

Travaux pratiques - Utilisation de l'interface en ligne de commande pour la collecte d'informations sur les périphériques réseau

Topologie

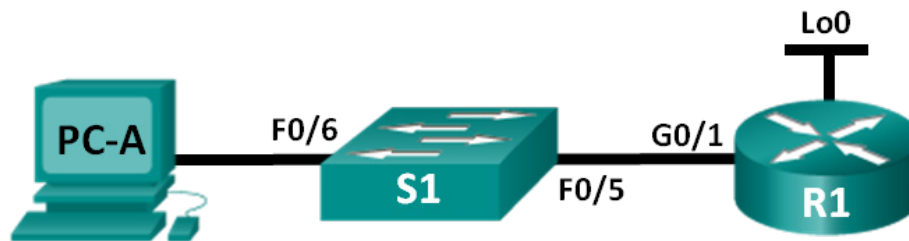


Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	Carte réseau	192.168.1.3	255.255.255.0	192.168.1.1

Objectifs

Partie 1 : Configurer la topologie et initialiser les périphériques

Partie 2 : Configurer les périphériques et vérifier la connectivité

Partie 3 : Collecter des informations sur les périphériques réseau

Contexte/scénario

La documentation d'un réseau en état de fonctionnement est l'une des tâches les plus importantes que doit effectuer un professionnel des réseaux. Le fait de documenter correctement les adresses IP, les numéros de modèle, les versions de l'IOS, les ports utilisés, et de faire des tests de sécurité facilite grandement le dépannage d'un réseau.

Dans ces travaux pratiques, vous allez créer un petit réseau, configurer les périphériques, ajouter une sécurité de base, puis documenter les configurations en exécutant différentes commandes sur le routeur, le commutateur et le PC pour recueillir les informations nécessaires.

Remarque : les routeurs utilisés lors des travaux pratiques CCNA sont des routeurs à services intégrés (ISR) Cisco 1941 équipés de Cisco IOS version 15.2(4)M3 (image universalk9). Les commutateurs utilisés sont des modèles Cisco Catalyst 2960 équipés de Cisco IOS version 15.0(2) (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent différer de ceux indiqués dans les travaux pratiques. Reportez-vous au tableau récapitulatif des interfaces de routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque : vérifiez que la mémoire des routeurs et des commutateurs a été effacée et qu'aucune configuration de démarrage n'est présente. En cas de doute, contactez votre formateur.

Ressources requises

- 1 routeur (Cisco 1941 équipé de Cisco IOS version 15.2(4)M3 image universelle ou similaire)
- 1 commutateur (Cisco 2960 équipé de Cisco IOS version 15.0(2) image lanbasek9 ou similaire)
- 1 PC (Windows 7 ou 8, équipé d'un programme d'émulation de terminal tel que Tera Term)
- Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
- Câbles Ethernet conformément à la topologie

Partie 1: Configurer la topologie et initialiser les périphériques

Dans la première partie, vous allez mettre en place la topologie du réseau, effacer les configurations s'il y a lieu, et configurer les paramètres de base sur le routeur et le commutateur.

Étape 1: Câblez le réseau conformément à la topologie.

- a. Connectez les périphériques représentés dans la topologie et effectuez le câblage nécessaire.
- b. Mettez sous tension tous les périphériques de la topologie.

Étape 2: Initialisez et redémarrez le routeur et le commutateur.

Partie 2: Configurer les périphériques et vérifier la connectivité

Dans cette deuxième partie, vous allez mettre en place la topologie du réseau et configurer les paramètres de base sur le routeur et le commutateur. Reportez-vous à la topologie et à la table d'adressage au début de ces travaux pratiques pour trouver le nom des périphériques et les informations d'adressage.

Étape 1: Configurez l'adresse IPv4 du PC.

Configurez l'adresse IPv4, le masque de sous-réseau et l'adresse de la passerelle par défaut de PC-A en fonction de la table d'adressage.

Étape 2: Configurez le routeur.

