ENI Ecole Informatique

Une formation, un diplôme, un emploi

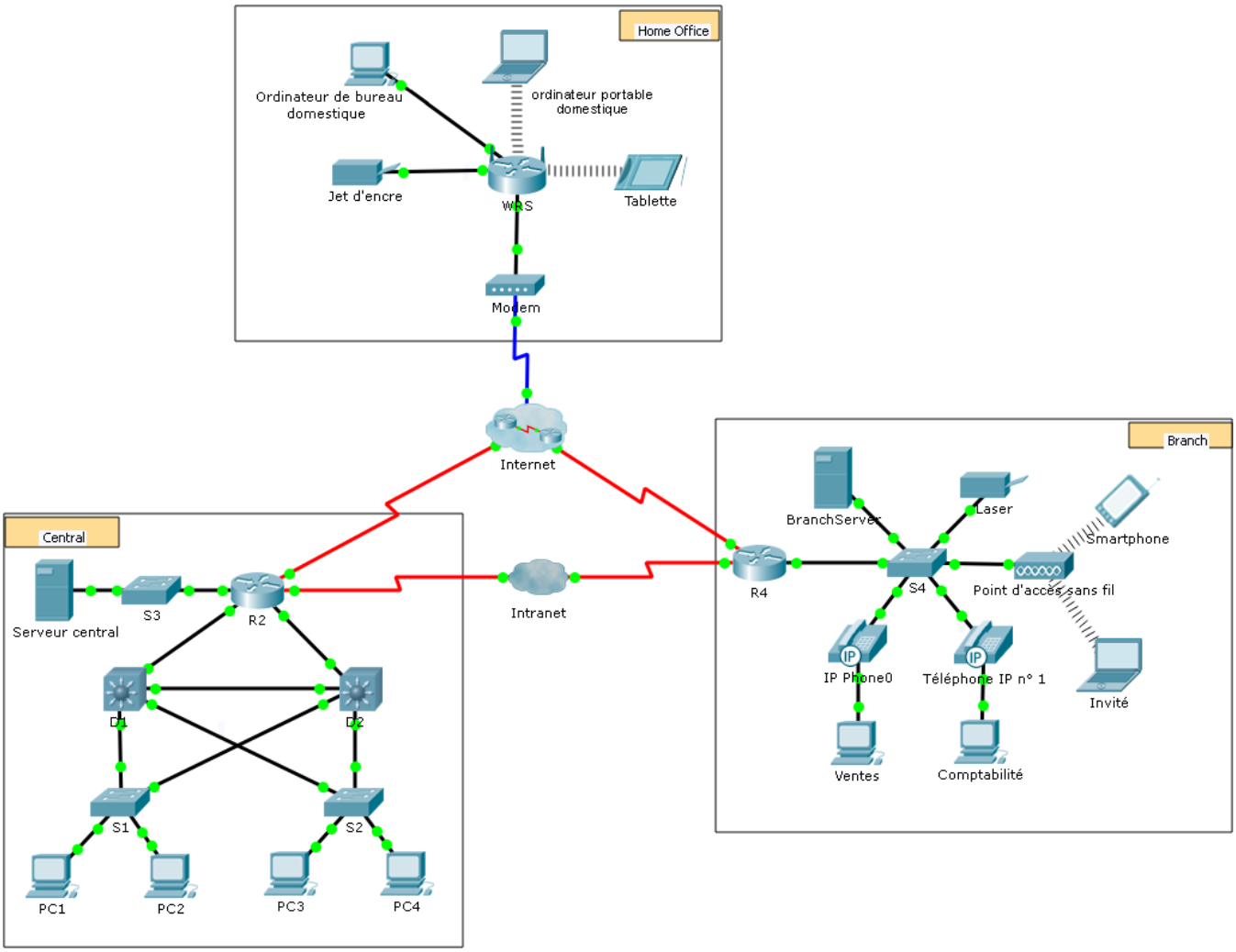
Cisco 1 – Initiation aux réseaux

Cahier d'ateliers Packet Tracer

Version 1.0

Packet Tracer – Aide et conseils pour la navigation

Topologie



Objectifs

Présentation du programme Packet Tracer

Contexte

Packet Tracer est un logiciel flexible et interactif que vous pouvez utiliser chez vous et qui vous aidera dans le cadre de votre préparation à la certification CCNA (Cisco Certified Network Associate). Packet Tracer vous permet de tester le comportement d'un réseau, de concevoir des modèles de réseau et de mettre en pratique des hypothèses.

Dans cet exercice, vous découvrirez un réseau relativement complexe qui permet d'illustrer certaines fonctionnalités de Packet Tracer. Ainsi, vous apprendrez comment accéder à l'Aide et aux didacticiels. Vous découvrirez comment utiliser les différents modes et espaces de travail. Vous devrez peut-être ajuster la taille de la fenêtre de Packet Tracer pour afficher la totalité du réseau. Au besoin, utilisez les outils de zoom avant et arrière pour adapter la taille de la fenêtre de Packet Tracer.

Remarque : il n'est pas indispensable de comprendre tout ce que vous voyez et faites au cours de cet exercice. N'hésitez pas à explorer le réseau par vous-même. Si vous souhaitez poursuivre de manière plus méthodique, procédez comme suit. Répondez de votre mieux aux questions.

Étape 1: Accédez aux pages d'aide de Packet Tracer, aux vidéos du didacticiel et aux ressources en ligne.

a. Vous pouvez accéder de deux manières aux pages d'aide de Packet Tracer :

- Cliquez sur l'icône en forme de point d'interrogation située dans le coin supérieur droit de la barre d'outils de menu.
- Cliquez sur le menu Help (Aide), puis choisissez Contents (Sommaire).

b. Accédez aux vidéos du didacticiel de Packet Tracer en cliquant sur **Help** (Aide) > **Tutorials** (Didacticiels). Ces vidéos constituent une démonstration visuelle des informations affichées dans les pages de l'Aide et présentent divers aspects du logiciel Packet Tracer. Avant de poursuivre cet exercice, vous devez vous familiariser avec l'interface et le mode Simulation de Packet Tracer.

1) Regardez la vidéo **Interface Overview** (Présentation de l'interface) proposée dans la section **Getting Started** (Premiers pas) des Tutorials (Didacticiels).

2) Regardez la vidéo **Simulation Environment** (Environnement de simulation) proposée dans la section modes **Realtime** (Temps réel) et **Simulation** des **Tutorials** (Didacticiels).

c. Recherchez le didacticiel « Configuring Devices Using the Desktop Tab » (« Configuration des périphériques à l'aide de l'onglet Bureau »). Regardez la première partie du didacticiel et répondez à la question suivante : quelles informations pouvez-vous configurer dans la fenêtre Configuration IP ?

_____

_____

Étape 2: Alternez entre les modes Realtime (Temps réel) et Simulation.

a. Recherchez le terme **Realtime** (Temps réel) dans le coin inférieur droit de l'interface de Packet Tracer. En mode Temps réel, votre réseau fonctionne toujours comme un vrai, que vous soyez ou non en train d'y travailler. Vos configurations sont effectuées en temps réel et le réseau aussi répond presque instantanément.

b. Cliquez sur l'onglet situé juste derrière l'onglet **Realtime** (Temps réel) pour passer en mode **Simulation**. Le mode Simulation permet d'observer le fonctionnement du réseau au ralenti, d'analyser les trajets empruntés par les données et d'inspecter en détail les paquets de données.

c. Cliquez sur **Auto Capture / Play** (Capture automatique/Lecture) dans le panneau de simulation. Vous devriez maintenant voir les paquets de données, représentés sous la forme d'enveloppes de différentes couleurs, se déplaçant entre les périphériques.

d. Cliquez à nouveau sur **Auto Capture / Play** (Capture automatique/Lecture) pour interrompre la simulation.

e. Cliquez sur **Capture / Forward** (Capture/Avance) pour parcourir la simulation. Cliquez à plusieurs reprises sur le bouton pour voir l'effet produit.

f. Dans la topologie réseau de gauche, cliquez sur l'une des enveloppes d'un périphérique intermédiaire et analysez ce qui se trouve à l'intérieur. Au cours de votre certification CCNA, vous aurez l'occasion d'étudier la quasi-totalité du contenu de ces enveloppes. Pour l'instant, voyez si vous pouvez répondre aux questions suivantes :

- Dans l'onglet **OSI Model** (Modèle OSI), combien de colonnes **In Layers** (Couches internes) et **Out Layers** (Couches externes) contiennent des informations ?

  _____

- Sous les onglets **Inbound PDU Details** (Entrée de l'unité de données de protocole) et **Outbound PDU Details** (Sortie de l'unité de données de protocole), quels sont les en-têtes des principales sections ?

  _____

- Cliquez alternativement sur les onglets **Inbound PDU Details** (Entrée de l'unité de données de protocole) et **Outbound PDU Details** (Sortie de l'unité de données de protocole). Les informations affichées varient-elles ? Si oui, lesquelles ?

  _____

  _____

g. Cliquez sur le bouton bascule situé au-dessus de **Simulation** dans le coin inférieur droit pour revenir au mode **Realtime** (Temps réel).

Étape 3: Alternez entre les vues Logique et Physique.

a. Repérez le terme **Logical** (Logique) dans le coin supérieur gauche de l'interface de Packet Tracer. Vous vous trouvez actuellement dans l'espace de travail Logique, où vous passerez la majorité de votre temps à créer, configurer, étudier et dépanner des réseaux.

Remarque : bien que vous puissiez ajouter une carte géographique en guise d'image d'arrière-plan à l'espace de travail Logique, elle n'a généralement aucun lien avec l'emplacement physique réel des périphériques.

b. Cliquez sur l'onglet situé en dessous de **Logical** (Logique) pour accéder à l'espace de travail **Physical** (Physique). Le rôle de l'espace de travail Physique est de donner une dimension physique à la topologie de votre réseau logique. Il vous donne ainsi une idée de l'échelle et du positionnement de votre réseau, vous permettant de voir à quoi il ressemblerait dans un environnement réel.

c. Au cours de votre certification CCNA, vous utiliserez parfois cet espace de travail. Pour l'instant, sachez simplement que vous pouvez l'utiliser. Pour en savoir plus sur l'espace de travail Physique, reportez-vous aux fichiers d'aide et aux vidéos du didacticiel.

d. Cliquez sur le bouton bascule situé sous **Physical** (Physique) dans le coin supérieur droit pour revenir à l'espace de travail **Logical** (Logique).

Défi

Maintenant que vous avez eu l'occasion d'explorer le réseau illustré dans cet exercice Packet Tracer, vous avez peut-être acquis certaines compétences que vous souhaitez mettre en pratique. Ou peut-être voulez-vous explorer ce réseau de manière plus détaillée. Nous sommes conscients que la majeure partie de ce que vous voyez et utilisez dans Packet Tracer dépasse votre niveau de compétences actuel. Toutefois, vous voudrez peut-être relever quelques défis. Ne vous inquiétez pas si vous rencontrez des difficultés. Vous maîtriserez bientôt l'utilisation et la conception des réseaux avec Packet Tracer.

- Ajoutez un périphérique terminal à la topologie et raccordez-le à l'un des réseaux locaux à l'aide d'une connexion multimédia. Que faut-il d'autre à ce périphérique pour envoyer des données aux autres utilisateurs finaux ? Pouvez-vous fournir ces informations ? Existe-t-il un moyen de vérifier que vous avez correctement connecté le périphérique ?
- Ajoutez un nouveau périphérique intermédiaire à l'un des réseaux et connectez-le à l'un des LAN ou des WAN à l'aide d'une connexion avec le support. Que faut-il d'autre à ce périphérique pour servir d'intermédiaire aux autres équipements du réseau ?

- Ouvrez une nouvelle instance de Packet Tracer. Créez un nouveau réseau avec au moins deux LAN connectés par l'intermédiaire d'un WAN. Connectez l'ensemble des périphériques. Examinez l'exercice Packet Tracer initial et voyez ce que vous pouvez faire d'autre pour rendre votre nouveau réseau fonctionnel. Notez vos idées et enregistrez votre fichier Packet Tracer. Vous voudrez peut-être revenir plus tard sur votre réseau, lorsque vous aurez acquis plus de compétences.

Suggestion de barème de notation

Emplacement de la question	Nombre maximum de points	Points obtenus
Étape 1c	4	
Étape 2f	6	
Score total	**10**	

Packet Tracer - Utilisation de Cisco IOS

Topologie

Objectifs

Partie 1 : Établir des connexions de base, accéder à l'interface en ligne de commande et découvrir l'Aide

Partie 2 : Découvrir les modes d'exécution

Partie 3 : Régler l'horloge

Contexte

Cet exercice vous permettra d'acquérir les aptitudes nécessaires à l'utilisation de Cisco IOS, notamment les différents modes d'accès utilisateur, les divers modes de configuration, ainsi que les commandes régulièrement utilisées. Vous accéderez également à l'aide contextuelle en configurant la commande **clock**.

Partie 1: Établir des connexions de base, accéder à l'interface en ligne de commande et découvrir l'Aide

Dans la partie 1 de cet exercice, vous connecterez un ordinateur à un commutateur par le biais d'une connexion console et découvrirez divers modes de commande et fonctions d'aide.

Étape 1: Raccordez PC1 à S1 à l'aide d'un câble de console.

a. Cliquez sur l'icône **Connexions** (celle ayant la forme d'un éclair) située dans le coin inférieur gauche de la fenêtre Packet Tracer.

b. Sélectionnez le câble Console bleu clair en cliquant dessus. Le pointeur de la souris prend une apparence similaire à celle d'un connecteur sur lequel pend un câble.

c. Cliquez sur **PC1**. Une fenêtre affiche une option relative à une connexion RS-232.

d. Faites glisser l'autre extrémité de la connexion console vers le commutateur S1, puis cliquez sur le commutateur afin d'accéder à la liste des connexions.

e. Sélectionnez le port **Console** afin d'établir la connexion.

Étape 2: Établissez une session de terminal avec S1.

a. Cliquez sur **PC1** puis sélectionnez l'onglet **Bureau**.

b. Cliquez sur l'icône de l'application **Terminal**. Vérifiez que les paramètres de configuration des ports par défaut sont corrects.

Quelle est la valeur du paramètre des bits par seconde ? _____

c. Cliquez sur **OK**.

d. L'écran qui s'affiche peut contenir plusieurs messages. Le message suivant doit figurer quelque part sur l'écran : `Press RETURN to get started!` (Appuyez sur ENTRÉE pour démarrer). Appuyez sur ENTRÉE.

Quelle est l'invite affichée à l'écran ? _____

Étape 3: Découvrez l'Aide IOS.

a. L'IOS peut fournir de l'aide sur les commandes en fonction du niveau auquel l'utilisateur accède. L'invite actuellement affichée est appelée **User EXEC** (mode d'exécution utilisateur) et le périphérique attend une commande. La forme la plus simple de l'aide consiste à entrer un point d'interrogation (?) à l'invite afin d'afficher la liste des commandes.

```
S1> ?
```

Quelle commande commence par la lettre « C » ? _____

b. À l'invite, tapez **t**, suivi d'un point d'interrogation (**?**).

```
S1> t?
```

Quelles sont les commandes affichées ? _____

c. À l'invite, tapez **te**, suivi d'un point d'interrogation (**?**).

```
S1> te?
```

Quelles sont les commandes affichées ? _____

Ce type d'aide porte le nom d'aide **contextuelle**. Elle fournit davantage d'informations une fois que les commandes sont développées.

Partie 2: Découvrir les modes d'exécution

Dans la partie 2 de cet exercice, vous passerez en mode d'exécution privilégié et exécuterez des commandes supplémentaires.

Étape 1: Passez en mode d'exécution privilégié.

a. À l'invite, tapez un point d'interrogation (**?**).

```
S1> ?
```

Quelle information affichée décrit la commande **enable** ? _____

b. Tapez **en** et appuyez sur la touche **Tab**.

```
S1> en<Tab>
```

Que voyez-vous apparaître après avoir appuyé sur la touche **Tab** ? _____

La touche Tabulation peut être utilisée pour compléter une commande partielle. Lorsque vous ne tapez qu'une partie d'une commande, la touche **Tab** peut être utilisée pour compléter cette commande. Si les caractères saisis sont suffisants pour identifier la commande, comme dans le cas de la commande **enable**, le reste de cette commande s'affiche.

Que se passerait-il si vous saisissiez **te<Tab>** à l'invite ?

_____

_____

_____

_____

c. Entrez la commande **enable** et appuyez sur Entrée. Quel changement observez-vous sur l'invite ?

_____

_____

d. À l'invite, tapez le point d'interrogation (**?**).

```
S1# ?
```

Une seule commande commence par la lettre « C » en mode d'exécution utilisateur. Combien de commandes sont affichées maintenant que le mode d'exécution privilégié est actif ? (**Conseil** : pour afficher uniquement les commandes commençant par « C », vous pouvez taper « c? ».)

_____

_____

Étape 2: Passez en mode de configuration globale.

a. Lorsque vous êtes en mode d'exécution privilégié, **configure** est l'une des commandes qui commencent par la lettre « C ». Tapez soit la commande complète, soit suffisamment de lettres pour qu'elle soit identifiable. Appuyez sur la touche <**Tab**> pour exécuter la commande, puis sur Entrée.

```
S1# configure
```

Quel est le message affiché ?

_____

b. Appuyez sur Entrée pour accepter le paramètre par défaut qui est inclus entre crochets **[terminal]**.

Quel changement observez-vous sur l'invite ? _____

c. Il s'agit du mode de configuration globale. Ce mode sera examiné en détail dans les prochains exercices et à l'occasion des travaux pratiques. Pour l'instant, revenez en mode d'exécution privilégié en tapant **end**, **exit** ou **Ctrl-Z**.

```
S1(config)# exit
S1#
```

Partie 3: Régler l'horloge

Étape 1: Utilisez la commande clock.

a. Utilisez la commande **clock** pour examiner plus en détail l'aide et la syntaxe de la commande. Tapez **show clock** à l'invite du mode d'exécution privilégié.

```
S1# show clock
```

Quelle information s'affiche ? Quelle est l'année affichée ?

_____

b. Utilisez l'aide contextuelle et la commande **clock** pour régler l'heure du commutateur à l'heure actuelle. Entrez la commande **clock** et appuyez sur Entrée.

```
S1# clock<ENTER>
```

Quelle information s'affiche ? _____

c. Le message « % Incomplete command » (commande incomplète) est renvoyé par l'IOS. Il indique que la commande **clock** requiert plus de paramètres. Lorsque des informations supplémentaires sont nécessaires, vous pouvez obtenir de l'aide en insérant un espace après la commande suivi du point d'interrogation (?).

```
S1# clock ?
```

Quelle information s'affiche ? _____

d. Réglez l'horloge à l'aide de la commande **clock set**. Poursuivez pas à pas l'exécution de la commande.

```
S1# clock set ?
```

Quelle est l'information demandée ? _____

Qu'auriez-vous vu s'afficher si seule la commande **clock set** avait été entrée, sans demande d'aide par le biais du point d'interrogation ? _____

e. En tenant compte des informations demandées lors de l'exécution de la commande **clock set ?**, entrez 3 heures de l'après-midi en utilisant le format 24 heures, c'est-à-dire 15:00:00. Vérifiez si d'autres paramètres sont requis.

```
S1# clock set 15:00:00 ?
```

Le résultat renvoie une demande pour plus d'informations :

```
<1-31>  Day of the month
MONTH   Month of the year
```

f. Essayez de définir la date au 01/31/2035 en utilisant le format demandé. Il peut être nécessaire de demander une assistance supplémentaire en utilisant l'aide contextuelle pour terminer le processus. Lorsque vous avez terminé, exécutez la commande **show clock** pour afficher les paramètres de l'horloge. Le résultat de la commande devrait s'afficher comme suit :

```
S1# show clock
*15:0:4.869 UTC Tue Jan 31 2035
```

g. En cas d'échec, essayez la commande suivante afin d'obtenir le résultat ci-dessus :

```
S1# clock set 15:00:00 31 Jan 2035
```

Étape 2: Examinez d'autres messages de commande.

a. IOS fournit divers résultats pour les commandes incorrectes ou incomplètes. Continuez à utiliser la commande **clock** pour découvrir des messages supplémentaires que vous êtes susceptible de rencontrer en apprenant à utiliser IOS.

b. Exécutez la commande suivante et notez les messages :

```
S1# cl
```

Quelle information a été renvoyée ? _____

```
S1# clock
```

Quelle information a été renvoyée ? _____

```
S1# clock set 25:00:00
```

Quelle information a été renvoyée ?

