Cisco | Networking Academy®
Mind Wide Open™

CCNA Exploration 4.0

Notions de base sur les réseaux

Manuel de travaux pratiques du participant

Exercice 1.1.1 : utilisation de Google Earth™ pour découvrir le monde

Objectifs pédagogiques

À la fin de cet exercice, vous saurez :

- expliquer la fonction de Google Earth ;
- présenter les différentes versions de Google Earth ;
- expliquer les configuration matérielle et logicielle requises pour utiliser Google Earth (édition gratuite) ;
- utiliser les fonctions de Google Earth, telles que Aide | Tutoriel ;
- utiliser Google Earth pour explorer les continents, les pays et les lieux d'intérêt.

Contexte

Google Earth est une application populaire exécutable dans la plupart des systèmes d'exploitation. Il nécessite une connexion haut-débit à Internet et affiche la terre sous forme d'image 2D ou 3D manipulée. La chaîne d'informations mondiale CNN utilise régulièrement Google Earth pour situer les théâtres d'événements.

Au moment de la rédaction de cet exercice, il existe trois versions de Google Earth. La version gratuite de Google Earth répond à la plupart des besoins. La version Google Earth Plus propose une prise en charge GPS, un importateur de feuilles de calcul et d'autres fonctions de support La version Google Earth Pro se destine à une utilisation professionnelle et commerciale. L'URL http://earth.google.com/product_comparison.html contient une description des versions. Utilisez ce lien pour répondre aux questions suivantes :

Quelles versions prennent en charge l'inclinaison et la rotation 3D ? _____

Quelle version de Google Earth propose la plus haute résolution ? _____

Pour utiliser Google Earth version 4, la configuration matérielle minimale requise est la suivante :

Système d'exploitation	Microsoft Windows 2000 ou Windows XP
Processeur	Pentium 3 à 500 MHz
Mémoire vive (RAM)	128 Mo
Disque dur	400 Mo d'espace libre
Débit réseau	128 kbits/s
Carte graphique	3D avec 16 Mo de mémoire VRAM
Écran	1024x768 pixels, couleur 16 bits

Scénario

Cet exercice doit être effectué sur un ordinateur possédant une connexion Internet et sur lequel vous pouvez installer le logiciel.

L'exercice prend environ 30 minutes, selon le débit réseau.

Tâche 1 : installation de Google Earth

Si Google Earth n'est pas installé sur l'ordinateur, vous pouvez télécharger la version gratuite à partir de l'URL suivante : http://earth.google.com/download-earth.html. Suivez les instructions d'installation. Google Earth démarre automatiquement. N'oubliez pas de désactiver les bloqueurs de fenêtres publicitaires intempestives de votre navigateur.

Figure 1. Écran d'accueil de Google Earth

Tâche 2 : exécution de Google Earth

Étape 1 : reportez-vous à l'écran d'accueil (figure 1). La barre de menus se trouve dans le coin supérieur gauche de l'écran. Dans le menu **Aide**, sélectionnez **Guide de l'utilisateur** pour lancer un navigateur Web par défaut et afficher le Guide de l'utilisateur de Google Earth. http://earth.google.com/userguide/v4/. Prenez quelques minutes pour parcourir le Guide de l'utilisateur. Avant de quitter le site Web du Guide de l'utilisateur, répondez aux questions suivantes :

Donnez les trois techniques de déplacement de l'image.

_____

_____

_____

Quelle commande de la souris permet d'effectuer un zoom avant ou un zoom arrière ?

_____

Quelle est la fonction du bouton gauche de la souris ?

_____

Tâche 3 : navigation dans l'interface Google Earth.

Étape 1 : utilisation de la fonction Planisphère.

Dans le menu **Affichage**, sélectionnez **Planisphère**. Cette fonction pratique fournit une position globale relative de l'image agrandie.

Étape 2 : présentation des contrôles de navigation.

Les contrôles de navigation se trouvent dans le quart supérieur droit. Ils permettent de contrôler l'agrandissement et la position de l'image. Le pointeur de la souris doit être déplacé à proximité des contrôles, auquel cas seule une boussole s'affichera. Pour obtenir la description des contrôles de navigation, reportez-vous à la figure 2.

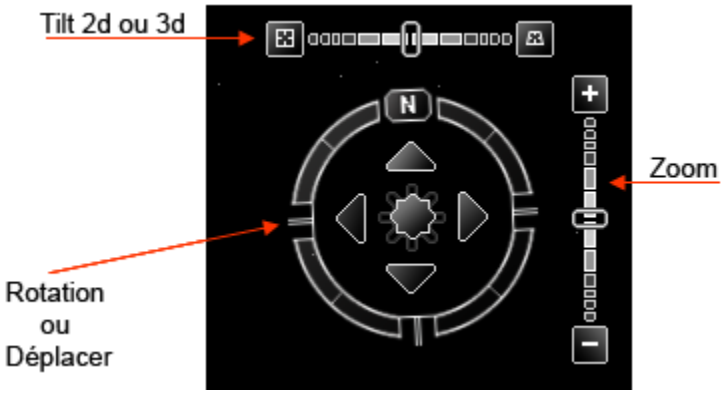


Figure 2. Outils de navigation à l'écran de Google Earth

Étape 3 : utilisation de la fonction Visite touristique.

Dans la barre de navigation de gauche, accédez au dossier **Mes lieux préférés > Visite touristique**. Développez le dossier Visite touristique, sélectionnez le lieu que vous souhaitez voir, puis double-cliquez sur cet emplacement. L'image vous dirige vers ce lieu. Une fois le lieu atteint, un indicateur vous informe de la fin de la résolution de l'image.

Étape 4 : utilisation du dossier Rechercher > Aller à.

Entrez le code postal américain 95134.

Quel état et quelle ville s'affichent ? _____

Vous préférez aller à Londres ? Quelles données devez vous saisir ?

_____

_____

Étape 5 : utilisation de la fonction Aller à.

Certains lieux possèdent de meilleures résolutions. En outre, des images de lieux peuvent être anciennes. Par exemple, un utilisateur peut trouver sa maison, mais pas la maison voisine car elle n'a pas encore été construite. Recherchez votre maison à l'aide du dossier **Rechercher > Aller à**.

La résolution de votre maison est-elle de même qualité que celle du lieu sélectionné dans Visite touristique de l'étape 3 ? _____

Si la résolution de votre voisinage est suffisante, naviguez dans la zone environnante pour déterminer l'ancienneté de l'image.

Figure 3. Planisphère avec lignes de latitude et de longitude

Étape 6 : affichage des coordonnées géographiques.

Les coordonnées géographiques s'affichent dans le quart inférieur gauche de l'image. Le premier nombre est la latitude. Il s'agit de l'angle entre un point et l'équateur. L'équateur est une ligne imaginaire qui divise le globe en deux hémisphères : l'hémisphère nord et l'hémisphère sud. La latitude de l'équateur est 0°. Le deuxième nombre est la longitude. Il s'agit de l'angle à l'est ou à l'ouest d'un point terrestre arbitraire. Le Royal Observatory (Royaume-uni) est le point international de longitude zéro. La combinaison de la longitude et de la latitude se nomme un graticule. Les mesures des coordonnées se font en degrés°, minutes, secondes et dixièmes de seconde. En ce qui concerne la latitude, la référence est le Nord (N) ou le Sud (S) de l'équateur. Pour la longitude, la référence est l'Est (E) ou l'Ouest (W) du Royal Observatory. Reportez-vous à la figure 3. Pour obtenir une définition simple des coordonnées géographiques, accédez à l'URL http://en.wikipedia.org/wiki/Geographic_coordinate_system. Dans le menu **Affichage**, sélectionnez **Grille** pour afficher les lignes de grille de Google Earth.

À l'aide du pointeur et des coordonnées disponibles dans le quart inférieur gauche de l'image, quelles sont les coordonnées de votre maison ? _____

Tâche 4 : Remarques générales

Google Earth amène le monde entier à votre domicile ou à votre bureau. Tout en profitant des images, imaginez les ressources de communication numérique qui ont été utilisées. Par exemple, une communication satellite avec une station terrestre a transmis l'image de votre maison. Un type de base de données a été utilisé pour stocker l'image. Un réseau local (LAN) a envoyé votre demande d'image via Internet et plusieurs réseaux étendus (WAN), puis vers un autre réseau local avec un ordinateur qui vous a retourné l'image. Le délai de récupération de l'image peut être court ou long, en fonction de la plus basse vitesse de toutes les connexions réseau du chemin entre le référentiel de base de données et votre ordinateur.

L'image aurait-elle pu s'afficher plus rapidement si des techniques de compression de données étaient utilisées ?

Tenez compte de la sécurité du réseau. Quelqu'un pourrait-il espionner votre connexion réseau ?

Tâche 5 : confirmation

Google Earth affiche les coordonnées géographiques dans le quart inférieur gauche de l'image. Utilisez l'URL suivante pour en savoir plus sur les différents systèmes de coordonnées : http://www.colorado.edu/geography/gcraft/notes/coordsys/coordsys.html. Wikipedia propose une définition pratique des termes géographiques courants.

Utilisez le système de coordonnées géographiques pour décrire votre maison avec un maximum de précision et de détail.

Tâche 6 : nettoyage

Il peut vous être demandé de supprimer Google Earth de l'ordinateur. Dans ce cas, procédez comme suit :

1. Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration**.
2. Double-cliquez sur **Ajout/Suppression de programmes**.
3. Sélectionnez **Google Earth**.
4. Cliquez sur **Supprimer** et suivez les instructions.

D'autres informations relatives à la suppression sont disponibles à l'URL suivante : http://earth.google.com/support/bin/answer.py?answer=20738&ctx=sibling.

Sauf indication contraire, éteignez votre ordinateur.

Exercice 1.4.5 : identification des principaux points faibles en matière de sécurité

Objectifs pédagogiques

À la fin de cet exercice, vous saurez :

- utiliser le site SANS pour identifier rapidement les menaces de sécurités présentes sur Internet ;
- expliquer la façon dont s'organisent les menaces ;
- répertorier plusieurs failles de sécurité récentes ;
- utiliser les liens SANS pour accéder à d'autres informations de sécurité.

Contexte

Le site SANS est l'un des sites les plus populaires et efficaces en matière de défense contre les menaces de sécurité informatiques et réseau. SANS fait référence à SysAdmin, Audit, Network, Security (Administration système, audit, réseau, sécurité). SANS contient plusieurs composants, chacun contribuant de façon significative à la sécurité des informations. Pour plus d'informations sur le site SANS, accédez à l'URL http://www.sans.org/, puis sélectionnez des éléments dans le menu Resources.

Comment un administrateur de sécurité d'entreprise peut-il identifier rapidement les menaces de sécurité ? SANS et le FBI ont compilé la liste des 20 principales cibles d'attaque de sécurité Internet à l'URL http://www.sans.org/top20/. La liste est régulièrement mise à jour avec des informations formatées par :

- des systèmes d'exploitation : Windows; Unix/Linux, MAC ;
- des applications : plate-forme croisée, y compris Web, base de données, peer-to-peer, messagerie instantanée, lecteurs média, serveurs DNS, logiciel de sauvegarde et serveurs de gestion ;
- des périphériques réseau : périphériques d'infrastructure réseau (routeurs, commutateurs, etc.), périphériques VoIP ;
- des éléments humains : règles de sécurité, comportement humain, problèmes personnels ;
- une section spéciale : problèmes de sécurité étrangers aux catégories ci-dessus.

Scénario

Ces travaux pratiques vont permettre aux participants d'aborder les failles de sécurité informatiques. Le site Web SANS sera utilisé comme outil d'identification, de compréhension et de défense contre les menaces.

Ces travaux pratiques doivent être réalisés en dehors des travaux pratiques de Cisco, à partir d'un ordinateur doté d'un accès à Internet.

Cette session de travaux pratiques prend environ une heure.

Tâche 1 : localisation des ressources SANS.

Étape 1 : ouverture de SANS Top 20 List.

À partir d'un navigateur Web, accédez à l'URL http://www.sans.org. Dans le menu **resources**, sélectionnez **top 20 list**, comme illustré dans la figure 1.

Figure 1. Menu SANS

La liste SANS Top-20 Internet Security Attack Targets est organisée par catégorie. Une lettre d'identification indique le type de catégorie. Les nombres permettent d'effectuer la distinction entre les différentes rubriques d'une même catégorie. Les rubriques Router et Switch appartiennent à la même catégorie : Network Devices (**N**). Il existe deux rubriques principales :

N1. VoIP Servers and Phones
N2. Network and Other Devices Common Configuration Weaknesses

Étape 2 : Cliquez sur N2. Network and Other Devices Common Configuration Weaknesses pour accéder à cette rubrique.

Tâche 2 : examen des ressources SANS.

Étape 1 : examen du contenu de N2.2 Common Default Configuration Issues.

Par exemple, N.2.2.2 (en janvier 2007) contient des informations sur les menaces associées aux comptes et aux valeurs par défaut. Une recherche dans Google sur « wireless router passwords »" retourne des liens vers plusieurs sites qui publient une liste de mots de passe et de noms de compte administrateur de routeurs sans fil. En cas d'échec de modification de ces mots de passe, les périphériques peuvent être exposés aux attaques.

Étape 2 : note des références CVE.

La dernière ligne située sous les rubriques fait référence à l'exposition aux failles standard (CVE). Ce nom est lié à la National Vulnerability Database (NVD) du National Institute of Standards and Technology (NIST), sponsorisé par le Department of Homeland Security (DSH) National Cyber Security Division et l'US-CERT, qui contient des informations sur les failles.

Tâche 3 : collecte des données.

Le reste des travaux pratiques est consacré à un exercice de recherche et de résolution de failles.

Étape 1 : choix d'un domaine à examiner, puis clic sur un exemple de lien hypertexte CVE.

Remarque : en raison de la constante évolution de la liste CVE, la liste actuelle peut ne pas contenir les mêmes failles que celles observées en janvier 2007.

Le lien doit ouvrir un nouveau navigateur Web connecté à http://nvd.nist.gov/ et à la page de résumé des failles de la liste CVE.

Étape 2 : renseignement des informations sur la faille :

Date de version d'origine : _____

Dernière révision : _____

Source : _____

Présentation générale :

_____

_____

_____

_____

_____

Plusieurs valeurs sont disponibles sous la zone Impact. La sévérité Common Vulnerability Scoring System (CVSS) s'affiche et contient une valeur entre 1 et 10.

Étape 3 : renseignement des informations sur l'impact de la vulnérabilité :

Sévérité CVSS : _____

Plage : _____

Authentification : _____

Type d'impact : _____

L'en-tête suivant contient des liens avec des informations sur la faille et les solutions éventuelles s'y rapportant.

Étape 4 : rédaction d'une brève description de la solution trouvée sur ces pages à l'aide des liens hypertexte.

_____

_____

_____

_____

_____

_____

_____

_____

Tâche 4 : Remarques générales

Le nombre de failles sur les ordinateurs, réseaux et données continue d'augmenter. Les gouvernements ont consacré d'importantes ressources à la coordination et à la distribution des informations sur les failles et les solutions éventuelles. Il revient à l'utilisateur final d'implémenter la solution. Pensez à des solutions qui permettraient aux utilisateurs de renforcer la sécurité. Pensez aux habitudes des utilisateurs qui génèrent des risques de sécurité.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Tâche 5 : confirmation

Essayez de trouver une entreprise qui souhaite nous rencontrer pour expliquer comment les failles sont détectées et éliminées. Trouver une entreprise désireuse de le faire peut être difficile pour des raisons de sécurité, mais peut profiter aux participants, qui comprendront comment les failles sont éliminées dans le monde entier. Cela permettra également aux représentants de l'entreprise de rencontrer la classe et de mener des entretiens internes informels.

Travaux pratiques 1.6.1 : utilisation des outils collaboratifs : conversation IRC et messagerie instantanée

Schéma de la topologie

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- définir ce que sont des services de messagerie instantanée et IRC (Internet Relay Chat) ;
- décrire diverses façons d'utiliser la messagerie instantanée dans le cadre d'une collaboration ;
- décrire plusieurs mauvaises utilisations et problèmes de sécurité liés à la messagerie instantanée ;
- collaborer à l'aide d'un outil IRC.

Contexte

La messagerie électronique permet à de multiples utilisateurs de collaborer, partager des idées et transférer des fichiers. Toutefois, à moins que l'utilisateur ne surveille constamment son compte de messagerie, certains courriels risquent de ne pas être lus avant un certain temps. Pour contacter un interlocuteur sans attendre, le téléphone était l'option généralement choisie jusqu'ici. Malheureusement, il ne permet pas de transférer des fichiers. Les collaborateurs ont donc besoin d'un outil de communication aussi flexible que la messagerie électronique et aussi rapide que le téléphone. Les technologies IRC (Internet Relay Chat) et de messagerie instantanée répondent à ces besoins. Grâce à ces outils, les utilisateurs peuvent facilement échanger des idées et des fichiers sur Internet ou sur un réseau d'entreprise privé. Les messageries instantanées et les outils IRC permettent de communiquer en temps réel. Toutefois, leurs mises en œuvre diffèrent.

Une communication par messagerie instantanée est uniquement possible entre deux interlocuteurs « autorisés ». Pour pouvoir démarrer une session avec un interlocuteur, l'utilisateur doit d'abord lui envoyer une « invitation ». Le destinataire identifie alors l'expéditeur à l'aide de son nom d'affichage et, s'il accepte l'invitation, la session peut démarrer. Les clients de messagerie instantanée permettent de disposer d'une liste de contacts approuvés. Vous pouvez ouvrir des fenêtres de messagerie instantanée supplémentaires pour communiquer avec plusieurs personnes à la fois. Chaque fenêtre représente une communication avec une personne.

La technologie IRC, quant à elle, permet à plusieurs personnes d'interagir. Les interlocuteurs bénéficient en outre d'un certain degré d'anonymat. Pour participer à une discussion, vous devez vous connecter à un serveur de discussion et rejoindre une discussion sur un sujet spécifique. Vous rejoignez ainsi une salle de discussion. Vous devez généralement créer votre propre identité lorsque vous rejoignez la salle de discussion, mais vous êtes libre de fournir la quantité d'informations que vous souhaitez vous concernant.

Bien que la discussion qui suit concerne principalement la messagerie instantanée, vous pourrez constater à quel point il est facile d'utiliser la technologie IRC au cours de brefs travaux pratiques où le « nuage Internet » sera utilisé.

Pour que les utilisateurs puissent communiquer par messagerie instantanée, un équipement fournissant ce type de services est nécessaire. Il s'agit d'un *serveur de messagerie instantanée*. Les utilisateurs doivent également disposer d'un périphérique final tel qu'un ordinateur sur lequel un logiciel appelé *Client de messagerie instantanée* est installé. Cette disposition correspond à une relation client/serveur. Les clients de messagerie instantanée se connectent au serveur de messagerie instantanée, qui relie les clients entre eux. L'ensemble constitue le réseau de messagerie instantanée. Il existe de nombreux réseaux de messagerie instantanée disposant chacun d'un groupe d'utilisateurs dédiés. Les plus courants sont les suivants : America On Line (AOL) Instant Messenger (AIM), Windows Live Messenger (MSN), Yahoo!, Messenger et ICQ (I Seek You). La figure 1 présente un client de messagerie instantanée AIM connecté au réseau AIM.

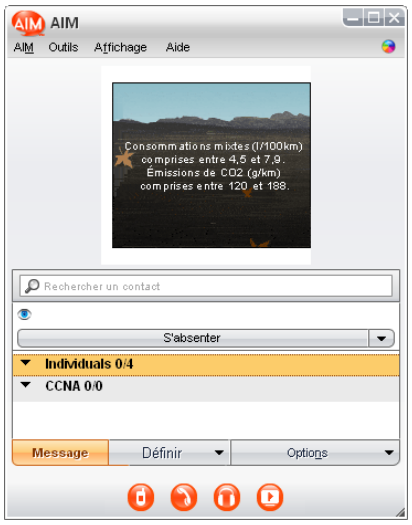


Figure 1. Client AIM

Caractéristiques

Les services de messagerie instantanée ont plusieurs caractéristiques en commun :

- Lorsque la communication est établie entre un client de messagerie instantanée et le réseau de messagerie instantanée, vous pouvez distinguer les personnes connectées dans la liste des contacts.
- Il est possible de partager des fichiers entre clients de messagerie instantanée.
- Les clients permettent également d'envoyer et de consigner des messages textuels.
- Certains réseaux de messagerie instantanée proposent des services audio.
- De nouveaux services ont également vu le jour sur certains réseaux de messagerie instantanée, dont la vidéoconférence, la voix sur IP (VoIP), la cyberconférence, le partage de bureaux et même la radio et la télévision sur IP.

Protocoles

Une méthode de communication approuvée appelée protocole est utilisée sur chaque réseau de messagerie instantanée. Il s'agit de protocoles propriétaires pour la plupart des réseaux. Le protocole propriétaire OSCAR (Open System for Communication in Realtime) est utilisé sur les réseaux AIM et ICQ (acquis par AOL). Microsoft et Yahoo! disposent également de protocoles propriétaires mais proposent des services en partenariat afin d'offrir une connectivité commune.

De nombreux protocoles sont présentés dans le cadre de ce cours. Le groupe de travail IETF (Internet Engineering Task Force) a essayé de standardiser les protocoles de messagerie instantanée, notamment à l'aide du protocole SIP (Session Initialization Protocol). Le protocole SIPv2 a été défini dans la RFC 2543, puis décrit comme obsolète dans la RFC 3261. Comme pour les protocoles propriétaires, il existe de nombreux protocoles de messagerie instantanée ouverts (Open Source).

Certaines applications de client de messagerie instantanée telles que Gaim et Trillian sont capables de faire la distinction entre les protocoles de messagerie instantanée. Certains serveurs de messagerie instantanée proposent également ce type de prise en charge. Le groupe IETF a mis au point un standard ouvert, Jabber, basé sur le protocole EMPP (Extensible Messaging and Presence Protocol). Les RFC 3290 et RFC 3291 y font référence. Les communications cryptées sont prises en charge.

Les problèmes liés aux mauvaises utilisations de la messagerie instantanée représentent un réel souci pour les parents, et de nombreux réseaux de messagerie instantanée encouragent le contrôle parental. Les parents peuvent ainsi restreindre l'accès des enfants en limitant les contacts et en les supervisant lorsqu'ils sont en ligne. AIM et Yahoo! Messenger fournissent des logiciels de supervision gratuits. Certains outils de contrôle parental permettent de se connecter en arrière-plan, de limiter la durée de connexion, de bloquer l'accès aux salles de discussion, d'interdire des utilisateurs et de désactiver des fonctions du client.

Securité

De multiples problèmes de sécurité ont été détectés concernant la messagerie instantanée, ce qui a conduit bon nombre de sociétés à limiter l'accès de ce type de messagerie au réseau d'entreprise voire de le bloquer entièrement. Les vers, virus et chevaux de Troie informatiques, logiciels malveillants, s'attaquent également aux ordinateurs sur lesquels des clients de messagerie instantanée sont installés. Sans mesures de sécurité efficaces, les informations échangées entre les utilisateurs peuvent être capturées et divulguées. Les applications de client et serveur de messagerie instantanée présentent des vulnérabilités, ce qui rend les ordinateurs vulnérables eux aussi. Les utilisateurs peuvent également encombrer le réseau s'ils transfèrent des fichiers volumineux par messagerie instantanée.

Comment un administrateur système peut-il protéger le réseau des vulnérabilités et des cas de mauvaise utilisation de la messagerie instantanée ? Le SANS (SysAdmin, Audit, Network, Security) Institute recommande plusieurs contre-mesures. La liste suivante est tirée du site Web SANS et est accessible à l'adresse suivante : `http://www.sans.org/top20/#c4`.

C4.4 Protection contre les vulnérabilités et les utilisations non autorisées de la messagerie instantanée

- Établir des règles d'utilisation raisonnable de la messagerie instantanée. S'assurer que tous les utilisateurs sont informés de ces règles et qu'ils comprennent clairement les risques potentiels.
- Ne pas autoriser les utilisateurs à installer des logiciels. Restreindre les droits d'administrateur et de superutilisateur au personnel du support chargé de les assister. Si un utilisateur spécifique doit disposer de droits d'administrateur ou de superutilisateur, créez un compte distinct pour ses tâches quotidiennes, ses consultations Internet et ses communications en ligne.
- Veillez à ce que les correctifs du fournisseur soient immédiatement appliqués au logiciel de messagerie instantanée, aux applications interconnectées et au système d'exploitation sous-jacent.

- Utilisez des logiciels antivirus et anti-espion.
- Ne faites pas appel à des serveurs de messagerie instantanée externes pour utiliser une messagerie instantanée en interne ; mettez un serveur interne ou un serveur proxy de qualité commerciale à disposition.
- Créez des voies de communication sécurisées lorsque vous utilisez une messagerie instantanée avec des partenaires de confiance.
- Configurez des systèmes de détection et de prévention contre les intrusions de façon appropriée. De nombreuses applications de messagerie instantanée peuvent être utilisées pour activer des communications liées passant pour du trafic légitime (par exemple, http).
- Pensez à déployer des produits spécialement conçus pour sécuriser les messageries instantanées.
- Filtrez l'intégralité du trafic http à l'aide d'un serveur proxy d'authentification afin de bénéficier de capacités de filtrage et de contrôle supplémentaires pour le trafic relatif à la messagerie instantanée.
- Bloquez l'accès aux serveurs de messagerie instantanée publics connus non autorisés de façon explicite. Remarque : notez que cette opération ne permet d'assurer qu'une protection partielle en raison du nombre de serveurs externes potentiels.
- Bloquez les ports de messagerie instantanée prisés. Remarque : notez que cette opération ne permet d'assurer qu'une protection partielle en raison du nombre de protocoles et ports associés potentiels et de la capacité des applications à passer outre les restrictions de port.
- Utilisez un système de détection/prévention contre les intrusions au cas où des utilisateurs créeraient des tunnels pour la messagerie instantanée ou passeraient outre les proxy.

Avenir de la messagerie instantanée

La messagerie instantanée est promise à un avenir certain permettant aux utilisateurs d'utiliser de nouvelles technologies pour collaborer. Par exemple, il est désormais possible d'avoir accès à des services de messagerie instantanée sur votre téléphone portable. La plupart des fabricants de téléphones portables disposent de leur propre système de messagerie instantanée mobile. Un autre fabricant de terminaux de poche est également prisé : Blackberry. Les terminaux Blackberry prennent en charge les fonctionnalités de messagerie instantanée courantes telles que les messages textuels, la redirection des courriels (« push email »), la téléphonie et la navigation sur le Web.

Scénario

Dans le schéma de la topologie, deux ordinateurs sont reliés à un « nuage ». En langage réseau, le nuage symbolise souvent un réseau plus complexe, par exemple Internet, qui ne constitue pas l'objet actuel de la discussion. Vous utiliserez deux ordinateurs dans le cadre de ces travaux pratiques. La première étape constituera à récupérer un logiciel de communication à partir du nuage. Une fois le logiciel installé, vous devrez toujours utiliser le nuage pour avoir accès aux services de communication. Les chapitres suivants vous permettront d'examiner en détail les périphériques et les protocoles utilisés au sein du nuage. Le serveur *eagle-server* ainsi que d'autres périphériques réseau sont des éléments du nuage. Au cours de ces travaux pratiques, le serveur eagle-server sera utilisé comme serveur IRC et l'application Gaim comme client IRC. Vous pouvez toutefois choisir un autre client IRC que Gaim. Un client IRC à télécharger est disponible sur le serveur eagle-server à l'adresse suivante : http://eagle-server.example.com/pub.

Cette session de travaux pratiques prend environ 45 minutes.

Tâche 1 : configuration du client de discussion

Le protocole IRC est un standard ouvert défini à l'origine dans la RFC 1459. Il permet de communiquer à travers des liens de texte brut.

Étape 1 : vérification de la présence d'un client IRC sur l'ordinateur.

Si aucun client IRC n'est présent, téléchargez et installez le fichier exécutable Windows gaim-1.5.0.exe à partir de l'URL `ftp://eagle-server.example.com/pub/eagle labs/eagle1/chapter1`. Acceptez les paramètres par défaut au cours de l'installation. Vérifiez que le client de discussion Gaim est installé, puis suivez la procédure ci-dessous pour le configurer.

Étape 2 : ouverture de la fenêtre des comptes

1. Ouvrez l'application Gaim, puis sélectionnez l'icône **Accounts (Comptes)** dans la fenêtre de connexion. La fenêtre des comptes est présentée à la figure 2.

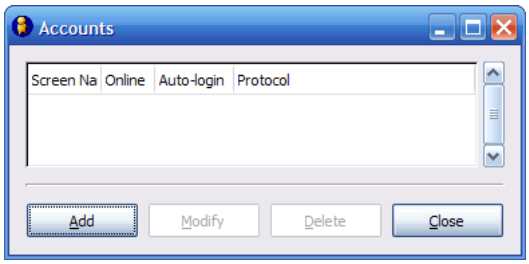


Figure 2. Fenêtre des comptes de l'application Gaim

2. Dans la fenêtre Accounts (Comptes), cliquez sur **Add (Ajouter).**.

Étape 2 : ajout d'un compte.

1. Reportez-vous à la figure 3. Dans la fenêtre Add Account (Ajout de compte), développez l'option `Show more options (Plus d'options)`. Renseignez les champs requis :

   Protocol (Protocole) : `IRC`
   Screen Name (Nom d'affichage) : `(ce qui permet aux autres de vous reconnaître)`
   Serveur : `eagle-server.example.com`
   Proxy Type (Type de proxy) : `No Proxy (Aucun)`

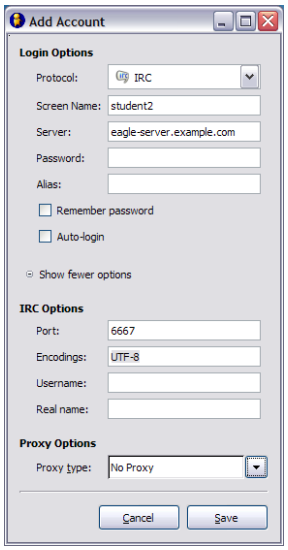


Figure 3. Fenêtre Add Account de l'application Gaim

2. Une fois terminé, cliquez sur **Save (Enregistrer)**.
3. Fermez la fenêtre des comptes.

Tâche 2 : connexion à un serveur de discussion

Étape 1 : ouverture de session.

Revenez à la fenêtre de connexion, où le nouveau compte de connexion au serveur eagle-server doit désormais apparaître. Cliquez sur **Sign-on (Ouvrir une session)**. Deux fenêtres s'ouvrent. La fenêtre d'état de la connexion IRC est présentée à la figure 4. La fenêtre principale du client Gaim permettant de discuter ou d'utiliser la messagerie instantanée est présentée à la figure 5.

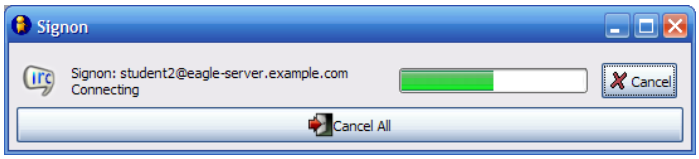


Figure 4. Fenêtre d'état de la connexion IRC

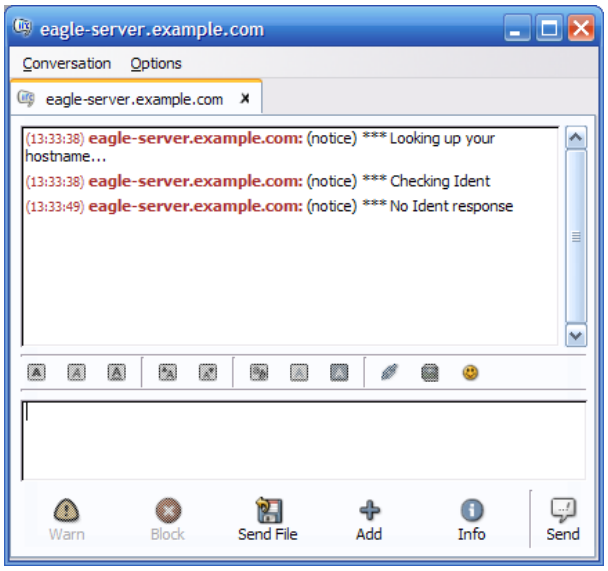


Figure 5. Fenêtre principale du client IRC Gaim

Étape 2 : procédure permettant de rejoindre une discussion.

Lorsque la connexion entre le client IRC et le serveur IRC est établie, la fenêtre d'état se ferme et une fenêtre Buddy List (Liste de contacts) s'affiche. Cliquez sur **Chat (Discuter)**, comme illustré à la figure 6.

Remarque : pour rejoindre une discussion, vous *devez* indiquer un nom commençant par # dans le champ Channel. Si cette consigne n'est pas respectée, vous vous retrouverez tout seul dans la salle de discussion (à moins que d'autres participants aient fait la même erreur).

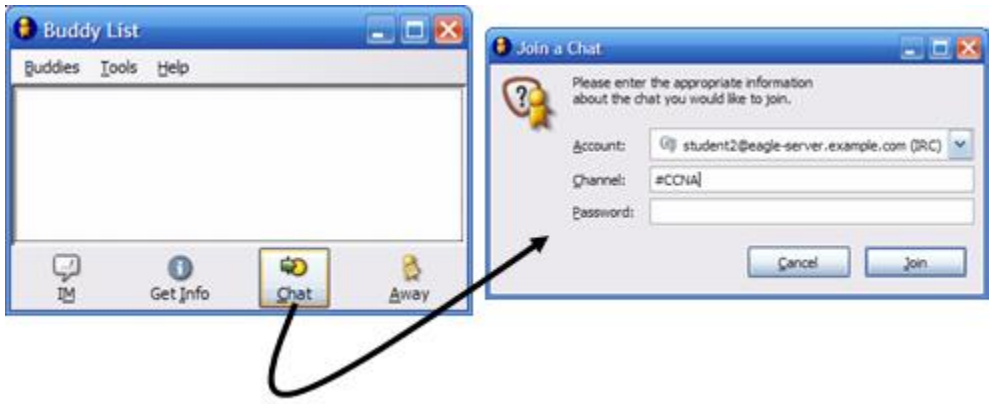


Figure 6. Procédure permettant de rejoindre une discussion

Tâche 3 : session de discussion

Une brève discussion entre les utilisateurs *Root* et *student2* est présentée à la figure 7. Plusieurs participants peuvent rejoindre la discussion et interagir entre eux.

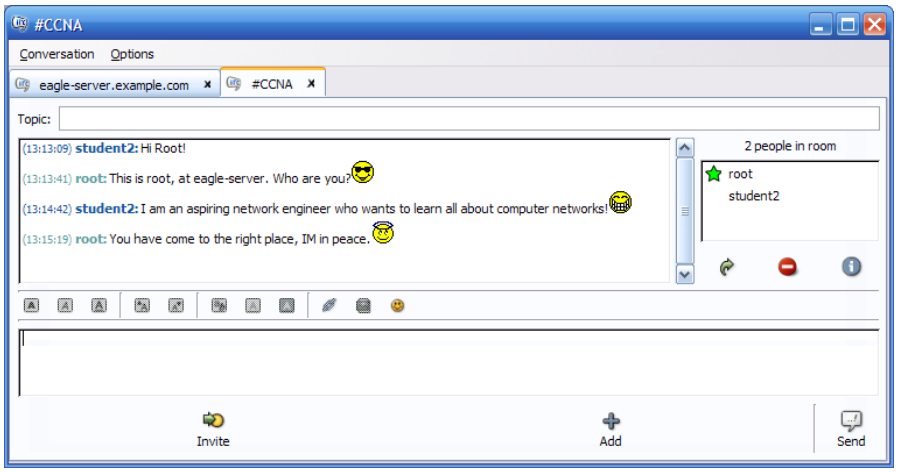


Figure 7. Participation à une discussion

Au cours de la discussion, réfléchissez à la façon dont vous, en tant que parent ou administrateur réseau, géreriez ce type de connexion.

Tâche 4 : Remarques générales

Si votre réseau est connecté à Internet, vous pouvez utiliser le client Gaim pour vous connecter à plusieurs fournisseurs de services de messagerie instantanée. Ce type de communication est très prisé chez les adolescents et les jeunes adultes, qui l'utilisent pour discuter avec leurs amis et partager des fichiers. Toutefois, il est possible qu'ils ne comprennent pas ce qu'une communication entre client et serveur implique. En tant que futur ingénieur réseau, il vous appartient de comprendre les problèmes sociaux et de sécurité liés à l'utilisation de la messagerie instantanée et de la technologie IRC.

Tâche 5 : confirmation

Transférez-vous des fichiers entre partenaires au cours d'une discussion. Depuis l'hôte, envoyez une commande ping continue vers le serveur eagle-server afin de surveiller le débit réseau. Examinez le temps de réponse avant et pendant le transfert des fichiers. Décrivez brièvement ce temps lorsque des fichiers sont transférés et lorsque aucun fichier n'est transféré.

_____

_____

_____

_____

_____

Tâche 6 : nettoyage

Demandez à votre formateur si vous pouvez procéder à la suppression de l'application Gaim et arrêter votre ordinateur.

Travaux pratiques 1.6.2 : utilisation des outils collaboratifs : wikis et blogs

Schéma de la topologie

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- définir les termes *wiki* et *blog* ;
- explorer les fonctionnalités des wiki.

Contexte

La topologie à respecter pour cette session de travaux pratiques doit être préconfigurée et prête à l'emploi. Si vous ne parvenez pas à vous connecter à Eagle Server depuis l'ordinateur, demandez de l'aide auprès du formateur.

Dans le schéma de la topologie, deux ordinateurs sont reliés à un « nuage ». En langage réseau, le nuage symbolise souvent un réseau plus complexe qui ne constitue pas l'objet actuel de la discussion. Au cours de ces travaux pratiques, vous utiliserez un ordinateur hôte relié au nuage afin de pouvoir accéder à un Twiki. Les chapitres suivants vous permettront d'examiner en détail les périphériques et les protocoles utilisés au sein du nuage.

Scénario

Ces travaux pratiques vous permettront de découvrir les différents composants d'un wiki. Si vous avez déjà utilisé *Wikipedia*, vous savez déjà à quoi ressemble un wiki. Après avoir utilisé *Wikipedia*, son contenu enrichi et ses liens flexibles, il est généralement frustrant et contraignant de revenir à des fichiers plats.

Vous serez amené à explorer le serveur wiki TWiki installé sur Eagle Server afin de vous familiariser avec les wiki.

Tâche 1 : définition des termes wiki et blog.

Wiki

En hawaïen, « Wiki » signifie *rapide*. Dans le langage réseau, un wiki est un outil de collaboration Web permettant à quasiment n'importe quelle personne de publier des informations, des fichiers ou des graphiques sur un site commun afin que d'autres utilisateurs puissent les lire et les modifier. Sa page d'accueil (première page qui s'affiche) comporte un outil de recherche grâce auquel les utilisateurs peuvent trouver les articles qui les intéressent. Vous pouvez installer un wiki afin qu'il soit disponible à l'ensemble de la communauté Internet, ou bien derrière un pare-feu d'entreprise afin qu'il soit uniquement accessible à ses employés. L'utilisateur est autorisé à lire le contenu du wiki, mais il peut également participer à la création du contenu au sein d'un navigateur Web.

Bien qu'il existe de nombreux serveurs wiki différents, les fonctionnalités suivantes sont standard :

- Vous pouvez modifier des pages ou créer du contenu dans n'importe quel navigateur Web.
- Des fonctions d'édition et de liens automatiques permettent de modifier les pages et de relier automatiquement plusieurs pages entre elles. Les fonctions de formatage de texte s'apparentent à celles disponibles sur les messageries électroniques.
- Un moteur de recherche permet de trouver rapidement du contenu.
- L'auteur du sujet peut définir des restrictions d'accès, notamment les personnes autorisées à modifier le contenu.
- Un wiki Web est un ensemble de pages auquel sont associés différents groupes de collaboration.

Pour plus d'informations sur le terme « Wiki », visitez les sites Web suivants en dehors de la formation :

http://www.wiki.org/wiki.cgi?WhatsWiki
http://www.wikispaces.com/

Blogs

Un blog est un journal sur le Web. Il s'apparente au wiki en ce sens qu'il permet de créer et publier du contenu accessible en lecture aux autres utilisateurs. Un blog est généralement créé par une personne, l'auteur du blog, qui contrôle son contenu. Certains blogs permettent aux lecteurs de laisser des commentaires et de donner leur avis à l'auteur ; d'autres sont plus restrictifs. Des services d'hébergement de blog Internet gratuits, tels que www.blogger.com, sont mis à disposition. Ils sont semblables aux comptes de messagerie ou sites Web disponibles gratuitement.

Tâche 2 : exploration de fonctionnalités de wiki courantes à l'aide du didacticiel Twiki Tutorial.

Le didacticiel TWiki Tutorial permet de découvrir les fonctionnalités les plus courantes des wiki. Vous trouverez ci-dessous les principaux sujets abordés dans ce didacticiel :

Didacticiel TWiki de 20 min
1. **Get set... (Préparation)**
2. **Take a quick tour... (Petite visite guidée)**
3. **Open a private account… (Ouverture d'un compte privé)**
4. **Check out TWiki users, groups. (Présentation des utilisateurs et des groupes TWiki)**
5. **Test the page controls... (Test des contrôles des pages)**
6. **Change a page, and create a new one... (Modification et création d'une page)**
7. **Use your browser to upload files as page attachments... (Téléchargement de fichiers sous forme de pièces jointes aux pages à l'aide d'un navigateur)**
8. **Get e-mail alerts whenever pages are changed... (Affichage d'alertes par messagerie électronique en cas de modification de page)**

Répondez aux questions posées dans le cadre de cette tâche au fur et à mesure que chaque sujet du didacticiel est étudié. Le sujet 3 relatif à l'ouverture d'un compte privé constitue une exception. Twiki effectue une vérification par courriel des nouveaux comptes. Toutefois, aucune messagerie électronique n'a été configurée sur les ordinateurs hôte à disposition pour cette session de travaux pratiques, c'est pourquoi des comptes utilisateur ont déjà été créés afin de pouvoir effectuer les étapes nécessitant des informations de connexion.

Toute la puissance des wiki réside dans le contenu enrichi des hyperliens à disposition. Le suivi des hyperliens peut cependant présenter des problèmes de continuité. Il est donc conseillé d'ouvrir deux navigateurs. Utilisez un navigateur pour accéder à l'URL TWiki et l'autre pour travailler sur les pages. Ajustez la taille de la fenêtre du navigateur afin de pouvoir consulter les instructions dans l'un des navigateurs et effectuer les opérations dans l'autre. Si vous sélectionnez un lien externe, une erreur se produira.

Étape 1 : établissement d'une connexion client Web au wiki sur Eagle Server.

Ouvrez un navigateur Web et connectez-vous à TWiki Sandbox, à l'adresse http://eagle-server.example.com/twiki/bin/view/Sandbox/WebHome. Saisissez exactement cette URL tel qu'indiqué, en respectant également la casse. Sandbox est un sujet sur le Web, conçu pour tester les fonctionnalités wiki. Reportez-vous à la figure 1.

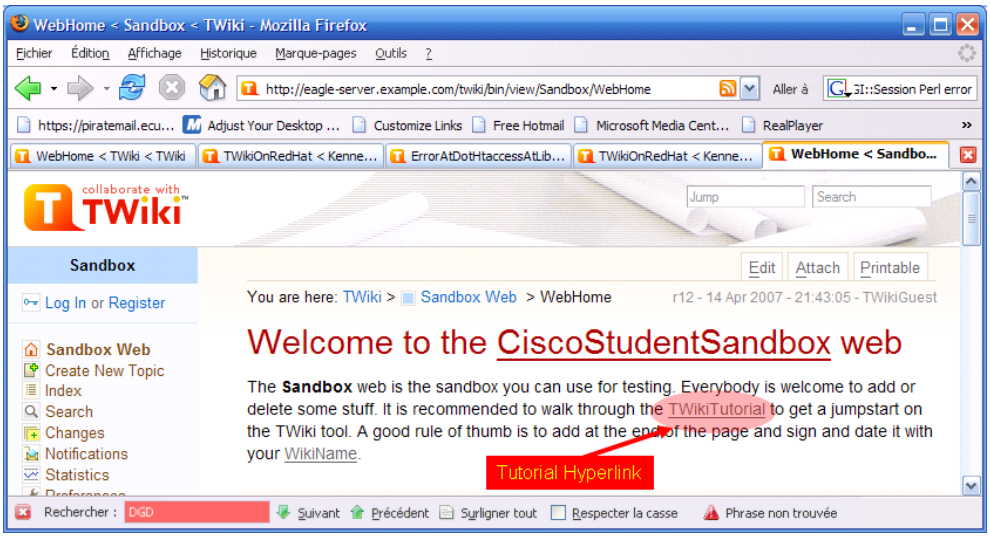


Figure 1. Site Web de TWiki Sandbox

Étape 2 : ouverture du didacticiel TWiki Tutorial.

Cliquez sur le lien TWiki mis en surbrillance rouge à la figure 1 afin d'ouvrir la page du didacticiel.

Étape 3 : visualisation du didacticiel TWiki Tutorial.

Reportez-vous à l'étape 1 du didacticiel (`Get set...`) et à l'étape 2 (`Take a quick tour...`). Une fois les deux sections parcourues, répondez aux questions suivantes :

Qu'est-ce qu'un WikiWord ?

_____
_____
_____

Combien de résultats une recherche WebSearch permet-elle d'obtenir ? _____

Reportez-vous à l'étape 3 du didacticiel (`Open a private account…`). Les adresses électroniques ne sont pas prises en charge à ce stade ; vous ne pourrez donc pas vous enregistrer. Des ID utilisateur ont été créés pour vous dans le cadre de ces travaux pratiques.

L'élément important à retenir pour cette étape est que l'enregistrement se fait en deux parties. Les utilisateurs doivent d'abord remplir un formulaire d'enregistrement et l'envoyer à TWiki.

Indiquez les informations obligatoires à fournir lors de l'enregistrement :

_____
_____
_____
_____
_____
_____
_____

Lorsque l'utilisateur envoie un formulaire d'enregistrement, TWiki lui transmet un code d'activation unique par messagerie électronique.

Au cours de la deuxième partie de l'enregistrement, l'utilisateur (1) doit saisir le code reçu dans la fenêtre d'activation ou (2) répondre par messagerie électronique en cliquant sur le lien TWiki réservé à cet effet. Le compte de l'utilisateur est alors ajouté à la base de données TWiki.

Reportez-vous à l'étape 4 du didacticiel (`Check out TWiki users, groups.`). La liste des utilisateurs et des groupes TWiki s'affiche. Une fois cette étape terminée, répondez aux questions suivantes relatives aux problèmes que les utilisateurs ou groupes peuvent rencontrer :

Quelle procédure l'utilisateur doit-il suivre pour réinitialiser son mot de passe ?

_____
_____
_____

Comment est-il possible de corriger des modifications inappropriées apportées à un sujet wiki ?

_____

Reportez-vous à l'étape 5 du Didacticiel (`Test the page controls...`) pour vous familiariser avec les fonctions d'édition de page. Une fois cette étape terminée, répondez aux questions suivantes :

Quel est le dernier numéro de révision ?

_____

Placez le lien d'action approprié en regard de chaque description de contrôle sur la page :

Attach (Joindre) **Backlinks (Liens inversés)** **Edit (Édition)**
History (Historique) **More (Plus)** **Printable (Version imprimable)**
r3 > r2 > r1 **Raw View (Affichage brut)**

Description	Lien d'action
ajout ou modification d'un sujet	
affichage du texte source sans modifier le sujet	
attachement des fichiers à un sujet	
recherche de sujets reliés à ce sujet (lien inversé)	

Description	Lien d'action
contrôles supplémentaires (par exemple, rename (renommer) / move (déplacer)), contrôle de version et définition d'un élément parent.	
sujets soumis à révision, avec historique complet des changements effectués (par exemple, auteurs des modifications et dates de modification).	
affichage d'une version précédente du sujet ou différence entre deux versions	
affichage d'une version simplifiée de la page afin de pouvoir l'imprimer	

Reportez-vous à l'étape 6 (`Change a page, and create a new one...`) afin de découvrir comment ajouter du contenu à un wiki. Utilisez la table ci-dessous pour vous connecter au serveur wiki et effectuer cette étape du didacticiel.

Un groupe de comptes privés a été créé sur Eagle Server afin de pouvoir participer à un sujet TWiki à caractère privé. Il s'agit des comptes **StudentCcna1** à **StudentCcna22.** Le même mot de passe est utilisé pour tous les comptes (**cisco**). Choisissez le compte correspondant aux numéros de votre pod et de votre ordinateur hôte. Pour ce faire, reportez-vous à la table suivante :

Numéro_pod_Numéro_hôte	ID de connexion au compte (tient compte de la casse)
Pod1host1	**StudentCcna1**
Pod1host2	**StudentCcna2**
Pod2host1	**StudentCcna3**
Pod2host2	**StudentCcna4**
Pod3host1	**StudentCcna5**
Pod3host2	**StudentCcna6**
Pod4host1	**StudentCcna7**
Pod4host2	**StudentCcna8**
Pod5host1	**StudentCcna9**
Pod5host2	**StudentCcna10**
Pod6host1	**StudentCcna11**
Pod6host2	**StudentCcna12**
Pod7host1	**StudentCcna13**
Pod7host2	**StudentCcna14**
Pod8host1	**StudentCcna15**
Pod8host2	**StudentCcna16**
Pod9host1	**StudentCcna17**
Pod9host2	**StudentCcna18**
Pod10host1	**StudentCcna19**
Pod10host2	**StudentCcna20**
Pod11host1	**StudentCcna21**
Pod11host2	**StudentCcna22**

Dans l'écran de bienvenue du wiki, cliquez sur le lien **Log In (Connexion)** situé dans le coin supérieur gauche de la page. Reportez-vous à la figure 2.

Figure 2. Lien de connexion

Une fenêtre de connexion semblable à celle présentée à la figure 3 s'affiche. Saisissez le nom d'utilisateur approprié et le mot de passe **`cisco`**. Vous devez respecter la casse à la fois pour le nom d'utilisateur et pour le mot de passe.

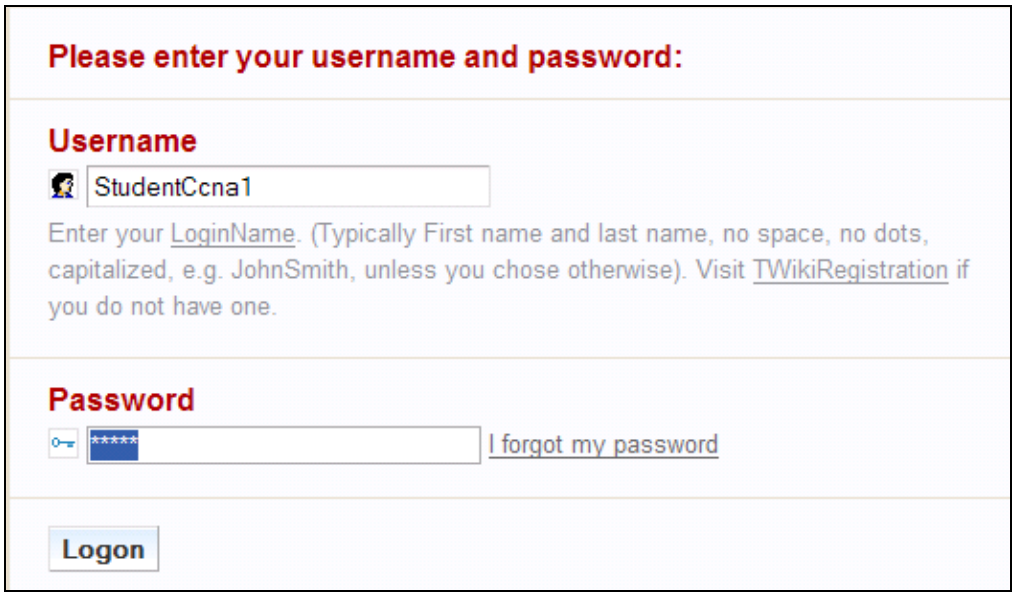


Figure 3. Fenêtre de connexion

La page de votre sujet wiki s'affiche. Elle s'apparente à celle présentée ci-dessous, à la figure 4.

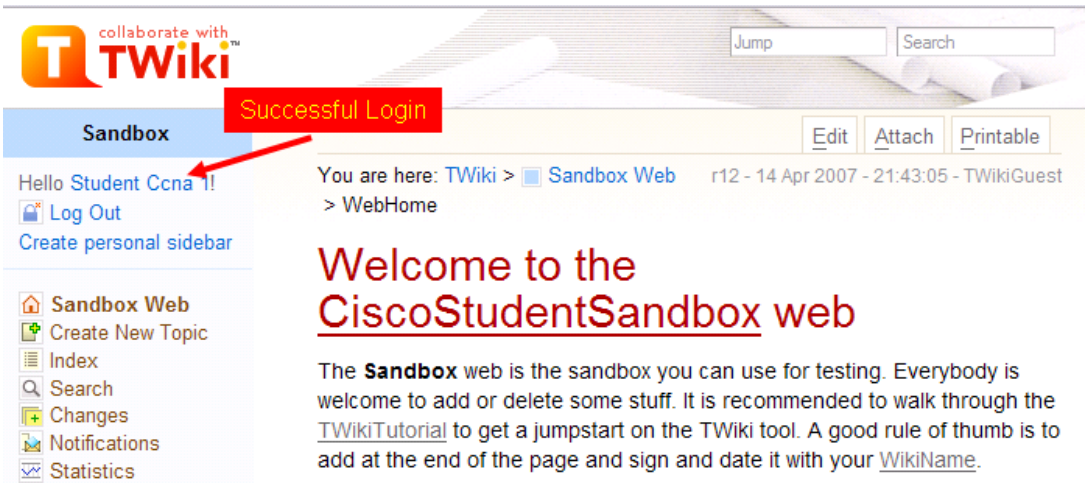


Figure 4. Page d'un sujet wiki

L'étape 7 du didacticiel (`Use your browser to upload files as page attachments...`) décrit la procédure à suivre pour télécharger des fichiers sur la page wiki. Pour ce faire, créez un document à l'aide du Bloc-notes, puis téléchargez-le sur le serveur wiki.

Quelle taille maximale votre fichier doit-il faire pour pouvoir être transféré ?

_____

L'étape 8 du didacticiel (`Get e-mail alerts whenever pages are changed...`) permet de découvrir comment recevoir des alertes par messagerie électronique lors de la mise à jour d'une page. En effet, il n'est pas très pratique de revenir régulièrement à un wiki pour vérifier si les articles publiés ont été mis à jour. Dans la mesure où la messagerie électronique n'est pas configurée sur les ordinateurs hôte dans le cadre de ces travaux pratiques, aucune alerte ne sera envoyée.

Indiquez la procédure à suivre pour recevoir des notifications de mise à jour de sujet par messagerie électronique :

_____

_____

_____

Tâche 3 : Remarques générales

Ces travaux pratiques ont permis de découvrir le fonctionnement des wiki. Vous devez rejoindre un wiki pour pouvoir l'utiliser et collaborer. Vous trouverez ci-dessous la liste de quelques wiki susceptibles de vous intéresser :

- CCNA : http://en.wikibooks.org/wiki/CCNA_Certification
- Historique de Cisco Systems : http://en.wikipedia.org/wiki/Cisco_Systems
- Wiki Web sur les produits et la technologie de Cisco : http://www.nyetwork.org/wiki/Cisco
- Network+ : http://en.wikibooks.org/wiki/Network_Plus_Certification/Study_Guide
- Dictionnaire réseau : http://wiki.networkdictionary.com/index.php/Main_Page
- Analyseur de protocole réseau Wireshark : http://wiki.wireshark.org/

Tâche 4 : confirmation

Il est possible que la classe puisse utiliser le serveur wiki TWiki pour publier des sujets d'intérêt relatifs à la théorie des réseaux informatiques et à la progression de la classe, en fonction du type d'installation effectuée pour Eagle Server.

Créez un blog personnel sur votre formation réseau. Cette opération nécessite un accès à Internet.

Tâche 5 : nettoyage

Sauf indication contraire, fermez tous les navigateurs Web et arrêtez votre ordinateur.

1.7.1 : exercice d'intégration des compétences : présentation de Packet Tracer

Diagramme de topologie

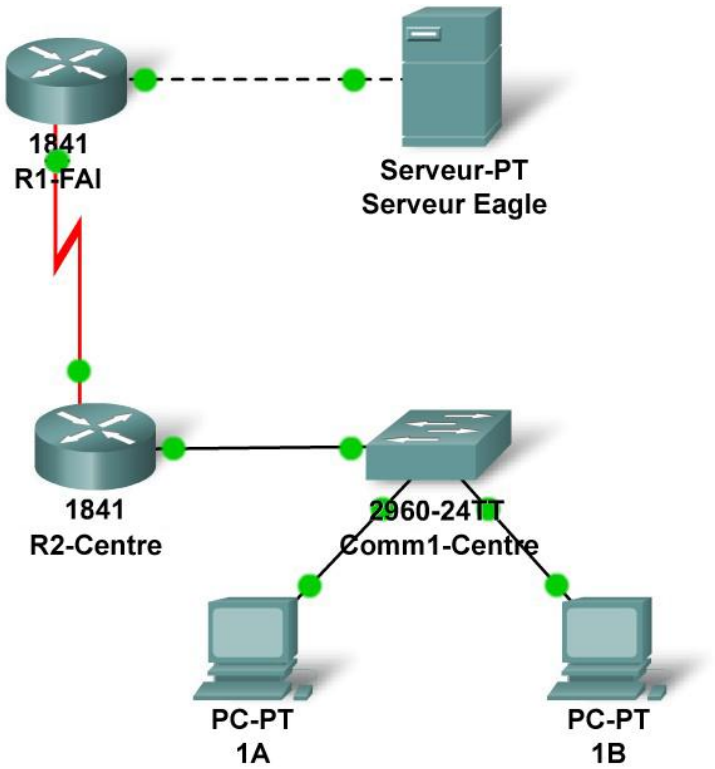


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	Fa0/0	192.168.254.253	255.255.255.0	N/A
	S0/0/0	10.10.10.6	255.255.255.252	N/A
R2-Central	Fa0/0	172.16.255.254	255.255.0.0	N/A
	S0/0/0	10.10.10.5	255.255.255.252	N/A
S1-Central	VLAN 1	172.16.254.1	255.255.0.0	172.16.255.254
PC 1A	La carte réseau	172.16.1.1	255.255.0.0	172.16.255.254
PC 1B	La carte réseau	172.16.1.2	255.255.0.0	172.16.255.254
Serveur Eagle	La carte réseau	192.168.254.254	255.255.255.0	192.168.254.253

Objectifs pédagogiques

- Explorer le mode Real-time de Packet Tracer
- Explorer la zone Logical Workplace
- Explorer le fonctionnement de Packet Tracer
- Connecter les périphériques
- Examiner la configuration d'un périphérique
- Analyser la configuration de travaux pratiques type
- Vue d'ensemble des périphériques

Contexte

Tout au long de ce cours, vous allez utiliser une configuration de travaux pratiques type constituée de PC, de serveurs, de routeurs et de commutateurs réels pour apprendre des concepts liés aux réseaux. Cette méthode offre la plus large palette de fonctions et l'expérience la plus réaliste. L'équipement et le temps étant limités, cette expérience peut être étoffée par un environnement simulé. Le simulateur qui est utilisé dans ce cours se nomme Packet Tracer. Packet Tracer propose un vaste choix de protocoles, d'équipements et de fonctions, mais peu sont ceux qui peuvent être utilisés avec un équipement réel. Packet Tracer complète, mais ne remplace pas l'expérience tirée de l'utilisation d'un équipement réel. Nous vous encourageons à comparer les résultats obtenus à partir des modèles réseau de Packet Tracer au comportement d'un équipement réel. De même, nous vous recommandons d'examiner les fichiers d'aide intégrés à Packet Tracer, où vous trouverez des travaux pratiques complets intitulés « My First PT Lab », des didacticiels et des indications sur les avantages et les limites liés à l'utilisation de Packet Tracer pour modéliser des réseaux.

Dans cet exercice, vous pourrez analyser la configuration de base en utilisant le simulateur Packet Tracer. Packet Tracer peut créer deux formats de fichiers : des fichiers .pkt (fichiers modèles de simulation de réseau) et des fichiers .pka (fichiers d'exercice pour la mise en pratique). Lorsque vous créerez vos propres réseaux dans Packet Tracer ou que vous modifierez des fichiers existants créés par votre formateur ou vos collègues, vous utiliserez généralement le format de fichier .pkt. Lorsque vous avez débuté cet exercice dans le cadre du cursus, ces instructions vous ont été présentées. Elles résultent du .pka, le format de fichier d'exercice Packet Tracer. Au bas de ces instructions figurent deux boutons : **Check Results** (qui indique votre état d'avancement dans l'exercice) et **Reset Activity** (qui vous permet de reprendre l'exercice au début dans le cas où vous souhaiteriez effacer votre travail ou acquérir davantage de pratique).

Tâche 1 : exploration de l'interface de PT

Étape 1 : analyse de la zone Logical Workplace

Lorsque Packet Tracer démarre, vous obtenez une vue logique du réseau en mode Real-time (temps réel). L'interface de PT est occupée en grande partie par la zone **Logical Workplace**. Il s'agit de la grande zone où sont placés et connectés les périphériques.

Étape 2 : utilisation des symboles

En bas à gauche de l'interface de PT, en dessous de la barre jaune, se trouve la partie de l'interface où vous sélectionnez les périphériques et les placez dans la zone Logical Workplace. La première zone située en bas à gauche contient des symboles qui représentent des groupes de périphériques. Lorsque vous placez le pointeur de la souris sur l'un de ces symboles, le nom du groupe s'affiche dans la zone de texte située au centre. Lorsque vous cliquez sur l'un de ces symboles, les périphériques qui forment le groupe s'affichent dans la zone de droite. Si vous pointez sur un périphérique spécifique, une description de celui-ci s'affiche dans la zone de texte située en dessous du périphérique. Cliquez sur chaque groupe et examinez les différents périphériques qui les composent, ainsi que les symboles associés.

Tâche 2 : exploration du fonctionnement de PT

Étape 1 : connexion des périphériques à l'aide de la fonction de connexion automatique

Cliquez sur le symbole de groupe de connexions. Les symboles de connexion spécifiques fournissent différents types de câbles qui peuvent être utilisés pour connecter des périphériques. Le premier type, représenté par un éclair doré, sélectionne automatiquement le type de connexion en fonction des interfaces disponibles sur les périphériques. Lorsque vous cliquez sur ce symbole, le pointeur prend la forme d'un connecteur de câble.
Pour relier deux périphériques, cliquez successivement sur le symbole de connexion automatique, sur le premier périphérique, puis sur le second. En utilisant le symbole de connexion automatique, opérez les connexions suivantes :

- reliez le serveur Eagle Server au routeur R1-ISP ;
- reliez le PC-PT 1A au commutateur S1-Central.

Étape 2 : analyse de la configuration des périphériques avec la souris

Placez le pointeur de la souris sur les périphériques figurant dans la zone Logical Workplace. La configuration des périphériques s'affiche dans une zone de texte aussitôt que vous placez le pointeur sur ces symboles.

- Dans le cas d'un **routeur**, des paramètres de configuration des ports s'affichent, notamment l'adresse IP, l'état des ports et l'adresse MAC.
- Pour un **serveur**, les informations affichées portent sur l'adresse IP, l'adresse MAC et la passerelle.
- Dans le cas d'un **commutateur**, des informations de configuration de port s'affichent, y compris l'adresse IP, l'adresse MAC, l'état des ports et l'appartenance à un réseau local virtuel (VLAN).
- S'agissant d'un **PC**, les informations affichées portent sur l'adresse IP, l'adresse MAC et la passerelle.

Étape 3 : examen de la configuration des périphériques

Cliquez avec le bouton gauche de la souris sur chaque type de périphérique présent dans la zone Logical Workplace pour afficher leur configuration.

- **Aux périphériques de type routeur et commutateur** correspondent trois onglets. Ces onglets s'intitulent Physical, Config et CLI (Command Line Interface).
  - L'onglet Physical présente les composants physiques du périphérique, tels que les modules. Il est également possible d'ajouter de nouveaux modules à partir de cet onglet.
  - L'onglet Config présente des informations de configuration générales, telles que le nom du périphérique.
  - L'onglet CLI permet à l'utilisateur de configurer le périphérique par le biais de l'interface de ligne de commande.
- **Aux périphériques de type serveur et concentrateur** correspondent deux onglets. Ces onglets s'intitulent Physical et Config.
  - L'onglet Physical présente les composants du périphérique, tels que les ports. Il est également possible d'ajouter de nouveaux modules à partir de cet onglet.
  - L'onglet Config présente des informations générales, telles que le nom du périphérique.
- **Aux périphériques de type PC** correspondent trois onglets. Ces onglets s'intitulent Physical, Config et Desktop.
  - L'onglet Physical présente les composants du périphérique. Il est également possible d'ajouter de nouveaux modules à partir de cet onglet.
  - L'onglet Config présente le nom du périphérique, l'adresse IP, le masque de sous-réseau, le serveur DNS et la passerelle.
  - L'onglet Desktop permet à l'utilisateur de configurer l'adresse IP, le masque de sous-réseau, la passerelle par défaut, le serveur DNS, la connexion commutée et sans fil. Cet onglet donne également accès à un émulateur de terminal et à un navigateur Web simulé.

Tâche 3 : analyse de la configuration de travaux pratiques type

Étape 1 : vue d'ensemble des périphériques

La configuration standard comprend deux routeurs, un commutateur, un serveur et deux PC. Chaque périphérique est pré-configuré (noms, adresses IP, passerelles et paramètres de connexion).

Remarques générales :

nous vous recommandons de vous procurer Packet Tracer auprès de votre formateur et d'effectuer les travaux pratiques « My First PT Lab ».

Exercice 2.2.5 : utilisation de NeoTrace™ pour afficher des interréseaux

Objectifs pédagogiques

- Expliquer l'utilisation des programmes de traçage de route tels que tracert et NeoTrace.
- Utiliser tracert et NeoTrace pour tracer une route de son PC vers un serveur distant.
- Décrire la nature interconnectée et globale d'Internet en termes de flux de données.

Contexte

Le logiciel informatique de traçage de route permet de répertorier les réseaux que doivent traverser les données du périphérique final d'origine de l'utilisateur à un réseau de destination distant.

Cet outil de réseau s'exécute généralement dans une ligne de commande comme suit :

traceroute <nom du réseau de destination ou adresse du périphérique final>

(Unix et systèmes identiques)

ou

tracert <nom du réseau de destination ou adresse du périphérique final>

(systèmes MS Windows)

et détermine la route prise par les paquets dans un réseau IP.

L'outil **traceroute** (ou **tracert**) est souvent utilisé pour dépanner les réseaux. En affichant la liste des routeurs traversés, il permet à l'utilisateur d'identifier le chemin pris pour atteindre une destination particulière sur le réseau ou les interréseaux. Chaque routeur représente un point de connexion entre deux réseaux où a été transféré le paquet. Le nombre de routeurs correspond au nombre de « sauts » effectués par les données depuis la source jusqu'à la destination.

La liste affichée permet d'identifier les problèmes de flux de données lors de la tentative d'accès à un service tel qu'un site Web. Elle permet également d'effectuer des tâches telles que le téléchargement de données. Si plusieurs sites Web (miroirs) sont disponibles pour le même fichier de données, il est possible de tracer chaque miroir pour déterminer le plus rapide.

Cependant, il faut noter qu'en raison de la nature « maillée » des réseaux interconnectés qui composent Internet et de la possibilité donnée au protocole Internet de sélectionner plusieurs chemins sur lesquels envoyer les paquets, deux routes de traçage entre la même source et la même destination exécutées à un intervalle donné peuvent générer des résultats différents.