- a. Accédez au routeur par la console et passez en mode d'exécution privilégié.
- b. Réglez l'heure sur le routeur.
- c. Passez en mode de configuration globale.
 - 1) Attribuez un nom de périphérique au routeur d'après la topologie et la table d'adressage.
 - 2) Désactivez la recherche DNS.
 - 3) Créez une bannière MOTD (Message Of The Day, autrement dit, message du jour) qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit.
 - 4) Attribuez **class** comme mot de passe chiffré d'exécution privilégié.
 - 5) Choisissez **cisco** comme mot de passe de console et activez l'accès par connexion de console.
 - 6) Chiffrez les mots de passe en clair.
 - 7) Créez un nom de domaine, **cisco.com**, pour l'accès SSH.
 - 8) Créez un utilisateur, **admin**, avec le mot de passe secret **cisco** pour l'accès SSH.

- 9) Générez une clé de module RSA. Indiquez **1024** pour le nombre de bits.
- d. Configurez l'accès avec les lignes VTY.
 - 1) Utilisez la base de données locale pour l'authentification pour SSH.
 - 2) Activez SSH uniquement pour l'accès par connexion.
- e. Repassez en mode de configuration globale.
 - 1) Créez l'interface Loopback 0 et attribuez l'adresse IP selon la table d'adressage.
 - 2) Configurez et activez l'interface G0/1 sur le routeur.
 - 3) Configurez les descriptions d'interface pour G0/1 et L0.
 - 4) Enregistrez le fichier de configuration en cours dans le fichier de configuration initiale.

Étape 3: Configurez le commutateur.

- a. Accédez au commutateur par la console et passez en mode d'exécution privilégié.
- b. Réglez l'heure sur le commutateur.
- c. Passez en mode de configuration globale.
 - 1) Attribuez un nom de périphérique au commutateur d'après la topologie et la table d'adressage.
 - 2) Désactivez la recherche DNS.
 - 3) Créez une bannière MOTD (Message Of The Day, autrement dit, message du jour) qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit.
 - 4) Attribuez **class** comme mot de passe chiffré d'exécution privilégié.
 - 5) Chiffrez tous les mots de passe en clair.
 - 6) Créez un nom de domaine, **cisco.com**, pour l'accès SSH.
 - 7) Créez un utilisateur, **admin**, avec le mot de passe secret **cisco** pour l'accès SSH.
 - 8) Générez une clé RSA. Indiquez **1024** pour le nombre de bits.
 - 9) Créez et activez une adresse IP sur le commutateur d'après la topologie et la table d'adressage.
 - 10) Configurez la passerelle par défaut sur le commutateur.
 - 11) Choisissez **cisco** comme mot de passe de console et activez l'accès par connexion de console.
- d. Configurez l'accès avec les lignes VTY.
 - 1) Utilisez la base de données locale pour l'authentification pour SSH.
 - 2) Activez SSH uniquement pour l'accès par connexion.
 - 3) Enregistrez le fichier de configuration en cours dans le fichier de configuration initiale.
- e. Passez au mode approprié pour configurer les descriptions d'interface pour F0/5 et F0/6.

Étape 4: Vérifiez la connectivité du réseau.

- a. À partir d'une invite de commande sur PC-A, envoyez une requête ping à l'adresse IP du VLAN 1 de S1. Rectifiez vos configurations physiques et logiques si les requêtes ping n'aboutissent pas.
- b. À partir de l'invite de commande de PC-A, envoyez une requête ping à l'adresse IP de la passerelle par défaut sur R1. Rectifiez vos configurations physiques et logiques si les requêtes ping n'aboutissent pas.
- c. À partir de l'invite de commande de PC-A, envoyez une requête ping à l'interface de bouclage sur R1. Rectifiez vos configurations physiques et logiques si les requêtes ping n'aboutissent pas.

- d. Reconnectez-vous via la console au commutateur et envoyez une requête ping à l'adresse IP G0/1 sur R1. Rectifiez vos configurations physiques et logiques si les requêtes ping n'aboutissent pas.

Partie 3: Collecter des informations sur les périphériques réseau

Dans la troisième partie, vous allez utiliser différentes commandes pour recueillir des informations sur les périphériques de votre réseau, ainsi que sur les caractéristiques des performances. La documentation du réseau est un élément très important de la gestion du réseau. Il est essentiel d'inclure les deux topologies, physique et logique, autant que de vérifier les modèles de plate-forme et les versions IOS de vos périphériques réseau. Un professionnel doit savoir quelles commandes utiliser pour collecter ces informations.

