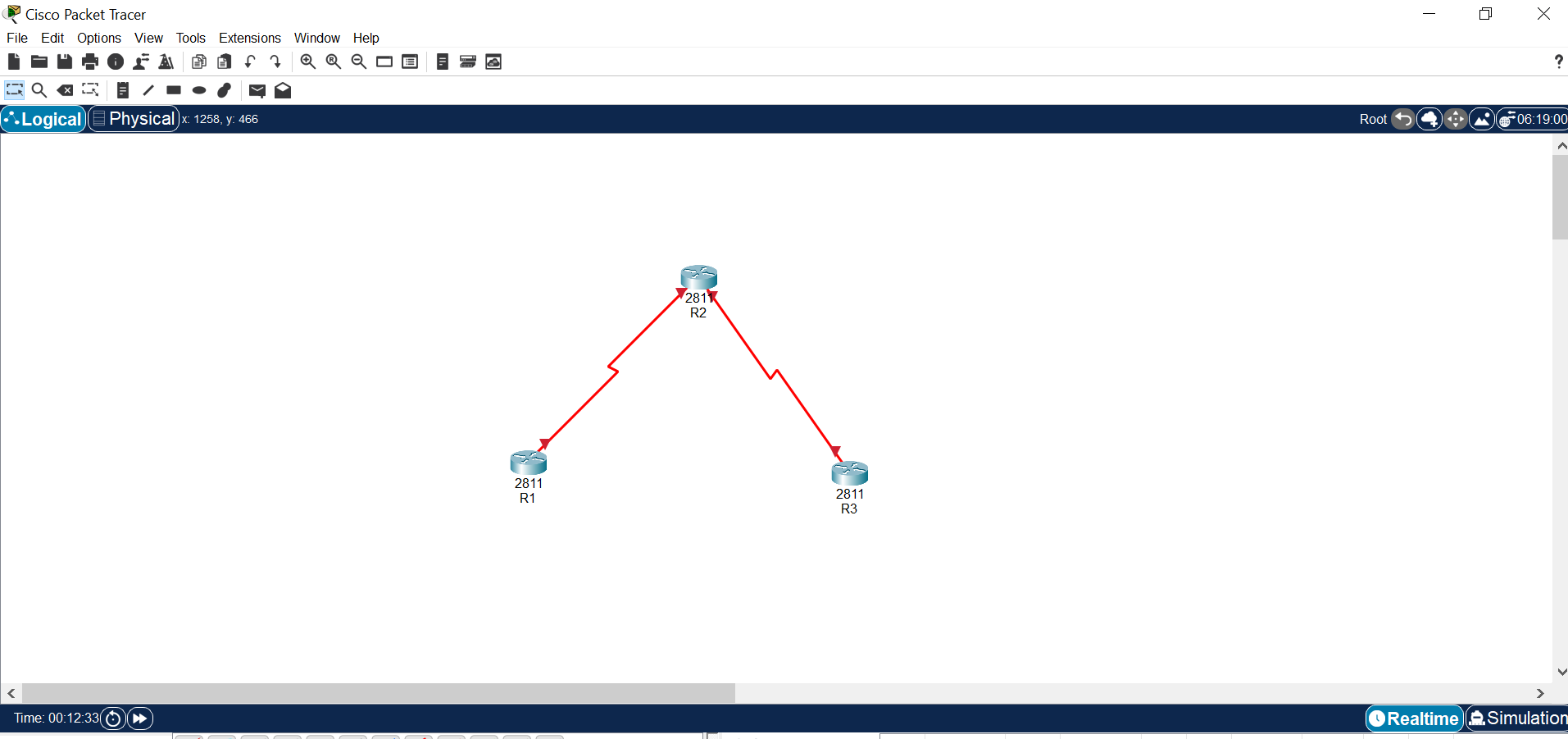
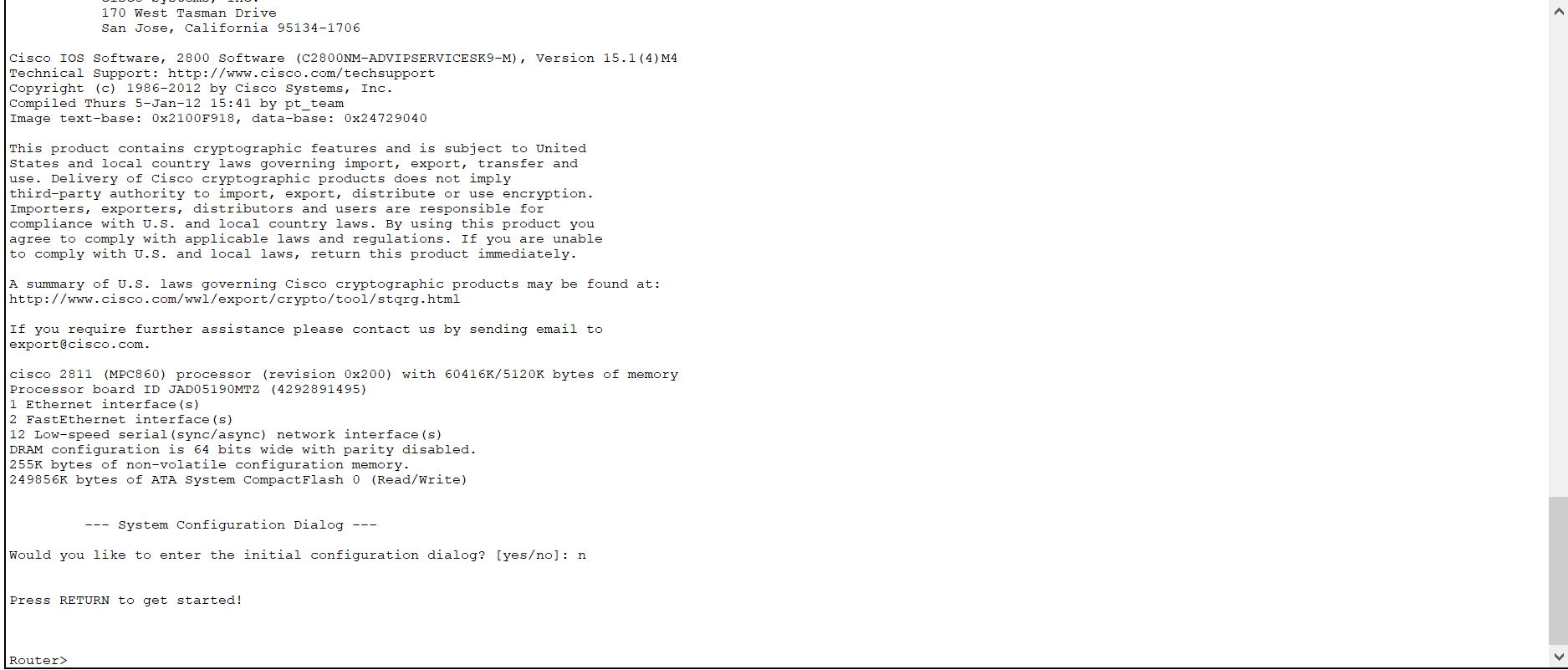
Étape 1 : Câblez le réseau conformément à la topologie.