Ce genre d'outils est généralement intégré au système d'exploitation du périphérique final.

Les autres outils tels que NeoTrace™ sont des programmes propriétaires qui fournissent des informations supplémentaires. Neotrace utilise les informations en ligne disponibles pour afficher sous forme graphique la route tracée sur une carte mondiale, par exemple.

Scénario

Avec une connexion Internet, vous allez utiliser deux programmes de traçage de route pour examiner le chemin Internet menant aux réseaux de destination.

Cet exercice doit être effectué sur un ordinateur doté d'un accès à Internet et à la fenêtre de ligne de commande. Premièrement, vous allez utiliser l'utilitaire Windows intégré **tracert**, puis le programme avancé NeoTrace. Ces travaux pratiques nécessitent d'avoir installé préalablement NeoTrace.

Tâche 1 : traçage de la route jusqu'au serveur distant.

Étape 1 : traçage de la route jusqu'à un réseau distant.

Pour tracer la route jusqu'à un réseau distant, le PC utilisé doit disposer d'une connexion au réseau de la classe/des travaux pratiques.

1. Dans l'invite de ligne de commande, saisissez ce qui suit : **`tracert www.cisco.com`**

   La première ligne de résultat doit afficher le nom de domaine qualifié complet (FQDN) suivi de l'adresse IP. Le serveur DNS des travaux pratiques a pu convertir le nom en une adresse IP. Sans cela, **`tracert`** aurait échoué car cet outil fonctionne au niveau de couches TCP/IP qui ne comprennent que les adresses IP valides.

   Si le serveur DNS n'est pas disponible, l'adresse IP du périphérique de destination doit être saisie après la commande **`tracert`** au lieu du nom de serveur.

2. Examinez le résultat affiché.

   Combien de sauts séparent la source et la destination ? _____

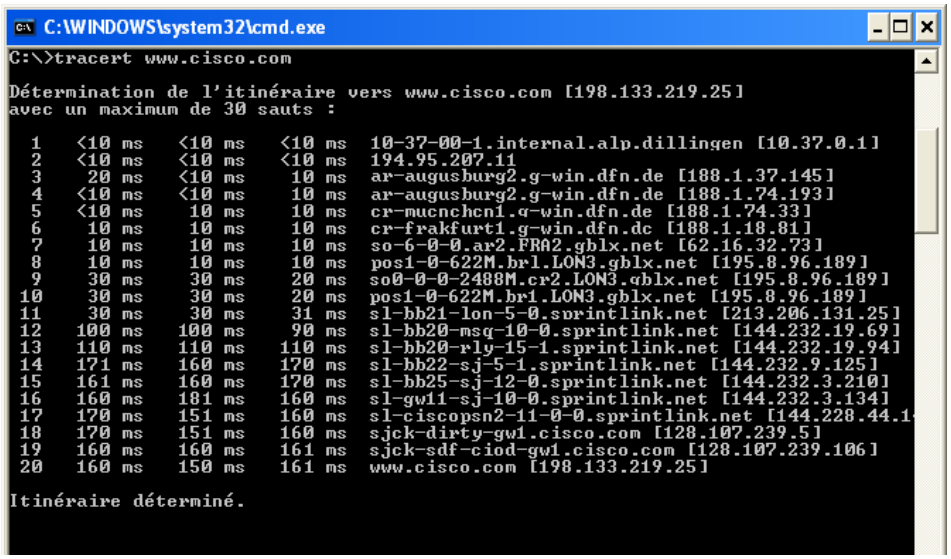


Figure 1. Commande `tracert`

La figure 1 affiche un résultat correct lors de l'exécution de :

`tracert www.cisco.com`

depuis un lieu en Bavière (Allemagne).

La première ligne du résultat affiche le nom de domaine qualifié complet, suivi de l'adresse IP. Par conséquent, un serveur DNS a pu convertir le nom en une adresse IP. Tous les routeurs que doivent traverser les requêtes **`tracert`** pour atteindre la destination sont ensuite répertoriés.

3. Essayez la même route de traçage sur un PC connecté à Internet, puis examinez le résultat.

   Nombre de sauts jusqu'à www.cisco.com : _____

Étape 2 : tentative d'une autre route de traçage sur le même PC et examen du résultat.

URL de destination : _____

Adresse IP de destination : _____

Tâche 2 : traçage d'une route à l'aide de NeoTrace.

1. Lancez le programme NeoTrace.
2. Dans le menu **View (Affichage)**, sélectionnez **Options**. Cliquez sur l'onglet **Map (Carte)** , puis cliquez sur le bouton **Set Home Location (Définir mon domicile)** dans la section **Home Location (Domicile)**.
3. Suivez les instructions pour sélectionner votre pays et votre ville.
   Vous pouvez sinon cliquer sur le bouton **Advanced (Avancé)**, qui permet de saisir la latitude et la longitude précises de votre ville. Reportez-vous à la section Confirmation de l'exercice 1.2.5(1).
4. Entrez « www.cisco.com » dans le champ **Target (Cible)**, puis cliquez sur **Go (Aller)**.
5. Dans le menu **View (Affichage)**, **List View (Liste)** affiche la liste des routeurs comme **`tracert`**.

   L'option **Node View (Affichage des nœuds)** du menu **View (Affichage)** affiche les connexions sous forme graphique avec des symboles.

   L'option **Map View (Affichage de la carte)** du menu **View (Affichage)** affiche l'emplacement géographique des liens et des routeurs sur une carte mondiale.
6. Sélectionnez chaque vue de façon séquentielle afin de relever les différences et les similarités.
7. Essayez différentes URL et affichez les routes jusqu'à ces destinations.

Tâche 3 : Remarques générales

Passez en revue la fonction et l'utilité des programmes de traçage de route.

Faites le lien entre les écrans de résultat de NeoTrace et le concept de réseaux interconnectés et de la nature mondiale d'Internet.

Tâche 4 : confirmation

Répertoriez les problèmes de sécurité réseau éventuels susceptibles de survenir avec l'utilisation de programmes tels que traceroute et NeoTrace. Répertoriez les détails techniques fournis et comment ces informations peuvent être mal employées.

Tâche 5 : nettoyage

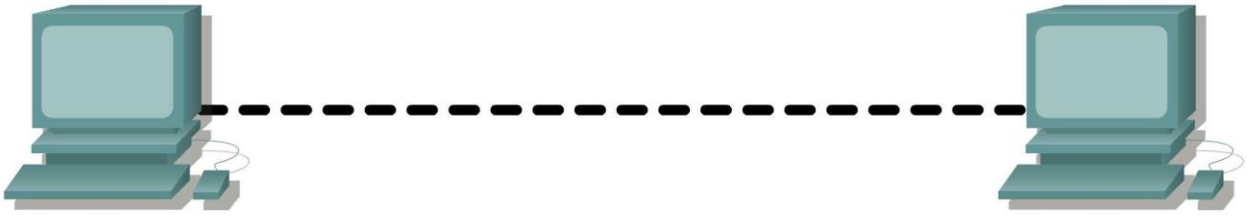
Quittez le programme NeoTrace.

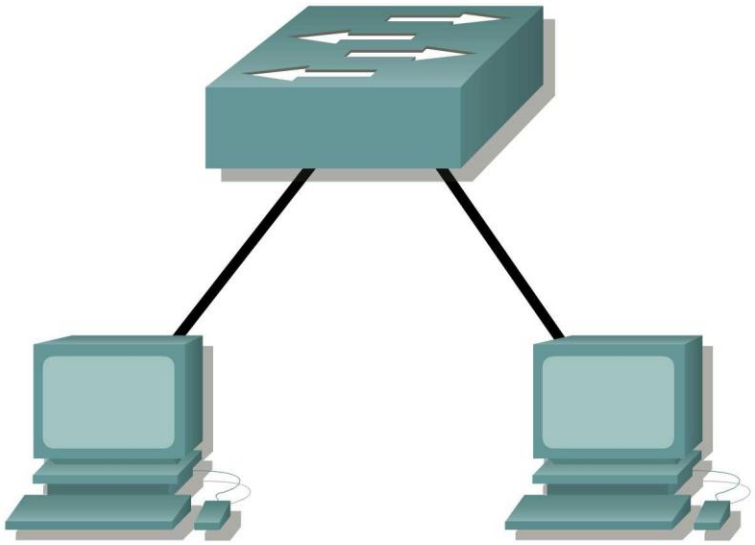
Sauf instruction contraire de votre formateur, éteignez correctement l'ordinateur.

Travaux pratiques 2.6.1 : orientation de la topologie et création d'un petit réseau

Schéma de la topologie

Réseau peer-to-peer





Réseau commuté

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- identifier correctement les câbles à utiliser au sein du réseau ;
- relier physiquement un réseau peer-to-peer et commuté ;
- vérifier la connectivité de base de chaque réseau.

Contexte

Vous pouvez résoudre un grand nombre de problèmes de réseau au niveau de sa couche physique. Il est donc important de bien comprendre quels câbles utiliser pour les connexions réseau.

Au niveau de la couche physique (couche 1) du modèle OSI, vous devez relier les périphériques finaux entre eux par un dispositif approprié (des câbles). Le type de dispositif utilisé dépend du type de périphérique connecté. Dans la partie élémentaire de cette session de travaux pratiques, vous utiliserez des câbles de liaison directe (câbles de raccordement) pour relier les stations de travail aux commutateurs.

Une adresse est également nécessaire pour que deux périphériques puissent communiquer. Vous devez spécifier une adresse unique (également connue sous le nom d'adresse logique ou adresse IP) pour la couche réseau (couche 3) afin que les données puissent être transférées au périphérique de destination approprié.

Dans le cadre de ces travaux pratiques, l'adressage s'appliquera aux stations de travail et sera utilisé pour permettre aux périphériques de communiquer.

Scénario

Ces travaux pratiques consistent tout d'abord à créer un réseau simple (peer-to-peer), puis à effectuer des connexions via un commutateur.

Tâche 1 : création d'un réseau peer-to-peer

Étape 1 : sélection d'un partenaire.

Étape 2 : obtention de l'équipement et des ressources nécessaires pour effectuer ces travaux pratiques.

Équipement requis :

- 2 stations de travail
- 2 câbles droits (câbles de raccordement)
- 1 câble croisé
- 1 commutateur (ou concentrateur)

Tâche 2 : identification des câbles utilisés au sein du réseau.

Avant de relier les périphériques, vous devez identifier le dispositif à utiliser. Dans le cadre de ces travaux pratiques, vous utiliserez des câbles de croisement et de liaison directe.

Reliez les deux stations de travail à l'aide d'un **câble croisé** via le port Ethernet de leur carte réseau. Il s'agit d'un câble Ethernet. Observez son connecteur : la position des fils orange et vert est inversée à chaque extrémité du câble.

Reliez le port Ethernet du routeur ou une station de travail à un port du commutateur à l'aide d'un **câble droit**. Il s'agit également d'un câble Ethernet. Observez son connecteur : la position de chaque broche est identique aux deux extrémités du câble.

Tâche 3 : câblage du réseau peer-to-peer.

Étape 1 : connexion de deux stations de travail.

Reliez les deux stations de travail à l'aide du câble Ethernet approprié. Connectez une extrémité du câble au port de la carte réseau du PC1 et l'autre au PC2.

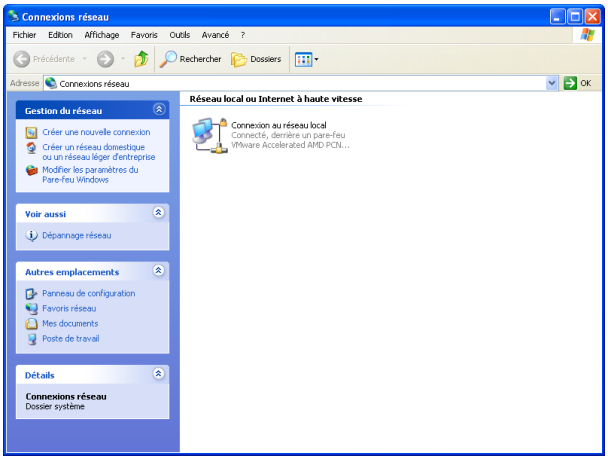
Quel câble avez-vous utilisé ? _____

Étape 2 : définition d'une adresse de couche 3 pour les deux stations de travail.

Pour effectuer cette tâche, suivez les instructions pas à pas ci-dessous.

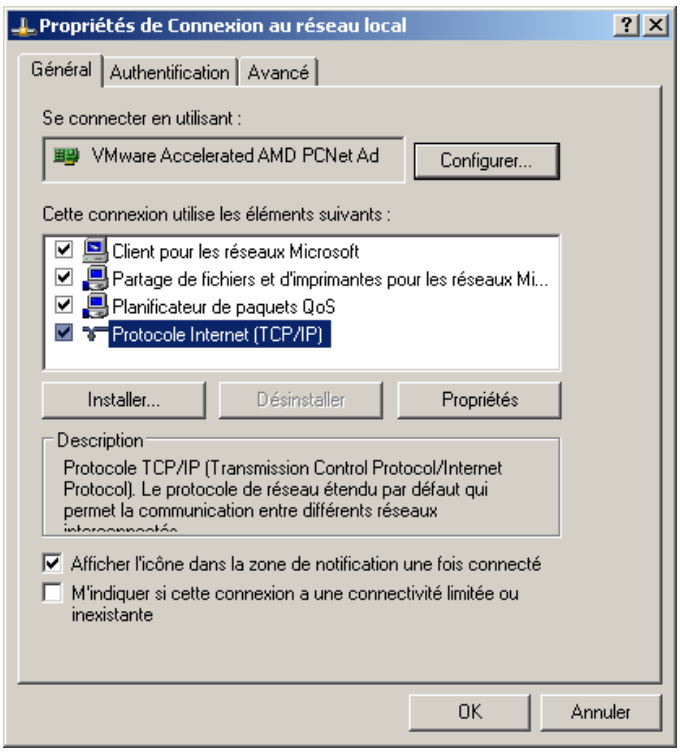
Remarque : vous devez effectuer ces étapes sur *chaque* station de travail. Les instructions ci-dessous supposent que vous utilisiez Windows XP. Les étapes peuvent varier légèrement si vous utilisez un autre système d'exploitation.

1. Sur votre ordinateur, cliquez sur **Démarrer**, puis cliquez avec le bouton droit de la souris sur **Favoris réseau**. Cliquez ensuite sur **Propriétés.** La fenêtre Connexions réseau s'affiche. Elle comprend des icônes indiquant les différentes connexions.

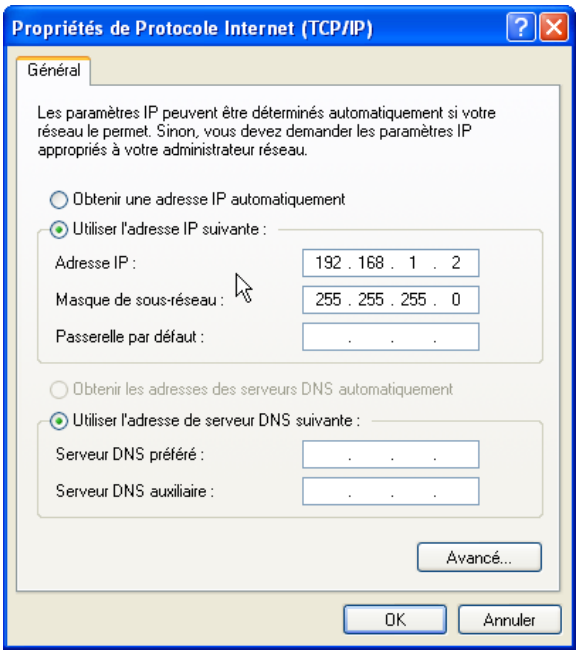


2. Cliquez avec le bouton droit de la souris sur **Connexion au réseau local** , puis cliquez sur **Propriétés**.

3. Sélectionnez **Protocole Internet (TCP/IP)**, puis cliquez sur le bouton **Propriétés**.



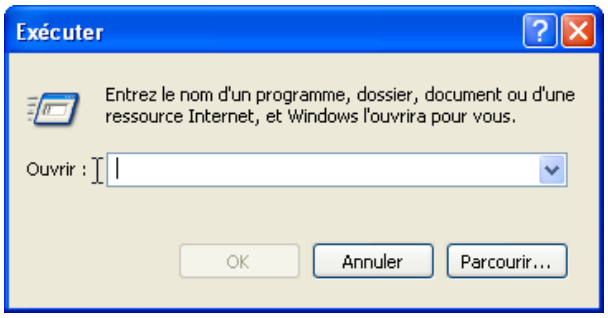
4. Dans l'onglet Général de la fenêtre qui s'affiche, sélectionnez l'option **Utiliser l'adresse IP suivante**.
5. Dans le champ **Adresse IP**, saisissez l'adresse 192.168.1.2 pour le PC1. Pour le PC2, vous devrez saisir l'adresse 192.168.1.3.
6. Appuyez sur la touche de tabulation afin de renseigner automatiquement le masque de sous-réseau. L'adresse de sous-réseau 255.255.255.0 s'affiche. Si elle ne s'affiche pas automatiquement, saisissez-la manuellement.
7. Cliquez sur **OK**.



8. Fermez la fenêtre Propriétés de connexion au réseau local.

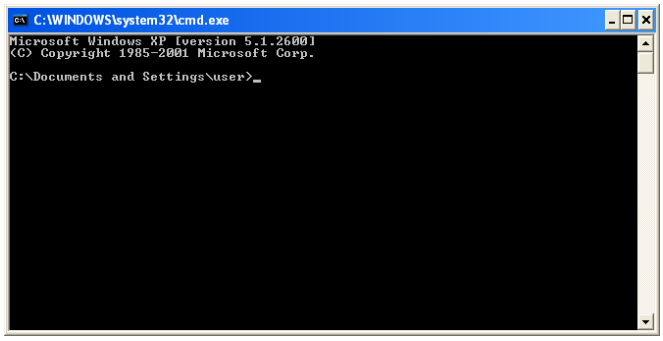
Étape 3 : vérification de la connectivité.

1. Sur votre ordinateur, cliquez sur **Démarrer**, puis sur **Exécuter**.



2. Tapez **cmd** dans le champ Ouvrir, puis cliquez sur **OK**.

   La fenêtre de commande DOS (cmd.exe) s'affiche. Utilisez-la pour saisir des commandes DOS. Dans le cadre de ces travaux pratiques, vous devrez saisir des commandes réseau de base pour tester les connexions.



La commande **ping** est un outil de test réseau permettant de vérifier si un hôte (une station de travail, un routeur, un serveur, etc.) est joignable sur un réseau IP.

3. Utilisez la commande **ping** pour vérifier si le PC1 peut joindre le PC2, et inversement. Saisissez **ping 192.168.1.3** au niveau de l'invite de commande DOS du PC1. Saisissez **ping 192.168.1.2** au niveau de l'invite de commande DOS du PC2.

   Quel est le résultat de la commande **ping** ?

   _____

   _____

   _____

   _____

   Si la commande **ping** affiche un message d'erreur ou que vous ne recevez aucune réponse de la part de l'autre station de travail, essayez de résoudre le problème. Vous pouvez effectuer les opérations de dépannage suivantes :

   - Vérifier que les adresses IP sont correctes pour les deux stations de travail
   - Vérifier que vous avez relié les stations de travail à l'aide du câble approprié

   Quel résultat obtenez-vous si vous débranchez le câble réseau et que vous envoyez une commande **ping** à l'autre station de travail ?

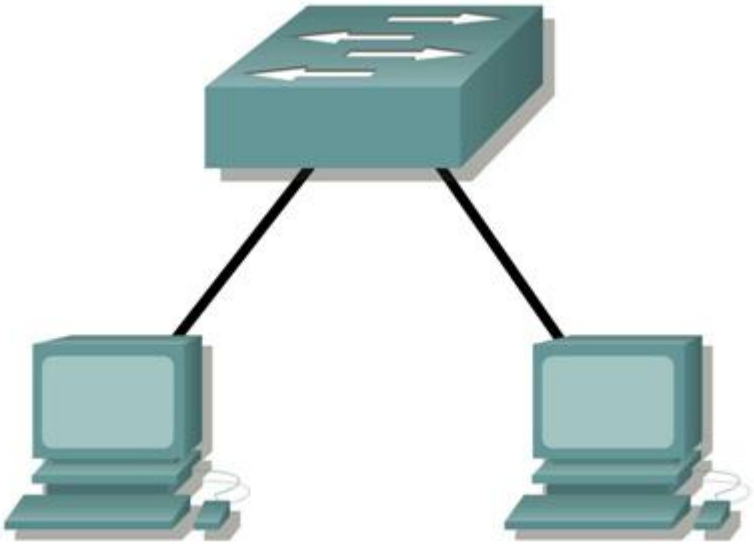
   _____

   _____

   _____

   _____

Tâche 4 : connexion des stations de travail au commutateur de la classe utilisé pour les travaux pratiques.



Étape 1 : connexion d'une station de travail au commutateur.

Reliez une extrémité du câble approprié au port de la carte réseau d'une station de travail et l'autre extrémité à l'un des ports du commutateur.

Étape 2 : suivi de la même procédure pour chaque station de travail du réseau.

Quel câble avez-vous utilisé ? _____

Étape 3 : vérification de la connectivité.

Vérifiez la connectivité réseau en envoyant une commande **`ping`** aux autres stations de travail reliées au commutateur.

Quel est le résultat de la commande **`ping`** ?

_____

_____

_____

_____

Quel résultat obtenez-vous si vous envoyez une commande **`ping`** à une adresse non connectée au réseau ?

_____

_____

_____

_____

Étape 4 : partage d'un document entre plusieurs ordinateurs.

1. Créez un nouveau dossier intitulé **test** sur votre bureau.
2. Cliquez sur ce dossier avec le bouton droit de la souris, puis sélectionnez l'option de partage de fichier. **Remarque :** une main s'affiche sous l'icône.
3. Placez un fichier dans le dossier.
4. Sur le bureau, double-cliquez sur **Favoris réseau** , puis sur **Ordinateurs proches de moi**.
5. Double-cliquez sur l'icône de station de travail. Le dossier **test** s'affiche. Vous pouvez alors accéder à ce dossier sur le réseau. Une fois que le fichier s'affiche et que vous pouvez travailler avec, vous bénéficiez d'un accès à travers les 7 couches du modèle OSI.

Tâche 5 : Remarques générales

Dans quels cas est-il impossible d'envoyer une commande ping d'une station de travail à une autre lorsqu'elles sont directement reliées ?

_____

_____

_____

_____

Dans quels cas est-il impossible d'envoyer une commande ping aux stations de travail lorsqu'elles sont reliées via un commutateur ?

_____

_____

_____

_____

Travaux pratiques 2.6.2 : utilisation de Wireshark™ pour afficher des unités de données de protocole

Objectifs pédagogiques

- Expliquer l'objectif d'un analyseur de protocoles (Wireshark)
- Exécuter une capture de base des unités de données de protocole (PDU) à l'aide de Wireshark
- Exécuter une analyse de base des PDU sur un trafic de données réseau simple
- Se familiariser aux fonctionnalités et options de Wireshark telles que la capture des PDU et le filtrage de l'affichage

Contexte

Wireshark est un analyseur de protocoles (analyseur de paquets) utilisé pour dépanner les réseaux, effectuer des analyses, développer des logiciels et des protocoles et s'informer. Avant juin 2006, Wireshark répondait au nom d'Ethereal.

Un analyseur de paquets (ou analyseur de réseaux ou de protocoles) est un logiciel permettant d'intercepter et de consigner le trafic des données transférées sur un réseau de données. L'analyseur « capture » chaque PDU des flux de données circulant sur le réseau. Il permet de décoder et d'analyser leur contenu conformément aux spécifications RFC ou autres appropriées.

Wireshark est programmé pour reconnaître la structure de différents protocoles réseau. Vous pouvez l'utiliser pour afficher l'encapsulation et les champs spécifiques aux PDU, puis interpréter leur signification.

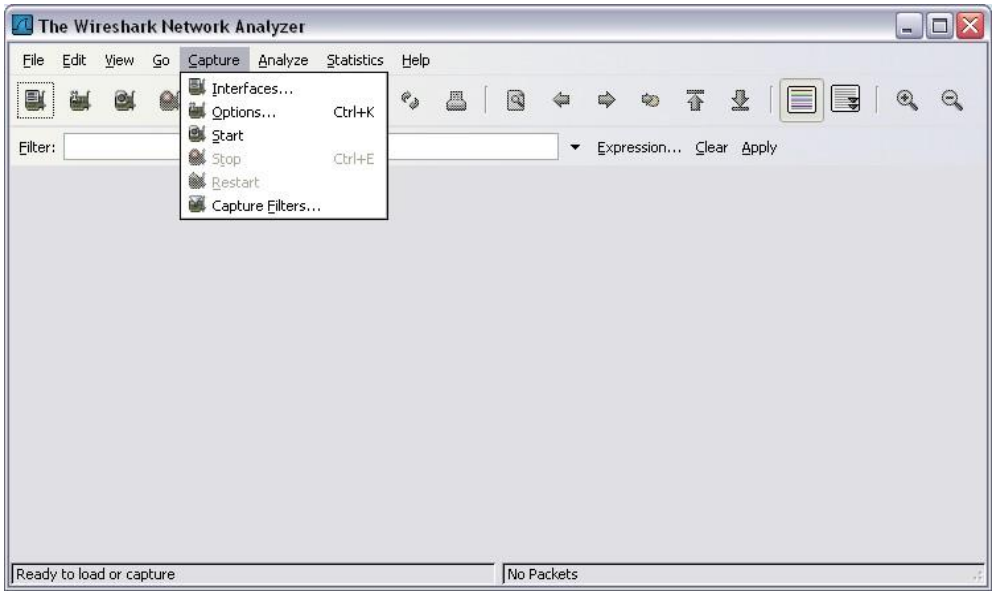
Cet outil est utile pour toutes les personnes intervenant au niveau des réseaux. Vous pouvez vous en servir dans le cadre de la plupart des travaux pratiques des cours CCNA, à des fins d'analyse de données et de dépannage.

Pour en savoir plus sur cet analyseur et télécharger le programme correspondant, accédez au site http://www.Wireshark.org

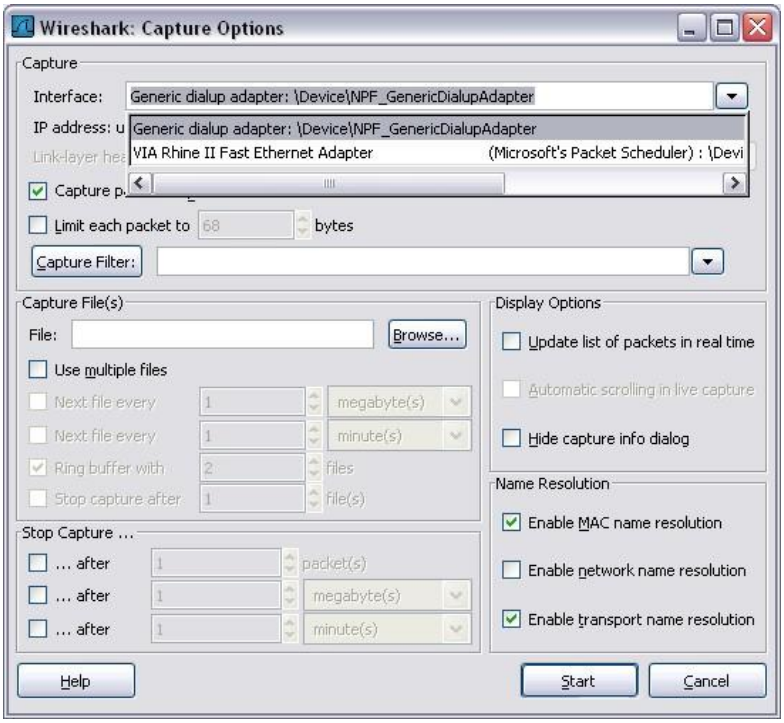
Scénario

Pour pouvoir capturer des données, vous devez d'abord vous connecter au réseau depuis l'ordinateur sur lequel Wireshark est installé et exécuter Wireshark.

Lorsque vous lancez Wireshark, l'écran ci-dessous s'affiche.

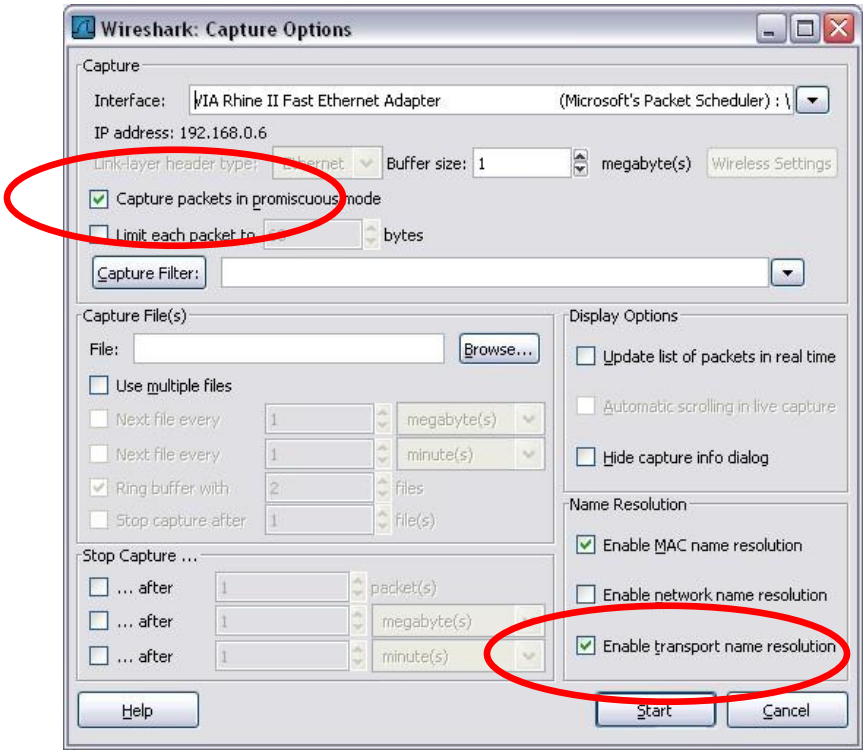


Pour lancer la capture des données, sélectionnez d'abord l'élément **Options** dans le menu **Capture**. La boîte de dialogue **Options** comprend tout un ensemble de paramètres et de filtres déterminant le trafic de données capturé et le mode de capture utilisé.



Vous devez commencer par vous assurer que Wireshark est configuré pour l'interface appropriée. Dans la liste déroulante **Interface**, sélectionnez la carte réseau utilisée. Pour un ordinateur, il s'agit généralement de la carte Ethernet connectée.

Vous pouvez ensuite définir les **Capture options**. Examinez les deux options mises en relief ci-dessous.



Configuration de Wireshark permettant de capturer des paquets en mode de proximité

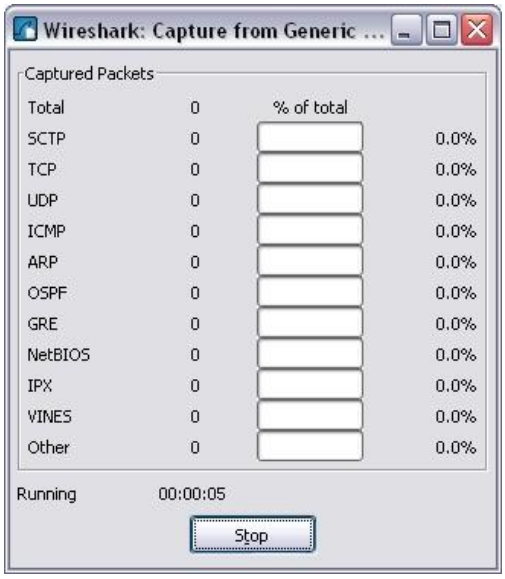
Si vous ne sélectionnez pas l'option Capture packets in promiscious mode, seules les PDU destinées à l'ordinateur sont capturées.
Si vous la sélectionnez, toutes les PDU destinées à l'ordinateur et toutes celles détectées par la carte réseau de l'ordinateur sur le même segment de réseau (c'est-à-dire les PDU transitant par la carte réseau non destinées à l'ordinateur) sont capturées.
Remarque : la capture de ces PDU supplémentaires dépend du périphérique utilisé pour connecter les ordinateurs finaux sur le réseau. Les résultats d'analyse Wireshark varient en fonction des différents périphériques (concentrateurs, commutateurs, routeurs) utilisés au cours de la formation.

Configuration de Wireshark permettant de résoudre les noms réseau

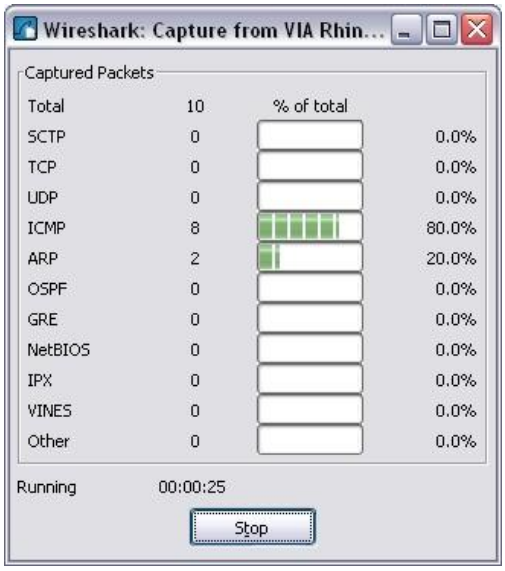
Utilisez l'option Enable... name resolution pour indiquer si Wireshark doit convertir les adresses réseau détectées dans les PDU en noms. Bien que cette fonction soit utile, notez que le processus de résolution des noms risque d'ajouter des PDU aux données capturées et ainsi peut-être de fausser l'analyse.

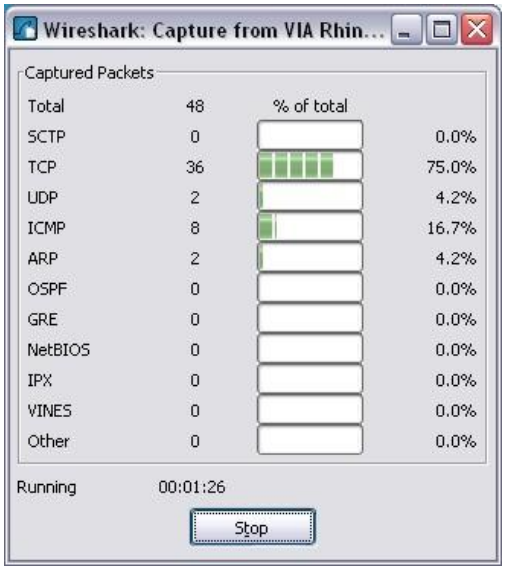
Un certain nombre d'autres paramètres de filtrage et processus de capture sont également disponibles.

Cliquez sur le bouton **Start** (Démarrer) pour lancer la capture des données. Une fenêtre affiche l'état d'avancement.



Le type et le nombre de PDU capturées sont indiqués au fur et à mesure du déroulement du processus.

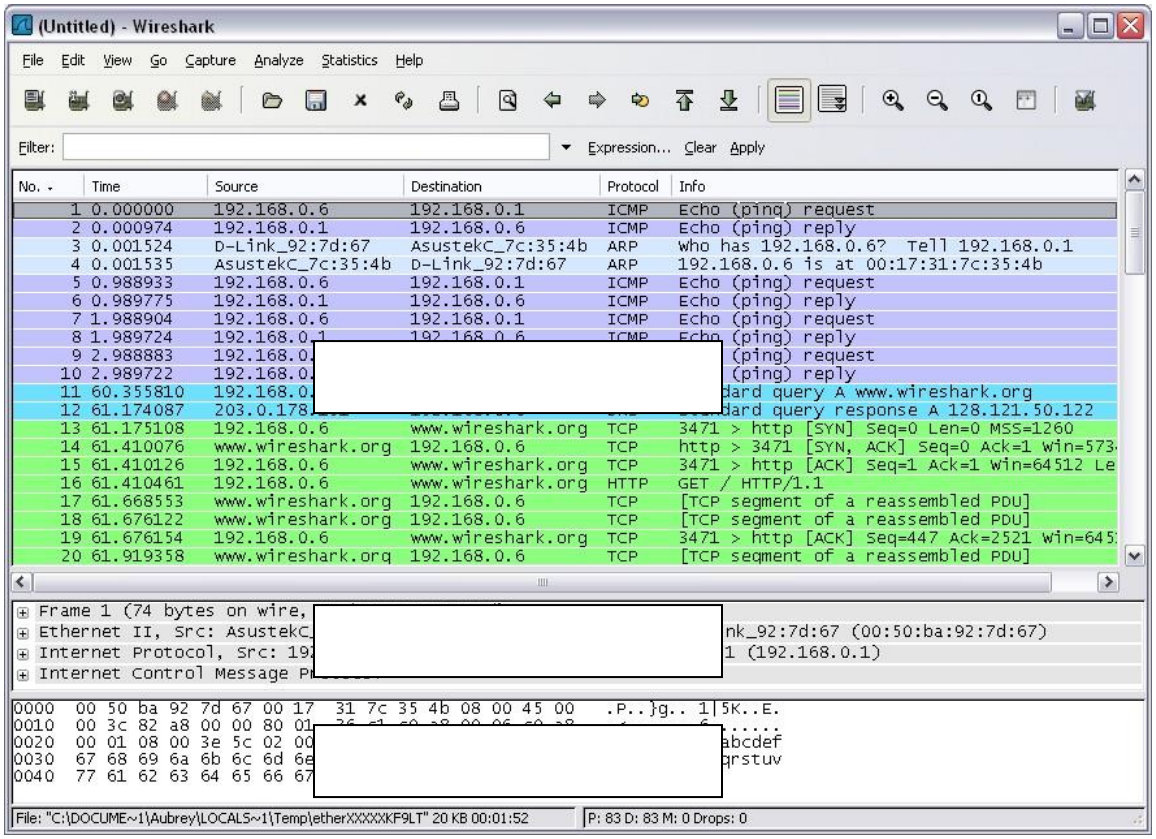




Les exemples ci-dessus montrent la capture d'un processus ping suivi d'un accès à une page Web.

Cliquez sur le bouton **Stop** pour mettre fin à la capture. L'écran principal s'affiche.

La fenêtre principale de Wireshark est constituée de trois volets.



Le volet supérieur de l'écran présenté ci-dessus comprend un récapitulatif des PDU (ou paquets) capturées. Le contenu des deux autres volets dépend des paquets sélectionnés au sein de ce volet.

Le volet du milieu comprend des informations détaillées sur le paquet sélectionné dans le premier volet.

Enfin, le volet inférieur affiche les données (au format hexadécimal correspondant à la représentation binaire) issues du paquet sélectionné dans le premier volet, en mettant en surbrillance les éléments correspondant au champ sélectionné dans le volet du milieu.

Chaque ligne de la liste des paquets (premier volet) correspond à une PDU (un paquet) de données capturée. Si vous sélectionnez une ligne dans ce volet, ses détails s'affichent dans les volets du milieu et inférieur. Dans l'exemple ci-dessus, le volet supérieur comprend les PDU capturées lors de l'utilisation d'une commande ping et d'un accès au site http://www.Wireshark.org. Le paquet numéro 1 est sélectionné.

Le volet du milieu affiche les détails de ce paquet. Les protocoles et les champs de protocole du paquet sélectionné sont indiqués. Ils s'affichent sous la forme d'une arborescence que vous pouvez développer ou réduire.

Le volet inférieur présente les données du paquet sélectionné dans le volet supérieur au format « hexdump ». Ce volet ne sera pas examiné en détail au cours de la présente session de travaux pratiques. Notez toutefois que ces informations sont utiles lors des analyses plus approfondies car elles permettent de passer en revue les valeurs binaires et le contenu des PDU.

Vous pouvez enregistrer les informations capturées pour les PDU de données dans un fichier. Le fichier peut ensuite être ouvert dans Wireshark en vue d'une analyse ultérieure sans qu'il soit nécessaire de capturer à nouveau le trafic de données. Les informations qui s'affichent lorsque vous ouvrez un fichier de capture sont identiques à celles de la capture d'origine.

Vous êtes invité à enregistrer les PDU capturées lorsque vous fermez un écran de capture ou que vous quittez Wireshark.

Cliquez sur **Continue without Saving** (Poursuivre sans enregistrer) pour fermer le fichier ou quitter Wireshark sans enregistrer les données capturées.

Tâche 1 : capture des PDU associées à un processus ping

Étape 1 : vérification de la topologie et de la configuration standard utilisées dans le cadre des travaux pratiques et lancement de Wireshark sur un ordinateur de pod

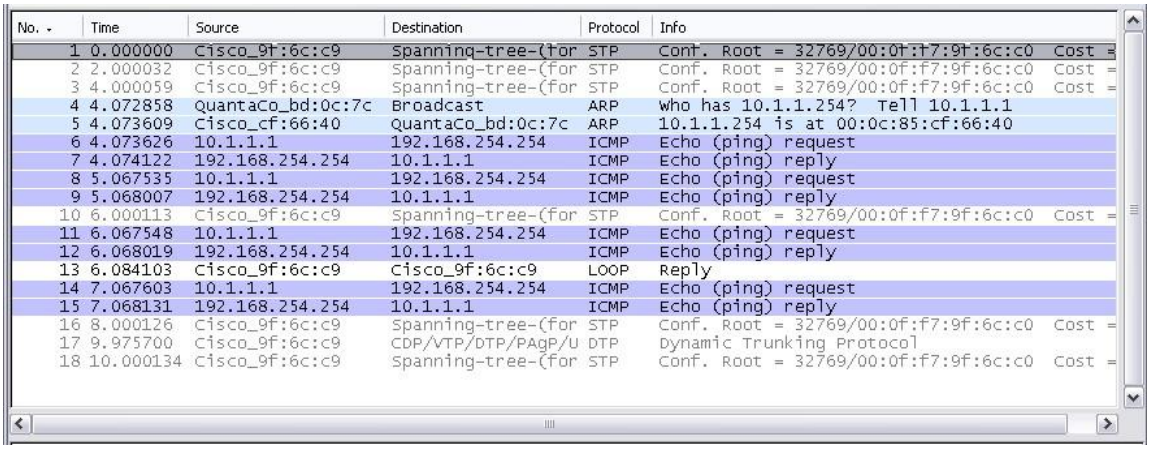
Définissez les options de capture comme indiqué ci-dessus, dans la présentation, puis lancez la capture.

Sur la ligne de commande de l'ordinateur, envoyez une commande ping à l'adresse IP ///d'un autre périphérique connecté au réseau (voir le schéma de la topologie fourni pour cette session de travaux pratiques). Ici, il s'agit d'une commande ping envoyée au serveur Eagle en spécifiant l'adresse **192.168.254.254**.

Une fois que vous avez reçu le résultat attendu, arrêtez la capture des paquets.

Étape 2 : observation du volet de la liste des paquets

Le volet supérieur de Wireshark doit ressembler à ce qui suit :



No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
2	2.000032	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
3	4.000059	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
4	4.072858	QuantaCo_bd:0c:7c	Broadcast	ARP	Who has 10.1.1.254? Tell 10.1.1.1
5	4.073609	Cisco_cf:66:40	QuantaCo_bd:0c:7c	ARP	10.1.1.254 is at 00:0c:85:cf:66:40
6	4.073626	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
7	4.074122	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
8	5.067535	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
9	5.068007	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
10	6.000113	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
11	6.067548	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
12	6.068019	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
13	6.084103	Cisco_9f:6c:c9	Cisco_9f:6c:c9	LOOP	Reply
14	7.067603	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
15	7.068131	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
16	8.000126	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
17	9.975700	Cisco_9f:6c:c9	CDP/VTP/DTP/PAgP/U	DTP	Dynamic Trunking Protocol
18	10.000134	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =

Examinez les paquets de la liste ci-dessus, notamment les paquets 6, 7, 8, 9, 11, 12, 14 et 15.

Localisez les paquets équivalents au sein de la liste de paquets affichée sur votre ordinateur.
Si vous avez effectué l'étape 1A ci-dessus, faites le lien entre les messages affichés dans la fenêtre de ligne de commande suite à l'envoi de la commande ping et les six paquets capturés par Wireshark.

Observez la liste des paquets de Wireshark et répondez aux questions suivantes :

Quel protocole est utilisé avec la commande ping ? _____

Quel est le nom complet du protocole ? _____

Quels sont les noms des deux messages ping ? _____

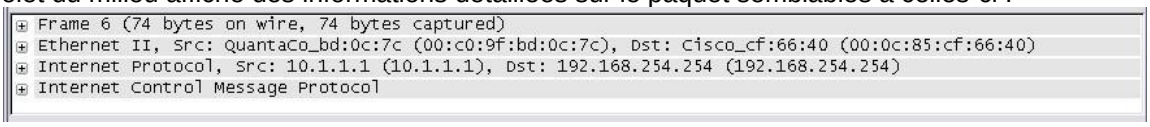
_____

Vous attendiez-vous à obtenir les adresses IP source et de destination indiquées ? Oui/Non

Pourquoi ? _____

Étape 3 : sélection (mise en surbrillance) du premier paquet de requête d'écho de la liste à l'aide de la souris

Le volet du milieu affiche des informations détaillées sur le paquet semblables à celles-ci :



Cliquez sur les quatre signes « **+** » pour développer les arborescences correspondantes.

Le volet se présente alors comme suit :

```
Frame 6 (74 bytes on wire, 74 bytes captured)
    Arrival Time: Jan 10, 2007 01:54:07.860436000
    [Time delta from previous packet: 0.000017000 seconds]
    [Time since reference or first frame: 4.073626000 seconds]
    Frame Number: 6
    Packet Length: 74 bytes
    Capture Length: 74 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp]
Ethernet II, Src: QuantaCo_bd:0c:7c (00:c0:9f:bd:0c:7c), Dst: Cisco_cf:66:40 (00:0c:85:cf:66:40)
  Destination: Cisco_cf:66:40 (00:0c:85:cf:66:40)
  Source: QuantaCo_bd:0c:7c (00:c0:9f:bd:0c:7c)
    Type: IP (0x0800)
Internet Protocol, Src: 10.1.1.1 (10.1.1.1), Dst: 192.168.254.254 (192.168.254.254)
    Version: 4
    Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 60
    Identification: 0x0bf7 (3063)
  Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (0x01)
  Header checksum: 0x6421 [correct]
    Source: 10.1.1.1 (10.1.1.1)
    Destination: 192.168.254.254 (192.168.254.254)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x2a5c [correct]
    Identifier: 0x0300
    Sequence number: 0x2000
```

Comme vous pouvez le constater, vous pouvez développer encore chaque section et protocole. Consacrez un peu de temps à l'étude de ces informations. Il se peut que vous ne compreniez pas toutes les informations affichées à ce stade du cours, mais notez toutefois celles que vous reconnaissez.

Localisez les deux types de « Source » et « Destination » différents. Pourquoi y en a-t-il deux ?

_____

Quels sont les protocoles inclus dans la trame Ethernet ?

_____

Lorsque vous sélectionnez une ligne dans ce volet, tout ou partie des informations correspondantes sont mises en surbrillance dans le volet inférieur des octets associés aux paquets.

Par exemple, si vous sélectionnez la deuxième ligne (+ Ethernet II) dans le volet du milieu, les valeurs correspondantes sont mises en surbrillance dans le volet inférieur.

```
0000  00 0c 85 cf 66 40 00 c0  9f bd 0c 7c 08 00 45 00   ....f@.. ...|..E.
0010  00 3c 0b f7 00 00 80 01  64 21 0a 01 01 01 c0 a8   .<...... d!......
0020  fe fe 08 00 2a 5c 03 00  20 00 61 62 63 64 65 66   ....*\.. .abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```

Il s'agit des valeurs binaires spécifiques à ces informations concernant la PDU. Il n'est pas nécessaire de comprendre toutes ces informations en détail à ce stade du cours.

Étape 4 : sélection de l'élément Close (Fermer) dans le menu File (Fichier)

Lorsque ce message s'affiche, cliquez sur **Continue without Saving** (Poursuivre sans enregistrer).

Tâche 2 : capture des PDU associées à un processus FTP

Étape 1 : lancement de la capture des paquets

En supposant que Wireshark soit toujours en cours d'exécution suite aux étapes précédentes, cliquez sur l'option **Start** (Démarrer) du menu **Capture** de Wireshark pour lancer la capture des paquets.

Tapez **ftp 192.168.254.254** au niveau de la ligne de commande de l'ordinateur sur lequel Wireshark est exécuté.

Une fois la connexion établie, spécifiez l' ID utilisateur **anonymous** sans mot de passe.
Userid: **anonymous**
Password: <ENTRÉE>
Vous pouvez également utiliser l'ID utilisateur **cisco** et le mot de passe **cisco**.

Une fois connecté, tapez **`get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe`**, puis appuyez sur la touche <ENTRÉE>. Le processus de téléchargement du fichier à partir du serveur ftp démarre. Vous obtenez un résultat semblable à celui-ci :

```
C:\Documents and Settings\ccna1>ftp eagle-server.example.com
Connected to eagle-server.example.com.
 220 Welcome to the eagle-server FTP service.
User (eagle-server.example.com:(none)): anonymous
331 Please specify the password.
Password:<ENTRÉE>
230 Login successful.
ftp> get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for
pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe (6967072 bytes).
226 File send OK.
ftp: 6967072 bytes received in 0.59Seconds 11729.08Kbytes/sec.
```

Une fois le fichier téléchargé, tapez **quit :**

```
ftp> quit
221 Goodbye.
C:\Documents and Settings\ccna1>
```

Arrêtez ensuite la capture des PDU dans Wireshark.

Étape 2 : agrandissement du volet de la liste des paquets de Wireshark et passage en revue des PDU répertoriées

Localisez et notez les PDU associées au téléchargement du fichier.
Il s'agit des PDU issues du protocole TCP de la couche 4 et du protocole FTP de la couche 7.

Identifiez les trois groupes de PDU associés au transfert du fichier.

Si vous avez effectué l'étape ci-dessus, faites le lien entre les paquets et les messages et invites de la fenêtre de ligne de commande FTP.

Le premier groupe correspond à la phase de connexion au serveur.
Fournissez quelques exemples de messages échangés au cours de cette phase.

_____

Localisez et notez quelques exemples de messages échangés au cours de la deuxième phase, c'est-à-dire celle de la requête de téléchargement et du transfert de données.

_____

_____

Le troisième groupe de PDU se rapporte à la déconnexion.
Fournissez quelques exemples de messages échangés au cours de cette phase.

_____

_____

Localisez les échanges TCP récurrents au cours du processus FTP. Quels types d'opérations TCP indiquent-ils ?

_____

_____

Étape 3 : analyse des informations détaillées sur les paquets

Sélectionnez (mettez en surbrillance) un paquet de la liste associé à la première phase du processus FTP.
Observez ses détails dans le volet du milieu.

Quels sont les protocoles encapsulés dans la trame ?

_____

Sélectionnez les paquets contenant le nom d'utilisateur et le mot de passe.
Examinez la partie mise en surbrillance dans le volet des octets.

Que pouvez-vous en déduire sur la sécurité de ce processus de connexion FTP ?

_____

Sélectionnez un paquet associé à la deuxième phase.

À partir de n'importe quel volet, localisez le paquet comportant le nom du fichier.

Le nom de fichier est : _____

Sélectionnez un paquet comportant le contenu du fichier ; notez le texte brut visible dans le volet des octets.

Dans les volets des informations détaillées et des octets, sélectionnez puis examinez quelques paquets échangés au cours de la troisième phase correspondant au téléchargement du fichier.
Qu'est-ce qui différencie le contenu de ces paquets ?

_____

Une fois terminé, fermez le fichier Wireshark en choisissant l'option Continue without Saving (Poursuivre sans enregistrer).

Tâche 3 : capture des PDU associées à un processus HTTP

Étape 1 : lancement de la capture des paquets

En supposant que Wireshark soit toujours en cours d'exécution suite aux étapes précédentes, cliquez sur l'option **Start** (Démarrer) du menu **Capture** de Wireshark pour lancer la capture des paquets.

Remarque : vous n'avez pas besoin de définir les options de capture si vous effectuez cette étape à la suite des étapes précédentes de cette session de travaux pratiques.

Ouvrez un navigateur Web sur l'ordinateur sur lequel vous exécutez Wireshark.
Saisissez l'URL du serveur Eagle de **example.com** ou bien l'adresse IP 192.168.254.254. Une fois la page Web téléchargée dans son intégralité, arrêtez la capture des paquets dans Wireshark.

Étape 2 : agrandissement du volet de la liste des paquets de Wireshark et passage en revue des PDU répertoriées

Localisez et identifiez les paquets TCP et HTTP associés au téléchargement de la page Web.

Notez les similarités qui existent entre cet échange de messages et celui du processus FTP.

Étape 3 : mise en surbrillance d'un paquet HTTP du volet supérieur portant la mention « (text/html) » au niveau de la colonne Info

Dans le volet des détails de paquet (volet du milieu), cliquez sur le signe « + » situé en regard de **Line-based text data: html**"
Quel type d'informations s'affiche-t-il lorsque vous développez cet élément ?

_____

Examinez la partie mise en surbrillance dans le volet des octets.
Elle indique les données HTML transportées par le paquet.

Une fois terminé, fermez le fichier Wireshark en choisissant l'option Continue without Saving (Poursuivre sans enregistrer).

Tâche 4 : réflexion

Examinez les informations d'encapsulation relatives aux données réseau capturées fournies par Wireshark. Faites-les correspondre aux modèles de couche TCP/IP et OSI. Il est important que vous puissiez reconnaître et associer les deux protocoles représentés et les ///types de couche de protocole et d'encapsulation des modèles aux informations fournies par Wireshark.

Tâche 5 : travaux pratiques avancés

Discutez de l'utilité des analyseurs de protocoles tels que Wireshark dans le cadre des opérations suivantes :

(1) Résolution d'un problème de téléchargement de page Web sur le navigateur d'un ordinateur

et

(2) Identification du trafic des données demandées par les utilisateurs sur un réseau

_____

_____

_____

_____

_____

_____

_____

Tâche 6 : nettoyage

Sauf indication contraire de la part du formateur, quittez Wireshark et arrêtez votre ordinateur de façon appropriée.

2.7.1 : exercice d'intégration des compétences : analyse des paquets IP

Diagramme de topologie

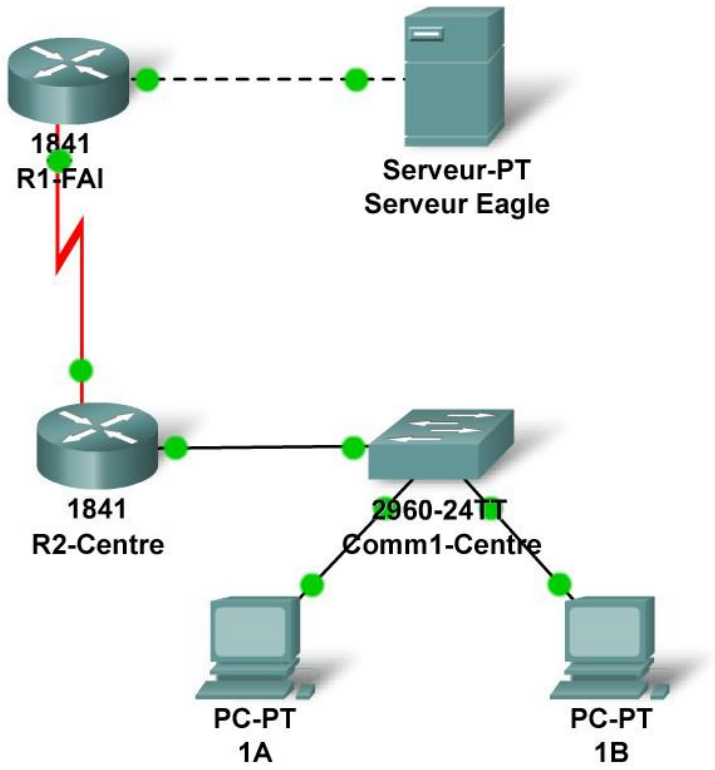


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	Fa0/0	192.168.254.253	255.255.255.0	N/A
	S0/0/0	10.10.10.6	255.255.255.252	N/A
R2-Central	Fa0/0	172.16.255.254	255.255.0.0	N/A
	S0/0/0	10.10.10.5	255.255.255.252	N/A
S1-Central	VLAN 1	172.16.254.1	255.255.0.0	172.16.255.254
PC 1A	La carte réseau	172.16.1.1	255.255.0.0	172.16.255.254
PC 1B	La carte réseau	172.16.1.2	255.255.0.0	172.16.255.254
Serveur Eagle	La carte réseau	192.168.254.254	255.255.255.0	192.168.254.253

Objectifs pédagogiques

- Compléter la topologie
- Ajouter des unités de données de protocole (ou PDU) simples en mode Realtime
- Analyser des unités de données de protocole en mode simulation
- Faire des expériences avec le modèle de configuration de travaux pratiques type

Contexte

Tout au long de ce cours, vous allez utiliser une configuration de travaux pratiques type constituée de PC, de serveurs, de routeurs et de commutateurs réels pour apprendre des concepts liés aux réseaux. Dans cet exercice, vous allez apprendre à créer et à analyser cette topologie standard. Si ce n'est déjà fait, nous vous invitons à examiner les fichiers d'aide accessibles depuis le menu déroulant Help situé dans la partie supérieure de l'interface graphique utilisateur de Packet Tracer. Ils contiennent des ressources utiles, telles que des travaux pratiques intitulés « My First PT Lab » destinés à vous apprendre les rudiments de Packet Tracer, des didacticiels visant à vous aider à effectuer diverses tâches, ainsi que des indications sur les avantages et les limites liés à l'utilisation de Packet Tracer pour la modélisation de réseaux.

Dans cet exercice, vous pourrez analyser la configuration de base en utilisant le simulateur Packet Tracer. Packet Tracer peut créer deux formats de fichiers : des fichiers .pkt (fichiers modèles de simulation de réseau) et des fichiers .pka (fichiers d'exercice pour la mise en pratique). Lorsque vous créerez vos propres réseaux dans Packet Tracer ou que vous modifierez des fichiers existants créés par votre formateur ou vos collègues, vous utiliserez généralement le format de fichier .pkt. Lorsque vous avez débuté cet exercice dans le cadre du cursus, ces instructions vous ont été présentées. Elles résultent du .pka, le format de fichier d'exercice Packet Tracer. Au bas de ces instructions figurent deux boutons : Check Results (qui indique votre état d'avancement dans l'exercice) et Reset Activity (qui vous permet de reprendre l'exercice au début dans le cas vous souhaiteriez effacer votre travail ou acquérir davantage de pratique).

Tâche 1 : compléter la topologie

Ajoutez un PC à l'espace de travail. Configurez-le avec les paramètres suivants : adresse IP 172.16.1.2, masque de sous-réseau 255.255.0.0, passerelle par défaut 172.16.255.254, serveur DNS 192.168.254.254, nom complet « 1B » (sans les guillemets). Reliez le PC 1B au port Fa0/2 du commutateur S1-Central et vérifiez votre travail à l'aide du bouton **Check Results** pour déterminer si la topologie est finalisée.

Tâche 2 : ajout d'unités de données de protocole (ou PDU) simples en mode Realtime

À l'aide de la fonction Add Simple PDU, envoyez un message de test : un message entre le PC 1B et Eagle Server. Sachez que ce paquet apparaîtra dans la liste d'événements comme un élément « détecté » ou « reniflé » sur le réseau et dans la partie inférieure droite comme PDU créée par l'utilisateur et pouvant être manipulée à des fins de test.

Tâche 3 : analyse des unités de données de protocole en mode Simulation (Packet Tracer)

Passez en mode Simulation. Double-cliquez sur le bouton « Fire » dans la fenêtre User Created PDU. Utilisez le bouton **Capture / Forward** pour déplacer le paquet sur le réseau. Pour examiner le paquet à chaque étape de son trajet, cliquez sur l'enveloppe du paquet ou sur le carré de couleur figurant dans la colonne Info de la liste d'événements.

Tâche 4 : expériences à partir du modèle de configuration de travaux pratiques type

La configuration de travaux pratiques type se compose de deux routeurs, d'un commutateur, d'un serveur et de deux PC. Essayez de créer différentes combinaisons de paquets de test et d'analyser leur trajet sur le réseau.

Remarques générales

Si ce n'est déjà fait, nous vous recommandons de vous procurer Packet Tracer auprès de votre formateur et d'effectuer les travaux pratiques « My First PT Lab » (accessibles depuis le menu déroulant HELP via l'option CONTENTS).

Exercice 3.4.1 : capture de flux de données

Objectifs pédagogiques

À la fin de cet exercice, vous saurez :

- capturer ou télécharger un flux audio ;
- enregistrer les caractéristiques du fichier ;
- examiner les taux de transfert de données associés au fichier.

Contexte

Lorsque vous créez un fichier dans une application, vous devez stocker les données de ce fichier à un emplacement. Vous pouvez choisir de les stocker sur le périphérique final utilisé lors de leur création ou de les transférer vers un autre périphérique.

Cet exercice présente comment capturer un flux audio à l'aide d'un microphone et de l'outil Magnétophone de Microsoft. L'outil Magnétophone est un accessoire Windows disponible sous Windows XP. Pour y accéder, sélectionnez **Démarrer > Programmes > Accessoires > Divertissement > Magnétophone**. Si vous ne disposez ni d'un microphone ni de l'outil Magnétophone, téléchargez un fichier audio sur le site http://newsroom.cisco.com/dlls/podcasts/audio_feeds.html afin d'effectuer cet exercice.

Scénario

Pour pouvoir réaliser cet exercice, vous devez disposer d'un ordinateur équipé d'un microphone et sur lequel l'outil Magnétophone est installé ou d'un accès à Internet afin de pouvoir télécharger un fichier audio.

L'exercice prend environ 30 minutes, selon le débit réseau.

Tâche 1 : création d'un fichier audio

Étape 1 : ouverture de l'application Windows Magnétophone.

Cette application est disponible sous Windows XP. Pour y accéder, sélectionnez **Démarrer > Programmes >Accessoires > Divertissement > Magnétophone**. L'interface de Magnétophone se présente comme illustré à la figure 1.

Figure 1. Interface de Magnétophone

Étape 2 : enregistrement d'un fichier audio.

1. Pour commencer à enregistrer, cliquez sur le bouton d'enregistrement disponible sur l'interface de l'application Magnétophone.
2. Parlez dans le microphone ou créez des sons que le microphone peut détecter. Au fur et à mesure de l'enregistrement du son, une onde sonore s'affiche sur l'interface de l'application, comme illustré à la figure 2.

Figure 2. Enregistrement en cours

3. Une fois terminé, cliquez sur le bouton d'arrêt.

Étape 3 : vérification du fichier audio enregistré.

1. Appuyez sur le bouton Lire pour écouter l'enregistrement. L'enregistrement effectué est alors lu, comme illustré à la figure 3.

Figure 3. Lecture de l'enregistrement

Si vous n'entendez pas l'enregistrement, vérifiez la configuration du microphone et des haut-parleurs, ainsi que le réglage du volume, puis procédez à un nouvel enregistrement.

Si vous ne parvenez pas à réaliser un enregistrement, téléchargez un fichier audio à partir du site Web News@Cisco, à l'adresse suivante : http://newsroom.cisco.com/dlls/podcasts/audio_feeds.html

2. Enregistrez le fichier audio sur le bureau, puis passez à la tâche 2.

Étape 4 : enregistrement du fichier audio.

1. Enregistrez le fichier audio que vous avez créé dans le bureau. Nommez le fichier **monaudio.wav**.
2. Une fois le fichier enregistré, fermez l'application Magnétophone.

Tâche 2 : observation des propriétés du fichier audio

Étape 1 : affichage des propriétés du fichier audio.

Cliquez avec le bouton droit de la souris sur le fichier audio enregistré sur le bureau, puis cliquez sur **Propriétés** dans le menu contextuel qui s'affiche.

Quelle est la taille du fichier en kilo-octets ? _____
Quelle est la taille du fichier en octets ? _____

Quelle est la taille du fichier en bits ? _____

Étape 2 : ouverture du fichier audio dans l'application Lecteur Windows Media.

1. Cliquez avec le bouton droit de la souris sur le fichier audio, puis sélectionnez **Ouvrir avec > Lecteur Windows Media**.
2. Une fois le fichier ouvert, cliquez avec le bouton droit de la souris dans la partie supérieure de l'interface de Lecteur Windows Media, puis sélectionnez **Fichier > Propriétés** dans le menu contextuel qui s'affiche.

Quelle est la durée du fichier audio en secondes ? _____

Calculez la quantité de données par seconde du fichier audio, puis enregistrez le résultat.

_____

Tâche 3 : Remarques générales

Les fichiers de données ne doivent pas nécessairement se trouver sur les périphériques finaux utilisés lors de leur création. Par exemple, vous pouvez copier le fichier audio créé sur un autre ordinateur ou un périphérique audio portable.

Imaginons que le fichier audio enregistré sur le bureau soit transféré à un taux de 100 mégabits par seconde (Mbits/s). Combien de temps faudrait-il pour transférer le fichier dans son intégralité ?

__ _____

Même si vous disposez d'une connexion Ethernet à 100 Mbits/s, les données du fichier ne sont pas transférées à cette vitesse. Toutes les trames Ethernet comportent d'autres informations nécessaires à la transmission, telles que les adresses de la source et de la destination.

Si ces informations Ethernet complémentaires prennent 5 % de la bande passante de 100 Mbits/s et qu'il reste 95 % de disponible pour la transmission des données utiles, combien de temps faut-il pour transférer un fichier dans son intégralité ?

___ _____

Tâche 4 : nettoyage

Vous devrez peut-être supprimer le fichier audio enregistré sur l'ordinateur. Si tel est le cas, supprimez-le du bureau.

Sauf indication contraire, éteignez votre ordinateur.

Travaux pratiques 3.4.2 : gestion d'un serveur Web

Schéma de la topologie

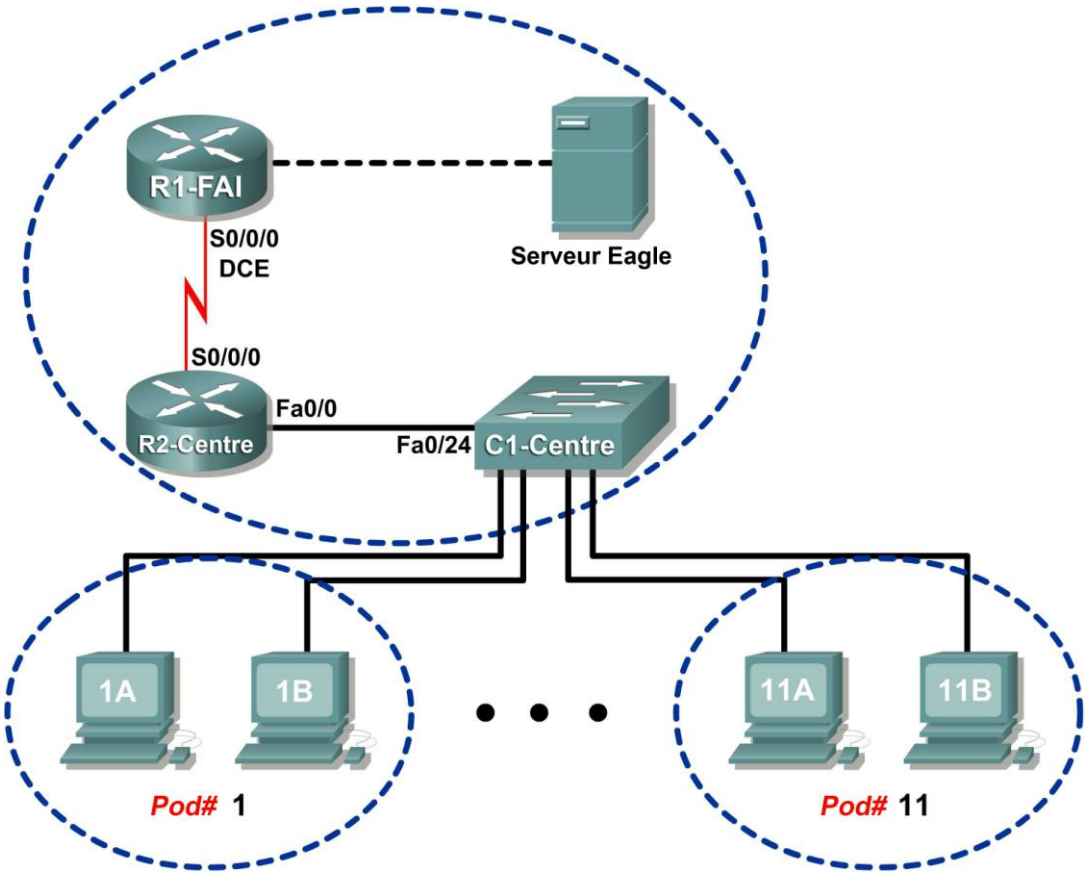


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	**S0/0/0**	10.10.10.6	255.255.255.252	N/D
	Fa0/0	192.168.254.253	255.255.255.0	N/D
R2-Central	**S0/0/0**	10.10.10.5	255.255.255.252	N/D
	Fa0/0	172.16.255.254	255.255.0.0	N/D
Eagle Server	**N/D**	192.168.254.254	255.255.255.0	192.168.254.253
	N/D	172.31.24.254	255.255.255.0	N/D
hôteA	**N/D**	172.16..1	255.255.0.0	172.16.255.254
hôteB	**N/D**	172.16..2	255.255.0.0	172.16.255.254
S1-Central	**N/D**	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- télécharger, installer et vérifier une application de serveur Web ;
- vérifier le fichier de configuration du serveur Web par défaut ;
- capturer et analyser le trafic HTTP à l'aide de Wireshark.

Contexte

Les serveurs Web sont une partie importante du plan commercial de toute entreprise présente sur Internet. Les navigateurs Web sont utilisés par les clients pour accéder aux sites Web professionnels. Cependant, ils ne constituent que la moitié de la chaîne de communication. L'autre moitié de la chaîne de communication est représentée par la prise en charge du serveur Web. La prise en charge du serveur Web est une compétence importante pour tout administrateur réseau. D'après un sondage Netcraft mené en janvier 2007, la table suivante indique les trois premières applications de serveur Web par pourcentage d'utilisation :

Serveur Web	Pourcentage d'utilisation
Apache	60 %
Microsoft	31 %
Sun	1.6 %

Scénario

Dans ces travaux pratiques, vous allez télécharger, installer et configurer le serveur Web Apache. Un navigateur Web sera utilisé pour établir la connexion au serveur et Wireshark sera utilisé pour capturer la communication. L'analyse de la capture vous permettra de comprendre le mode de fonctionnement du protocole HTTP.

Tâche 1 : téléchargement, installation et vérification du serveur Web Apache.

Les travaux pratiques doivent être configurés comme illustré dans le schéma de topologie et dans la table d'adressage logique. Si ce n'est pas le cas, demandez de l'aide auprès de votre formateur.

Étape 1 : téléchargement du logiciel depuis Eagle Server.

L'application de serveur Web Apache peut être téléchargée à partir d'Eagle Server.

1. Utilisez un navigateur Web et l'URL `ftp://eagle-server.example.com/pub/eagle labs/eagle1/chapter3` pour accéder au / télécharger le logiciel. Reportez-vous à la figure 1.

Figure 1. Écran de téléchargement de l'application du serveur Web Apache sur FTP

2. Cliquez avec le bouton droit de la souris sur le fichier et enregistrer le logiciel dans l'ordinateur hôte pod.

Étape 2 : installation du serveur Web Apache sur l'ordinateur hôte pod.

1. Ouvrez le dossier où a été enregistré le logiciel, puis double-cliquez sur le fichier Apache pour commencer l'installation. Choisissez les valeurs par défaut et acceptez l'accord de licence. La prochaine étape de l'installation nécessite de personnaliser la configuration du serveur Web, illustrée dans la figure 2.

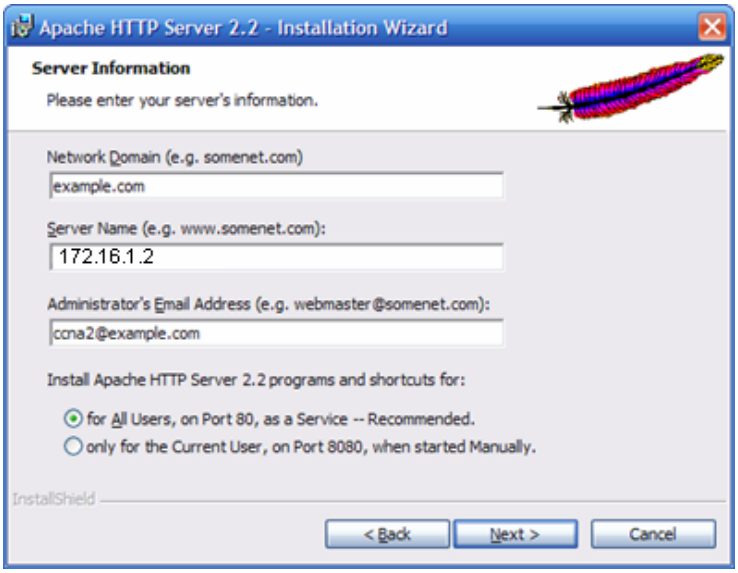


Figure 2. Écran Configuration personnalisée

Utilisez les valeurs suivantes :

Informations	Valeur
Domaine réseau	example.com
Nom du serveur	Adresse IP de l'ordinateur
Adresse électronique de l'administrateur	ccna*@example.com

* Par exemple, pour les utilisateurs 1 à 22, si l'ordinateur se trouve sur l'hôte B du pod 5, le numéro de l'adresse électronique de l'administrateur est ccna10@example.com

2. Acceptez le port et l'état de service recommandés. Cliquez sur **Suivant**.
3. Acceptez l'installation type par défaut, puis cliquez sur **Suivant**.

Quel est le dossier d'installation par défaut ?

_____

4. Acceptez le dossier d'installation par défaut, cliquez sur **Suivant**, puis sur **Installer**. Une fois l'installation terminée, fermez l'écran.

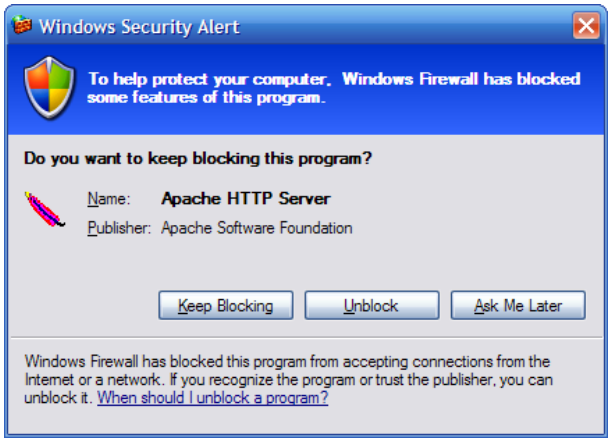


Figure 3. Alerte de sécurité Windows

Remarque : si une alerte de sécurité Windows s'affiche, sélectionnez Débloquer. Reportez-vous à la figure 3. Vous autoriserez ainsi les connexions au serveur Web.

Étape 3 : vérification du serveur Web.

La commande **`netstat`** affiche les statistiques de protocole et les informations de connexion de cet ordinateur de travaux pratiques.

1. Choisissez **Démarrer > Exécuter**, puis ouvrez une fenêtre de ligne de commande. Saisissez **cmd**, puis cliquez sur **OK**. Utilisez la commande **`netstat -a`** pour connaître les ports ouverts et connectés de votre ordinateur :