Étape 1: Recueillez des informations sur R1 en utilisant les commandes de l'IOS.

L'une des étapes de base consiste à recueillir des informations sur le périphérique physique, ainsi que des informations relatives au système d'exploitation.

- a. Exécutez la commande adéquate pour obtenir les informations suivantes :

Modèle de routeur : _____
Version de l'IOS : _____
RAM totale : _____
NVRAM totale : _____
Mémoire Flash totale : _____
Fichier d'image IOS : _____
Registre de configuration : _____
Module technologique : _____

Quelle commande avez-vous exécutée pour recueillir ces informations ?

- b. Exécutez la commande appropriée pour afficher un récapitulatif des informations importantes sur les interfaces de routeur. Inscrivez ci-dessous la commande utilisée, avec les résultats obtenus.

Remarque : indiquez uniquement les interfaces qui possèdent des adresses IP.

- c. Exécutez la commande appropriée pour afficher la table de routage. Inscrivez ci-dessous la commande utilisée, avec les résultats obtenus.

- d. Quelle commande utiliseriez-vous pour afficher le mappage des adresses couche 2 -> couche 3 sur le routeur ? Inscrivez ci-dessous la commande utilisée, avec les résultats obtenus.

- e. Quelle commande utiliseriez-vous pour avoir des informations détaillées sur toutes les interfaces du routeur ou sur une interface spécifique ? Inscrivez cette commande ci-dessous.

- f. Cisco propose un protocole très puissant. Celui-ci fonctionne sur la couche 2 du modèle OSI. Il peut vous aider à déterminer comment les périphériques Cisco sont physiquement connectés, ainsi que les numéros de modèle et même les versions IOS et l'adressage IP. Quelle commande (ou quelles commandes) utiliseriez-vous sur le routeur R1 pour recueillir des informations sur le commutateur S1 qui vous aideront à compléter le tableau ci-dessous ?

ID de périphérique	Interface locale	Fonctionnalité	Numéro de modèle	ID du port distant	Adresse IP	Version du logiciel IOS

- g. Vous pouvez tester très simplement vos périphériques réseau en essayant d'y accéder via Telnet. Souvenez-vous toutefois que Telnet n'est pas un protocole sécurisé. En principe, il ne doit pas être activé. À l'aide d'un client Telnet, tel que Tera Term ou PuTTY, essayez d'établir une connexion Telnet avec R1 en utilisant l'adresse IP de la passerelle par défaut. Notez vos résultats ci-dessous.

- h. À partir de PC-A, faites un test pour vous assurer que SSH fonctionne correctement. Avec un client SSH, tel que Tera Term ou PuTTY, établissez une connexion SSH avec R1 à partir de PC-A. Si vous obtenez un message d'avertissement relatif à une autre clé, cliquez sur **Continue** (Continuer). Connectez-vous avec le nom d'utilisateur et le mot de passe appropriés, ceux que vous avez créés dans la deuxième partie. Avez-vous réussi ?

Les différents mots de passe configurés sur votre routeur doivent être aussi fiables et protégés que possible.

Remarque : les mots de passe utilisés dans les travaux pratiques (**cisco** et **class**) ne respectent pas les bonnes pratiques en matière de mots de passe forts. Ils sont utilisés uniquement pour les travaux pratiques. Par défaut, le mot de passe de console et tous les mots de passe vty configurés s'affichent en clair dans votre fichier de configuration.

- i. Vérifiez que tous vos mots de passe du fichier de configuration sont chiffrés. Inscrivez ci-dessous la commande utilisée, avec les résultats obtenus.

Commande : _____

Le mot de passe de console est-il chiffré ? _____

Le mot de passe SSH est-il chiffré ? _____

Étape 2: Recueillez des informations sur S1 avec les commandes IOS.

De nombreuses commandes utilisées sur R1 peuvent également l'être avec le commutateur. Cependant, il y a des différences pour certaines commandes.