_____

_____

```
S1# clock set 15:00:00 32
```

Quelle information a été renvoyée ?

_____

_____

Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points obtenus
Partie 1 : Établir des connexions de base, accéder à l'interface en ligne de commande et découvrir l'Aide	Étape 2b	5	
	Étape 2d	5	
	Étape 3a	5	
	Étape 3b	5	
	Étape 3c	5	
Total de la Partie 1		**25**	
Partie 2 : Découvrir les modes d'exécution	Étape 1a	5	
	Étape 1b	5	
	Étape 1c	5	
	Étape 1d	5	
	Étape 2a	5	
	Étape 2b	5	
Total de la Partie 2		**30**	
Partie 3 : Régler l'horloge	Étape 1a	5	
	Étape 1b	5	
	Étape 1c	5	
	Étape 1d	5	
	Étape 2b	5	
Total de la Partie 3		**25**	
Score relatif à Packet Tracer		**20**	
Score total		**100**	

Packet Tracer - Mise en œuvre de la connectivité de base

Topologie

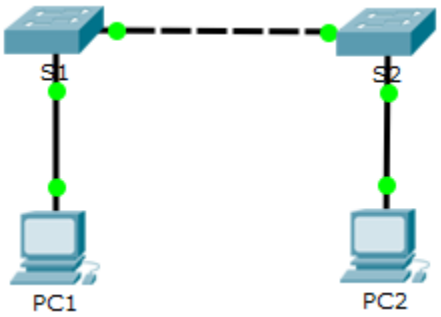


Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	Carte réseau	192.168.1.1	255.255.255.0
PC2	Carte réseau	192.168.1.2	255.255.255.0

Objectifs

Partie 1 : Effectuer la configuration de base des commutateurs S1 et S2

Partie 2 : Configurer les ordinateurs

Partie 3 : Configurer l'interface de gestion des commutateurs

Contexte

Au cours de cet exercice, vous allez effectuer des configurations de base sur les commutateurs. Vous mettrez ensuite en œuvre la connectivité de base en configurant l'adressage IP sur les commutateurs et les ordinateurs. Après la configuration de l'adressage IP, vous utiliserez plusieurs commandes **show** pour vérifier les configurations et la commande **ping** pour vérifier la connectivité de base entre les périphériques.

Partie 1: Effectuer une configuration de base sur S1 et S2

Exécutez les étapes suivantes sur S1 et S2.

Étape 1: Configurez S1 avec un nom d'hôte.

a. Cliquez sur S1, puis sur l'onglet **CLI**.

b. Entrez la commande appropriée pour configurer le nom d'hôte en tant que **S1**.

Étape 2: Configurez le mot de passe de console ainsi que celui du mode d'exécution privilégié.

a. Utilisez **cisco** comme mot de passe de console.

b. Utilisez **class** comme mot de passe d'exécution privilégié.

Étape 3: Vérifiez les configurations de mot de passe pour S1.

Comment vérifier que les deux mots de passe ont été configurés correctement ?

_____

_____

_____

Étape 4: Configurez une bannière MOTD.

Utilisez un texte de bannière approprié pour avertir de l'accès non autorisé. Voici un exemple de texte :

Accès autorisé uniquement. Violators will be prosecuted to the full extent of the law.

Étape 5: Enregistrez le fichier de configuration dans la mémoire NVRAM.

Quelle commande devez-vous exécuter pour accomplir cette étape ?

_____

_____

Étape 6: Répétez les étapes 1 à 5 pour S2.

Partie 2: Configurer les ordinateurs

Configurez PC1 et PC2 avec des adresses IP.

Étape 1: Configurez les deux ordinateurs avec des adresses IP.

a. Cliquez sur PC1 puis sélectionnez l'onglet **Bureau**.

b. Cliquez sur **IP Configuration** (Configuration IP). Dans la table d'adressage ci-dessus, vous pouvez constater que l'adresse IP de PC1 est 192.168.1.1 et que le masque de sous-réseau est 255.255.255.0. Entrez ces informations pour PC1 dans la fenêtre **IP Configuration** (Configuration IP).

c. Répétez les étapes 1a et 1b pour PC2.

Étape 2: Testez la connectivité avec les commutateurs.

a. Cliquez sur PC1. Fermez la fenêtre **IP Configuration** (Configuration IP) si elle est toujours ouverte. Dans l'onglet **Bureau**, cliquez sur **Command Prompt** (Invite de commandes).

b. Entrez la commande **ping** et l'adresse IP de S1, puis appuyez sur Entrée.

```
Packet Tracer PC Command Line 1.0
PC> ping 192.168.1.253
```

Avez-vous réussi ? Expliquez votre réponse.

_____

_____

_____

Partie 3: Configurer l'interface de gestion du commutateur

Configurez S1 et S2 avec une adresse IP.

Étape 1: Configurez S1 avec une adresse IP.

Les commutateurs peuvent être utilisés en tant que périphériques prêts à l'emploi. Cela signifie qu'ils n'ont pas besoin d'être configurés pour fonctionner. Les commutateurs transmettent les informations d'un port à un autre en fonction des adresses MAC. Dans ce cas, pourquoi faut-il les configurer avec une adresse IP ?

_____

_____

_____

Utilisez les commandes suivantes pour configurer S1 avec une adresse IP.