```
C:\>netstat -a
Connexions actives

Proto  : Adresse locale                 Adresse distante       Etat
TCP      GW-desktop-hom:http            GW-desktop-hom:0       LISTENING
TCP      GW-desktop-hom:epmap           GW-desktop-hom:0       LISTENING
TCP      GW-desktop-hom:microsoft-ds    GW-desktop-hom:0       LISTENING
TCP      GW-desktop-hom:3389            GW-desktop-hom:0       LISTENING
<output omitted>
C:\>
```

2. À l'aide de la commande **`netstat -a`**, vérifiez si le serveur Web fonctionne correctement sur l'ordinateur hôte pod.

   L'icône de contrôle du serveur Web Apache doit s'afficher dans le coin inférieur droit de l'écran, à proximité de l'horloge.

3. Ouvrez un navigateur Web, puis établissez la connexion avec l'URL de votre ordinateur. Une page Web identique à celle illustrée dans la figure 4 s'affiche si le serveur Web fonctionne correctement.

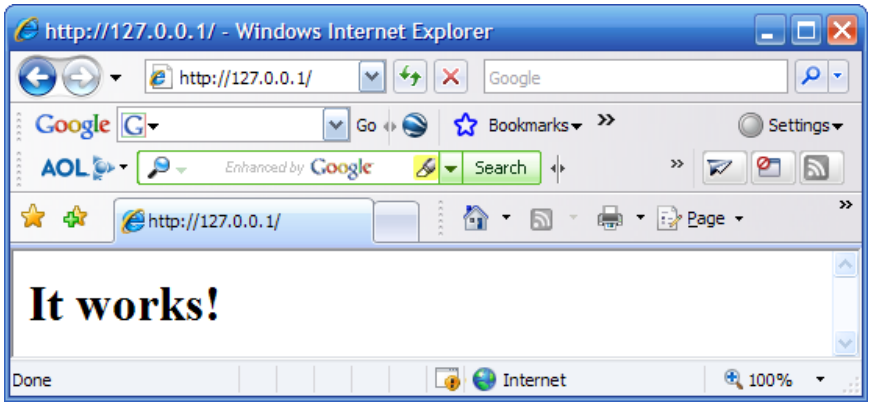


Figure 4. Page par défaut du serveur Web

L'adresse réseau 127.0.0.0 / 8 est réservée et utilisée pour les adresses IP locales. La même page doit s'afficher si l'URL devient l'adresse IP de l'interface Ethernet ou une adresse IP d'hôte de la plage de réseaux 127.0.0.0 / 8.

4. Testez le serveur Web avec plusieurs adresses IP de la plage de réseaux 127.0.0.0 / 8. Insérez les résultats dans la table suivante :

Adresse IP	État	Explication
127.0.0.1		
127.255.255.254		
127.255.255.255		
127.0.0.0		

Tâche 2 : vérification du fichier de configuration du serveur Web par défaut.

Étape 1 : accès au fichier `httpd.conf`.

Un administrateur système peut avoir besoin de vérifier ou de modifier le fichier de configuration par défaut.

Ouvrez le fichier de configuration du serveur Web Apache (C:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf). Reportez-vous à la figure 5.

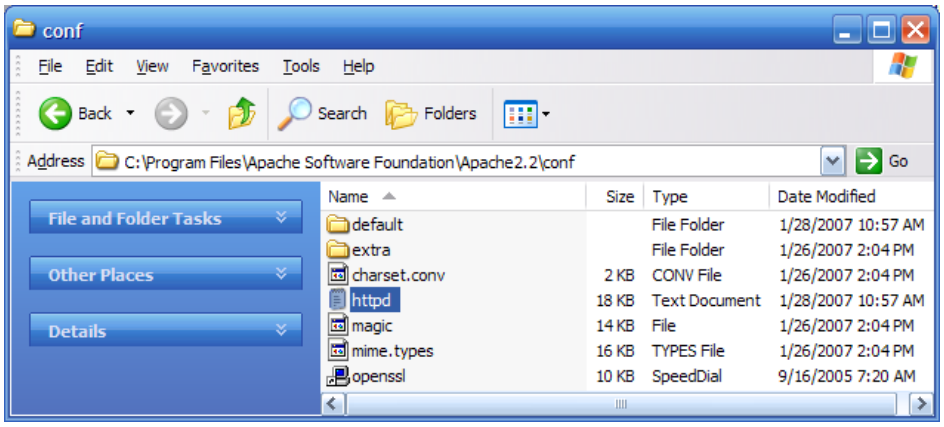


Figure 5. Fichier de configuration du serveur Web Apache

Étape 2 : examen du fichier `httpd.conf`.

De nombreux paramètres de configuration permettent de personnaliser en profondeur le serveur Web Apache. Le caractère « # » indique un commentaire destiné aux administrateurs système, exemptés d'accès au serveur Web. Faites défiler le fichier de configuration, puis vérifiez les paramètres suivants :

Valeur	Signification
`#Listen 12.34.56.78:80` `Listen 80`	Écoute du port TCP 80 pour toutes les connexions entrantes. Pour n'accepter que les connexions de cet hôte, définissez la ligne `Listen 127.0.0.1 80`.
`ServerAdmin ccna2@example.com`	En cas de problème, envoyez un courriel à l'adresse suivante.
`ServerName 172.16.1.2:80`	Pour les serveurs sans noms DNS, utilisez Adresse IP:numéro de port
`DocumentRoot "C:/Program Files/Apache Software Foundation/Apache2.2/htdocs"`	Répertoire racine du serveur Web.

`<IfModule dir_module>`
`DirectoryIndex index.html`
`</IfModule>`
	`DirectoryIndex` définit le fichier qu'Apache servira si un répertoire est demandé. Si aucune page n'est demandée depuis ce répertoire, affichez `index.html` s'il est présent.

Étape 3 : modification de la page par défaut du serveur Web.

La figure 4 illustre la page Web par défaut du fichier index.html. Bien que cette page suffise au test, vous devez afficher des données plus personnelles.

1. Ouvrez le dossier C:\Program Files\Apache Software Foundation\Apache2.2\htdocs. Le fichier index.html doit s'y trouver. Cliquez avec le bouton droit de la souris sur le fichier, puis

sélectionnez **Ouvrir avec**. Dans la liste déroulante, sélectionnez **Bloc-notes**. Définissez le contenu de la liste de telle manière qu'elle ressemble à l'exemple suivant :

```
<html><body><h1>Welcome to the Pod1HostB Web Server!!!</h1>
<center><bold>
Operated by me!
</center></bold>
Contact web administrator: ccna2@example.com
</body></html>
```

2. Enregistrez le fichier, puis actualisez le navigateur Web. Vous pouvez sinon ouvrir l'URL http://127.0.0.1. La nouvelle page par défaut doit s'afficher. Une fois les modifications effectuées et enregistrées dans index.html, actualisez le navigateur Web afin de visualiser le nouveau contenu.

Tâche 3 : capture et analyse du trafic HTTP à l'aide de Wireshark.

Wireshark ne capturera pas les paquets envoyés depuis / vers le réseau 127.0.0.0 sur un ordinateur Windows. L'interface ne s'affichera pas. Pour effectuer cette tâche, connectez-vous à l'ordinateur d'un participant ou à Eagle Server, puis analysez l'échange des données.

Étape 1 : analyse du trafic HTTP.

1. Démarrez Wireshark, puis définissez l'interface liée au réseau 172.16 comme interface de capture. Ouvrez un navigateur Web, puis connectez-vous à un autre ordinateur à l'aide d'un serveur Web actif.

Pourquoi le fichier index.html ne doit-il *pas* être saisi dans l'URL pour afficher le contenu du fichier ?

_____

2. Entrez volontairement une page Web qui ne se trouve pas sur le serveur Web, comme illustré à la figure 6. Notez qu'un message d'erreur s'affiche dans le navigateur Web.

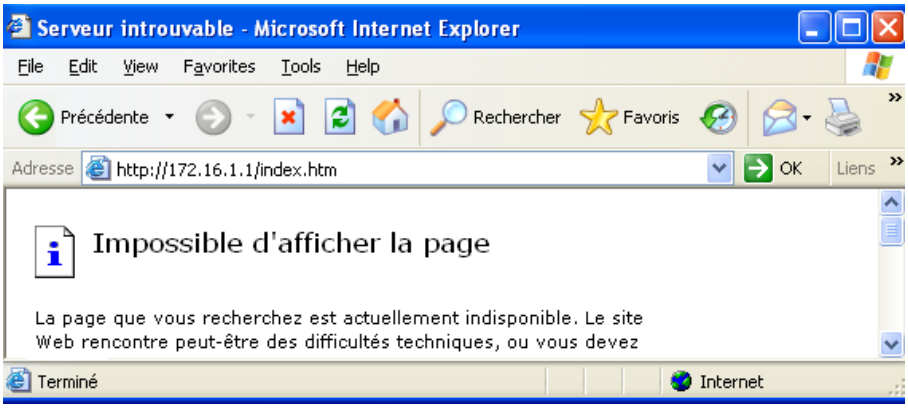
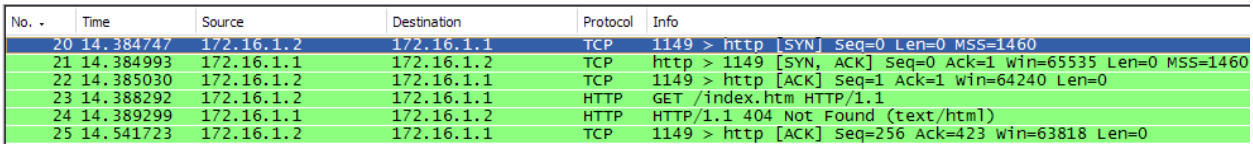


Figure 6. Erreur 404 Page introuvable

La figure contient une session HTTP capturée. Le fichier index.htm a été demandé depuis le serveur Web, mais le serveur ne disposait pas du fichier. Le serveur a renvoyé une erreur **404**. Le navigateur Web a simplement affiché « Page introuvable ».



No.	Time	Source	Destination	Protocol	Info
20	14.384747	172.16.1.2	172.16.1.1	TCP	1149 > http [SYN] Seq=0 Len=0 MSS=1460
21	14.384993	172.16.1.1	172.16.1.2	TCP	http > 1149 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
22	14.385030	172.16.1.2	172.16.1.1	TCP	1149 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
23	14.388292	172.16.1.2	172.16.1.1	HTTP	GET /index.htm HTTP/1.1
24	14.389299	172.16.1.1	172.16.1.2	HTTP	HTTP/1.1 404 Not Found (text/html)
25	14.541723	172.16.1.2	172.16.1.1	TCP	1149 > http [ACK] Seq=256 Ack=423 Win=63818 Len=0

Figure 7. Capture Wireshark du trafic HTTP

3. Sélectionnez la ligne de capture avec l'erreur 404, et déplacez-la dans la deuxième fenêtre Wireshark (celle du milieu). Développez l'enregistrement de données texte basé sur la ligne.

   Que contient-il ?

   _____

Tâche 4 : confirmation

Modifiez le fichier de configuration du serveur Web par défaut httpd.conf et remplacez la ligne `Listen 80` par `Listen 8080`. Ouvrez un navigateur Web et accédez à l'URL http://127.0.0.1:8080. À l'aide de la commande **`netstat`**, vérifiez que le nouveau port TCP du serveur est 8080.

Tâche 5 : Remarques générales

Les serveurs Web sont un composant important du commerce électronique. Selon l'entreprise, l'administrateur réseau ou Web est responsable de la maintenance du serveur Web de l'entreprise. Ces travaux pratiques ont démontré comment installer et configurer le serveur Web Apache, tester le fonctionnement et identifier les divers paramètres de configuration clés.

Le participant a modifié la page Web par défaut index.html et observé les résultats sur le navigateur Web.

Enfin, nous avons utilisé Wireshark pour capturer la session HTTP d'un fichier introuvable. Le serveur Web a renvoyé une erreur 404 HTTP 1.1 et le message « Fichier introuvable » au navigateur Web.

Tâche 6 : nettoyage

Lors de ces travaux pratiques, nous avons installé le serveur Web Apache sur l'ordinateur hôte pod. Il devrait être désinstallé. Pour désinstaller Wireshark, cliquez sur **Démarrer > Panneau de configuration > Ajout/Suppression de programmes**. Cliquez sur **Serveur Web Apache**, puis sur **Supprimer**.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

Travaux pratiques 3.4.3 : services et protocoles de messagerie

Schéma de la topologie

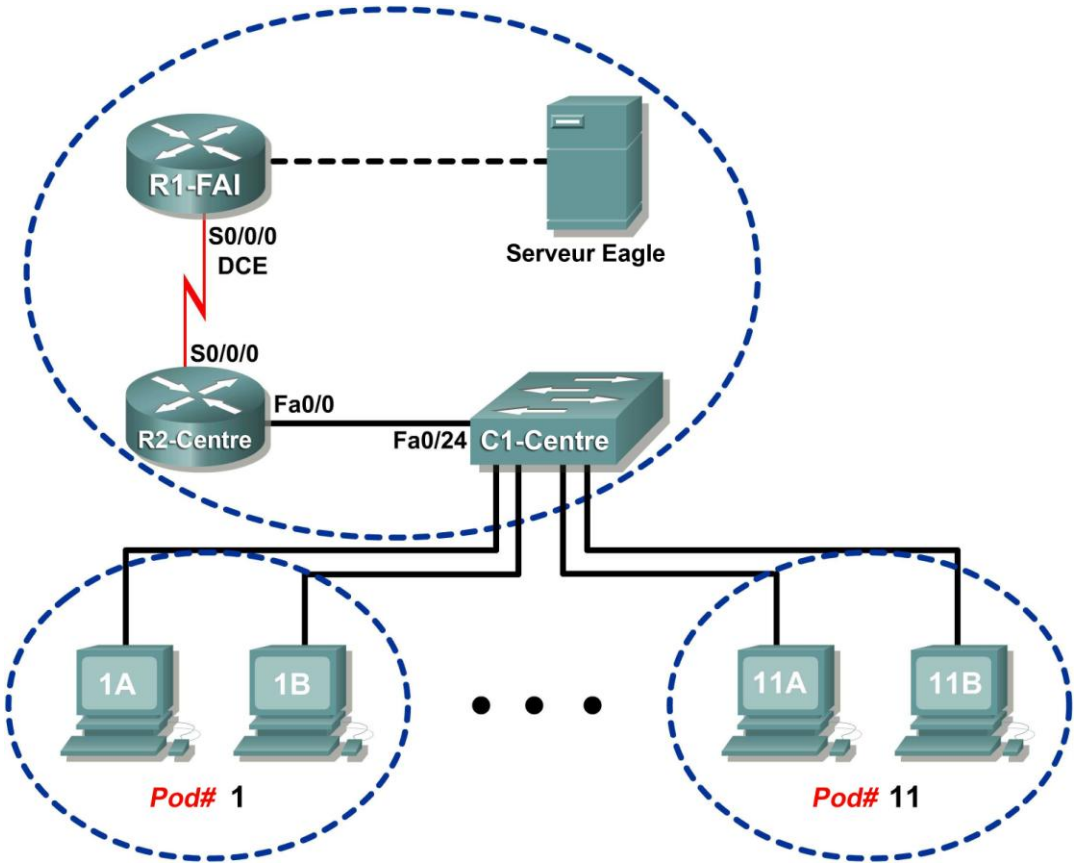


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/D
	Fa0/0	192.168.254.253	255.255.255.0	N/D
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/D
	Fa0/0	172.16.255.254	255.255.0.0	N/D
Eagle Server	N/D	192.168.254.254	255.255.255.0	192.168.254.253
	N/D	172.31.24.254	255.255.255.0	N/D
hôte*Pod#*A	N/D	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
hôte*Pod#*B	N/D	172.16. *Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	N/D	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- configurer l'ordinateur hôte pod du service de messagerie ;
- capturer et analyser la communication de messagerie électronique entre l'ordinateur hôte pod et un serveur de messagerie ;

Contexte

La messagerie électronique est l'un des services réseau les plus populaires utilisé par le modèle client/serveur. Le client de messagerie électronique est configuré sur l'ordinateur d'un utilisateur, puis configuré pour se connecter à un serveur de messagerie. La plupart des fournisseurs de services Internet donnent des instructions pas à pas pour utiliser des services de messagerie électronique. Par conséquent, l'utilisateur type peut ne pas être familiarisé aux complexités de la messagerie électronique ou des protocoles utilisés.

Dans les environnements réseau où le client MUA doit se connecter à un serveur de messagerie sur un autre réseau pour envoyer et recevoir les courriels, les deux protocoles suivants sont utilisés.

- Le protocole SMTP a été défini en août 1982 par la RFC 821 et a depuis fait l'objet de nombreuses modifications et améliorations. La RFC 2821 d'avril 2001 regroupe et met à jour les RFC précédents relatifs à la messagerie électronique. Le serveur SMTP écoute le port TCP 25. Il est utilisé pour envoyer les courriels du client de messagerie électronique au serveur de messagerie électronique, diffuser les courriels aux comptes locaux et les relayer entre les serveurs SMTP.
- Le protocole POPv3 (Post Office Protocol version 3) est utilisé lorsqu'un client de messagerie externe souhaite recevoir les courriels à partir du serveur de messagerie électronique. Le serveur POPv3 écoute le port TCP 110.

Les versions antérieures des deux protocoles ne doivent pas être utilisées. En outre, il existe des versions sécurisées des deux protocoles qui utilisent la technologie SSL/TSL dans le cadre de la communication.

Les courriels sont exposés à diverses vulnérabilités de sécurité informatique. Les attaques de courrier indésirable saturent les réseaux de courriels inutiles et non sollicités. Il en résulte une consommation excessive de la bande passante et des ressources réseau. Les serveurs de messagerie électronique ont connu de nombreuses vulnérabilités qui laissaient l'ordinateur exposé aux menaces.

Scénario

Dans ces travaux pratiques, vous utiliserez des applications de client de messagerie électronique pour vous connecter aux services réseau d'Eagle Server. Vous surveillerez les communications à l'aide du logiciel Wireshark et analyserez les paquets capturés.

Un client de messagerie électronique tel que Outlook Express ou Mozilla Thunderbird sera utilisé pour établir la connexion au service réseau d'Eagle Server. Les services de messagerie électronique SMTP d'Eagle Server sont préconfigurés avec des comptes utilisateur capables d'envoyer et de recevoir des courriels externes.

Tâche 1 : configuration de l'ordinateur hôte pod du service de messagerie.

Les travaux pratiques doivent être configurés comme illustré dans le schéma de topologie et dans la table d'adressage logique. Si ce n'est pas le cas, demandez de l'aide auprès de votre formateur.

Étape 1 : téléchargement et installation de Mozilla Thunderbird.

Si Thunderbird n'est pas installé sur l'ordinateur hôte pod, vous pouvez le télécharger à l'adresse eagle-server.example.com. Reportez-vous à la figure 1. L'URL de téléchargement est la suivante : `ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter3`.

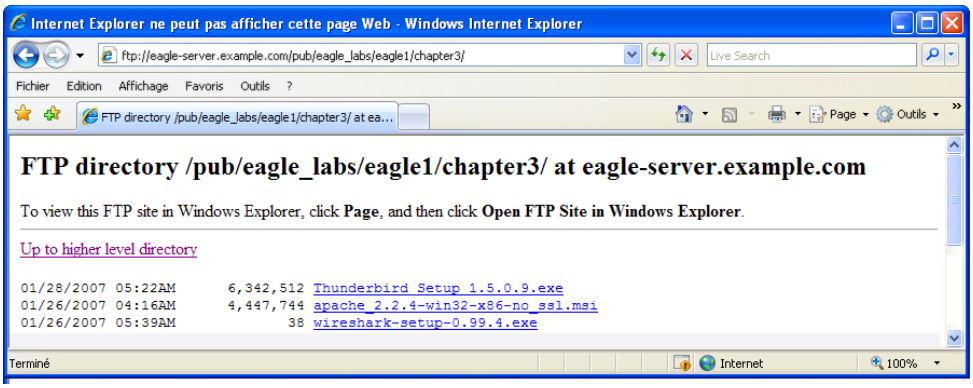


Figure 1. Page de téléchargement de Thunderbird sur FTP

1. Cliquez avec le bouton droit sur le nom de fichier de Thunderbird, puis enregistrez le fichier dans l'ordinateur hôte pod.
2. Une fois le fichier téléchargé, double-cliquez sur le nom de fichier et installez Thunderbird avec les paramètres par défaut.
3. Une fois terminé, démarrez Thunderbird.

Étape 2 : configuration de Thunderbird afin de recevoir et d'envoyer des courriels.

1. Au démarrage de Thunderbird, les paramètres de compte de messagerie doivent être configurés. Renseignez les informations du compte comme suit :

Champ	Valeur
Account Name (Nom du compte)	Le nom du compte se base sur l'ordinateur hôte pod. 22 comptes sont configurés sur Eagle Server, marqués ccna[1..22]. Si cet hôte pod se trouve sur l'hôte A de Pod1, le nom du compte est `ccna1`. Si cet hôte pod se trouve sur l'hôte B de Pod3, le nom du compte est `ccna6`. Etc.
Your Name (Nom)	Utilisez le même nom que ci-dessus.
E-mail Address (Adresse électronique)	*votre_nom*`@eagle-server.example.com`
Type de serveur entrant que vous utilisez	`POP`
Serveur entrant (SMTP)	`eagle-server.example.com`
Serveur sortant (SMTP)	`eagle-server.example.com`

2. Vérifiez les paramètres de compte dans **Tools > Account Settings (Outils > Paramètres de compte)**. Reportez-vous à la figure 2.

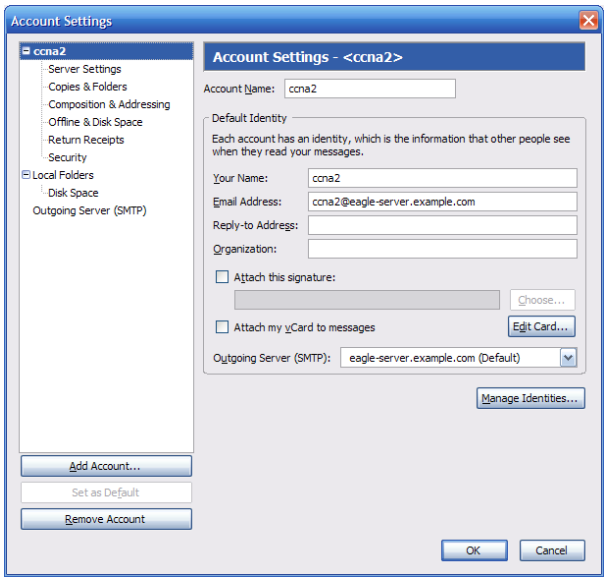


Figure 2. Paramètres de compte Thunderbird

3. Dans le panneau de gauche de l'écran Account Settings (Paramètres de compte), cliquez sur **Server Settings (Paramètres du serveur)**. Un écran semblable à celui de la figure 3 s'affiche.

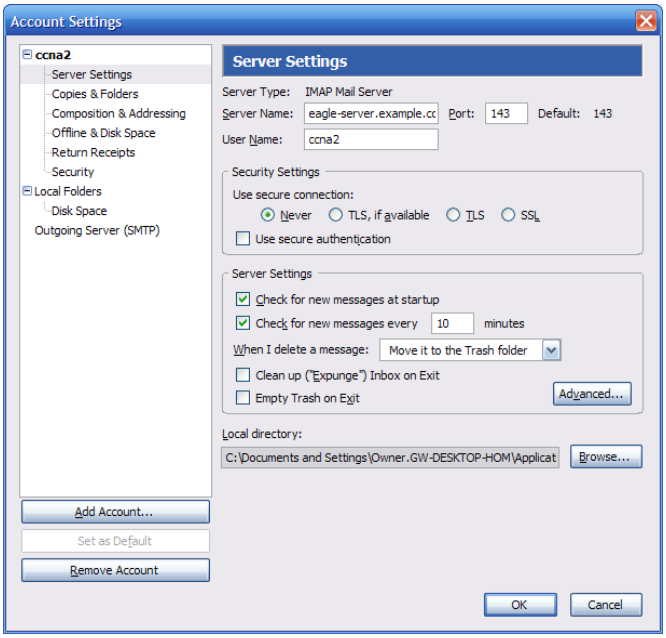


Figure3. Écran Server Settings (Paramètres du serveur) de Thunderbird

La figure 4 illustre une configuration correcte du serveur sortant (SMTP).

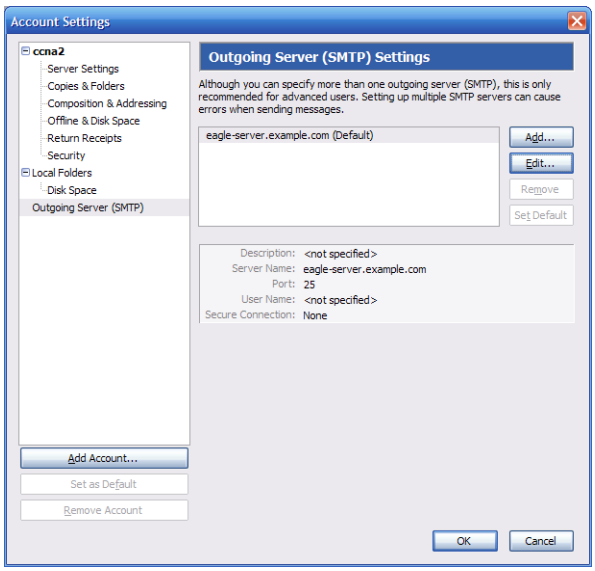


Figure 4. Écran Outgoing Server (SMTP) Settings (Paramètres du serveur sortant (SMTP)

Quelle est la fonction du protocole SMTP et quel est le numéro de port TCP bien connu ?

_____

_____

Tâche 2 : capture et analyse de la communication de messagerie électronique entre l'ordinateur hôte pod et un serveur de messagerie.

Étape 1 : envoi d'un courriel non capturé.

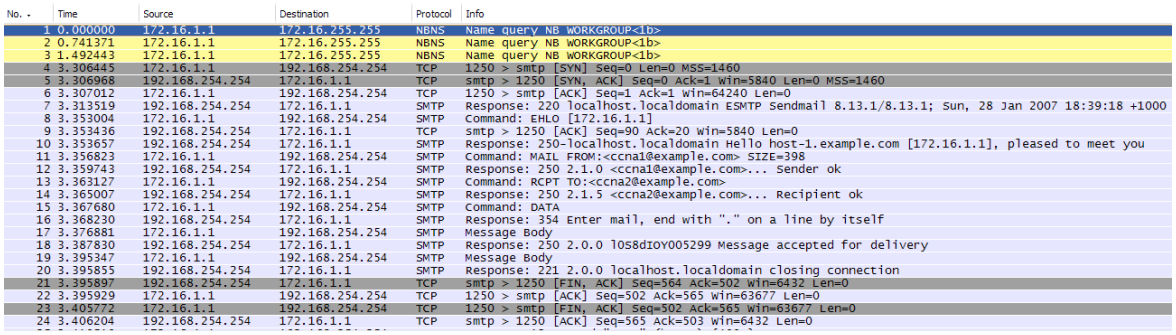
1. Demandez à un autre participant son nom de courriel.
2. Utilisez ce nom pour composer et envoyer un message amical au participant.

Étape 2 : lancement de la capture à l'aide de Wireshark.

Lorsque vous êtes certain du déroulement correct de l'opération en envoi et en réception, démarrez une capture Wireshark. Les résultats s'affichent par type de paquet.

Étape 3 : analyse d'une session de capture de protocole SMTP à l'aide de Wireshark

1. Utilisez à nouveau ce client de messagerie pour envoyer et recevoir un courriel à/d'un autre participant. Cette fois-ci, les transactions seront capturées.
2. Une fois un courriel envoyé et reçu, arrêtez la capture Wireshark. La figure 5 présente une capture partielle Wireshark d'un courriel sortant à l'aide de SMTP.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
2	0.741371	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
3	1.492443	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
4	3.306445	172.16.1.1	192.168.254.254	TCP	1250 > smtp [SYN] Seq=0 Len=0 MSS=1460
5	3.306968	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
6	3.307012	172.16.1.1	192.168.254.254	TCP	1250 > smtp [ACK] Seq=1 Ack=1 Win=64240 Len=0
7	3.313519	192.168.254.254	172.16.1.1	SMTP	Response: 220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13.1; Sun, 28 Jan 2007 18:39:18 +1000
8	3.353004	172.16.1.1	192.168.254.254	SMTP	Command: EHLO [172.16.1.1]
9	3.353436	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [ACK] Seq=90 Ack=20 Win=5840 Len=0
10	3.353657	192.168.254.254	172.16.1.1	SMTP	Response: 250-localhost.localdomain Hello host-1.example.com [172.16.1.1], pleased to meet you
11	3.356823	172.16.1.1	192.168.254.254	SMTP	Command: MAIL FROM:<ccna1@example.com> SIZE=398
12	3.359743	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.1.0 <ccna1@example.com>... Sender ok
13	3.363127	172.16.1.1	192.168.254.254	SMTP	Command: RCPT TO:<ccna2@example.com>
14	3.365007	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.1.5 <ccna2@example.com>... Recipient ok
15	3.367680	172.16.1.1	192.168.254.254	SMTP	Command: DATA
16	3.368230	192.168.254.254	172.16.1.1	SMTP	Response: 354 Enter mail, end with "." on a line by itself
17	3.376881	172.16.1.1	192.168.254.254	SMTP	Message Body
18	3.387830	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.0.0 l0S8dIOY005299 Message accepted for delivery
19	3.395347	172.16.1.1	192.168.254.254	SMTP	Message Body
20	3.395855	192.168.254.254	172.16.1.1	SMTP	Response: 221 2.0.0 localhost.localdomain closing connection
21	3.395897	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [FIN, ACK] Seq=564 Ack=502 Win=6432 Len=0
22	3.395929	172.16.1.1	192.168.254.254	TCP	1250 > smtp [ACK] Seq=502 Ack=565 Win=63677 Len=0
23	3.405772	172.16.1.1	192.168.254.254	TCP	1250 > smtp [FIN, ACK] Seq=502 Ack=565 Win=63677 Len=0
24	3.406204	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [ACK] Seq=565 Ack=503 Win=6432 Len=0

Figure 5. Capture SMTP

3. Sélectionnez la première capture SMTP dans la fenêtre Wireshark supérieure. Dans la figure 5, il s'agit de la ligne 7.
4. Dans la seconde fenêtre Wireshark, développez l'enregistrement Simple Mail Transfer Protocol.

   Il existe différents types de serveur SMTP. Les pirates malveillants peuvent obtenir des informations vitales par la simple connaissance du type et de la version du serveur SMTP.

Nom et version du serveur SMTP ?

_____

Les applications de client de messagerie électronique envoient des commandes aux serveurs de messagerie électronique et ceux-ci renvoient les réponses. Lors de chaque premier échange SMTP, le client de messagerie électronique envoie la commande **EHLO**. La syntaxe peut cependant varier entre les clients. La commande peut également apparaître sous la forme **HELO** ou **HELLO**. Le serveur de messagerie électronique doit répondre à la commande.

Quelle est la réponse du serveur SMTP à la commande EHLO ?

_____

Les échanges suivants entre le client et le serveur de messagerie électronique contiennent des informations sur le courriel. À l'aide de la capture Wireshark, remplissez les réponses du serveur de messagerie électronique aux commandes du client de messagerie électronique :

E-mail Client (Client de messagerie électronique)	E-mail Server (Serveur de messagerie électronique)
MAIL FROM:,ccna1@excmaple.com>	
RCPT TO:<ccna2@example.com>	
DATA	
(le corps du message est envoyé)	

Que contient le corps du dernier message du client de messagerie électronique ?

_____

Comment le serveur de messagerie électronique répond-il ?

_____

Tâche 3 : confirmation

Utilisez un ordinateur disposant d'un accès à Internet. Jetez un coup d'œil au nom et à la version du serveur SMTP pour en déduire les failles et menaces connues. Une version plus récente est-elle disponible ?

Tâche 4 : Remarques générales

La messagerie électronique est probablement le service réseau le plus utilisé. La compréhension du flux du trafic avec le protocole SMTP vous permettra de comprendre comment le protocole gère la connexion des données client/serveur. La messagerie électronique peut également connaître des problèmes de configuration. Le problème se situe-t-il au niveau du client de messagerie ou du serveur de messagerie ? Une façon simple de tester le fonctionnement du serveur SMTP consiste à utiliser la ligne de commande Windows de l'utilitaire Telnet pour établir une connexion Telnet avec le serveur SMTP.

1. Pour tester le fonctionnement du serveur SMTP, ouvrez la fenêtre de ligne de commande Windows et démarrez une session Telnet avec le serveur SMTP.

```
C:\>telnet eagle-server.example.com 25
220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13.1; Sun, 28 Jan
2007 20:41:0
3 +1000
HELO eagle-server.example.com
250 localhost.localdomain Hello [172.16.1.2], pleased to meet you
MAIL From: ccna2@example.com
250 2.1.0 ccna2@example.com... Sender ok
RCPT To: instructor@example.com
250 2.1.5 instructor@example.com... Recipient ok
DATA
354 Please start mail input.
e-mail SMTP server test...
.
250 Mail queued for delivery.
QUIT
221 Closing connection. Good bye.
Connection to host lost.
C:\ >
```

Tâche 5 : nettoyage

Si l'installation de Thunderbird a eu lieu sur l'ordinateur hôte pod pour ces travaux pratiques, il se peut que le formateur souhaite la suppression de l'application. Pour supprimer Thunderbird, cliquez sur **Démarrer > Panneau de configuration > Ajout/Suppression de programmes**. Faites défiler la liste jusqu'à atteindre **Thunderbird**, puis cliquez sur **Supprimer**.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

3.5.1 : intégration des compétences : configuration des hôtes et des services

Diagramme de topologie

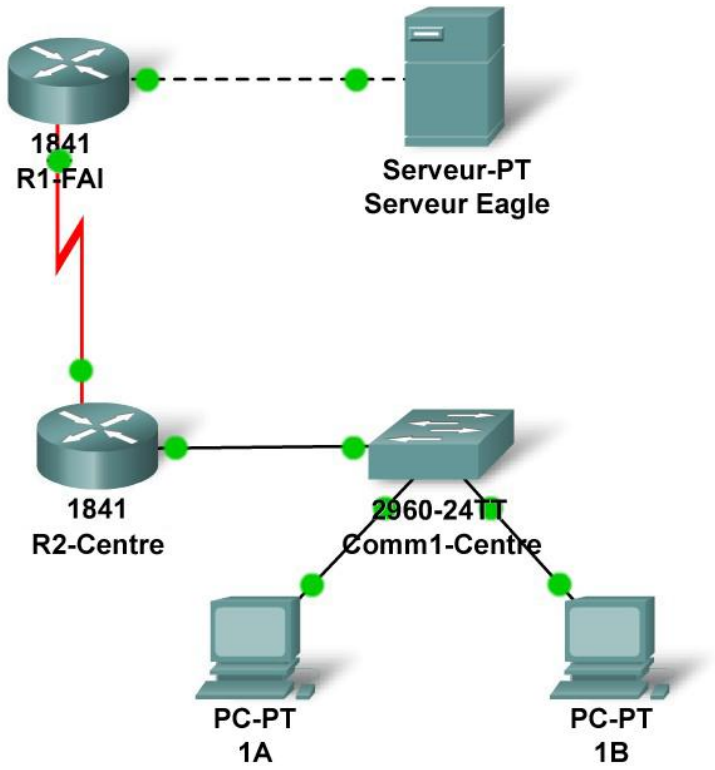


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	Fa0/0	192.168.254.253	255.255.255.0	N/A
	S0/0/0	10.10.10.6	255.255.255.252	N/A
R2-Central	Fa0/0	172.16.255.254	255.255.0.0	N/A
	S0/0/0	10.10.10.5	255.255.255.252	N/A
S1-Central	VLAN 1	172.16.254.1	255.255.0.0	172.16.255.254
PC 1A	La carte réseau	172.16.1.1	255.255.0.0	172.16.255.254
PC 1B	La carte réseau	172.16.1.2	255.255.0.0	172.16.255.254
Serveur Eagle	La carte réseau	192.168.254.254	255.255.255.0	192.168.254.253

Objectifs pédagogiques

- Configurer les hôtes et les services
- Ajouter, configurer et connecter les hôtes et les serveurs
- Analyser l'interaction entre DNS et HTTP
- Afficher les détails des paquets générés par DNS et HTTP en mode Simulation

Contexte

Tout au long de ce cours, vous allez utiliser une configuration de travaux partiques type constituée de PC, de serveurs, de routeurs et de commutateurs réels pour apprendre des concepts liés aux réseaux. À la fin de chaque chapitre, vous construirez des parties de plus en plus importantes de cette topologie dans Packet Tracer.

Tâche 1 : « réparation » et test de la topologie

Ajoutez à la topologie un PC nommé 1B. Configurez-le avec les paramètres suivants : adresse IP 172.16.1.2, masque de sous-réseau 255.255.0.0, passerelle par défaut 172.16.255.254 et serveur DNS 192.168.254.254. Reliez le PC 1B au port Fa0/2 du commutateur S1-Central.

Reliez le serveur Eagle Server au port Fa0/0 du routeur R1-ISP. Activez les services Web sur le serveur en activant le protocole HTTP. Activez les services DNS et ajoutez une entrée DNS associant « eagle-server.example.com » (sans guillemets) à l'adresse IP du serveur. Vérifiez votre travail en vous basant sur les informations affichées par le bouton **Check Results** et l'onglet **Assessment Items**. Testez la connectivité en temps réel entre le PC 1B et le serveur Eagle Server en utilisant l'option ADD SIMPLE PDU.

Sachez que lorsque vous ajoutez une unité de données de protocole simple, elle apparaît dans la fenêtre PDU List en tant que partie intégrante du « Scénario 0 ». La première fois que vous émettrez ce message ping ponctuel, celui-ci ne produira aucun résultat (libellé « **Failed** ») en raison du processus ARP, qui vous sera expliqué ultérieurement. Si vous double-cliquez sur le bouton « Fire » dans la fenêtre PDU List, ce message de test ping unique sera envoyé une deuxième fois. Cette fois, il aboutira. Dans Packet, le terme « scenario » représente une configuration spécifique d'un ou plusieurs paquets de test. Vous pouvez créer différents scénarios de paquet de test en utilisant le bouton **New**. Par exemple, Scenario 0 peut représenter un paquet de test entre le PC 1B et le serveur Eagle Server ; Scenario 1 peut correspondre à des paquets de test entre le PC 1A et les routeurs ; et ainsi de suite. Vous pouvez supprimer tous les paquets de testés d'un scénario donné en utilisant le bouton **Delete**. Ainsi, si vous utilisez le bouton **Delete** pour Scenario 0, le paquet de test que vous venez de créer entre le PC 1B et le serveur Eagle Server sera supprimé (veillez à effecteur cette opération avant la prochaine tâche).

Tâche 2 : analyse de l'interaction entre DNS et http

Passez du mode Realtime au mode Simulation. Ouvrez un navigateur Web à partir du Bureau du PC 1B. Tapez eagle-server.example.com, appuyez sur Entrée, puis utilisez le bouton **Capture / Forward** dans la liste d'événements (**Event List**) pour capturer l'interaction entre DNS et HTTP. Visualisez cette animation et examinez le contenu des paquets (fenêtre **PDU Information**, **Inbound PDU Details, Outbound PDU Details**) pour chaque événement contenu dans la liste, particulièrement lorsque les paquets se trouvent au niveau du PC 1B ou du serveur Eagle Server. Si vous recevez le message « Buffer Full » (mémoire tampon saturée), cliquez sur le bouton **View Previous Events**. Bien que le traitement des paquets par le commutateur et les routeurs puisse encore vous paraître étranger, vous devriez être en mesure d'observer la façon dont DNS et HTTP interagissent.

Remarques générales

Êtes-vous à présent en mesure d'expliquer le processus qui s'enclenche lorsque vous tapez une adresse URL dans un navigateur et qu'une page Web vous est renvoyée ? Quels types d'interactions client-serveur sont concernés ?
Si ce n'est déjà fait, nous vous recommandons de vous procurer Packet Tracer auprès de votre formateur et d'effectuer les travaux partiques « My First PT Lab » (choisissez le menu déroulant HELP, puis l'option CONTENTS).

Travaux pratiques 4.5.1 : observation des protocoles TCP et UDP à l'aide de Netstat

Schéma de la topologie

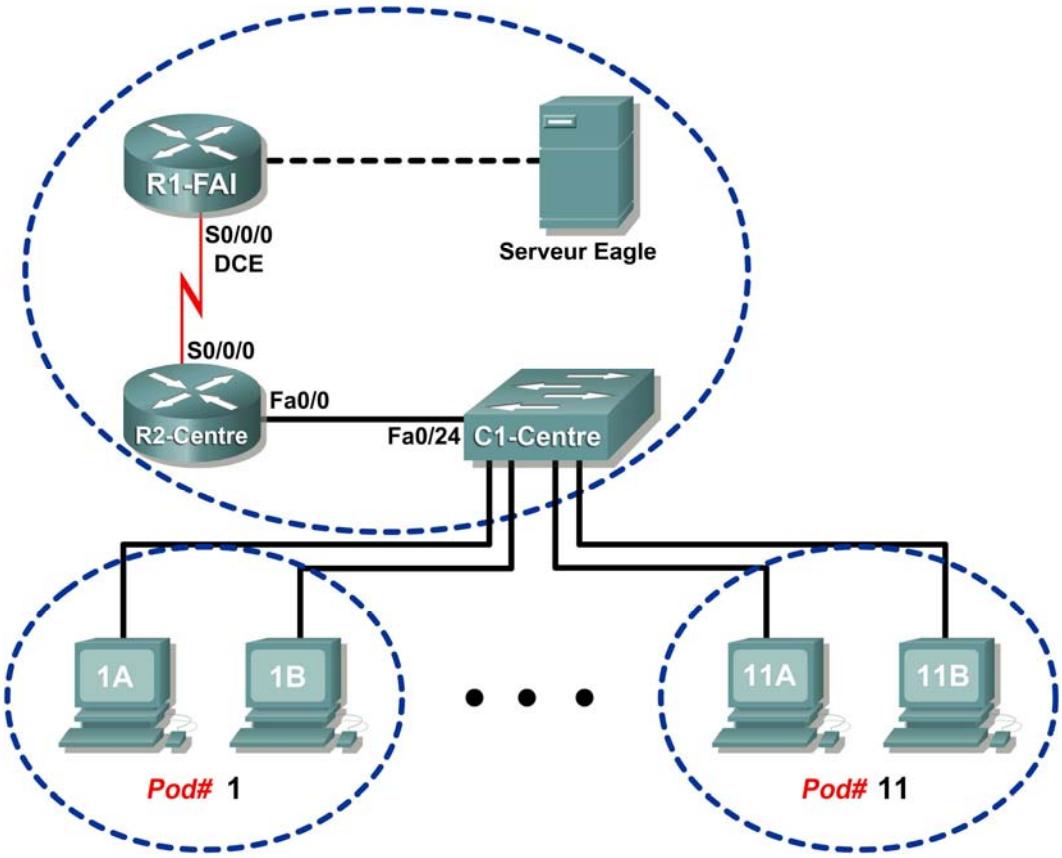


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/D
	Fa0/0	192.168.254.253	255.255.255.0	N/D
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/D
	Fa0/0	172.16.255.254	255.255.0.0	N/D
Eagle Server	N/D	192.168.254.254	255.255.255.0	192.168.254.253
	N/D	172.31.24.254	255.255.255.0	N/D
hôte*Pod#*A	N/D	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
hôte*Pod#*B	N/D	172.16. *Pod#.*2	255.255.0.0	172.16.255.254
S1-Central	N/D	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

- Décrire les paramètres et les résultats courants de la commande **netstat**.
- Observer les informations de protocole sur un ordinateur hôte pod à l'aide de la commande **netstat**.

Contexte

netstat est l'abréviation d'un utilitaire de statistiques réseau disponible à la fois sur les ordinateurs fonctionnant sous Windows et Unix / Linux. L'attribution de paramètres optionnels à cette commande génère des résultats différents. La commande **netstat** permet d'afficher les connexions réseau entrantes et sortantes (TCP et UDP), les informations de table de routage d'ordinateur hôte et les statistiques d'interface.

Scénario

Cette session de travaux pratiques consiste à étudier la commande **netstat** sur un ordinateur hôte pod et à lui attribuer des options pour analyser et comprendre l'état du protocole de couche de transport TCP/IP.

Tâche 1 : description des paramètres et des résultats courants de la commande netstat.

Cliquez sur Démarrer | Exécuter pour ouvrir une fenêtre de ligne commande. Tapez **cmd**, puis cliquez sur **OK**.

Pour afficher l'aide sur la commande **netstat**, utilisez les options **/?** comme affiché ci-dessous :

```
C:\> netstat /? <ENTRÉE>
```

Reportez-vous au résultat obtenu avec la commande **netstat** /? pour indiquer les options qui correspondent le mieux aux descriptions dans le tableau suivant :

Option	Description
	Affiche toutes les connexions et tous les ports d'écoute.
	Affiche les adresses et les numéros de port sous forme numérique.
	Affiche de nouvelles statistiques toutes les cinq secondes. Appuyez sur CTRL+C pour mettre fin à ce nouvel affichage.
	Affiche les connexions relatives au protocole défini pour proto : TCP, UDP, TCPv6 ou UDPv6. Si vous utilisez l'option -s pour afficher les statistiques par protocole, n'importe laquelle de ces valeurs peut être associée à proto : IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP ou UDPv6.
	Affiche à nouveau toutes les connexions et tous les ports d'écoute toutes les 30 secondes.
	Affiche uniquement les connexions ouvertes. Il s'agit d'un problème délicat.

Lorsque les statistiques **netstat** relatives aux connexions TCP s'affichent, l'état du protocole TCP s'affiche également. Au cours de sa durée de vie, une connexion TCP passe par toute une série d'états. Le tableau suivant comprend la liste des états TCP rapportés par **netstat**tels que définis dans la RFC 793, Transmission Control Protocol, de septembre 1981 :

État	Description de la connexion
LISTEN	La connexion locale attend une demande de connexion de la part d'un périphérique distant.
ESTABLISHED	La connexion est établie et des données peuvent être échangées via cette connexion. Il s'agit de l'état normal correspondant à la phase de transfert de données.
TIME-WAIT	La connexion locale attend qu'un délai par défaut soit écoulé avant d'envoyer une demande de fin de connexion et de fermer la connexion. Il s'agit d'une condition normale. Ce délai est généralement compris entre 30 et 120 secondes.
CLOSE-WAIT	La connexion est fermée, mais attend une demande de fin de la part de l'utilisateur local.
SYN-SENT	La connexion locale attend une réponse à la demande de connexion envoyée. La connexion passe rapidement par cet état.
SYN_RECEIVED	La connexion locale attend une validation de la demande de connexion. La connexion passe rapidement par cet état. Si vous remarquez que de multiples connexions sont en état SYN_RECEIVED, une attaque TCP SYN est peut-être en cours.

Les adresses IP qui s'affichent avec la commande **netstat** se répartissent en plusieurs catégories :

Adresse IP	Description
127.0.0.1	Cette adresse se réfère à l'hôte local, soit cet ordinateur.
0.0.0.0	Adresse globale signifiant « N'importe lequel ».
Adresse distante	Adresse du périphérique distant connecté à l'ordinateur.

Tâche 2 : observation des informations de protocole sur un ordinateur hôte pod à l'aide de la commande netstat

Étape 1 : affichage des connexions existantes à l'aide de la commande netstat

Dans la fenêtre de ligne de commande utilisée au cours de la tâche 1 ci-dessus, tapez la commande **netstat –a** :

```
C:\> netstat –a <ENTRÉE>
```

Un tableau récapitulant les informations de protocoles (TCP et UDP), d'adresse locale, d'adresse distante et d'état s'affiche. Les adresses et protocoles pouvant être convertis en noms s'affichent.

L'option –n force netstat à afficher le résultat au format brut. Dans la fenêtre de ligne de commande, tapez la commande **netstat –an**:

```
C:\> netstat –an <ENTRÉE>
```

Naviguez entre les résultats des deux commandes à l'aide de la barre de défilement vertical. Comparez les résultats, en notant les numéros de port connus convertis en noms.

Indiquez trois connexions TCP et trois connexions UDP provenant du résultat de la commande **`netstat –a`**, ainsi que les numéros de port convertis correspondants du résultat de la commande **`netstat –an`**. Si une conversion est possible pour moins de trois connexions, notez-le dans le tableau.

Connexion	Proto	Adresse locale	Adresse distante	Etat

Reportez-vous au résultat suivant de la commande **`netstat`**. Un nouvel ingénieur réseau soupçonne une attaque externe sur les ports 1070 et 1071 de son ordinateur hôte. Que pourriez-vous lui répondre ?

```
C:\> netstat –n
Connexions actives
Proto  Adresse locale          Adresse distante        Etat
TCP    127.0.0.1:1070         127.0.0.1:1071         ESTABLISHED
TCP    127.0.0.1:1071         127.0.0.1:1070         ESTABLISHED
C:\ >
```

_____

_____

Étape 2 : établissement de plusieurs connexions TCP simultanées et enregistrement du résultat de la commande `netstat`.

Au cours de cette tâche, vous allez établir plusieurs connexions simultanées avec Eagle Server. Vous utiliserez la commande **`telnet`** pour accéder aux services réseau d'Eagle Server et disposerez ainsi de plusieurs protocoles à examiner à l'aide de `netstat`.

Ouvrez quatre fenêtres de ligne de commande supplémentaires. Organisez-les de façon à ce qu'elles soient toutes visibles. Ces quatre fenêtres utilisées pour les connexions telnet à Eagle Server peuvent être relativement petites et occuper environ la moitié de la largeur de l'écran et le quart de la hauteur de l'écran. Les fenêtres de collecte des informations de connexion doivent, quant à elles, occuper environ la moitié de la largeur de l'écran et la totalité de sa hauteur.

Plusieurs services réseau d'Eagle Server répondront à une connexion telnet. Les informations suivantes seront utilisées :

- DNS : serveur de noms de domaine, port 53
- FTP : serveur FTP, port 21
- SMTP : serveur de messagerie SMTP, port 25
- TELNET : serveur Telnet, port 23

-

Comment expliquer l'échec d'une commande telnet envoyée aux ports UDP ?

_____

_____

Pour fermer une connexion telnet, appuyez à la fois sur les touches <CTRL>]. L'invite telnet s'affiche (Microsoft Telnet>). Tapez **quit <ENTRÉE>** pour fermer la session.

Dans la première fenêtre de ligne de commande telnet, envoyez une commande telnet à Eagle Server sur le port 53. Dans la deuxième fenêtre de ligne de commande telnet, envoyez une commande telnet sur le 21. Dans la troisième fenêtre de ligne de commande telnet, envoyez une commande telnet sur le port 25. Enfin, dans la quatrième fenêtre de ligne de commande telnet, envoyez une commande telnet sur le port 23. Voici la commande à utiliser pour une connexion telnet sur le port 21 :

```
C:\>telnet eagle-server.example.com 53
```

Dans la grande fenêtre de ligne de commande, enregistrez les connexions établies avec Eagle Server. Le résultat qui s'affiche est semblable à celui présenté ci-dessous. Si votre vitesse de frappe est lente, il est possible qu'une connexion soit fermée avant que toutes les connexions soient effectuées. Les connexions prennent fin au bout d'un certain délai d'inactivité.