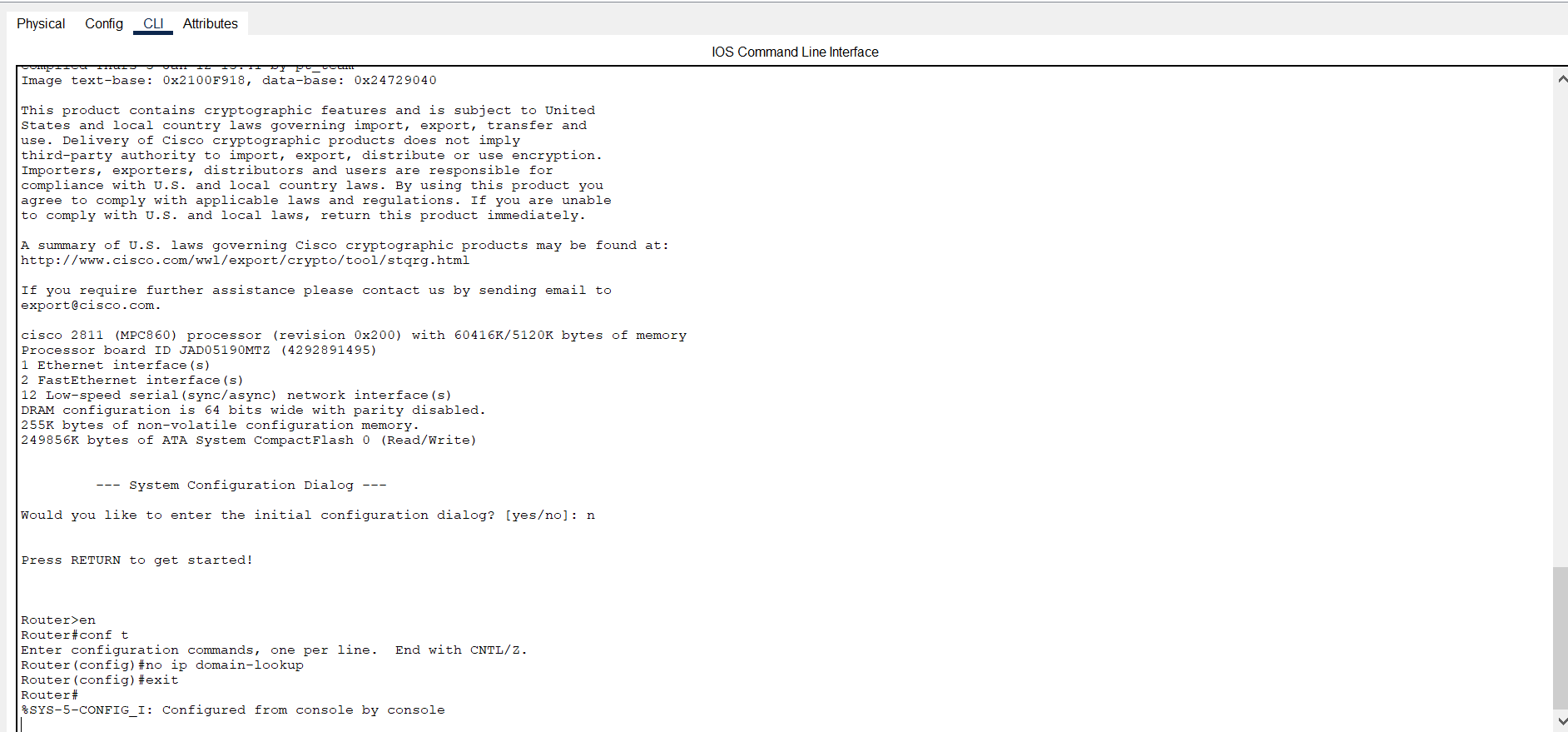


Étape 2 : Initialisez et redémarrez les routeurs, le cas échéant.



Étape 3 : Configurez les paramètres de base pour chaque routeur.

a. Désactivez la recherche DNS.



b. Configurez le nom du périphérique conformément à la topologie.



c. Attribuez class comme mot de passe du mode d’exécution privilégié.



d. Attribuez cisco comme mots de passe de console et vty.



e. Configurez logging synchronous pour la ligne de console.



f. Configurez une bannière MOTD pour avertir les utilisateurs que tout accès non autorisé est interdit.



g. Configurez les adresses IP indiquées dans la table d’adressage pour toutes les interfaces. Les interfaces DCE doivent être configurées avec une fréquence d’horloge de 128 000. La bande passante doit être de 128 Kb/s sur toutes les interfaces série.