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.253 255.255.255.0
S1(config-if)# no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#
S1(config-if)# exit
S1#
```

Pourquoi devez-vous inclure la commande **no shutdown** ?

_____

_____

Étape 2: Configurez S2 avec une adresse IP.

Utilisez les informations de la table d'adressage pour configurer S2 avec une adresse IP.

Étape 3: Vérifiez la configuration des adresses IP sur S1 et S2.

Utilisez la commande **show ip interface brief** pour afficher l'adresse IP et l'état de tous les ports et interfaces des commutateurs. Vous pouvez également utiliser la commande **show running-config**.

Étape 4: Enregistrez les configurations de S1 et S2 en mémoire NVRAM.

Quelle commande permet d'enregistrer le fichier de configuration contenu dans la mémoire vive (RAM) en mémoire NVRAM ?

_____

Étape 5: vérification de la connectivité du réseau.

La commande **ping** permet de vérifier la connectivité réseau. Il est très important de disposer d'une connectivité sur tout le réseau. En cas d'échec, une mesure corrective doit être prise. Envoyez une requête ping à l'adresse IP de S1 et S2 à partir de PC1 et PC2.

a. Cliquez sur PC1 puis sélectionnez l'onglet **Bureau**.

b. Cliquez sur **Command Prompt**.

c. Envoyez une requête ping à l'adresse IP de PC2.

d. Envoyez une requête ping à l'adresse IP de S1.

e. Envoyez une requête ping à l'adresse IP de S2.

Remarque : vous pouvez également utiliser la commande **ping** dans l'interface de ligne de commande du commutateur et sur PC2.

Toutes les requêtes ping doivent aboutir. Si le résultat de votre première requête ping est 80 %, recommencez ; il devrait maintenant être égal à 100 %. Vous apprendrez plus tard pourquoi une requête ping peut parfois échouer la première fois. Si vous ne pouvez envoyer de requête ping vers aucun des périphériques, vérifiez de nouveau votre configuration pour vous assurer qu'elle ne comporte pas d'erreurs.

Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points obtenus
Partie 1 : Effectuer la configuration de base des commutateurs S1 et S2	Étape 3	2	
	Étape 5	2	
Partie 2 : Configurer les ordinateurs	Étape 2b	2	
Partie 3 : Configurer l'interface de gestion des commutateurs	Étape 1, q1	2	
	Étape 1, q2	2	
	Étape 4	2	
	Questions	**12**	
	Score relatif à Packet Tracer	**88**	
	Score total	**100**	

Packet Tracer - Projet d'intégration des compétences

Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau
	VLAN 1		255.255.255.0
	VLAN 1		255.255.255.0
	Carte réseau		255.255.255.0
	Carte réseau		255.255.255.0

Objectifs

- Configurer des noms d'hôtes et des adresses IP sur deux commutateurs Cisco Internetwork Operating System (IOS) à l'aide de l'interface en ligne de commande.
- Utiliser les commandes Cisco IOS pour spécifier ou limiter l'accès aux configurations de périphérique.
- Utiliser les commandes IOS pour enregistrer la configuration en cours.
- Configurer deux périphériques hôtes avec des adresses IP.
- Vérifier la connectivité entre les deux périphériques finaux PC.

Scénario

Vous êtes le nouveau technicien responsable du réseau local (LAN). L'administrateur réseau vous demande de démontrer votre capacité à configurer un petit réseau local. Vos tâches comprennent la configuration des paramètres initiaux sur deux commutateurs à l'aide de Cisco IOS et la configuration des paramètres d'adresse IP sur les périphériques hôtes afin de fournir une connectivité de bout en bout. Vous devez utiliser deux commutateurs et deux hôtes/PC sur un réseau câblé et sous tension.

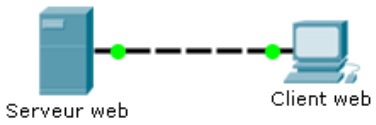
Conditions requises

- Utilisez une connexion console pour accéder à chaque commutateur.
- Attribuez aux commutateurs les noms _____ et _____.
- Utilisez le mot de passe _____ pour toutes les lignes.
- Utilisez le mot de passe secret _____ .
- Chiffrez tous les mots de passe en texte clair.
- Incluez le terme **warning** dans la bannière MOTD (« message of the day », ou message du jour).
- Configurez l'adressage pour tous les périphériques selon la table d'adressage.
- Enregistrez vos configurations.
- Vérifiez la connectivité entre tous les périphériques.

Remarque : cliquez sur **Check Results** (Vérifier les résultats) pour voir votre progression. Cliquez sur **Reset Activity** (Réinitialiser l'activité) pour générer un nouvel ensemble de conditions requises. Si vous cliquez sur ce bouton avant de terminer l'exercice, toutes les configurations seront perdues.

Packet Tracer - Analyse des modèles OSI et TCP/IP en action

Topologie



Objectifs

Partie 1 : Inspecter le trafic web HTTP

Partie 2 : Afficher les éléments de la suite de protocoles TCP/IP

Contexte

Cet exercice de simulation vise à fournir une base pour comprendre la suite de protocoles TCP/IP et sa relation avec le modèle OSI. Le mode Simulation vous permet d'afficher le contenu de données envoyé sur tout le réseau à chaque couche.

Au fur et à mesure de leur transmission sur le réseau, les données sont divisées en parties plus petites et sont identifiées, afin que ces parties puissent être réassemblées lorsqu'elles arrivent à destination. Chaque partie reçoit un nom spécifique (unité de données de protocole, PDU) et est associée à une couche spécifique des modèles OSI et TCP/IP. Le mode Simulation de Packet Tracer vous permet d'afficher chacune des couches et la PDU associée. Les étapes suivantes guident l'utilisateur tout au long du processus de demande d'une page web à partir d'un serveur web, à l'aide du navigateur disponible sur un PC client.

Même si une grande partie des informations affichées seront traitées plus en détail plus loin, c'est l'occasion de découvrir le fonctionnement de Packet Tracer et de pouvoir visualiser le processus d'encapsulation.

Partie 1: Inspecter le trafic web HTTP

Dans la partie 1 de cet exercice, vous allez utiliser le mode Simulation de Packet Tracer (PT) pour générer du trafic web et examiner le protocole HTTP.

Étape 1: Passez du mode Temps réel au mode Simulation.

Le coin inférieur droit de l'interface de Packet Tracer comporte des onglets permettant de passer du mode **Realtime** (Temps réel) au mode **Simulation**. Packet Tracer démarre toujours en mode **Realtime** (Temps réel), dans lequel les protocoles réseau fonctionnent avec des temporisations réalistes. Cependant, une fonctionnalité puissante de Packet Tracer permet à l'utilisateur d'« arrêter le temps » en basculant vers le mode Simulation. En mode Simulation, les paquets sont affichés en tant qu'enveloppes animées, le temps est basé sur les événements et l'utilisateur peut parcourir les événements réseau.

a. Cliquez sur l'icône du mode **Simulation** pour passer du mode **Realtime** (Temps réel) au mode **Simulation**.

b. Sélectionnez **HTTP** dans les **Event List Filters** (Filtres de listes d'événements).

   1) Il se peut que HTTP soit déjà le seul événement visible. Cliquez sur **Edit Filters** (Modifier les filtres) pour afficher les événements visibles disponibles. Cliquez sur la case à cocher **Show All/None** (Afficher Tout/Aucun) et observez comment les différentes cases à cocher passent de l'état désactivé à l'état activé, ou vice versa, en fonction de leur état.

2) Cliquez sur la case à cocher **Show All/None** (Afficher Tout/Aucun) jusqu'à ce que toutes les cases à cocher soient désactivées, puis sélectionnez **HTTP**. Cliquez n'importe où en dehors de la zone **Edit Filters** (Modifier les filtres) pour la masquer. Les événements visibles ne doivent désormais afficher que HTTP.

Étape 2: Générez le trafic web (HTTP).

Le panneau de simulation (Simulation Panel) est actuellement vide. La liste des événements située en haut du panneau de simulation contient six colonnes. Les divers événements apparaissent dans cette liste au fur et à mesure de la génération et de l'acheminement du trafic. La colonne **Info** est utilisée pour examiner le contenu d'un événement spécifique.

Remarque : le serveur web (Web Server) et le client web (Web Client) sont affichés dans le volet de gauche. Vous pouvez ajuster la taille des panneaux en amenant le curseur de la souris à côté de la barre de défilement et en le faisant glisser vers la gauche ou vers la droite lorsque la double flèche apparaît.

a. Cliquez sur **Web Client** (Client web) dans le volet situé le plus à gauche.

b. Cliquez sur l'onglet **Bureau**, puis sur l'icône **Web Browser** (Navigateur web) pour ouvrir le programme.

c. Dans le champ URL, entrez **www.osi.local** et cliquez sur **Go** (Accéder).

   Comme le temps en mode Simulation est basé sur les événements, vous devez utiliser le bouton **Capture/Forward** (Capture/Avance) pour afficher les événements réseau.

d. Cliquez à quatre reprises sur **Capture/Forward** (Capture/Avance). La liste des événements doit comporter quatre événements.

   Examinez la page du navigateur web de Web Client. Constatez-vous un quelconque changement ?

   _____

   _____

Étape 3: Explorez le contenu du paquet HTTP.

a. Cliquez sur la première case en couleur située sous la colonne **Event List** (Liste d'événements) > **Info**. Vous devrez peut-être développer le panneau **Simulation Panel** (Panneau de simulation) ou utiliser la barre de défilement située directement sous la liste d'événements **Event List** (Liste d'évènements).

   La fenêtre **PDU Information at Device: Web Client** (Informations PDU au périphérique : client web) s'affiche. Cette fenêtre ne comporte que deux onglets, à savoir **OSI Model** (Modèle OSI) et **Outbound PDU Details** (Sortie de l'unité de données de protocole), étant donné que la transmission n'en est qu'à son début. Trois onglets de plus s'afficheront au fur et à mesure que les événements seront examinés, avec l'ajout d'un onglet pour **Inbound PDU Details** (Entrée de l'unité de données de protocole). Pour le dernier événement du flux de trafic, seuls les onglets **OSI Model** (Modèle OSI) et **Inbound PDU Details** (Entrée de l'unité de données de protocole) s'affichent.

b. Assurez-vous que l'onglet **OSI Model** (Modèle OSI) est sélectionné. Sous la colonne **Out Layers** (Couches externes), vérifiez que la zone **Layer 7** (Couche 7) est en surbrillance.

   Quel est le texte affiché à côté de l'étiquette **Layer 7** (Couche 7) ? _____

   Quelles informations sont répertoriées dans les étapes numérotées directement sous les zones **In Layers** (Couches internes) et **Out Layers** (Couches externes) ?

   _____

   _____

c. Cliquez sur **Next Layer** (Couche suivante). La couche 4 (Layer 4) doit être en surbrillance. Quelle est la valeur **Dst Port** ? _____

d. Cliquez sur **Next Layer** (Couche suivante). La couche 3 (Layer 3) doit être en surbrillance. Quelle est la valeur **Dest. IP** ? _____

e. Cliquez sur **Next Layer** (Couche suivante). Quelles informations sont affichées au niveau de cette couche ?

_____

_____

f. Cliquez sur l'onglet **Outbound PDU Details** (Sortie de l'unité de données de protocole).

Les informations répertoriées sous **PDU Details** (Détails PDU) reflètent les couches du modèle TCP/IP.

Remarque : les informations affichées dans la section **Ethernet II** fournissent davantage de détails que celles qui figurent sous la zone Layer 2 (Couche 2) de l'onglet **OSI Model** (Modèle OSI). L'onglet **Outbound PDU Details** (Sortie de l'unité de données de protocole) fournit des informations plus descriptives et détaillées. Les valeurs figurant sous **DEST MAC** et **SRC MAC** dans la section **Ethernet II** de **PDU Details** (Détails PDU) apparaissent dans l'onglet **OSI Model** (Modèle OSI) sous Layer 2 (Couche 2), mais ne sont pas identifiées en tant que telles.

Quelles sont les informations répertoriées à la fois dans la section **IP** de **PDU Details** (Détails PDU) et dans l'onglet **OSI Model** (Modèle OSI) ? À quelle couche ces informations sont-elles associées ?

_____

Quelles sont les informations communes répertoriées dans la section **TCP** de **PDU Details** (Détails PDU), par rapport à celles qui figurent dans l'onglet **OSI Model** (Modèle OSI), et à quelle couche sont-elles associées ?

_____

Quelle est la valeur **Host** (Hôte) répertoriée dans la section **HTTP** de **PDU Details** (Détails PDU) ? À quelle couche ces informations sont-elles associées dans l'onglet **OSI Model** (Modèle OSI) ?

_____

g. Cliquez sur la case en couleur suivante située sous la colonne **Event List** (Liste d'évènements) > **Info**. Seule la couche 1 est active (non grisée). Le périphérique prend la trame dans la mémoire tampon et la place sur le réseau.

h. Passez à la zone **Info** HTTP suivante dans **Event List** (Liste d'évènements) et cliquez sur la case en couleur. Cette fenêtre contient à la fois **In Layers** (Couches internes) et **Out Layers** (Couches externes). Notez la direction de la flèche juste sous la colonne **In Layers** (Couches internes) ; elle pointe vers le haut, indiquant le sens d'acheminement des informations. Faites défiler les différentes couches en observant les éléments précédemment affichés. La flèche située en haut de la colonne pointe vers la droite. Cela indique que le serveur renvoie désormais les informations au client.

Lorsque vous comparez les informations affichées dans les colonnes **In Layers** (Couches internes) et **Out Layers** (Couches externes), quelles différences remarquez-vous principalement ?

_____

_____

i. Cliquez sur l'onglet **Outbound PDU Details** (Sortie de l'unité de données de protocole). Faites défiler le contenu jusqu'à la section **HTTP**.

Quelle est la première ligne du message HTTP qui s'affiche ?

_____

_____

j. Cliquez sur la dernière case en couleur dans la colonne **Info**. Combien d'onglets sont affichés avec cet événement et pourquoi ?

_____

_____

Partie 2: Afficher les éléments de la suite de protocoles TCP/IP

Dans la partie 2 de cet exercice, vous allez utiliser le mode Simulation de Packet Tracer pour afficher et examiner quelques-uns des autres protocoles inclus dans la suite TCP/IP.

Étape 1: Afficher les événements supplémentaires

a. Fermez toutes les fenêtres d'information liées au protocole PDU.

b. Dans la section Event List Filters (Filtres de la liste d'événements) > Visible Events (Événements visibles), cliquez sur **Show All** (Afficher tout).

Quels types d'événements supplémentaires sont affichés ?

_____

_____

_____

_____

Ces entrées supplémentaires jouent divers rôles au sein de la suite TCP/IP. Si le protocole ARP (Address Resolution Protocol) est indiqué, il recherche des adresses MAC. Le protocole DNS est chargé de la conversion d'un nom (par exemple, **www.osi.local**) en adresse IP. Les événements TCP supplémentaires sont responsables de la connexion, de la configuration des paramètres de transmission et de la déconnexion des sessions de communication entre les périphériques. Ces protocoles ont été évoqués précédemment et ils feront également l'objet d'une discussion ultérieure dans ce cours. Il existe actuellement plus de 35 protocoles possibles (types d'événements) disponibles pour la capture dans Packet Tracer.

c. Cliquez sur le premier événement DNS dans la colonne **Info**. Examinez les onglets **OSI Model** (Modèle OSI) et **PDU Detail** (Détails PDU), et observez le processus d'encapsulation. Pendant que vous examinez l'onglet **OSI Model** (Modèle OSI) avec la zone **Layer 7** (Couche 7) en surbrillance, une description de ce qui se passe s'affiche directement sous **In Layers** (Couches internes) et **Out Layers** (Couches externes) (« 1. Le client DNS envoie une requête DNS au serveur DNS. »). Il s'agit d'informations très utiles pour mieux comprendre ce qui se produit durant le processus de communication.

d. Cliquez sur l'onglet **Outbound PDU Details** (Sortie de l'unité de données de protocole). Quelles informations sont répertoriées dans la zone **NAME** (NOM) : de la section DNS QUERY ?

_____

e. Cliquez sur la dernière case en couleur **Info** DNS dans la liste des événements. Quel périphérique est affiché ?

_____

Quelle est la valeur indiquée en regard de la zone **ADDRESS** (ADRESSE) : de la section DNS ANSWER de l'onglet **Inbound PDU Details** (Entrée de l'unité de données de protocole) ?

_____

_____

f. Recherchez le premier événement **HTTP** de la liste et cliquez sur la case en couleur de l'événement **TCP** situé juste après. Mettez en surbrillance la couche 4 (**Layer 4**) de l'onglet **OSI Model** (Modèle OSI). Dans la liste numérotée située directement sous **In Layers** (Couches internes) et **Out Layers** (Couches externes), quelles sont les informations affichées sous les points 4 et 5 ?

_____

_____

Entre autres tâches, TCP gère la connexion et la déconnexion du canal de communication. Cet événement particulier indique que la connexion du canal de communication a été ESTABLISHED (ÉTABLIE).

g. Cliquez sur le dernier événement TCP. Mettez en surbrillance la couche 4 (Layer 4) de l'onglet **OSI Model** (Modèle OSI). Examinez les étapes répertoriées directement sous **In Layers** (Couches internes) et **Out Layers** (Couches externes). Quel est le rôle de cet événement, sur la base des informations fournies dans le dernier élément de la liste (il doit s'agir du point 4) ? _____

Défi

Cette simulation a illustré un exemple de session web entre un client et un serveur sur un réseau local (LAN). Le client envoie des requêtes à des services spécifiques s'exécutant sur le serveur. Le serveur doit être configuré de manière à écouter sur des ports spécifiques en cas de requête du client. (Conseil : observez la zone Layer 4 (Couche 4) de l'onglet **OSI Model** (Modèle OSI) pour obtenir des informations sur les ports.)

D'après les informations collectées durant la capture dans Packet Tracer, sur quel numéro de port le serveur web (**Web Server**) écoute-t-il la requête web ?

_____

_____

Sur quel port le serveur web (**Web Server**) est-il à l'écoute d'une requête DNS ?

_____

_____

Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points obtenus
Partie 1 : Inspecter le trafic web HTTP	Étape 2d	5	
	Étape 3b-1	5	
	Étape 3b-2	5	
	Étape 3c	5	
	Étape 3d	5	
	Étape 3e	5	
	Étape 3f-1	5	
	Étape 3f-2	5	
	Étape 3f-3	5	
	Étape 3h	5	
	Étape 3i	5	
	Étape 3j	5	
	Total de la Partie 1	**60**	
Partie 2 : Afficher les éléments de la suite de protocoles TCP/IP	Étape 1b	5	
	Étape 1d	5	
	Étape 1e-1	5	
	Étape 1e-2	5	
	Étape 1f	5	
	Étape 1g	5	
	Total de la Partie 2	**30**	
Défi	1	5	
	2	5	
	Total de la Partie 3	**10**	
	Score total	**100**	

Packet Tracer : connexion d'un LAN filaire et d'un LAN sans fil

Topologie

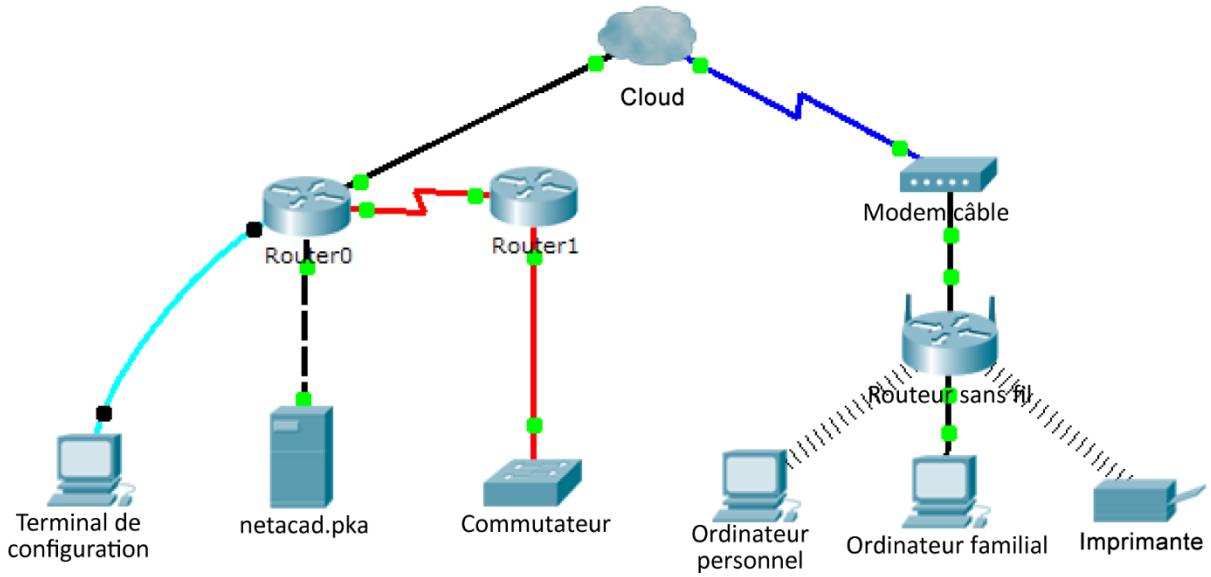


Table d'adressage

Périphérique	Interface	Adresse IP	Connecté à
Cloud	Eth6	N/A	F0/0
	Coax7	N/A	Port0
Modem câble	Port0	N/A	Coax7
	Port1	N/A	Internet
Routeur0	Console	N/A	RS232
	F0/0	192.168.2.1/24	Eth6
	F0/1	10.0.0.1/24	F0
	Ser0/0/0	172.31.0.1/24	Ser0/0
Routeur1	Ser0/0	172.31.0.2/24	Ser0/0/0
	F1/0	172.16.0.1/24	F0/1
Routeur sans fil	Internet	192.168.2.2/24	Port 1
	Eth1	192.168.1.1	F0
Ordinateur familial	F0	192.168.1.102	Eth1
Commutateur	F0/1	172.16.0.2	F1/0
netacad.pka	F0	10.0.0.254	F0/1
Terminal de configuration	RS232	N/A	Console

Objectifs

Partie 1 : Se connecter au cloud

Partie 2 : Connecter le Routeur0

Partie 3 : Connecter les périphériques restants

Partie 4 : Vérifier les connexions

Partie 5 : Examiner la topologie physique

Contexte

Lorsque vous utilisez Packet Tracer (dans le cadre d'un environnement de test ou de travail), vous devez savoir comment choisir les câbles adéquats et connecter correctement les périphériques. Dans cet exercice, vous pourrez découvrir des configurations de périphériques dans Packet Tracer, sélectionner le câble approprié en fonction de la configuration et connecter les périphériques. Enfin, vous explorerez la vue physique du réseau dans Packet Tracer.

Partie 1: Se connecter au cloud

Étape 1: Connectez le cloud au Routeur0.

a. Pour afficher les **connexions** disponibles, cliquez sur l'icône en forme d'éclair orange situé sur le coin inférieur gauche de la fenêtre.

b. Choisissez le câble adéquat pour relier le **port Fa0/0 du Routeur0** au **port Eth6 du Cloud**. Le **Cloud** étant un type de commutateur, il faut utiliser une connexion par **câble droit en cuivre**. Si vous avez branché le câble adéquat, les voyants de liaison de ce dernier s'allument en vert.

Étape 2: Connectez le cloud au modem câble.

Choisissez le câble adéquat pour relier le **port Coax7 du Cloud** au **port0 du modem**.

Si vous avez branché le câble adéquat, les voyants de liaison de ce dernier s'allument en vert.

Partie 2: Connecter le Routeur0

Étape 1: Connectez le Routeur0 au Routeur1.

Choisissez le câble adéquat pour relier le **port Ser0/0/0 du Routeur0** au **port Ser0/0 du Routeur1**. Utilisez l'un des câbles **série** disponibles.

Si vous avez branché le câble adéquat, les voyants de liaison de ce dernier s'allument en vert.

Étape 2: Connectez le Routeur0 à netacad.pka.

Choisissez le câble adéquat pour relier le **port F0/1 du Routeur0** au **port F0 de netacad.pka**. Les routeurs et les ordinateurs utilisent généralement les mêmes fils pour la transmission (1 et 2) et la réception (3 et 6). Le câble adéquat est composé de ces fils croisés. Bien que de nombreuses cartes réseau soient désormais capables de détecter automatiquement quelle paire est utilisée pour la transmission et la réception, le **Routeur0** et **netacad.pka** ne possèdent pas de telles cartes réseau.

Si vous avez branché le câble adéquat, les voyants de liaison de ce dernier s'allument en vert.

Étape 3: Connectez le Routeur0 au Terminal de configuration.

Choisissez le câble adéquat pour relier la **Console** du **Routeur0** au **Terminal de configuration RS232**. Ce câble n'offre pas d'accès réseau au **Terminal de configuration**, mais il vous permet de configurer le **Routeur0** par l'intermédiaire de son terminal.

Si vous avez branché le câble adéquat, les voyants de liaison de ce dernier s'allument en noir.

Partie 3: Connecter les périphériques restants

Étape 1: Connectez le Routeur1 au commutateur.

Choisissez le câble adéquat pour relier le **port F1/0 du Routeur1** au **port F0/1 du commutateur**.

Si vous avez branché le câble adéquat, les voyants de liaison de ce dernier s'allument en vert. Attendez quelques secondes que le voyant passe de l'orange au vert.

Étape 2: Connectez le modem câble au routeur sans fil.

Choisissez le câble adéquat pour relier le **Port 1** du **Modem** au port **Internet** du **Routeur sans fil**.

Si vous avez branché le câble adéquat, les voyants de liaison de ce dernier s'allument en vert.

Étape 3: Connectez le routeur sans fil à l'ordinateur familial.

Choisissez le câble adéquat pour relier le **Routeur sans fil Ethernet 1** à l'**ordinateur familial**.

Si vous avez branché le câble adéquat, les voyants de liaison de ce dernier s'allument en vert.

Partie 4: Vérifier les connexions

Étape 1: Testez la connexion de l'ordinateur familial à netacad.pka.

a. Ouvrez l'invite de commandes de l'**ordinateur familial** et envoyez une requête ping à **netacad.pka**.

b. Ouvrez le **navigateur web** et accédez à l'adresse web **http://netacad.pka**.

Étape 2: Envoyez une requête ping au commutateur à partir de l'ordinateur personnel.

Ouvrez l'invite de commandes de l'**ordinateur personnel** et envoyez une requête ping à l'adresse IP du **Commutateur** afin de vérifier la connexion.

Étape 3: Ouvrez le Routeur0 à partir du Terminal de configuration.

a. Ouvrez l'**interface** du **Terminal de configuration** et acceptez les paramètres par défaut.

b. Appuyez sur **Entrée** pour afficher l'invite de commandes du **Routeur0**.

c. Tapez **show ip interface brief** (afficher un résumé des interfaces ip) pour afficher les états des interfaces.

Partie 5: Examiner la topologie physique

Étape 1: Examinez le cloud.

a. Cliquez sur l'onglet **Physical Workspace** (Espace de travail physique) ou appuyez sur **Maj**+**P** et **Maj**+**L** pour alterner entre les espaces de travail logique et physique.

b. Cliquez sur l'icône **Home City** (Ville du domicile).

c. Cliquez sur l'icône **Cloud**. Combien de fils sont connectés au commutateur dans le rack bleu ? _____

d. Cliquez sur **Back** (Précédent) pour revenir à **Home City** (Ville du domicile).

Étape 2: Examinez le réseau principal.

a. Cliquez sur l'icône **Primary Network** (Réseau principal). Placez le pointeur de la souris sur les différents câbles. Que trouve-t-on sur la table à la droite du rack bleu ?

_____

b. Cliquez sur **Back** (Précédent) pour revenir à **Home City** (Ville du domicile).

Étape 3: Examinez le réseau secondaire.

a. Cliquez sur l'icône **Secondary Network** (Réseau secondaire). Placez le pointeur de la souris sur les différents câbles. Pourquoi y a-t-il deux câbles orange connectés à chaque périphérique ?

_____

b. Cliquez sur **Back** (Précédent) pour revenir à **Home City** (Ville du domicile).

Étape 4: Examinez le réseau domestique.

a. Pourquoi y a-t-il un maillage ovale couvrant le réseau domestique ?

_____

b. Cliquez sur l'icône **Home Network** (Réseau domestique) Pourquoi n'y a-t-il pas de rack pour supporter l'équipement ?

_____

c. Cliquez sur l'onglet **Logical Workspace** (Espace de travail logique) pour revenir à la topologie logique.

Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points obtenus
Partie 5 : Examiner la topologie physique	Étape 1c	4	
	Étape 2a	4	
	Étape 3a	4	
	Étape 4a	4	
	Étape 4b	4	
Total de la Partie 5		**20**	
Score relatif à Packet Tracer		**80**	
Score total		**100**	

Packet Tracer - Examen d'une table ARP

Topologie

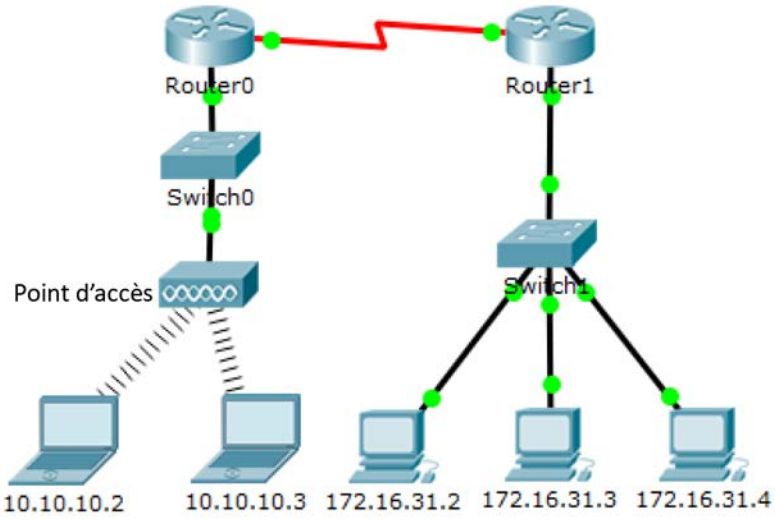


Table d'adressage

Appareil	Interface	Adresse MAC	Interface du commutateur
Router0	Gg0/0	0001.6458.2501	G0/1
	S0/0/0	N/A	N/A
Router1	G0/0	00E0.F7B1.8901	G0/1
	S0/0/0	N/A	N/A
10.10.10.2	Sans fil	0060.2F84.4AB6	F0/2
10.10.10.3	Sans fil	0060.4706.572B	F0/2
172.16.31.2	F0	000C.85CC.1DA7	F0/1
172.16.31.3	F0	0060.7036.2849	F0/2
172.16.31.4	G0	0002.1640.8D75	F0/3

Objectifs

Partie 1 : examiner une requête ARP

Partie 2 : analyser la table d'adresses MAC du commutateur

Partie 3 : examiner le processus ARP dans les communications distantes

Le contexte

Cet exercice est optimisé pour l'affichage des PDU. Les périphériques sont déjà configurés. Vous allez recueillir des informations sur les PDU en mode Simulation et répondre à une série de questions sur les données recueillies.

Partie 1: Examiner une requête ARP

Étape 1: Générez des requêtes ARP en envoyant une requête ping à 172.16.31.3 à partir de 172.16.31.2.

a. Cliquez sur **172.16.31.2** et ouvrez l'**invite de commandes**.

b. Exécutez la commande **arp -d** pour effacer la table ARP.

c. Passez en mode **Simulation** et exécutez la commande **ping 172.16.31.3**. Deux unités de données de protocole (PDU) sont générées. La commande **ping** ne peut pas traiter le paquet ICMP sans connaître l'adresse MAC de destination. L'ordinateur envoie donc une trame de diffusion ARP en vue de connaître l'adresse MAC de destination.

d. Cliquez une seule fois sur **Capture/Forward** (capture/avance). La PDU ARP déplace **Switch1** tandis que la PDU ICMP disparaît, en attendant la réponse ARP. Ouvrez la PDU et notez l'adresse MAC de destination. Cette adresse figure-t-elle dans le tableau ci-dessus ?

_____

e. Cliquez sur **Capture/Forward** (capture/avance) pour déplacer l'unité de données de protocole vers le périphérique suivant. Combien d'exemplaires de PDU le commutateur **Switch1** a-t-il réalisés ?

_____

f. Quelle adresse IP du périphérique a accepté l'unité de données de protocole ? _____

g. Ouvrez la PDU et examinez la couche 2. Qu'est-il arrivé aux adresses MAC source et de destination ?

_____

h. Cliquez sur **Capture/Forward** jusqu'à ce que la PDU revienne à **172.16.31.2**. Combien d'exemplaires de PDU le commutateur a-t-il réalisés pendant la réponse ARP ?

_____

Étape 2: Examinez la table ARP.

a. Notez que le paquet ICMP réapparaît. Ouvrez la PDU et examinez les adresses MAC. Les adresses MAC source et de destination correspondent-elles à leurs adresses IP ? _____

b. Repassez en mode **Realtime** afin que la requête ping se termine.

c. Cliquez sur **172.16.31.2** et exécutez la commande **arp –a**. À quelle adresse IP l'entrée d'adresse MAC correspond-elle ? _____

d. D'une manière générale, à quel moment un périphérique final émet-il une requête ARP ?

_____

Partie 2: Analyser la table d'adresses MAC du commutateur

Étape 1: Générez du trafic supplémentaire afin de remplir la table d'adresses MAC du commutateur.

a. À partir de **172.16.31.2**, exécutez la commande **ping 172.16.31.4**.

b. Cliquez sur **10.10.10.2** et ouvrez l'**invite de commandes**.

c. Saisissez la commande **ping 10.10.10.3**. Combien de réponses ont été envoyées et reçues ?

_____

Étape 2: Examinez la table des adresses MAC sur les commutateurs.

a. Cliquez sur **Switch1**, puis sur l'onglet **CLI**. Saisissez la commande **show mac-address-table**. Les entrées correspondent-elles aux adresses figurant dans le tableau ci-dessus ?

_____

b. Cliquez sur **S/witch0**, puis sur l'onglet **CLI**. Saisissez la commande **show mac-address-table**. Les entrées correspondent-elles aux adresses figurant dans le tableau ci-dessus ?

_____

c. Pourquoi deux adresses MAC sont-elles associées à un seul port ?

_____

Partie 3: Examiner le processus ARP dans les communications distantes

Étape 1: Générez du trafic en vue de produire du trafic ARP.

a. Cliquez sur **172.16.31.2** et ouvrez l'**invite de commandes**.

b. Saisissez la commande **ping 10.10.10.1**.

c. Tapez **arp –a**. Quelle est l'adresse IP de la nouvelle entrée de la table ARP ? _____

d. Exécutez la commande **arp -d** pour effacer la table ARP et passez en mode **Simulation**.

e. Répétez la requête ping vers 10.10.10.1. Combien d'unités de données de protocole apparaissent ?

_____

f. Cliquez sur **Capture / Forward**. Cliquez sur la PDU qui est maintenant sur **Switch1**. Quelle est l'adresse IP de destination cible de la requête ARP ? _____

g. L'adresse IP de destination n'est pas égale à 10.10.10.1. Pourquoi ?

_____

_____

_____

Étape 2: Examinez la table ARP sur Router1.

a. Passez en mode **Realtime**. Cliquez sur **Router1**, puis sur l'onglet **CLI**.

b. Passez en mode d'exécution privilégié, puis exécutez la commande **show mac-address-table**. Combien y a-t-il d'adresses MAC dans la table ? Pourquoi ?

_____

_____

c. Saisissez la commande **show arp**. Existe-t-il une entrée pour **172.16.31.2** ? _____

d. Qu'arrive-t-il à la première requête ping si le routeur répond à la requête ARP ?

_____

Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points obtenus
Partie 1 : Examiner une requête ARP	Étape 1	10	
	Étape 2	15	
Total de la partie 1		**25**	
Partie 2 : analyser la table d'adresses MAC du commutateur	Étape 1	5	
	Étape 2	20	
Total de la partie 2		**25**	
Partie 3 : examiner le processus ARP dans les communications distantes	Étape 1	25	
	Étape 2	25	
Total de la partie 3		**50**	
Score total		**100**	

Packet Tracer - Configuration des paramètres initiaux du routeur

Topologie

Objectifs

Partie 1 : vérifier la configuration par défaut du routeur

Partie 2 : configurer et vérifier la configuration initiale du routeur

Partie 3 : enregistrer le fichier de configuration en cours

Le contexte

Au cours de cet exercice, vous allez effectuer des configurations de base sur les routeurs, sécuriser l'accès à l'interface en ligne de commande (CLI) et au port de console à l'aide de mots de passe chiffrés et en texte clair et configurer les messages affichés lors de la connexion des utilisateurs au routeur. Ces bannières avertissent également les utilisateurs non autorisés que l'accès est interdit. Enfin, vous allez vérifier et enregistrer votre configuration en cours.

Partie 1: Vérifier la configuration par défaut du routeur

Étape 1: Établissez une connexion console avec R1.

a. Choisissez un câble **Console** parmi les connexions disponibles.

b. Cliquez sur **PCA** et sélectionnez **RS 232**.

c. Cliquez sur **R1** et sélectionnez **Console**.

d. Cliquez sur **PCA** > onglet **Desktop** (bureau) > **Terminal**.

e. Cliquez sur **OK** et appuyez sur **Entrée**. Vous êtes maintenant en mesure de configurer **R1**.

Étape 2: Accédez au mode privilégié et examinez la configuration actuelle.

Vous pouvez accéder à l'ensemble des commandes du routeur en mode d'exécution privilégié. Toutefois, comme un grand nombre des commandes du mode privilégié permettent de configurer des paramètres d'exploitation, l'accès privilégié doit être protégé par mot de passe pour empêcher toute utilisation non autorisée.

a. Accédez au mode d'exécution privilégié en entrant la commande **enable**.

```
Router> enable
Router#
```

Notez que l'invite a changé dans la configuration pour représenter le mode d'exécution privilégié.

b. Entrez la commande **show running-config**.

```
Router# show running-config
```

c. Répondez aux questions suivantes :

Quel est le nom d'hôte du routeur ? _____

Combien d'interfaces Fast Ethernet le routeur possède-t-il ? _____

Combien d'interfaces Gigabit Ethernet le routeur possède-t-il ? _____

Combien d'interfaces série le routeur possède-t-il ? _____

Quelle est la plage de valeurs affichée pour les lignes vty ? _____

d. Examinez le contenu actuel de la mémoire vive non volatile (NVRAM).

```
Router# show startup-config
startup-config is not present
```

Pourquoi le routeur répond-il avec le message `startup-config is not present` ?

_____

_____

_____

_____

Partie 2: Configurer et vérifier la configuration initiale du routeur

Pour configurer les paramètres d'un routeur, vous devrez peut-être passer d'un mode de configuration à l'autre. Notez que l'invite change lorsque vous utilisez le routeur.

Étape 1: Configurez les paramètres initiaux du routeur R1.

Remarque : si vous avez du mal à vous souvenir des commandes, référez-vous au contenu de cette rubrique. Les commandes sont les mêmes que celles que vous avez configurées sur le commutateur.

a. **R1** est le nom d'hôte.

b. Utilisez les mots de passe suivants :

1) Console : **letmein**

2) Mode d'exécution privilégié, non chiffré : **cisco**

3) Mode d'exécution privilégié, chiffré : **itsasecret**

c. Chiffrez tous les mots de passe en clair.

d. Bannière MOTD (message of the day ou message du jour) : `Unauthorized access is strictly prohibited`.

Étape 2: Vérifiez les paramètres initiaux du routeur R1.

a. Vérifiez les paramètres initiaux en affichant la configuration de R1. Quelle commande utilisez-vous ?

_____

_____

b. Quittez la session actuelle en mode console jusqu'à ce que le message suivant apparaisse :

```
R1 con0 is now available

Press RETURN to get started.
```

c. Appuyez sur **Entrée** pour obtenir le message suivant :

```
Unauthorized access is strictly prohibited.

User Access Verification

Password:
```

Pourquoi chaque routeur doit-il avoir une bannière de message du jour (MOTD) ?

_____

_____

_____

Si vous n'êtes pas invité à entrer un mot de passe, quelle commande de ligne de console avez-vous oublié de configurer ?

_____

d. Entrez les mots de passe requis pour revenir au mode d'exécution privilégié.

Pourquoi le mot de passe secret actif (**enable secret**) permettrait-il d'accéder au mode d'exécution privilégié et le mot de passe d'activation (**enable password**) ne serait-il plus valide ?

_____

_____

_____

Si vous configurez d'autres mots de passe sur le routeur, s'affichent-ils dans le fichier de configuration en texte clair ou chiffrés ? Expliquez votre réponse.

_____

_____

Partie 3: Enregistrer le fichier de configuration en cours

Étape 1: Enregistrez le fichier de configuration dans la mémoire NVRAM.

a. Vous avez configuré les paramètres initiaux du routeur **R1**. Sauvegardez le fichier de configuration en cours dans la mémoire vive non volatile pour vous assurer que les modifications apportées seront conservées en cas de redémarrage du système ou de coupure de courant.

Quelle commande avez-vous exécutée pour enregistrer la configuration dans la mémoire NVRAM ?

_____

Quelle est la version la plus courte et non ambiguë de cette commande ? _____

Quelle commande affiche le contenu de la mémoire NVRAM ?

_____

b. Vérifiez que tous les paramètres configurés ont été enregistrés. Si ce n'est pas le cas, analysez le résultat et déterminez quelles commandes n'ont pas été exécutées ou ont été saisies incorrectement. Vous pouvez également cliquer sur **Check Results** (vérifier les résultats) dans la fenêtre d'instructions.

Étape 2: Bonus facultatif : enregistrez le fichier de configuration initiale dans la mémoire Flash.

Vous en apprendrez plus sur la gestion du stockage Flash d'un routeur dans les chapitres ultérieurs. Toutefois, sachez qu'en guise de procédure de sauvegarde supplémentaire, vous pouvez enregistrer votre fichier de configuration initiale dans la mémoire Flash. Par défaut, le routeur continue à charger la configuration initiale à partir de la mémoire NVRAM, mais si cette mémoire est endommagée, vous pouvez restaurer la configuration initiale en la copiant à partir de la mémoire Flash.

Procédez comme suit pour enregistrer la configuration initiale dans la mémoire Flash.

a. Examinez le contenu de la mémoire Flash à l'aide de la commande **show flash** :

```
R1# show flash
```

Combien de fichiers sont actuellement stockés dans la mémoire Flash ? _____

Selon vous, lequel de ces fichiers est le fichier d'image IOS ? _____

Pourquoi pensez-vous que ce fichier est le fichier d'image IOS ?

_____

_____

b. Enregistrez le fichier de configuration initiale dans la mémoire Flash à l'aide des commandes suivantes :

```
R1# copy startup-config flash
Destination filename [startup-config]
```

Le routeur vous invite à stocker le fichier dans la mémoire Flash avec le nom entre parenthèses. Si le nom vous convient, appuyez sur **Entrée**, sinon, tapez un nom approprié et appuyez sur **Entrée**.

c. Utilisez la commande **show flash** pour vérifier que le fichier de configuration initiale est à présent stocké dans la mémoire Flash.

Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points obtenus
Partie 1 : vérifier la configuration par défaut du routeur	Étape 2c	10	
	Étape 2d	2	
Total de la partie 1		**12**	
Partie 2 : configurer et vérifier la configuration initiale du routeur	Étape 2a	2	
	Étape 2c	5	
	Étape 2d	6	
Total de la partie 2		**13**	
Partie 3 : enregistrer le fichier de configuration en cours	Étape 1a	5	
	Étape 2a (bonus)	5	
Total de la partie 3		**10**	
Score relatif à Packet Tracer		**80**	
Score total (avec le bonus)		**105**	

Packet Tracer - Connexion d'un routeur à un réseau local

Topologie

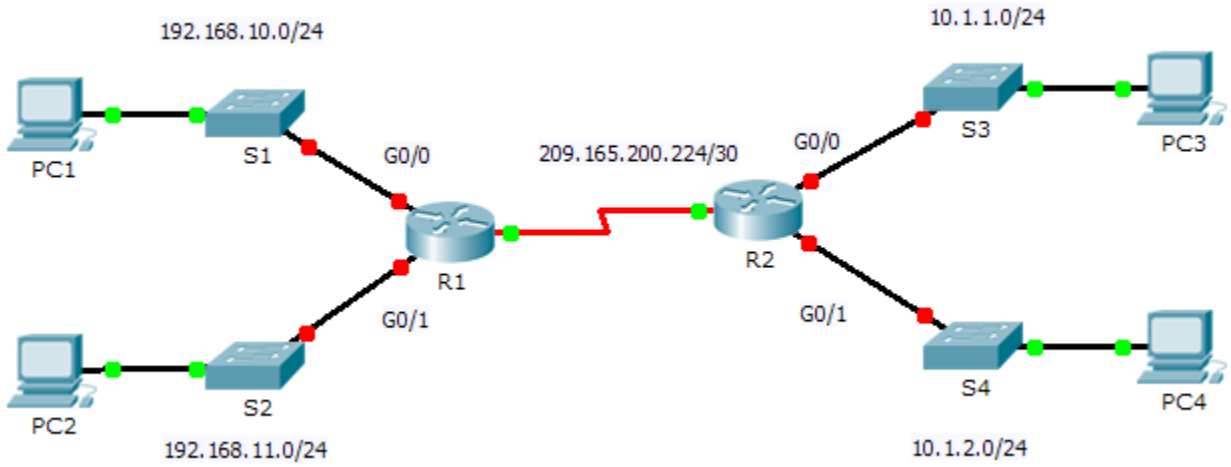


Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0 (ETCD)	209.165.200.225	255.255.255.252	N/A
R2	G0/0	10.1.1.1	255.255.255.0	N/A
	G0/1	10.1.2.1	255.255.255.0	N/A
	S0/0/0	209.165.200.226	255.255.255.252	N/A
PC1	Carte réseau	192.168.10.10	255.255.255.0	192.168.10.1
PC2	Carte réseau	192.168.11.10	255.255.255.0	192.168.11.1
PC3	Carte réseau	10.1.1.10	255.255.255.0	10.1.1.1
PC4	Carte réseau	10.1.2.10	255.255.255.0	10.1.2.1

Objectifs

Partie 1 : afficher des informations sur les routeurs

Partie 2 : configurer les interfaces des routeurs

Partie 3 : vérifier la configuration

Le contexte

Dans cet exercice, vous allez utiliser plusieurs commandes **show** pour afficher l'état actuel du routeur. Vous utiliserez ensuite la Table d'adressage pour configurer les interfaces Ethernet du routeur. Enfin, vous utiliserez des commandes pour vérifier et tester vos configurations.

Remarque : les routeurs utilisés dans cet exercice sont partiellement configurés. Certaines configurations ne sont pas traitées dans ce cours. Elles sont fournies pour vous aider à utiliser les commandes de vérification.

Partie 1: Afficher les informations du routeur

Étape 1: Affichez les informations d'interface sur R1.

Remarque : cliquez sur un périphérique, puis sur l'onglet **CLI** pour accéder directement à la ligne de commande. Le mot de passe de console est **cisco**. Le mot de passe en mode d'exécution privilégié est **class**.

a. Quelle commande permet d'afficher les statistiques de toutes les interfaces configurées sur un routeur ?

_____

b. Quelle commande affiche uniquement les informations relatives à l'interface série 0/0/0 ?

_____

c. Entrez la commande permettant d'afficher les statistiques de l'interface série 0/0/0 sur R1 et répondez aux questions suivantes :

1) Quelle est l'adresse IP configurée sur **R1** ? _____

2) Quelle est la bande passante de l'interface série 0/0/0 ? _____

d. Entrez la commande permettant d'afficher les statistiques de l'interface GigabitEthernet 0/0 et répondez aux questions suivantes :

1) Quelle est l'adresse IP sur **R1** ? _____

2) Quelle est l'adresse MAC de l'interface GigabitEthernet 0/0 ? _____

3) Quelle est la bande passante de l'interface GigabitEthernet 0/0 ? _____

Étape 2: Affichez la liste récapitulative des interfaces de R1.

a. Quelle commande affiche un résumé des interfaces, états et adresses IP actuellement affectés ?

_____

b. Entrez la commande sur chaque routeur et répondez aux questions suivantes :

1) Combien y a-t-il d'interfaces série sur **R1** et **R2** ? _____

2) Combien y a-t-il d'interfaces Ethernet sur **R1** et **R2** ?

_____

3) Toutes les interfaces Ethernet de **R1** sont-elles identiques ? Si ce n'est pas le cas, expliquez la ou les différences.

_____

_____

_____

Étape 3: Affichez la table de routage sur R1.

a. Quelle commande permet d'afficher le contenu de la table de routage ? _____

b. Entrez la commande sur **R1** et répondez aux questions suivantes :

1) Combien y a-t-il de routes connectées (utilisant le code C) ? _____

2) Quelle route est indiquée ? _____

3) Comment un routeur traite-t-il un paquet destiné à un réseau qui ne figure pas dans la table de routage ?

_____

_____

_____

Partie 2: Configurer les interfaces du routeur

Étape 1: Configurez l'interface GigabitEthernet 0/0 sur R1.

a. Exécutez les commandes suivantes pour préparer l'adressage et activer l'interface GigabitEthernet 0/0 sur **R1** :

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up
```

b. Il est conseillé de configurer une description sur chaque interface pour mieux documenter les informations du réseau. Configurez une description d'interface indiquant à quel périphérique elle est connectée.

```
R1(config-if)# description LAN connection to S1
```

c. **R1** devrait maintenant être en mesure d'envoyer une requête ping à PC1.

```
R1(config-if)# end
%SYS-5-CONFIG_I: Configured from console by console
R1# ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms
```

Étape 2: Configurez les interfaces Gigabit Ethernet restantes sur R1 et R2.

a. Utilisez les informations de la Table d’adressage pour terminer les configurations des interfaces de **R1** et **R2**. Pour chaque interface, procédez comme suit :

1) Entrez l'adresse IP et activez l'interface.

2) Configurez une description appropriée.

b. vérification des configurations des interfaces

Étape 3: Sauvegardez les configurations dans la mémoire NVRAM.

Enregistrez les fichiers de configuration des deux routeurs dans la mémoire NVRAM. Quelle commande avez-vous utilisée ?

_____

Partie 3: Vérifier la configuration

Étape 1: Utilisez des commandes de vérification pour contrôler les configurations de vos interfaces.

a. Utilisez la commande **show ip interface brief** à la fois sur **R1** et **R2** afin de vérifier rapidement que les interfaces sont configurées avec l'adresse IP correcte et qu'elles sont actives.

Combien d'interfaces sur **R1** et **R2** sont configurées avec des adresses IP et se trouvent à l'état « up » ?

_____

Quelle partie de la configuration d'interface NE s'affiche PAS dans le résultat de la commande ?

_____

Quelles commandes pouvez-vous utiliser pour vérifier cette partie de la configuration ?

_____

b. Utilisez la commande **show ip route** à la fois sur **R1** et **R2** afin d'afficher les tables de routage actuelles, puis répondez aux questions suivantes :

1) Combien de routes connectées (utilisant le code **C**) voyez-vous sur chaque routeur ? _____

2) Combien de routes EIGRP (utilisant le code **D**) voyez-vous sur chaque routeur ? _____

3) Si le routeur connaît toutes les routes du réseau, le nombre de routes connectées et de routes découvertes dynamiquement (EIGRP) doit être égal au nombre total de LAN et de WAN. Combien de LAN et de WAN y a-t-il dans la topologie ? _____

4) Ce nombre correspond-il au nombre de routes C et D affichées dans la table de routage ? _____

Remarque : si vous répondez « non », cela signifie qu'il vous manque une configuration requise. Passez en revue les étapes décrites dans la 2e partie.

Étape 2: Testez la connectivité de bout en bout sur le réseau.

Vous devriez maintenant pouvoir envoyer une requête ping à partir de n'importe quel ordinateur et vers n'importe quel autre ordinateur du réseau. Vous devriez également pouvoir envoyer une requête ping aux interfaces actives sur les routeurs. Par exemple, les tests suivants doivent réussir :

- À partir de la ligne de commande de PC1, envoyez une requête ping à PC4.
- À partir de la ligne de commande de R2, envoyez une requête ping à PC2.

Remarque : pour simplifier cet exercice, les commutateurs ne sont pas configurés et vous ne pourrez pas leur envoyer de requêtes ping.

Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points obtenus
Partie 1 : afficher des informations sur les routeurs	Étape 1a	2	
	Étape 1b	2	
	Étape 1c	4	
	Étape 1d	6	
	Étape 2a	2	
	Étape 2b	6	
	Étape 3a	2	
	Étape 3b	6	
Total de la partie 1		**30**	
Partie 2 : configurer les interfaces des routeurs	Étape 3	2	
Total de la partie 2		**2**	
Partie 3 : vérifier la configuration	Étape 1a	6	
	Étape 1b	8	
Total de la partie 3		**14**	
Score relatif à Packet Tracer		**54**	
Score total (avec le bonus)		**100**	

Packet Tracer - Configuration de l'adressage IPv6

Topologie

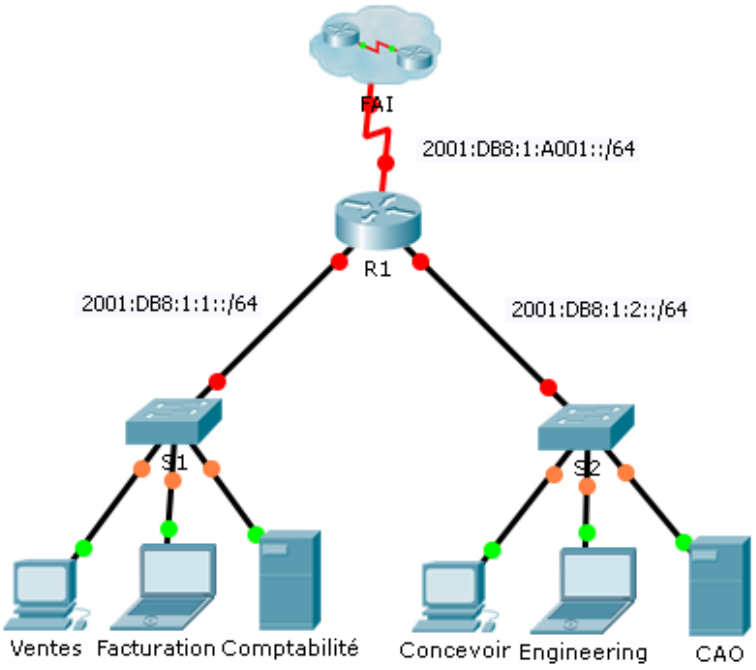


Table d'adressage

Appareil	Interface	Préfixe/adresse IPv6	Passerelle par défaut
R1	G0/0	2001:DB8:1:1::1/64	N/A
	G0/1	2001:DB8:1:2::1/64	N/A
	S0/0/0	2001:DB8:1:A001::2/64	N/A
	Link-local	FE80::1	N/A
Ventes	Carte réseau	2001:DB8:1:1::2/64	FE80::1
Facturation	Carte réseau	2001:DB8:1:1::3/64	FE80::1
Comptabilité	Carte réseau	2001:DB8:1:1::4/64	FE80::1
Concevoir	Carte réseau	2001:DB8:1:2::2/64	FE80::1
Engineering	Carte réseau	2001:DB8:1:2::3/64	FE80::1
CAO	Carte réseau	2001:DB8:1:2::4/64	FE80::1

Objectifs

Partie 1 : configurer l'adressage IPv6 sur le routeur

Partie 2 : configurer l'adressage IPv6 sur les serveurs

Partie 3 : configurer l'adressage IPv6 sur les clients

Partie 4 : tester et vérifier la connectivité réseau

Le contexte

Dans cet exercice, vous allez vous entraîner à configurer des adresses IPv6 sur un routeur, des serveurs et des clients. Vous vous exercerez également à vérifier l'adressage IPv6.

Partie 1: Configurer l'adressage IPv6 sur le routeur

Étape 1: Autorisez le routeur à transférer des paquets IPv6.

a. Exécutez la commande de configuration globale ipv6 unicast-routing. Cette commande doit être configurée de sorte que le routeur puisse transférer des paquets IPv6. Cette commande sera traitée au cours d'un prochain semestre.

```
R1(config)# ipv6 unicast-routing
```

Étape 2: Configurez l'adressage IPv6 sur GigabitEthernet0/0.

a. Cliquez sur **R1**, puis sur l'onglet **CLI**. Appuyez sur **Entrée**.

b. Passez en mode d'exécution privilégié.

c. Exécutez les commandes nécessaires pour passer en mode de configuration d'interface pour GigabitEthernet0/0.

d. Configurez l'adresse IPv6 à l'aide de la commande suivante :

```
R1(config-if)# ipv6 address 2001:DB8:1:1::1/64
```

e. Configurez l'adresse IPv6 link-local à l'aide de la commande suivante :

```
R1(config-if)# ipv6 address FE80::1 link-local
```

f. Activez l'interface.

Étape 3: Configurez l'adressage IPv6 sur GigabitEthernet0/1.

a. Exécutez les commandes nécessaires pour passer en mode de configuration d'interface pour GigabitEthernet0/1.

b. Consultez la **table d'adressage** pour obtenir l'adresse IPv6 adéquate.

c. Configurez l'adresse IPv6, l'adresse link-local et activez l'interface.

Étape 4: Configurez l'adressage IPv6 sur Serial0/0/0.

a. Exécutez les commandes nécessaires pour passer en mode de configuration d'interface pour Serial0/0/0.

b. Consultez la **table d'adressage** pour obtenir l'adresse IPv6 adéquate.

c. Configurez l'adresse IPv6, l'adresse link-local et activez l'interface.

Partie 2: Configurer l'adressage IPv6 sur les serveurs

Étape 1: Configurez l'adressage IPv6 sur le serveur Accounting.

a. Cliquez sur **Accounting** (comptabilité), puis sur l'onglet **Desktop** (bureau) > **IP Configuration** (configuration IP).

b. Configurez l'**adresse IPv6 2001:DB8:1:1::4** avec le préfixe **/64**.

c. Attribuez l'adresse link-local, **FE80::1**, à la **passerelle IPv6**.

Étape 2: Configurez l'adressage IPv6 sur le serveur CAD.

Répétez les étapes 1a à 1c pour le serveur **CAD**. Consultez la **table d'adressage** pour déterminer l'adresse IPv6.

Partie 3: Configurer l'adressage IPv6 sur les clients

Étape 1: Configurez l'adressage IPv6 sur les clients Sales et Billing (ventes et facturation).

a. Cliquez sur **Billing** (facturation) et sélectionnez l'onglet **Desktop**, puis **IP Configuration**.

b. Configurez l'**adresse IPv6 2001:DB8:1:1::3** avec le préfixe **/64**.

c. Attribuez l'adresse link-local, **FE80::1**, à la **passerelle IPv6**.

d. Répétez les étapes 1a à 1c pour le client **Sales** (ventes). Consultez la **table d'adressage** pour déterminer l'adresse IPv6.

Étape 2: Configurez l'adressage IPv6 sur les clients Engineering et Design (ingénierie et conception).

a. Cliquez sur **Engineering** (ingénierie) et sélectionnez l'onglet **Desktop** (bureau), puis **IP Configuration** (configuration IP).

b. Configurez l'**adresse IPv6 2001:DB8:1:2::3** avec le préfixe **/64**.

c. Attribuez l'adresse link-local, **FE80::1**, à la **passerelle IPv6**.

d. Répétez les étapes 1a à 1c pour le client **Design** (conception). Consultez la **table d'adressage** pour déterminer l'adresse IPv6.

Partie 4: Tester et vérifier la connectivité réseau

Étape 1: Ouvrez les pages web de serveur à partir des clients.

a. Cliquez sur **Sales** (ventes), puis sur l'onglet **Desktop** (bureau). Fermez la fenêtre **IP Configuration** (configuration IP), le cas échéant.

b. Cliquez sur **Web Browser** (navigateur web). Entrez **2001:DB8:1:1::4** dans la zone de l'URL et cliquez sur **Go** (OK). Le site web **Accounting** doit apparaître.

c. Entrez **2001:DB8:1:2::4** dans la zone de l'URL et cliquez sur **Go** (OK). Le site web **CAD** doit apparaître.

d. Répétez les étapes 1a à 1d pour les autres clients.

Étape 2: Envoyez une requête ping au FAI.

a. Ouvrez la fenêtre de configuration de n'importe quel ordinateur client en cliquant sur l'icône correspondante.

b. Cliquez sur l'onglet **Desktop** > **Command Prompt** (bureau >invite de commandes).

c. Testez la connectivité avec le FAI en exécutant la commande suivante :

```
PC> ping 2001:DB8:1:A001::1
```

d. Répétez la commande **ping** avec d'autres clients jusqu'à ce que la connectivité complète ait été vérifiée.

Packet Tracer - Contrôle de l'adressage IPv4 et IPv6

Topologie

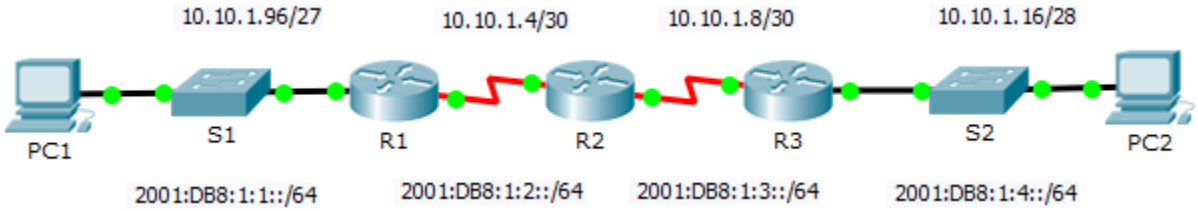


Table d'adressage

Appareil	Interface	Adresse IPv4	Masque de sous-réseau	Passerelle par défaut
		Préfixe/adresse IPv6		
R1	G0/0	10.10.1.97	255.255.255.224	N/A
		2001:DB8:1:1::1/64		N/A
	S0/0/1	10.10.1.6	255.255.255.252	N/A
		2001:DB8:1:2::2/64		N/A
	Link-local	FE80::1		N/A
R2	S0/0/0	10.10.1.5	255.255.255.252	N/A
		2001:DB8:1:2::1/64		N/A
	S0/0/1	10.10.1.9	255.255.255.252	N/A
		2001:DB8:1:3::1/64		N/A
	Link-local	FE80::2		N/A
R3	G0/0	10.10.1.17	255.255.255.240	N/A
		2001:DB8:1:4::1/64		N/A
	S0/0/1	10.10.1.10	255.255.255.252	N/A
		2001:DB8:1:3::2/64		N/A
	Link-local	FE80::3		N/A
PC1	Carte réseau			
PC2	Carte réseau			

Objectifs

Partie 1 : compléter la table d'adressage

Partie 2 : tester la connectivité à l'aide de la commande ping

Partie 3 : découvrir le chemin en le traçant

Le contexte

La technologie double pile (dual-stack) permet aux adresses IPv4 et IPv6 de coexister sur un même réseau. Dans cet exercice, vous allez étudier une mise en œuvre de type double pile (dual-stack), documenter les configurations IPv4 et IPv6 pour des périphériques finaux, tester la connectivité à la fois pour IPv4 et IPv6 à l'aide de la commande **ping** et tracer un chemin de bout en bout pour IPv4 et IPv6.

Partie 1: Compléter la table d'adressage

Étape 1: Utilisez ipconfig pour vérifier l'adressage IPv4.

a. Cliquez sur **PC1** et sur l'onglet **Desktop** (bureau) > **Command Prompt** (invite de commandes).

b. Saisissez la commande **ipconfig /all** pour obtenir les informations relatives à IPv4. Complétez la **table d'adressage** avec l'adresse IPv4, le masque de sous-réseau et la passerelle par défaut.

c. Cliquez sur **PC2** et cliquez sur l'onglet **Desktop** (bureau) > **Command Prompt** (invite de commandes).

d. Saisissez la commande **ipconfig /all** pour obtenir les informations relatives à IPv4. Complétez la **table d'adressage** avec l'adresse IPv4, le masque de sous-réseau et la passerelle par défaut.

Étape 2: Utilisez ipv6config pour vérifier l'adressage IPv6.

a. Sur **PC1**, exécutez la commande **ipv6config /all** pour collecter les informations IPv6. Complétez la **table d'adressage** avec l'adresse IPv6, le masque de sous-réseau et la passerelle par défaut.

b. Sur **PC2**, exécutez la commande **ipv6config /all** pour collecter les informations IPv6. Complétez la **table d'adressage** avec l'adresse IPv6, le masque de sous-réseau et la passerelle par défaut.

Partie 2: Tester la connectivité à l'aide de la commande ping

Étape 1: Utilisez une requête ping pour vérifier la connectivité IPv4.

a. À partir de **PC1**, envoyez une requête ping à l'adresse IPv4 de **PC2**. La requête a-t-elle abouti ? _____

b. À partir de **PC2**, envoyez une requête ping à l'adresse IPv4 de **PC1**. La requête a-t-elle abouti ? _____

Étape 2: Utilisez une requête ping pour vérifier la connectivité IPv6.

a. À partir de **PC1**, envoyez une requête ping à l'adresse IPv6 de **PC2**. La requête a-t-elle abouti ? _____

b. À partir de **PC2**, envoyez une requête ping à l'adresse IPv6 de **PC1**. La requête a-t-elle abouti ? _____

Partie 3: Découvrir le chemin en le traçant

Étape 1: Utilisez la commande tracert pour connaître le chemin IPv4.

a. À partir de **PC1**, tracez la route vers **PC2**.

PC> **`tracert 10.10.1.20`**

Quelles adresses ont été trouvées en chemin ? _____

À quelles interfaces les quatre adresses sont-elles associées ?

_____

b. À partir de **PC2**, tracez la route vers **PC1**.

Quelles adresses ont été trouvées en chemin ? _____

À quelles interfaces les quatre adresses sont-elles associées ?

_____

Étape 2: Utilisez la commande tracert pour connaître le chemin IPv6.

a. À partir de **PC1**, tracez la route vers l'adresse IPv6 de **PC2**.

PC> **`tracert 2001:DB8:1:4::A`**

Quelles adresses ont été trouvées en chemin ?

_____

À quelles interfaces les quatre adresses sont-elles associées ?

_____

b. À partir de **PC2**, tracez la route vers l'adresse IPv6 de **PC1**.

Quelles adresses ont été trouvées en chemin ?

_____

À quelles interfaces les quatre adresses sont-elles associées ?

_____

Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points obtenus
Partie 1 : compléter la table d'adressage	Étape 1b	10	
	Étape 1d	10	
	Étape 2a	10	
	Étape 2b	10	
Total de la partie 1		**40**	
Partie 2 : tester la connectivité à l'aide de la commande ping	Étape 1a	7	
	Étape 1b	7	
	Étape 2a	7	
	Étape 2b	7	
Total de la partie 2		**28**	
Partie 3 : découvrir le chemin en le traçant	Étape 1a	8	
	Étape 1b	8	
	Étape 2a	8	
	Étape 2b	8	
Total de la partie 3		**32**	
Score total		**100**	

Packet Tracer - Commandes ping et tracert pour tester le chemin

Topologie

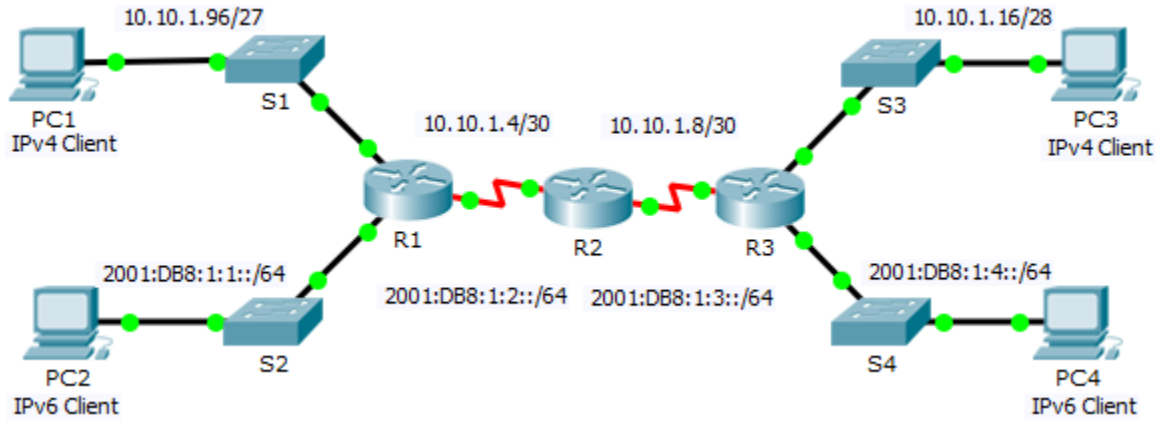


Table d'adressage

Appareil	Interface	Adresse IPv4	Masque de sous-réseau	Passerelle par défaut
		Préfixe/adresse IPv6		
R1	G0/0	2001:DB8:1:1::1/64		N/A
	G0/1	10.10.1.97	255.255.255.224	N/A
	S0/0/1	10.10.1.6	255.255.255.252	N/A
		2001:DB8:1:2::2/64		N/A
	Link-local	FE80::1		N/A
R2	S0/0/0	10.10.1.5	255.255.255.252	N/A
		2001:DB8:1:2::1/64		N/A
	S0/0/1	10.10.1.9	255.255.255.252	N/A
		2001:DB8:1:3::1/64		N/A
	Link-local	FE80::2		N/A
R3	G0/0	2001:DB8:1:4::1/64		N/A
	G0/1	10.10.1.17	255.255.255.240	N/A
	S0/0/1	10.10.1.10	255.255.255.252	N/A
		2001:DB8:1:3::2/64		N/A
	Link-local	FE80::3		N/A
PC1	Carte réseau			
PC2	Carte réseau			
PC3	Carte réseau			
PC4	Carte réseau			

Objectifs

Partie 1 : tester et restaurer la connectivité IPv4

Partie 2 : tester et restaurer la connectivité IPv6

Scénario

Des problèmes de connectivité se cachent dans cet exercice. Vous devrez non seulement collecter des informations relatives au réseau et les noter, mais également identifier les problèmes et mettre en œuvre des solutions acceptables pour rétablir la connectivité.

Remarque : le mot de passe d'exécution utilisateur est **cisco**. Le mot de passe en mode d'exécution privilégié est **class**.

Partie 1: Tester et restaurer la connectivité IPv4

Étape 1: Utilisez les commandes ipconfig et ping pour vérifier la connectivité.

a. Cliquez sur **PC1** et sur l'onglet **Desktop** (bureau) > **Command Prompt** (invite de commandes).

b. Saisissez la commande **ipconfig /all** pour obtenir les informations relatives à IPv4. Complétez la **table d'adressage** avec l'adresse IPv4, le masque de sous-réseau et la passerelle par défaut.

c. Cliquez sur **PC3** et cliquez sur l'onglet **Desktop** (bureau) > **Command Prompt** (invite de commandes).

d. Saisissez la commande **ipconfig /all** pour obtenir les informations relatives à IPv4. Complétez la **table d'adressage** avec l'adresse IPv4, le masque de sous-réseau et la passerelle par défaut.

e. Testez la connectivité entre **PC1** et **PC3**. La requête ping devrait échouer.

Étape 2: Identifiez la source du problème de connectivité.

a. À partir de **PC1**, exécutez la commande requise pour tracer la route vers **PC3**. Quelle était la dernière adresse IPv4 correcte atteinte ? _____

b. La commande trace s'arrête finalement après 30 tentatives. Appuyez sur **Ctrl** + **C** pour arrêter la commande trace avant les 30 tentatives.

c. À partir de **PC3**, exécutez la commande requise pour tracer la route vers **PC1**. Quelle était la dernière adresse IPv4 correcte atteinte ? _____

d. Appuyez sur **Ctrl** + **C** pour arrêter la commande trace.

e. Cliquez sur **R1**, puis sur l'onglet **CLI**. Appuyez sur **Entrée** et connectez-vous au routeur.

f. Exécutez la commande **show ip interface brief** pour répertorier les interfaces ainsi que leur état. Il existe deux adresses IPv4 sur le routeur. Une de ces adresses doit avoir été enregistrée à l'étape 2a. Quelle est l'autre adresse ? _____

g. Exécutez la commande **show ip route** pour répertorier les réseaux auxquels le routeur est connecté. Notez qu'il existe deux réseaux connectés à l'interface **Serial0/0/1**. Quelles sont-elles ? _____

h. Répétez les étapes 2e à 2g avec **R3** et les réponses indiquées ici. _____

Notez la modification de l'interface série de R3.

i. Effectuez plusieurs tests si cela vous permet d'identifier le problème. Le mode Simulation est disponible.

Étape 3: Proposez une solution pour résoudre le problème.

a. Comparez les réponses que vous avez fournies à l'étape 2 avec la documentation relative au réseau dont vous disposez. Quelle est l'origine de l'erreur ?

_____

b. Quelle solution proposeriez-vous pour résoudre le problème ?

_____

Étape 4: Mettez en œuvre le plan.

Mettez en œuvre la solution que vous avez proposée à l'étape 3b.

Étape 5: Vérifiez que la connexion est rétablie.

a. À partir de **PC1**, testez la connectivité avec **PC3**.

b. À partir de **PC3**, testez la connectivité avec **PC1**. Le problème est-il résolu ? _____

Étape 6: Documenter la solution

Partie 2: Tester et restaurer la connectivité IPv6

Étape 1: Utilisez les commandes ipv6config et ping pour vérifier la connectivité.

a. Cliquez sur **PC2** et cliquez sur l'onglet **Desktop** (bureau) > **Command Prompt** (invite de commandes).

b. Saisissez la commande **ipv6config /all** pour obtenir les informations relatives à IPv6. Complétez la **table d'adressage** avec l'adresse IPv6, le préfixe de sous-réseau et la passerelle par défaut.

c. Cliquez sur **PC4** et cliquez sur l'onglet **Desktop** (bureau) > **Command Prompt** (invite de commandes).

d. Saisissez la commande **ipv6config /all** pour obtenir les informations relatives à IPv6. Complétez la **table d'adressage** avec l'adresse IPv6, le préfixe de sous-réseau et la passerelle par défaut.

e. Testez la connectivité entre **PC2** et **PC4**. La requête ping devrait échouer.

Étape 2: Identifiez la source du problème de connectivité.

a. À partir de **PC2**, exécutez la commande requise pour tracer la route vers **PC4**. Quelle était la dernière adresse IPv6 correcte atteinte ? _____

b. La commande trace s'arrête finalement après 30 tentatives. Appuyez sur **Ctrl** + **C** pour arrêter la commande trace avant les 30 tentatives.

c. À partir de **PC4**, exécutez la commande requise pour tracer la route vers **PC2**. Quelle était la dernière adresse IPv6 correcte atteinte ? _____

d. Appuyez sur **Ctrl** + **C** pour arrêter la commande trace.

e. Cliquez sur **R3**, puis sur l'onglet **CLI**. Appuyez sur **Entrée** et connectez-vous au routeur.

f. Exécutez la commande **show ipv6 interface brief** pour répertorier les interfaces ainsi que leur état. Il existe deux adresses IPv6 sur le routeur. L'une d'entre elles doit correspondre à l'adresse de passerelle enregistrée à l'étape 1d. Y a-t-il une différence ? _____

g. Effectuez plusieurs tests si cela vous permet d'identifier le problème. Le mode Simulation est disponible.

Étape 3: Proposez une solution pour résoudre le problème.

a. Comparez les réponses que vous avez fournies à l'étape 2 avec la documentation relative au réseau dont vous disposez. Quelle est l'origine de l'erreur ?

_____

b. Quelle solution proposeriez-vous pour résoudre le problème ?

_____

Étape 4: Mettez en œuvre le plan.

Mettez en œuvre la solution que vous avez proposée à l'étape 3b.

Étape 5: Vérifiez que la connexion est rétablie.

a. À partir de **PC2**, testez la connectivité avec **PC4**.

b. À partir de **PC4**, testez la connectivité avec **PC2**. Le problème est-il résolu ? _____

Étape 6: Documenter la solution

Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points obtenus
Partie 1 : tester et restaurer la connectivité entre PC1 et PC3	Étape 1b	5	
	Étape 1d	5	
	Étape 2a	5	
	Étape 2c	5	
	Étape 2f	5	
	Étape 2g	5	
	Étape 2h	5	
	Étape 3a	5	
	Étape 3b	5	
Total de la partie 1		**45**	
Partie 2 : tester et restaurer la connectivité entre PC2 et PC4	Étape 1b	5	
	Étape 1d	5	
	Étape 2a	5	
	Étape 2c	5	
	Étape 2f	5	
	Étape 3a	5	
	Étape 3b	5	
Total de la partie 2		**35**	
Score relatif à Packet Tracer		**20**	
Score total		**100**	

Packet Tracer - Conception et mise en œuvre d'un système d'adressage VLSM

Topologie

Vous recevrez l'une des trois topologies possibles.

Table d’adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
	G0/0			N/A
	G0/1			N/A
	S0/0/0			N/A
	G0/0			N/A
	G0/1			N/A
	S0/0/0			N/A
	VLAN 1			
	VLAN 1			
	VLAN 1			
	VLAN 1			
	Carte réseau			
	Carte réseau			
	Carte réseau			
	Carte réseau			

Objectifs

Partie 1 : étudier les besoins du réseau

Partie 2 : concevoir le schéma d'adressage VLSM

Partie 3 : attribuer des adresses IP aux périphériques et vérifier la connectivité

Le contexte

Dans cet exercice, vous disposez d'une adresse réseau /24 à utiliser pour concevoir un schéma d'adressage VLSM. En fonction d'une série de conditions requises, vous allez attribuer les sous-réseaux et l'adressage, configurer des périphériques et vérifier la connectivité.

Partie 1: Étudier les besoins du réseau

Étape 1: Déterminer le nombre de sous-réseaux nécessaires

Vous allez subdiviser l'adresse réseau _____ . Le réseau présente les besoins suivants :

- Le LAN _____ nécessitera des adresses IP de l'hôte _____ .
- Le LAN _____ nécessitera des adresses IP de l'hôte _____ .
- Le LAN _____ nécessitera des adresses IP de l'hôte _____ .
- Le LAN _____ nécessitera des adresses IP de l'hôte _____ .

Combien de sous-réseaux sont nécessaires dans la topologie du réseau ? _____

Étape 2: Déterminez les informations de masque de sous-réseau pour chaque sous-réseau.

a. Quel masque de sous-réseau permettra de gérer le nombre d'adresses IP nécessaires à _____ ?

Combien d'adresses d'hôte utilisables ce sous-réseau prendra-t-il en charge ? _____

b. Quel masque de sous-réseau permettra de gérer le nombre d'adresses IP nécessaires à _____ ?

Combien d'adresses d'hôte utilisables ce sous-réseau prendra-t-il en charge ? _____

c. Quel masque de sous-réseau permettra de gérer le nombre d'adresses IP nécessaires à _____ ?

Combien d'adresses d'hôte utilisables ce sous-réseau prendra-t-il en charge ? _____

d. Quel masque de sous-réseau permettra de gérer le nombre d'adresses IP nécessaires à _____ ?

Combien d'adresses d'hôte utilisables ce sous-réseau prendra-t-il en charge ?_____

e. Quel masque de sous-réseau permettra de gérer le nombre d'adresses IP nécessaires à la connexion entre _____ et _____ ?

Partie 2: Concevoir le schéma d'adressage VLSM

Étape 1: Divisez le réseau _____ en fonction du nombre d'hôtes par sous-réseau.

a. Utilisez le premier sous-réseau pour accueillir le LAN le plus grand.

b. Utilisez le deuxième sous-réseau pour accueillir le deuxième LAN le plus grand.

c. Utilisez le troisième sous-réseau pour accueillir le troisième LAN le plus grand.

d. Utilisez le quatrième sous-réseau pour accueillir le quatrième LAN le plus grand.

e. Utilisez le cinquième sous-réseau pour gérer la connexion entre _____ et _____.

Étape 2: Documentez les sous-réseaux VLSM.

Complétez la **Table des sous-réseaux**, en indiquant les descriptions des sous-réseaux (par exemple LAN _____), le nombre d'hôtes nécessaires, l'adresse du sous-réseau, la première adresse d'hôte utilisable et l'adresse de diffusion. Répétez l'opération jusqu'à ce que toutes les adresses soient présentes.

Table des sous-réseaux

Description du sous-réseau	Nombre d'hôtes nécessaires	Adresse réseau/CIDR	Première adresse d'hôte utilisable	Adresse de diffusion

Étape 3: documentation du schéma d'adressage

a. Attribuez les premières adresses IP utilisables à _____ pour les deux liaisons LAN et la liaison WAN.

b. Attribuez les premières adresses IP utilisables à _____ pour les deux liaisons LAN. Attribuez la dernière adresse IP utilisable à la liaison WAN.

c. Attribuez la deuxième adresse IP utilisable aux commutateurs.

d. Attribuez les dernières adresses IP utilisables aux hôtes.

Partie 3: Attribuer des adresses IP aux périphériques et vérifier la connectivité

L'adressage IP est déjà configuré en grande partie sur ce réseau. Procédez comme suit pour terminer la configuration de l'adressage.

Étape 1: Configurez l'adressage IP sur les interfaces LAN de _____.

Étape 2: Configurez l'adressage IP sur _____ , y compris la passerelle par défaut.

Étape 3: Configurez l'adressage IP sur _____ , y compris la passerelle par défaut.

Étape 4: Vérifier la connectivité

Vous ne pouvez vérifier la connectivité qu'à partir de _____, _____ et _____. Vous devriez toutefois pouvoir envoyer une requête ping à toutes les adresses IP figurant dans la **table d'adressage**.

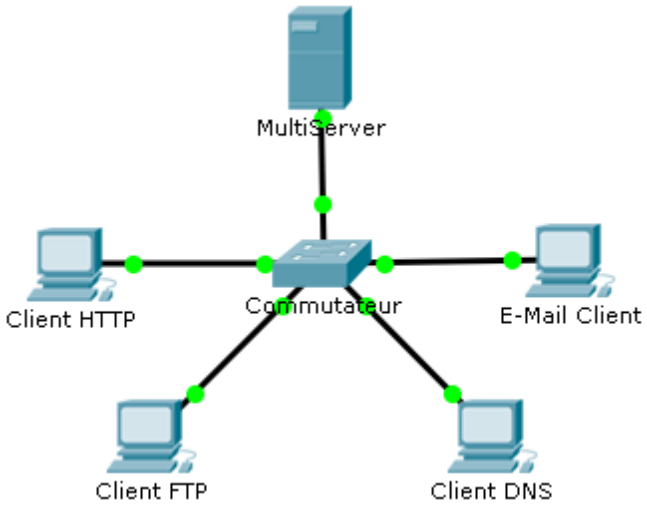
Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points obtenus
Partie 1 : étudier les besoins du réseau	Étape 1	1	
	Étape 2	4	
Total de la partie 1		**5**	
Partie 2 : concevoir le schéma d'adressage VLSM			
Compléter la table des sous-réseaux		25	
Documenter l'adressage		40	
Total de la partie 2		**65**	
Score relatif à Packet Tracer		**30**	
Score total		**100**	

ID:

Simulation Packet Tracer - Communications TCP et UDP

Topologie



Objectifs

Partie 1 : Générer du trafic sur le réseau en mode Simulation

Partie 2 : Examiner les fonctionnalités des protocoles TCP et UDP

Contexte

Cet exercice de simulation vise à fournir une base pour comprendre les protocoles TCP et UDP en détail. Le mode Simulation permet de voir les fonctionnalités des différents protocoles.

Lors de la transmission des données sur le réseau, ces dernières sont divisées en parties plus petites et sont étiquetées afin de pouvoir ensuite être réassemblées. Chacune de ces parties reçoit un nom spécifique (unité de données de protocole, PDU) et est associée à une couche donnée. Le mode Simulation de Packet Tracer permet à l'utilisateur de consulter tous les protocoles et les PDU associées. Les étapes présentées ci-dessous guident l'utilisateur tout au long du processus de demande de services à l'aide de diverses applications disponibles sur un PC client.

Cet exercice permet de découvrir les fonctionnalités des protocoles TCP et UDP, le multiplexage et l'utilité des numéros de port lors de l'identification de l'application locale qui a demandé les données ou qui les envoie.

Partie 1: Générer du trafic sur le réseau en mode Simulation

Étape 1: Générez du trafic pour compléter les tables ARP (Address Resolution Protocol).

Effectuez les tâches suivantes afin de diminuer le trafic réseau affiché dans la simulation.

a. Cliquez sur **MultiServer** (Multiserveur) puis sur l'onglet **Desktop** (Bureau) > **Command Prompt** (Invite de commande).

b. Exécutez la commande **ping 192.168.1.255**. Il faudra attendre quelques secondes pour que chaque périphérique du réseau réponde à **MultiServer** (Multiserveur).

c. Fermez la fenêtre **MultiServer** (Multiserveur).

Étape 2: Générez le trafic web (HTTP).

a. Passez en mode Simulation.

b. Cliquez sur **HTTP Client** (Client HTTP), puis sur l'onglet **Desktop** (Bureau) > **Web Browser** (Navigateur web).

c. Dans le champ URL, entrez **192.168.1.254** et cliquez sur **Go** (OK). Les PDU s'affichent dans la fenêtre de simulation.

d. Réduisez la fenêtre de configuration **HTTP Client** (Client HTTP), mais ne la fermez pas.

Étape 3: Générez du trafic FTP.

a. Cliquez sur **FTP Client** (Client FTP), puis sur l'onglet **Desktop** (Bureau) > **Command Prompt** (Invite de commande).

b. Exécutez la commande **ftp 192.168.1.254**. Les PDU s'affichent dans la fenêtre de simulation.

c. Réduisez la fenêtre de configuration **FTP Client** (Client FTP), mais ne la fermez pas.

Étape 4: Générez du trafic DNS.

a. Cliquez sur **DNS Client** (Client DNS) puis sur l'onglet **Desktop** (Bureau) > **Command Prompt** (Invite de commande).

b. Exécutez la commande **nslookup multiserver.pt.ptu**. Une PDU s'affichera dans la fenêtre de simulation.

c. Réduisez la fenêtre de configuration **DNS Client** (Client DNS), mais ne la fermez pas.

Étape 5: Générez du trafic de messagerie.

a. Cliquez sur **E-Mail Client** (Client de messagerie), puis sur l'onglet **Desktop** (Bureau) > **E Mail** (E-mail).

b. Cliquez sur **Compose** (Composer) et entrez les informations suivantes :

1) **À :** user@multiserver.pt.ptu

2) **Objet :** Personnalisez la ligne d'objet.

3) **Corps du message** : Personnalisez l'e-mail.

c. Cliquez sur **Send** (Envoyer).

d. Réduisez la fenêtre de configuration **E-Mail Client** (Client de messagerie), mais ne la fermez pas.

Étape 6: Vérifiez que le trafic est généré et prêt pour la simulation.

Chaque ordinateur client doit posséder des PDU répertoriées dans le panneau de simulation.

Partie 2: Examiner les fonctionnalités des protocoles TCP et UDP

Étape 1: Examinez le multiplexage lorsque la totalité du trafic transite par le réseau.

Vous allez maintenant utiliser le bouton **Capture/Forward** (Capture/Transfert) ainsi que le bouton **Back** (Précédent) du panneau de simulation.

a. Cliquez une seule fois sur **Capture/Forward** (Capture/Transfert). Toutes les PDU sont transférées vers le commutateur.

b. Cliquez à nouveau sur **Capture/Forward** (Capture/Transfert). Certaines PDU disparaissent. Selon vous, que leur est-il arrivé ?

_____

c. Cliquez à six reprises sur **Capture/Forward** (Capture/Transfert). Tous les clients doivent avoir reçu une réponse. Notez qu'une seule PDU peut traverser un fil dans une direction à un moment donné. Comment cela s'appelle-t-il ?

_____

d. Diverses PDU apparaissent dans la liste des événements dans le volet supérieur droit de la fenêtre de simulation. Pourquoi sont-elles de tant de couleurs différentes ?

_____

e. Cliquez à huit reprises sur **Back** (Précédent). Cela devrait réinitialiser la simulation.

Remarque : ne cliquez pas sur le bouton **Reset Simulation** (Réinitialiser la simulation) au cours de cet exercice ; sinon, vous devrez répéter les étapes de la partie 1.

Étape 2: Inspectez le trafic HTTP lorsque les clients communiquent avec le serveur.

a. Filtrez le trafic de manière à n'afficher que les PDU **HTTP** et **TCP** :

1) Cliquez sur **Edit Filters** (Modifier les filtres) et cochez la case **Show All/None** (Afficher tous/aucun).

2) Sélectionnez **HTTP** et **TCP**. Cliquez n'importe où en dehors de la zone Edit Filters (Modifier les filtres) pour la masquer. Les événements visibles doivent maintenant afficher uniquement les PDU **HTTP** et **TCP**.

b. Cliquez sur **Capture/Forward** (Capture/Transfert). Placez le pointeur de la souris sur chacune des PDU jusqu'à ce que vous en trouviez une qui provient de **HTTP Client** (Client HTTP). Cliquez sur l'enveloppe PDU pour l'ouvrir.

c. Cliquez sur l'onglet **Inbound PDU Details** (Entrée de l'unité de données de protocole) et faites défiler l'écran jusqu'à la dernière section. Quelle étiquette est attribuée à la section ?

_____

Ces communications sont-elles considérées comme fiables ?

_____

d. Notez les valeurs **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** et **ACK NUM**. Quel est le contenu du champ situé à gauche du champ **WINDOW** ?

_____

e. Fermez la PDU et cliquez sur **Capture/Forward** (Capture/Transfert) jusqu'à ce qu'une PDU revienne au périphérique **HTTP Client** avec une coche.

f. Cliquez sur l'enveloppe PDU et sélectionnez **Inbound PDU Details** (Entrée de l'unité de données de protocole). Quelles modifications observez-vous sur les numéros de port et d'ordre ?

_____

_____

g. Il y a une deuxième **PDU** de couleur différente que **HTTP Client** (Client HTTP) a préparée en vue de l'envoyer à **MultiServer** (Multiserveur). Il s'agit du début de la communication HTTP. Cliquez sur la deuxième enveloppe PDU et sélectionnez **Outbound PDU Details** (Sortie de l'unité de données de protocole).

h. Quelles informations s'affichent maintenant dans la section TCP ? Quelles modifications observez-vous sur les numéros de port et d'ordre par rapport aux deux PDU précédentes ?

_____

_____

i. Cliquez sur **Back** (Précédent) jusqu'à ce que la simulation soit réinitialisée.

Étape 3: Inspectez le trafic FTP lorsque les clients communiquent avec le serveur.

a. Dans le panneau de simulation, changez **Edit Filters** (Modifier les filtres) de manière à n'afficher que **FTP** et **TCP**.

b. Cliquez sur **Capture/Forward** (Capture/Transfert). Placez le pointeur de la souris sur chacune des PDU jusqu'à ce que vous en trouviez une qui provient de **FTP Client** (Client FTP). Cliquez sur l'enveloppe PDU pour l'ouvrir.

c. Cliquez sur l'onglet **Inbound PDU Details** (Entrée de l'unité de données de protocole) et faites défiler l'écran jusqu'à la dernière section. Quelle étiquette est attribuée à la section ?

_____

Ces communications sont-elles considérées comme fiables ?

_____

d. Notez les valeurs **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** et **ACK NUM**. Quel est le contenu du champ situé à gauche du champ **WINDOW** ?

_____

e. Fermez la PDU et cliquez sur **Capture/Forward** (Capture/Transfert) jusqu'à ce qu'une PDU revienne au périphérique **FTP Client** (Client FTP) avec une coche.

f. Cliquez sur l'enveloppe PDU et sélectionnez **Inbound PDU Details** (Entrée de l'unité de données de protocole). Quelles modifications observez-vous sur les numéros de port et d'ordre ?

_____

_____

g. Cliquez sur l'onglet **Outbound PDU Details** (Sortie de l'unité de données de protocole). Quelles modifications observez-vous sur les numéros de port et d'ordre par rapport aux deux résultats précédents ?

_____

_____

h. Fermez la PDU et cliquez sur **Capture/Forward** (Capture/Transfert) jusqu'à ce qu'une deuxième PDU revienne au périphérique **FTP Client** (Client FTP). La PDU est de couleur différente.

i. Ouvrez la PDU et sélectionnez **Inbound PDU Details** (Entrée de l'unité de données de protocole). Faites défiler l'affichage jusqu'après la section TCP. Quel est le message en provenance du serveur ?

_____

j. Cliquez sur **Back** (Précédent) jusqu'à ce que la simulation soit réinitialisée.

Étape 4: Inspectez le trafic DNS lorsque les clients communiquent avec le serveur.

a. Dans le panneau de simulation, changez **Edit Filters** (Modifier les filtres) de manière à n'afficher que **DNS** et **UDP**.

b. Cliquez sur l'enveloppe PDU pour l'ouvrir.

c. Cliquez sur l'onglet **Inbound PDU Details** (Entrée de l'unité de données de protocole) et faites défiler l'écran jusqu'à la dernière section. Quelle étiquette est attribuée à la section ?

_____

Ces communications sont-elles considérées comme fiables ?

_____

d. Notez les valeurs **SRC PORT** et **DEST PORT**. Pourquoi n'y a-t-il ni numéro d'ordre ni numéro d'accusé de réception ?

_____

e. Fermez la **PDU** et cliquez sur **Capture/Forward** (Capture/Transfert) jusqu'à ce qu'une PDU revienne au périphérique **DNS Client** (Client DNS) avec une coche.

f. Cliquez sur l'enveloppe PDU et sélectionnez **Inbound PDU Details** (Entrée de l'unité de données de protocole). Quelles modifications observez-vous sur les numéros de port et d'ordre ?

_____

g. Comment s'appelle la dernière section de la **PDU** ?

_____

h. Cliquez sur **Back** (Précédent) jusqu'à ce que la simulation soit réinitialisée.

Étape 5: Inspectez le trafic de messagerie lorsque les clients communiquent avec le serveur.

a. Dans le panneau de simulation, changez **Edit Filters** (Modifier les filtres) de manière à n'afficher que **POP3, SMTP** et **TCP**.

b. Cliquez sur **Capture/Forward** (Capture/Transfert). Placez le pointeur de la souris sur chacune des PDU jusqu'à ce que vous en trouviez une qui provient de **E-mail Client** (Client de messagerie). Cliquez sur l'enveloppe PDU pour l'ouvrir.

c. Cliquez sur l'onglet **Inbound PDU Details** (Entrée de l'unité de données de protocole) et faites défiler l'écran jusqu'à la dernière section. Quel protocole de couche transport le trafic de messagerie utilise-t-il ?

_____

Ces communications sont-elles considérées comme fiables ?

_____

d. Notez les valeurs **SRC PORT**, **DEST PORT**, **SEQUENCE NUM** et **ACK NUM.** Quel est le contenu du champ situé à gauche du champ **WINDOW** ?

_____

e. Fermez la **PDU** et cliquez sur **Capture/Forward** (Capture/Transfert) jusqu'à ce qu'une PDU revienne au périphérique **E-Mail Client** (Client de messagerie) avec une coche.

f. Cliquez sur l'enveloppe PDU et sélectionnez **Inbound PDU Details** (Entrée de l'unité de données de protocole). Quelles modifications observez-vous sur les numéros de port et d'ordre ?

_____

g. Cliquez sur l'onglet **Outbound PDU Details** (Sortie de l'unité de données de protocole). Quelles modifications observez-vous sur les numéros de port et d'ordre par rapport aux deux résultats précédents ?

_____

h. Il y a une deuxième **PDU** de couleur différente que **HTTP Client** (Client HTTP) a préparée en vue de l'envoyer à **MultiServer** (Multiserveur). Il s'agit du début de la communication par messagerie. Cliquez sur la deuxième enveloppe PDU et sélectionnez **Outbound PDU Details** (Sortie de l'unité de données de protocole).

i. Quelles modifications observez-vous sur les numéros de port et d'ordre par rapport aux deux **PDU** précédentes ?

_____

_____

j. Quel protocole de messagerie est associé au port TCP 25 ? Quel protocole de messagerie est associé au port TCP 110 ?

_____

k. Cliquez sur **Back** (Précédent) jusqu'à ce que la simulation soit réinitialisée.

Étape 6: Examinez l'utilisation des numéros de port à partir du serveur.

a. Procédez rapidement comme suit pour afficher les sessions TCP actives :

1) Repassez en mode **Realtime** (Temps réel).

2) Cliquez sur **MultiServer** (Multiserveur) puis sur l'onglet **Desktop** (Bureau) > **Command Prompt** (Invite de commande).

b. Exécutez la commande **netstat**. Quels sont les protocoles répertoriés dans la colonne de gauche ?

_____

Quels sont les numéros de port utilisés par le serveur ?

_____

c. Quels sont les états des sessions ?

_____

d. Exécutez à plusieurs reprises la commande **netstat** jusqu'à ce qu'une seule session soit toujours à l'état ESTABLISHED. Pour quel service cette connexion est-elle encore ouverte ? _____

Pourquoi cette session ne se ferme-t-elle pas comme les trois autres ? (Conseil : vérifiez les clients réduits.)

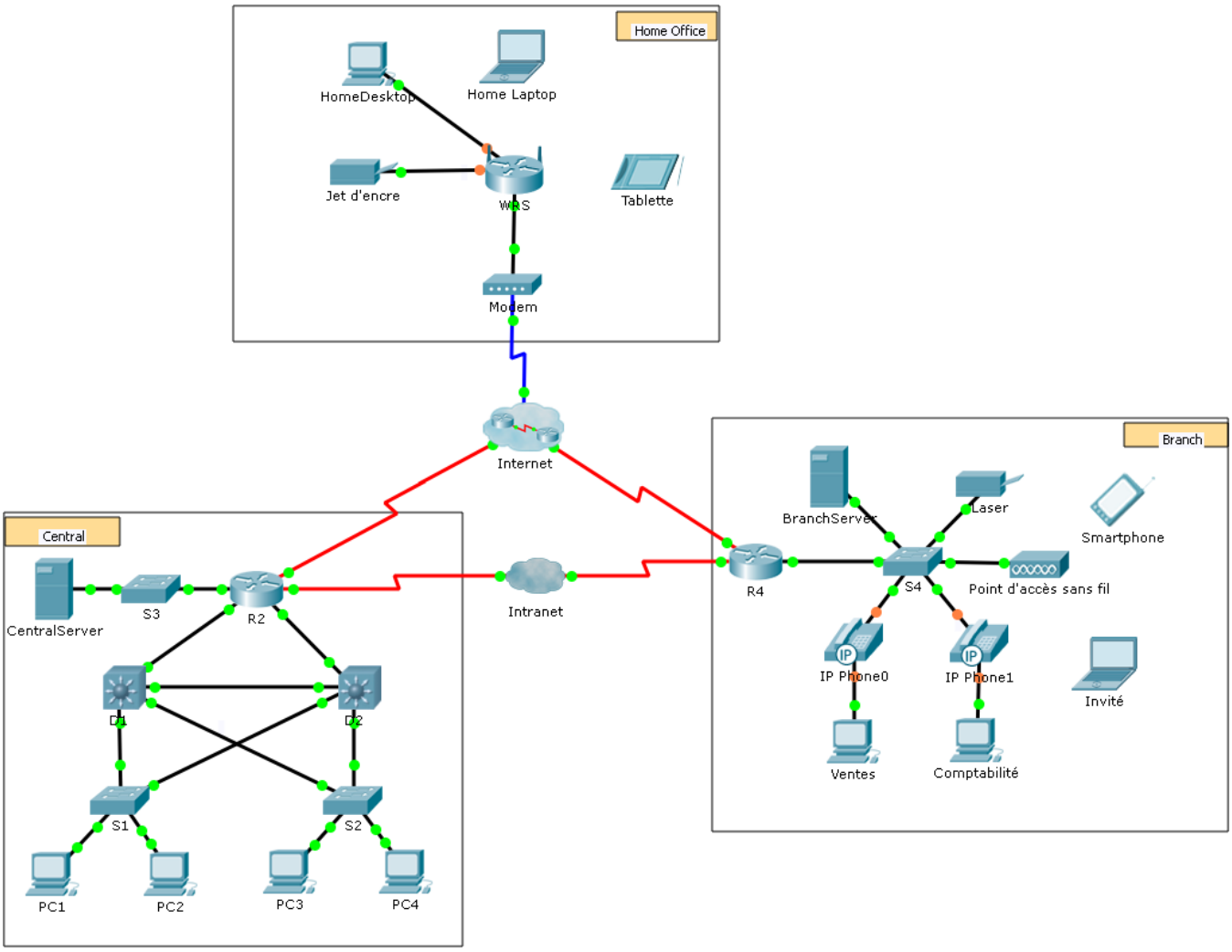
_____

Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points obtenus
Partie 2 : Examiner les fonctionnalités des protocoles TCP et UDP	Étape 1	15	
	Étape 2	15	
	Étape 3	15	
	Étape 4	15	
	Étape 5	15	
	Étape 6	25	
	Score total	**100**	

Packet Tracer - Web et messagerie

Topologie



Objectifs

Partie 1 : Configurer et vérifier des services web

Partie 2 : Configurer et vérifier des services de messagerie

Contexte

Dans cet exercice, vous allez configurer des services web et de messagerie à l'aide du serveur simulé dans Packet Tracer. Vous configurerez ensuite des clients pour accéder aux services web et de messagerie.

Remarque : Packet Tracer simule uniquement le processus de configuration de ces services. Les logiciels relatifs aux services web et de messagerie possèdent chacun leurs propres instructions d'installation et de configuration.

Partie 1: Configurer et vérifier des services web

Étape 1: Configurez des services web sur CentralServer et BranchServer.

a. Cliquez sur **CentralServer**, puis sur l'onglet **Services** > **HTTP**.

b. Cliquez sur **On** (Actif) pour activer HTTP et HTTP Secure (HTTPS).

c. En option. Personnalisez le code HTML.

d. Répétez les étapes 1a à 1c sur **BranchServer**.

Étape 2: Vérifiez les serveurs web en accédant aux pages web.

Ce réseau comporte de nombreux terminaux, mais utilisez **PC3** pour les besoins de cette étape.

a. Cliquez sur **PC3**, puis sur l'onglet **Desktop** (Bureau) > **Web Browser** (Navigateur web).

b. Dans la zone URL, entrez **10.10.10.2** comme adresse IP et cliquez sur **Go** (OK). Le site web **CentralServer** s'affiche.

c. Dans la zone URL, entrez **64.100.200.1** comme adresse IP et cliquez sur **Go** (OK). Le site web **BranchServer** s'affiche.

d. Dans la zone URL, entrez **centralserver.pt.pka** et cliquez sur **Go** (OK). Le site web **CentralServer** s'affiche.

e. Dans la zone URL, entrez **branchserver.pt.pka** et cliquez sur **Go** (OK). Le site web **BranchServer** s'affiche.

f. Quel protocole traduit les noms **centralserver.pt.pka** et **branchserver.pt.pka** en adresses IP ?

_____

Partie 2: Configurer et vérifier des services de messagerie sur des serveurs

Étape 1: Configurez CentralServer pour l'envoi (SMTP) et la réception (POP3) du courrier électronique.

a. Cliquez sur **CentralServer**, puis sélectionnez l'onglet **Services** suivi du bouton **EMAIL**.

b. Cliquez sur **On** (Actif) pour activer SMTP et POP3.

c. Choisissez le nom de domaine **centralserver.pt.pka** et cliquez sur **Set** (Définir).

d. Créez un utilisateur appelé **central-user** avec le mot de passe **cisco**. Cliquez sur **+** pour ajouter l'utilisateur.

Étape 2: Configurez BranchServer pour l'envoi (SMTP) et la réception (POP3) du courrier électronique.

a. Cliquez sur **BranchServer**, puis sur l'onglet **Services** > **EMAIL**.

b. Cliquez sur **On** (Actif) pour activer SMTP et POP3.

c. Choisissez le nom de domaine **branchserver.pt.pka** et cliquez sur **Set** (Définir).

d. Créez un utilisateur appelé **branch-user** avec le mot de passe **cisco**. Cliquez sur **+** pour ajouter l'utilisateur.

Étape 3: Configurez PC3 pour utiliser le service de messagerie de CentralServer.

a. Cliquez sur **PC3**, puis sur l'onglet **Desktop** (Bureau) > **E Mail** (E-mail).

b. Saisissez les valeurs suivantes dans les champs correspondants :

1) Votre nom : **Central User**

2) Adresse de messagerie : **central-user@centralserver.pt.pka**

3) Serveur de messagerie entrant : **10.10.10.2**

4) Serveur de messagerie sortant : **10.10.10.2**

5) Nom de l'utilisateur : **central-user**

6) Mot de passe : **cisco**

c. Cliquez sur **Save** (Enregistrer). La fenêtre Mail Browser (Navigateur de messagerie) s'affiche.

d. Cliquez sur **Receive** (Recevoir). Si tout a été correctement configuré sur le client et le serveur, la fenêtre Mail Browser (Navigateur de messagerie) affiche le message de confirmation `Receive Mail Success (E-mail correctement reçu).`

Étape 4: Configurez Sales pour utiliser le service de messagerie de BranchServer.

a. Cliquez sur **Sales**, puis sur l'onglet **Desktop** (Bureau) > **E Mail** (E-mail).

b. Saisissez les valeurs suivantes dans les champs correspondants :

1) Votre nom : **Branch User**

2) Adresse de messagerie : **branch-user@branchserver.pt.pka**

3) Serveur de messagerie entrant : **172.16.0.3**

4) Serveur de messagerie sortant : **172.16.0.3**

5) Nom de l'utilisateur : **branch-user**

6) Mot de passe : **cisco**

c. Cliquez sur **Save** (Enregistrer). La fenêtre Mail Browser (Navigateur de messagerie) s'affiche.

d. Cliquez sur **Receive** (Recevoir). Si tout a été correctement configuré sur le client et le serveur, la fenêtre Mail Browser (Navigateur de messagerie) affiche le message de confirmation `Receive Mail Success (E-mail correctement reçu).`

e. L'exercice doit être complètement terminé. Ne fermez pas la fenêtre de configuration de Sales ou la fenêtre Mail Browser (Navigateur de messagerie).

Étape 5: Envoyez un e-mail à partir du client Sales et du client PC3.

a. Dans la fenêtre **Mail Browser** (Navigateur de messagerie) de **Sales**, cliquez sur **Compose** (Composer).

b. Saisissez les valeurs suivantes dans les champs correspondants :

1) À : **central-user@centralserver.pt.pka**

2) Objet : *Personnalisez la ligne d'objet*.

3) Corps du message : *Personnalisez l'e-mail*.

c. Cliquez sur **Send** (Envoyer).

d. Vérifiez que **PC3** a reçu l'e-mail. Cliquez sur **PC3**. Si la fenêtre Mail Browser (Navigateur de messagerie) est fermée, cliquez sur **E Mail** (E-mail).

e. Cliquez sur **Receive** (Recevoir). Un e-mail provenant de Sales s'affiche. Double-cliquez sur ce message.

f. Cliquez sur **Reply** (Répondre), personnalisez votre réponse, puis cliquez sur **Send** (Envoyer).

g. Vérifiez que **Sales** a reçu la réponse.

Packet Tracer - Configuration de mots de passe sécurisés et de SSH

Topologie

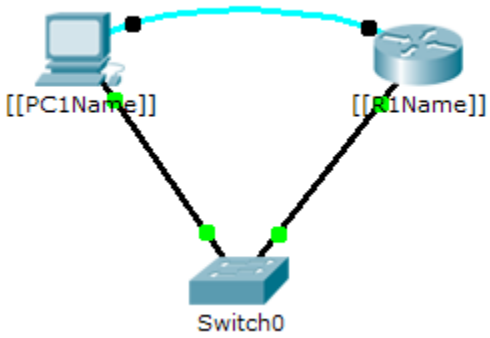


Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
	G0/0		255.255.255.0	
	Carte réseau		255.255.255.0	

Scénario

L'administrateur réseau vous a demandé de préparer _____ en vue de son déploiement. Avant de le connecter au réseau, il faut mettre en place des mesures de sécurité.

Conditions requises

- Configurez l'adressage IP sur _____ conformément à la table d'adressage.
- Accédez à _____ par la console à partir du terminal sur PC-A.
- Configurez l'adressage IP sur _____ et activez l'interface.
- Configurez le nom d'hôte en tant que _____.
- Chiffrez tous les mots de passe en clair.
  _____ `(config)# service password-encryption`
- Choisissez un mot de passe secret fort.
- Choisissez le nom de domaine _____**.com** (sensible à la casse pour la notation dans Packet Tracer).
  _____ `(config)# ip domain-name [[R1Name]].com`
- Créez un utilisateur au choix avec un mot de passe fort.
  _____ `(config)# username any_user password any_password`
- Générez des clés RSA de 1 024 bits.

Remarque : dans Packet Tracer, exécutez la commande **crypto key generate rsa**, puis appuyez sur Entrée pour continuer.

_____ (config)# **crypto key generate rsa**

- Bloquez pendant trois minutes quiconque n'arrive pas à se connecter au bout de quatre tentatives en deux minutes.

  _____ (config)# **login block-for 180 attempts 4 within 120**

- Configurez les lignes VTY pour l'accès SSH et utilisez les profils utilisateur locaux pour l'authentification.

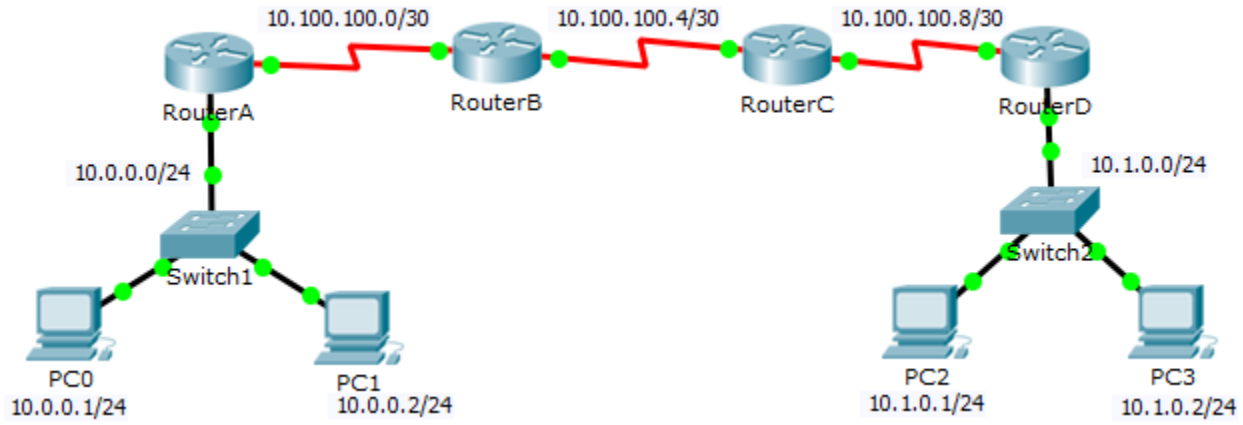
  _____ (config)# **line vty 0 4**
  _____ (config-line)# **transport input ssh**
  _____ (config-line)# **login local**

- Enregistrez la configuration en mémoire NVRAM.
- Soyez prêt à montrer au formateur que vous avez établi un accès SSH à partir de _____ vers _____.

ID isomorphe : _____ _____ _____

Packet Tracer - Test de la connectivité avec

Topologie



Objectifs

Partie 1 : Tester la connectivité de bout en bout à l'aide de la commande tracert

Partie 2 : Comparer avec la commande traceroute sur un routeur

Contexte

Cet exercice a pour objectif de vous aider à résoudre les problèmes de connectivité sur un réseau à l'aide de commandes vous permettant de suivre l'itinéraire (ou la route) du trafic de la source à la destination. Vous devez examiner les résultats de **tracert** (la commande de Windows) et de **traceroute** (la commande d'IOS) lors du transport des paquets sur le réseau et déterminer la cause d'un problème sur le réseau. Une fois le problème résolu, utilisez les commandes **tracert** et **traceroute** pour vérifier que le paquet est arrivé à destination.

Parte 1: Tester la connectivité de bout en bout à l'aide de la commande tracert

Etapa 1: Envoyez une requête ping à partir d'une extrémité du réseau vers l'autre extrémité.

Cliquez sur **PC1** et ouvrez l'**invite de commande**. Envoyez une requête ping à **PC3** à l'adresse **10.1.0.2**. Quel message s'affiche en réponse à la requête ping ?

_____

Etapa 2: Suivez le trafic à partir de PC1 afin de déterminer où se situe le problème de connectivité.

a. À partir de l'**invite de commande** de **PC1**, tapez **tracert 10.1.0.2**.

b. Lorsque vous recevez un message indiquant que le **délai d'attente de la demande est dépassé**, appuyez sur **CTRL+C**. Quelle est la première adresse IP affichée dans les résultats de la commande **tracert** ?

_____

c. Observez les résultats de la commande **tracert**. Quelle est la dernière adresse atteinte avec la commande **tracert** ?

_____

Etapa 3: Résolvez le problème réseau.

a. Comparez la dernière adresse atteinte à l'aide de la commande **tracert** avec les adresses réseau répertoriées dans la topologie. Le périphérique le plus éloigné de l'hôte 10.0.0.2 et dont l'adresse figure dans la plage réseau trouvée correspond au point de défaillance. Quels périphériques ont des adresses configurées pour le réseau correspondant à l'emplacement de la défaillance ?

_____

b. Cliquez sur **RouterC** puis sur l'onglet **CLI**. Quel est l'état des interfaces ?

_____

c. Comparez les adresses IP sur les interfaces avec les adresses réseau dans la topologie. Voyez-vous quelque chose de particulier ?

_____

d. Effectuez les modifications nécessaires en vue de restaurer la connectivité, mais ne modifiez pas les sous-réseaux. Quelle est la solution ?

_____

Etapa 4: Vérifiez que la connectivité de bout en bout est établie.

a. À partir de l'**invite de commande** de PC1, tapez **tracert 10.1.0.2**.

b. Observez les résultats de la commande **tracert**. La commande s'est-elle exécutée correctement ? _____

Parte 2: Comparer avec la commande traceroute sur un routeur

a. Cliquez sur **RouterA** puis sur l'onglet **CLI**.

b. Exécutez la commande **traceroute 10.1.0.2**. La commande s'est-elle exécutée correctement ? _____

c. Comparez les résultats de la commande **traceroute** du routeur avec ceux de la commande **tracert** de l'ordinateur. Qu'est-ce qui a changé dans la liste des adresses renvoyées ?