```
Proto  Adresse locale          Adresse distante        Etat
TCP    192.168.254.1:1688     192.168.254.254:21     ESTABLISHED
TCP    192.168.254.1:1691     192.168.254.254:25     ESTABLISHED
TCP    192.168.254.1:1693     192.168.254.254:53     ESTABLISHED
TCP    192.168.254.1:1694     192.168.254.254:23     ESTABLISHED
```

Tâche 3 : Remarques générales.

L'utilitaire **netstat** permet d'afficher les connexions réseau (TCP et UDP) entrantes et sortantes, les informations de table de routage d'ordinateur hôte et les statistiques d'interface.

Tâche 4 : confirmation.

Fermez les connexions établies de façon abrupte (en fermant la fenêtre de ligne de commande), puis exécutez une commande **netstat –an**. Essayez de déterminer les connexions qui se trouvent dans un état différent de ESTABLISHED.

Tâche 5 : nettoyage

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

Travaux pratiques 4.5.2 : protocoles TCP et UDP de la couche transport TCP/IP

Schéma de la topologie

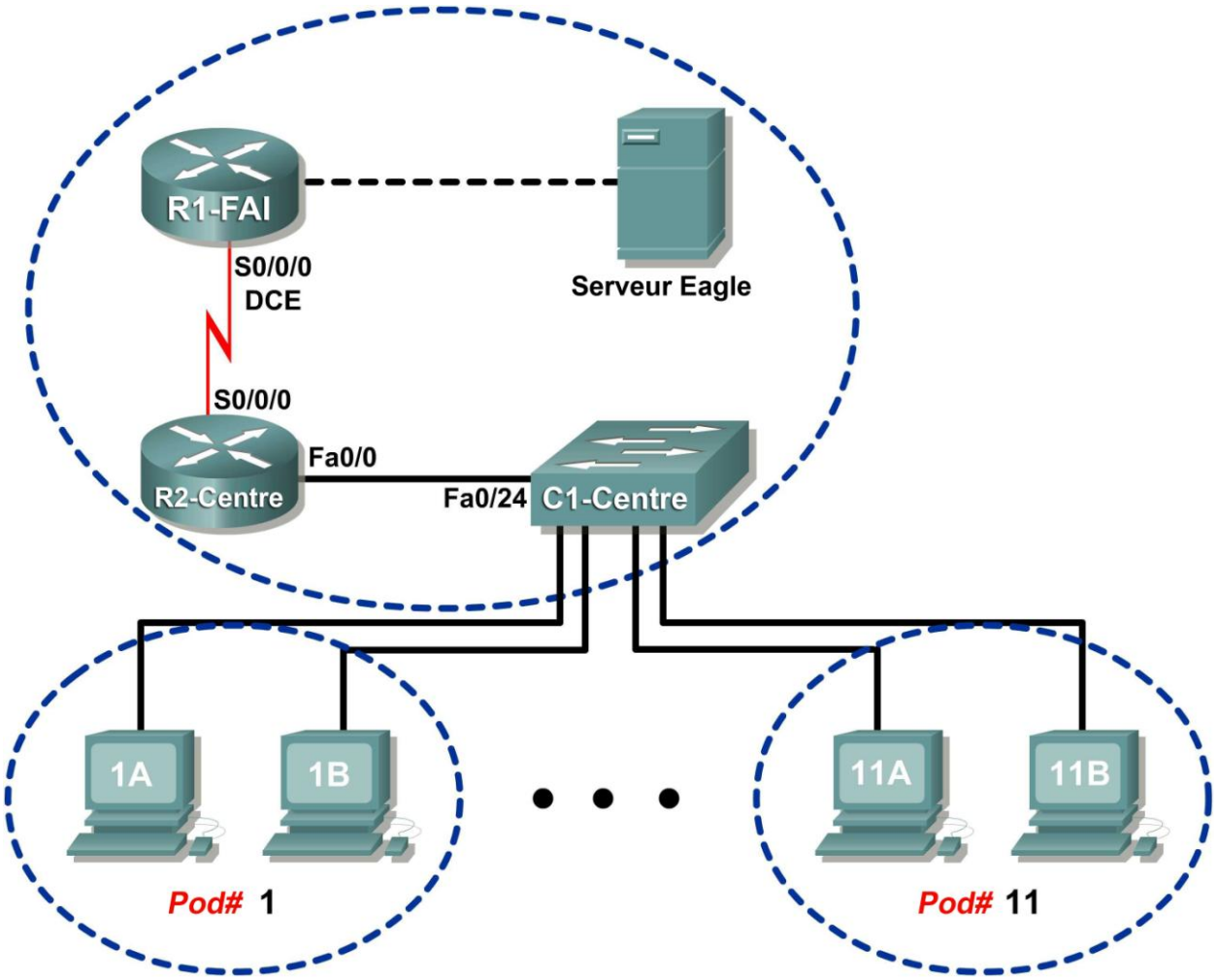


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/D
	Fa0/0	192.168.254.253	255.255.255.0	N/D
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/D
	Fa0/0	172.16.255.254	255.255.0.0	N/D
Eagle Server	N/D	192.168.254.254	255.255.255.0	192.168.254.253
	N/D	172.31.24.254	255.255.255.0	N/D
hôte*Pod#***A**	N/D	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
hôte*Pod#***B**	N/D	172.16. *Pod#.*2	255.255.0.0	172.16.255.254
S1-Central	N/D	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

- Identifier les champs d'en-tête TCP ainsi que les opérations à l'aide de la capture de session FTP de Wireshark.
- Identifier les champs d'en-tête UDP ainsi que les opérations à l'aide de la capture de session TFTP de Wireshark.

Contexte

Les deux protocoles dans la couche transport du modèle TCP/IP sont TCP (Transmission Control Protocol), défini dans la RFC 761 de janvier 1980, et UDP (User Datagram Protocol), défini dans la RFC 768 d'août 1980. Ces deux protocoles prennent en charge la communication de protocoles de couche supérieure. Par exemple, TCP permet d'offrir la prise en charge de la couche transport pour les protocoles HTTP et FTP, entre autres. Quant à UDP, il fournit cette prise en charge pour les services de noms de domaines (DNS) et le protocole TFTP (Trivial File Transfer Protocol), entre autres.

La capacité à comprendre les éléments des en-têtes TCP et UDP ainsi que les opérations représentent une compétence cruciale pour les ingénieurs réseau.

Scénario

À l'aide de la capture Wireshark, analysez les champs d'en-têtes des protocoles TCP et UDP pour les transferts de fichiers entre l'ordinateur hôte et Eagle Server. Si vous n'avez pas effectué le téléchargement de Wireshark sur l'ordinateur hôte pod, utilisez l'adresse URL `ftp://eagle-server.example.com/pub/eagle labs/eagle1/chapter4/`, fichier `wireshark-setup-0.99.4.exe`.

Les utilitaires de ligne de commande Windows `ftp` et `tftp` servent à la connexion à Eagle Server et au téléchargement des fichiers.

Tâche 1 : identification des champs d'en-tête TCP ainsi que les opérations à l'aide de la capture de session FTP de Wireshark.

Étape 1 : capture d'une session FTP.

Les sessions TCP sont parfaitement contrôlées et gérées par les informations échangées dans les champs d'en-tête TCP. Dans cette tâche, une session FTP est effectuée dans Eagle Server. Ensuite, la capture de session est analysée. Les ordinateurs Windows utilisent le client FTP, **`ftp`**, pour la connexion au serveur FTP. Une fenêtre de ligne de commande démarre la session FTP, et le fichier de configuration du texte pour S1-central est téléchargé depuis Eagle Server, `/pub/eagle_labs/eagle1/chapter4/s1-central`, vers l'ordinateur hôte.

Ouvrez une fenêtre de ligne de commande en cliquant sur Démarrer | Exécuter, tapez cmd, puis appuyez sur OK.

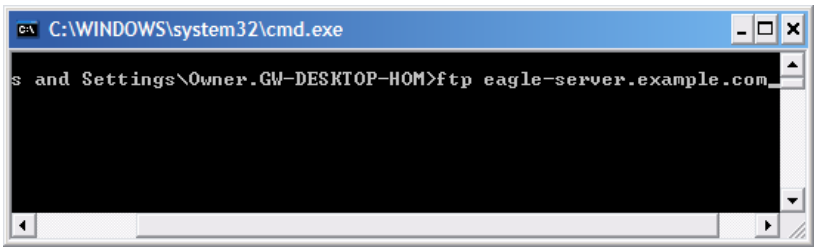


Figure 1. Fenêtre de ligne de commande

Une fenêtre semblable à la figure 1 doit s'afficher.

Démarrez une capture Wireshark sur l'interface dont l'adresse IP est `172.16.`*`Pod#`*`.[1-2]`.

Démarrez une connexion FTP à Eagle Server. Tapez la commande :

```
> ftp eagle-server.example.com
```

À l'invite d'un ID utilisateur, tapez **`anonyme`**. Lorsque le système vous demande un mot de passe, appuyez sur **`<ENTRÉE>`**.

Allez au répertoire FTP `/pub/eagle_labs/eagle1/chapter4/` :

```
ftp> cd /pub/eagle_labs/eagle1/chapter4/
```

Téléchargez le fichier `s1-central` :

```
ftp> get s1-central
```

Ensuite, fermez les sessions FTP dans chaque fenêtre de ligne de commande avec la commande **`quit`** :

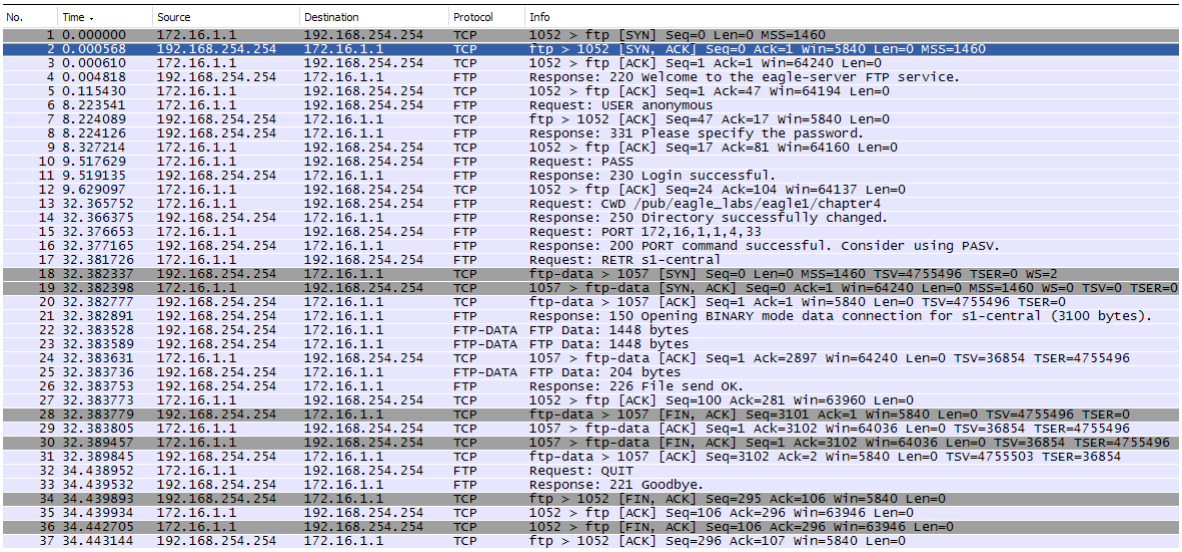
```
ftp> quit
```

Fermez la fenêtre de ligne de commande avec la commande **`exit`** :

```
> exit
```

Arrêtez la capture Wireshark.

Étape 2 : analyse des champs TCP.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.1	192.168.254.254	TCP	1052 > ftp [SYN] Seq=0 Len=0 MSS=1460
2	0.000568	192.168.254.254	172.16.1.1	TCP	ftp > 1052 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
3	0.000610	172.16.1.1	192.168.254.254	TCP	1052 > ftp [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.004818	192.168.254.254	172.16.1.1	FTP	Response: 220 Welcome to the eagle-server FTP service.
5	0.115430	172.16.1.1	192.168.254.254	TCP	1052 > ftp [ACK] Seq=1 Ack=47 Win=64194 Len=0
6	8.223541	172.16.1.1	192.168.254.254	FTP	Request: USER anonymous
7	8.224089	192.168.254.254	172.16.1.1	TCP	ftp > 1052 [ACK] Seq=47 Ack=17 Win=5840 Len=0
8	8.224126	192.168.254.254	172.16.1.1	FTP	Response: 331 Please specify the password.
9	8.327214	172.16.1.1	192.168.254.254	TCP	1052 > ftp [ACK] Seq=17 Ack=81 Win=64160 Len=0
10	9.517629	172.16.1.1	192.168.254.254	FTP	Request: PASS
11	9.519135	192.168.254.254	172.16.1.1	FTP	Response: 230 Login successful.
12	9.629097	172.16.1.1	192.168.254.254	TCP	1052 > ftp [ACK] Seq=24 Ack=104 Win=64137 Len=0
13	32.365752	172.16.1.1	192.168.254.254	FTP	Request: CWD /pub/eagle_labs/eagle1/chapter4
14	32.366375	192.168.254.254	172.16.1.1	FTP	Response: 250 Directory successfully changed.
15	32.376653	172.16.1.1	192.168.254.254	FTP	Request: PORT 172,16,1,1,4,33
16	32.377165	192.168.254.254	172.16.1.1	FTP	Response: 200 PORT command successful. Consider using PASV.
17	32.381726	172.16.1.1	192.168.254.254	FTP	Request: RETR s1-central
18	32.382337	192.168.254.254	172.16.1.1	TCP	ftp-data > 1057 [SYN] Seq=0 Len=0 MSS=1460 TSV=4755496 TSER=0 WS=2
19	32.382398	172.16.1.1	192.168.254.254	TCP	1057 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
20	32.382777	192.168.254.254	172.16.1.1	TCP	ftp-data > 1057 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=4755496 TSER=0
21	32.382891	192.168.254.254	172.16.1.1	FTP	Response: 150 Opening BINARY mode data connection for s1-central (3100 bytes).
22	32.383528	192.168.254.254	172.16.1.1	FTP-DATA	FTP Data: 1448 bytes
23	32.383589	192.168.254.254	172.16.1.1	FTP-DATA	FTP Data: 1448 bytes
24	32.383631	172.16.1.1	192.168.254.254	TCP	1057 > ftp-data [ACK] Seq=1 Ack=2897 Win=64240 Len=0 TSV=36854 TSER=4755496
25	32.383736	192.168.254.254	172.16.1.1	FTP-DATA	FTP Data: 204 bytes
26	32.383753	192.168.254.254	172.16.1.1	FTP	Response: 226 File send OK.
27	32.383773	172.16.1.1	192.168.254.254	TCP	1052 > ftp [ACK] Seq=100 Ack=281 Win=63960 Len=0
28	32.383779	192.168.254.254	172.16.1.1	TCP	ftp-data > 1057 [FIN, ACK] Seq=3101 Ack=1 Win=5840 Len=0 TSV=4755496 TSER=0
29	32.383805	172.16.1.1	192.168.254.254	TCP	1057 > ftp-data [ACK] Seq=1 Ack=3102 Win=64036 Len=0 TSV=36854 TSER=4755496
30	32.389457	172.16.1.1	192.168.254.254	TCP	1057 > ftp-data [FIN, ACK] Seq=1 Ack=3102 Win=64036 Len=0 TSV=36854 TSER=4755496
31	32.389845	192.168.254.254	172.16.1.1	TCP	ftp-data > 1057 [ACK] Seq=3102 Ack=2 Win=5840 Len=0 TSV=4755503 TSER=36854
32	34.438952	172.16.1.1	192.168.254.254	FTP	Request: QUIT
33	34.439532	192.168.254.254	172.16.1.1	FTP	Response: 221 Goodbye.
34	34.439893	192.168.254.254	172.16.1.1	TCP	ftp > 1052 [FIN, ACK] Seq=295 Ack=106 Win=5840 Len=0
35	34.439934	172.16.1.1	192.168.254.254	TCP	1052 > ftp [ACK] Seq=106 Ack=296 Win=63946 Len=0
36	34.442705	172.16.1.1	192.168.254.254	TCP	1052 > ftp [FIN, ACK] Seq=106 Ack=296 Win=63946 Len=0
37	34.443144	192.168.254.254	172.16.1.1	TCP	ftp > 1052 [ACK] Seq=296 Ack=107 Win=5840 Len=0

Figure 2. Capture FTP

Basculez vers les fenêtres de capture Wireshark. La fenêtre supérieure contient les informations récapitulatives pour chaque enregistrement capturé. La capture par le participant doit être semblable à celle illustrée à la figure 2. Avant d'approfondir le concept de paquet TCP, une explication des informations récapitulatives s'impose. Lorsque le client FTP est connecté au serveur FTP, le protocole TCP de la couche transport a créé une session fiable. TCP est couramment utilisé au cours d'une session pour contrôler la transmission et l'arrivée des datagrammes ainsi que pour gérer la taille des fenêtres. Pour chaque échange de données entre le client FTP et le serveur FTP, une session TCP est créée. Au terme du transfert de données, la session TCP est fermée. Ainsi, une fois la session FTP terminée, TCP exécute un arrêt et une déconnexion normalement.

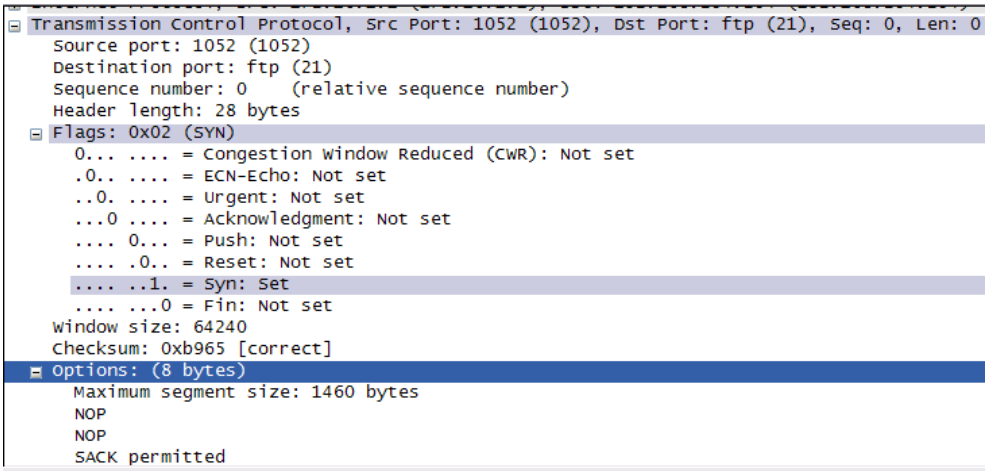


Figure 3. Capture Wireshark d'un datagramme TCP

Dans Wireshark, les informations TCP détaillées sont disponibles dans la fenêtre du milieu. Sélectionnez le premier datagramme TCP à partir de l'ordinateur hôte, et déplacez le pointeur de la souris vers la fenêtre du milieu. Il peut s'avérer nécessaire de modifier la fenêtre du milieu et de développer l'enregistrement TCP en cliquant sur la zone de développement du protocole. Le datagramme TCP développé doit être semblable à la figure 3.

Quelle est la méthode d'identification du premier datagramme dans une session TCP ?

_____

_____

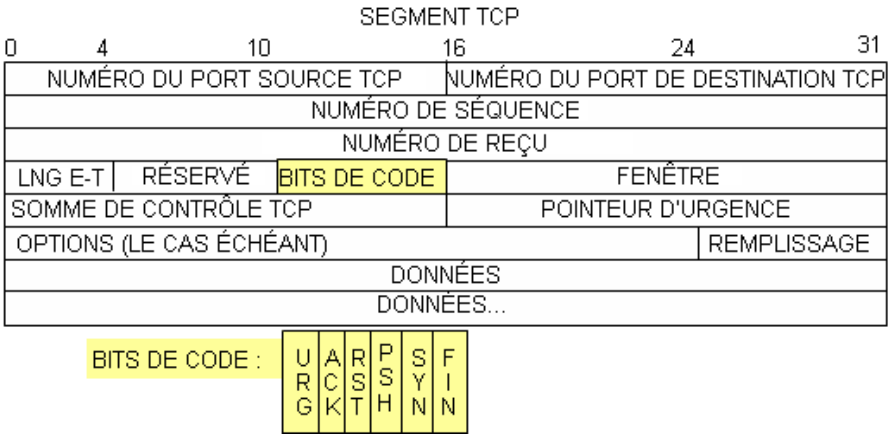


Figure 4. Champs de paquet TCP

Reportez-vous à la figure 4, un schéma de datagramme TCP. Une explication de chaque champ est disponible pour rafraîchir la mémoire du participant :

- **Le numéro de port source TCP** appartient à l'hôte de session TCP qui a ouvert une connexion. Il s'agit généralement d'une valeur aléatoire supérieure à 1023.
- **Le numéro de port de destination** permet d'identifier le protocole de couche supérieure ou l'application sur le site distant. Les valeurs dans la plage 0–1023 représentent les « ports bien connus » et sont associées aux services et aux applications standard (selon la description dans la RFC 1700, comme Telnet, FTP (File Transfer Protocol), HTTP (HyperText Transfer Protocol), etc.). La combinaison de quatre champs (Adresse IP source, Port source, Adresse IP de destination, Port de destination) identifie de façon unique la session à l'émetteur et au récepteur.
- **Le numéro d'ordre** indique le numéro du dernier octet dans un segment.
- **Le numéro de reçu** indique l'octet suivant prévu par le récepteur.
- **les Bits de code** ont une signification spécifique dans la gestion des sessions et dans le traitement des segments. Valeurs intéressantes :
    - ACK (reçu d'un segment) ;
    - SYN (Synchronize, uniquement défini lorsqu'une nouvelle session TCP est négociée au cours de la connexion en trois étapes) ;
    - FIN (Finish, requête pour fermer la session TCP) ;
- **La taille de la fenêtre** est la valeur de la fenêtre glissante : le nombre d'octets qui peuvent être envoyés avant d'attendre le reçu.
- **Le pointeur d'urgence** n'est utilisé qu'avec un indicateur URG (Urgent) : lorsque l'émetteur doit envoyer des données urgentes au récepteur.
- **Options** : la seule option actuellement définie est la taille de segment TCP maximale (valeur facultative).

À l'aide de la capture Wireshark du démarrage de la première session TCP (bit SYNC défini sur 1), renseignez les informations concernant l'en-tête TCP :

De l'ordinateur hôte pod vers Eagle Server (seul le bit SYN est défini sur 1) :

Adresse IP source : 172.16.___.___	
Adresse IP de destination : _____	
Numéro du port source : _____	
Numéro du port de destination : _____	
Numéro d'ordre : _____	
Numéro de reçu : _____	
Longueur de l'en-tête : _____	
Taille de fenêtre : _____	

D'Eagle Server vers l'ordinateur hôte pod (seul les bits SYN et ACK sont définis sur 1) :

Adresse IP source : _____	
Adresse IP de destination : 172.16.___.___	
Numéro du port source : _____	
Numéro du port de destination :_____	
Numéro d'ordre : _____	
Numéro de reçu : _____	
Longueur de l'en-tête : _____	
Taille de fenêtre : _____	

De l'ordinateur hôte pod vers le Eagle Server (seul le bit ACK est défini sur 1) :

Adresse IP source : 172.16.___.___	
Adresse IP de destination : _____	
Numéro du port source : _____	
Numéro du port de destination : _____	
Numéro d'ordre : _____	
Numéro de reçu : _____	
Longueur de l'en-tête : _____	
Taille de fenêtre : _____	

Sans tenir compte de la session IP démarrée lors d'un transfert de données, combien d'autres datagrammes TCP contenaient un bit SYN ?

Les pirates informatiques profitent de la connexion en trois étapes en amorçant une connexion « semi-ouverte ». Dans cette séquence, la session TCP d'ouverture envoie un datagramme TCP avec le bit SYN défini. En outre, le récepteur envoie un datagramme TCP associé avec les bits SYN ACK définis. Un bit ACK final n'est jamais envoyé pour terminer la connexion TCP. À la place, une nouvelle connexion TCP est démarrée de manière semi-ouverte. Avec un nombre suffisant de sessions TCP dans l'état semi-ouvert, l'ordinateur récepteur risque d'épuiser les ressources et de tomber en panne. Cela pourrait entraîner une perte de services réseau ou endommager le système d'exploitation. Dans les deux cas, le pirate informatique a gagné. Le service réseau a été arrêté sur le récepteur. Ceci est un exemple d'attaque par déni de service.

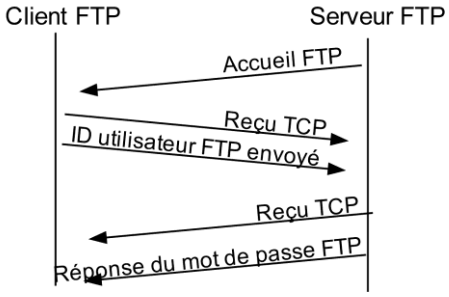


Figure 5. Gestion des sessions TCP

Le client FTP et le serveur communiquent entre eux sans tenir compte du contrôle et de la gestion de la session par TCP. Lorsque le serveur FTP envoie une réponse : 220 au client FTP, la session TCP sur le client FTP envoie un reçu à la session TCP sur Eagle Server. Cette séquence est illustrée à la figure 5, et est visible dans la capture Wireshark.

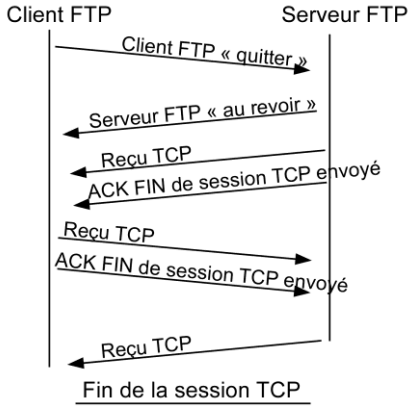


Figure 6. Fin normale de la session TCP

Une fois la session FTP terminée, le client FTP envoie une commande pour « `quitter` ». Le serveur FTP accuse réception de la fin de la session FTP avec un message `Response :221 Goodbye`. À ce stade, la session TCP du serveur FTP envoie un datagramme TCP au client FTP, et annonce ainsi la fin de la session TCP. La session TCP du client FTP accuse réception du datagramme de fin, puis envoie la fin de sa propre session TCP. Lorsque l'émetteur de la fin de la session TCP, le serveur FTP, reçoit une fin en double, un datagramme ACK est envoyé pour accuser réception de la fin et la session TCP est fermée. Cette séquence est illustrée à la figure 6, et est visible dans la capture Wireshark.

Sans fin normale, comme dans le cas d'une connexion rompue, les sessions TCP attendent un certain délai avant la fermeture. Le délai d'attente varie, mais il est généralement de 5 minutes.

Tâche 2 : identification des champs d'en-tête UDP ainsi que les opérations à l'aide de la capture de session TFTP de Wireshark.

Étape 1 : capture d'une session TFTP.

Suivant la procédure dans la tâche 1 ci-dessus, ouvrez une fenêtre de ligne de commande. La commande TFTP possède une syntaxe différente de FTP. Par exemple, l'authentification n'est pas disponible. En outre, il n'existe que deux commandes, **`get`**, pour récupérer un fichier et **`put`**, pour envoyer un fichier.

```
>tftp –help

Transfère des fichiers vers/depuis un ordinateur distant exécutant le
service TFTP.

TFTP [-i] host [GET | PUT] source [destination]

        -i        Indique le mode de transfert d'image binaire
                  (également nommé octet). En mode d'image binaire, le
                  fichier est déplacé littéralement, octet par octet.
                  Utilisez ce mode lors du transfert des fichiers
                  binaires.
        host      Spécifie l'hôte local ou distant.
        GET       transfère la destination du fichier sur l'hôte distant
                  vers la source du fichier sur l'hôte local.
        PUT       Transfère la source du fichier sur l'hôte local vers
                  la destination du fichier sur l'hôte distant.
        source    Indique le fichier à transférer.
  destination     Indique où transférer le fichier.
```

Tableau 1. Syntaxe TFTP pour un client TFTP de Windows

Le tableau 1 contient la syntaxe du client TFTP de Windows. Le serveur TFTP possède son propre répertoire sur Eagle Server, `/tftpboot`, qui est différent de la structure de répertoires prise en charge par le serveur FTP. L'authentification n'est pas prise en charge.

Démarrez une capture Wireshark, puis téléchargez le fichier de configuration `s1-central` à partir d'Eagle Server avec le client TFTP de Windows. La commande et la syntaxe pour effectuer cette opération sont indiquées ci-dessous :

```
>tftp eagle-server.example.com get s1-central
```

Étape 2 : analyse des champs UDP.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.1	192.168.254.254	TFTP	Read Request, File: s1-central, Transfer type: netascii
2	0.003171	192.168.254.254	172.16.1.1	TFTP	Data Packet, Block: 1
3	0.003314	172.16.1.1	192.168.254.254	TFTP	Acknowledgement, Block: 1
4	0.003962	192.168.254.254	172.16.1.1	TFTP	Data Packet, Block: 2
5	0.004021	172.16.1.1	192.168.254.254	TFTP	Acknowledgement, Block: 2
6	0.004615	192.168.254.254	172.16.1.1	TFTP	Data Packet, Block: 3
7	0.004673	172.16.1.1	192.168.254.254	TFTP	Acknowledgement, Block: 3
8	0.005274	192.168.254.254	172.16.1.1	TFTP	Data Packet, Block: 4
9	0.005332	172.16.1.1	192.168.254.254	TFTP	Acknowledgement, Block: 4
10	0.005930	192.168.254.254	172.16.1.1	TFTP	Data Packet, Block: 5
11	0.005989	172.16.1.1	192.168.254.254	TFTP	Acknowledgement, Block: 5
12	0.006588	192.168.254.254	172.16.1.1	TFTP	Data Packet, Block: 6
13	0.006644	172.16.1.1	192.168.254.254	TFTP	Acknowledgement, Block: 6
14	0.007078	192.168.254.254	172.16.1.1	TFTP	Data Packet, Block: 7 (last)
15	0.007131	172.16.1.1	192.168.254.254	TFTP	Acknowledgement, Block: 7

Figure 7. Résumé d'une capture d'une session UDP

Basculez vers les fenêtres de capture Wireshark. La capture par le participant doit être semblable à celle illustrée à la figure 7. Un transfert TFTP permet d'analyser les opérations UDP de la couche transport.

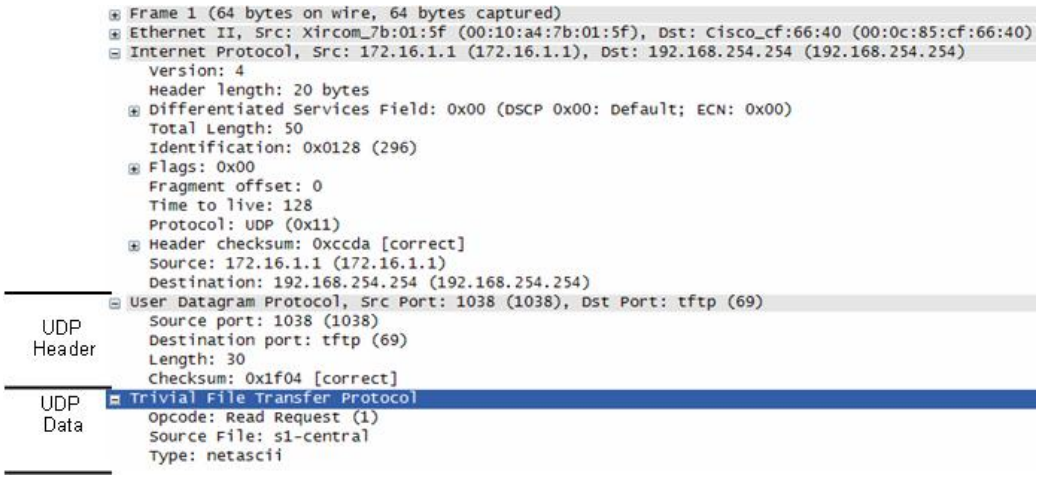


Figure 8. Capture Wireshark d'un datagramme UDP

Dans Wireshark, les informations UDP détaillées sont disponibles dans la fenêtre du milieu. Sélectionnez le premier datagramme UDP à partir de l'ordinateur hôte, et déplacez le pointeur de la souris vers la fenêtre du milieu. Il peut s'avérer nécessaire de modifier la fenêtre du milieu et de développer l'enregistrement UDP en cliquant sur la zone de développement du protocole. Le datagramme UDP développé doit être semblable à la figure 8.

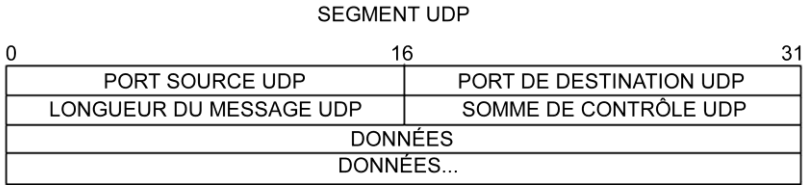


Figure 9. Format UDP

Reportez-vous à la figure 9, un schéma de datagramme UDP. Les informations d'en-tête sont peu nombreuses par rapport au datagramme TCP. Des similitudes existent cependant. Chaque datagramme UDP est identifié par les ports source et de destination UDP.

À l'aide de la capture Wireshark du premier datagramme IDP, renseignez les informations concernant l'en-tête UDP. La somme de contrôle est une valeur hexadécimale (base 16), identifiée par le code 0x précédent :

Adresse IP source : 172.16.___.___	
Adresse IP de destination : _____	
Numéro du port source : _____	
Numéro du port de destination : _____	
Longueur du message UDP : _____	
Somme de contrôle UDP : _____	

De quelle manière UDP vérifie-t-il l'intégrité du datagramme ?

_____

_____

Examinez le premier paquet retourné par Eagle Server. Renseignez les informations sur l'en-tête UDP :

Adresse IP source :	
Adresse IP de destination : 172.16.___.___	
Numéro du port source : _____	
Numéro du port de destination : _____	
Longueur du message UDP : _____	
Somme de contrôle UDP : 0x _____	

Remarque : le datagramme UDP de retour possède un port de source UDP différent. Toutefois, ce dernier sert au transfert TFTP restant. Comme la connexion n'est pas fiable, seul le port source d'origine utilisé pour commencer la session TFTP sert à gérer le transfert TFTP.

Tâche 5 : Remarques générales.

Ces travaux pratiques ont permis aux participants d'analyser les opérations des protocoles TCP et UDP à partir de sessions FTP et TFTP capturées. La gestion de la communication par TCP est très différente de celle par UDP. Toutefois, la fiabilité et la transmission garantie nécessitent un contrôle supplémentaire sur le canal de communication. UDP comporte moins de surcharge et de contrôle, et le protocole de couche supérieure doit fournir un certain type de contrôle des reçus. Les deux protocoles, cependant, transportent des données entre les clients et les serveurs à l'aide des protocoles de la couche application. En outre, ils sont applicables au protocole de couche supérieure que chacun prend en charge.

Tâche 6 : confirmation.

Comme les protocoles FTP et TFTP ne sont pas sécurisés, toutes les données transférées sont envoyées en texte clair. Ceci comprend les ID d'utilisateurs, les mots de passe ou le contenu des fichiers en texte clair. L'analyse de la session FTP de couche supérieure permet d'identifier rapidement l'ID d'utilisateur, le mot de passe ainsi que les mots de passe pour le fichier de configuration. L'analyse des données TFTP de couche supérieure est un peu plus complexe. Toutefois, le champ de données peut être examiné et les informations d'ID d'utilisateur et de mot de passe pour la configuration peuvent être extraites.

Tâche 7 : nettoyage

Au cours de ces travaux pratiques, plusieurs fichiers ont été transférés vers l'ordinateur hôte et doivent être supprimés.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

Travaux pratiques 4.5.3 : examen des protocoles de la couche application et de la couche transport

Schéma de la topologie

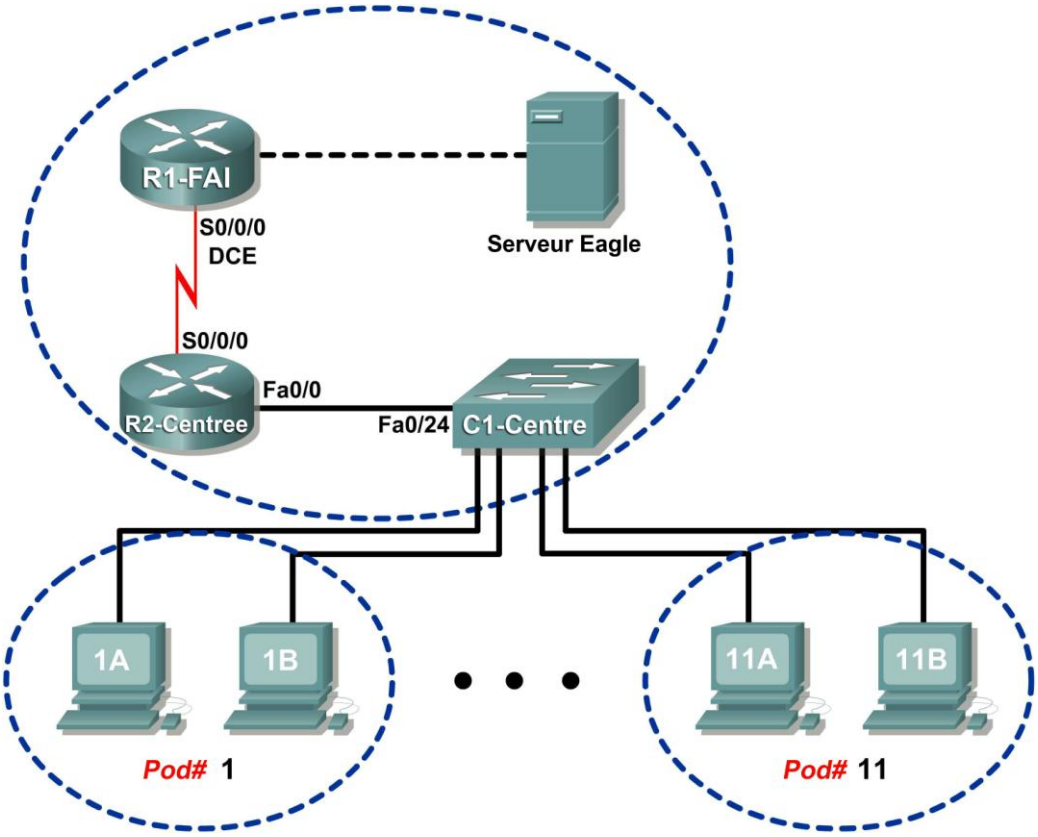


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/D
	Fa0/0	192.168.254.253	255.255.255.0	N/D
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/D
	Fa0/0	172.16.255.254	255.255.0.0	N/D
Eagle Server	N/D	192.168.254.254	255.255.255.0	192.168.254.253
	N/D	172.31.24.254	255.255.255.0	N/D
hôte*Pod#*A	N/D	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
hôte*Pod#*B	N/D	172.16. *Pod#.*2	255.255.0.0	172.16.255.254
S1-Central	N/D	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- configurer l'ordinateur hôte pour capturer les protocoles de la couche application ;
- capturer et analyser la communication HTTP entre l'ordinateur hôte pod et un serveur Web ;
- capturer et analyser la communication FTP entre l'ordinateur hôte pod et un serveur FTP ;
- observer l'établissement et la gestion des canaux de communication par TCP avec les connexions HTTP et FTP.

Contexte

La fonction principale de la couche transport consiste à effectuer le suivi des conversations des applications sur le même hôte. Toutefois, les besoins de données sont différents selon les applications. Par conséquent, divers protocoles de transport ont été développés pour y répondre.
Les protocoles de couche application définissent la communication entre les services réseau, un serveur Web et un client, et un serveur FTP et un client, par exemple. Le client établit la communication avec le serveur approprié et ce dernier lui répond. Pour chaque service réseau, un serveur différent écoute sur un autre port les connexions de clients. Plusieurs serveurs sont susceptibles de figurer sur le même périphérique final. Il est possible qu'un utilisateur ouvre plusieurs applications clientes sur le même serveur. Toutefois, chaque client communique de façon exclusive avec une session établie entre le client et le serveur.

Les protocoles de couche application reposent sur les protocoles TCP/IP de niveau inférieur, tels que TCP ou UDP. Ces travaux pratiques examinent deux protocoles de couche application standard, HTTP et FTP, ainsi que la gestion du canal de communication par les protocoles TCP et UDP de la couche transport. Les requêtes standard du client et les réponses correspondantes du serveur seront également étudiées.

Scénario

Dans ces travaux pratiques, vous utiliserez des applications clientes pour vous connecter aux services réseau d'Eagle Server. Vous surveillerez les communications à l'aide du logiciel Wireshark et analyserez les paquets capturés.

Un navigateur Web, tel qu'Internet Explorer ou Firefox, sera utilisé pour vous connecter au service réseau d'Eagle Server. Ce dernier comprend plusieurs services réseau préconfigurés, tels que HTTP, en attente de répondre aux requêtes du client.

Le navigateur Web sera également utilisé pour examiner le protocole FTP, ainsi que le client de ligne de commande FTP. Cet exercice démontrera que la communication sous-jacente avec le serveur reste identique même si les clients sont différents.

Tâche 1 : configuration de l'ordinateur hôte pod pour capturer les protocoles de couche application.

Les travaux pratiques doivent être configurés comme illustré dans le schéma de topologie et dans la table d'adressage logique. Si ce n'est pas le cas, demandez de l'aide auprès de votre formateur.

Étape 1 : téléchargement et installation de wireshark.

Figure 1. Page de téléchargement de Thunderbird sur FTP

Si Wireshark n'est pas installé sur l'ordinateur hôte pod, vous pouvez le télécharger à l'adresse eagle-server.example.com. Reportez-vous à la figure 1. L'URL de téléchargement est ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter3.

1. Cliquez avec le bouton droit sur le nom de fichier de wireshark, puis enregistrez le fichier dans l'ordinateur hôte pod.
2. Une fois le fichier téléchargé, double-cliquez sur le nom de fichier et installez Wireshark avec les paramètres par défaut.

Étape 2 : démarrage de Wireshark et configuration de l'interface de capture.

1. Démarrez Wireshark à partir de **Démarrer > Tous les programmes > Wireshark > Wireshark**.
2. Lorsque l'écran d'ouverture s'affiche, définissez l'interface de capture appropriée. L'interface avec l'adresse IP de l'ordinateur hôte pod est correcte. Reportez-vous à la figure 2.

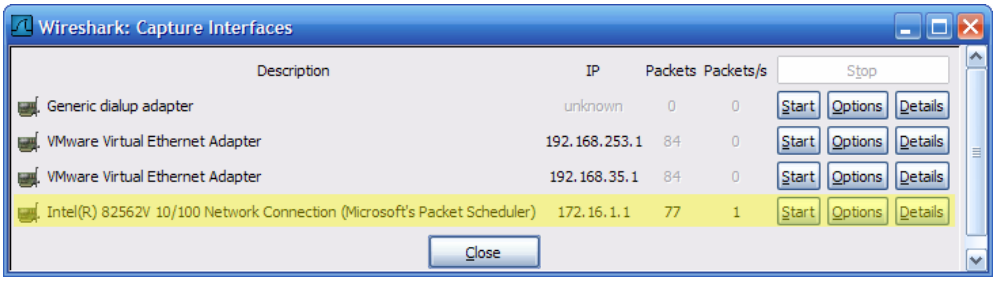


Figure 2. Écran de capture de l'interface Wireshark

Vous pouvez lancer Wireshark en cliquant sur le bouton **Démarrer** de l'interface. Ensuite, cette dernière est utilisée comme celle par défaut et ne nécessite pas de modifications.

Wireshark doit commencer la consignation des données.

3. Arrêtez Wireshark pour le moment. Vous l'utiliserez dans les tâches à venir.

Tâche 2 : capture et analyse de la communication HTTP entre l'ordinateur hôte pod et un serveur Web.

HTTP est un protocole de couche application qui repose sur des protocoles de niveau inférieur comme TCP pour établir et gérer le canal de communication. HTTP version 1.1 est défini dans la RFC 2616 de 1999. Cette partie des travaux pratiques démontre la manière dont les sessions entre plusieurs clients Web et le serveur Web restent distinctes.

Étape 1 : lancement de la capture à l'aide de Wireshark.

Démarrez une capture Wireshark. Les résultats s'affichent par type de paquet.

Étape 2 : démarrage du navigateur Web de l'hôte pod.

1. À l'aide d'un navigateur Web tel qu'Internet Explorer ou Firefox, connectez-vous à l'URL http://eagle-server.example.com. Une page Web semblable à la figure 3 s'affiche. Ne fermez pas ce navigateur Web avant que le système ne vous le demande.

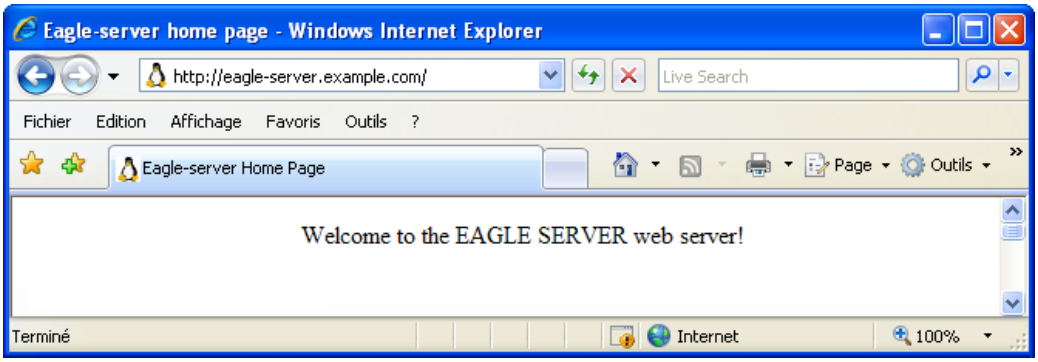


Figure 3. Navigateur Web connecté au serveur Web

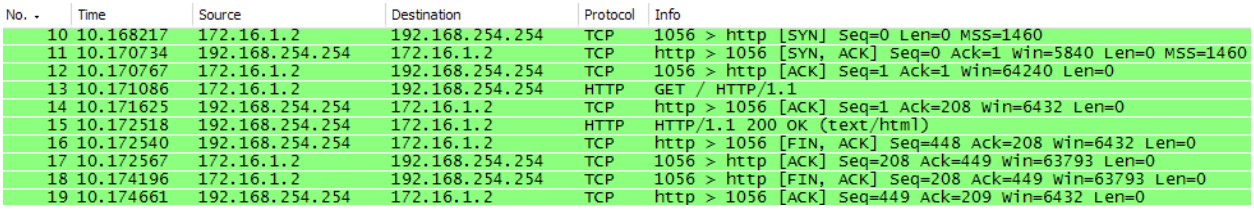
2. Cliquez sur le bouton **Actualiser** du navigateur Web. L'affichage dans le client Web reste le même.
3. Ouvrez un deuxième navigateur Web et connectez-vous à l'URL http://eagle-server.example.com/page2.html. Ceci permet d'afficher une page Web différente.

   Ne fermez aucun des deux navigateurs jusqu'à l'arrêt de la capture Wireshark.

Étape 3 : arrêt des captures Wireshark et analyse des données capturées.

1. Arrêtez les captures Wireshark.
2. Fermez les navigateurs Web.

Les données Wireshark obtenues sont affichées. Au moins trois sessions HTTP ont été créées dans l'étape 2. La première session HTTP a démarré avec une connexion à http://eagle-server.example.com. La deuxième session s'est produite avec une actualisation. La troisième session a eu lieu avec l'accès du deuxième navigateur Web à http://eagle-server.example.com/page2.html.



No.	Time	Source	Destination	Protocol	Info
10	10.168217	172.16.1.2	192.168.254.254	TCP	1056 > http [SYN] Seq=0 Len=0 MSS=1460
11	10.170734	192.168.254.254	172.16.1.2	TCP	http > 1056 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
12	10.170767	172.16.1.2	192.168.254.254	TCP	1056 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
13	10.171086	172.16.1.2	192.168.254.254	HTTP	GET / HTTP/1.1
14	10.171625	192.168.254.254	172.16.1.2	TCP	http > 1056 [ACK] Seq=1 Ack=208 Win=6432 Len=0
15	10.172518	192.168.254.254	172.16.1.2	HTTP	HTTP/1.1 200 OK (text/html)
16	10.172540	192.168.254.254	172.16.1.2	TCP	http > 1056 [FIN, ACK] Seq=448 Ack=208 Win=6432 Len=0
17	10.172567	172.16.1.2	192.168.254.254	TCP	1056 > http [ACK] Seq=208 Ack=449 Win=63793 Len=0
18	10.174196	172.16.1.2	192.168.254.254	TCP	1056 > http [FIN, ACK] Seq=208 Ack=449 Win=63793 Len=0
19	10.174661	192.168.254.254	172.16.1.2	TCP	http > 1056 [ACK] Seq=449 Ack=209 Win=6432 Len=0

Figure 4. Session HTTP capturée

Un exemple de session HTTP capturée est illustré à la figure 4. Avant que HTTP puisse commencer, vous devez créer la session TCP. Ceci est visible dans les trois premières lignes de session, numéros 10,11 et 12. Utilisez la capture ou les données Wireshark semblables pour répondre aux questions suivantes :

3. Renseignez le tableau suivant à partir des informations disponibles dans la session HTTP :

Adresse IP du navigateur Web	
Adresse IP du serveur Web	
Protocole de couche transport (UDP/TCP)	
Numéro de port du navigateur Web	
Numéro de port du serveur Web	

4. Quel ordinateur a lancé la session HTTP, et comment ?

_____

_____

5. Quel ordinateur a signalé au départ une fin de la session HTTP, et comment ?

_____

_____

6. Sélectionnez la première ligne du protocole HTTP, une requête **GET** provenant du navigateur Web. Dans la figure 4 ci-dessus, la requête **GET** s'affiche sur la ligne 13. Allez dans la deuxième fenêtre Wireshark (du milieu) pour examiner les protocoles en couches. Si nécessaire, développez les champs.
7. Quel protocole est intégré (encapsulé) au segment TCP ?

_____

8. Développez le dernier enregistrement de protocole, et tout sous-champ. Il s'agit des informations réelles envoyées au serveur Web. Renseignez le tableau suivant à l'aide des informations provenant du protocole.

Version du protocole	
Méthode de requête	
* URI de requête	
Langue	

* L'URI de requête est le chemin d'accès au document demandé. Dans le premier navigateur, le chemin d'accès est le répertoire racine du serveur Web. Bien qu'aucune page ne soit demandée, certains serveurs Web sont configurés pour afficher un fichier par défaut (si disponible).

Le serveur Web répond avec le paquet HTTP suivant. À la figure 4, ceci s'affiche sur la ligne 15. Une réponse au serveur Web est possible car le serveur Web (1) comprend le type de requête et (2) dispose d'un fichier à retourner. Parfois, les pirates informatiques envoient des requêtes inconnues ou déformées au serveur Web afin d'arrêter le serveur ou d'accéder à la ligne de commande du serveur. En outre, une requête de page Web inconnue entraîne un message d'erreur.

9. Sélectionnez la réponse du serveur Web, puis accédez à la deuxième fenêtre (du milieu). Ouvrez tous les sous-champs réduits de HTTP. Notez les informations renvoyées à partir du serveur. Dans cette réponse, seules quelques lignes de texte figurent (les réponses du serveur web peuvent contenir des milliers ou des millions d'octets). Le navigateur Web comprend et met en forme correctement les données dans la fenêtre du navigateur. .
10. Quelle est la réponse du serveur Web à la requête **GET** du client Web ?

_____

11. Que signifie cette réponse ?

_____

12. Faites défiler la fenêtre supérieure de Wireshark jusqu'à ce que la deuxième session HTTP, actualisation, soit visible. Un exemple de capture est illustré à la figure 5.

```
21 12.487941   172.16.1.2        192.168.254.254   TCP    1057 > http [SYN] Seq=0 Len=0 MSS=1460
22 12.488485   192.168.254.254   172.16.1.2        TCP    http > 1057 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
23 12.488526   172.16.1.2        192.168.254.254   TCP    1057 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
24 12.488864   172.16.1.2        192.168.254.254   HTTP   GET / HTTP/1.1
25 12.489370   192.168.254.254   172.16.1.2        TCP    http > 1057 [ACK] Seq=1 Ack=294 Win=6432 Len=0
26 12.489927   192.168.254.254   172.16.1.2        HTTP   HTTP/1.1 304 Not Modified
27 12.489953   192.168.254.254   172.16.1.2        TCP    http > 1057 [FIN, ACK] Seq=145 Ack=294 Win=6432 Len=0
28 12.489989   172.16.1.2        192.168.254.254   TCP    1057 > http [ACK] Seq=294 Ack=146 Win=64096 Len=0
29 12.490345   172.16.1.2        192.168.254.254   TCP    1057 > http [FIN, ACK] Seq=294 Ack=146 Win=64096 Len=0
30 12.490705   192.168.254.254   172.16.1.2        TCP    http > 1057 [ACK] Seq=146 Ack=295 Win=6432 Len=0
```

Figure 5. Session HTTP capturée pour l'actualisation

La signification de l'actualisation figure dans la réponse du serveur, `304 Not Modified`. Avec un seul paquet retourné pour la requête **GET** initiale et l'actualisation, la bande passante utilisée est minime. Toutefois, pour une réponse initiale qui contient des millions d'octets, un seul paquet de réponse peut faire gagner une bande passante significative.

Comme cette page Web a été enregistrée dans le cache du client Web, la requête **GET** contenait les instructions supplémentaires suivantes à l'intention du serveur Web :

```
If-modified-since: Fri, 26 Jan 2007 06:19:33 GMT\r\n
If-None-Match: "98072-b8-82da8740"\r\n
```
<- numéro d'étiquette de la page (ETAG)

13. Quelle est la réponse ETAG du serveur Web ?

_____

Tâche 3 : capture et analyse de la communication FTP entre l'ordinateur hôte pod et un serveur Web.

Le protocole FTP de la couche application a subi une révision significative depuis sa première publication dans la RFC 114 de 1971. FTP version 5.1 est défini dans la RFC 959 d'octobre 1985

Vous pouvez utiliser ce navigateur Web standard pour communiquer avec d'autres composants que le serveur HTTP. Dans cette tâche, le navigateur Web et un utilitaire FTP de ligne de commande sont utilisés pour télécharger les données à partir d'un serveur FTP.

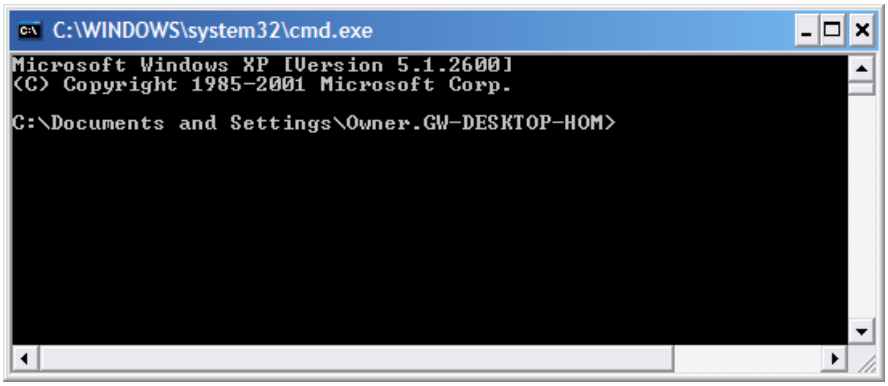


Figure 6. Écran de ligne de commande Windows

En préparation de cette tâche, ouvrez une ligne de commande sur l'ordinateur hôte pod. Pour effectuer ceci, cliquez sur **Démarrer > Exécuter**, tapez **CMD**, puis cliquez sur **OK**. Un écran similaire à la figure 6 apparaît.

Étape 1 : lancement de la capture à l'aide de Wireshark.

Si nécessaire, reportez-vous aux tâches 1 et 2 pour ouvrir Wireshark.

Étape 2 : démarrage du client FTP de la ligne de commande de l'hôte pod.

1. Démarrez une session FTP de l'ordinateur hôte pod avec le serveur FTP, à l'aide de l'utilitaire de client FTP de Windows. Pour l'authentification, utilisez l'ID d'utilisateur **anonyme**. En réponse à l'invite du mot de passe, appuyez sur <**ENTRÉE**>.

```
> ftp eagle-server.example.com
Connected to eagle-server.example.com.
 220 Welcome to the eagle-server FTP service.
User (eagle-server.example.com:(none)): anonymous
331 Please specify the password.
Password: <ENTRÉE>
230 Login successful.
```

2. L'invite du client FTP est `ftp>`. Le client attend donc une commande à envoyer au serveur FTP. Pour afficher une liste de commandes pour le client FTP, tapez **`help <ENTRÉE>`** :

```
ftp> help
Les commandes peuvent être abrégées.  Les commandes sont les
suivantes :

!           delete      literal     prompt      send
?           debug       ls          put         status
append      dir         mdelete     pwd         trace
ascii       disconnect  mdir        quit        type
bell        get         mget        quote       user
binary      glob        mkdir       recv        verbose
bye         hash        mls         remotehelp
cd          help        mput        rename
close       lcd         open        rmdir
```

Malheureusement, la plupart des commandes du client FTP complique l'emploi de l'utilitaire de ligne de commande pour un novice. Nous n'utilisons que quelques commandes pour l'évaluation de Wireshark.

3. Tapez la commande **dir** pour afficher le contenu de répertoire actuel :

```
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Jan 12 04:32 pub
```

Le client FTP figure au répertoire racine du serveur FTP. Il ne s'agit pas du répertoire réel mais du niveau le plus haut auquel l'utilisateur **anonyme** peut accéder. L'utilisateur **anonymous** a été placé dans une prison racine, qui lui interdit l'accès en dehors du répertoire actuel.

4. Les sous-répertoires peuvent être cependant parcourus, et les fichiers transférés vers l'ordinateur hôte pod. Allez dans le répertoire pub/eagle_labs/eagle1/chapter2, téléchargez un fichier, et quittez le répertoire.

```
ftp> cd pub/eagle_labs/eagle1/chapter2
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 0 100     5853 Jan 12 04:26 ftptoeagle-server.pcap
-rw-r--r--  1 0 100     4493 Jan 12 04:27 http to eagle-server.pcap
-rw-r--r--  1 0 100     1486 Jan 12 04:27 ping to 192.168.254.254.pcap
-rw-r--r--  1 0 100 15163750 Jan 12 04:30 wireshark-setup-0.99.4.exe
226 Directory send OK.
ftp: 333 bytes received in 0.04Seconds 8.12Kbytes/sec.
ftp> get "ftptoeagle-server.pcap"
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ftptoeagle-server.pcap (5853 bytes).
226 File send OK.
ftp: 5853 bytes received in 0.34Seconds 17.21Kbytes/sec.
ftp> quit
221 Goodbye.
```

5. Fermez la fenêtre de ligne de commande avec la commande exit.
6. Arrêtez les captures Wireshark, et enregistrez-les sous FTP_Command_Line_Client.

Étape 3 : démarrage du navigateur Web de l'hôte pod.

1. Démarrez à nouveau les captures Wireshark.

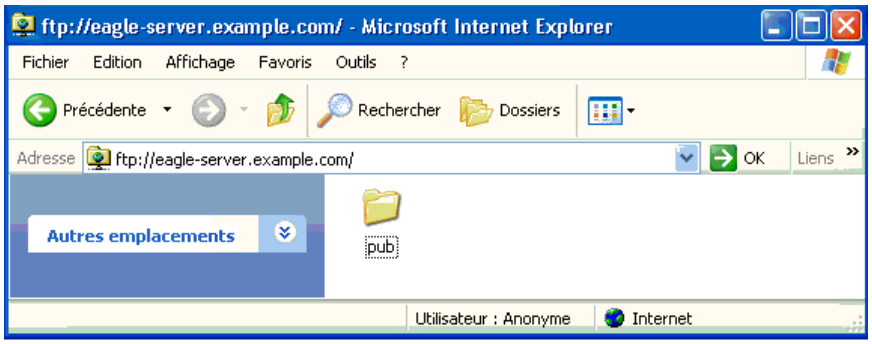


Figure 7. Navigateur Web utilisé comme client FTP

2. Ouvrez un navigateur Web comme illustré à la figure 7, et tapez l'URL `ftp://eagle-server.example.com`. Une fenêtre de navigateur s'ouvre avec le répertoire pub affiché. En outre, le navigateur Web s'est connecté au serveur FTP en tant qu'utilisateur Anonyme, comme illustré au bas de la capture d'écran.
3. À l'aide du navigateur, faites défiler vers le bas la liste de répertoires jusqu'à ce que le chemin d'accès à l'URL soit `pub/eagle-labs/eagle1/chapter2`. Double-cliquez sur le fichier `ftptoeagle-server.pcap` et enregistrez-le.
4. Une fois que vous avez terminé, fermez le navigateur Web.
5. Arrêtez les captures Wireshark, et enregistrez-les sous FTP_Web_Browser_Client.

Étape 4 : arrêt des captures Wireshark et analyse des données capturées.

1. Si ce n'est pas déjà fait, ouvrez la capture Wireshark FTP_Web_Browser_Client.
2. Dans la fenêtre Wireshark supérieure, sélectionnez la capture FTP qui est la première transmission de protocole FTP, Réponse : 220. Il s'agit de la ligne 23 à la figure 8.

No.	Time	Source	Destination	Protocol	Info
12	16.276555	172.16.1.2	192.168.254.254	DNS	Standard query A eagle-server.example.com
13	16.277284	192.168.254.254	172.16.1.2	DNS	Standard query response A 192.168.254.254
14	16.278059	172.16.1.2	192.168.254.254	TCP	1073 > ftp [SYN] Seq=0 Len=0 MSS=1460
15	16.278540	192.168.254.254	172.16.1.2	TCP	ftp > 1073 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
16	16.278575	172.16.1.2	192.168.254.254	TCP	1073 > ftp [ACK] Seq=1 Ack=1 Win=64240 Len=0
23	26.281472	192.168.254.254	172.16.1.2	FTP	Response: 220 Welcome to the eagle-server FTP service.
24	26.281672	172.16.1.2	192.168.254.254	FTP	Request: USER anonymous
25	26.282120	192.168.254.254	172.16.1.2	TCP	ftp > 1073 [ACK] Seq=47 Ack=17 Win=5840 Len=0
26	26.282137	192.168.254.254	172.16.1.2	FTP	Response: 331 Please specify the password.
27	26.282201	172.16.1.2	192.168.254.254	FTP	Request: PASS IEUser@
28	26.283451	192.168.254.254	172.16.1.2	FTP	Response: 230 Login successful.
29	26.313423	172.16.1.2	192.168.254.254	FTP	Request: opts utf8 on
30	26.313959	192.168.254.254	172.16.1.2	FTP	Response: 501 Option not understood.
31	26.314042	172.16.1.2	192.168.254.254	FTP	Request: syst
32	26.314493	192.168.254.254	172.16.1.2	FTP	Response: 215 UNIX Type: L8
33	26.314595	172.16.1.2	192.168.254.254	FTP	Request: site help
34	26.315028	192.168.254.254	172.16.1.2	FTP	Response: 550 Permission denied.
35	26.315113	172.16.1.2	192.168.254.254	FTP	Request: PWD
36	26.315566	192.168.254.254	172.16.1.2	FTP	Response: 257 "/"
37	26.352350	172.16.1.2	192.168.254.254	FTP	Request: noop
38	26.352821	192.168.254.254	172.16.1.2	FTP	Response: 200 NOOP ok.
39	26.482680	172.16.1.2	192.168.254.254	FTP	Request: CWD /
40	26.483243	192.168.254.254	172.16.1.2	FTP	Response: 250 Directory successfully changed.
41	26.484334	172.16.1.2	192.168.254.254	FTP	Request: TYPE A
42	26.484824	192.168.254.254	172.16.1.2	FTP	Response: 200 Switching to ASCII mode.
43	26.485292	172.16.1.2	192.168.254.254	FTP	Request: PORT 172,16,1,2,4,50
44	26.485800	192.168.254.254	172.16.1.2	FTP	Response: 200 PORT command successful. Consider using PASV.
45	26.485892	172.16.1.2	192.168.254.254	FTP	Request: LIST
46	26.486503	192.168.254.254	172.16.1.2	TCP	ftp-data > 1074 [SYN] Seq=0 Len=0 MSS=1460 TSV=12998374 TSER=0 WS=2
47	26.486558	172.16.1.2	192.168.254.254	TCP	1074 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=0 TSV=0 TSER=
48	26.486948	192.168.254.254	172.16.1.2	TCP	ftp-data > 1074 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=12998375 TSER=0
49	26.487052	192.168.254.254	172.16.1.2	FTP	Response: 150 Here comes the directory listing.
50	26.487252	192.168.254.254	172.16.1.2	FTP-DA	FTP Data: 61 bytes
51	26.487267	192.168.254.254	172.16.1.2	FTP	Response: 226 Directory send OK.

Figure 8. Capture Wireshark d'une session FTP avec un navigateur Web

3. Allez dans la fenêtre Wireshark du milieu et développez le protocole FTP. Ce dernier communique à l'aide de codes, tout comme HTTP.

Qu'est-ce que la réponse 220 du serveur FTP ?

_____

Lorsque le serveur FTP a envoyé une réponse : 331 Spécifiez le mot de passe, quelle a été la réponse du navigateur Web ?

_____

Quel numéro de port le client FTP utilise-t-il pour se connecter au port 21 du serveur FTP ?

_____

Lors du transfert de données ou avec une simple liste de répertoires, un nouveau port est ouvert. Il s'agit du mode de transfert. Ce mode peut être actif ou passif. En mode actif, le serveur ouvre une session TCP à l'intention du client FTP et transfère les données sur ce port précis. Le numéro du port source du serveur FTP est 20. En outre, le numéro du port du client FTP est un numéro supérieur à 1023. Toutefois, le client ouvre un nouveau port à l'intention du serveur pour le transfert des données. Les deux numéros de ports sont supérieurs à 1023.

Quel est le numéro de port FTP-DATA que le serveur FTP utilise ?

_____

4. Ouvrez la capture Wireshark FTP_Web_Browser_Client, et observez la communication FTP. Bien que les clients soient différents, les commandes sont semblables.

Étape 5 : modes de transfert actif et passif de FTP

Les implications entre les deux modes sont très importantes d'un point de vue de la sécurité des informations. Le mode de transfert définit la configuration du port de données.

En mode de transfert actif, un client démarre une session FTP avec le serveur sur le port 21 standard de TCP. Pour le transfert des données, le serveur lance une connexion à partir du port 20 standard de TCP vers le port élevé d'un client, un numéro de port supérieur à 1023. Reportez-vous à la figure 9.

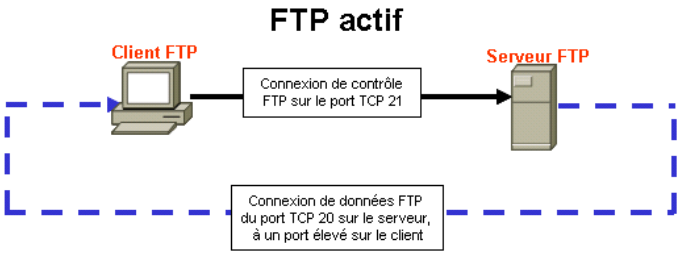


Figure 9.

Sauf si le pare-feu du client FTP est configuré pour autoriser les connexions de l'extérieur, le transfert de données risque d'échouer. Afin d'établir la connectivité pour le transfert des données, le client FTP doit autoriser les connexions FTP (ce qui sous-entend le filtrage dynamique des paquets), ou désactiver le blocage.

En mode de transfert passif, un client démarre une session FTP avec le serveur sur le port 21 standard de TCP. Il s'agit de la même connexion utilisée en mode de transfert actif. Pour le transfert des données, cependant, deux modifications majeures interviennent. Premièrement, le client établit la connexion des données avec le serveur. Deuxièmement, les ports élevés sont utilisés aux deux extrémités de la connexion. Reportez-vous à la figure 10.

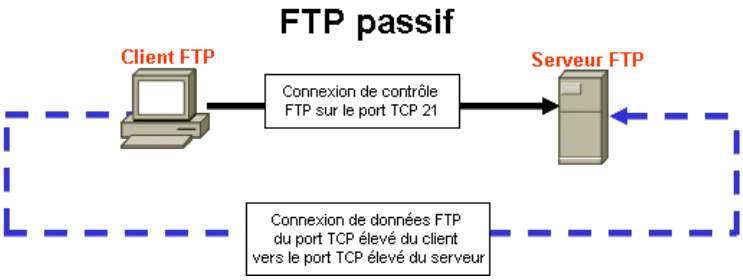


Figure 10.

Sauf si le serveur FTP est configuré pour autoriser une connexion avec un port élevé aléatoire, le transfert des données échoue. Seules quelques applications clientes de FTP acceptent les modifications apportées au mode de transfert.

Tâche 4 : Remarques générales

La communication des protocoles HTTP et FTP repose sur TCP. TCP gère la connexion entre le client et le serveur pour garantir la transmission des datagrammes.

Une application cliente peut être soit un navigateur Web soit un utilitaire de ligne de commande. Toutefois, chacun doit envoyer et recevoir des messages qui peuvent être correctement interprétés. Le protocole de communication est généralement défini dans une RFC.

Le client FTP doit s'authentifier auprès du serveur FTP, même si l'authentification est ouverte à tout le monde. L'utilisateur Anonyme dispose normalement d'un accès restreint au serveur FTP et ne peut donc pas télécharger de fichiers.

Une session HTTP commence lorsqu'une requête est transmise au serveur HTTP et se termine lorsque le client HTTP a accusé réception de la réponse. Une session FTP, cependant, dure jusqu'à ce que le client signale qu'il la quitte avec la commande **`quit`**.

HTTP utilise un protocole unique pour communiquer avec le serveur HTTP. Le serveur écoute les connexions de clients sur le port 80. FTP utilise, cependant, deux protocoles. Le serveur FTP écoute sur le port 21 de TCP, comme la ligne de commande. Selon le mode de transfert, le serveur ou le client peut établir la connexion des données.

Vous pouvez accéder à plusieurs protocoles de la couche application par un simple navigateur Web. Alors que seuls HTTP et FTP ont été examinés, le navigateur peut également prendre en charge Telnet et Gopher. Le navigateur sert de client au serveur. Il envoie des requêtes et traite les réponses.

Tâche 5 : confirmation

Tout en activant la capture Wireshark, utilisez un navigateur Web pour accéder à R2 à l'adresse http://172.16.255.254/level/7/exec ou utilisez un client Telnet pour vous connecter à un périphérique Cisco tel que S1-Central ou R2-Central. Observez le comportement du protocole HTTP ou Telnet. Transmettez les commandes pour observer les résultats.

Dans quelle mesure le protocole Telnet de la couche application est-il semblable à HTTP et FTP ? En quoi TELNET est-il différent ?

_____

_____

Tâche 6 : nettoyage

Si l'installation de Wireshark a eu lieu sur l'ordinateur hôte pod pour ces travaux pratiques, il se peut que le formateur souhaite la suppression de l'application. Pour supprimer Wireshark, cliquez sur **Démarrer > Panneau de configuration > Ajout/Suppression de programmes**. Faites défiler la liste vers le bas, cliquez avec le bouton droit sur **Wireshark**, puis cliquez sur **Supprimer**.

Si vous devez supprimer les fichiers téléchargés de l'ordinateur hôte pod, effacez tous les fichiers récupérés à partir du serveur FTP.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

4.6.1 : exercice d'intégration des compétences : analyse des couches application et transport

Diagramme de topologie

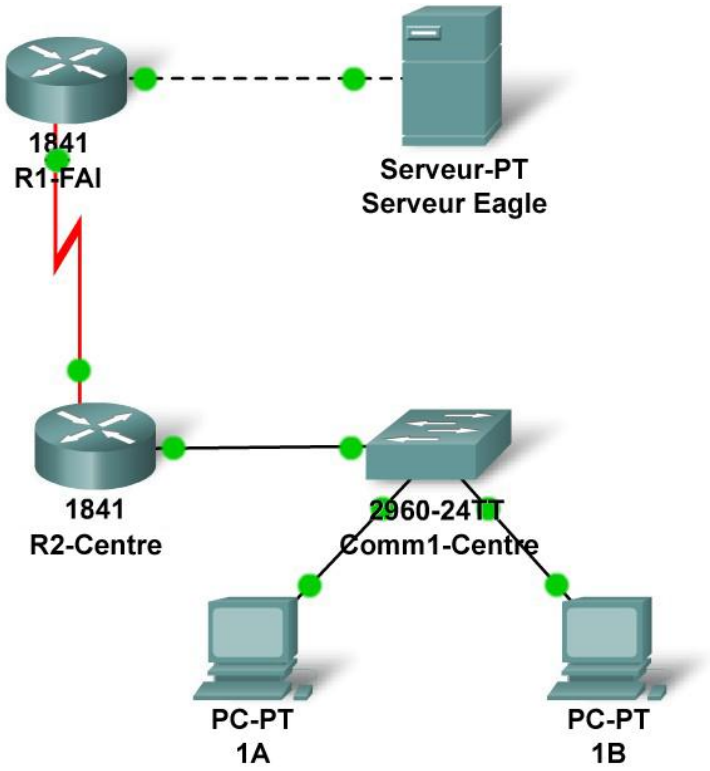


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	Fa0/0	192.168.254.253	255.255.255.0	N/A
	S0/0/0	10.10.10.6	255.255.255.252	N/A
R2-Central	Fa0/0	172.16.255.254	255.255.0.0	N/A
	S0/0/0	10.10.10.5	255.255.255.252	N/A
S1-Central	VLAN 1	172.16.254.1	255.255.0.0	172.16.255.254
PC 1A	La carte réseau	172.16.1.1	255.255.0.0	172.16.255.254
PC 1B	La carte réseau	172.16.1.2	255.255.0.0	172.16.255.254
Serveur Eagle	La carte réseau	192.168.254.254	255.255.255.0	192.168.254.253

Objectifs pédagogiques

- Configurer les hôtes et les services
- Connecter et configurer les hôtes et les services sur le modèle de réseau des travaux pratiques
- Analyser l'interaction entre DNS, UDP, HTTP et UDP
- Visualiser le fonctionnement de DNS, UDP, HTTP et TCP sur le modèle de réseau des travaux pratiques en mode Simulation

Contexte

Tout au long de ce cours, vous allez utiliser une configuration de travaux pratiques type constituée de PC, de serveurs, de routeurs et de commutateurs réels dans l'optique d'apprendre des concepts liés aux réseaux. À la fin de chaque chapitre, vous construirez des parties de plus en plus importantes de cette topologie dans Packet Tracer et analyserez des interactions de protocoles de plus en plus complexes.

Tâche 1 : réparation et test de la topologie

Le serveur a été remplacé. Il doit être mis sous tension. Configurez-le ensuite avec les paramètres suivants : adresse IP 192.168.254.254, masque de sous-réseau 255.255.255.0, passerelle par défaut 192.168.254.253, service DNS activé, en associant eagle-server.example.com à l'adresse IP du serveur, service HTTP activé. Reliez le serveur Eagle Server au port Fa0/0 du routeur R1-ISP avec un câble de croisement.

Le PC 1A a perdu ses informations d'adresse IP. Configurez-le avec les paramètres suivants : adresse IP 172.16.1.1, masque de sous-réseau 255.255.0.0, passerelle par défaut 172.16.255.254 et serveur DNS 192.168.254.254. Reliez le PC 1A au port Fa0/1 du commutateur S1-Central avec un câble direct.

Vérifiez votre travail en vous basant sur les informations affichées par le bouton **Check Results** et l'onglet **Assessment Items**. Testez la connectivité en temps réel entre le PC 1A et le serveur Eagle Server en utilisant l'option ADD SIMPLE PDU.

Sachez que lorsque vous ajoutez une unité de données de protocole simple, elle apparaît dans la fenêtre PDU List en tant que partie intégrante du « Scenario 0 ». La première fois que vous émettrez ce message ping ponctuel, celui-ci échouera (libellé « **Failed** ») en raison du processus ARP, qui vous sera expliqué ultérieurement. Si vous double-cliquez sur le bouton Â« Fire Â» dans la fenêtre PDU List, ce message de test ping unique sera envoyé une deuxième fois. Cette fois, il aboutira. Dans Packet Tracer, le terme « scenario » représente une configuration spécifique d'un ou plusieurs paquets de test. Vous pouvez créer différents scénarios de paquet de test en utilisant le bouton **New**. Par exemple, Scenario 0 peut représenter un paquet de test entre le PC 1A et le serveur Eagle Server ; Scenario 1 peut correspondre à des paquets de test entre le PC 1B et les routeurs ; et ainsi de suite. Vous pouvez supprimer tous les paquets de test d'un scénario donné en utilisant le bouton **Delete**. Ainsi, si vous utilisez le bouton **Delete** pour Scenario 0, le paquet de test que vous venez de créer entre le PC 1A et le serveur Eagle Server sera supprimé (veillez à effecteur cette opération avant la prochaine tâche).

Tâche 2 : analyse de l'interaction entre DNS, UDP, HTTP et TCP

Passez du mode Realtime au mode Simulation. Assurez-vous que le filtre d'événements (Event Filter) est défini de façon à afficher DNS, UDP, HTTP, TCP et ICMP. Ouvrez un navigateur Web à partir du Bureau de 1A. Tapez l'adresse URL du serveur eagle-server.example.com, appuyez sur Entrée, puis utilisez le bouton **Capture / Forward** dans la liste d'événements (**Event List**) pour capturer l'interaction de DNS, UDP, HTTP et TCP.

Vous pouvez examiner le paquet de deux façons différentes : en cliquant sur l'enveloppe du paquet lorsque celle-ci s'affiche dans l'animation ou en cliquant sur la colonne **Info** du paquet dès qu'il apparaît dans la liste d'événements (**Event List**). Visualisez cette animation et examinez le contenu des paquets (fenêtre **PDU Information**, **Inbound PDU Details, Outbound PDU Details**) pour chaque événement contenu dans la liste, particulièrement lorsque les paquets se trouvent au niveau du PC 1A ou du serveur Eagle Server. Si vous recevez le message « Buffer Full » (mémoire tampon saturée), cliquez sur le bouton **View Previous Events**. Bien que le traitement des paquets par le commutateur et les routeurs puisse encore vous paraître étranger, vous devriez être en mesure d'observer la façon dont DNS, UDP, HTTP et TCP interagissent en étudiant le traçage des paquets et en utilisant la fenêtre PDU Information pour les examiner de l'intérieur.

Remarques générales

Êtes-vous en mesure de schématiser la séquence d'événements de protocoles impliqués dans la demande d'une page Web en utilisant une adresse URL ? Quels sont les points à risques ? Comparez et confrontez DNS et HTTP, puis UDP et TCP.

Travaux pratiques 5.5.1 : examen d'une passerelle de périphérique

Schéma de la topologie

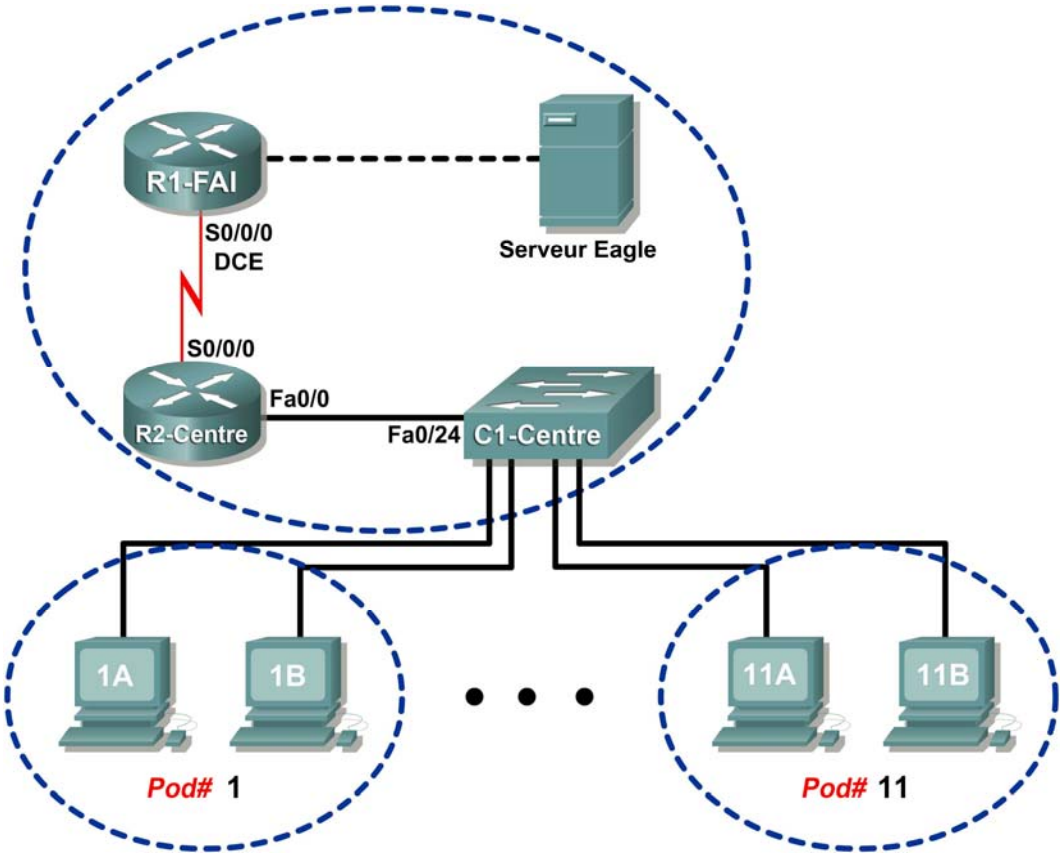


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/D
	Fa0/0	192.168.254.253	255.255.255.0	N/D
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/D
	Fa0/0	172.16.255.254	255.255.0.0	N/D
Eagle Server	N/D	192.168.254.254	255.255.255.0	192.168.254.253
	N/D	172.31.24.254	255.255.255.0	N/D
hôte*Pod#***A**	N/D	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
hôte*Pod#***B**	N/D	172.16. *Pod#.*2	255.255.0.0	172.16.255.254
S1-Central	N/D	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- comprendre et expliquer la fonction d'une adresse de passerelle ;
- comprendre la configuration des informations réseau sur un ordinateur Windows ;
- dépanner un problème d'adresse de passerelle masquée.

Contexte

Une adresse IP comprend deux parties : réseau et hôte. Un ordinateur, qui communique avec un autre périphérique, doit d'abord connaître le mode d'accès de ce dernier. Pour les périphériques sur le même réseau local, la partie hôte de l'adresse IP sert d'identificateur. La partie réseau du périphérique de destination est identique à celle du périphérique hôte.

Toutefois, les numéros de réseaux source et destination sont différents pour les périphériques sur des réseaux distincts. La partie réseau de l'adresse IP permet d'identifier le moment où un paquet doit être envoyé à une adresse passerelle. Cette dernière est attribuée à un périphérique réseau qui transfère les paquets entre les réseaux distants.

Une adresse de passerelle est attribuée au routeur pour tous les périphériques qui figurent sur le réseau local. Une des fonctions du routeur consiste à servir de point d'entrée aux paquets qui entrent dans le réseau et de point de sortie à ceux qui le quittent.

Les adresses de passerelles sont primordiales pour les utilisateurs. Cisco estime que 80 % du trafic réseau sont destinés aux périphériques sur d'autres réseaux. Les autres 20 % s'appliquent aux périphériques locaux. Il s'agit de la règle 80/20. Par conséquent, si des périphériques de réseau local ne peuvent pas accéder à une passerelle, les utilisateurs ne pourront pas effectuer leur tâche.

Scénario

Les ordinateurs hôtes pod doivent communiquer avec Eagle Server. Toutefois, ce dernier figure sur un réseau différent. Si la configuration de l'adresse de passerelle de l'ordinateur hôte pod est incorrecte, la connectivité avec le Eagle Server échoue.

À l'aide de plusieurs utilitaires courants, la configuration réseau sur un ordinateur hôte pod est vérifiée.

Tâche 1 : compréhension et explication de la fonction d'une adresse de passerelle.

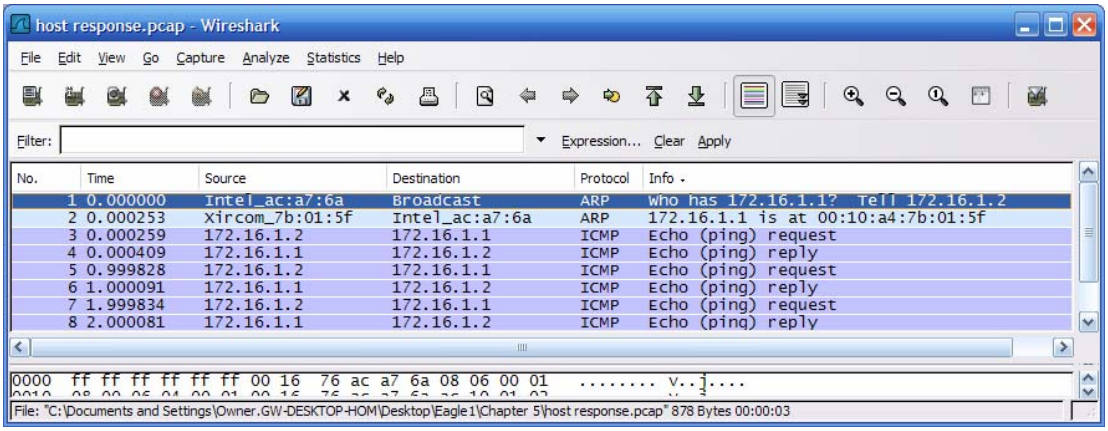


Figure 1. Communication entre les périphériques de réseau local

Pour le trafic LAN (réseau local), l'adresse de passerelle est celle de l'interface Ethernet connectée au réseau local. La figure 1 illustre deux périphériques qui communiquent avec la commande **ping** sur le même réseau. Tout périphérique qui possède la même adresse réseau, dans cet exemple : `172.16.0.0`, figure sur le même réseau local.

Selon la figure 1, quelle est l'adresse MAC du périphérique réseau sur l'adresse IP 172.16.1.1 ?

___ _____

Plusieurs commandes de Windows permettent d'afficher une adresse de passerelle réseau. Une commande standard est **`netstat –r`**. Dans le texte suivant, la commande **`netstat –r`** permet de visualiser les adresses de passerelle de cet ordinateur. La sélection du haut indique l'adresse de passerelle qui permet de transférer tous les paquets réseau destinés à l'extérieur du réseau local. Les valeurs Network Destination et Netmask « à 4 zéros », `0.0.0.0` et `0.0.0.0`, font référence à *tout* réseau non spécifiquement connu. Pour tout réseau non local, cet ordinateur utilise `172.16.255.254` comme adresse par défaut. La deuxième sélection en jaune affiche les informations au format lisible par l'homme. D'autres réseaux spécifiques sont accessibles par d'autres adresses de passerelles. Une interface locale, appelée interface de bouclage, est automatiquement attribuée au réseau `127.0.0.0`. Cette interface permet d'identifier l'hôte local des services du réseau local. Reportez-vous à l'entrée sélectionnée en gris. Finalement, tout périphérique sur le réseau `172.16.0.0` est accessible par la passerelle `172.16.0.0`, l'adresse IP de cette interface Ethernet. Cette entrée est sélectionnée en vert.

```
C:\>netstat –r

Table de routage
===========================================================================
Liste d'Interfaces
0x1 ........................ MS TCP Loopback interface
0x20005 ...00 16 76 ac a7 6a  Intel(R) 82562V 10/100 Network Connection
===========================================================================
===========================================================================
Itinéraires actifs :
Destination réseau     Masque réseau        Adr. passerelle     Adr.
interface  Métrique
          0.0.0.0          0.0.0.0   172.16.255.254  172.16.1.2   1
        127.0.0.0        255.0.0.0        127.0.0.1   127.0.0.1   1
      172.16.0.0      255.255.0.0       172.16.1.2  172.16.1.2  20
      172.16.1.2  255.255.255.255        127.0.0.1   127.0.0.1  20
  172.16.255.255  255.255.255.255       172.16.1.2  172.16.1.2  20
255.255.255.255  255.255.255.255       172.16.1.2  172.16.1.2   1
Passerelle par défaut :    172.16.255.254
===========================================================================
Routes persistantes :
  Aucun
C:\ >
```

Étape 1 : ouverture d'une fenêtre de ligne de commande sur un ordinateur hôte pod.

Quelle est l'adresse de passerelle par défaut ?

_____

Étape 2 : utilisation de la commande `ping` pour vérifier la connectivité avec l'adresse IP `127.0.0.1`.

La commande a-t-elle été exécutée correctement ? _____

Étape 3 : utilisation de la commande ping pour envoyer une requête ping vers différentes adresses sur le réseau `127.0.0.0`, `127.10.1.1`, et `127.255.255.255`.

Les réponses ont-elles été validées ? Si non, pourquoi ?

_____

_____

Une adresse de passerelle par défaut permet à un périphérique réseau de communiquer avec d'autres périphériques sur différents réseaux. Par essence, c'est la porte vers d'autres réseaux. Tout le trafic destiné à différents réseaux doit passer par le périphérique réseau qui possède l'adresse de passerelle par défaut.

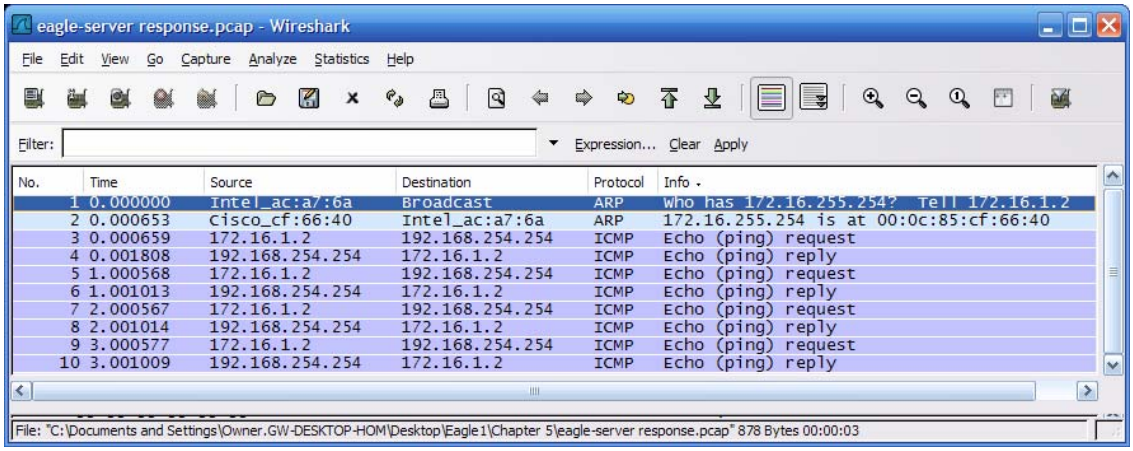


Figure 2. Communication entre des périphériques sur différents réseaux

Comme illustré à la figure 2, la communication entre des périphériques sur des réseaux distincts est différente d'un réseau local. L'ordinateur hôte pod N°2, adresse IP `172.16.1.2`, exécute une requête ping à l'adresse IP `192.168.254.254`. Comme le réseau `172.16.0.0` est différent de `192.168.254.0`, l'ordinateur hôte pod demande l'adresse MAC du périphérique de passerelle par défaut. Ce dernier, un routeur, répond avec son adresse MAC. L'ordinateur compose l'en-tête de couche 2 avec l'adresse MAC de destination du routeur et place des trames sur le fil relié au périphérique de passerelle.

Selon la figure 2, quelle est l'adresse MAC du périphérique de passerelle ?

_____

Selon la figure 2, quelle est l'adresse MAC du périphérique réseau avec l'adresse IP 192.168.254.254 ?

_____

Tâche 2 : compréhension de la configuration des informations réseau sur un ordinateur Windows.

Les problèmes de connectivité sont souvent attribués à des paramètres réseau incorrects. Dans le dépannage des problèmes de connectivité, plusieurs outils sont disponibles pour déterminer rapidement la configuration réseau pour tout ordinateur Windows.

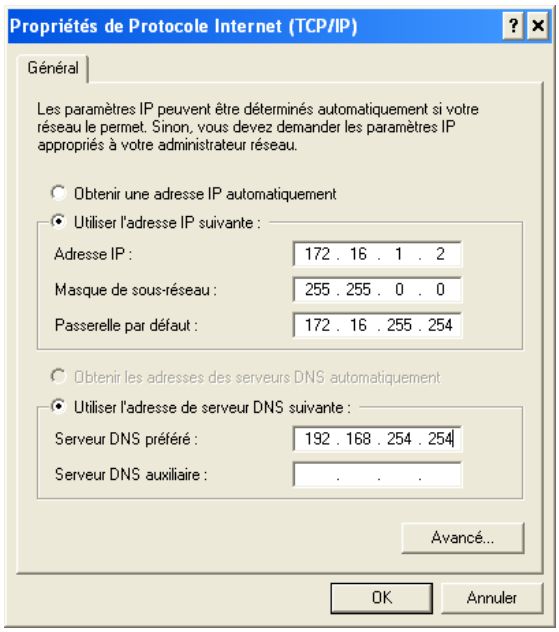


Figure 3. Interface réseau avec adresse IP statique

Étape 1 : examen des paramètres de propriétés réseau.

L'examen des paramètres de propriétés réseau de l'ordinateur hôte pod constitue une méthode qui peut s'avérer utile pour déterminer les propriétés IP de l'interface réseau. Pour accéder à cette fenêtre :

1. Cliquez sur **Démarrer > Panneau de configuration > Connexions réseau**.
2. Cliquez avec le bouton droit sur **Connexion au réseau local**, puis choisissez **Propriétés**.
3. Sur l'onglet **Général**, faites défiler la liste vers le bas, sélectionnez **Protocole Internet (TCP/IP)**, puis cliquez sur le bouton **Propriétés**. Une fenêtre semblable à celle de la figure 3 s'affiche.

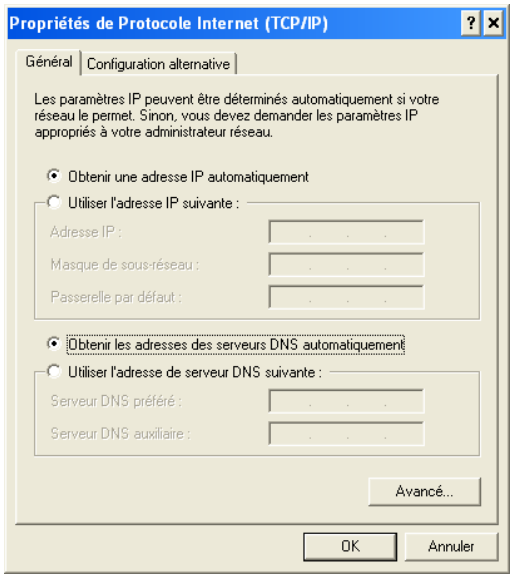


Figure 4. Interface réseau avec adresse IP dynamique

Toutefois, il est possible de configurer une adresse IP dynamique, comme illustré à la figure 4. Dans ce cas, la fenêtre des paramètres de Propriétés réseau n'est pas très utile pour déterminer les informations relatives à l'adresse IP.

L'utilisation de la commande **ipconfig** représente une méthode plus fiable pour déterminer les paramètres réseau sur un ordinateur sous Windows :

```
C:\>ipconfig
Configuration IP de Windows
Carte Ethernet Connexion au réseau local:

        Suffixe DNS propre à la connexion :
❶       Adresse IP. . . . . . . . . . . . : 172.16.1.2
❷       Masque de sous-réseau . . . . . . : 255.255.0.0
❸       Passerelle par défaut . . . . . . : 192.168.254.254
```

❶ Adresse IP pour cet ordinateur hôte pod.
❷ Masque de sous-réseau.
❸ Adresse de la passerelle par défaut.

Plusieurs options sont disponibles avec la commande **ipconfig**. Vous pouvez y accéder à l'aide de la commande **ipconfig /?**. Pour afficher des informations complémentaires sur les connexions réseau, utilisez la commande **ipconfig /all**.

```
C:\>ipconfig /all

Configuration IP de Windows

        Nom de l'hôte . . . . . . . . . . : GW-desktop-hom
        Suffixe DNS principal . . . . . . :
        Type de noud . . . . . . . . . . : Diffusion
        Routage IP activé . . . . . . . . : Non
        Proxy WINS activé . . . . . . . . : Non

Carte Ethernet Connexion au réseau local:

        Suffixe DNS propre à la connexion :
        Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter

        Adresse physique . . . . . . . . .: 00-0C-29-65-FD-80
        DHCP activé. . . . . . . . . . . : Non
        Adresse IP. . . . . . . . . . . . : 172.16.1.2
        Masque de sous-réseau . . . . . . : 255.255.0.0
        Passerelle par défaut . . . . . . : 172.16.254.254
      ❶ Serveurs DNS . . . . . . . . . .  : 192.168.254.254

C:\>
```

❶ Adresse IP du serveur de noms de domaine.

Étape 2 : utilisation de la commande `ipconfig /all` pour renseigner le tableau suivant avec les informations de votre ordinateur hôte pod :

Description	Adresse
Adresse IP	
Masque de sous-réseau	
Passerelle par défaut	
Serveur DNS	

Tâche 3 : dépannage d'un problème d'adresse de passerelle masquée.

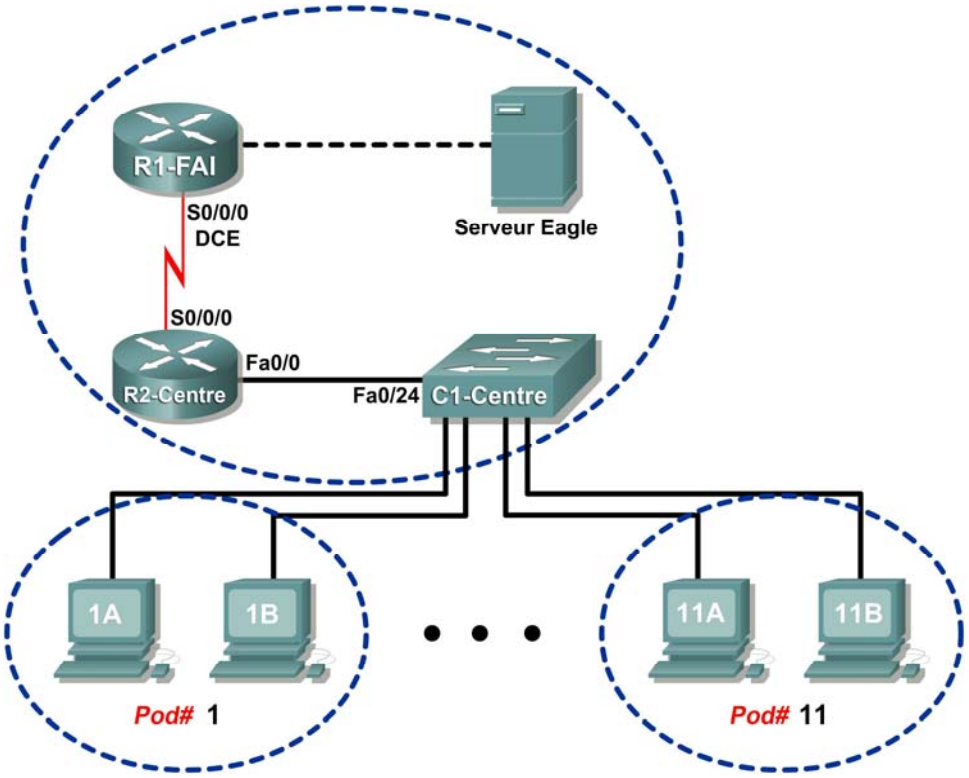


Figure 5. Schéma de topologie

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.4	255.255.255.252	N/D
	Fa0/0	192.168.254.253	255.255.255.0	N/D
R2-Central	S0/0/0	10.10.10.3	255.255.255.252	N/D
	Fa0/0	172.16.255.254	255.255.0.0	N/D
Eagle Server	N/D	192.168.254.254	255.255.255.0	192.168.254.253
	N/D	172.31.24.254	255.255.255.0	N/D
hôte*Pod#***A**	N/D	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
hôte*Pod#***B**	N/D	172.16. *Pod#.*2	255.255.0.0	172.16.255.254
S1-Central	N/D	172.16.254.1	255.255.0.0	172.16.255.254

Tableau 1. Attribution des adresses logiques

Lors du dépannage de problèmes réseau, une connaissance approfondie du réseau peut souvent permettre d'identifier le réel problème. Reportez-vous à la topologie de réseau à la figure 5 et à l'attribution des adresses IP logiques dans le tableau 1.

En tant qu'ingénieur Cisco du centre d'assistance de l'équipe de nuit, le technicien du centre d'assistance sollicite votre aide. Le technicien a reçu un rapport d'incident d'un utilisateur sur l'ordinateur hôte 1A, qui se plaint que l'ordinateur hôte 11B, `host-11B.example.com`, ne répond pas aux requêtes ping. Le technicien a vérifié les câbles et paramètres réseau sur les deux ordinateurs, mais rien d'anormal n'a été détecté. Vous vérifiez auprès de l'ingénieur de réseau d'entreprise, qui signale que R2-Central a été temporairement arrêté pour une mise à niveau du matériel.

Vous acquiescez d'un signe de tête et vous demandez au technicien d'envoyer une requête ping à l'adresse IP pour l'hôte 11B, `172.16.11.2` à partir de l'hôte 1A. Les requêtes ping sont réussies. Ensuite, vous demandez au technicien d'envoyer une requête, `172.16.254.254` et les requêtes ping échouent.

Quel est le problème ?

_____

_____

Vous demandez au technicien du centre d'assistance d'informer l'utilisateur d'employer temporairement l'adresse IP pour l'hôte 11B. L'utilisateur peut ainsi établir la connectivité avec l'ordinateur. Dans l'heure qui suit, le routeur de passerelle fonctionne à nouveau, et le réseau est opérationnel.

Tâche 4 : Remarques générales

Une adresse de passerelle est cruciale à la connectivité du réseau. Dans certains cas, les périphériques du réseau local nécessitent une passerelle par défaut pour communiquer avec d'autres périphériques sur le réseau local.

L'emploi des utilitaires de ligne de commande Windows tels que **`netstat –r`** et **`ipconfig /all`** permet de signaler les paramètres de la passerelle sur les ordinateurs hôtes.

Tâche 5 : confirmation

Wireshark permet de capturer une requête ping entre deux ordinateurs hôtes pod. Il peut s'avérer nécessaire de redémarrer l'ordinateur hôte pour vider le cache du DNS. D'abord, utilisez le nom d'hôte de l'ordinateur pod de destination pour que DNS réponde avec l'adresse IP de destination. Observez la séquence de communication entre les périphériques réseau, particulièrement la passerelle. Ensuite, capturez une requête ping entre les périphériques réseau à l'aide des seules adresses IP. L'adresse de la passerelle est inutile.

Tâche 6 : nettoyage.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

Travaux pratiques 5.5.2 : examen d'une route

Schéma de la topologie

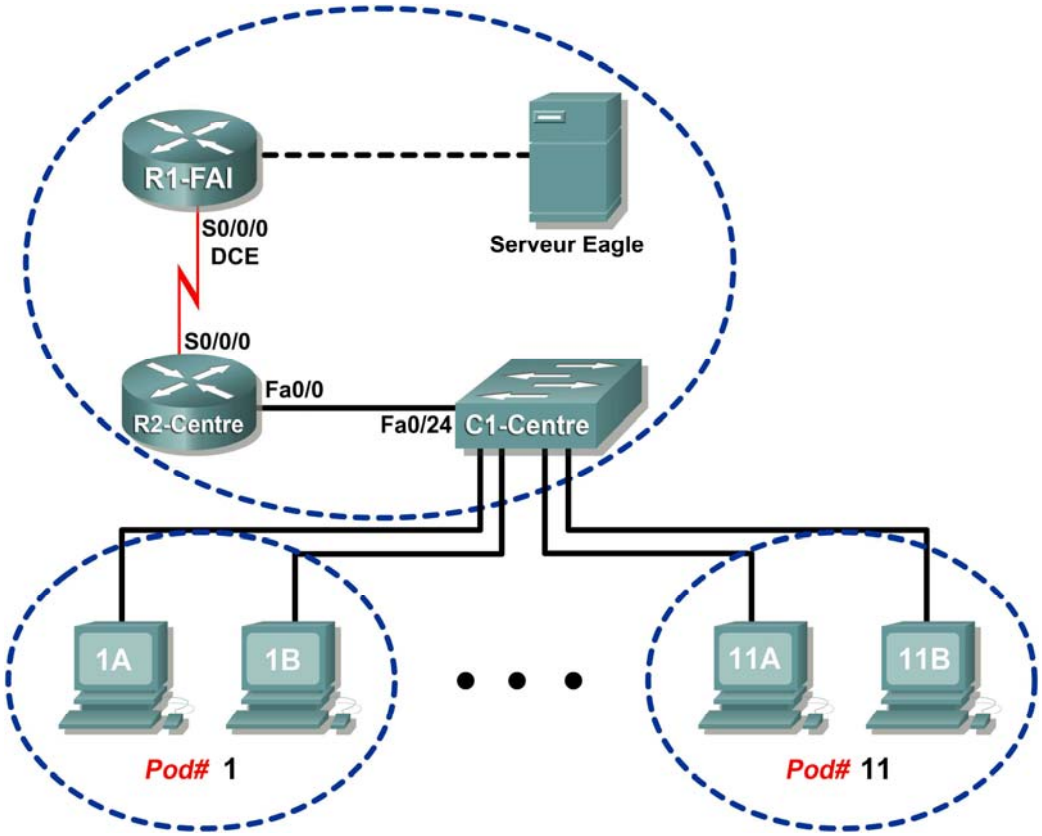


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/D
	Fa0/0	192.168.254.253	255.255.255.0	N/D
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/D
	Fa0/0	172.16.255.254	255.255.0.0	N/D
Eagle Server	N/D	192.168.254.254	255.255.255.0	192.168.254.253
	N/D	172.31.24.254	255.255.255.0	N/D
hôte*Pod#***A**	N/D	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
hôte*Pod#***B**	N/D	172.16. *Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	N/D	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- utiliser la commande **`route`** pour modifier une table de routage pour un ordinateur Windows ;
- utiliser la commande **`telnet`** du client Telnet de Windows pour vous connecter à un routeur Cisco ;
- examiner les routes du routeur à l'aide des commandes IOS standard de Cisco.

Contexte

Un périphérique doit être informé de la route vers le réseau de destination pour que les paquets soient acheminés sur tout le réseau. Ces travaux pratiques comparent l'utilisation des routes dans les ordinateurs Windows et dans le routeur Cisco.

L'ajout de certaines routes aux tables de routage s'effectue automatiquement selon les données de configuration sur l'interface réseau. Le périphérique considère qu'un réseau est directement connecté lorsque son adresse IP et masque de sous-réseau sont configurés. En outre, la route du réseau doit être saisie automatiquement dans la table de routage. Pour les réseaux qui ne sont pas connectés directement, une adresse IP de passerelle par défaut est configurée. Elle envoie le trafic à un périphérique qui doit connaître le réseau.

Scénario

À l'aide d'un ordinateur hôte pod, examinez la table de routage avec la commande **`route`** et identifiez les différentes routes et l'adresse IP de passerelle pour la route. Supprimez la route de la passerelle par défaut, testez la connexion puis réaffectez cette route à la table d'hôtes.

Utilisez un ordinateur hôte pod pour établir une connexion Telnet avec R2-Central, et examinez la table de routage.

Tâche 1 : utilisation de la commande route pour modifier une table de routage d'ordinateur Windows.

```
C:\>netstat –r

Table de routage
===========================================================================
Liste d'Interfaces
0x1 ........................... MS TCP Loopback interface
0x20005 ...00 16 76 ac a7 6a  Intel(R) 82562V 10/100 Network Connection
===========================================================================
===========================================================================
Itinéraires actifs :
Destination réseau     Masque réseau        Adr. passerelle     Adr.
interface  Métrique
        0.0.0.0          0.0.0.0   172.16.255.254  172.16.1.2   1
      127.0.0.0        255.0.0.0        127.0.0.1   127.0.0.1   1
     172.16.0.0      255.255.0.0       172.16.1.2  172.16.1.2  20
     172.16.1.2  255.255.255.255        127.0.0.1   127.0.0.1  20
 172.16.255.255  255.255.255.255       172.16.1.2  172.16.1.2  20
255.255.255.255  255.255.255.255       172.16.1.2  172.16.1.2   1
Passerelle par défaut :    172.16.255.254
===========================================================================
Routes persistantes :
  Aucun
C:\>
```

Figure 1. Résultats de la commande netstat

Illustrés à la figure 1, les résultats de la commande **netstat –r** sont utiles pour déterminer les informations relatives aux routes et aux passerelles.

Étape 1 : examen des routes actives sur un ordinateur Windows.

La commande **route** est utile pour la modification de la table de routage. Contrairement à la commande **netstat –r**, la commande **route** permet d'afficher, d'ajouter, de supprimer ou de modifier les entrées de la table de routage. Pour afficher des informations détaillées sur la **commande route,** utilisez l'option **route /?**.

Vous trouverez ci-après la liste des options abrégées de la commande **route** :

route PRINT	Imprime les routes actives
route ADD	Ajoute une route : route ADD *réseau* MASK *masque passerelle*
route DELETE	Supprime une route : route DELETE *réseau*
route CHANGE	Modifie une route existante

Pour afficher les routes actives, exécutez la commande **route PRINT** :

```
C:\ >route PRINT
===========================================================================
Liste d'Interfaces
0x1 ........................... MS TCP Loopback interface
0x70003 ...00 16 76 ac a7 6a .Intel(R) 82562V 10/100 Network Connection
===========================================================================
===========================================================================
Itinéraires actifs :
Destination réseau    Masque réseau        Adr. passerelle     Adr.
interface  Métrique
        0.0.0.0          0.0.0.0  172.16.255.254      172.16.1.2     1
      127.0.0.0        255.0.0.0       127.0.0.1       127.0.0.1     1
     172.16.0.0      255.255.0.0      172.16.1.2      172.16.1.2    20
     172.16.1.2  255.255.255.255       127.0.0.1       127.0.0.1    20
 172.16.255.255  255.255.255.255      172.16.1.2      172.16.1.2    20
255.255.255.255  255.255.255.255      172.16.1.2      172.16.1.2     1
Passerelle par défaut :    172.16.255.254
===========================================================================
Routes persistantes :
  Aucun
C:\>
```

Vérifiez la connectivité réseau avec Eagle Server :

```
C:\> ping eagle-server.example.com
Envoi d'une requête ping sur eagle-server.example.com
[192.168.254.254] avec 32 octets de données :

Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63

Statistiques Ping pour 192.168.254.254 :
    Paquets : Envoyés = 4, Reçus = 4, Perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
   Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms
C:\>
```

Quelle est l'adresse de passerelle pour `eagle-server.example.com` ?

Étape 2 : suppression d'une route de la table de routage pour l'ordinateur Windows.

Dans quelle mesure la route de passerelle par défaut est-elle importante ? Supprimez la route de passerelle et essayez d'envoyer une requête ping à Eagle Server. Pour effectuer ceci, utilisez la syntaxe :

route DELETE *réseau*

```
C:/> route DELETE 0.0.0.0
```

Examinez la table de routage actif et vérifiez que la route de passerelle par défaut a été supprimée :

Quelle est l'adresse IP de la passerelle par défaut ?

_____

Essayez d'envoyer une requête active à Eagle Server. Quels sont les résultats ?

_____

Si l'adresse IP de passerelle par défaut est supprimée, comment accéder au serveur de noms de domaine (DNS) pour résoudre `eagle-server.example.com` ?

Est-il possible d'accéder à d'autres périphériques du réseau local, tels que `172.16.255.254` ?

_____

Étape 3 : insertion d'une route de la table de routage pour l'ordinateur Windows.

Dans la configuration suivante, utilisez l'adresse IP affectée à votre interface hôte pod. La syntaxe pour ajouter une route à la table de routage pour l'ordinateur Windows est :

`route ADD` *`réseau`* **`MASK`** *`masque Adresse IP de la passerelle`*

`C:/>` **`route ADD 0.0.0.0 MASK 0.0.0.0 172.16.255.`**254

Examinez la table de routage actif et vérifiez que la route de passerelle par défaut a été restaurée :

La route de passerelle par défaut a-t-elle été restaurée ? _____:

Essayez d'envoyer une requête active à Eagle Server. Quels sont les résultats ?

_____

Tâche 2 : utilisation d'une commande telnet du client `telnet` de Windows pour vous connecter à un routeur Cisco.

Dans cette tâche, vous établissez une connexion avec le routeur R2-Central et utilisez les commandes IOS standard pour examiner la table de routage du routeur. Les périphériques Cisco possèdent un serveur Telnet et, si la configuration est correcte, autorisent des connexions distantes Toutefois, l'accès au routeur est restreint et nécessite un nom d'utilisateur et un mot de passe. Le mot de passe pour tous les noms d'utilisateurs est `cisco`. Le nom d'utilisateur dépend du pod. Le nom d'utilisateur `ccna1` s'applique aux utilisateurs de l'ordinateur pod 1, `ccna2` s'adresse aux participants sur l'ordinateur pod2, etc.

Étape 1 : utilisation du client Telnet de Windows pour se connecter à un routeur Cisco.

Ouvrez une fenêtre de terminal en cliquant sur **Démarrer > Exécuter**. Tapez `cmd`, puis cliquez sur **OK**. Une fenêtre de ligne de commande et une invite doivent être disponibles. L'utilitaire Telnet possède plusieurs options et vous pouvez les afficher avec la commande **`telnet /?`**. Vous devez disposer d'un nom d'utilisateur et d'un mot de passe pour vous connecter au routeur. Pour tous les noms d'utilisateurs, le mot de passe correspondant est `cisco`.

Numéro de pod	Nom d'utilisateur
1	ccna1
2	ccna2
3	ccna3
4	ccna4
5	ccna5
6	ccna6
7	ccna7
8	ccna8
9	ccna9
10	ccna10
11	ccna11

Pour démarrer une session Telnet avec un routeur R2-central, tapez la commande :

```
C:/> telnet 172.16.255.254 <ENTRÉE>
```

Une fenêtre de connexion vous demande un nom d'utilisateur, comme illustré ci-dessous. Indiquez le nom d'utilisateur applicable et appuyez sur **<ENTRÉE>**. Entrez le mot de passe `cisco`, puis appuyez sur **<ENTRÉE>**. L'invite du routeur doit être visible après une connexion réussie.

```
**************************************************************
            Ceci est le routeur Router1 des travaux pratiques Eagle 1.
            Accès autorisé uniquement.
**************************************************************

Contrôle de l'accès de l'utilisateur

Nom d'utilisateur : ccna1
Mot de passe : cisco (masqué)
R2-Central#
```

À l'invite, `R2-Central#`, une connexion Telnet réussie a été créée. Seules des autorisations limitées pour les noms d'utilisateurs `ccnax` sont disponibles ; par conséquent, il n'est pas possible de modifier les paramètres du routeur ou d'afficher la configuration. La fonction de cette tâche consiste à établir une session Telnet, qui a été effectuée. Dans la tâche suivante, la table de routage du routeur sera examinée.

Tâche 3 : examen des routes du routeur à l'aide des commandes IOS standard de Cisco.

Comme avec tout périphérique réseau, les adresses de passerelle indiquent au périphérique le mode d'accès à d'autres réseaux en l'absence d'informations. Un routeur est également susceptible d'utiliser une passerelle par défaut, à la manière d'une adresse IP de passerelle par défaut pour l'ordinateur hôte. Un routeur connaît parfaitement les réseaux directement connectés, tout comme un ordinateur hôte.

Cette tâche examine les commandes IOS Cisco en détail. Cependant, elle utilise une commande IOS standard pour afficher la table de routage. La syntaxe pour afficher la table de routage est :

```
show ip route <ENTRÉE>
```

Étape 1 : saisie de la commande pour afficher la table de routage du routeur

Les informations relatives aux routes sont beaucoup plus détaillées que celles qui figurent sur un ordinateur hôte. Ceci est normal, car la tâche d'un routeur consiste à acheminer le trafic entre les

réseaux. Les informations requises de cette tâche sont, cependant, faciles à recueillir. La figure 2 illustre la table de routage pour `R2-Central`.

```
R2-Central#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.10.10.6 to network 0.0.0.0

C    172.16.0.0/16 is directly connected, FastEthernet0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.4 is directly connected, Serial0/2/0
S*   0.0.0.0/0 [1/0] via 10.10.10.6
R2-Central#
```

Figure 2. Résultats de la commande show `ip route` IOS de Cisco

La section `Codes` illustrée à la figure 3 offre une description des symboles à gauche de chaque entrée de route.

```
R2-Central#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.10.10.6 to network 0.0.0.0

C    172.16.0.0/16 is directly connected, FastEthernet0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.4 is directly connected, Serial0/2/0
S*   0.0.0.0/0 [1/0] via 10.10.10.6
R2-Central#
```

Figure 3. Explication des codes

- ❶ C indique des réseaux directement connectés et l'interface qui prend en charge la connexion.
- ❷ S indique une route statique, qui est manuellement saisie par l'ingénieur réseau Cisco.
- ❸ Comme la route est « à quatre zéros », il s'agit d'une route `par défaut candidate`.
- ❹ S'il n'existe aucune autre route dans la table de routage, utilisez l'adresse de cette `passerelle de dernier recours IP` pour la transmission des paquets.

Quel est le mode d'affichage des données du masque IP dans une table de routage de routeur ?

Que fait le routeur avec les paquets destinés à 192.168.254.254 ?

_____

_____

Une fois que vous avez terminé l'examen de la table de routage, quittez le routeur avec la commande **exit <ENTRÉE>.** Le client Telnet ferme également la connexion avec la séquence d'échappement Telnet **<CTRL>]** et **quit**. Fermez la fenêtre de ligne de commande.

Tâche 4 : Remarques générales

Deux nouvelles commandes Windows ont été utilisées dans ces travaux pratiques. La commande **route** permet d'afficher, de supprimer et d'ajouter les données de routes sur l'ordinateur hôte pod.

Le client Telnet de Windows, **telnet**, a été utilisé pour la connexion au routeur des travaux pratiques, R2-Central. Cette technique sera employée dans d'autres travaux pratiques pour la connexion aux périphériques réseau Cisco.

La table de routage du routeur a été examinée avec la commande IOS de Cisco **show ip route**. Les routes pour les réseaux directement connectés, les routes attribuées de façon statique, et les données de la passerelle de dernier recours sont affichées.

Tâche 5 : confirmation

Il est possible d'utiliser d'autres commandes IOS Cisco pour afficher les données des adresses IP sur un routeur. Tout comme la commande **ipconfig** de Windows, la commande IOS de Cisco **show ip interface brief** affiche l'affectation des adresses IP.

```
R2-Central#show ip interface brief
Interface        IP-Address      OK? Method Status             Protocol
FastEthernet0/0  172.16.255.254  YES manual up                   up
FastEthernet0/1        unassigned      YES unset  administratively down
down
Serial0/2/0      10.10.10.5      YES manual up                   up
Serial0/2/1            unassigned      YES unset  administratively down
down
R2-Central#
```

À l'aide des commandes de Windows et IOS de Cisco dans ces travaux pratiques, comparez les résultats des données de réseau. Que manquait-il ? Quelles informations réseau critiques étaient semblables ?

_____

_____

Tâche 6 : nettoyage.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

5.6.1 : exercice d'intégration des compétences : routage des paquets IP

Diagramme de topologie

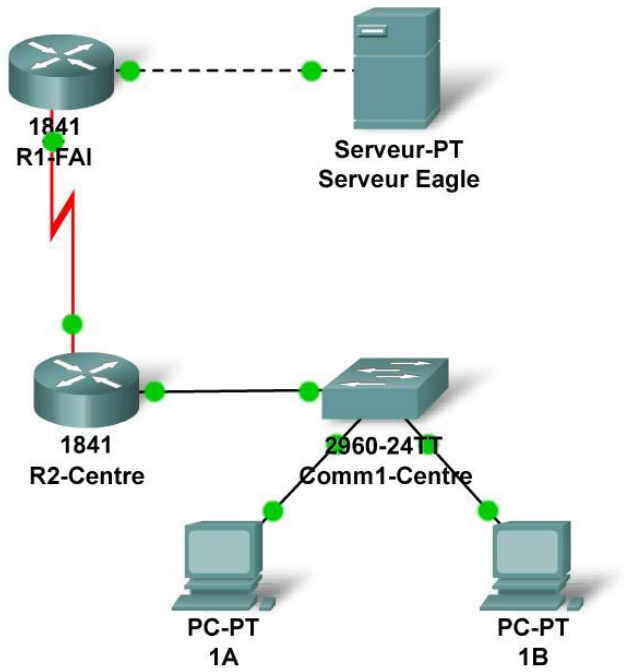


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	Fa0/0	192.168.254.253	255.255.255.0	N/A
	S0/0/0	10.10.10.6	255.255.255.252	N/A
R2-Central	Fa0/0	172.16.255.254	255.255.0.0	N/A
	S0/0/0	10.10.10.5	255.255.255.252	N/A
S1-Central	VLAN 1	172.16.254.1	255.255.0.0	172.16.255.254
PC 1A	La carte réseau	172.16.1.1	255.255.0.0	172.16.255.254
PC 1B	La carte réseau	172.16.1.2	255.255.0.0	172.16.255.254
Serveur Eagle	La carte réseau	192.168.254.254	255.255.255.0	192.168.254.253

Objectifs pédagogiques

- Configurer une interface de routeur à l'aide d'une interface graphique utilisateur
- Explorer une table de routage
- Configurer une route statique à l'aide d'une interface graphique utilisateur
- Explorer le routage des paquets IP

Contexte

Tout au long de ce cours, vous allez utiliser une configuration de travaux pratiques type constituée de PC, de serveurs, de routeurs et de commutateurs réels pour apprendre des concepts liés aux réseaux. À la fin de chaque chapitre, vous construirez des parties de plus en plus importantes de cette topologie dans Packet Tracer et analyserez des interactions de protocoles de plus en plus complexes. Vous avez déjà étudié divers protocoles de couche application, tels que DNS, HTTP, TFTP, DHCP et Telnet, ainsi que deux protocoles de couche transport : TCP et UDP. Peut-être avez-vous remarqué que quels que soient les protocoles application et transport utilisés, ils sont toujours encapsulés dans des paquets IP, aussi bien dans la vue **Inbound PDU Details** que dans la vue **Outbound PDU Details**. À travers cet exercice, nous examinerons la façon dont opère le protocole Internet (IP), protocole de couche réseau dominant sur Internet, dans le contexte d'un exemple simple de routage IP.

Tâche 1 : configuration d'une interface de routeur

Des problèmes existent sur le réseau local : le PC 1A ne parvient pas à atteindre le serveur Eagle Server (vérifiez cela en mode Realtime). Un problème a été détecté au niveau du routeur. Placez le pointeur de la souris sur le routeur R2-Central, puis notez l'état de l'interface Fa0/0 (à laquelle le commutateur est connecté). Cette interface doit avoir une adresse IP, un masque de sous-réseau et être activée pour faire office de passerelle par défaut du réseau local. Cliquez sur le routeur R2-Central, puis accédez à l'onglet **Config**. À la fin du cours, vous apprendrez à effectuer cette tâche par le biais de l'interface de ligne de commande (CLI) de Cisco IOS (Internetwork Operating System). Pour l'instant, il est vous sera plus simple d'utiliser l'onglet **Config**, ce qui vous permettra du reste de vous concentrer sur l'idée de base, à savoir, le routage IP. Dans la liste ci-après, recherchez **INTERFACE, FastEthernet0/0**. Ajoutez l'adresse IP 172.16.255.254 au masque de sous-réseau 255.255.0.0, puis activez le port. Fermez la fenêtre du routeur. Vérifiez que l'interface (port) du routeur fonctionne actuellement en plaçant le curseur dessus. Essayez d'atteindre le serveur Eagle Server. La requête échoue toujours. Quelles sont les raisons possibles et pourquoi ?

Tâche 2 : examen des routes

Utilisez l'outil **Inspect Tool** (loupe) pour examiner la table de routage de R2-Central. Bien que les réseaux directement connectés du routeur soient affichés, il n'y a pas moyen d'atteindre le réseau du serveur Eagle Server.

Tâche 3 : configuration d'une route à l'aide d'une interface graphique utilisateur

Cliquez sur le routeur R2-Central, puis accédez à l'onglet **Config**. Dans la liste affichée, recherchez **ROUTING, Static**. Configurez ce que l'on appelle une route statique par défaut en utilisant l'adresse 0.0.0.0, le masque 0.0.0.0 et le tronçon suivant 10.10.10.6 (l'interface S0/0/0 sur le routeur R1-ISP), puis cliquez sur le bouton **Add**. Cette route est configurée de sorte que les paquets en provenance du réseau local 172.16.0.0 /16 soient systématiquement acheminés vers le routeur R1-ISP, quelle que soit la destination prévue. Sous **GLOBAL, Settings**, cliquez sur le bouton **Save** pour enregistrer en mémoire NVRAM la configuration d'interface et de route que vous venez de définir dans le cas où le routeur serait mis hors tension, puis sous tension. Utilisez l'outil **Inspect Tool** (loupe) pour examiner à nouveau la table de routage de R2-Central. La route que vous avez configurée doit à présent figurer dans la table de routage.

Vérifiez votre travail en vous basant sur les informations affichées par le bouton **Check Results** et l'onglet **Assessment Items**. Testez la connectivité en mode Realtime entre le PC 1A et le serveur Eagle Server en utilisant l'option ADD SIMPLE PDU. L'unité de données de protocole (PDU), requête ping ponctuelle, apparaîtra également dans la fenêtre User Created PDU List pour une utilisation ultérieure. Avec la première commande ping, vous n'obtiendrez aucun résultat, car il n'y aura aucune entrée dans les tables ARP. Cliquez deux fois sur **Fire** pour relancer l'opération.

Tâche 4 : examen du routage du paquet IP

Passez en mode Simulation. Suivez le trajet du paquet du PC 1A au serveur Eagle Server et inversement en utilisant le bouton **Capture / Forward** et en examinant le contenu du paquet, soit en cliquant sur l'enveloppe, soit en cliquant sur le carré de couleur dans la colonne **Info** de la liste d'événements (**Event List**).

Remarques générales

Quelles données un paquet IP peut-il contenir ? Que signifie l'expression : « le paquet IP est acheminé » ? Qu'est-ce qu'une route ? Quels sont les risques ?

Travaux pratiques 6.7.1 : commandes ping et traceroute

Schéma de la topologie

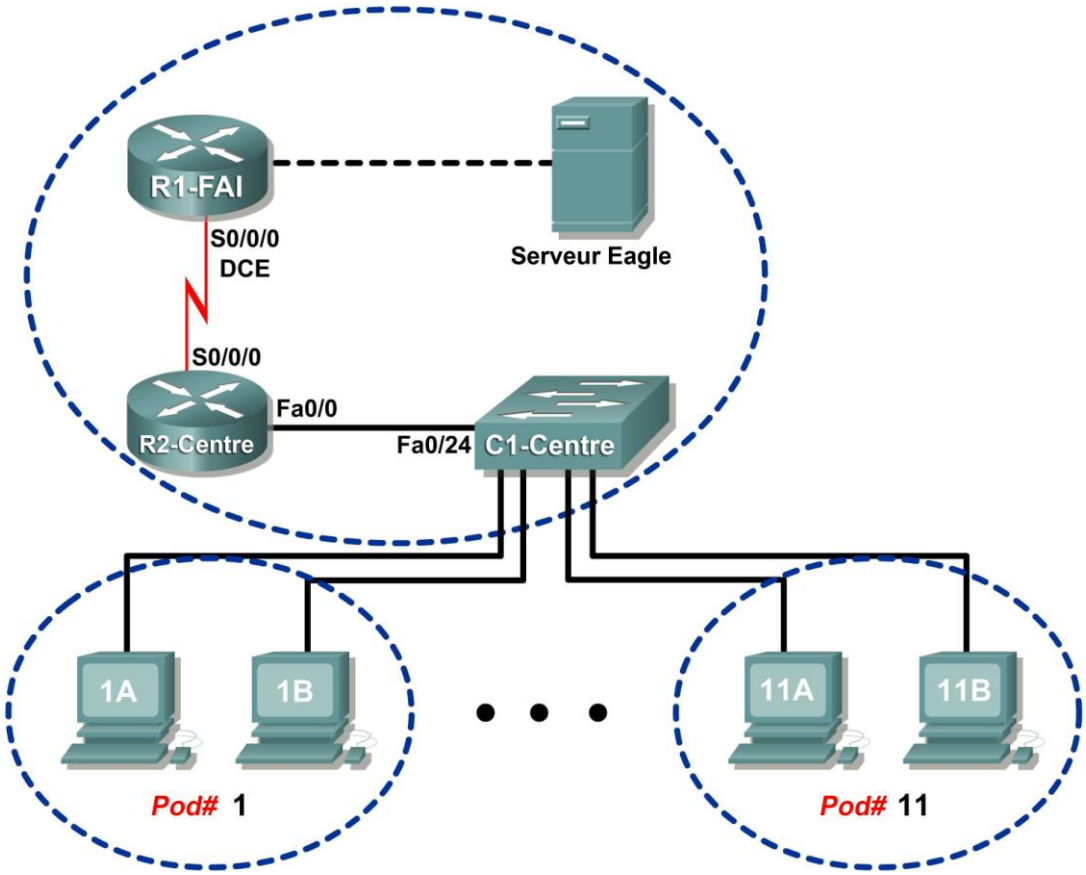


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/D
	Fa0/0	192.168.254.253	255.255.255.0	N/D
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/D
	Fa0/0	172.16.255.254	255.255.0.0	N/D
Eagle Server	N/D	192.168.254.254	255.255.255.0	192.168.254.253
	N/D	172.31.24.254	255.255.255.0	N/D
hôte*Pod#*A	N/D	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
hôte*Pod#*B	N/D	172.16. *Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	N/D	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- utiliser la commande **ping** pour vérifier la connectivité réseau TCP/IP simple ;
- utiliser la commande **tracert/traceroute** pour vérifier la connectivité TCP/IP.

Contexte

ping et **tracert** sont deux outils indispensables pour le test de la connectivité réseau TCP/IP. L'utilitaire **ping** est disponible sous Windows, Linux et Cisco IOS, et teste la connectivité réseau. **tracert** est disponible sous Windows, et un utilitaire similaire, **traceroute**, est disponible sous Linux et Cisco IOS. Outre le test de la connectivité, **tracert** permet de vérifier la latence du réseau.

Par exemple, lorsqu'un navigateur Web ne parvient pas à se connecter à un serveur Web, le problème peut être n'importe où entre le client et le serveur. Un ingénieur réseau peut utiliser la commande **ping** pour tester la connectivité du réseau local ou les connexions où ne figurent que quelques périphériques. Dans un réseau complexe, la commande **tracert** est utilisée. De longues discussions ont eu lieu pour savoir où commencer les tests de connectivité. Cela dépend généralement de l'expérience de l'ingénieur réseau et de sa connaissance du réseau.

Le protocole ICMP (Internet Control Message Protocol) est utilisé par à la fois **ping** et **tracert** pour envoyer des messages entre les périphériques. ICMP est un protocole de couche réseau TCP/IP, d'abord défini dans la RFC 792, en septembre 1981. Les types de messages ICMP ont été développés ultérieurement dans la RFC 1700.

Scénario

Dans ces travaux pratiques, les commandes **ping** et **tracert** sont examinées, et les options de commandes sont utilisées pour modifier le comportement des commandes. Des périphériques sont testés dans les travaux pratiques Cisco pour familiariser les participants avec l'utilisation des commandes.

Il est probable que le délai d'attente mesuré soit moins long que celui sur un réseau de production. Le trafic réseau moindre dans les travaux pratiques Eagle 1 en est la raison.

Tâche 1 : utilisation de la commande ping pour vérifier la connectivité réseau TCP/IP simple.

La commande **ping** permet de vérifier la connectivité de couche réseau TCP/IP sur l'ordinateur hôte local ou sur un autre périphérique dans le réseau. Vous pouvez utiliser la commande avec une adresse IP de destination ou un nom qualifié, comme eagle-server.example.com, pour tester les fonctionnalités des services de noms de domaines (DNS). Pour ces travaux pratiques, seules les adresses IP sont utilisées.

L'opération **ping** est simple. L'ordinateur source envoie une requête d'écho ICMP à la destination. Cette dernière répond avec une réponse d'écho. En cas d'interruption entre la source et la destination, il est possible qu'un routeur réponde avec un message ICMP qui indique que l'hôte ou le réseau de destination est inconnu.

Étape 1 : vérification de la connectivité de la couche réseau TCP/IP sur l'ordinateur hôte local.

```
C:\> ipconfig
Configuration IP de Windows
Carte Ethernet Connexion au réseau local :
        Suffixe DNS propre à la connexion  . :
        Adresse IP. . . . . . . . . . . . . : 172.16.1.2
        Masque de sous-réseau . . . . . . . . : 255.255.0.0
        Passerelle par défaut . . . . . . . . : 172.16.255.254
C:\>
```

Figure 1. Informations sur le réseau TCP/IP local

1. Ouvrez un terminal Windows et déterminez l'adresse IP de l'ordinateur hôte pod avec la commande **ipconfig**, comme illustré à la figure 1.

   Les résultats doivent être semblables sauf pour l'adresse IP. Chaque ordinateur hôte pod doit posséder le masque de réseau et l'adresse de passerelle par défaut identiques. Seule l'adresse IP est susceptible de différer. Si des informations sont manquantes ou que le masque de sous-réseau et la passerelle par défaut sont différents, reconfigurez les paramètres TCP/IP pour les faire correspondre avec ceux de l'ordinateur hôte pod.

2. Consignez les informations sur le réseau TCP/IP local :

Informations TCP/IP	Valeur
Adresse IP	
Masque de sous-réseau	
Passerelle par défaut	

```
C:\>ping 172.16.1.2❶

Envoi d'une requête 'ping' sur 172.16.1.2 avec 32 octets de données :

❷Réponse de 172.16.1.2 : octets=32 temps<1ms TTL=128
Réponse de 172.16.1.2 : octets=32 temps<1ms TTL=128
Réponse de 172.16.1.2 : octets=32 temps<1ms TTL=128
Réponse de 172.16.1.2 : octets=32 temps<1ms TTL=128

❸Statistiques Ping pour 172.16.1.2:
    Paquets : envoyés ❹= 4, reçus ❺= 4, perdus ❻= 0 (perte 0%),
❼Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\>
```

Figure 2. Résultats de la commande ping sur la pile TCP/IP locale

3. Utilisez la commande **ping** pour vérifier la connectivité de la couche réseau TCP/IP sur l'ordinateur hôte local.

   Par défaut, quatre requêtes ping sont transmises à la destination et les informations de réponse sont reçues. Les résultats doivent être semblables à ceux illustrés à la figure 2.

   ❶ Adresse de destination, définie sur l'adresse IP de l'ordinateur local.

   ❷ Informations de réponse :

   octets : taille du paquet ICMP.

   temps : délai écoulé entre la transmission et la réponse.

   TTL : valeur TTL par défaut du périphérique de DESTINATION, moins le nombre de routeurs dans le chemin. La valeur TTL maximale est 255, mais pour les ordinateurs Windows plus récents, la valeur par défaut est 128.

❸ Résumé des informations sur les réponses :

❹ Paquets envoyés : nombre de paquets transmis. Par défaut, quatre paquets sont envoyés.

❺ Paquets reçus : nombre de paquets reçus.

❻ Paquets perdus : différence entre le nombre de paquets envoyés et reçus.

❼ Informations sur le retard dans les réponses, mesuré en millisecondes. Une durée de transmission plus courte indique des liaisons plus rapides. Une horloge d'ordinateur est réglée sur 10 millisecondes. Des valeurs plus rapides que 10 millisecondes affichent 0.

4. Renseignez les résultats de la commande **`ping`** sur votre ordinateur :

Champ	Valeur
Taille du paquet	
Nombre de paquets envoyés	
Nombre de réponses	
Nombre de paquets perdus	
Latence minimum	
Latence maximum	
Latence moyenne	

Étape 2 : vérification de la connectivité de la couche réseau TCP/IP sur le réseau local.

```
C:\> ping 172.16.255.254
Envoi d'une requête sur 172.16.255.254 avec 32 octets de
données :
Réponse de 172.16.255.254 : octets=32 temps=1 ms TTL=255
Réponse de 172.16.255.254 : octets=32 temps=<1 ms TTL=255
Réponse de 172.16.255.254 : octets=32 temps=<1 ms TTL=255
Réponse de 172.16.255.254 : octets=32 temps=<1 ms TTL=255
Statistiques Ping pour 172.16.255.254 :
    Paquets : Envoyés = 4, Reçus = 4, Perdus = 0 (perte
0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0 ms, Maximum = 1 ms, Moyenne = 0 ms
C:\>
```

Figure 3. Résultats de la commande `ping` pour la passerelle par défaut

1. Utilisez la commande **ping** pour vérifier la connectivité de la couche réseau TCP/IP à la passerelle par défaut. Les résultats doivent être semblables à ceux illustrés à la figure 3.

   La valeur TTL par défaut de Cisco IOS est réglée sur 255. Comme les datagrammes n'ont pas traversé un routeur, la valeur TTL retournée est 255.

2. Renseignez les résultats de la commande **ping** sur votre passerelle par défaut :

Champ	Valeur
Taille du paquet	
Nombre de paquets envoyés	
Nombre de réponses	
Nombre de paquets perdus	
Latence minimum	
Latence maximum	
Latence moyenne	

Quel est le résultat d'une perte de connectivité à la passerelle par défaut ?

_____

Étape 3 : vérification de la connectivité de la couche réseau TCP/IP à un réseau distant.

```
C:\> ping 192.168.254.254
Envoi d'une requête sur 192.168.254.254 avec 32 octets de
données :
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=62
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=62
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=62
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=62
Statistiques Ping pour 192.168.254.254 :
    Paquets : Envoyés = 4, Reçus = 4, Perdus = 0 (perte
0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms
C:\>
```

Figure 4. Résultats de la commande `ping` pour Eagle Server

1. Utilisez la commande **`ping`** pour vérifier la connectivité de la couche réseau TCP/IP sur un réseau distant. Dans ce cas précis, Eagle Server est utilisé. Les résultats doivent être semblables à ceux illustrés à la figure 4.

   La valeur TTL par défaut de Linux est réglée sur 64. Deux routeurs ont été croisés pour accéder à Eagle Server. Par conséquent, la valeur TTL retournée est 62.

2. Renseignez les résultats de la commande **`ping`** sur votre ordinateur :

Champ	Valeur
Taille du paquet	
Nombre de paquets envoyés	
Nombre de réponses	
Nombre de paquets perdus	
Latence minimum	
Latence maximum	
Latence moyenne	

```
C:\> ping 192.168.254.254
Envoi d'une requête sur 192.168.254.254 avec 32 octets de
données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Statistiques Ping pour 192.168.254.254 :
    Paquets : Envoyés = 4, Reçus = 0, Perdus = 4 (perte
100%),
C:\>
```

Figure 5. Résultats d'une commande `ping` avec des paquets perdus

La commande **`ping`** est extrêmement utile lors du dépannage de la connectivité réseau.. Toutefois, des restrictions existent. Dans la figure 5, les résultats indiquent qu'un utilisateur ne peut pas accéder à Eagle Server. Le problème réside-t-il dans Eagle Server ou dans un périphérique dans le chemin ? La commande **`tracert`**, examinée ensuite, peut afficher les informations de latence réseau et de chemin.

Tâche 2 : utilisation de la commande **tracert** pour vérifier la connectivité TCP/IP.

La commande **tracert** s'avère utile pour obtenir plus d'informations sur la latence réseau et le chemin. Au lieu d'utiliser la commande **ping** pour tester la connectivité de chaque périphérique à la destination, un par un, vous pouvez exécuter la commande **tracert**.

Sur des périphériques Linux et Cisco IOS, la commande équivalente est **traceroute**.

Étape 1 : vérification de la connectivité de la couche réseau TCP/IP avec la commande **tracert**.

1. Ouvrez un terminal Windows et exécutez la commande suivante :

```
C:\> tracert 192.168.254.254
```

```
C:\> tracert 192.168.254.254
Détermination de l'itinéraire vers 192 168 254 254 avec un maximum de
30 sauts.
  1    <1 ms    <1 ms    <1 ms  172.16.255.254
  2    <1 ms    <1 ms    <1 ms  10.10.10.6
  3    <1 ms    <1 ms    <1 ms  192 168 254 254
Itinéraire déterminé.
C:\>
```

Figure 6. Résultats de la commande tracert pour Eagle Server

Les résultats de la commande **tracert** doivent être semblables à ceux illustrés à la figure 6.

2. Consignez vos résultats dans le tableau suivant :

Champ	Valeur
Nombre maximum de sauts	
Première adresse IP du routeur	
Deuxième adresse IP du routeur	
Destination atteinte ?	

Étape 2 : observation des résultats de la commande **tracert** pour un hôte dont la connectivité réseau a été perdue.

En cas de perte de connectivité d'un périphérique final tel que Eagle Server, la commande **tracert** peut vous fournir des indices précieux quant à l'origine du problème. La commande **ping** indique la panne mais pas d'informations sur les périphériques dans le chemin. Selon le schéma de topologie des travaux pratiques Eagle 1, R2-Central et R1-ISP sont utilisés pour la connectivité entre les ordinateurs hôtes pod et Eagle Server.

```
C:\> tracert -w 5 -h 4 192.168.254.254
Détermination de l'itinéraire vers 192 168 254 254 avec un maximum de 4
sauts.
  1    <1 ms    <1 ms    <1 ms  172.16.255.254
  2    <1 ms    <1 ms    <1 ms  10.10.10.6
  3     *        *        *     Délai d'attente de la demande dépassé.
  4     *        *        *     Délai d'attente de la demande dépassé.

Itinéraire déterminé.
C:\>
```

Figure 7. Résultats de la commande tracert

Reportez-vous à la figure 7. Les options sont utilisées avec la commande **tracert** pour réduire le délai d'attente (en millisecondes), **-w 5**, et le nombre maximal de sauts, **-h 4**. Si Eagle Server a été déconnecté du réseau, la passerelle par défaut répond correctement, ainsi que R1-ISP. Le problème doit être sur le réseau 192.168.254.0/24. Dans cet exemple, Eagle Server a été désactivé.

Quels sont les résultats de la commande **tracert** si R1-ISP tombe en panne ?

_____

Quels sont les résultats de la commande **tracert** si R2-Central tombe en panne ?

_____

Tâche 3 : confirmation

Les valeurs par défaut pour la commande **ping** fonctionnent normalement pour la plupart des scénarios de dépannage. Cependant, le réglage des options **ping** peut s'avérer parfois utile. L'exécution de la commande **ping** sans adresse de destination permet d'afficher les options illustrées à la figure 8 :

```
C:\> ping

Utilisation : ping [-t] [-a] [-n échos] [-l taille] [-f] [-i vie] [-v
TypServ]
            [-r NbSauts] [-s NbSauts] [[-j ListeHôtes] | [-k
ListeHôtes]]
            [-w Délai] NomCible

Options :
    -t              Envoie la requête Ping sur l'hôte spécifié jusqu'à
                    interruption.
                    Entrez Ctrl-Attn pour afficher les statistiques et
continuer,
                    Ctrl-C pour arrêter.
    -a              Recherche les noms d'hôte à partir des adresses.
    -n échos        Nombre de requêtes d'écho à envoyer.
    -l taille         Envoie la taille du tampon.
    -f              Active l'indicateur Ne pas fragmenter dans le
paquet.
    -i vie          Durée de vie.
    -v TypServ          Type de service.
    -r NbSauts        Enregistre l'itinéraire pour le nombre de sauts.
    -s NbSauts        Dateur pour le nombre de sauts.
    -j ListeHôtes   Itinéraire source libre parmi la liste d'hôtes.
    -k ListeHôtes   Itinéraire source libre parmi la liste d'hôtes.
    -w Délai     Délai d'attente pour chaque réponse, en
millisecondes.
C:\>
```

Figure 8. Résultats d'une commande ping sans adresse de destination

Les options les plus utiles sont sélectionnées en jaune. Les options, telles que **-t** et **-n** ne fonctionnent pas ensemble. Il est possible d'utiliser ensemble d'autres options. Testez les options suivantes :

Pour envoyer une requête **ping** à l'adresse de destination jusqu'à l'arrêt, utilisez l'option **–t**. Pour arrêter, appuyez sur <CTRL> C :

```
C:\> ping –t 192.168.254.254
Envoi d'une requête sur 192.168.254.254 avec 32 octets de données :
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Statistiques Ping pour 192.168.254.254 :
    Paquets : Envoyés = 6, Reçus = 6, Perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms
Ctrl+C
^C
C:\>
```

Figure 9. Résultats d'une commande ping avec l'option –t

Pour envoyer une requête **ping** à la destination une fois et consigner les sauts du routeur, utilisez les options **–n** et **–r**, comme illustré à la figure 10. **Remarque :** seuls quelques périphériques répondent à l'option **–r**.

```
C:\> ping -n 1 –r 9 192.168.254.254
Envoi d'une requête sur 192.168.254.254 avec 32 octets de données :
Réponse de 192.168.254.254 : octets=32 temps=1 ms TTL=63
    Itinéraire :      10.10.10.5 ->
                  192.168.254.253 ->
                  192.168.254.254 ->
                       10.10.10.6 ->
                   172.16.255.254
Statistiques Ping pour 192.168.254.254 :
    Paquets : Envoyés = 1, Reçus = 1, Perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1 ms, Maximum = 1 ms, Moyenne = 1 ms
C:\>
```

Figure 10. Résultats d'une commande ping avec les options –n et –r

Tâche 4 : Remarques générales

Les ingénieurs réseaux utilisent à la fois **ping** et **tracert** pour tester la connectivité réseau. Pour la connectivité réseau de base, la commande **ping** fonctionne le mieux. Pour tester la latence et le chemin du réseau, la commande **tracert** est privilégiée.

La capacité à diagnostiquer avec précision et rapidité les problèmes de connectivité réseau est une compétence attendue d'un ingénieur réseau. La connaissance des protocoles TCP/IP et la pratique des commandes pour le dépannage permettent de développer cette compétence.

Tâche 5 : nettoyage.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

Travaux pratiques 6.7.2 : examen d'un paquet ICMP

Schéma de la topologie

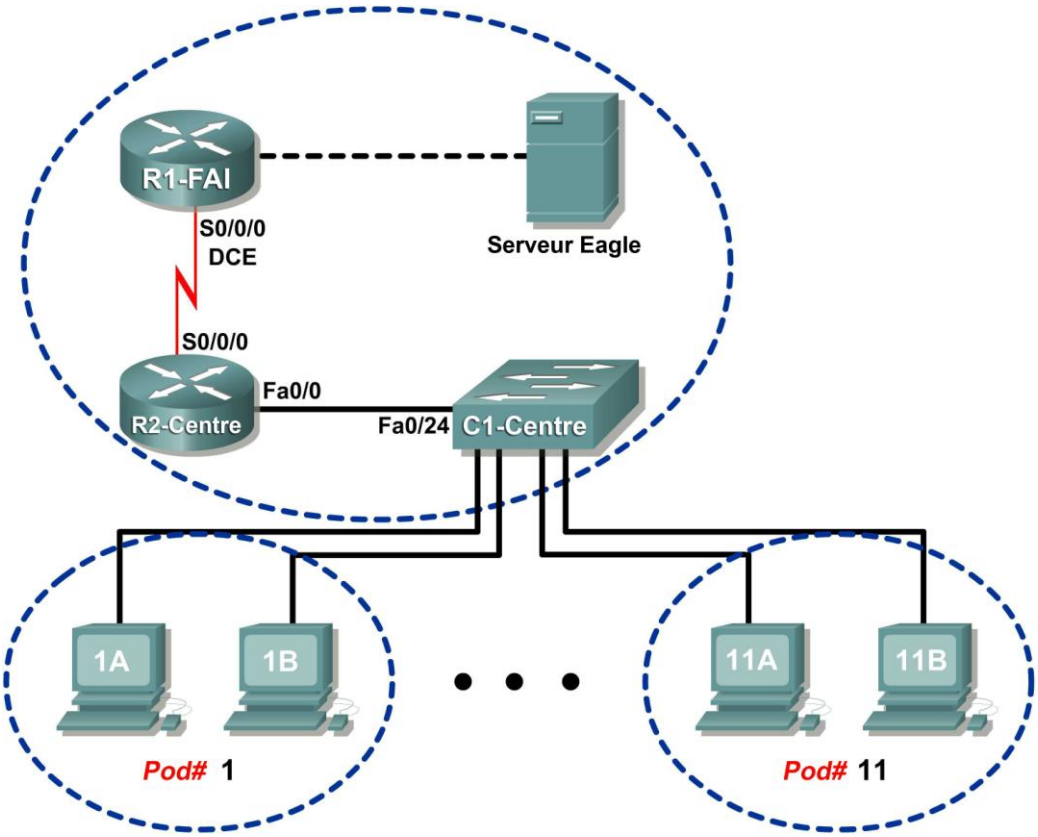


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/D
	Fa0/0	192.168.254.253	255.255.255.0	N/D
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/D
	Fa0/0	172.16.255.254	255.255.0.0	N/D
Eagle Server	N/D	192.168.254.254	255.255.255.0	192.168.254.253
	N/D	172.31.24.254	255.255.255.0	N/D
hôte*Pod#***A**	N/D	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
hôte*Pod#***B**	N/D	172.16. *Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	N/D	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- comprendre le format des paquets ICMP ;
- utiliser Wireshark pour capturer et examiner les messages ICMP.

Contexte

Le protocole ICMP (Internet Control Message Protocol) a d'abord été défini dans la RFC 792, en septembre 1981. Les types de message ICMP ont été développés ultérieurement dans la RFC 1700. ICMP fonctionne sur la couche réseau TCP/IP et permet d'échanger les informations entre des périphériques.

Les paquets ICMP remplissent de nombreuses fonctions dans le réseau informatique actuel. Lorsqu'un routeur ne peut pas transmettre un paquet au réseau ou à l'hôte de destination, un message informatif est retourné à la source. En outre, les commandes **ping** et **tracert** envoient des messages ICMP aux destinations. Ensuite, ces dernières répondent avec des messages ICMP.

Scénario

À l'aide des travaux pratiques Eagle 1, les captures Wireshark se composent des paquets ICMP entre les périphériques réseau.

Tâche 1 : compréhension du format des paquets ICMP.

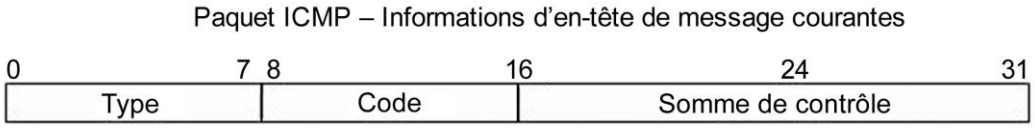


Figure 1. En-tête de message ICMP

Reportez-vous à la figure 1, les champs d'en-tête ICMP communs à tous les types de messages ICMP. Chaque message ICMP commence par un champ Type 8 bits, un champ Code 8 bits et une somme de contrôle 16 bits calculée. Le type de message ICMP décrit les champs ICMP restants. Le tableau dans la figure 2 illustre les types de message provenant de la RFC 792 :

Valeur	Signification
0	Réponse d'écho
3	Destination inaccessible
4	Épuisement de la source
5	Redirection
8	Écho
11	Dépassement du délai
12	Problème de paramètre
13	Horodatage
14	Réponse d'horodatage
15	Demande d'informations
16	Réponse à la demande d'informations

Figure 2. Types de message ICMP

Les codes offrent des informations complémentaires au champ Type. Par exemple, si le champ Type est 3, la destination inaccessible, d'autres informations sur le problème sont retournées dans le champ Code.

Le tableau dans la figure 3 indique les codes pour le message Type 3 ICMP, la destination inaccessible, provenant de la RFC 1700 :

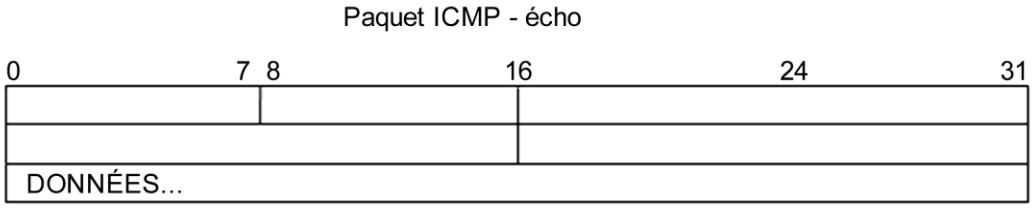
Code Valeur	Signification
0	Réseau inaccessible
1	Hôte inaccessible
2	Protocole inaccessible
3	Port inaccessible
4	Fragmentation requise et l'option Don't Fragment a été définie
5	Échec de la route source
6	Réseau de destination inconnu
7	Hôte de destination inconnu
8	Hôte source isolé
9	Communication avec réseau de destination interdit par l'administration
10	Communication avec hôte de destination Interdit par l'administration
11	Réseau de destination inaccessible pour le type de service
12	Hôte de destination inaccessible pour le type de service

Figure 3. Codes de messages type 3 ICMP

À l'aide de la capture de messages ICMP illustrée à la figure 4, renseignez les champs pour la requête d'écho des paquets ICMP. Les valeurs qui commencent par `0x` sont des nombres hexadécimaux :

```
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x365c [correct]
  Identifier: 0x0200
  Sequence number: 0x1500
  Data (32 bytes)
```

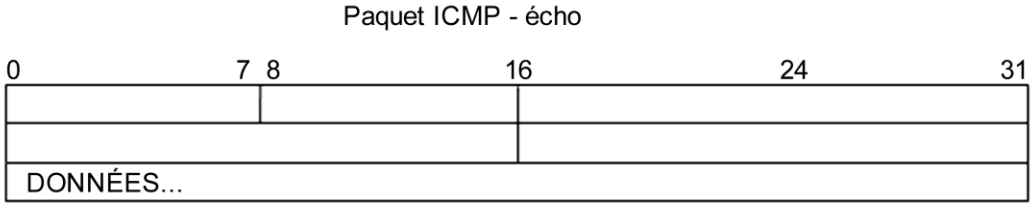
Figure 4. Requête d'écho des paquets ICMP



À l'aide de la capture de messages ICMP illustrée à la figure 5, renseignez les champs pour la réponse d'écho des paquets ICMP.

```
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x3e5c [correct]
  Identifier: 0x0200
  Sequence number: 0x1500
  Data (32 bytes)
```

Figure 5. Réponse d'écho des paquets ICMP



Sur la couche réseau TCP/IP, la communication entre les périphériques n'est pas garantie. Toutefois, ICMP n'offre pas de vérifications minimales pour qu'une réponse corresponde à la requête. À partir des informations disponibles dans les messages ICMP ci-dessus, comment l'expéditeur sait-il que la réponse s'applique à un écho spécifique ?

_____

_____

Tâche 2 : utilisation de Wireshark pour capturer et examiner les messages ICMP.

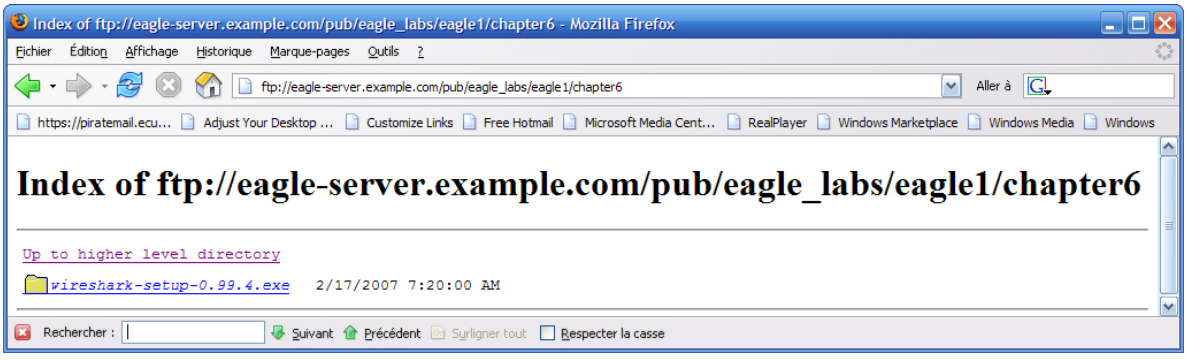


Figure 6. Site de téléchargement Wireshark

Si vous n'avez pas téléchargé Wireshark sur l'ordinateur hôte pod, il peut l'être à partir d'Eagle Server.

1. Ouvrez un navigateur Web, URL FTP://eagle-server.example.com/pub/eagle labs/eagle1/chapter6, comme illustré à la figure 6.
2. Cliquez avec le bouton droit sur le nom de fichier de Wireshark, cliquez sur **Save Link As**, puis enregistrez le fichier dans l'ordinateur hôte pod.
3. Une fois le fichier téléchargé, ouvrez et installez Wireshark.

Étape 1 : capture et évaluation les messages d'écho ICMP vers Eagle Server.

Dans cette étape, Wireshark permet d'examiner les messages d'écho ICMP.

1. Ouvrez un terminal Windows sur l'ordinateur hôte pod.
2. Une fois prêt, démarrez la capture Wireshark.

```
C:\> ping eagle-server.example.com
Envoi d'une requête ping sur eagle-server.example.com [192.168.254.254]
avec 32 octets de données :
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Statistiques Ping pour 192.168.254.254 :
    Paquets : Envoyés = 4, Reçus = 4, Perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms
C:\>
```

Figure 7. Réponses `ping` validées depuis Eagle Server

3. À partir de la ligne de commande Windows, envoyez une requête **`ping`** à Eagle Server Quatre réponses validées doivent être reçues d'Eagle Server, comme illustré à la figure 7.
4. Arrêtez la capture Wireshark. Il doit y avoir un total de quatre requêtes d'écho ICMP et de réponses d'écho correspondantes, comme illustré à la figure 8.

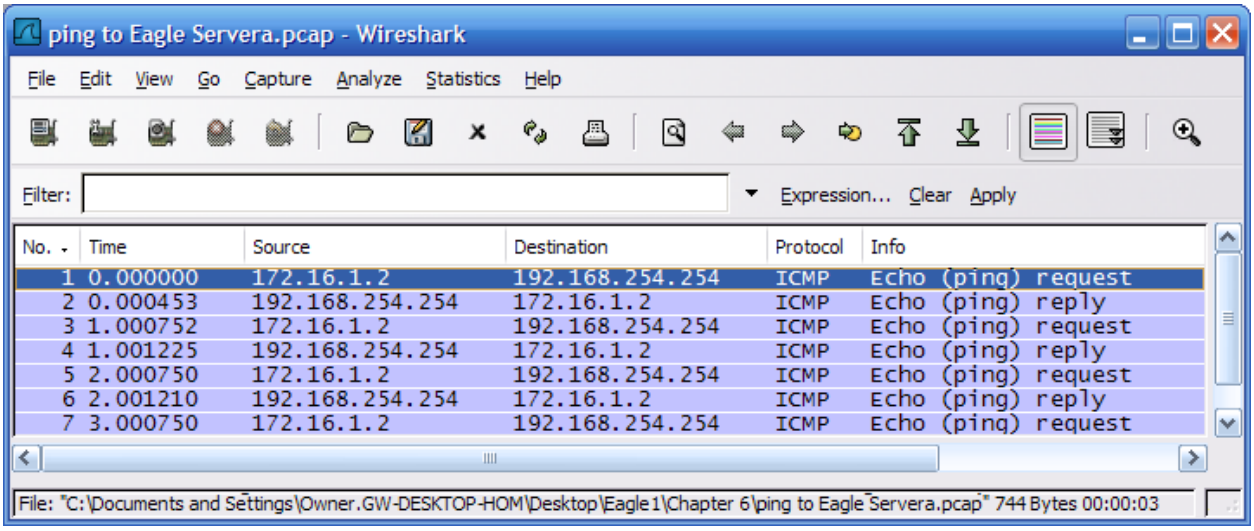


Figure 8. Capture Wireshark des requêtes et réponses `ping`

Quel périphérique réseau répond à la requête d'écho ICMP ? _____

5. Développez la fenêtre du milieu dans Wireshark, et l'enregistrement du protocole ICMP jusqu'à ce que tous les champs soient visibles. La fenêtre inférieure est également nécessaire à l'examen du champ Données.
6. Consignez les informations du *premier* paquet de requêtes d'écho vers Eagle Server :

Champ	Valeur
Type	
Code	
Somme de contrôle	
Identificateur	
Numéro d'ordre	
Données	

Y a-t-il 32 octets de données ? _____

7. Consignez les informations du *premier* paquet de réponses d'écho depuis Eagle Server :

Champ	Valeur
Type	
Code	
Somme de contrôle	
Identificateur	
Numéro d'ordre	
Données	

Quels champs, si c'est le cas, sont modifiés à partir de la requête d'écho ?

_____

8. Continuez d'évaluer les requêtes et réponses d'écho restantes. Renseignez les informations suivantes provenant de chaque nouveau ping :

Paquet	Somme de contrôle	Identificateur	Numéro d'ordre
Requête n°2			
Réponse n°2			
Requête n°3			
Réponse n°3			
Requête n°4			
Réponse n°4			

Pourquoi les valeurs de la somme de contrôle ont-elles changé avec chaque nouvelle requête ?

_____

Étape 2 : capture et évaluation des messages d'écho ICMP vers 192.168.253.1.

Dans cette étape, les requêtes ping sont envoyées vers un réseau et hôte fictifs. Les résultats de la capture Wireshark sont évalués, et sont parfois surprenants.

Essayez d'envoyer une requête à l'adresse IP 192.168.253.1.

```
C:\> ping 192.168.253.1
```

```
C:\> ping 192.168.253.1
Envoi d'une requête sur 192.168.253.1 avec 32 octets de données :
Réponse de 172.16.255.254 : Impossible de rejoindre l'hôte de
destination.
Réponse de 172.16.255.254 : Impossible de rejoindre l'hôte de
destination.
Réponse de 172.16.255.254 : Impossible de rejoindre l'hôte de
destination.
Réponse de 172.16.255.254 : Impossible de rejoindre l'hôte de
destination.
Statistiques Ping pour 192.168.253.1 :
    Paquets : Envoyés = 4, Reçus = 4, Perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms
C:\>
```

Figure 9. Résultat du ping à partir d'une destination fictive

Reportez-vous à la figure 9. Au lieu d'un délai d'attente de la requête, une réponse d'écho a lieu.

Quel périphérique réseau répond à des requêtes ping vers une destination fictive ?

_____

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
2	0.000816	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
3	1.000854	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
4	1.001686	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
5	2.001815	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
6	2.002547	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
7	3.002815	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
8	3.003588	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)

Figure 10. Capture Wireshark à partir d'une destination fictive

Les captures Wireshark vers une destination fictive sont illustrées à la figure 10. Développez la fenêtre du milieu dans Wireshark, et l'enregistrement du protocole ICMP

Quel type de message ICMP permet de retourner les informations à l'expéditeur ?

_____

Quel est le code associé au type de message ?

_____

Étape 3 : capture et évaluation des messages d'écho ICMP qui dépassent la valeur TTL.

Dans cette étape, les requêtes ping sont envoyées avec une valeur TTL basse, et simule ainsi une destination inaccessible. Envoyez une requête ping à Eagle Server, et définissez la valeur TTL sur **1** :

```
C:\> ping -i 1 192.168.254.254
```

```
C:\> ping -i 1 192.168.254.254
Envoi d'une requête sur 192.168.254.254 avec 32 octets de données :
Réponse de 172.16.255.254 : Durée de vie expirée lors du transit.
Réponse de 172.16.255.254 : Durée de vie expirée lors du transit.
Réponse de 172.16.255.254 : Durée de vie expirée lors du transit.
Réponse de 172.16.255.254 : Durée de vie expirée lors du transit.
Statistiques Ping pour 192.168.254.254 :
    Paquets : Envoyés = 4, Reçus = 4, Perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms
C:\>
```

Figure 11. Résultats du ping pour une valeur TTL dépassée

Reportez-vous à la figure 11, qui indique les réponses ping lors du dépassement de la valeur TTL.

Quel périphérique réseau répond aux requêtes ping qui dépassent la valeur TTL ?

_____

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
2	0.000701	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
3	1.000003	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
4	1.000687	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
5	1.999996	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
6	2.000761	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
7	3.000970	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
8	3.001723	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)

Figure 12. Capture Wireshark d'une valeur TTL dépassée

Les captures Wireshark vers une destination fictive sont illustrées à la figure 12. Développez la fenêtre du milieu dans Wireshark, et l'enregistrement du protocole ICMP.

Quel type de message ICMP permet de retourner les informations à l'expéditeur ?

_____

Quel est le code associé au type de message ?

_____

Quel périphérique réseau est responsable de la décrémentation de la valeur TTL ?

_____

Tâche 3 : confirmation

Utilisez Wireshark pour capturer une session **`tracert`** vers Eagle Server, puis vers 192.168.254.251. Examinez le message de la valeur TTL dépassée pour ICMP. Ceci montre la manière dont la commande **`tracert`** suit le chemin du réseau vers la destination.

Tâche 4 : Remarques générales

Le protocole ICMP est très utile lors du dépannage de problèmes de connectivité réseau. Sans messages ICMP, un expéditeur est dans l'incapacité d'expliquer l'échec de la connexion de la destination. À l'aide de la commande **`ping`**, différentes valeurs de types de message ICMP ont été capturées et évaluées.

Tâche 5 : nettoyage

Il se peut que Wireshark ait été chargé sur l'ordinateur hôte pod. Si le programme doit être supprimé, cliquez sur **Démarrer > Panneau de configuration > Ajout/Suppression de programmes**, puis faites défiler la liste vers le bas jusqu'à Wireshark. Cliquez sur le nom de fichier, sur **Supprimer**, puis suivez les instructions de désinstallation.

Supprimez tout fichier pcap de Wireshark qui a été créé sur l'ordinateur hôte pod.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

Exercice 6.7.3 : création d'un sous-réseau avec une adresse IPv4 - Partie 1

Objectifs pédagogiques

À la fin de cet exercice, vous serez en mesure de déterminer les informations de réseau relatives à une adresse IP et à un masque de réseau spécifiques.

Contexte

Cet exercice a pour objectif de décrire comment obtenir des informations de réseau à partir d'une adresse IP donnée.

Scénario

Une adresse IP et un masque de réseau permettent de déterminer d'autres informations sur l'adresse IP :

- Adresse réseau
- Adresse de diffusion réseau
- Nombre total de bits d'hôte
- Nombre d'hôtes

Tâche 1 : détermination des informations de réseau relatives à une adresse IP spécifiqueCompte tenu des données suivantes :

Adresse IP d'hôte	**172.25.114.250**
Masque de réseau	**255.255.0.0 (/16)**

Recherchez les éléments suivants :

Adresse réseau	
Adresse de diffusion réseau	
Nombre total de bits d'hôte	
Nombre d'hôtes	

Étape 1 : conversion de l'adresse IP d'hôte et du masque de réseau en notation binaire.

Convertissez l'adresse IP d'hôte et le masque de réseau en notation binaire :

	172	**25**	**114**	**250**
Adresse IP	10101100	00011001	01110010	11111010
Masque de réseau	11111111	11111111	00000000	00000000
	255	**255**	**0**	**0**

Étape 2 : détermination de l'adresse réseau

1. Tracez une ligne sous le masque.
2. Exécutez une opération AND de type binaire sur l'adresse IP et le masque de sous-réseau.

   Remarque : l'opération 1 AND génère le résultat 1 ; l'opération 0 AND une valeur quelconque génère le résultat 0.
3. Exprimez le résultat sous forme de notation en décimale à points.
4. Il s'agit de l'adresse réseau correspondant à l'adresse IP d'hôte ci-dessus, soit **172.25.0.0.**

	172	**25**	**114**	**250**
Adresse IP	10101100	00011001	01110010	11111010
Masque de sous-réseau	11111111	11111111	00000000	00000000
Adresse réseau	10101100	00011001	00000000	00000000
	172	**25**	**0**	**0**

Étape 3 : détermination de l'adresse de diffusion relative à l'adresse réseau

Dans le masque de réseau, la partie réseau de l'adresse est séparée de la partie hôte. Tous les 0 s'affichent dans la partie hôte de l'adresse réseau tandis que tous les 1 s'affichent dans la partie hôte de l'adresse de diffusion.

	172	**25**	0	**0**
Adresse réseau	10101100	00011001	00000000	00000000
Mask	11111111	11111111	00000000	00000000
Diffusion.	10101100	00011001	11111111	11111111
	172	**25**	**255**	**255**

Pour déterminer le nombre total d'hôtes utilisables sur le réseau, comptez le nombre de bits d'hôte.

Bits d'hôte : 16

Nombre total d'hôtes :

2^{16} = 65,536

65 536 – 2 = 65 534 (adresses ne pouvant pas utiliser l'adresse *avec tous les 0*, soit l'adresse réseau, ou l'adresse *avec tous les 1*, soit l'adresse de diffusion)

Ajoutez ces informations au tableau :

Adresse IP d'hôte	**172.25.114.250**
Masque de réseau	**255.255.0.0 (/16)**
Adresse réseau	
Adresse de diffusion réseau	
Nombre total de bits d'hôte Nombre d'hôtes	

Tâche 2 : confirmation

Pour chaque problème :

Créez une fiche de travail pour présenter et enregistrer les résultats obtenus.

Problème 1

Adresse IP d'hôte	**172.30.1.33**
Masque de réseau	**255.255.0.0**
Adresse réseau	
Adresse de diffusion réseau	
Nombre total de bits d'hôte	
Nombre d'hôtes	

Problème 2

Adresse IP d'hôte	**172.30.1.33**
Masque de réseau	**255.255.255.0**
Adresse réseau	
Adresse de diffusion réseau	
Nombre total de bits d'hôte	
Nombre d'hôtes	

Problème 3

Adresse IP d'hôte	**192.168.10.234**
Masque de réseau	**255.255.255.0**
Adresse réseau	
Adresse de diffusion réseau	
Nombre total de bits d'hôte	
Nombre d'hôtes	

Problème 4

Adresse IP d'hôte	**172.17.99.71**
Masque de réseau	**255.255.0.0**
Adresse réseau	
Adresse de diffusion réseau	
Nombre total de bits d'hôte	
Nombre d'hôtes	

Problème 5

Adresse IP d'hôte	**192.168.3.219**
Masque de réseau	**255.255.0.0**
Adresse réseau	
Adresse de diffusion réseau	
Nombre total de bits d'hôte	
Nombre d'hôtes	

Problème 6

Adresse IP d'hôte	**192.168.3.219**
Masque de réseau	**255.255.255.224**
Adresse réseau	
Adresse de diffusion réseau	
Nombre total de bits d'hôte	
Nombre d'hôtes	

Tâche 3 : nettoyage

Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

Exercice 6.7.4 : création d'un sous-réseau avec une adresse IPv4 - Partie 2

Objectifs pédagogiques

À la fin de cet exercice, vous serez en mesure de déterminer les informations de sous-réseau relatives à une adresse IP et un masque de sous-réseau spécifiques.

Contexte

Bits empruntés

Combien de bits faut-il emprunter pour créer un certain nombre de sous-réseaux ou d'hôtes par sous-réseau ?

Le tableau ci-dessous permet de déterminer facilement le nombre de bits à emprunter.

N'oubliez pas d'effectuer l'opération suivante :

- Soustraire le chiffre 2 pour obtenir le nombre d'hôtes utilisables par sous-réseau (1 pour l'adresse de sous-réseau et 1 pour l'adresse de diffusion du sous-réseau).

2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
1,024	512	256	128	64	32	16	8	4	2	1
Nombre de bits empruntés :										
10	9	8	7	6	5	4	3	2	1	1
1,024	512	256	128	64	32	16	8	4	2	1
Hôtes ou sous-réseaux										

Valeurs de masque de sous-réseau possibles

Dans la mesure où les masques de sous-réseau doivent être désignés par des 1 continus suivis de 0 continus, la notation en décimale à point doit correspondre à l'une des valeurs de la liste ci-dessous :

Déc.	*Binaire*
255	11111111
254	11111110
252	11111100
248	11111000
240	11110000
224	11100000
192	11000000
128	10000000
0	00000000

Scénario

Une adresse IP, un masque de réseau et un masque de sous-réseau permettent de déterminer d'autres informations sur l'adresse IP :

- Adresse du sous-réseau
- Adresse de diffusion du sous-réseau
- Plage d'adresses d'hôte du sous-réseau
- Nombre maximal de sous-réseaux du masque de sous-réseau
- Nombre d'hôtes de chaque sous-réseau
- Nombre de bits de sous-réseau
- Numéro du sous-réseau

Tâche 1 : détermination des informations de sous-réseau relatives à une adresse IP et un masque de sous-réseau spécifiques.

Compte tenu des données suivantes :

Adresse IP d'hôte	**172.25.114.250**
Masque de réseau	**255.255.0.0 (/16)**
Masque de sous-réseau	**255.255.255.192 (/26)**

Recherchez les éléments suivants :

Nombre de bits de sous-réseau	
Nombre de sous-réseaux	
Nombre de bits d'hôte par sous-réseau	
Nombre d'hôtes utilisables par sous-réseau	
Adresse de sous-réseau pour cette adresse IP	
Adresse IP du premier hôte sur le sous-réseau	
Adresse IP du dernier hôte sur le sous-réseau	
Adresse de diffusion du sous-réseau	

Étape 1 : conversion de l'adresse IP d'hôte et du masque de sous-réseau en notation binaire.

	172	**25**	**114**	**250**
Adresse IP	10101100	11001000	01110010	11111010
	11111111	11111111	11111111	11000000
Masque de sous-réseau	**255**	**255**	**255**	**192**

Étape 2 : détermination du réseau (ou sous-réseau) sur lequel réside l'adresse hôte.

1. Tracez une ligne sous le masque.
2. Exécutez une opération AND de type binaire sur l'adresse IP et le masque de sous-réseau.

   Remarque : l'opération 1 AND génère le résultat 1 ; l'opération 0 AND une valeur quelconque génère le résultat 0.
3. Exprimez le résultat sous forme de notation en décimale à points.
4. Il s'agit de l' adresse du sous-réseau**,** à savoir **172.25.114.192**

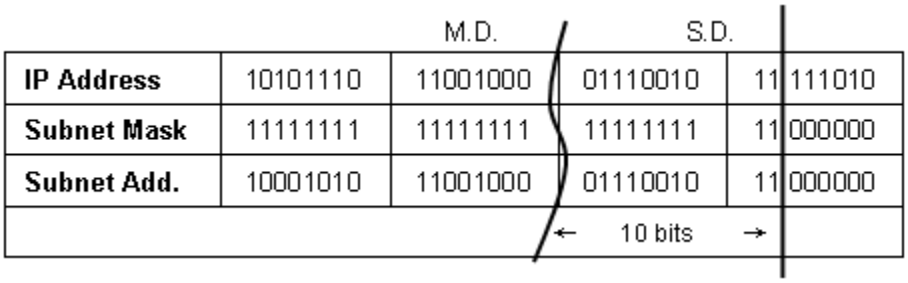
	172	**25**	**114**	**250**
Adresse IP	10101100	11001000	01110010	11111010
Masque de sous-réseau	11111111	11111111	11111111	11000000
Adresse de sous-réseau	10101100	11001000	01110010	11000000
	172	**25**	**114**	**192**

Ajoutez ces informations au tableau :

Adresse de sous-réseau pour cette adresse IP	172.25.114.192

Étape 3 : détermination des bits de l'adresse contenant les informations de réseau et de ceux contenant les informations d'hôte.

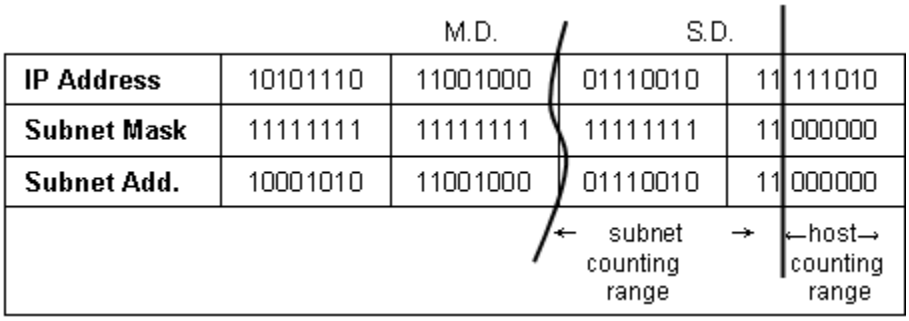
1. Tracez une ligne ondulée symbolisant la *division principale* (M.D, Major Divide) à l'endroit où les 1 du masque de sous-réseau principal se terminent (c'est-à-dire le masque si aucun sous-réseau n'existe). Dans cet exemple, le masque de réseau principal est 255.255.0.0, soit les 16 premiers bits les plus à gauche.
2. Tracez une ligne droite symbolisant la *division de sous-réseau* à l'endroit où les 1 du masque de sous-réseau donné se terminent. Les informations relatives au réseau se terminent là où se terminent les 1 dans le masque.



3. Pour déterminer le nombre de bits de sous-réseau en toute simplicité, comptez les bits entre la division principale et la division de sous-réseau. Dans cet exemple, il s'élève à 10.

Étape 4 : détermination des plages de bits des sous-réseaux et des hôtes

1. Marquez la *plage de comptage de sous-réseaux* comprise entre la principale division et la division de sous-réseau. Elle se compose des bits incrémentés pour constituer les numéros ou adresses de sous-réseau.
2. Marquez la *plage de comptage d'hôtes* comprise entre la division de sous-réseau et les derniers bits à l'extrémité droite. Elle se compose des bits incrémentés pour constituer les numéros ou adresses d'hôte.



Étape 5 : détermination de la plage d'adresses d'hôte disponibles sur le sous-réseau et de l'adresse de diffusion du sous-réseau

1. Notez tous les bits de réseau/sous-réseau de l'adresse réseau (c'est-à-dire tous les bits situés avant la division de sous-réseau).
2. Dans la partie hôte (à droite de la division de sous-réseau), faites en sorte que tous les bits d'hôte soient des 0, sauf le bit le plus à droite (soit le bit le moins significatif) qui doit être 1. Vous obtenez ainsi la *première* adresse IP d'hôte du sous-réseau, qui correspond à la *première partie* de la réponse relative à la *plage d'adresses d'hôte du sous-réseau*. . Dans cet exemple, il s'agit de **172.25.114.193.**
3. Dans la partie hôte (à droite de la division de sous-réseau), faites en sorte que tous les bits d'hôte soient des 1, sauf le bit le plus à droite (soit le bit le moins significatif) qui doit être 0. Vous obtenez ainsi la *dernière* adresse IP d'hôte du sous-réseau, qui correspond à la dernière partie de la réponse relative à la*plage d'adresses d'hôte du sous-réseau*. Dans cet exemple, il s'agit de **172.25.114.254.**
4. Enfin, dans la partie hôte (à droite de la division de sous-réseau), faites en sorte que tous les bits d'hôte soient des 1. Cela permet d'obtenir l'adresse IP de diffusion du sous-réseau. Vous obtenez ainsi la réponse relative à l'*adresse de diffusion du sous-réseau.* Dans cet exemple, il s'agit de **172.25.114.255.**

		M.D.	S.D.		
IP Address	10101100	11001000	01110010	11	111010
Subnet Mask	11111111	11111111	11111111	11	000000
Subnet Add.	10101100	11001000	01110010	11	000000
			← **subnet** → **counting range**		← **host** → **counting range**
First Host	10101100	11001000	01110010	11	000001
	172	25	114		193
Last Host	10101100	11001000	01110010	11	111110
	172	25	114		254
Broadcast	10101100	11001000	01110010	11	111111
	172	25	114		255

Ajoutons une partie de ces informations à notre table :

Adresse IP d'hôte	**172.25.114.250**
Masque de réseau principal	**255.255.0.0 (/16)**
Adresse réseau principale (de base)	172.25.0.0
Adresse de diffusion réseau principale	172.25.255.255
Nombre total de bits d'hôte Nombre d'hôtes	16 bits ou 2^{16} ou 65 536 hôtes au total 65 536 – 2 = 65 534 hôtes utilisables
Masque de sous-réseau	**255.255.255.192 (/26)**
Nombre de bits de sous-réseau Nombre de sous-réseaux	
Nombre de bits d'hôte par sous-réseau Nombre d'hôtes utilisables par sous-réseau	
Adresse de sous-réseau pour cette adresse IP	
Adresse IP du premier hôte sur le sous-réseau	
Adresse IP du dernier hôte sur le sous-réseau	
Adresse de diffusion du sous-réseau	

Étape 6 : déterminer le nombre de sous-réseaux ;

Le nombre de sous-réseaux est déterminé par le nombre de bits qui se trouvent dans la *plage de comptage de sous-réseaux* (soit 10 bits dans cet exemple).

Utilisez la formule 2^n, où *n* est le nombre de bits dans la *plage de comptage de sous-réseaux*.

1. $2^{10} = 1024$

Nombre de bits de sous-réseau Nombre de sous-réseaux (tous les 0 sont utilisés ; tous les 1 ne sont pas utilisés)	10 bits $2^{10} = 1024$ sous-réseaux

Étape 7 : détermination du nombre d'hôtes utilisables par sous-réseau.

Pour déterminer le nombre d'hôtes par sous-réseau, soustrayez le chiffre 2 (1 pour l'adresse de sous-réseau et 1 pour l'adresse de diffusion du sous-réseau) au nombre de bits d'hôte (dans cet exemple, il s'agit de 6 bits).

$2^6 – 2 = 64 – 2 = 62$ hôtes par sous-réseau

Nombre de bits d'hôte par sous-réseau Nombre d'hôtes utilisables par sous-réseau	6 bits $2^6 – 2 = 64 – 2 = 62$ hôtes par sous-réseau

Étape 8 : réponses finales

Adresse IP d'hôte	**172.25.114.250**
Masque de sous-réseau	**255.255.255.192 (/26)**
Nombre de bits de sous-réseau Nombre de sous-réseaux	10 bits $2^{10} = 1024$ sous-réseaux
Nombre de bits d'hôte par sous-réseau Nombre d'hôtes utilisables par sous-réseau	6 bits $2^6 – 2 = 64 – 2 = 62$ hôtes par sous-réseau
Adresse de sous-réseau pour cette adresse IP	172.25.114.192
Adresse IP du premier hôte sur le sous-réseau	172.25.114.193
Adresse IP du dernier hôte sur le sous-réseau	172.25.114.254
Adresse de diffusion du sous-réseau	172.25.114.255

Tâche 2 : confirmation.

Pour chaque problème :

Créez une fiche de travail pour présenter et enregistrer les résultats obtenus.

Problème 1

Adresse IP d'hôte	**172.30.1.33**
Masque de sous-réseau	**255.255.255.0**
Nombre de bits de sous-réseau	
Nombre de sous-réseaux	
Nombre de bits d'hôte par sous-réseau	
Nombre d'hôtes utilisables par sous-réseau	
Adresse de sous-réseau pour cette adresse IP	
Adresse IP du premier hôte sur le sous-réseau	
Adresse IP du dernier hôte sur le sous-réseau	
Adresse de diffusion du sous-réseau	

Problème 2

Adresse IP d'hôte	**172.30.1.33**
Masque de sous-réseau	**255.255.255.252**
Nombre de bits de sous-réseau	
Nombre de sous-réseaux	
Nombre de bits d'hôte par sous-réseau	
Nombre d'hôtes utilisables par sous-réseau	
Adresse de sous-réseau pour cette adresse IP	
Adresse IP du premier hôte sur le sous-réseau	
Adresse IP du dernier hôte sur le sous-réseau	
Adresse de diffusion du sous-réseau	

Problème 3

Adresse IP d'hôte	**192.192.10.234**
Masque de sous-réseau	**255.255.255.0**
Nombre de bits de sous-réseau	
Nombre de sous-réseaux	
Nombre de bits d'hôte par sous-réseau	
Nombre d'hôtes utilisables par sous-réseau	
Adresse de sous-réseau pour cette adresse IP	
Adresse IP du premier hôte sur le sous-réseau	
Adresse IP du dernier hôte sur le sous-réseau	
Adresse de diffusion du sous-réseau	

Problème 4

Adresse IP d'hôte	**172.17.99.71**
Masque de sous-réseau	**255.255.0.0**
Nombre de bits de sous-réseau	
Nombre de sous-réseaux	
Nombre de bits d'hôte par sous-réseau	
Nombre d'hôtes utilisables par sous-réseau	
Adresse de sous-réseau pour cette adresse IP	
Adresse IP du premier hôte sur le sous-réseau	
Adresse IP du dernier hôte sur le sous-réseau	
Adresse de diffusion du sous-réseau	

Problème 5

Adresse IP d'hôte	**192.168.3.219**
Masque de sous-réseau	**255.255.255.0**
Nombre de bits de sous-réseau	
Nombre de sous-réseaux	
Nombre de bits d'hôte par sous-réseau	
Nombre d'hôtes utilisables par sous-réseau	
Adresse de sous-réseau pour cette adresse IP	
Adresse IP du premier hôte sur le sous-réseau	
Adresse IP du dernier hôte sur le sous-réseau	
Adresse de diffusion du sous-réseau	

Problème 6

Adresse IP d'hôte	**192.168.3.217**
Masque de sous-réseau	**255.255.255.252**
Nombre de bits de sous-réseau	
Nombre de sous-réseaux	
Nombre de bits d'hôte par sous-réseau	
Nombre d'hôtes utilisables par sous-réseau	
Adresse de sous-réseau pour cette adresse IP	
Adresse IP du premier hôte sur le sous-réseau	
Adresse IP du dernier hôte sur le sous-réseau	
Adresse de diffusion du sous-réseau	

Tâche 3 : nettoyage

Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

Travaux pratiques 6.7.5 : configuration d'un sous-réseau et d'un routeur

Schéma de la topologie

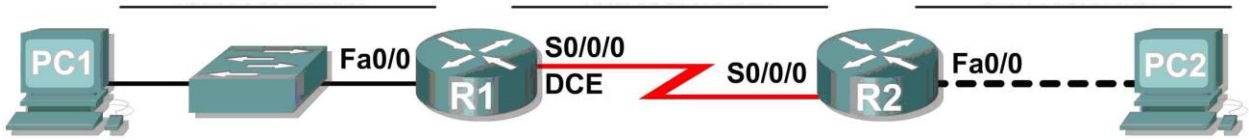


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	Fa0/0			N/D
	S0/0/0			N/D
R2	Fa0/0			N/D
	S0/0/0			N/D
PC1	Carte réseau			
PC2	Carte réseau			

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- créer des sous-réseaux et des espaces d'adressage selon les consignes données ;
- attribuer des adresses appropriées aux interfaces et les noter par écrit ;
- configurer et activer des interfaces Série et FastEthernet ;
- tester et vérifier les configurations ;
- réfléchir à la mise en œuvre du réseau et la noter par écrit.

Scénario

Au cours de ces travaux pratiques, vous concevrez et appliquerez un système d'adressage IP pour la topologie présentée dans le schéma. Il vous est fourni un bloc d'adresses que vous devez diviser en sous-réseaux pour proposer un schéma d'adressage logique pour le réseau. Les routeurs sont ensuite prêts pour la configuration d'adressage d'interface en fonction de votre système d'adressage IP. Une fois la configuration terminée, vérifiez que le réseau fonctionne correctement.

Tâche 1 : découpage en sous-réseaux de l'espace d'adressage.

Étape 1 : examen des besoins du réseau.

L'espace d'adressage 192.168.1.0/24 a été mis à votre disposition pour votre conception de réseau. Le réseau est constitué des segments suivants :

- Le réseau local connecté au routeur R1 a besoin d'adresses IP en nombre suffisant pour prendre en charge 15 hôtes.
- Le réseau local connecté au routeur R2 a besoin d'adresses IP en nombre suffisant pour prendre en charge 30 hôtes.
- La liaison entre le routeur R1 et le routeur R2 exige des adresses IP à chacune de ses extrémités.

Le plan doit disposer de sous-réseaux de taille égale et utiliser les tailles de sous-réseaux les plus petites pour s'ajuster au nombre approprié d'hôtes.

Étape 2 : tenez compte des questions suivantes lorsque vous créez votre conception de réseau.

De combien de sous-réseaux ce réseau a-t-il besoin ? _____

Quel est le masque de sous-réseau de ce réseau au format avec point ? _____

Quel est le masque de sous-réseau de ce réseau au format avec barre oblique ? _____

Combien y a-t-il d'hôtes utilisables par sous-réseau ? _____

Étape 3 : attribution d'adresses de sous-réseau au schéma de la topologie.

1. Attribuez le deuxième sous-réseau au réseau raccordé à R1.
2. Attribuez le troisième sous-réseau à la liaison entre R1 et R2.
3. Attribuez le quatrième sous-réseau au réseau raccordé à R2.

Tâche 2 : détermination des adresses des interfaces.

Étape 1 : attribution des adresses appropriées aux interfaces des périphériques.

1. Attribuez la première adresse hôte valide du deuxième sous-réseau à l'interface du réseau local sur R1.
2. Attribuez la dernière adresse d'hôte valide du réseau 3 au PC1.
3. Attribuez la première adresse d'hôte valide du troisième sous-réseau à l'interface du réseau étendu sur R1.
4. Attribuez la dernière adresse d'hôte valide du troisième sous-réseau à l'interface du réseau étendu sur R2.
5. Attribuez la première adresse d'hôte valide du quatrième sous-réseau à l'interface du réseau local sur R2.
6. Attribuez la dernière adresse d'hôte valide du quatrième sous-réseau au PC2.

Étape 2 : description des adresses à utiliser dans le tableau fourni sous le schéma de la topologie.

Tâche 3 : configuration des adresses série et FastEthernet.

Étape 1 : configuration des interfaces des routeurs.

Configurez les interfaces des routeurs R1 et R2 avec les adresses IP provenant de votre conception de réseau. Remarque : utilisez l'onglet Config pour effectuer l'exercice dans Packet Tracer. Une fois que vous avez terminé, veillez à enregistrer la configuration en cours d'exécution sur le NVRAM du routeur.

Étape 2 : configuration des interfaces des PC.

Configurez les interfaces Ethernet de PC1 et de PC2 avec les adresses IP et les passerelles par défaut provenant de votre conception de réseau.

Tâche 4 : vérification des configurations.

Répondez aux questions suivantes pour vérifier que le réseau fonctionne comme prévu.

Depuis l'hôte raccordé à R1, est-il possible d'envoyer une requête ping sur la passerelle par défaut ?

_____

Depuis l'hôte raccordé à R2, est-il possible d'envoyer une requête ping sur la passerelle par défaut ?

_____

Depuis le routeur R1, est-il possible d'envoyer une requête ping sur l'interface Serial 0/0/0 de R2 ?

_____

Depuis le routeur R2, est-il possible d'envoyer une requête ping sur l'interface Serial 0/0/0 de R1 ?

_____

La réponse aux questions précédentes doit être **oui**. Si l'une des requêtes ping ci-dessus a échoué, vérifiez vos connexions physiques et vos configurations.

Tâche 5 : Remarques générales

Le réseau contient-il des périphériques ne pouvant pas s'envoyer mutuellement des requêtes ping ?

_____

_____

Que manque-t-il au réseau pour que la communication entre ces périphériques soit possible ?

_____

_____

6.8.1 : exercice d'intégration des compétences - Planification de sous-réseaux et configuration d'adresses IP

Diagramme de topologie

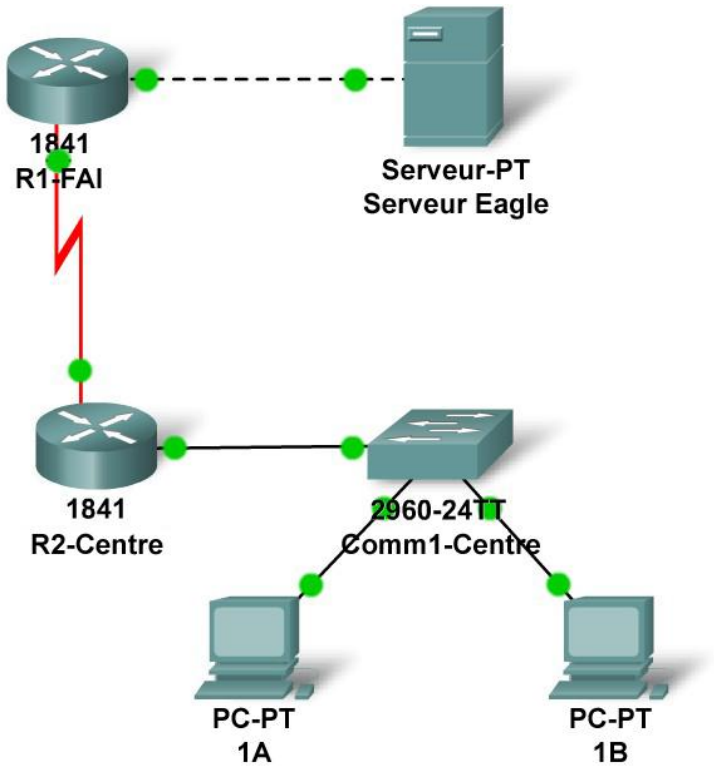


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	Fa0/0			N/A
	S0/0/0			N/A
R2-Central	Fa0/0			N/A
	S0/0/0			N/A
PC 1A	La carte réseau			
PC 1B	La carte réseau			
Serveur Eagle	La carte réseau			

Objectifs pédagogiques

- Planifier des sous-réseaux IP
  - Mise en pratique de vos compétences en matière de sous-réseaux
- Construire le réseau
  - Connexion des périphériques avec des câbles Ethernet et série
- Configurer le réseau
  - Application de votre schéma de découpage en sous-réseaux au serveur, aux PC et aux interfaces de routeur ; configuration des services et du routage statique
- Tester le réseau.
  - Utilisation de la commande ping, du traçage, du trafic Web et de l'outil **Inspect**

Contexte

Vous avez été chargé de mettre en œuvre la topologie de travaux pratiques type mais avec un nouveau modèle d'adressage IP. Vous allez exploiter les nombreuses compétences que vous avez acquises jusqu'ici à travers ce cours.

Tâche 1 : planification de sous-réseaux IP

On vous a attribué le bloc d'adresses IP 192.168.23.0 /24. Vous devez configurer les réseaux existants et prévoir les besoins ultérieurs.

Les attributions de sous-réseaux sont les suivantes :

- 1er sous-réseau, réseau local existant des participants (connecté au routeur R2-Central), jusqu'à 60 hôtes ;
- 2ème sous-réseau, futur réseau local des participants, jusqu'à 28 hôtes ;
- 3ème sous-réseau, réseau local existant du fournisseur de services Internet (ISP), jusqu'à 12 hôtes ;
- 4ème sous-réseau, futur réseau local du fournisseur de services Internet (ISP), jusqu'à 8 hôtes ;
- 5ème sous-réseau, réseau étendu (WAN) existant, liaison point à point ;
- 6ème sous-réseau, futur réseau WAN, liaison point à point ;
- 7ème sous-réseau, futur réseau WAN, liaison point à point

Adresses IP d'interface :

- Pour le serveur, configurez la deuxième adresse IP utilisable la plus élevée sur le sous-réseau LAN existant du fournisseur de services Internet.
- Pour l'interface Fa0/0 du routeur R1-ISP, configurez l'adresse IP utilisable la plus élevée sur le sous-réseau LAN existant du fournisseur de services Internet.
- Pour l'interface S0/0/0 du routeur R1-ISP, configurez l'adresse utilisable la plus élevée sur le sous-réseau WAN existant.
- Pour l'interface S0/0/0 du routeur R2-Central, utilisez l'adresse utilisable la plus basse sur le sous-réseau WAN existant.
- Pour l'interface Fa0/0 du routeur R2-Central, utilisez l'adresse utilisable la plus élevée sur le sous-réseau LAN existant des participants.
- Pour les hôtes 1A et 1B, utilisez les deux premières adresses IP (les deux adresses utilisables les plus basses) du sous-réseau LAN existant des participants.

Configurations supplémentaires :

- Pour les PC 1A et 1B, outre la configuration IP, configurez-les de sorte qu'ils utilisent les services DNS.
- Pour le serveur, activez les services DNS, utilisez le nom de domaine eagle-server.example.com, puis activez les services HTTP.
- Pour l'interface série du routeur R1-ISP, vous devrez définir la fréquence d'horloge (mécanisme de synchronisation requis sur l'extrémité ETCD des liaisons série) à 64 000.
- La fréquence d'horloge n'est pas nécessaire du côté de l'ETTD, en l'occurrence l'interface série du routeur R2-Central.

Tâche 2 : finalisation de la construction du réseau dans Packet Tracer

Ajoutez des câbles là où il en manque.

- Connectez une extrémité d'un câble série ETCD à l'interface S0/0/0 du routeur R1-ISP et l'autre extrémité à l'interface S0/0/0 du routeur R2-Central.
- Connectez le PC 1A au premier port FastEthernet du commutateur S1-Central.
- Connectez le PC 1B au second port FastEthernet du commutateur S1-Central.
- Connectez l'interface Fa0/0 du routeur R2-Central au port FastEthernet le plus élevé du commutateur S1-Central.
- Pour tous les périphériques, assurez-vous qu'ils sont sous tension et que leurs interfaces sont activées.

Tâche 3 : configuration du réseau

Vous devez configurer le serveur, les deux routeurs et les deux PC..Vous n'avez pas besoin de configurer le commutateur. Vous n'avez pas non plus besoin de configurer les routeurs IOS CLI. La configuration du routeur a en partie déjà été définie pour vous : tout ce qu'il vous reste à faire est de configurer les routes statiques et les interfaces via l'interface graphique utilisateur. La route statique du routeur R1-ISP doit pointer vers le sous-réseau LAN existant des participants via l'adresse IP de l'interface série du routeur R2-Central ; la route statique du routeur R2-Central doit être une route statique par défaut qui pointe vers l'adresse IP de l'interface série du routeur R1-SP. Ces procédures ont été expliquées au chapitre 5 de l'exercice d'intégration des compétences.

Tâche 4 : test du réseau

Utilisez la commande ping, le traçage, le trafic Web et l'outil **Inspect**. Suivez le flux de paquets en mode Simulation, sans masquer HTTP, DNS, TCP, UDP et ICMP, pour vérifier si vous avez compris le fonctionnement du réseau.

Tâche 5 : remarques générales

Réfléchissez à ce que vous avez appris jusqu'ici. La mise en pratique des compétences acquises en matière de sous-réseaux IP, de construction, de configuration et de test de réseau vous serons très utiles tout au long des cours sur les réseaux.

Travaux pratiques 7.5.2 : examen des trames

Schéma de la topologie

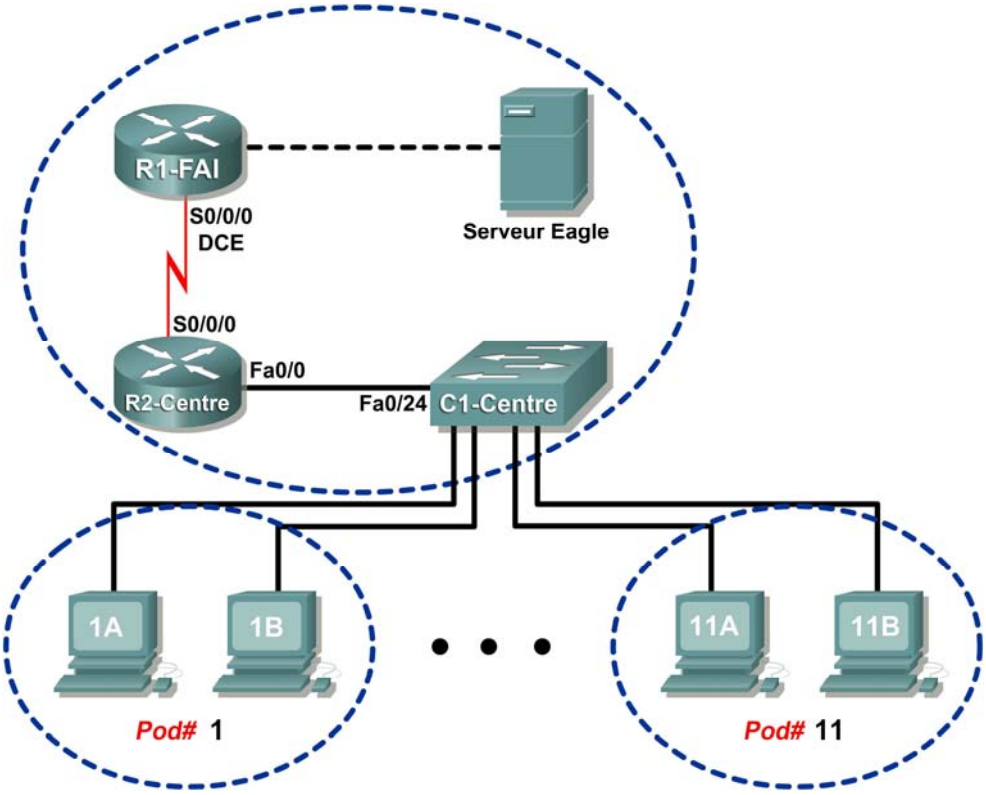


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/D
	Fa0/0	192.168.254.253	255.255.255.0	N/D
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/D
	Fa0/0	172.16.255.254	255.255.0.0	N/D
Eagle Server	N/D	192.168.254.254	255.255.255.0	192.168.254.253
	N/D	172.31.24.254	255.255.255.0	N/D
hôte*Pod#***A**	N/D	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
hôte*Pod#***B**	N/D	172.16. *Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	N/D	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- expliquer les champs d'en-tête dans une trame Ethernet II ;
- utiliser Wireshark pour capturer et analyser les trames Ethernet II.

Contexte

Lorsque des protocoles de couche supérieure communiquent entre eux, les données circulent dans les couches du modèle OSI et sont encapsulées dans une trame de couche 2. La composition des trames dépend du type d'accès aux supports. Par exemple, si le protocole de couche supérieure est TCP/IP et que l'accès aux supports est Ethernet, l'encapsulation des trames de couche 2 est Ethernet II.

Lorsque vous étudiez les concepts de couche 2, il est utile d'analyser les informations d'en-tête des trames. L'en-tête de trame Ethernet II est examiné dans ces travaux pratiques. Les trames Ethernet II peuvent prendre en charge différents protocoles de couche supérieure, tels que TCP/IP.

Scénario

Wireshark permet de capturer et d'analyser les champs d'en-tête de trames Ethernet II. Si vous n'avez pas effectué le téléchargement de Wireshark sur l'ordinateur hôte pod, utilisez l'adresse URL `ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter7/`, fichier `wireshark-setup-0.99.4.exe`.

La commande **`ping`** de Windows permet de générer le trafic réseau pour la capture Wireshark.

Tâche 1 : expliquer les champs d'en-tête dans une trame Ethernet II.

Le format d'une trame Ethernet II est illustré à la figure 1.

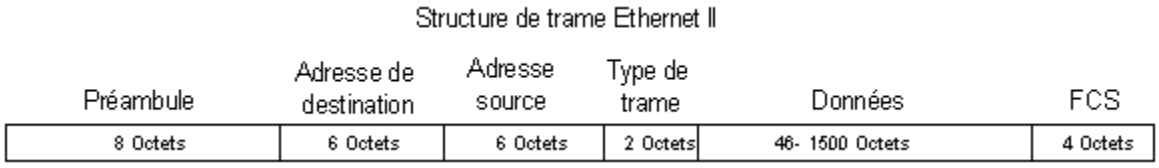


Figure 1. Format de trame Ethernet II

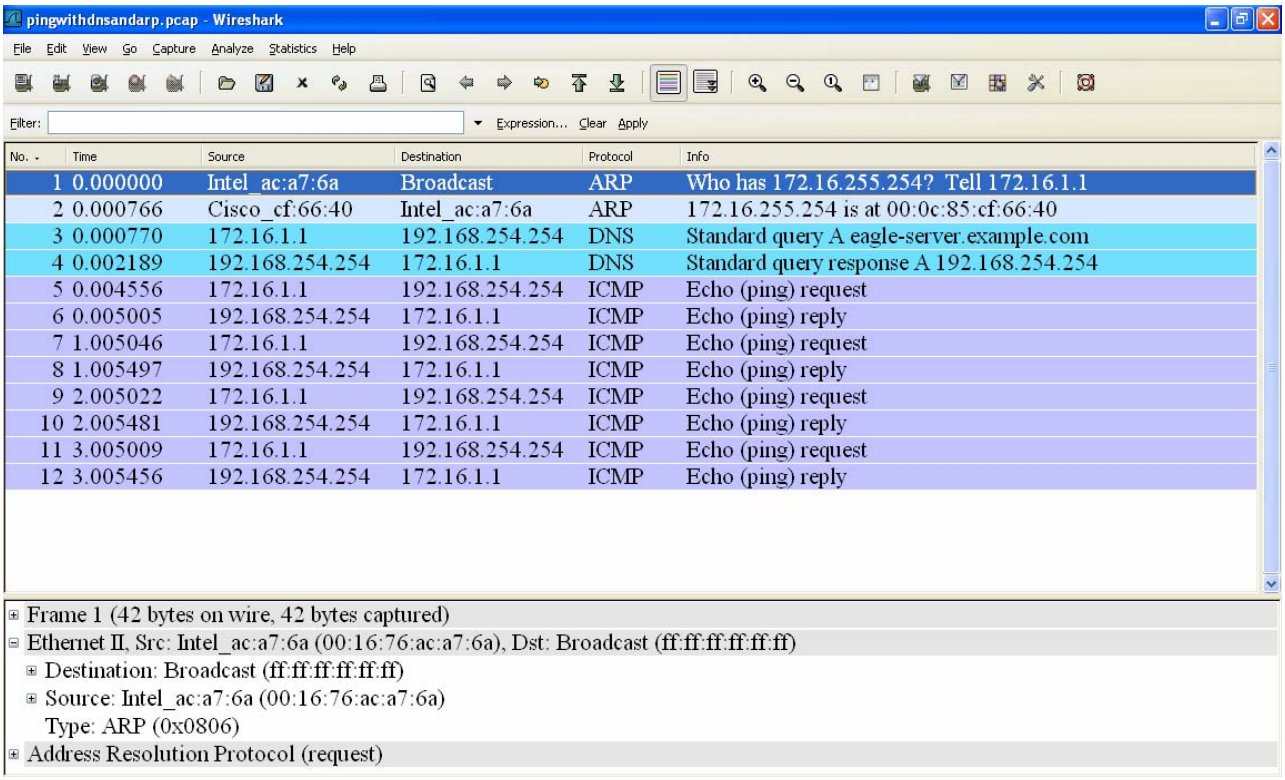


Figure 2. Capture Wireshark de la commande `ping`

À la figure 2, la fenêtre Panel List affiche une capture Wireshark d'une commande **`ping`** entre un ordinateur hôte pod et Eagle Server. La session commence par le protocole qui recherche l'adresse MAC du routeur de passerelle, suivi d'une demande DNS. Finalement, la commande **`ping`** exécute des requêtes d'écho.

À la figure 2, la fenêtre Packet Details affiche les informations détaillées de la trame 1. À l'aide de cette fenêtre, il est possible d'obtenir les informations suivantes sur la trame Ethernet II :

Champ	Valeur	Description
Préambule	Non affichée dans la capture.	Ce champ contient des bits de synchronisation traités par la carte réseau.
Adresse de destination	`ff:ff:ff:ff:ff:ff`	Les adresses de couche 2 pour la trame. La longueur de chaque adresse est de 48 bits, ou 6 octets, exprimés en 12 chiffres hexadécimaux, `0-9,A-F`. Le format courant est le suivant : `12:34:56:78:9A:BC`. Les six premiers numéros hexadécimaux indiquent le fabricant de la carte réseau (NIC). Reportez-vous à http://www.neotechcc.org/forum/macid.htm pour obtenir une liste de codes fournisseurs. Les six derniers chiffres hexadécimaux, `ac:a7:6a`, ont le numéro de série de la carte réseau. L'adresse de destination peut être une adresse de diffusion qui ne contient que des 1 ou à monodiffusion. L'adresse source est toujours à monodiffusion.
Adresse source	`00:16:76:ac:a7:6a`	

Champ	Valeur	Description
Type de trame	0x0806	Pour les trames Ethernet II, ce champ contient une valeur hexadécimale qui permet d'indiquer le protocole de couche supérieure dans le champ de données. De nombreux protocoles de couche supérieure sont pris en charge par Ethernet II. Deux types de trame standard sont : Valeur Description 0x0800 Protocole IPv4 0x0806 Résolution de l'adresse ARP
Données	ARP	Contient le protocole encapsulé de niveau supérieur. Le champ de données comprend entre 46 et 1500 octets.
FCS	Non affichée dans la capture.	Séquence de contrôle de trame, que la carte réseau utilise pour identifier les erreurs au cours de la transmission. La valeur est calculée par l'ordinateur émetteur, et englobe les adresses de trames, le type et le champ de données. Elle est vérifiée par le récepteur.

Quelle est la signification de tous les **1** dans le champ adresse de destination ?

_____

_____

À partir des informations contenues dans la fenêtre Packet List pour la **première** trame, répondez aux questions suivantes sur les adresses MAC source et de destination.

Adresse de destination :

Adresse MAC : _____

Fabricant de la carte réseau : _____

Numéro de série de la carte réseau **:** _____

Adresse source :

Adresse MAC : _____

Fabricant de la carte réseau : _____

Numéro de série de la carte réseau **:** _____

À partir des informations contenues dans la fenêtre Packet List pour la **deuxième** trame, répondez aux questions suivantes sur les adresses MAC source et de destination.

Adresse de destination :

Adresse MAC : _____

Fabricant de la carte réseau : _____

Numéro de série de la carte réseau : _____

Adresse source :

Adresse MAC : _____

Fabricant de la carte réseau : _____

Numéro de série de la carte réseau : _____

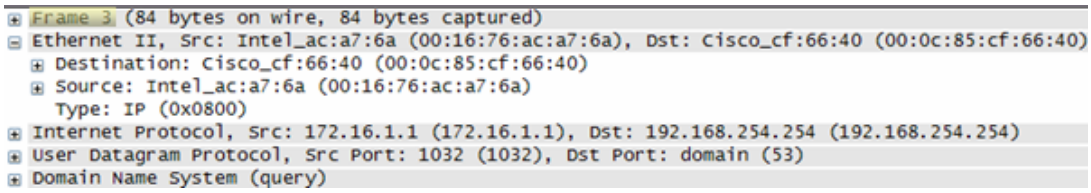


Figure 3. Champs de trame 3

La figure 3 contient une vue éclatée de la capture Wireshark de trame 3. Utilisez ces informations pour remplir le tableau suivant :

Champ	Valeur
Préambule	
Adresse de destination	
Adresse source	
Type de trame	
Données	
FCS	

Dans la tâche suivante, Wireshark permet de capturer et d'analyser des paquets capturés sur l'ordinateur hôte pod.

Tâche 2 : utilisation de Wireshark pour capturer et analyser les trames Ethernet II.

Étape 1 : configuration de Wireshark pour les captures de paquets.

Préparez Wireshark pour les captures. Cliquez sur **Capture > Interfaces**, puis cliquez sur le bouton Démarrer qui correspond à l'adresse IP de l'interface 172.16.x.y. Ceci permet de commencer la capture des paquets.

Étape 2 : démarrage d'une requête ping vers Eagle Server et capture de la session.

Ouvrez une fenêtre de terminal Windows. Cliquez sur **Démarrer > Exécuter**, tapez **cmd**, puis cliquez sur **OK**.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\> ping eagle-server.example.com

Envoi d'une requête ping sur eagle-server.example.com [192.168.254.254]
avec 32 octets de données :

Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=62
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=62
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=62
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=62

Statistiques Ping pour 192.168.254.254 :
    Paquets : Envoyés = 4, Reçus = 4, Perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms

C:\>
```

Figure 4. Ping vers eagle-server.example.com

Envoyez une requête ping vers eagle-server.example.com, comme illustré à la figure 4. Lorsque la commande a terminé l'exécution, arrêtez les captures Wireshark.

Étape 3 : analyse de la capture Wireshark.

La fenêtre Packet List de Wireshark démarre avec une requête et une réponse ARP pour l'adresse MAC de la passerelle. Ensuite, une requête DNS est effectuée pour l'adresse IP de eagle-server.example.com. Finalement, la commande **ping** est exécutée. Votre capture doit être semblable à celle illustrée à la figure 2.

Utilisez votre capture Wireshark de la commande **ping** pour répondre aux questions suivantes :

Informations sur l'adresse MAC de l'ordinateur pod :

Adresse MAC : _____

Fabricant de la carte réseau : _____

Numéro de série de la carte réseau : _____

Informations sur l'adresse MAC de R2-Central :

Adresse MAC : _____

Fabricant de la carte réseau : _____

Numéro de série de la carte réseau : _____

Un participant d'un autre établissement souhaite connaître l'adresse MAC d'Eagle Server. Que lui diriez-vous ?

Quelle est la valeur du type de trame Ethernet II pour une requête ARP ? _____

Quelle est la valeur du type de trame Ethernet II pour une réponse ARP ? _____

Quelle est la valeur du type de trame Ethernet II pour une requête DNS ? _____

Quelle est la valeur du type de trame Ethernet II pour une réponse de requête DNS ? _____

Quelle est la valeur du type de trame Ethernet II pour un écho ICMP ? _____

Quelle est la valeur du type de trame Ethernet II pour une réponse d'écho ICMP ? _____

Tâche 3 : confirmation

Wireshark permet de capturer des sessions provenant d'autres protocoles TCP/IP, tels que FTP et HTTP. Analysez les paquets capturés et vérifiez que le type de trame Ethernet II reste `0x0800`.

Tâche 4 : Remarques générales

Dans ces travaux pratiques, les informations d'en-tête de trames Ethernet II ont été examinées. Un champ préambule contient sept octets de séquences `0101` alternatives, et un octet qui signale le début de la trame, `01010110`. Les adresses MAC source et de destination contiennent 12 chiffres hexadécimaux. Les six premiers chiffres hexadécimaux contiennent le fabricant de la carte réseau, et les six derniers chiffres hexadécimaux contiennent le numéro de série de la carte réseau. Si la trame est une diffusion, l'adresse MAC de destination ne contient que des `1`. Un champ type de trame à 4 octets contient une valeur qui indique le protocole dans le champ de données. Pour IPv4, la valeur est `0x0800`. Le champ de données est variable et contient le protocole encapsulé de la couche supérieure. À la fin de la trame, une valeur FCS de 4 octets permet de vérifier l'absence d'erreurs lors de la transmission.

Tâche 5 : nettoyage

Wireshark a été installé sur l'ordinateur hôte pod. Si Wireshark doit être désinstallé, cliquez sur **Démarrer > Panneau de configuration**. Ouvrez **Ajout/Suppression de programmes**. Sélectionnez Wireshark, puis cliquez sur **Supprimer**.

Supprimez tout fichier créé sur l'ordinateur hôte pod au cours des travaux pratiques.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

7.6.1 : exercice d'intégration des compétences : problèmes liés à la couche liaison de données

Diagramme de topologie

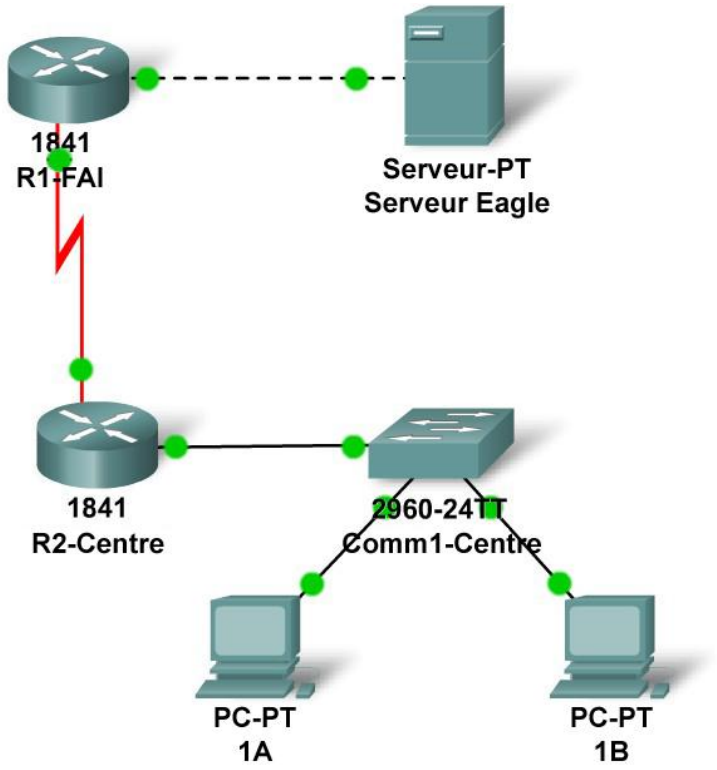


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	**Fa0/0**			N/A
	S0/0/0			N/A
R2-Central	**Fa0/0**			N/A
	S0/0/0			N/A
PC 1A	**La carte réseau**			
PC 1B	**La carte réseau**			
Serveur Eagle	**La carte réseau**			

Objectifs pédagogiques

- Planifier des sous-réseaux IP
  - Mise en pratique de vos compétences en matière de sous-réseaux
- Construire le réseau
  - Connexion des périphériques avec des câbles Ethernet et série
- Configurer le réseau
  - Application de votre schéma de découpage en sous-réseaux au serveur, aux PC et aux interfaces de routeur ; configuration des services et du routage statique
- Tester le réseau.
  - Utilisation de la commande ping, du traçage, du trafic Web et de l'outil **Inspect**

Contexte

Les cartes réseau sont parfois considérées comme des périphériques de couche 2 et de couche 1 (ou comme des composants de couche 2 ou de couche 1 de périphériques fonctionnant sur l'ensemble des 7 couches). Dans le cas d'une connexion série, qui est généralement utilisée dans les connexions de réseau étendu (WAN), la carte réseau est parfois appelée carte WAN (ou WIC). Dans le cadre de cet exercice, vous devez ajouter une carte WIC à un périphérique pour compléter le réseau. Par ailleurs, vous avez été chargé de mettre en œuvre un nouveau modèle d'adressage IP sur la topologie de travaux pratiques Exploration.

Tâche 1 : planification de sous-réseaux IP

On vous a attribué le bloc d'adresses IP 172.16.0.0 /22. Vous devez configurer les réseaux existants et prévoir les besoins ultérieurs.

Les attributions de sous-réseaux sont les suivantes :

- 1er sous-réseau, réseau local existant des participants, jusqu'à 400 hôtes (Fa0/0 sur R2-Central) ;
- 2ème sous-réseau, futur réseau local des participants, jusqu'à 180 hôtes (pas encore mis en œuvre) ;
- 3ème sous-réseau, réseau local existant du fournisseur de services Internet (ISP), jusqu'à 40 hôtes (Fa0/0 sur R1-ISP) ;
- 4ème sous-réseau, futur réseau local du fournisseur de services (ISP), jusqu'à 18 hôtes (pas encore mis en œuvre) ;
- 5ème sous-réseau, réseau étendu (WAN) existant, liaison point à point (S0/0/0 sur R1-ISP et R2-Central) ;
- 6ème sous-réseau, futur réseau WAN, liaison point à point (pas encore mis en œuvre) ;
- 7ème sous-réseau, futur réseau WAN, liaison point à point (pas encore mis en œuvre).

Adresses IP d'interface :

- Pour le serveur, configurez la deuxième adresse IP utilisable la plus élevée sur le sous-réseau LAN du fournisseur de services Internet (ISP).
- Pour l'interface Fa0/0 du routeur R1-ISP, configurez l'adresse IP utilisable la plus élevée sur le sous-réseau LAN du fournisseur de services Internet (ISP).
- Pour l'interface S0/0/0 du routeur R1-ISP, configurez l'adresse utilisable la plus élevée sur le sous-réseau WAN existant.

- Pour l'interface S0/0/0 du routeur R2-Central, utilisez l'adresse utilisable la plus basse sur le sous-réseau WAN existant.
- Pour l'interface Fa0/0 du routeur R2-Central, utilisez l'adresse utilisable la plus élevée sur le sous-réseau LAN existant des participants.
- Pour les PC 1A et 1B, utilisez les deux premières adresses IP (les deux adresses utilisables les plus basses) du sous-réseau LAN existant des participants.

Configurations supplémentaires :

- Pour les PC 1A et 1B, outre la configuration IP, configurez-les de sorte qu'ils utilisent les services DNS.
- Pour le serveur, activez les services DNS, utilisez le nom de domaine eagle-server.example.com, puis activez les services HTTP.

Tâche 2 : finalisation de la construction du réseau dans Packet Tracer, résolution de certains problèmes au niveau de la couche 2

Sur le routeur R2-Central, il manque une carte réseau pour la connexion série à R1-ISP : ajoutez un carte WIC-2T dans le logement de droite. De même, sur R2-Central, l'interface Fa0/0 est désactivée ; activez-la. Connectez un câble série DCE au périphérique R1-ISP S0/0/0. Reliez l'autre extrémité au R2-Central S0/0/0. Vérifiez que tous les périphériques et les interfaces sont sous tenson.

Tâche 3 : configuration du réseau

Vous devez configurer le serveur, les deux routeurs et les deux PC..Vous n'avez pas besoin de configurer le commutateur. Vous n'avez pas non plus besoin de configurer les routeurs IOS CLI. La configuration du routeur a en partie déjà été définie pour vous : tout ce qu'il vous reste à faire est de configurer les routes statiques et les interfaces via l'interface graphique utilisateur. La route statique du routeur R1-ISP doit pointer vers le sous-réseau LAN existant des participants via l'adresse IP de l'interface série du routeur R2-Central ; la route statique du routeur R2-Central doit être une route statique par défaut qui pointe vers l'adresse IP de l'interface série du routeur R1-SP. Ces procédures ont été expliquées au chapitre 5 de l'exercice d'intégration des compétences et mises en pratique au chapitre 6 du même exercice.

Tâche 4 : test du réseau

Utilisez la commande ping, le traçage, le trafic Web et l'outil **Inspect**. Suivez le flux de paquets en mode Simulation, sans masquer HTTP, DNS, TCP, UDP et ICMP, pour vérifier si vous avez compris le fonctionnement du réseau. Soyez en particulier attentif à l'encapsulation de couche 2 utilisée à chaque étape du trajet d'un paquet et à la façon dont les en-têtes changent au niveau des unités de données de protocole de couche 2.

Tâche 5 : remarques générales

Considérez le cas d'un paquet de requête d'écho ICMP envoyé du PC 1A au serveur Eagle Server et du paquet de réponse à l'écho ICMP qui en résulte. Quelles sont les adresses qui restent inchangées dans cette situation, et quelles sont celles qui changent ?

Travaux pratiques 8.4.1 : connecteurs de supports

Câblomètre standard

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- tester les câbles à l'aide d'un testeur de câbles et d'un multimètre réseau ;
- manipuler les fonctions standard d'un testeur de câbles ;
- tester les différents câbles à la recherche d'éventuels problèmes de compatibilité et de câblage.

Contexte

Les câbles à paires torsadées non blindées (UTP) de catégorie 5 (CAT 5) sont connectés de façon à fonctionner. Les périphériques finaux, tels que les routeurs et les ordinateurs hôtes, se connectent aux commutateurs avec des câbles directs de catégorie 5. Vous devez, cependant, utiliser un câble croisé CAT 5 lorsqu'ils sont reliés ensemble. Ceci est également valable pour les commutateurs. Lors de la connexion d'un commutateur à un autre, un câble croisé CAT 5 est de nouveau utilisé.

Les problèmes liés au câblage sont une des principales causes des pannes de réseau. Les tests de câblage de base sont très utiles pour le dépannage des problèmes liés aux câbles à paires torsadées non blindées. La qualité des composants du câblage, l'acheminement et l'installation des câbles ainsi que la qualité du raccordement des connecteurs sont les principaux facteurs pour déterminer le nombre et la gravité des pannes dues aux câbles.

Ressources requises :

- Des câbles droits et croisés fonctionnels de catégorie 5 de différentes couleurs.
- Des câbles droits et croisés de catégorie 5 avec des circuits ouverts au milieu ou des courts-circuits à une extrémité. Les fils doivent être de couleurs et de longueurs différentes.
- Un câblomètre.
- Un multimètre réseau.

TIA/EIA 568B est différent du câblage TIA/EIA 568A. Il est possible d'identifier les câbles directs TIA/EIA 568A par le codage par couleur. Semblable à la figure 2, le schéma de câblage de droite, qui commence par le câble vert-blanc, est identique à chaque extrémité.

Scénario

D'abord, vous déterminez visuellement si le type de câble de catégorie 5 est de croisement ou direct. Ensuite, vous utilisez le testeur de câbles pour vérifier le type de câble, ainsi que les fonctions standard disponibles avec le testeur.

Finalement, vous utilisez le testeur de câbles pour tester les câbles non fonctionnels dont l'inspection visuelle ne permet pas de les déterminer.

Tâche 1 : familiarisation aux fonctions standard d'un testeur de câbles.

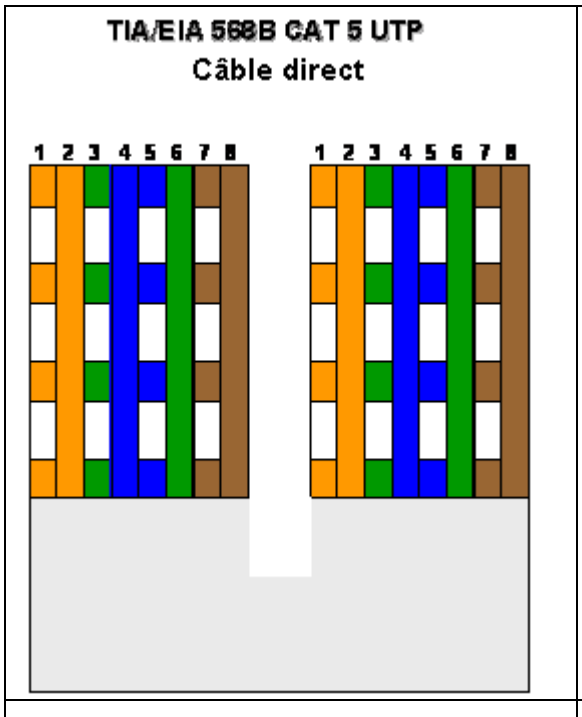


Figure 1. Emplacement du câble direct

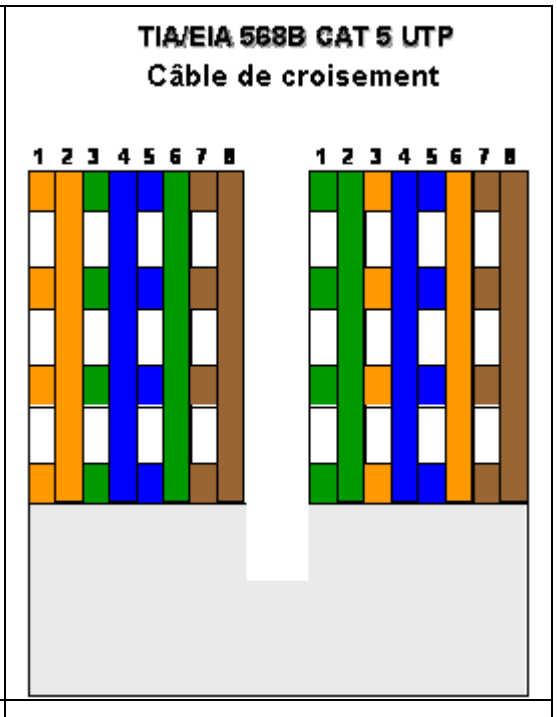


Figure 2. Emplacement du câble de croisement

Les figures 1 et 2 illustrent le positionnement du câblage UTP CAT 5 TIA/EIA 568B pour un câble direct et de croisement, respectivement. Lorsque les connecteurs CAT 5 sont reliés ensemble, la couleur du câble permet de déterminer rapidement son type.

Étape 1 : détermination visuelle des types de câble.

Deux câbles numérotés doivent être disponibles. Effectuez une inspection visuelle des câbles et renseignez le tableau ci-dessous avec la couleur, le type et l'utilisation du câble :

n° de câble	**Couleur de câble**	**Type de câble** (direct ou de croisement)	**Utilisation du câble** (Entourez le périphérique correct)
1			Basculez vers : hôte / périphérique
2			Basculez vers : hôte / périphérique

Il est temps désormais de vérifier le type de câble et d'étudier les fonctions standard du testeur de câbles.

Étape 2 : configuration initiale du câblomètre

Placez le câblomètre en mode schéma de câblage. Reportez-vous au manuel d'instructions si nécessaire. La fonction du schéma de câblage affiche à quelles broches d'une extrémité du câble correspondent les broches de l'autre extrémité du câble.

Reportez-vous au manuel d'instructions et choisissez les options appropriées jusqu'à ce que le testeur possède les paramètres de câblage suivants :

Option du testeur	**Réglage souhaité - UTP**
CÂBLE :	UTP
CÂBLAGE :	10BaseT ou EIA/TIA 4PR
CATÉGORIE :	CATÉGORIE 5
TAILLE DE CÂBLE	AWG 24
CAL à CÂBLE ?	NON
SIGNAL SONORE :	ON ou OFF
CONTRASTE LCD	De 1 à 10 (plus clair)

Lorsque les réglages corrects vous conviennent, quittez le mode de configuration.

Étape 3 : vérification du schéma de câblage.

Figure 3. Coupleur de câble et identificateur de câble

La procédure suivante permet de tester chaque câble avec le coupleur et l'identificateur du réseau local, comme illustré à la figure 3. Le coupleur et l'identificateur de câble sont des accessoires fournis avec de nombreux câblomètres.

Insérez l'extrémité proche du câble dans la prise RJ-45 du testeur étiquetée UTP/FTP. Placez le coupleur femelle RJ45-RJ45 sur l'extrémité éloignée du câble, puis insérez l'identificateur de câble de l'autre côté du coupleur.

Le câblage de l'extrémité proche et éloignée du câble est affiché. Les nombres affichés dans le haut de l'écran LCD représentent l'extrémité proche, et ceux affichés dans le bas l'extrémité éloignée.

Exécutez le test de câblage de chaque câble fourni et remplissez le tableau suivant en fonction des résultats. Pour chaque câble, indiquez son numéro ainsi que sa couleur et si le câble est droit ou croisé.

n° de câble	Couleur de câble	Type de câble (direct ou de croisement)
1		
2		

Notez tout problème rencontré au cours du test :

Étape 4 : vérifier la longueur de câble.

Reportez-vous au manuel d'instructions pour placer le câblomètre en mode TEST. Si l'alimentation a été coupée puis rétablie, répétez les étapes de configuration à l'étape 2. La fonction LENGTH du testeur affiche la longueur du câble.

Exécutez un test de câblage de base et remplissez le tableau suivant en fonction des résultats. Pour chaque câble, indiquez son numéro et sa couleur, sa longueur, les résultats affichés sur l'écran du testeur et, en cas de problème, votre diagnostic.

Numéro de câble	Couleur de câble	Type de câble
1		
2		

Notez tout problème rencontré au cours du test :

Répétez ces étapes jusqu'à que vous maîtrisiez l'utilisation du testeur de câbles. Dans la tâche suivante, les câbles inconnus sont testés.

Tâche 2 : test des différents câbles à la recherche d'éventuels problèmes de compatibilité et de câblage.

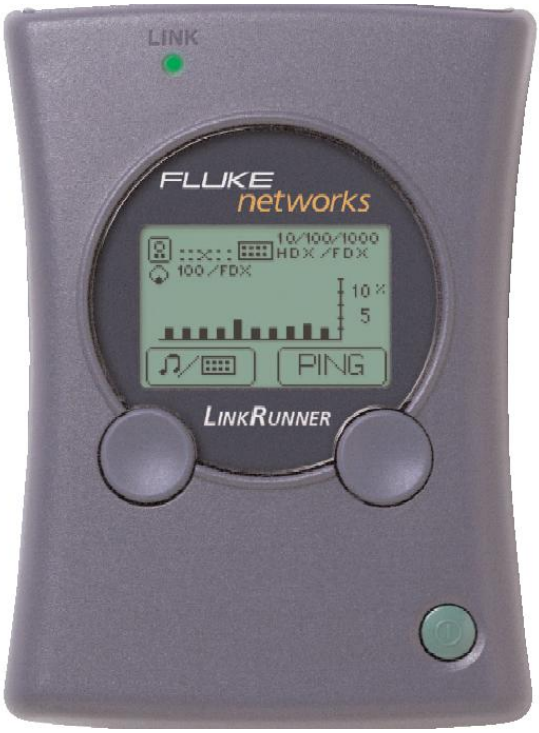
Procurez-vous au moins 5 câbles différents auprès du formateur. Tournez le sélecteur du testeur jusqu'à la position WIRE MAP. Si l'alimentation a été coupée puis rétablie, répétez les étapes de configuration décrites dans la tâche 1, à l'étape 2.

Reportez-vous aux instructions pour vérifier les différents câbles fournis à l'aide de la fonction WIRE MAP. Ensuite, remplissez le tableau suivant en fonction des résultats. Pour chaque câble, indiquez son numéro et sa couleur, si le câble est droit ou croisé, les résultats affichés sur l'écran du testeur et tout problème rencontré.

n° de câble	**Type de câble** (Inspection visuelle)	**Couleur du câble**	**Type de câble** (droit ou croisé)	*** Résultats du test**	**Description du problème**
1					
2					
3					
4					
5					

* Consultez le manuel relatif au produit pour plus de détails sur les résultats des tests de schéma de câblage.

Tâche 3 : configuration initiale du multimètre réseau



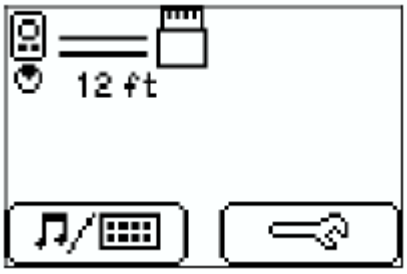
Multimètre réseau standard

Étape 1 : mise sous tension du multimètre réseau.

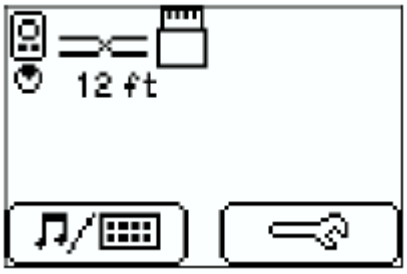
Étape 2 : mise hors tension.

Étape 3 : placement des deux extrémités du câble dans les ports LAN et MAP ou équivalents qui figurent en haut du multimètre réseau, puis mise sous tension.

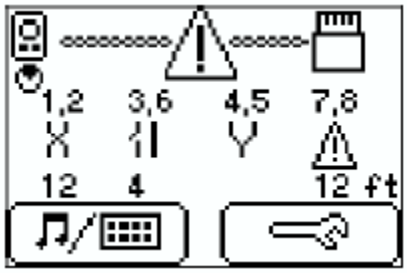
S'il s'agit d'un câble droit approprié, deux lignes parallèles (comme illustré ci-dessous) s'affichent en haut à gauche de l'écran. Reportez-vous aux instructions de fonctionnement si le multimètre n'affiche pas deux lignes parallèles dans cette étape et dans les suivantes.



S'il s'agit d'un câble croisé approprié, deux lignes qui se coupent (comme illustré ci-dessous) s'affichent en haut à gauche de l'écran.



S'il s'agit d'un câble non fonctionnel, ⚠ s'affiche et les détails figurent ci-dessous.



Open
Short
Split
Reversal
Unknown

Tâche 4 : vérification de la longueur de câble

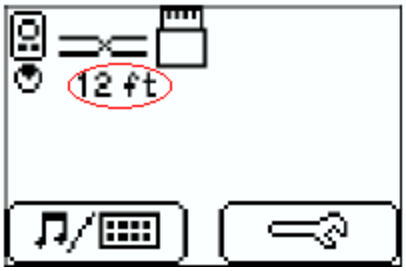
Remarque : les instructions pour tester un câble sont identiques à celles pour déterminer la longueur de câble.

Étape 1 : mise sous tension du multimètre réseau.

Étape 2 : mise hors tension.

Étape 3 : placement des deux extrémités du câble dans les ports LAN et MAP ou équivalents qui figurent en haut du multimètre réseau, puis mise sous tension.

Étape 4 : identification de la longueur de câble au-dessous de l'icône qui indique le type de câble (comme illustré ci-dessous).



Tâche 5 : Remarques générales

Les problèmes liés au câblage sont une des principales causes des pannes de réseau. Les techniciens réseau doivent être en mesure de déterminer le moment où utiliser les câbles droits et croisés UTP de catégorie 5.

Un testeur de câbles permet de déterminer le type et la longueur du câble ainsi que le schéma de câblage. Dans un environnement de travaux pratiques, les câbles sont constamment déplacés et reconnectés. Un câble qui est fonctionnel aujourd'hui est susceptible d'être endommagé demain. Ceci arrive souvent et fait partie du processus d'apprentissage.

Tâche 6 : confirmation

Recherchez les opportunités pour tester d'autres câbles avec le câblomètre. Les compétences acquises dans ces travaux pratiques permettent de dépanner rapidement les types de câbles incorrects ainsi que les câbles endommagés.

Tâche 7 : nettoyage

Le testeur de câbles est très coûteux et doit donc rester sous surveillance. Remettez le testeur de câbles au formateur une fois les travaux pratiques terminés.

Demandez-lui où retourner les câbles utilisés. Rangez soigneusement les câbles pour le cours suivant.

8.5.1 : exercice d'intégration des compétences : connexion des périphériques et exploration de la vue physique

Diagramme de topologie :

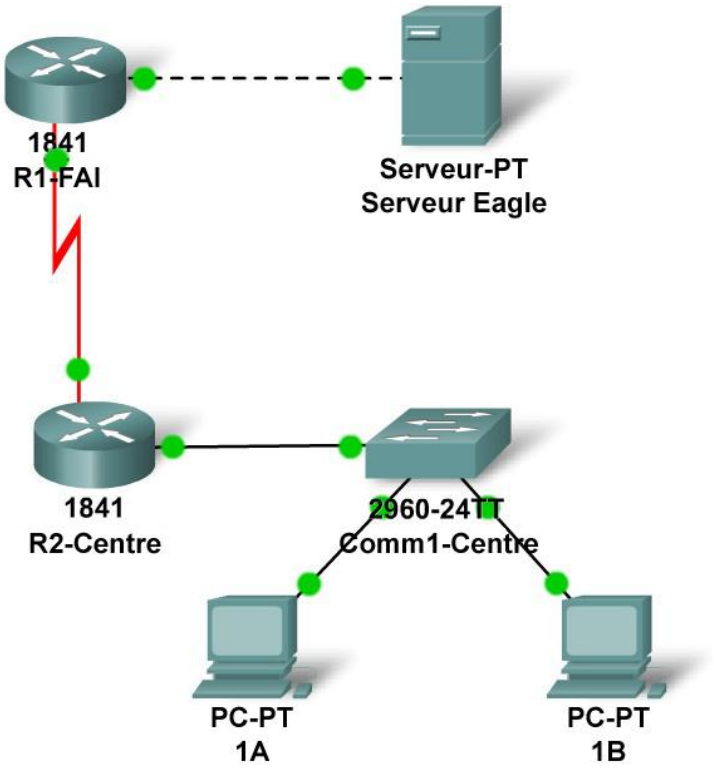


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	Fa0/0	192.168.254.253	255.255.255.0	N/A
	S0/0/0	10.10.10.6	255.255.255.252	N/A
R2-Central	Fa0/0	172.16.255.254	255.255.0.0	N/A
	S0/0/0	10.10.10.5	255.255.255.252	N/A
S1-Central	VLAN 1	172.16.254.1	255.255.0.0	172.16.255.254
PC 1A	La carte réseau	172.16.1.1	255.255.0.0	172.16.255.254
PC 1B	La carte réseau	172.16.1.2	255.255.0.0	172.16.255.254
Serveur Eagle	La carte réseau	192.168.254.254	255.255.255.0	192.168.254.253

Objectifs pédagogiques

- Connecter les périphériques inclus dans la configuration de travaux pratiques type
  - Connexion des périphériques
  - Vérification de la connectivité
- Visualiser la configuration de travaux pratiques type dans la zone Physical Workspace
  - Accès et visualisation de la zone Physical Workspace
  - Visualisation de la configuration de travaux pratiques type aux différents niveaux de la zone Physical Workspace

Présentation

Lorsque vous utilisez Packet Tracer, que ce soit dans un environnement de travaux pratiques ou dans un environnement d'entreprise, il est important de savoir comment choisir le câble adéquat et comment connecter correctement les périphériques. Au cours de cet exercice, vous allez examiner la configuration des périphériques dans Packet Tracer, sélectionner le câble adéquat en fonction de la configuration et connecter les périphériques. Enfin, vous explorerez la vue physique du réseau dans Packet Tracer.

Tâche 1 : connexion des périphériques inclus dans la configuration de travaux pratiques type

Étape 1 : connexion des périphériques

Connectez le PC 1A au premier port du commutateur S1-Central et le PC 1B au deuxième port de ce dernier en utilisant le câble adéquat.

Cliquez sur le routeur R2-Central et examinez-en la configuration sous l'onglet **Config**. Connectez l'interface appropriée du routeur à l'interface FastEthernet0/24 du commutateur S1-Central en utilisant le câble adéquat.

Cliquez sur les deux routeurs et examinez la configuration sous l'onglet **Config**. Connectez les routeurs ensemble en utilisant les interfaces et le câble adéquats.

Cliquez sur le routeur R1-ISP et examinez-en la configuration sous l'onglet **Config**. Connectez l'interface appropriée du routeur à l'interface appropriée du serveur Eagle Server en utilisant le câble adéquat.

Étape 2 : vérification de la connectivité

Ã€ partir de l'**Invite de commande** du **Bureau** des deux PC, émettez la commande **ping 192.168.254.254** (adresse IP du serveur Eagle Server). Si les commandes ping échouent, vérifiez vos connexions et dépannez jusqu'à ce que les commandes ping aboutissent. Vérifiez votre configuration en cliquant sur le bouton **Check Results**.

Tâche 2 : visualisation de la configuration de travaux pratiques type dans la zone Physical Workspace

Étape 1 : accès et visualisation de la zone Physical Workspace

La plupart des tâches que nous avons effectuées dans Packet Tracer l'ont été dans la zone Logical Workspace. Dans un interréseau, les routeurs peuvent se trouver sur différents sites, de l'autre côté de la rue voire à l'autre bout de la planète. La liaison série entre les routeurs représente une ligne spécialisée louée entre deux emplacements, constituée d'un équipement terminal de traitement de données (ETTD), tel qu'un routeur, qui est connecté à un équipement de communication de données (ETCD), tel qu'une unité CSU/DSU ou un modem. L'ETCD se connecte à la boucle locale d'un fournisseur services et les connexions sont répétées à l'autre extrémité de la liaison. La zone Physical Workspace vous permet de mieux identifier les relations.

Pour accéder à la zone Physical Workspace, cliquez sur l'onglet situé dans l'angle supérieur gauche de la zone Workspace. Elle présente la connexion entre Central City et ISP City.

Étape 2 : visualisation de la configuration de travaux pratiques type aux différents niveaux de la zone Physical Workspace

Cliquez sur Central City pour afficher la ville et l'emplacement du bâtiment Central Office. Cliquez sur le bâtiment Central Office pour obtenir le plan d'étage du bâtiment et l'emplacement de l'armoire de répartition (Wiring Closet). Cliquez sur Wiring Closet pour obtenir une représentation physique de l'équipement installé dans l'armoire de répartition et du câblage reliant l'équipement. Examinez cette vue de la topologie.

Cliquez sur **Intercity** dans la barre **Navigation**. Répétez les étapes pour visualiser l'équipement installé dans la ville du fournisseur de services Internet (ISP City).

Travaux pratiques 9.8.1 : protocole ARP (Address Resolution Protocol)

Schéma de la topologie

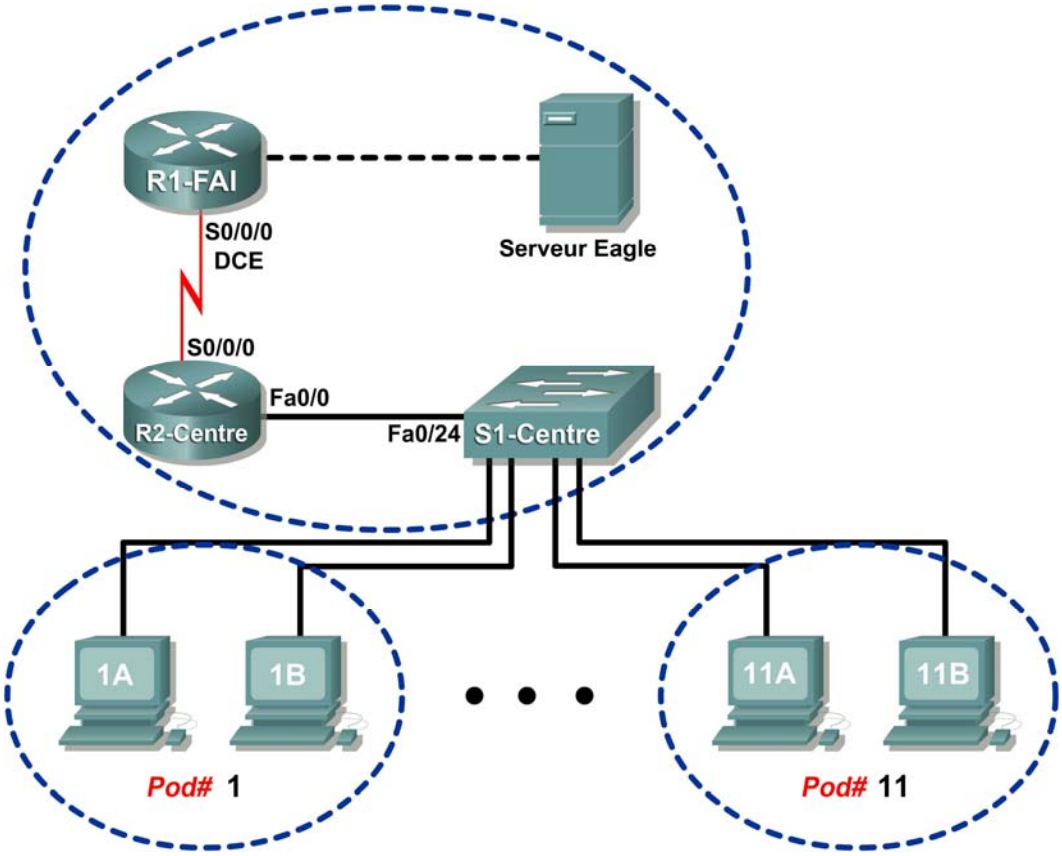


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/D
	Fa0/0	192.168.254.253	255.255.255.0	N/D
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/D
	Fa0/0	172.16.255.254	255.255.0.0	N/D
Eagle Server	N/D	192.168.254.254	255.255.255.0	192.168.254.253
	N/D	172.31.24.254	255.255.255.0	N/D
hôte*Pod#*A	N/D	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
hôte*Pod#*B	N/D	172.16. *Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	N/D	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- utiliser la commande **arp** de Windows ;
- utiliser Wireshark pour examiner les échanges de ARP.

Contexte

Le protocole ARP (Address Resolution Protocol) est utilisé par TCP/IP pour mapper une adresse IP de couche 3 à une adresse MAC de couche 2. Lorsqu'une trame est placée sur le réseau, elle doit posséder une adresse MAC de destination. Pour détecter de façon dynamique l'adresse MAC d'un périphérique de destination, une requête ARP est diffusée sur le réseau local. Le périphérique qui contient l'adresse IP de destination répond. Ensuite, l'adresse MAC est consignée dans le cache ARP. Chaque périphérique sur le réseau local conserve son propre cache ARP, ou un petit espace dans la mémoire vive qui contient les résultats d'ARP. Un temporisateur de cache ARP supprime les entrées correspondantes qui n'ont pas été utilisées pendant un certain temps. Les délais diffèrent selon le périphérique utilisé. Par exemple, certains systèmes d'exploitation Windows stockent les entrées de cache ARP pendant 2 minutes. Si l'entrée est de nouveau utilisée au cours de ce délai, le temporisateur ARP de cette entrée est prolongé de 10 minutes.

ARP constitue un parfait exemple de compromis de performances. Sans cache, ARM doit constamment demander des traductions d'adresses à chaque placement d'une trame sur le réseau. Ceci ajoute de la latence à la communication et peut encombrer le réseau local. Inversement, des temps d'attente illimités peuvent entraîner des erreurs avec des périphériques qui quittent le réseau ou modifient l'adresse de couche 3.

Un ingénieur réseau doit tenir compte d'ARP, mais ne peut pas communiquer régulièrement avec ce protocole. ARP est un protocole qui permet aux périphériques réseau de communiquer avec le protocole TCP/IP. Sans ARP, aucune méthode n'est efficace pour créer l'adresse de destination de couche 2 du datagramme. En outre, ARP représente un risque potentiel pour la sécurité. L'usurpation ARP ou l'empoisonnement ARP est une technique utilisée par un pirate informatique pour introduire l'association d'adresses MAC incorrectes dans un réseau. Un pirate informatique usurpe l'adresse MAC d'un périphérique, et les trames sont envoyées vers la destination incorrecte. La configuration manuelle d'associations ARP statiques est un moyen d'éviter l'usurpation ARP. En fin de compte, il est possible de configurer une liste d'adresses MAC autorisées pour limiter l'accès réseau aux seuls périphériques approuvés.

Scénario

Avec un ordinateur hôte pod, utilisez la commande de l'utilitaire **arp** de Windows pour examiner et modifier les entrées du cache ARP.

Dans la tâche 2, Wireshark permet de capturer et d'analyser les échanges ARP entre les périphériques réseau. Si vous n'avez pas effectué le téléchargement de Wireshark sur l'ordinateur hôte pod, utilisez l'adresse URL `ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter9/`, fichier `wireshark-setup-0.99.4.exe`.

Tâche 1 : utilisation de la commande **arp** de Windows.

Étape 1 : accès au terminal de Windows.

```
C:\> arp
Affiche et modifie les tables de conversion d'adresses IP en adresses
physiques utilisées par le protocole ARP.
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
-a          Affiche les entrées ARP actuelles en interrogeant les
            données de protocole actuelles. Si inet_addr est spécifié,
            seules les adresses IP et physique de l'ordinateur spécifié
            s'affichent. Si plusieurs interfaces réseau utilisent ARP,
            les entrées de chaque table ARP s'affichent.
-g          Identique à -a.
inet_addr   Spécifie une adresse Internet.
-N if_addr  Affiche les entrées ARP de l'interface réseau spécifiée par
            if_addr.
-d          Supprime l'hôte spécifié par inet_addr. inet_addr peut
            s'utiliser avec le caractère générique * pour supprimer
            tous les hôtes.
-s          Ajoute l'hôte et associe l'adresse Internet inet_addr à
            l'adresse physique eth_addr.  L'adresse physique est
            fournie sous forme de 6 octets hexadécimaux séparés par des
            traits d'union. L'entrée est permanente.
eth_addr    Spécifie une adresse physique.
if_addr     Si présent, spécifie l'adresse Internet de l'interface dont
            la table de conversion des adresses doit être modifiée. Si
            absent, la première interface applicable est utilisée.
Exemple :
 > arp -s 157.55.85.212 00-aa-00-62-c6-09  .... Ajoute une entrée
statique.
 > arp -a                                  .... Affiche la table arp.
C:\>
```

Figure 1. Syntaxe de la commande arp

1. Ouvrez une fenêtre de ligne de commande en cliquant sur **Démarrer > Exécuter**. Tapez **cmd**, puis cliquez sur **OK**.
   Sans options, la commande **arp** affiche des informations d'aide utiles. Reportez-vous à la figure 1.
2. Exécutez la commande **arp** sur l'ordinateur hôte pod, et examinez les résultats.
3. Répondez aux questions suivantes sur la commande **arp** :

   Quelle commande est utilisée pour afficher toutes les entrées dans le cache ARP ?

   _____

   Quelle commande est utilisée pour supprimer toutes les entrées du cache ARP (vider le cache ARP) ?

   _____

Quelle commande est utilisée pour supprimer l'entrée du cache ARP pour 172.16.255.254 ?

_____

Étape 2 : utilisation de la commande `arp` pour examiner le cache ARP local.

```
C:\> arp -a
Aucune entrée ARP trouvée
C:\>
```

Figure 2. Cache ARP vide

Sans communication réseau, le cache ARP doit être vide. Ceci est illustré dans la figure 2.

Exécutez la commande qui affiche les entrées ARP. Quels sont les résultats ?

_____

_____

Étape 3 : utilisation de la commande `ping` pour ajouter de façon dynamique des entrées dans le cache ARP.

La commande **`ping`** sert à tester la connectivité réseau. En accédant à d'autres périphériques, les associations ARP sont ajoutées de façon dynamique au cache ARP.

```
C:\> ping 172.16.1.2
Envoi d'une requête sur 172.16.1.2 avec 32 octets de
données :
Réponse de 172.16.1.2 : octets=32 temps<1 ms TTL=128
Réponse de 172.16.1.2 : octets=32 temps<1 ms TTL=128
Réponse de 172.16.1.2 : octets=32 temps<1 ms TTL=128
Réponse de 172.16.1.2 : octets=32 temps<1 ms TTL=128
Statistiques Ping pour 172.16.1.2 :
    Paquets : Envoyés = 4, Reçus = 4, Perdus = 0 (perte
0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms
C:\>
```

Figure 3. Commande `ping` vers un ordinateur hôte pod

1. Utilisez la commande **`ipconfig /all`** pour vérifier les données de la couche 2 et couche 3 de l'ordinateur hôte pod.
2. Exécutez la commande **`ping`** vers un autre ordinateur hôte, illustré à la figure 3. La figure 4 illustre la nouvelle entrée du cache ARP.

```
C:\> arp -a
Interface : 172.16.1.1 --- 0x60004
  Adresse Internet      Adresse physique      Type
  172.16.1.2            00-10-a4-7b-01-5f
dynamique
C:\>
```

Figure 4. Affichage du cache ARP

Comment l'entrée ARP a-t-elle été ajoutée au cache ARP ? Conseil : consultez la colonne Type.

_____

Quelle est l'adresse physique de l'ordinateur hôte pod de destination ?

_____

Quelle est l'adresse physique de l'ordinateur hôte pod de destination ?

Adresse IP	Adresse physique	Mode de détection ?

3. N'envoyez pas de trafic vers l'ordinateur auquel l'accès a eu lieu auparavant. Attendez 2 à 3 minutes, et vérifiez à nouveau le cache ARP. L'entrée du cache ARP a-t-elle été effacée ?

   _____

4. Exécutez la commande **ping** vers la passerelle, R2-Central. Examinez l'entrée du cache ARP. Quelle est l'adresse physique de la passerelle ? _____

Adresse IP	Adresse physique	Mode de détection ?

5. Exécutez la commande **ping** vers Eagle Server, eagle-server.example.com. Examinez l'entrée du cache ARP. Quelle est l'adresse physique d'Eagle Server ?

   _____

   _____

   _____

Étape 4 : modification manuelle des entrées dans le cache ARP.

Pour supprimer des entrées dans un cache ARP, exécutez la commande **arp –d {inet-addr | *}**. Il est possible de supprimer les adresses individuellement en indiquant l'adresse IP. Vous pouvez aussi supprimer toutes les entrées avec le caractère générique *****.

Vérifiez que le cache ARP contient deux entrées : une pour la passerelle et une pour l'ordinateur hôte pod de destination. L'exécution d'une commande ping vers les deux périphériques plusieurs fois peut s'avérer plus simple. Ce qui permet de conserver l'entrée du cache pendant environ 10 minutes.

```
C:\> arp –a
Interface : 172.16.1.1 --- 0x60004
  Adresse Internet      Adresse physique      Type
  172.16.1.2            00-10-a4-7b-01-5f     dynamique
  172.16.255.254        00-0c-85-cf-66-40     dynamique
C:\>
C:\>arp -d 172.16.255.254
C:\> arp -a
Interface : 172.16.1.1 --- 0x60004
  Adresse Internet      Adresse physique      Type
  172.16.1.2            00-10-a4-7b-01-5f     dynamique
C:\>
```

Figure 5. Suppression manuelle d'une entrée de cache ARP

Reportez-vous à la figure 5, qui illustre la méthode de suppression manuelle d'une entrée de cache ARP.

1. Sur votre ordinateur, vérifiez d'abord que les deux entrées sont disponibles. Sinon, exécutez une requête ping vers l'entrée manquante.
2. Ensuite, supprimez l'entrée pour l'ordinateur hôte pod.
3. Finalement, vérifiez vos modifications.
4. Consignez les deux entrées du cache ARP.

Périphérique	Adresse IP	Adresse physique	Mode de détection ?

5. Indiquez la commande qui permet de supprimer l'entrée pour l'ordinateur hôte pod :
   _____
6. Exécutez la commande sur l'ordinateur hôte pod. Consignez l'entrée restante du cache ARP :

Périphérique	Adresse IP	Adresse physique	Mode de détection ?

7. Simulez la suppression de toutes les entrées. Indiquez la commande qui permet de supprimer toutes les entrées dans le cache ARP :
   _____
8. Exécutez la commande sur votre ordinateur hôte pod, et examinez le cache ARP avec la commande **`arp -a`**. Toutes les autres entrées doivent être supprimées. __ _____
9. Prenez par exemple un environnement sécurisé où la passerelle contrôle l'accès à un serveur Web qui contient des informations classées « top secret ». Qu'est-ce qu'une couche de sécurité qui peut être appliquée à des entrées du cache ARP, qui peuvent aider à neutraliser l'usurpation ARP ? _____
10. Indiquez la commande qui ajoute une entrée ARP statique au cache ARP pour la passerelle :
    _____
11. Examinez à nouveau le cache ARP, et renseignez le tableau suivant :

Adresse IP	Adresse physique	Type

Pour la tâche suivante, Wireshark est utilisé pour capturer et examiner un échange ARP. Ne fermez pas le terminal Windows. Il sera utilisé pour afficher le cache ARP.

Tâche 2 : utilisation de Wireshark pour examiner les échanges de ARP.

Étape 1 : configuration de Wireshark pour les captures de paquets.

Préparez Wireshark pour les captures.

1. Cliquez sur **Capture > Options**.
2. Sélectionnez l'interface qui correspond au réseau local.
3. Cochez la case pour mettre à jour la liste de paquets en temps réel.
4. Cliquez sur **Démarrer**.

Ceci permet de commencer la capture des paquets.

Étape 2 : préparation de l'ordinateur hôte pod aux captures ARP.

1. Si ce n'est pas déjà fait, ouvrez une fenêtre de terminal Windows en cliquant sur **Démarrer > Exécuter**. Tapez **cmd**, puis cliquez sur **OK**.
2. Videz le cache ARP, qui requiert qu'ARP détecte à nouveau les mappages d'adresses. Indiquez la commande que vous avez utilisée : _____
3. Étape 3 : capture et évaluation de la communication ARP.

Dans cette étape, une requête ping est envoyée à la passerelle, et l'autre à Eagle Server. Ensuite, la capture Wireshark est stoppée et la communication ARP évaluée.

1. Envoyez une requête ping à la passerelle, à l'aide de la commande

   `ping –n 1 172.16.255.254.`.

2. Envoyez une requête ping à Eagle Server, à l'aide de la commande

   `ping –n 1 192.168.254.254`.

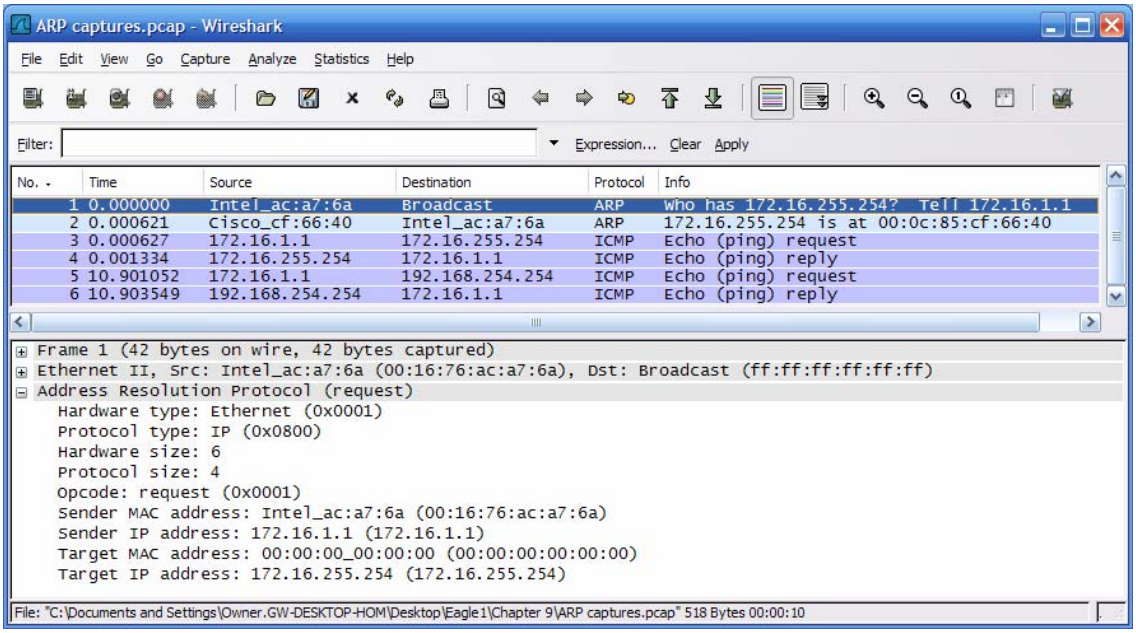


Figure 6. Capture Wireshark d'une communication ARP

3. Arrêtez Wireshark et évaluez la communication. Un écran Wireshark semblable à celui illustré à la figure 6 doit s'afficher. La fenêtre Packet list de Wireshark affiche le nombre de paquets capturés. La fenêtre Packet Details affiche le contenu du protocole ARP.
4. À l'aide de votre capture Wireshark, répondez aux questions suivantes :

   Quel était le premier paquet ARP ? _____

   Quel était le deuxième paquet ARP ? _____

   Renseignez le tableau suivant avec les informations sur le premier paquet ARP :

Champ	Valeur
Adresse MAC de l'expéditeur	
Adresse IP de l'expéditeur	
Adresse MAC cible	
Adresse IP cible	

Renseignez le tableau suivant avec les informations sur le deuxième paquet ARP :

Champ	Valeur
Adresse MAC de l'expéditeur	
Adresse IP de l'expéditeur	
Adresse MAC cible	
Adresse IP cible	

Si la trame Ethernet II pour une requête ARP est une diffusion, pourquoi l'adresse MAC cible ne contient que des **0** ? _____

Pourquoi n'y avait-t-il pas de requête ARP pour la commande ping envoyée à Eagle Server ?
_____

_____

_____

Combien de temps le mappage de la passerelle doit-il être stocké dans le cache ARP de l'ordinateur hôte pod ? Pourquoi ?

_____

_____

Tâche 3 : Remarques générales

Le protocole ARP mappe les adresses IP de couche 3 aux adresses MAC de couche 2. Si un paquet doit parcourir des réseaux, l'adresse MAC de couche 2 change avec chaque saut sur un routeur. Cependant, l'adresse de couche 3 reste la même.

Le cache ARP stocke les mappages d'adresses d'ARP. Si l'entrée a été étudiée de façon dynamique, elle est supprimée du cache. Si elle a été manuellement insérée dans le cache ARP, il s'agit d'une entrée statique. Ainsi, elle reste disponible jusqu'à la mise hors tension de l'ordinateur ou le vidage manuel du cache ARP.

Tâche 4 : confirmation

À l'aide des ressources externes, effectuez une recherche sur l'usurpation ARP. Abordez les différentes techniques pour neutraliser ce type d'attaque.

La majorité des routeurs sans fil prennent en charge l'accès au réseau sans fil. À l'aide de cette technique, les adresses MAC qui disposent de l'accès au réseau sans fil sont ajoutées manuellement au routeur sans fil. À l'aide des ressources externes, abordez les avantages de la configuration de l'accès au réseau sans fil. Discutez des moyens dont disposent les pirates informatiques pour contourner cette sécurité.

Tâche 5 : nettoyage

Wireshark a été installé sur l'ordinateur hôte pod. Si Wireshark doit être désinstallé, cliquez sur **Démarrer > Panneau de configuration**. Ouvrez **Ajout/Suppression de programmes**. Sélectionnez Wireshark, puis cliquez sur **Supprimer**.

Supprimez tout fichier créé sur l'ordinateur hôte pod au cours des travaux pratiques.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

Travaux pratiques 9.8.2 : examen de la table MAC du commutateur Cisco

Schéma de la topologie

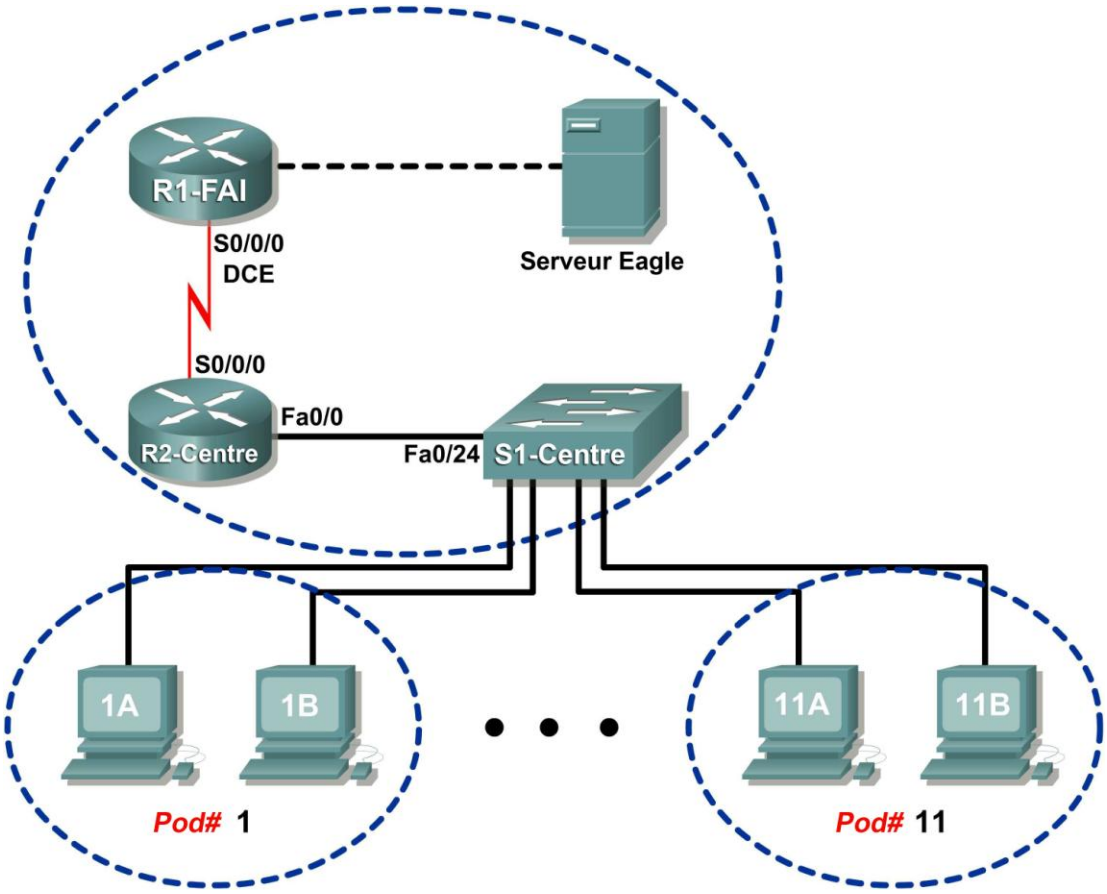


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/D
	Fa0/0	192.168.254.253	255.255.255.0	N/D
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/D
	Fa0/0	172.16.255.254	255.255.0.0	N/D
Eagle Server	N/D	192.168.254.254	255.255.255.0	192.168.254.253
	N/D	172.31.24.254	255.255.255.0	N/D
hôte*Pod#*A	N/D	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
hôte*Pod#*B	N/D	172.16. *Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	N/D	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- utiliser le protocole Telnet pour la connexion à un commutateur Cisco ;
- utiliser la commande **show mac-address-table** de Cisco IOS pour examiner les adresses MAC et les associations de ports.

Contexte

Les commutateurs permettent de conserver une table d'adresses MAC et le port de commutateur associé. Lorsqu'un commutateur reçoit une trame, l'adresse MAC de destination est vérifiée dans la table. Ensuite, le port correspondant permet de router la trame hors du commutateur. Si un commutateur ne connaît pas le port de routage de la trame ou que cette dernière est une diffusion, elle est routée en dehors de tous les ports sauf celui d'où elle provient.

Plusieurs méthodes permettent l'accès aux périphériques Cisco. Vous pouvez utiliser un port de console si le routeur ou le commutateur Cisco figure dans la même proximité physique d'un ordinateur. À l'aide de l'utilitaire hyperterm de Windows, vous pouvez établir une connexion série. Pour les périphériques à distance de l'ingénieur réseau, vous pouvez établir la connectivité réseau à l'aide de deux méthodes. Si le réseau n'est pas sécurisé, un modem configuré sur le port AUX permet l'accès téléphonique. Sinon, vous pouvez configurer le périphérique Cisco pour une session Telnet. Dans ces travaux pratiques, le participant se connecte au commutateur via une session Telnet.

Travaux pratiques

- Établir une connexion Telnet avec S1-Central.
- Se connecter avec le compte de participant.
- Utiliser la commande **show mac-address-table** pour examiner les adresses MAC et l'association aux ports.

Scénario

Utilisez la commande **show mac-address-table** pour examiner la table d'adresses Mac du commutateur et d'autres informations reliées aux adresses.

Telnet est un réseau qui utilise un modèle client-serveur. Les périphériques Cisco IOS offrent un serveur Telnet par défaut. En outre, les systèmes d'exploitation tels que Windows possèdent des clients Telnet intégrés. À l'aide de Telnet, les ingénieurs réseau peuvent se connecter aux périphériques réseau à partir d'un point quelconque sur un réseau sécurisé. Vous devez configurer le périphérique Cisco pour l'accès Telnet. Sinon, il est refusé. Dans Eagle 1, des privilèges limités ont été configurés pour le participant.

Tâche 1 : utilisation du protocole Telnet pour la connexion à un commutateur Cisco.

Étape 1 : accès à la fenêtre de ligne de commande Windows.

Ouvrez une fenêtre de ligne de commande en cliquant sur **Démarrer > Exécuter**. Tapez **cmd**, puis cliquez sur **OK**.

Étape 2 : utilisation du client Telnet de Windows pour accéder à S1-Central.

S1-Central a été configuré avec 11 comptes de participants, `ccna1` à `ccna11`. Pour fournir l'accès à chaque participant, utilisez l'ID d'utilisateur qui correspond à votre pod. Par exemple, utilisez `ccna1` pour les ordinateurs hôtes sur pod 1. Sauf indication contraire de votre formateur, le mot de passe est `cisco`.

1. Dans le terminal Windows, exécutez la commande Telnet, **telnet** *destination-ip-address* :

   C:/> **telnet 172.16.254.1**

   Une demande d'accès est affichée, semblable à celle illustrée à la figure 1.

```
**********************************************************************
                Ceci est le commutateur de travaux pratiques S1-
                Central.
                Accès autorisé uniquement.
**********************************************************************
Contrôle de l'accès de l'utilisateur
Nom d'utilisateur : ccna1
Mot de passe : cisco  (*masqué*)
S1-Central#
```

Figure 1. Client Telnet

2. Indiquez le nom d'utilisateur applicable. Lorsque la demande de mot de passe s'affiche, tapez `cisco <ENTER>`.

   L'invite de `S1-Central#` doit s'afficher.

Tâche 2 : utilisation de la commande `show mac-address-table` de Cisco IOS pour examiner les adresses MAC et les associations de ports.

Étape 1 : examen de la table d'adresses MAC du commutateur.

1. Exécutez la commande **`show mac-address-table ? <ENTRÉE>`**. Ceci permet de générer toutes les options pour la commande.
2. Utilisez le tableau suivant pour renseigner les options de commande.

Option	Description

Étape 2 : examen des entrées dynamiques de la table d'adresses MAC

1. Exécutez la commande **`show mac-address-table`**.
   Cette commande affichera des entrées statiques (unité centrale) et dynamiques, ou acquises.

2. Répertoriez les adresses MAC et les ports de commutateurs correspondants :

Adresse MAC	Port de commutation

Supposez qu'il y ait un concentrateur avec cinq hôtes actifs connectés au port commutateur `gi0/0`. Combien d'adresses MAC sont répertoriées pour le port de commutateur `gi0/0` ?

_____

Étape 3 : examen du délai d'expiration de la table d'adresses MAC.

1. Exécutez la commande **`show mac-address-table aging-time`**.
   Cette commande permet d'afficher l'heure par défaut, en secondes, à laquelle les entrées d'adresses MAC sont stockées.
2. Quel est le délai d'expiration par défaut pour VLAN 1 ? _____

Tâche 3 : confirmation

Quels sont les résultats si les entrées dynamiques sont supprimées de la table d'adresses MAC ?

_____

_____

Tâche 4 : Remarques générales

À l'aide du protocole Telnet, les ingénieurs réseau peuvent accéder aux périphériques Cisco à distance sur des réseaux locaux sécurisés. Ceci a l'avantage de permettre l'accès à des périphériques distants à des fins de dépannage et de surveillance.

Un commutateur contient une table d'adresses MAC qui répertorie l'adresse MAC connectée à chaque port de commutateur. Lorsqu'une trame entre dans le commutateur, ce dernier effectue une recherche de l'adresse MAC de destination de la trame. En l'absence de correspondance dans la table d'adresses MAC, la trame est routée en dehors du port associé. Sans table d'adresses MAC, le commutateur doit inonder la trame hors de chaque port.

Tâche 5 : nettoyage

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

Travaux pratiques 9.8.3 : périphérique intermédiaire en tant que périphérique final

Diagramme de topologie

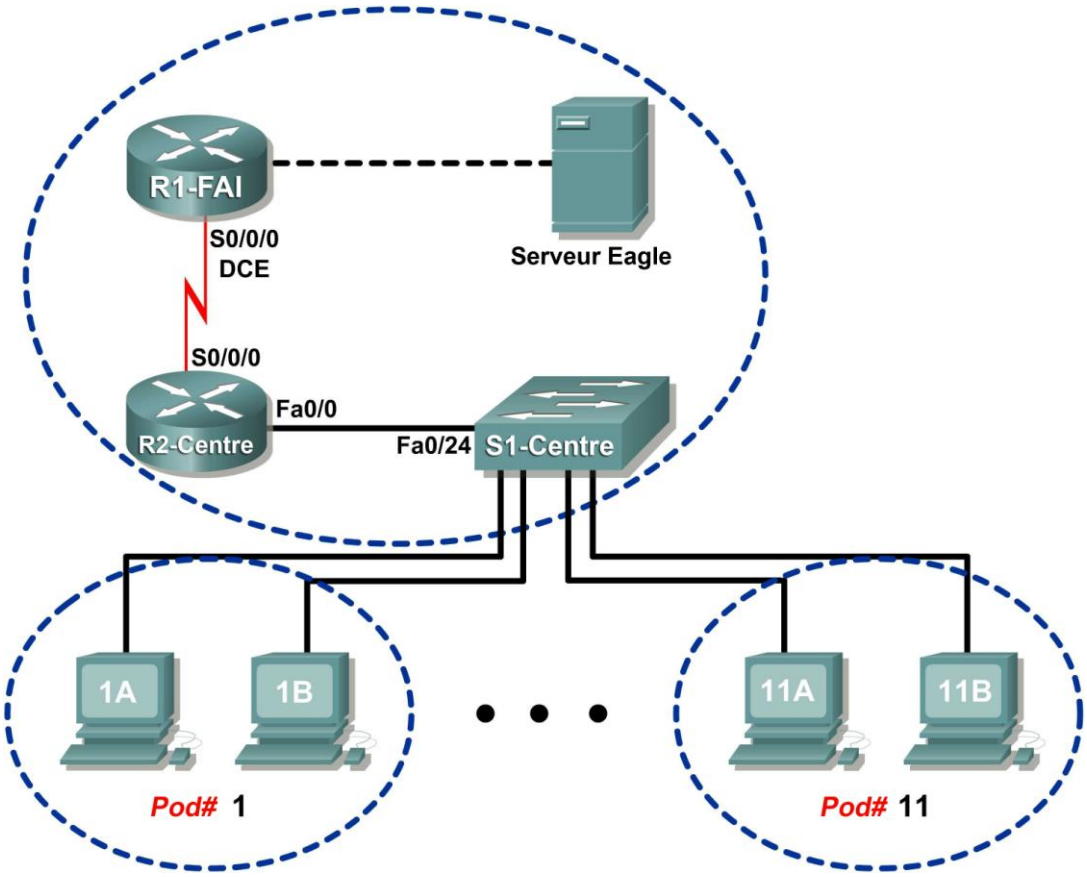


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0:	10.10.10.6	255.255.255.252	s/o
	Fa0/0	192.168.254.253	255.255.255.0	s/o
R2-Central	S0/0:	10.10.10.5	255.255.255.252	s/o
	Fa0/0	172.16.255.254	255.255.0.0	s/o
Serveur Eagle	s/o	192.168.254.254	255.255.255.0	192.168.254.253
	s/o	172.31.24.254	255.255.255.0	s/o
hôte*Pod n°***A**	s/o	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
hôte*Pod n°***B**	s/o	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	s/o	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Utiliser Wireshark pour capturer et analyser des trames provenant de nœuds réseau
- Examiner la provenance des trames dans un petit réseau

Contexte

Un commutateur permet de router des trames entre les périphériques réseau. En général, un commutateur n'est pas à l'origine de la trame transférée aux périphériques réseau. Il transmet plutôt efficacement la trame d'un périphérique à l'autre dans le réseau local.

Scénario

Wireshark permet de capturer et d'analyser les trames Ethernet. Si vous n'avez pas effectué le téléchargement de Wireshark sur l'ordinateur hôte pod, utilisez l'adresse URL ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter9/, fichier `wireshark-setup-0.99.4.exe`.

Dans ces travaux pratiques, vous allez envoyer une requête ping vers l'ordinateur hôte pod du voisin.

Inscrivez l'adresse IP et la connexion du port sur S1-Central pour l'ordinateur hôte pod du voisin.

Adresse IP : _____ Numéro de port de S1-Central : _____

Tâche 1 : utilisation de Wireshark pour capturer et analyser des trames provenant de nœuds réseau

Étape 1 : configuration de Wireshark pour les captures de paquets

Configurez Wireshark.

1. Cliquez sur **Capture > Options**.
2. Sélectionnez l'interface qui correspond au LAN.
3. Cochez la case pour mettre à jour la liste de paquets en temps réel.
4. Cliquez sur **Démarrer**.

Ceci permet de commencer la capture des paquets. Plus de 200 captures vont être probablement effectuées, ce qui rend l'analyse un peu fastidieuse. La communication Telnet entre l'ordinateur hôte pod et S1-Central est facile à filtrer.

Étape 2 : utilisation du client Telnet de Windows pour accéder à S1-Central

S1-Central a été configuré avec 11 comptes de participants, `ccna1` à `ccna11`. Pour fournir l'accès à chaque participant, utilisez l'ID d'utilisateur qui correspond à votre pod. Par exemple, utilisez `ccna1` pour les ordinateurs hôtes sur pod 1. Sauf indication contraire de votre formateur, le mot de passe est `cisco`.