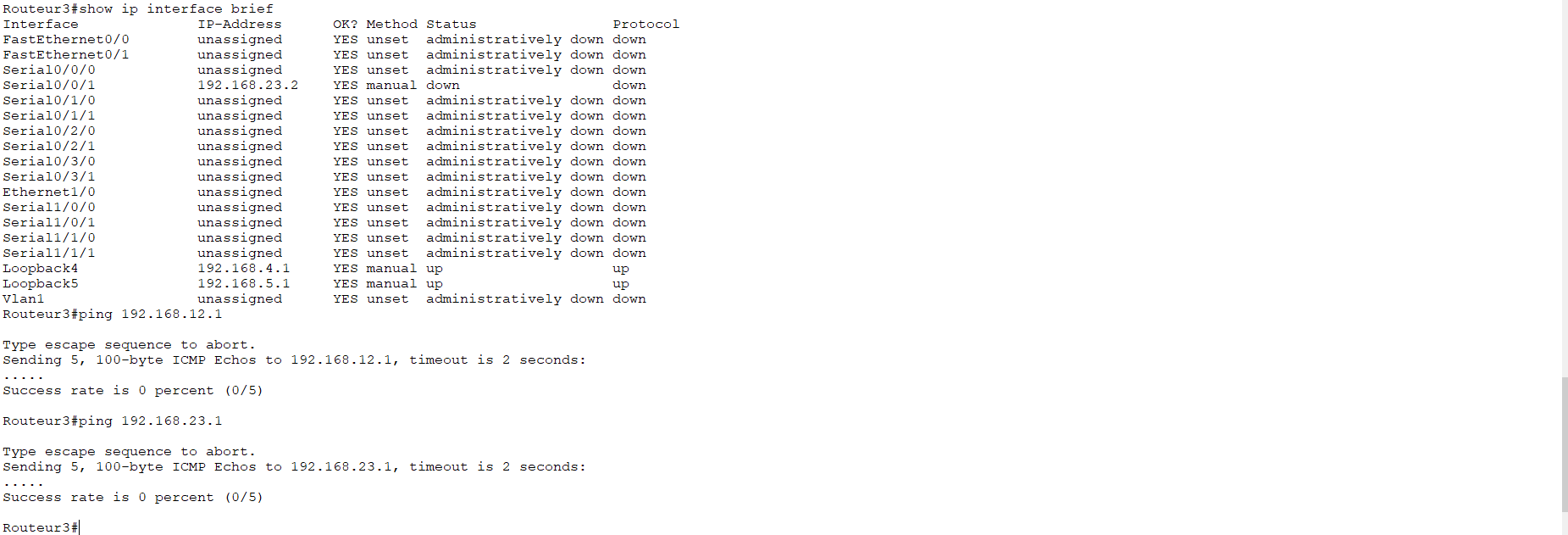




h. Copiez la configuration en cours en tant que configuration de démarrage.



Étape 4 : Vérifiez la connectivité de la couche 3. Utilisez la commande **show ip interface brief** pour vérifier que l’adressage IP est correct et que les interfaces sont actives. Vérifiez que chaque routeur peut envoyer une requête ping à l’interface série de ses voisins.



c. Configurez comme passives toutes les interfaces de bouclage LAN, Lo1 et Lo2.





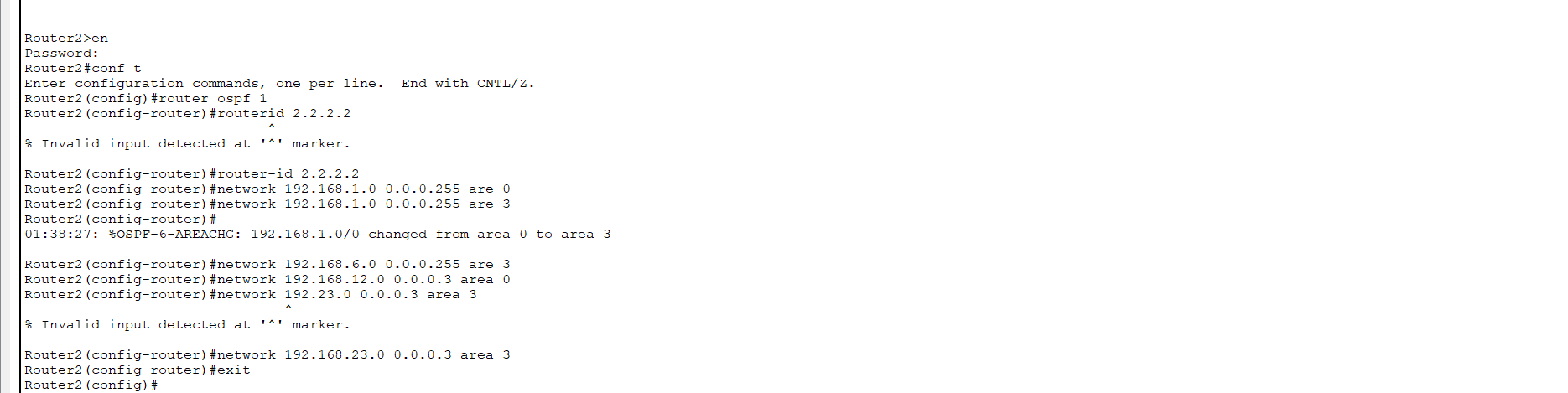
d. Créez une route par défaut vers Internet, à l’aide de l’interface de sortie Lo0.

En

Conf t

Ip route 0.0.0.0 0.0.0.0 209.165.200.225

b. Ajoutez les réseaux pour R2 au protocole OSPF. Ajoutez les réseaux à la zone appropriée. Indiquez les commandes utilisées dans l’espace ci-dessous.

****

b. Ajoutez les réseaux pour R3 au protocole OSPF. Indiquez les commandes utilisées dans l’espace ci-dessous.

****

Quel est le type de routeur OSPF pour chaque routeur ?

R1 : internal router

R2 : Backbone Router

R3 : Router Autonomous System Boundary

Étape 6 : Configurez l’authentification MD5 sur toutes les interfaces série. Configurez l’authentification MD5 OSPF au niveau interface, avec Cisco123 comme clé d’authentification. Pourquoi est-il recommandé de vérifier que le protocole OSPF fonctionne correctement avant de configurer l’authentification OSPF ?

****

Vérifier que le protocole OSPF fonctionne correctement avant la configuration de l’authentification permet de garantir une base solide pour une configuration stable et sécurisée. Cela réduit les complexités de dépannage et les risques d’erreurs dans le réseau.

b. Répétez la commande show ip ospf database pour R2 et R3. Enregistrez les ID de liaison des « Summary Net Link States » pour chaque zone.

R2 : 

R3:

