez une connexion Telnet avec la passerelle par défaut et poursuivez la collecte des données.

a. Si le PC choisi ne peut pas se connecter à sa passerelle par défaut, choisissez un autre PC afin d'aborder le problème d'un autre point de vue.

b. Après avoir établi la connectivité au travers d'une passerelle par défaut, le mot de passe de connexion est **cisco** et le mot de passe du mode d'exécution privilégié est **class**.

Étape 3 : Utilisez des outils de dépannage afin de vérifier la configuration.

Sur le routeur de la passerelle par défaut, utilisez les outils de dépannage afin de vérifier la configuration à partir de votre propre documentation. N'oubliez pas que vous devez également vérifier les commutateurs et pas uniquement les routeurs. N'oubliez pas de vérifier les éléments suivants :

- Informations d'adressage
- Activation d'interface
- Encapsulation
- Routage
- Configuration VLAN
- Non-concordance de mode bidirectionnel ou de vitesse

Étape 4 : Documentez les symptômes réseau ainsi que les solutions possibles.

Au fur et à mesure que vous détectez des symptômes relatifs au problème de la connectivité du PC, ajoutez-les à votre documentation.

Remarque à l'intention de l'instructeur : ce qui est indiqué ci-dessous ne constitue qu'une manière de réaliser cet exercice. L'étudiant peut commencer à partir de n'importe quel PC, à l'exception de **www.cisco.pka**. Pour les besoins de cet exemple de réponse, nous avons commencé sur **PC4**.

Problème 1 : à partir de **PC4**, vous pouvez accéder à la passerelle par défaut **R2**. Établissez une connexion Telnet avec **R2** et vérifiez la table de routage. **R2** ne possède que des routes connectées directement et vous devez par conséquent vérifier la configuration actuelle de l'interface à l'aide de la commande **show protocols** ou de la commande **show ip interface brief**. L'examen attentif des adresses IP montrera que l'adresse de S0/0/0 n'est pas correcte. Elle devrait être 10.1.0.3 au lieu de 10.1.100.3. La commande **show ip protocols** n'indique aucun problème lié à la configuration EIGRP sur **R2**.

Solution 1 : configurez l'adresse IP correcte de l'interface S0/0/0 sur **R2**.

Problème 2 : après la convergence du protocole EIGRP sur **R2**, exécutez la commande **show ip route** afin de collecter des informations supplémentaires sur les problèmes possibles. **R2** possède des routes correctement connectées, mais n'a que deux routes EIGRP. Les routes manquantes incluent les quatre VLAN de **R3**, le LAN de **R1** et le LAN de **R4**. La requête ping à **R3** a réussi, par conséquent établissez une connexion Telnet avec **R3**. Étant donné que **R2** ne reçoit pas les routes provenant de **R3**, vérifiez la configuration EIGRP sur **R3** à l'aide de la commande **show ip protocols**. **R3** envoie et reçoit les mises à jour EIGRP, et annonce le réseau correct. Toutefois, la récapitulation automatique des réseaux est active. Par conséquent, **R3** n'envoie que le réseau 10.0.0.0/8 par classe dans les mises à jour EIGRP périodiques.

Solution 2 : configurez **R3** à l'aide de la commande **no auto-summary**.

Problème 3 : revenez à **R3** et vérifiez la table de routage. Des routes sont manquantes pour les LAN de **R1** et **R4**. Testez la connectivité avec **R1** et **R4** en envoyant des requêtes ping aux interfaces série de ces routeurs. Les requêtes ping envoyées à **R1** échouent, mais celles envoyées à **R4** aboutissent. Établissez une connexion Telnet avec **R4**. Sur **R4**, affichez la table de routage. **R4** ne possède pas de routes EIGRP, par conséquent utilisez la commande **show ip protocols** pour vérifier le routage EIGRP. Cette commande ne génère aucun résultat dans la section « Routing for Networks », ce qui signifie que le protocole EIGRP n'est pas configuré correctement. Exécutez la commande **show run** pour vérifier les commandes EIGRP. La commande network est absente du protocole EIGRP.

Solution 3 : configurez **R4** à l'aide de la commande EIGRP suivante : network 10.0.0.0.

Problème 4 : après la convergence du protocole EIGRP, vérifiez la table de routage de **R4**. Le LAN de **R1** est toujours manquant. Étant donné l'échec des requêtes ping envoyées à **R1**, accédez à **R1** à partir de **PC6**. Commencez par envoyer une requête ping à la passerelle par défaut, puis établissez une connexion Telnet avec **R1**. Affichez la table de routage. Notez que seul le réseau F0/0 figure dans la table de routage. Vérifiez la configuration de l'interface à l'aide de la commande **show ip interface brief**. L'interface S0/0/0 est physiquement active (« up »), mais la couche liaison de données est désactivée (« down »). Examinez l'interface S0/0/0 à l'aide de la commande **show interface**. L'encapsulation est définie à PPP au lieu de Frame Relay.

Solution 4 : modifiez l'encapsulation de l'interface S0/0/0 sur R1 de PPP à Frame Relay à l'aide de la commande **encapsulation frame-relay**. Tous les PC doivent désormais pouvoir s'envoyer mutuellement des requêtes ping.

Problème 5 : les PC ne peuvent toujours pas envoyer de requête ping au serveur www.cisco.pka. Testez la connectivité à partir de n'importe quel périphérique, puis établissez une connexion Telnet avec **R5**. Déterminez l'état de l'interface à l'aide de la commande **show ip interface brief**. L'interface S0/0/1 est à l'état d'arrêt administratif (administratively down).

Solution 5 : activez l'interface S0/0/1 sur **R5** à l'aide de la commande **no shutdown**.

Problème 6 : les PC ne peuvent toujours pas envoyer de requête ping au serveur www.cisco.pka. Toutefois, les PC peuvent envoyer des requêtes ping au serveur DNS. Le problème est lié à la configuration de **R5** ou à celle du routeur ISP. Étant donné que vous n'avez pas accès au routeur ISP, vérifiez la configuration de **R5**. La commande **show run** indique que **R5** utilise la fonction NAT. L'instruction NAT reliant le pool NAT à la liste d'accès est manquante dans la configuration.

Solution 6 : configurez **R5** à l'aide de la commande **ip nat inside source list 1 pool LAN overload**.

Étape 5 : Apportez des modifications basées sur vos solutions de l'étape précédente.

Partie 4 : Test de connectivité

Étape 1 : Testez la connectivité du PC.

a. En principe, tous les PC sont capables de s'envoyer des requêtes ping et d'en envoyer vers le serveur **www.cisco.pka**. Si vous modifiez une configuration IP quelconque, relancez de nouvelles requêtes ping car les précédentes utilisent l'ancienne adresse IP.

b. Si les problèmes de connectivité entre les PC ou entre les PC et le serveur persistent, revenez à la Partie 3 et poursuivez le dépannage.

Étape 2 : Vérifier les résultats

Votre score Packet Tracer doit maintenant être égal à 70/70. Si ce n'est pas le cas, revenez à la Partie 2 et continuez à implémenter les solutions que vous avez proposées. Vous ne serez pas en mesure de cliquer sur **Check Results** et de voir les composants requis qui ne sont pas encore terminés.

Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points accumulés
Partie 2 : test de connectivité	Étape 2-a	15	
Total de la Partie 2		**15**	
Partie 3 : collecte de données et implémentation de solutions	Étape 4-a	15	
Total de la Partie 3		**15**	
Score relatif à Packet Tracer		**70**	
Score total		**100**	

Configurations des périphériques

Routeur R1

```
R1#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R1
enable secret class
spanning-tree mode pvst
interface Gig0/0
 ip address 10.4.1.1 255.255.255.0
 duplex auto
 speed auto
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 10.1.0.4 255.255.255.248
 encapsulation frame-relay
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 passive-interface Gig0/0
```

```
 network 10.0.0.0
 no auto-summary
ip classless
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```

Routeur R2

```
R2#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R2
enable secret class
spanning-tree mode pvst
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
interface GigabitEthernet0/0.100
 encapsulation dot1Q 100
 ip address 10.3.100.1 255.255.255.0
interface GigabitEthernet0/0.105
 encapsulation dot1Q 105 native
 ip address 10.3.105.1 255.255.255.0
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 10.1.0.3 255.255.255.248
 encapsulation frame-relay
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 network 10.0.0.0
 no auto-summary
ip classless
line con 0
```

```
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```

Routeur R3

```
R3#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R3
enable secret class
spanning-tree mode pvst
interface Gig0/0
 no ip address
 duplex auto
 speed auto
interface Gig0/0.5
 encapsulation dot1Q 5 native
 ip address 10.2.5.1 255.255.255.0
interface Gig0/0.15
 encapsulation dot1Q 15
 ip address 10.2.15.1 255.255.255.0
interface Gig0/0.25
 encapsulation dot1Q 25
 ip address 10.2.25.1 255.255.255.0
interface Gig0/0.35
 encapsulation dot1Q 35
 ip address 10.2.35.1 255.255.255.0
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 10.1.0.2 255.255.255.248
 encapsulation frame-relay
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 network 10.0.0.0
 no auto-summary
```

```
ip classless
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```

Routeur R4

```
R4#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R4
enable secret class
spanning-tree mode pvst
interface Gig0/0
 ip address 10.5.1.1 255.255.255.0
 duplex auto
 speed auto
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 10.1.0.5 255.255.255.248
 encapsulation frame-relay
interface Serial0/0/1
 no ip address
 shutdown
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 passive-interface Gig0/0
 network 10.0.0.0
 no auto-summary
ip classless
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```

Routeur R5

```
R5#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R5
enable secret class
spanning-tree mode pvst
interface Gig0/0
 ip address 10.1.100.1 255.255.255.0
 duplex auto
 speed auto
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 10.1.0.1 255.255.255.248
 encapsulation frame-relay
 ip nat inside
interface Serial0/0/1
 ip address 209.165.201.2 255.255.255.252
 ip nat outside
 no cdp enable
interface Vlan1
 no ip address
 shutdown
router eigrp 1
 passive-interface Gig0/0
 passive-interface Serial0/0/1
 network 10.0.0.0
 default-information originate
 no auto-summary
ip nat pool LAN 209.165.202.128 209.165.202.159 netmask 255.255.255.224
ip nat inside source list 1 pool LAN overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
access-list 1 permit 10.0.0.0 0.255.255.255
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```

Routeur ISP

```
ISP#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname ISP
spanning-tree mode pvst
interface Gig0/0
 ip address 209.165.200.225 255.255.255.252
 duplex auto
 speed auto
interface Gig0/1
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/0/0
 ip address 209.165.201.1 255.255.255.252
 clock rate 64000
interface Serial0/0/1
 no ip address
interface Serial0/2/0
 no ip address
interface Serial0/2/1
 no ip address
interface Vlan1
 no ip address
 shutdown
ip classless
ip route 209.165.202.128 255.255.255.224 Serial0/0/0
no cdp run
line con 0
line aux 0
line vty 0 4
 login
end
```

Commutateur S1

```
S1#sh run
hostname S1
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
```

```
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Commutateur S2

```
S2#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S2
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
 switchport trunk native vlan 105
 switchport mode trunk
interface FastEthernet0/2
 switchport trunk native vlan 105
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 105
```

```
 switchport mode trunk
interface FastEthernet0/4
interface FastEthernet0/5
 switchport access vlan 100
 switchport mode access
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
interface Vlan105
 ip address 10.3.105.21 255.255.255.0
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Commutateur S3

```
S3#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S3
enable secret class
spanning-tree mode pvst
```

```
interface FastEthernet0/1
interface FastEthernet0/2
 switchport trunk native vlan 105
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 105
 switchport mode trunk
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
 switchport access vlan 100
 switchport mode access
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
interface Vlan105
 ip address 10.3.105.22 255.255.255.0
ip default-gateway 10.3.1.1
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Commutateur S4

```
S4#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S4
enable secret class
spanning-tree mode pvst
spanning-tree vlan 1,5,15,25,35 priority 4096
interface FastEthernet0/1
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/2
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/4
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/5
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
interface Vlan5
```

```
 ip address 10.2.5.21 255.255.255.0
ip default-gateway 10.2.5.1
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Commutateur S5

```
S5#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S5
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/2
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/4
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
```

```
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
interface Vlan5
 ip address 10.2.5.23 255.255.255.0
ip default-gateway 10.2.5.1
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Commutateur S6

```
S6#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S6
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/2
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/3
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/4
 switchport trunk native vlan 5
 switchport mode trunk
interface FastEthernet0/5
interface FastEthernet0/6
 switchport access vlan 15
 switchport mode access
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
```

```
interface FastEthernet0/11
 switchport access vlan 25
 switchport mode access
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
 switchport access vlan 35
 switchport mode access
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
interface Vlan5
 ip address 10.2.5.22 255.255.255.0
ip default-gateway 10.2.5.1
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 login
end
```

Commutateur S7

```
S7#sh run
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S7
enable secret class
spanning-tree mode pvst
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
```

```
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1
interface GigabitEthernet1/2
interface Vlan1
 no ip address
 shutdown
line con 0
line vty 0 4
 login
line vty 5 15
 login
end
```