- a. Exécutez la commande adéquate pour obtenir les informations suivantes :

Modèle de commutateur : _____

Version de l'IOS : _____

NVRAM totale : _____

Fichier d'image IOS : _____

Quelle commande avez-vous exécutée pour recueillir ces informations ?

- b. Exécutez la commande appropriée pour afficher un récapitulatif des informations d'état sur les interfaces de commutateur. Inscrivez ci-dessous la commande utilisée, avec les résultats obtenus.

Remarque : n'indiquez que les interfaces actives.

- c. Exécutez la commande appropriée pour afficher la table des adresses MAC du commutateur. Indiquez les adresses MAC dynamiques uniquement dans l'espace prévu à cet effet ci-dessous.

- d. Assurez-vous que l'accès VTY via Telnet est désactivé sur S1. À l'aide d'un client Telnet, tel que Tera Term ou PuTTY, essayez d'établir une connexion Telnet avec S1 en utilisant l'adresse 192.168.1.11. Notez vos résultats ci-dessous.

- e. À partir de PC-A, faites un test pour vous assurer que SSH fonctionne correctement. Avec un client SSH, tel que Tera Term ou PuTTY, établissez une connexion SSH avec S1 à partir de PC-A. Si vous obtenez un message d'avertissement relatif à une autre clé, cliquez sur **Continue** (Continuer). Connectez-vous avec le nom d'utilisateur et le mot de passe appropriés. Avez-vous réussi ?

- f. Complétez le tableau ci-dessous avec les informations sur le routeur R1 en utilisant la ou les commandes appropriées sur S1.

ID de périphérique	Interface locale	Fonctionnalité	Numéro de modèle	ID du port distant	Adresse IP	Version du logiciel IOS

- g. Vérifiez que tous vos mots de passe du fichier de configuration sont chiffrés. Inscrivez ci-dessous la commande utilisée, avec les résultats obtenus.

Commande : _____

Le mot de passe de console est-il chiffré ? _____

Étape 3: Recueillez les informations sur PC-A.

Avec différentes commandes d'utilitaire Windows, rassemblez des informations sur PC-A.

- a. À l'invite de PC-A, exécutez la commande **ipconfig /all** et notez les résultats ci-dessous.

Quelle est l'adresse IP de PC-A ?

Quel est le masque de sous-réseau de PC-A ?

Quelle est l'adresse de la passerelle par défaut de PC-A ?

Quelle est l'adresse MAC de PC-A ?

- b. Exécutez la commande appropriée pour tester la pile de protocoles TCP/IP avec la carte réseau. Quelle commande avez-vous utilisée ?

- c. Envoyez une requête ping à l'interface de bouclage de R1 à partir de l'invite de commande de PC-A. La requête ping a-t-elle abouti ?

- d. Exécutez la commande appropriée sur PC-A pour tracer la liste de sauts de routeur pour les paquets provenant de PC-A et à destination de l'interface de bouclage de R1. Indiquez la commande et les résultats ci-dessous. Quelle commande avez-vous utilisée ?

- e. Exécutez la commande appropriée sur PC-A pour trouver les mappages d'adresses couches 2 -> couche 3 figurant sur votre carte réseau. Notez les résultats ci-dessous. Indiquez uniquement les réponses pour le réseau 192.168.1.0/24. Quelle commande avez-vous utilisée ?

Remarques générales

Pourquoi est-il important de documenter vos périphériques réseau ?

Tableau récapitulatif des interfaces des routeurs

Résumé des interfaces des routeurs				
Modèle du routeur	Interface Ethernet 1	Interface Ethernet 2	Interface série 1	Interface série 2
1 800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
<p>Remarque : pour savoir comment le routeur est configuré, observez les interfaces afin d'identifier le type de routeur ainsi que le nombre d'interfaces qu'il comporte. Il n'est pas possible de répertorier de façon exhaustive toutes les combinaisons de configurations pour chaque type de routeur. Ce tableau inclut les identifiants des différentes combinaisons d'interfaces Ethernet et série possibles dans le périphérique. Ce tableau ne comporte aucun autre type d'interface, même si un routeur particulier peut en contenir un. L'exemple de l'interface RNIS BRI peut illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans les commandes Cisco IOS.</p>				