_____

Parte 3: Utilisation de la commande extended traceroute

En plus de **traceroute**, Cisco IOS propose une commande extended traceroute. Extended Traceroute permet à l'administrateur d'ajuster des paramètres mineurs d'exécution traceroute en posant des questions simples.

Dans le cadre du processus de vérification, utilisez extended traceroute sur **RouterA** pour augmenter le nombre de paquets ICMP que la commande traceroute envoie à chaque saut.

Remarque : la commande **tracert** de Windows permet également à l'utilisateur de modifier certains aspects en utilisant des options de ligne de commande.

a. Cliquez sur **RouterA** puis sur l'onglet **CLI**.

b. Entrez la commande **traceroute** et appuyez sur **ENTRÉE**. Vous remarquerez que seule la commande traceroute doit être saisie.

c. Répondez aux questions posées par la commande extended traceroute, en procédant comme suit. La commande extended **traceroute** doit être exécutée immédiatement après avoir répondu à la dernière question.

```
Protocol [ip]: ip
Target IP address: 10.1.0.2
Source address: 10.100.100.1
Numeric display [n]: n
Timeout in seconds [3]: 3
Probe count [3]: 5
Minimum Time to Live [1]: 1
Maximum Time to Live [30]: 30
```

Remarque : la valeur affichée entre parenthèses correspond à la valeur par défaut. Elle sera utilisée par **traceroute** si aucune valeur n'est saisie. Il suffit d'appuyer sur **Entrée** pour utiliser la valeur par défaut.

À combien de questions a-t-on répondu avec des valeurs personnalisées ? Quelle était la nouvelle valeur ?

_____

Combien de paquets ICMP ont été envoyés par **RouterA** ?

_____

Remarque : « Probe count » indique le nombre de paquets ICMP envoyés à chaque saut par la commande **traceroute**. Un nombre plus élevé de sondes permet un meilleur temps de parcours (aller-retour) moyen pour les paquets.

d. Sur **RouterA** toujours, exécutez à nouveau la commande extended **traceroute** mais, cette fois, en définissant la valeur d'expiration sur 7 secondes.

Que s'est-il passé ? Comment la nouvelle valeur d'expiration affecte-t-elle la commande **traceroute** ?

_____

Pensez à une utilisation possible du paramètre timeout.

_____

Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points obtenus
Partie 1 : Tester la connectivité de bout en bout à l'aide de la commande **tracert**	Étape 1	10	
	Étape 2b	10	
	Étape 2c	10	
	Étape 3a	10	
	Étape 3c	10	
	Étape 3d	5	
	Étape 3e	5	
	Étape 4b	10	
Total de la Partie 1		**80**	
Partie 2 : Comparer avec la commande **traceroute** sur un routeur	a	2	
	b	3	
	c	5	
Total de la partie 2		**10**	
Partie 3 : Commande extended traceroute	a	2	
	b	3	
	c	2	
	d	3	
Total de la partie 3		**10**	
Score relatif à Packet Tracer		**10**	
Score total		**100**	

Packet Tracer - Utilisation des commandes show

Objectifs

Partie 1 : Analyser le résultat des commandes show

Partie 2 : Questions de réflexion

Contexte

Cet exercice a pour objectif de vous aider à mieux maîtriser les commandes **show** du routeur. Vous n'avez pas besoin d'effectuer la configuration. Examinez plutôt le résultat de plusieurs commandes **show**.

Partie 1: Analyser le résultat des commandes show

Étape 1: Connectez-vous à ISPRouter

a. Cliquez sur **ISP PC**, puis sur l'onglet **Desktop** (Bureau) et enfin sur **Terminal**.

b. Passez en mode d'exécution privilégié.

c. Utilisez les commandes **show** suivantes pour répondre aux questions de réflexion de la partie 2 :

```
show arp
show flash:
show ip route
show interfaces
show ip interface brief
show protocols
show users
show version
```

Partie 2: Questions de réflexion

1. Quelles commandes permettent d'obtenir l'adresse IP, le préfixe réseau et l'interface ?

   _____

   _____

2. Quelles commandes permettent d'obtenir l'adresse IP et l'affectation des interfaces, mais pas le préfixe réseau ?

   _____

   _____

3. Quelles commandes permettent d'obtenir l'état des interfaces ?

   _____

   _____

4. Quelles commandes permettent d'obtenir des informations sur l'IOS chargé sur le routeur ?

   _____

   _____

5. Quelles commandes permettent d'obtenir des informations sur les adresses des interfaces du routeur ?

   _____

   _____

6. Quelles commandes permettent d'obtenir des informations sur la quantité de mémoire Flash disponible ?

   _____

   _____

7. Quelles commandes permettent d'obtenir des informations sur les lignes utilisées pour le contrôle de la configuration ou du périphérique ?

   _____

   _____

8. Quelles commandes permettent d'obtenir les statistiques sur le trafic des interfaces du routeur ?

   _____

   _____

9. Quelles commandes permettent d'obtenir des informations sur les chemins d'accès disponibles pour le trafic réseau ?

   _____

   _____

10. Quelles interfaces sont actuellement actives sur le routeur ?

    _____

    _____

Suggestion de barème de notation

Chaque question vaut 10 points pour un score total de 100.

Packet Tracer – Résolution des problèmes de connectivité

Topologie

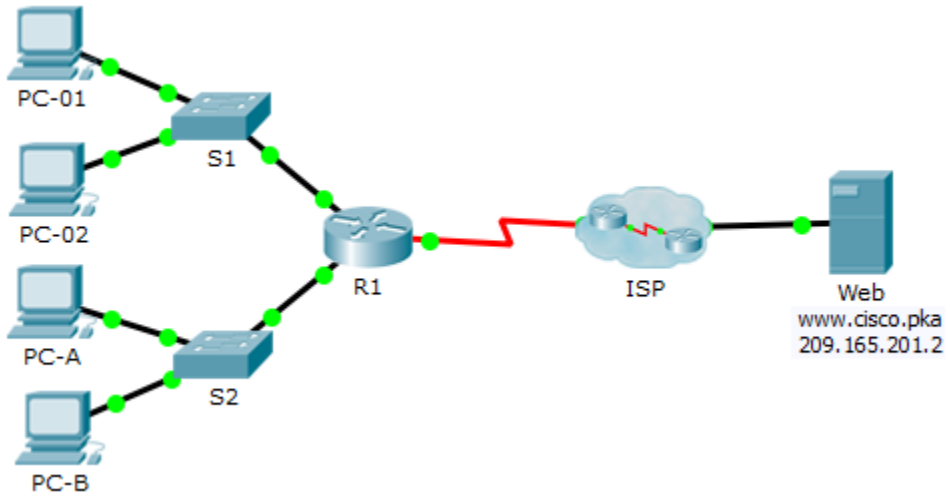


Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0	172.16.1.1	255.255.255.0	N/A
	G0/1	172.16.2.1	255.255.255.0	N/A
	S0/0/0	209.165.200.226	255.255.255.252	N/A
R2	G0/0	209.165.201.1	255.255.255.224	N/A
	S0/0/0 (ETCD)	209.165.200.225	255.255.255.252	N/A
PC-01	Carte réseau	172.16.1.3	255.255.255.0	172.16.1.1
PC-02	Carte réseau	172.16.1.4	255.255.255.0	172.16.1.1
PC-A	Carte réseau	172.16.2.3	255.255.255.0	172.16.2.1
PC-B	Carte réseau	172.16.2.4	255.255.255.0	172.16.2.1
Web	Carte réseau	209.165.201.2	255.255.255.224	209.165.201.1
DNS1	Carte réseau	209.165.201.3	255.255.255.224	209.165.201.1
DNS2	Carte réseau	209.165.201.4	255.255.255.224	209.165.201.1

Objectifs

L'objectif de cet exercice Packet Tracer est de résoudre les problèmes de connectivité, si possible. Sinon, les problèmes doivent être soigneusement notés et signalés.

Contexte/scénario

Les utilisateurs signalent qu'il leur est impossible d'accéder au serveur Web www.cisco.pka après une mise à niveau récente au cours de laquelle un second serveur DNS a été ajouté. Vous devez en déterminer la cause et tenter de résoudre les problèmes des utilisateurs. Décrivez clairement les problèmes et les solutions éventuelles. Vous n'avez accès ni aux périphériques dans le cloud, ni au serveur www.cisco.pka. Faites remonter le problème si nécessaire.

Le routeur R1 est accessible uniquement via SSH avec le nom d'utilisateur **Admin01** et le mot de passe **cisco12345**.

Etapa 1: Identifiez le problème de connectivité entre PC-01 et le serveur Web.

a. Ouvrez l'invite de commande sur PC-01. Saisissez la commande **ipconfig** pour vérifier l'adresse IP et la passerelle par défaut qui ont été attribuées à PC-01. Apportez les corrections nécessaires.

b. Après avoir corrigé les problèmes d'adressage IP sur PC-01, envoyez des requêtes ping à la passerelle par défaut, au serveur Web et à d'autres ordinateurs. Les requêtes ping ont-elles abouti ? Prenez note des résultats.

Requête ping vers la passerelle par défaut (172.16.1.1) ____ Vers le serveur Web (209.165.201.2) ____

Requête ping vers PC-02 _____ Vers PC-A _____ Vers PC-B _____

c. Utilisez le navigateur Web pour accéder au serveur Web sur PC-01. Saisissez l'URL www.cisco.pka et utilisez ensuite l'adresse IP 209.165.201.2. Prenez note des résultats.

PC-01 peut-il accéder à www.cisco.pka ? _____ À l'aide de l'adresse IP du serveur Web ? _____

d. Décrivez les problèmes et proposez une ou plusieurs solutions. Corrigez les problèmes, si possible.

_____

_____

Etapa 2: Identifiez le problème de connectivité entre PC-02 et le serveur Web.

a. Ouvrez l'invite de commande sur PC-02. Entrez la commande **ipconfig** pour vérifier la configuration de l'adresse IP et de la passerelle par défaut. Apportez les corrections nécessaires.

b. Après avoir corrigé les problèmes d'adressage IP sur PC-02, envoyez des requêtes ping à la passerelle par défaut, au serveur Web et à d'autres ordinateurs. Les requêtes ping ont-elles abouti ? Prenez note des résultats.

Requête ping vers la passerelle par défaut (172.16.1.1) ____ Vers le serveur Web (209.165.201.2) ____

Requête ping vers PC-01 _____ Vers PC-A _____Vers PC-B _____

c. Accédez à www.cisco.pka à l'aide du navigateur Web installé sur PC-02. Prenez note des résultats.

PC-01 peut-il accéder à www.cisco.pka ? _____ À l'aide de l'adresse IP du serveur Web ? _____

d. Décrivez les problèmes et proposez une ou plusieurs solutions. Corrigez les problèmes, si possible.

_____

_____

Etapa 3: Identifiez le problème de connectivité entre PC-A et le serveur Web.

a. Ouvrez l'invite de commande sur PC-A. Entrez la commande **ipconfig** pour vérifier la configuration de l'adresse IP et de la passerelle par défaut. Apportez les corrections nécessaires.

b. Après avoir corrigé les problèmes d'adressage IP sur PC-A, envoyez des requêtes ping à la passerelle par défaut, au serveur Web et à d'autres ordinateurs. Les requêtes ping ont-elles abouti ? Prenez note des résultats.

Requête ping vers la passerelle par défaut (172.16.2.1) ____Vers le serveur Web (209.165.201.2) ____

Requête ping vers PC-B _____ Vers PC-01 _____ Vers PC-02 _____

c. Accédez à www.cisco.pka.net à l'aide du navigateur Web installé sur PC-A. Prenez note des résultats.

PC-A peut-il accéder à www.cisco.pka ? _____ À l'aide de l'adresse IP du serveur Web ? _____

d. Décrivez les problèmes et proposez une ou plusieurs solutions. Corrigez les problèmes, si possible.

_____

_____

Etapa 4: Identifiez le problème de connectivité entre PC-B et le serveur Web.

a. Ouvrez l'invite de commande sur PC-B. Entrez la commande **ipconfig** pour vérifier la configuration de l'adresse IP et de la passerelle par défaut. Apportez les corrections nécessaires.

b. Après avoir corrigé les problèmes d'adressage IP sur PC-B, envoyez des requêtes ping à la passerelle par défaut, au serveur Web et à d'autres ordinateurs. Les requêtes ping ont-elles abouti ? Prenez note des résultats.

Requête ping vers la passerelle par défaut (172.16.2.1) ____ Vers le serveur Web (209.165.201.2) ____

Requête ping vers PC-A _____ Vers PC-01 _____ Vers PC-02 _____

c. Accédez à www.cisco.pka à l'aide du navigateur Web. Prenez note des résultats.

PC-B peut-il accéder à www.cisco.pka ? _____ À l'aide de l'adresse IP du serveur Web ? _____

d. Décrivez les problèmes et proposez une ou plusieurs solutions. Corrigez les problèmes, si possible.

_____

_____

Etapa 5: Vérifiez la connectivité.

Vérifiez que tous les ordinateurs peuvent accéder au serveur wWeb www.cisco.pka.

Votre pourcentage de réalisation devrait être égal à 100%. Si ce n'est pas le cas, cliquez sur **Check Results** (vérifier les résultats) pour voir quels composants requis ne sont pas encore terminés.

Suggestion de barème de notation

Section d'exercice	Nombre maximum de points	Points obtenus
Étape 1d	**5**	
Étape 2d	**5**	
Étape 3d	**5**	
Étape 4d	**5**	
Packet Tracer	**15**	
Score total	**35**	

Packet Tracer - Exercice d'intégration des compétences

Topologie

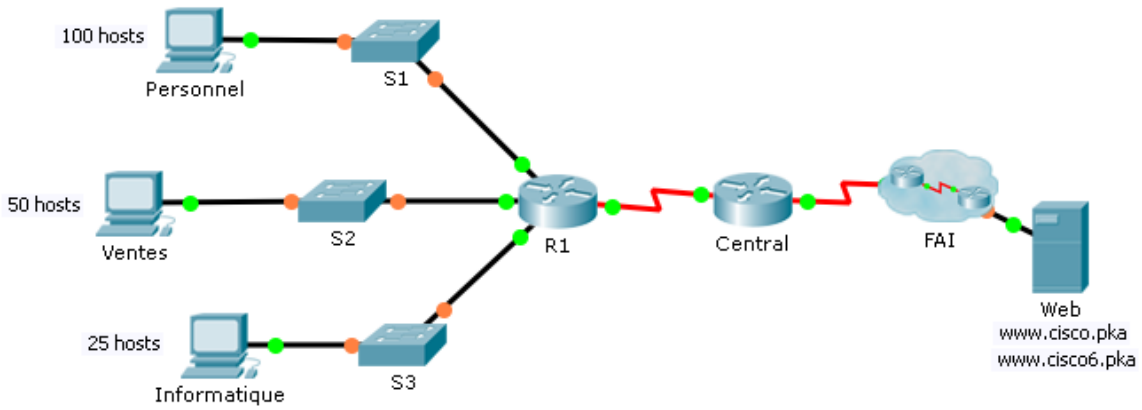


Table d'adressage

Appareil	Interface	Adresse IPv4	Masque de sous-réseau	Passerelle par défaut
		Adresse/Préfixe IPv6	Adresse IPv6 link-local	
R1	G0/0			N/A
		2001:DB8:ACAD::1/64	FE80::1	N/A
	G0/1			N/A
		2001:DB8:ACAD:1::1/64	FE80::1	N/A
	G0/2			N/A
		2001:DB8:ACAD:2::1/64	FE80::1	N/A
	S0/0/1	172.16.1.2	255.255.255.252	N/A
		2001:DB8:2::1/64	FE80::1	N/A
Central	S0/0/0	209.165.200.226	255.255.255.252	N/A
		2001:DB8:1::1/64	FE80::2	N/A
	S0/0/1	172.16.1.1	255.255.255.252	N/A
		2001:DB8:2::2/64	FE80::2	N/A
S1	VLAN 1			
S2	VLAN 1			
S3	VLAN 1			
Personnel	Carte réseau			
		2001:DB8:ACAD::2/64	FE80::2	FE80::1
Ventes	Carte réseau			
		2001:DB8:ACAD:1::2/64	FE80::2	FE80::1
IT	Carte réseau			
		2001:DB8:ACAD:2::2/64	FE80::2	FE80::1
Web	Carte réseau	64.100.0.3	255.255.255.248	64.100.0.1
		2001:DB8:CAFE::3/64	FE80::2	FE80::1

Contexte/scénario

Le routeur Central, le cluster ISP et le serveur web sont complètement configurés. Il vous a été demandé de créer un nouveau schéma d'adressage IPv4 comprenant 4 sous-réseaux au moyen du réseau 192.168.0.0/24. Le département IT a besoin de 25 hôtes. Le département des ventes a besoin de 50 hôtes. Le sous-réseau du reste de l'équipe a besoin de 100 hôtes. Un sous-réseau invité de 25 hôtes sera ajouté ultérieurement. Il vous a également été demandé de finaliser les paramètres de sécurité de base ainsi que les configurations des interfaces sur R1. Vous devrez aussi configurer l'interface SVI et la sécurité de base sur les commutateurs S1, S2 et S3.

Conditions requises

Adressage IPv4

- Créez des sous-réseaux qui satisfont les besoins des hôtes en utilisant l'adresse 192.168.0.0/24.
  - Staff : 100 hôtes
  - Ventes : 50 hôtes
  - IT : 25 hôtes
  - Réseau invité à ajouter ultérieurement : 25 hôtes
- Documentez les adresses IPv4 attribuées dans la table d'adressage.
- Enregistrez le sous-réseau du réseau invité : _____

Configurations des PC

- Configurez l'adresse IPv4 attribuée, le masque de sous-réseau et la passerelle par défaut des PC Personnel, Ventes et IT, conformément à votre schéma d'adressage.
- Attribuez les adresses IPv6 de monodiffusion et link-local ainsi que la passerelle par défaut des réseaux Personnel, Ventes et IT, conformément à la table d'adressage.

Configurations de R1

- Configurez le nom du périphérique conformément à la table d'adressage.
- Désactivez la recherche DNS.
- Attribuez **Ciscoenpa55** comme mot de passe chiffré du mode d'exécution privilégié.
- Attribuez **Ciscoconpa55** comme mot de passe de console et activez la connexion.
- 10 caractères minimum doivent être utilisés pour tous les mots de passe.
- Chiffrez tous les mots de passe en clair.
- Créez une bannière qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit. Veillez à inclure le terme **Warning** (Avertissement) dans la bannière.
- Configurez toutes les interfaces Gigabit Ethernet.
  - Configurez les adresses IPv4 conformément à votre schéma d'adressage.
  - Configurez les adresses IPv6 conformément à la table d'adressage.
- Configurez le protocole SSH sur R1 :
  - Choisissez le nom de domaine **CCNA-lab.com.**
  - Générez une clé RSA de **1024** bits.
  - Configurez les lignes VTY pour l'accès SSH.
  - Utilisez les profils utilisateur locaux pour l'authentification.
  - Créez un utilisateur **Admin1** avec un niveau de privilèges défini à **15** à l'aide du mot de passe chiffré pour **Admin1pa55**.
- Configurez la console et les lignes VTY de telle sorte qu'elles se déconnectent après cinq minutes d'inactivité.
- Bloquez pendant trois minutes quiconque n'arrive pas à se connecter au bout de quatre tentatives en deux minutes.

Configurations des commutateurs

- Configurez le nom du périphérique conformément à la table d'adressage.
- Configurez l'interface SVI avec l'adresse IPv4 et le masque de sous-réseau définis dans votre schéma d'adressage.
- Configurez la passerelle par défaut.
- Désactivez la recherche DNS.
- Attribuez **Ciscoenpa55** comme mot de passe chiffré du mode d'exécution privilégié.
- Attribuez **Ciscoconpa55** comme mot de passe de console et activez la connexion.
- Configurez la console et les lignes VTY de telle sorte qu'elles se déconnectent après cinq minutes d'inactivité.
- Chiffrez tous les mots de passe en clair.

Vérification de la connectivité

- Accédez à **www.cisco.pka** à l'aide du navigateur web à partir des PC Personnel, Ventes et IT.
- Accédez à **www.cisco6.pka** à l'aide du navigateur web à partir des PC Personnel, Ventes et IT.
- Tous les PC sont censés pouvoir envoyer des requêtes ping vers tous les périphériques.