1. Dans le terminal Windows, exécutez la commande **`telnet`** *`adresse IP de destination`*:

   C:/> **`telnet 172.16.254.1`**

2. Indiquez le nom d'utilisateur et le mot de passe appropriés (**`cisco`**).
   L'invite de S1-Central doit être retournée, `S1-Central#`.

Étape 3 : effacement de la table d'adresses MAC

1. Examinez la table d'adresses MAC du commutateur avec la commande **`show mac-address-table`**. Outre plusieurs entrées UC statiques, les entrées dynamiques de la table d'adresses doivent être nombreuses.
2. Pour effacer les entrées dynamiques de la table d'adresses MAC, utilisez la commande **`clear mac-address-table dynamic`**.
3. Répertoriez les entrées dynamiques de l'adresse MAC :

Adresse MAC	Port de commutation

4. Ouvrez une deuxième fenêtre de terminal. Envoyez une requête ping à l'adresse IP de votre voisin, qui a été consignée auparavant.

   C:>\ **ping –n 1** *adresse IP*

5. L'adresse MAC de cet ordinateur doit être ajoutée de façon dynamique dans la table d'adresses MAC de S1-Central
6. Répertoriez à nouveau les entrées dynamiques de l'adresse MAC :

Adresse MAC	Port de commutation

   Quelle conclusion peut-on tirer de la manière dont un commutateur obtient des informations sur les adresses MAC associées aux interfaces du commutateur ?

   _____

   _____

7. Fermez la capture Wireshark.

   La capture est analysée à l'étape suivante.

Tâche 2 : analyse de la provenance des trames dans un petit réseau

Étape 1 : analyse d'une session Telnet avec S1-Central

1. Sélectionnez l'un des paquets de la session Telnet. Dans le menu Wireshark, cliquez sur **Analyze | Follow TCP Stream**. Une fenêtre de contenu du flux affiche du texte ASCII par défaut. Si le nom d'utilisateur et le mot de passe ne sont pas visibles, basculez vers HEX Dump.
2. Vérifiez le nom d'utilisateur et le mot de passe saisis.
   Nom d'utilisateur : _____ Mot de passe : _____
3. Fermez la fenêtre du contenu du flux.

Étape 2 : analyse les résultats de la commande `show mac-address-table`

1. Ouvrez le Bloc-notes. Les données capturées sont transférées vers Bloc-notes pour l'analyse. Il se peut qu'il y ait de nombreux paquets capturés.
2. Dans le volet Packet List supérieur de Wireshark, faites défiler la liste vers le bas jusqu'à la requête ICMP capturée. Si la fenêtre Packet Byte inférieure de Wireshark n'est pas visible, cliquez sur **View > Packet bytes**.

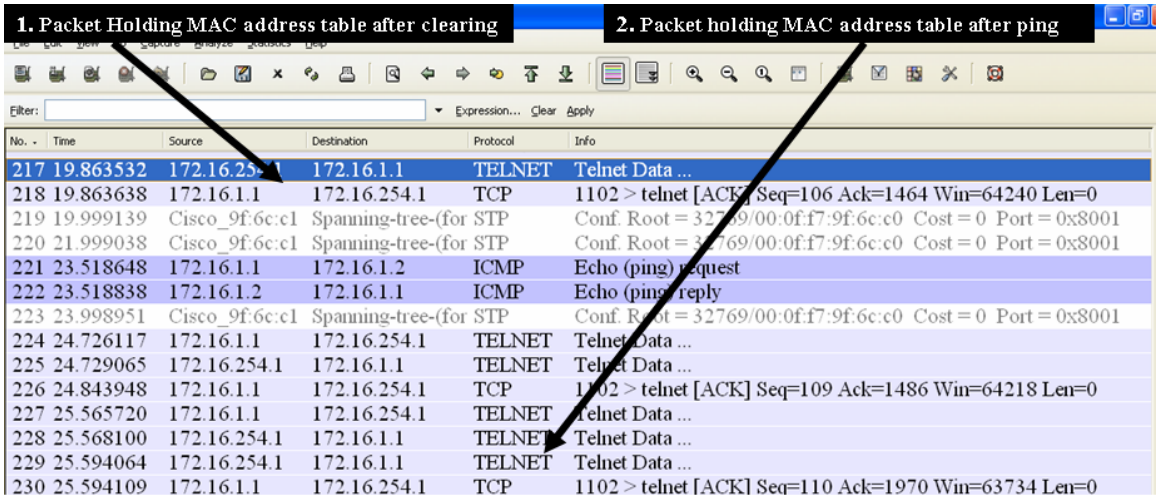


Figure 1. Capture Wireshark de Telnet

Reportez-vous à la figure 1, les résultats partiels de la capture Wireshark :

1 Sélectionnez le dernier paquet de données Telnet provenant de S1-Central avant la commande **`ping`**. Ensuite, sélectionnez l'octet de paquet correspondant. Cliquez avec le bouton droit sur l'octet de paquet et cliquez sur **Copier > Texte seulement**. Dans Bloc-notes, cliquez sur **Édition > Coller**. Les mappages dynamiques doivent être semblables aux résultats suivants :

```
{_lEMaNL;RPC          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000f.f79f.6cc0    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0010.a47b.015f    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 5
S1-Central#
```

3. Notez l'adresse MAC et le numéro de port affichés dans les résultats. Le port du commutateur correspond-il à votre ordinateur hôte pod ? _____

Adresse MAC	Type	Port

Pourquoi le mappage de l'ordinateur hôte pod figure-t-il encore dans la table d'adresses MAC, même après avoir été supprimé ?

_____

_____

2 Sélectionnez le dernier paquet de données Telnet immédiatement après la réponse ping. Ensuite, sélectionnez l'octet de paquet correspondant. Cliquez avec le bouton droit sur l'octet de paquet et cliquez sur **Copier > Texte seulement**. Dans Bloc-notes, cliquez sur **Édition > Coller**. Le texte doit être semblable à l'opération Coller suivante :

```
{_lEPaNM;VP          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000f.f79f.6cc0    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0010.a47b.015f    DYNAMIC     Fa0/1
   1    0016.76ac.a76a    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 6
S1-Central#
```

4. Notez l'adresse MAC et le numéro de port pour le deuxième type dynamique affiché dans les résultats. Le port du commutateur correspond-il à l'ordinateur hôte pod de votre voisin ? _____

Adresse MAC	Type	Port

Tâche 3 : remarques générales

La capture Wireshark d'une session Telnet entre un ordinateur hôte pod et S1-Central a été analysée pour indiquer la manière dont un commutateur obtient des informations dynamiques sur les nœuds auxquels il est directement connecté.

Tâche 4 : confirmation

Wireshark permet de capturer et d'analyser une session Telnet entre l'ordinateur hôte pod et le commutateur Cisco. Utilisez l'option du menu Wireshark **Analyze > Follow TCP Stream** pour afficher l'ID d'utilisateur et le mot de passe de connexion. Quel est le niveau de protection du protocole Telnet ? Comment sécuriser davantage la communication avec les périphériques Cisco ?

_____

_____

_____

_____

_____

Tâche 5 : nettoyage

Wireshark a été installé sur l'ordinateur hôte pod. Si vous souhaitez désinstaller Wireshark, cliquez sur **Démarrer > Panneau de configuration**. Ouvrez **Ajout ou suppression de programmes**. Sélectionnez Wireshark et cliquez sur **Supprimer**.

Supprimez tout fichier créé sur l'ordinateur hôte pod au cours des travaux pratiques.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques et préparez la salle pour le cours suivant.

9.9.1 : exercice d'intégration des compétences : Ethernet avec commutation

Diagramme de topologie

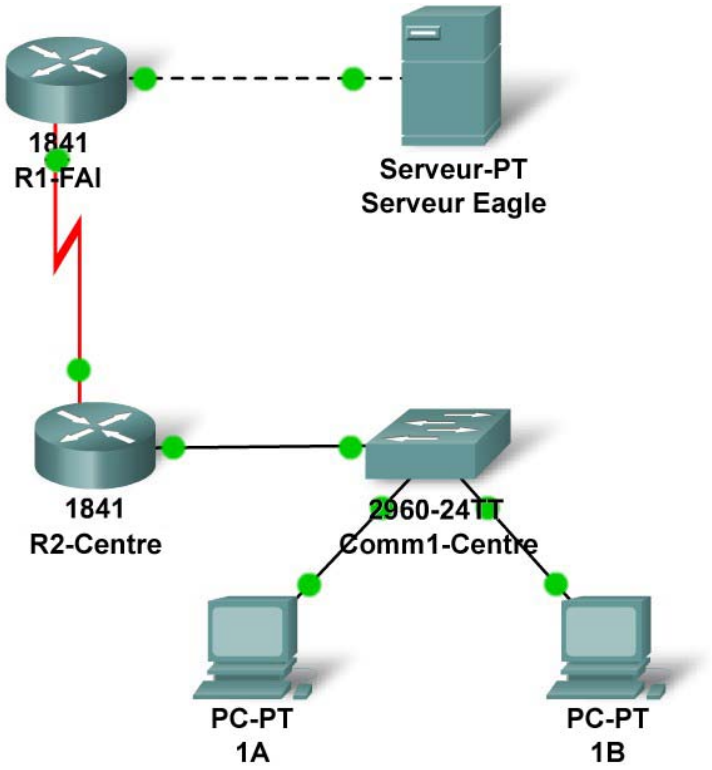


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	**Fa0/0**	192.168.111.134	255.255.255.248	N/A
	S0/0/0	192.168.111.138	255.255.255.252	N/A
R2-Central	**Fa0/0**			N/A
	S0/0/0	192.168.111.137	255.255.255.252	N/A
PC 1A	**La carte réseau**			
PC 1B	**La carte réseau**			
Serveur Eagle	**La carte réseau**	192.168.111.133	255.255.255.248	192.168.111.134

Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Déterminer la planification des sous-réseaux IP
- Résoudre les problèmes réseau liés à Ethernet
- Tester le réseau

Contexte

Vous avez été chargé de résoudre certains problèmes dans le modèle de réseau associé au réseau local Ethernet connecté au routeur R2-Central.

Tâche 1 : planification de sous-réseaux IP

On vous a attribué le bloc d'adresses IP 192.168.111.0 /24. Vous devez configurer les trois réseaux.

Les attributions de sous-réseaux sont les suivantes :

- 1er sous-réseau, réseau local existant des participants, jusqu'à 100 hôtes (Fa0/0 sur R2-Central) ;
- 2ème sous-réseau, réseau local existant du fournisseur de services Internet (ISP), jusqu'à 5 hôtes (déjà configuré) ;
- 3ème sous-réseau, réseau étendu (WAN) existant, liaison point à point (déjà configuré) ;

Adresses IP d'interface :

- L'interface série du serveur, de R1-ISP et de R2-Central a déjà été configurée.
- Pour l'interface Fa0/0 du routeur R2-Central, utilisez l'adresse utilisable la plus élevée sur le sous-réseau LAN existant des participants.
- Pour les hôtes 1A et 1B, utilisez les deux premières adresses IP (les deux adresses utilisables les plus basses) du sous-réseau LAN existant des participants.
- Pour les hôtes 1A et 1B, le serveur DNS est 192.168.111.133 /29.
- Le routeur du tronçon suivant (vers lequel la route par défaut doit pointer), R1-ISP, a pour adresse IP 192.168.111.138 /30.

Tâche 2 : résolution des problèmes liés au réseau local commuté Ethernet

- Le PC 1B est équipé d'une carte sans fil et ne peut pas Ãªtre connecté au commutateur ; ajoutez la carte d'interface Fast Ethernet PT-HOST-NM-1CFE au PC 1B.
- Connectez cette carte réseau Fast Ethernet à l'interface Fa0/2 du commutateur.
- Reliez le PC 1A à l'interface Fa0/1 du commutateur.
- Reliez l'interface Fa0/24 du commutateur à l'interface Fa0/0 du routeur R2-Central.

À première vue, les paramètres de vitesse et de mode duplex Ethernet de l'interface Fa0/0 de R2-Central, les interfaces du commutateur S1-Central (Fa0/1, Fa0/2 et Fa0/24) et les interfaces du PC 1A sont incorrects. Définissez toutes les interfaces Ethernet de sorte qu'elles négocient automatiquement la vitesse et le mode duplex (qui opteront pour le mode full duplex et une vitesse de 100 Mbit/s si les deux extrémités de la liaison le permettent). Assurez-vous que tous les périphériques sont sous tension et que leurs interfaces sont activées (vérifiez que les interfaces Ethernet ne sont pas désactivées). Ajoutez des adresses IP à l'interface Fa0/0 du routeur et aux deux ordinateurs (adresse de sous-réseau utilisable la plus élevée attribuée à la passerelle et les deux adresses utilisables les plus faibles associées aux ordinateurs). La route statique sur R2-Central doit être une route statique par défaut qui accède à l'adresse IP de l'interface série pour R1-ISP. Ces procédures ont été expliquées aux chapitres 5 et 6 de l'exercice d'intégration des compétences.

Tâche 3 : test du réseau

À l'aide de la commande ping, trace, du trafic Web et de l'outil **Inspect**, suivez le flux de paquets en mode Simulation, sans masquer HTTP, DNS, TCP, UDP, ICMP et ARP, pour vérifier si vous avez compris le fonctionnement du réseau.

Tâche 4 : remarques générales

Les deux technologies de couche 2 (et de couche 1) de ce modèle sont constituées d'une connexion série (entre les routeurs) et des réseaux locaux Ethernet (pour le serveur ISP et avec le commutateur S1-Central). Comparez et confrontez la connexion série à Ethernet: Vous en apprendrez beaucoup plus sur les technologies Ethernet commutées dans un cours à venir.

Travaux pratiques 10.3.2 : combien de réseaux ?

Objectifs pédagogiques

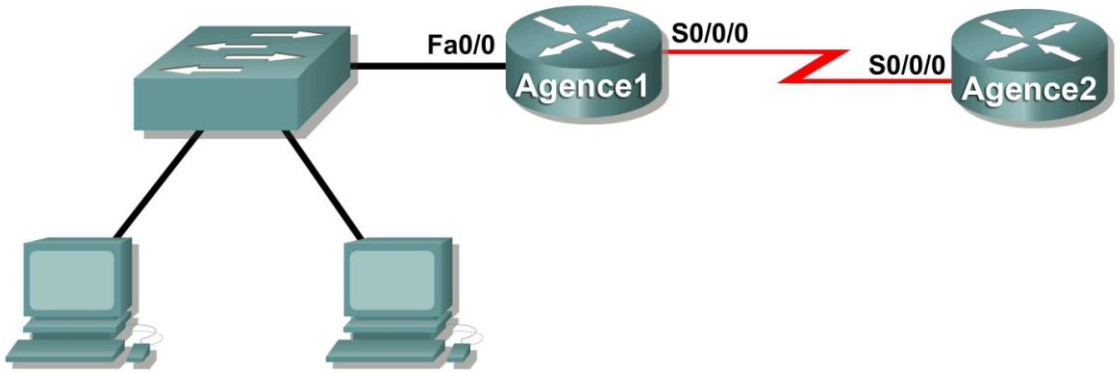
À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Déterminer le nombre de sous-réseaux
- Concevoir un système d'adressage approprié
- Attribuer des adresses et des paires de masques de sous-réseau aux interfaces des périphériques
- Examiner l'utilisation de l'espace d'adressage réseau disponible

Scénario

Dans le cadre de ces travaux pratiques, vous devez diviser l'adresse réseau 192.168.26.0/24 en sous-réseaux et définir l'adressage IP pour les réseaux illustrés dans les diagrammes de topologies. Vous devez déterminer le nombre de réseaux nécessaires pour ensuite concevoir un modèle d'adressage approprié. Enfin, vous devez insérer l'adresse et le masque adéquats dans la table d'adressage. Dans cet exemple, le nombre d'hôtes n'est pas important. Vous devez simplement déterminer le nombre de sous-réseaux par exemple de topologie.

Diagramme de topologie A



Tâche 1 : détermination du le nombre de sous-réseaux présents dans le diagramme de topologie

Étape 1 : combien de réseaux y a-t-il ? _____

Étape 2 : combien de bits devez-vous emprunter pour créer le nombre nécessaire de sous-réseaux ? _____

Étape 3 : combien d'adresses d'hôtes exploitables par sous-réseau obtenez-vous ? _____

Étape 4 : quel est le nouveau masque de sous-réseau en notation décimale ? _____

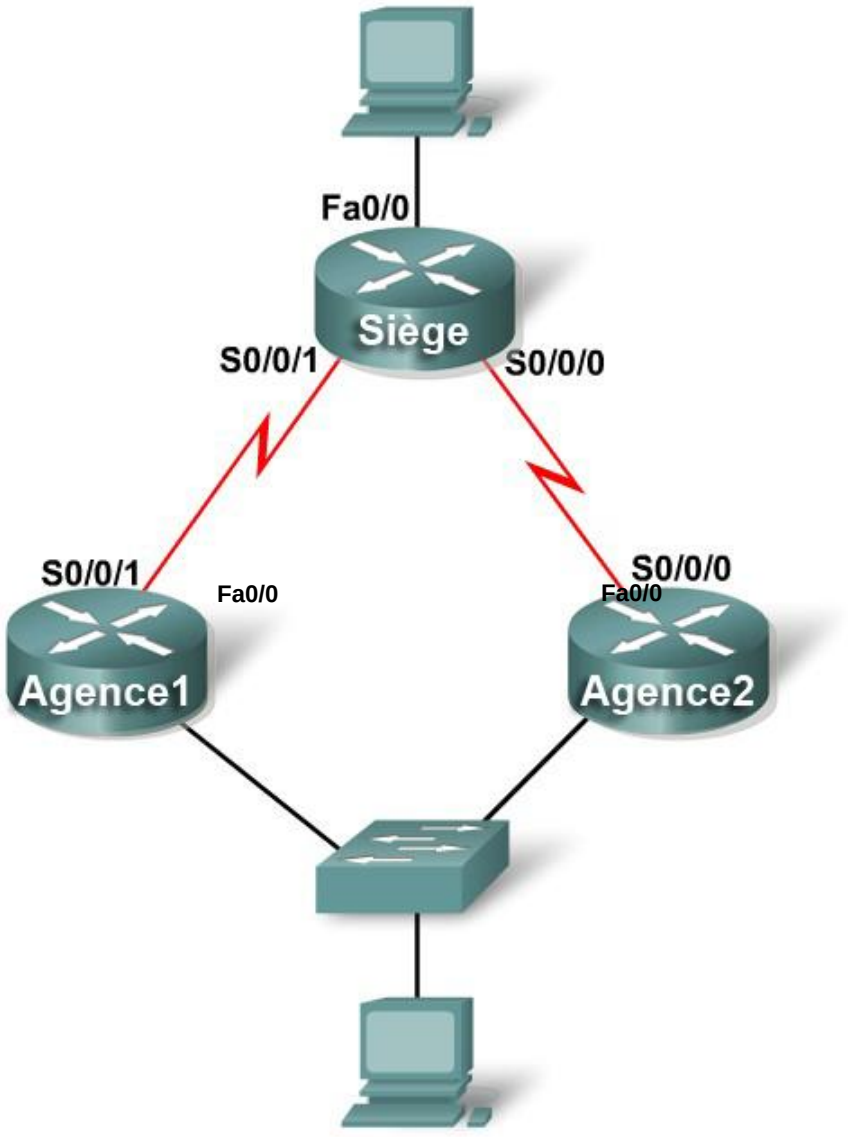
Étape 5 : quel est le nombre de sous-réseaux disponibles pour une utilisation ultérieure ? _____

Tâche 2 : inscription des paramètres des sous-réseaux

Étape 1 : complétez le tableau ci-dessous avec les paramètres des sous-réseaux.

N° de sous-réseau	Adresse de sous-réseau	Première adresse hôte utilisable	Dernière adresse hôte utilisable	Adresse de diffusion
0				
1				
2				
3				
4				
5				
6				
7				

Diagramme de topologie B



Tâche 3 : détermination du nombre de sous-réseaux présents dans le diagramme de topologie

Étape 1 : combien de réseaux y a-t-il ? ____
Étape 2 : combien de bits devez-vous emprunter pour créer le nombre nécessaire de sous-réseaux ? ____
Étape 3 : combien d'adresses d'hôtes exploitables par sous-réseau obtenez-vous ? ____
Étape 4 : quel est le nouveau masque de sous-réseau en notation décimale ? _____

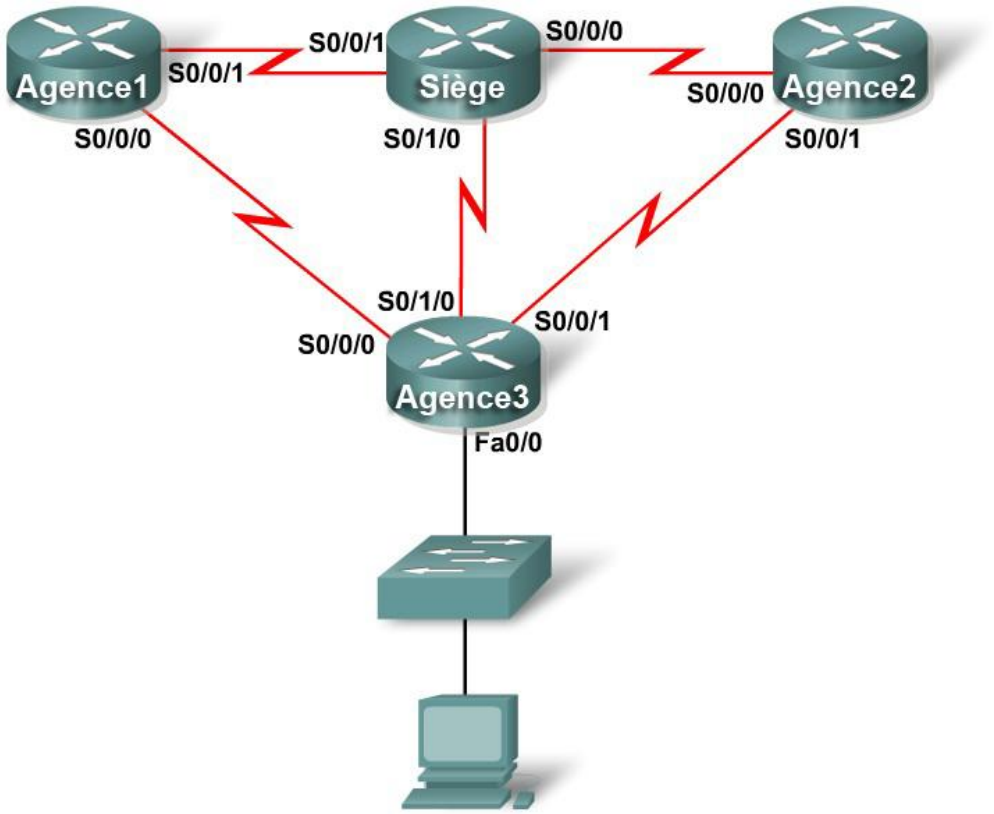
Étape 5 : quel est le nombre de sous-réseaux disponibles pour une utilisation ultérieure ? ____

Tâche 4 : inscription des paramètres des sous-réseaux

Étape 1 : complétez le tableau ci-dessous avec les paramètres des sous-réseaux.

N° de sous-réseau	Adresse de sous-réseau	Première adresse hôte utilisable	Dernière adresse hôte utilisable	Adresse de diffusion
0				
1				
2				
3				
4				
5				
6				
7				

Diagramme de topologie C



Tâche 5 : détermination du nombre de sous-réseaux présents dans le diagramme de topologie

Étape 1 : combien de réseaux y a-t-il ? ____
Étape 2 : combien de bits devez-vous emprunter pour créer le nombre nécessaire de sous-réseaux ? ____
Étape 3 : combien d'adresses d'hôtes exploitables par sous-réseau obtenez-vous ? ____
Étape 4 : quel est le nouveau masque de sous-réseau en notation décimale ? _____

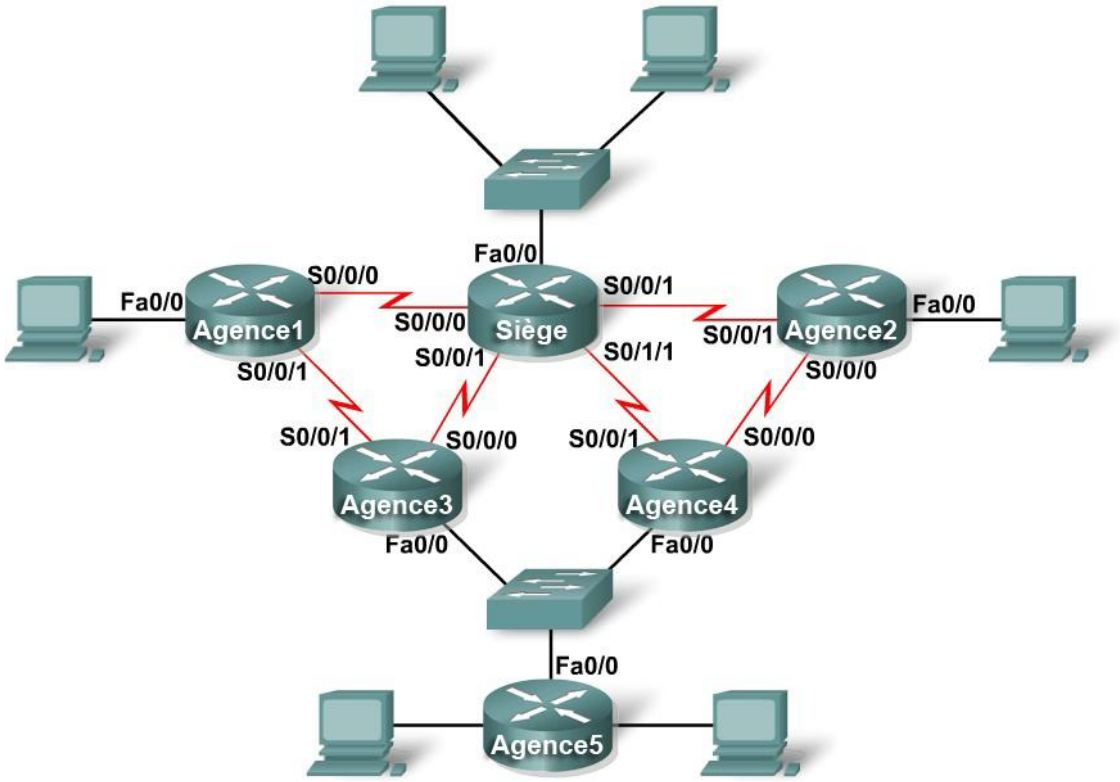
Étape 5 : quel est le nombre de sous-réseaux disponibles pour une utilisation ultérieure ? ____

Tâche 6 : inscription des informations sur les sous-réseaux

Étape 1 : complétez le tableau ci-dessous avec les paramètres des sous-réseaux.

N° de sous-réseau	Adresse de sous-réseau	Première adresse hôte utilisable	Dernière adresse hôte utilisable	Adresse de diffusion
0				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Diagramme de topologie D



Tâche 7 : détermination du nombre de sous-réseaux présents dans le diagramme de topologie

Étape 1 : combien de réseaux y a-t-il ? ____
Étape 2 : combien de bits devez-vous emprunter pour créer le nombre nécessaire de sous-réseaux ? ____
Étape 3 : combien d'adresses d'hôtes exploitables par sous-réseau obtenez-vous ? ____
Étape 4 : quel est le nouveau masque de sous-réseau en notation décimale ? _____

Étape 5 : quel est le nombre de sous-réseaux disponibles pour une utilisation ultérieure ? ____

Tâche 8 : inscription des informations sur les sous-réseaux

Étape 1 : complétez le tableau ci-dessous avec les paramètres des sous-réseaux.

N° de sous-réseau	Adresse de sous-réseau	Première adresse hôte utilisable	Dernière adresse hôte utilisable	Adresse de diffusion
0				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

Tâche 9 : remarques générales

De quelles informations avez-vous besoin pour définir un modèle d'adressage adapté à un réseau ?

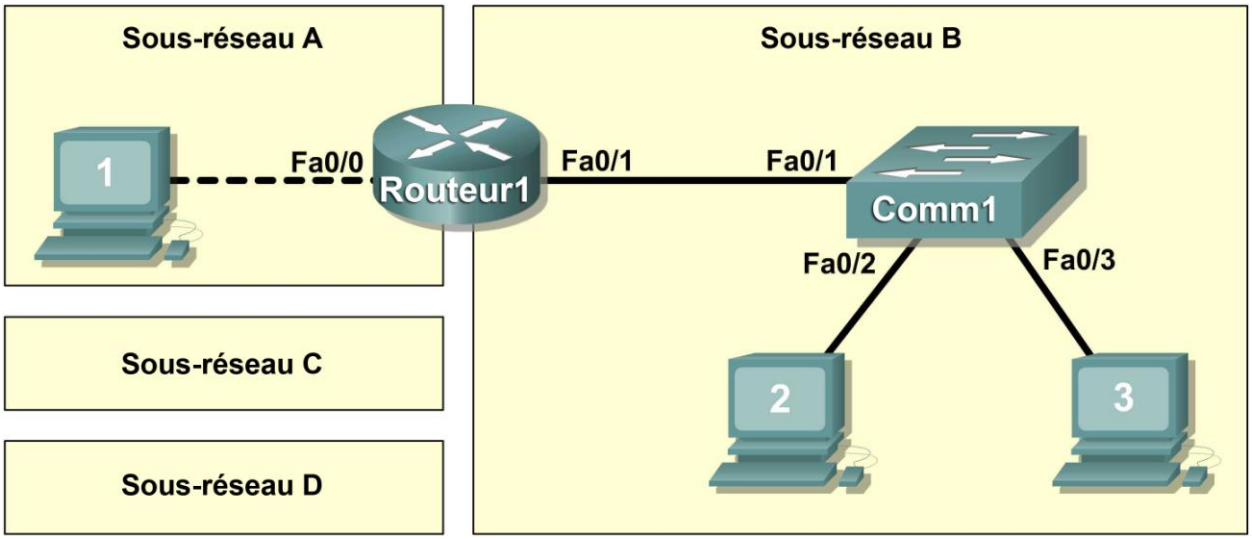
_____

_____

_____

Travaux pratiques 10.6.1 : création d'une petite topologie

Diagramme de topologie



Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Concevoir le réseau logique
- Configurer la topologie physique des travaux pratiques
- Configurer la topologie logique du réseau local (LAN)
- Vérifier la connectivité du réseau local

Contexte

Matériel	Qté	Description
Routeur Cisco	1	Inclus dans l'équipement de travaux pratiques CCNA
Commutateur Cisco	1	Inclus dans l'équipement de travaux pratiques CCNA
*Ordinateur (hôte)	3	Ordinateur de travaux pratiques
Câbles UTP droits de catégorie 5 ou supérieure	3	Relie le routeur Router1 et les ordinateurs Hôte1 et Hôte2 au commutateur Switch1
Câble de croisement UTP de catégorie 5	1	Relie l'ordinateur Hôte1 au routeur Router1

Tableau 1. Équipement et matériel pour les travaux pratiques

Regroupez l'équipement et les câbles nécessaires. Pour configurer les travaux pratiques, reportez-vous au Tableau 1 qui décrit l'équipement et le matériel nécessaires.

Scénario

Dans le cadre de ces travaux pratiques, vous allez créer un petit réseau, ce qui suppose de connecter des périphériques réseau et de configurer les ordinateurs hôtes pour une connectivité de base. SubnetA et SubnetB sont des sous-réseaux dont nous avons besoin. SubnetC et SubnetD sont des projets de sous-réseaux qui ne sont pas encore connectés au réseau. Nous allons utiliser le sous-réseau 0.

Remarque : vous trouverez dans l'annexe 1 le tableau des sous-réseaux avec le dernier octet d'adresse IP.

Tâche 1 : conception du réseau logique

À partir de l'adresse IP et du masque `172.20.0.0 / 24 (adresse / masque)`, concevez un modèle d'adressage IP qui remplisse les conditions suivantes :

Sous-réseau	Nombre d'hôtes
SubnetA	2
SubnetB	6
SubnetC	47
SubnetD	125

Les ordinateurs hôtes de chaque sous-réseau utilisent la première adresse IP disponible dans le bloc d'adresses. Les interfaces du routeur utilisent la dernière adresse IP disponible dans le bloc d'adresses.

Étape 1 : conception du bloc d'adresses de SubnetD

Débutez la phase de conception du réseau logique en répondant aux critères de SubnetD, qui nécessite le bloc d'adresses IP le plus grand. Reportez-vous au tableau des sous-réseaux et choisissez le premier bloc d'adresses qui prendra en charge SubnetD.

Dans le tableau suivant, indiquez les paramètres IP de SubnetD :

Adresse réseau	Masque	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion

Quel est le masque de bits ? _____

Étape 2 : conception du bloc d'adresses de SubnetC

Répondez aux critères de SubnetC, le prochain bloc d'adresses IP le plus grand. Reportez-vous au tableau des sous-réseaux et choisissez le prochain bloc d'adresses disponible prenant en charge SubnetD.

Dans le tableau suivant, indiquez les paramètres IP de SubnetC :

Adresse réseau	Masque	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion

Quel est le masque de bits ? _____

Étape 3 : conception du bloc d'adresses de SubnetB

Répondez aux critères de SubnetB, le prochain bloc d'adresses IP le plus grand. Reportez-vous au tableau des sous-réseaux et choisissez le prochain bloc d'adresses disponible prenant en charge SubnetB.

Dans le tableau suivant, indiquez les paramètres IP de SubnetB :

Adresse réseau	Masque	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion

Quel est le masque de bits ? _____

Étape 4 : conception du bloc d'adresses de SubnetA

Répondez aux critères de SubnetA. Reportez-vous au tableau des sous-réseaux et choisissez le prochain bloc d'adresses disponible prenant en charge SubnetA.

Dans le tableau suivant, indiquez les paramètres IP de SubnetA :

Adresse réseau	Masque	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion

Quel est le masque de bits ? _____

Tâche 2 : configuration de la topologie physique de travaux pratiques

Étape 1 : connexion physique des périphériques

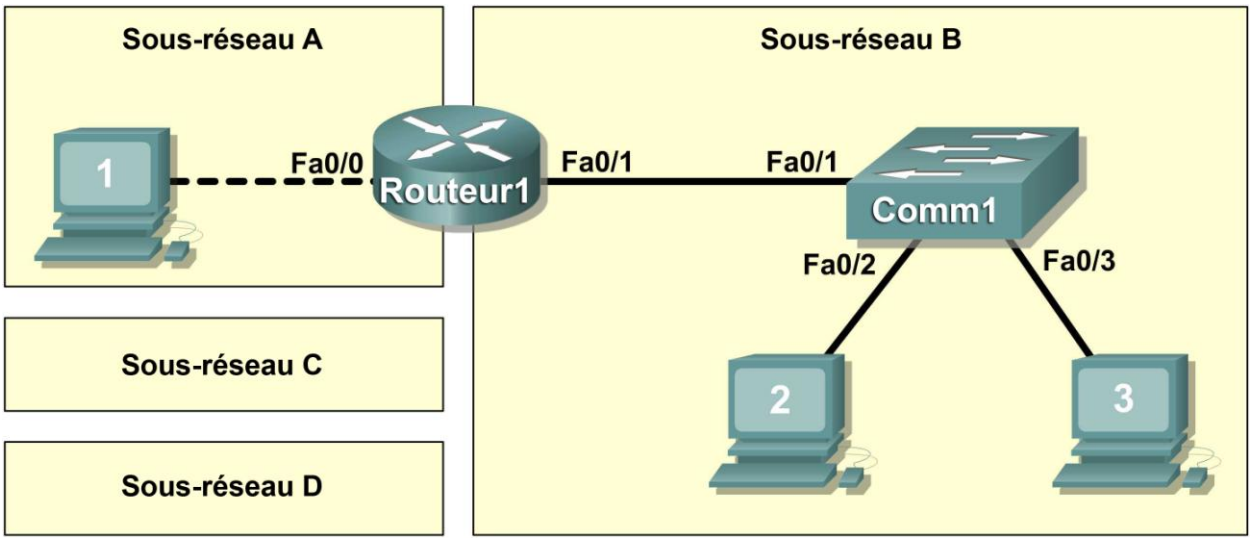


Figure 1. Installation du réseau

Installez les périphériques réseau comme illustré dans la figure 1.

De quel type de câble avez-vous besoin pour relier l'hôte 1 à Router1 ? Pourquoi ? _____

_____

De quel type de câble avez-vous besoin pour relier l'hôte 1, l'hôte 2 et Router1 à Switch1 ? Pourquoi ?

_____

_____

Si ce n'est déjà fait, mettez tous les périphériques sous tension.

Étape 2 : inspection visuelle des connexions réseau

Après avoir installé les périphériques réseau, prenez le temps de vérifier les connexions. C'est en faisant attention aux détails dès à présent que vous limiterez par la suite le temps passé à résoudre des problèmes de connectivité. Vérifiez que toutes les connexions du commutateur affichent la couleur verte. Toute connexion du commutateur qui ne passe pas de l'orange au vert doit être examinée. Le périphérique connecté est-il sous tension ? Le câble utilisé est-il approprié ? Le câble est-il en bon état ?

Quel est le type de câble qui relie l'interface `Fa0/0` de Router1 à l'hôte 1 ? ___ _____

Quel est le type de câble qui relie l'interface Fa0/1 de Router1 à Switch1 ? _____

Quel est le type de câble qui relie l'hôte 2 à Switch1 ? ____ _____

Quel est le type de câble qui relie l'hôte 3 à Switch1 ? ____ _____

Les équipements sont-ils tous sous tension ? _____

Tâche 3 : configuration de la topologie logique

Étape 1 : consignation des paramètres du réseau logique

L'adresse IP de la passerelle d'un ordinateur hôte sert à envoyer les paquets IP vers d'autres réseaux. Par conséquent, l'adresse de la passerelle correspond à l'adresse IP attribuée à l'interface du routeur de ce sous-réseau.

Compte tenu des informations notées dans le cadre de la tâche 1, inscrivez les paramètres IP de chaque ordinateur :

Hôte 1	
Adresse IP	
Masque IP	
Adresse de passerelle	

Hôte 2	
Adresse IP	
Masque IP	
Adresse de passerelle	

Hôte 3	
Adresse IP	
Masque IP	

Adresse de passerelle	

Étape 2 : configuration de l'ordinateur hôte 1

Sur l'hôte 1, cliquez sur **Démarrer > Panneau de configuration > Connexions réseau**. Cliquez avec le bouton droit de la souris sur l'icône du périphérique **Connexion au réseau local** et choisissez **Propriétés**.

Sous l'onglet **Général**, sélectionnez **Protocole Internet (TCP/IP)**, puis cliquez sur le bouton **Propriétés**.

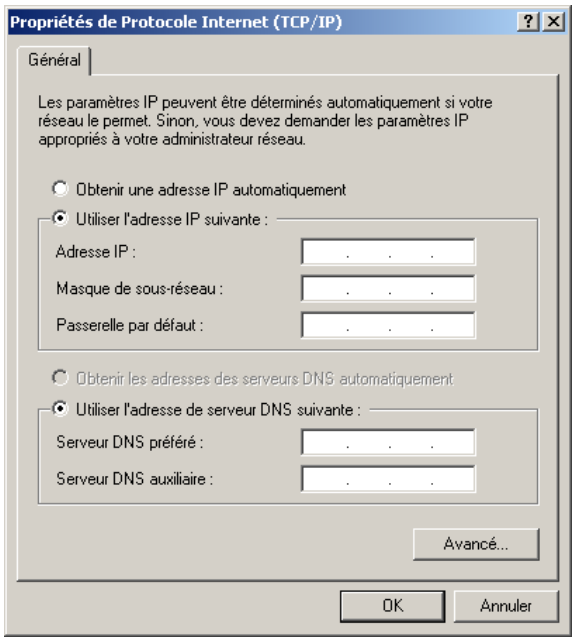


Figure 2. Paramètres d'adresse IP et de passerelle de l'hôte 1

Consultez les paramètres d'adresse IP et de passerelle de l'hôte 1 dans la figure 2. Entrez manuellement les informations ci-dessous inscrites à l'étape 1 précédente :

```
Adresse IP : Adresse IP de l'hôte 1
Masque de sous-réseau : Masque de sous-réseau de l'hôte 1
Passerelle par défaut : Adresse IP de la passerelle
```

À l'issue de cette opération, fermez la fenêtre Propriétés de Protocole Internet (TCP/IP) en cliquant sur **OK**. Fermez la fenêtre Connexion au réseau local. Selon le système d'exploitation Windows utilisé, vous serez peut-être amené à redémarrer l'ordinateur pour que les modifications prennent effet.

Étape 3 : configuration des ordinateurs Hôte 2 et Hôte 3

Répétez l'étape 2 pour les ordinateurs Hôte 2 et Hôte 3 en utilisant les paramètres IP de ces ordinateurs.

Tâche 4 : vérification de la connectivité du réseau

Vérifiez avec votre formateur que le routeur Router1 a été configuré. À défaut, la connectivité sera rompue entre les réseaux locaux. Switch1 doit présenter une configuration par défaut.

La connectivité réseau peut être vérifiée à l'aide d'une commande **`ping`** Windows. Ouvrez une fenêtre de terminal en cliquant sur **Démarrer > Exécuter**. Tapez **`cmd`** et appuyez sur **Entrée**.

Pour vérifier méthodiquement la connectivité avec chaque périphérique réseau et noter les résultats, servez-vous du tableau ci-dessous. En cas d'échec à un test, prenez des mesures correctives pour établir la connectivité :

Origine	Destination	Adresse IP	Résultats de la requête ping
Hôte 1	Passerelle (Router1, Fa0/0)		
Hôte 1	Router1, Fa0/1		
Hôte 1	Hôte 2		
Hôte 1	Hôte 3		
Hôte 2	Hôte 3		
Hôte 2	Passerelle (Router1, Fa0/1)		
Hôte 2	Router1, Fa0/0		
Hôte 2	Hôte 1		
Hôte 3	Hôte 2		
Hôte 3	Passerelle (Router1, Fa0/1)		
Hôte 3	Router1, Fa0/0		
Hôte 3	Hôte 1		

Notez toute interruption de connectivité. Au moment de résoudre les problèmes de connectivité, le diagramme de topologie peut s'avérer extrêmement utile.

Dans le scénario exposé ci-dessus, comment détecter une passerelle déficiente ?

_____

_____

Tâche 5 : remarques générales

Analysez les problèmes de configuration physique ou logique rencontrés au cours de ces travaux pratiques. Assurez-vous d'avoir bien compris les procédures utilisées pour vérifier la connectivité réseau.

Il s'agit de travaux pratiques particulièrement important. En plus de vous être exercé à la création de sous-réseaux IP, vous avez configuré les ordinateurs hôtes avec des adresses réseau et en avez testé la connectivité.

Il est recommandé de répéter plusieurs fois les exercices de configuration et de vérification des ordinateurs hôtes. Cela renforcera les compétences que vous avez acquises au cours de ces travaux pratiques et fera de vous un meilleur technicien réseau.

Tâche 6 : confirmation

Demandez à votre formateur ou à un autre participant d'introduire un ou deux problèmes dans votre réseau pendant que vous êtes occupé à une autre tâche ou que vous êtes absent de la salle de travaux

pratiques. Les problèmes peuvent être d'ordre physique (câble UTP inapproprié) ou logique (adresse IP ou passerelle incorrecte). Pour résoudre les problèmes, procédez comme suit :

1. Faites une inspection visuelle minutieuse. Vérifiez que les voyants de liaison du commutateur Switch1 sont verts.
2. Servez-vous du tableau fourni à la tâche 3 pour identifier les problèmes de connectivité. Énumérez les problèmes :

   _____

   _____

   _____

   _____

   _____

3. Notez la ou les solutions que vous proposez :

   _____

   _____

   _____

   _____

   _____

4. Testez votre solution. Si la solution est concluante, notez-la. Si la solution est inefficace, poursuivez le dépannage.

   _____

   _____

   _____

   _____

   _____

   _____

   _____

   _____

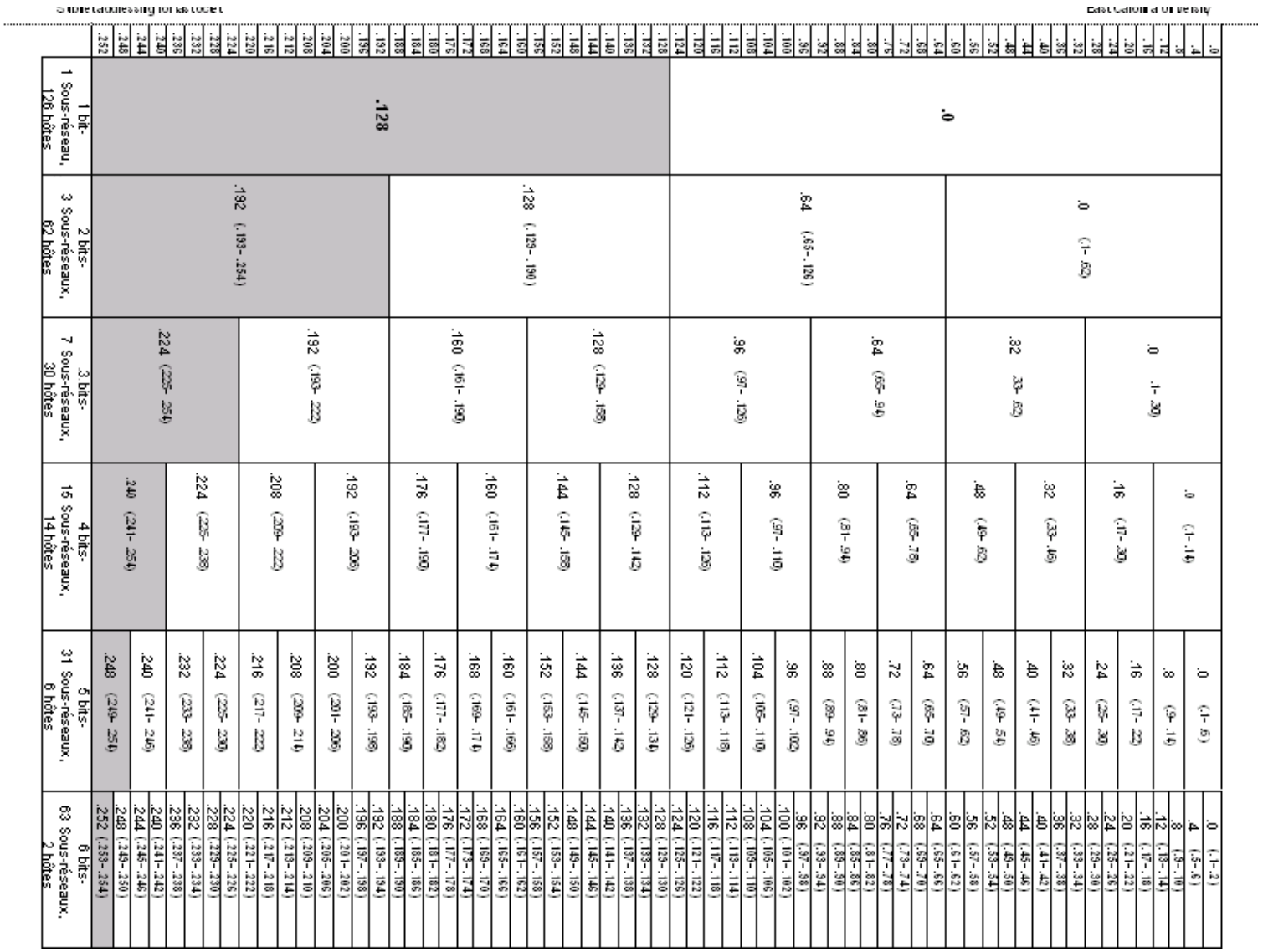
Tâche 7 : remise en état.

Sauf instruction contraire du formateur, rétablissez la connectivité réseau des ordinateurs hôtes, puis mettez-les hors tension.

Retirez les câbles avec précaution et rangez-les soigneusement. Rebranchez les câbles qui ont été débranchés pour les besoins de ces travaux pratiques.

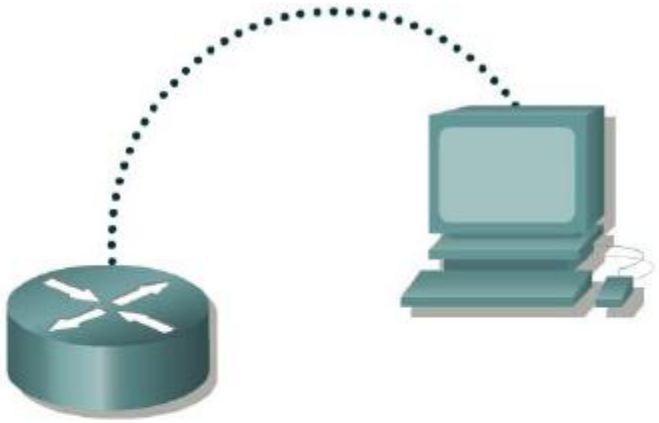
Enlevez le matériel utilisé durant les travaux pratiques et préparez la salle pour le cours suivant.

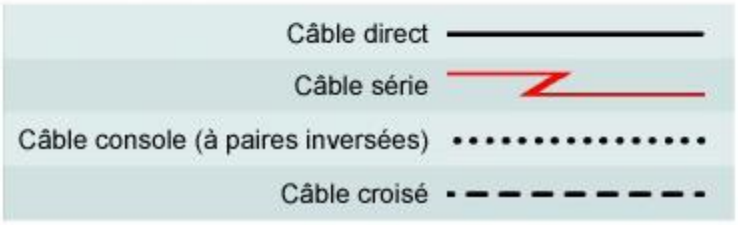
Annexe 1



Travaux pratiques 10.6.2 : établissement d'une session en mode console avec HyperTerminal

Diagramme de topologie





Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Connecter un routeur et un ordinateur à l'aide d'un câble console
- Configurer HyperTerminal pour ouvrir une session en mode console avec un routeur Cisco IOS
- Configurer HyperTerminal pour ouvrir une session en mode console avec un commutateur Cisco IOS

Contexte

HyperTerminal est un programme Windows. Il permet d'émuler un terminal basique pour une communication série et de se connecter au port console des périphériques Cisco IOS. L'interface série d'un ordinateur est reliée au périphérique Cisco par un câble de renversement. L'utilisation d'HyperTerminal est le moyen le plus simple d'accéder à un routeur afin de vérifier ou modifier sa configuration. Il existe un autre utilitaire de communication série très répandu : TeraTerm Web. Vous trouverez des instructions pour utiliser TeraTerm Web dans l'annexe A.

Scénario

Installez un réseau similaire à celui du diagramme de topologie. Tout routeur doté de l'interface appropriée peut être utilisé. Vous pouvez utiliser les routeurs 800, 1600, 1700, 2500, 2600 ou une combinaison de ces routeurs. Les ressources nécessaires sont les suivantes :

- un ordinateur doté d'une interface série et HyperTerminal ;
- un routeur Cisco ;
- un câble console (de renversement) pour connecter la station de travail au routeur.

Tâche 1 : connexion d'un routeur et d'un ordinateur à l'aide d'un câble console

Étape 1 : configuration d'une connexion physique de base

Connectez le câble console (de renversement) au port console du routeur. Connectez l'autre extrémité du câble au port COM 1 de l'ordinateur hôte avec un adaptateur DB-9 ou DB-25.

Étape 2 : mise sous tension des périphériques

Si ce n'est déjà fait, mettez l'ordinateur et le routeur sous tension.

Tâche 2 : configuration d'HyperTerminal en vue d'ouvrir une session en mode console avec un routeur Cisco IOS

Étape 1 : démarrage de l'application HyperTerminal

Dans la barre des tâches Windows, ouvrez le programme HyperTerminal en cliquant sur **Démarrer > Programmes > Accessoires > Communications > HyperTerminal**.

Étape 2 : configuration d'HyperTerminal

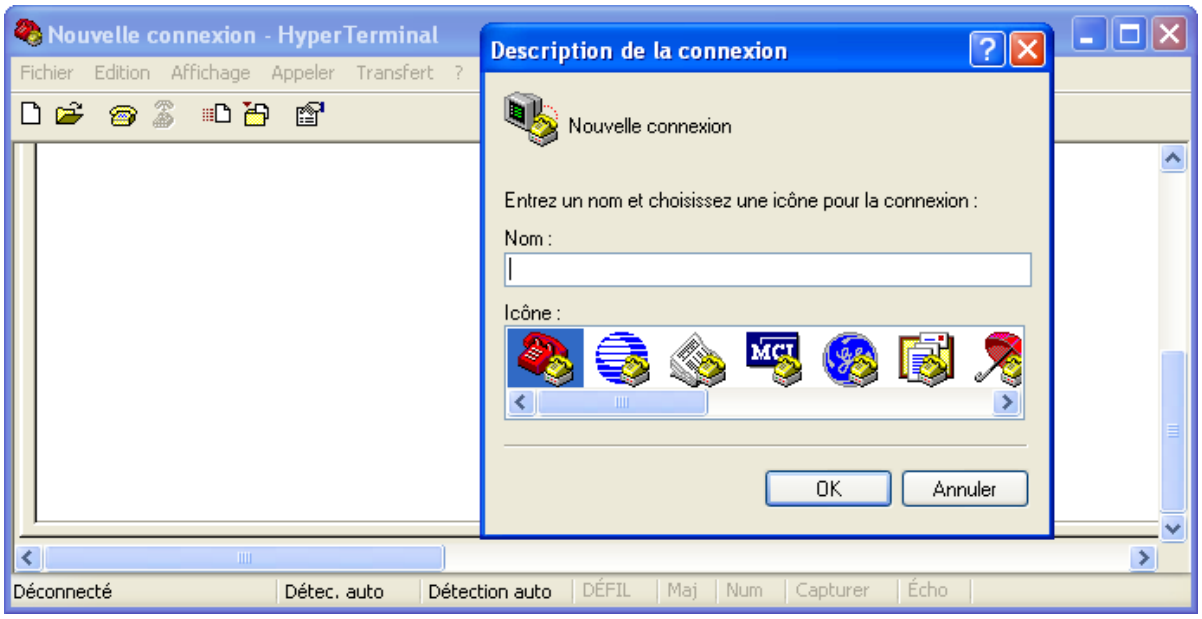


Figure 1. Fenêtre de configuration du nom de session dans HyperTerminal

Reportez-vous à la figure 1 pour obtenir une description de la fenêtre de configuration d'HyperTerminal qui s'affiche. Dans la fenêtre Description de la connexion, entrez un nom de session dans le champ Nom. Sélectionnez l'icône de votre choix ou conservez l'icône par défaut. Cliquez sur OK.

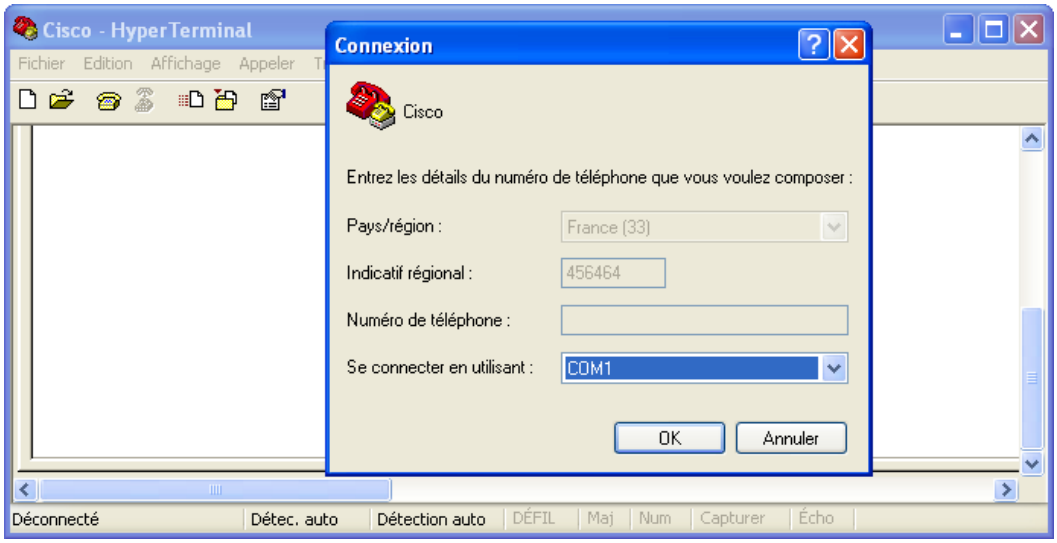


Figure 2. Type de connexion HyperTerminal

Reportez-vous à la figure 2. Entrez le type de connexion approprié, en l'occurrence COM1, dans le champ Se connecter en utilisant. Cliquez sur OK.

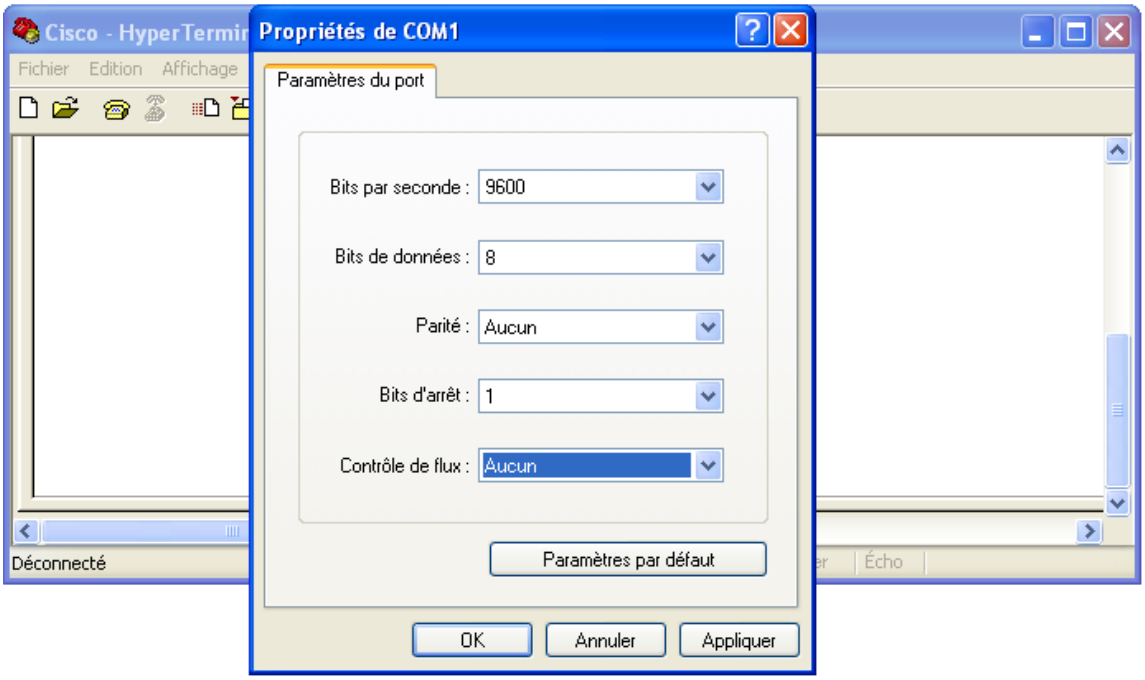


Figure 3. Paramètres du port COM1 dans HyperTerminal

Reportez-vous à la figure 3. Remplacez les paramètres du port par les valeurs suivantes :

Paramètre	Valeur
Bits par seconde	**9600**
Bits de données	**8**
Parité	**Aucun**
Bits d'arrêt	**1**
Contrôle de flux	**Aucun**

Cliquez sur **OK**.

Lorsque la fenêtre de session HyperTerminal s'affiche, appuyez sur la touche **Entrée**. Le routeur doit répondre. Cela indique que la connexion a été établie. En l'absence de connexion, procédez à un dépannage. Par exemple, vérifiez que le routeur est sous tension. Assurez-vous que le câble est bien connecté au port COM1 du PC et au port console du routeur. S'il n'y a toujours pas de connexion, demandez de l'aide au formateur.

Étape 3 : fermeture d'HyperTerminal

Lorsque vous avez terminé, fermez la session HyperTerminal. Cliquez sur **Fichier** > **Quitter**. Lorsque vous êtes invité à enregistrer la session, cliquez sur **Oui**. Attribuez un nom à la session.

Étape 4 : reconnexion de la session HyperTerminal.

Rouvrez la session HyperTerminal, comme indiqué à l'étape 1 de la tâche 2. Cette fois, cliquez sur **Annuler** lorsque la fenêtre Description de la connexion s'affiche (voir Figure 1).
Cliquez sur **Fichier > Ouvrir**. Sélectionnez la session enregistrée, puis cliquez sur **Ouvrir**. Employez cette technique pour reconnecter la session HyperTerminal à un périphérique Cisco sans avoir à reconfigurer une nouvelle session.

Lorsque vous avez terminé, quittez HyperTerminal.

Tâche 3 : configuration d'HyperTerminal en vue d'ouvrir une session en mode console avec un commutateur Cisco IOS

Les connexions série entre routeurs et commutateurs Cisco IOS sont très similaires. Vous allez établir une connexion série entre un ordinateur hôte et un commutateur CISCO IOS.

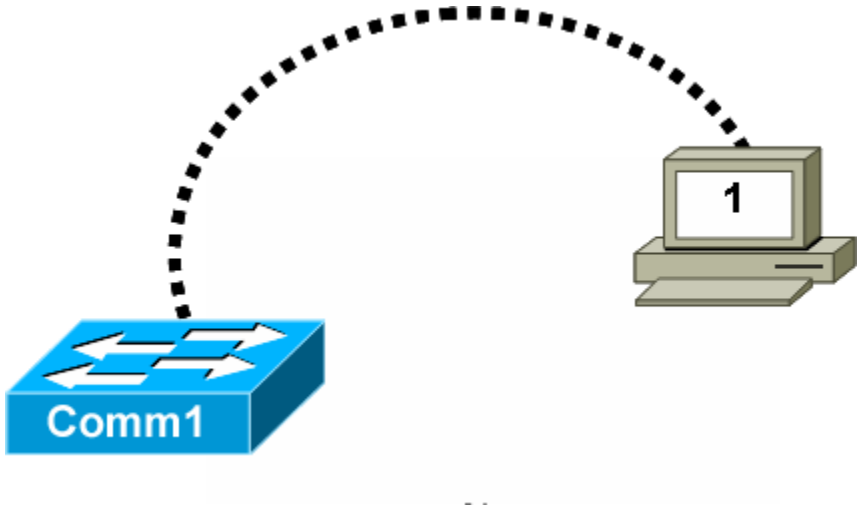


Figure 4. Connexion série entre un ordinateur hôte et un commutateur Cisco

Étape 1 : configuration d'une connexion physique de base

Reportez-vous à la figure 4. Connectez le câble console (de renversement) au port console du routeur. Connectez l'autre extrémité du câble au port COM1 de l'ordinateur hôte avec un adaptateur DB-9 ou DB-25.

Étape 2 : mise sous tension des périphériques

Si ce n'est déjà fait, mettez l'ordinateur et le commutateur sous tension.

Étape 3 : démarrage de l'application HyperTerminal

Dans la barre des tâches Windows, démarrez le programme HyperTerminal en cliquant sur **Démarrer > Programmes > Accessoires > Communications > HyperTerminal**.

Étape 4 : configuration d'HyperTerminal

Pour configurer HyperTerminal, suivez la procédure décrite à l'étape 2 de la tâche 2.

Reportez-vous à la figure 1 illustrant la fenêtre de configuration d'HyperTerminal au moment où elle s'affiche. Dans la fenêtre Description de la connexion, entrez un nom de session dans le champ Nom. Sélectionnez une icône ou conservez l'icône par défaut. Cliquez sur **OK**.

Reportez-vous à la figure 2. Entrez le type de connexion approprié, en l'occurrence COM1, dans le champ Se connecter en utilisant. Cliquez sur **OK**.

Reportez-vous à la figure 3. Remplacez les paramètres du port par les valeurs suivantes :

Paramètre	Valeur
Bits par seconde	9600
Bits de données	8
Parité	Aucun
Bits d'arrêt	1
Contrôle de flux	Aucun

Cliquez sur **OK**.

Lorsque la fenêtre de session HyperTerminal s'affiche, appuyez sur la touche **Entrée**. Le commutateur doit répondre. Cela indique que la connexion a été établie. En l'absence de connexion, procédez à un dépannage. Par exemple, vérifiez que le commutateur est sous tension. Assurez-vous que le câble est bien connecté au port COM1 du PC et au port console du commutateur. S'il n'y a toujours pas de connexion, demandez de l'aide au formateur.

Étape 5 : fermeture d'HyperTerminal

Lorsque vous avez terminé, fermez la session HyperTerminal. Cliquez sur **Fichier** > **Quitter**. Lorsque vous êtes invité à enregistrer la session, cliquez sur **Non**.

Tâche 3 : remarques générales

À travers ces travaux pratiques, vous avez appris à établir une connexion console à un routeur et à un commutateur Cisco IOS.

Tâche 4 : confirmation

Dessinez les connecteurs du câble de renversement et du câble droit. Comparez les différences au niveau des broches et soyez en mesure d'identifier les différents types de câbles.

Tâche 5 : remise en état

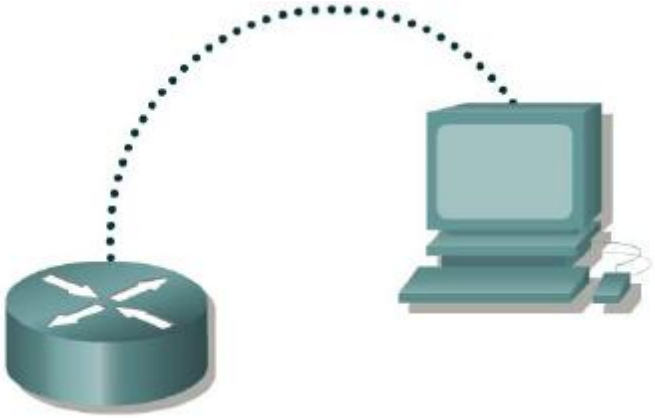
Sauf instructions contraires du formateur, mettez l'ordinateur hôte et le routeur hors tension. Retirez le câble de renversement.

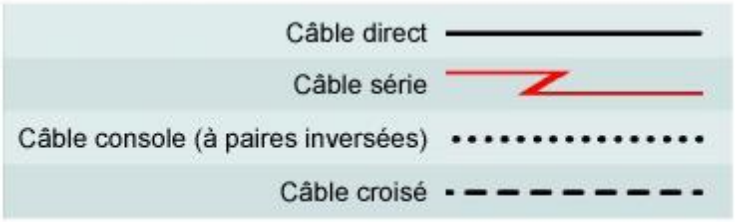
Enlevez le matériel utilisé durant les travaux pratiques et préparez la salle pour le cours suivant.

Annexe A :

Ouverture d'une session en mode console avec TeraTerm

Diagramme de topologie





Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Connecter un routeur et un ordinateur à l'aide d'un câble console
- Cnfigurer TeraTerm pour ouvrir une session en mode console avec le routeur

http://www.ayera.com/teraterm/

Contexte

TeraTerm est un autre programme Windows qui émule un terminal basique pour la communication série et qui peut être utilisé pour se connecter au port console des périphériques Cisco IOS.

Scénario

Installez un réseau similaire à celui illustré dans le diagramme de topologie. Tout routeur doté de l'interface appropriée peut être utilisé. Vous pouvez utiliser les routeurs 800, 1600, 1700, 2500, 2600 ou une combinaison de ces routeurs. Les ressources nécessaires sont les suivantes :

- un ordinateur doté d'une interface série et TeraTerm Pro ;
- un routeur Cisco ;
- un câble console (de renversement) pour connecter la station de travail au routeur.

Tâche 1 : connexion d'un routeur et d'un ordinateur à l'aide d'un câble console

Étape 1 : configuration d'une connexion physique de base

Assurez-vous que l'ordinateur et le routeur Cisco sont sous tension. Connectez le câble console (de renversement) au port console du routeur. Connectez l'autre extrémité du câble au port COM1 du PC avec un adaptateur DB-9 ou DB-25.

Étape 2 : mise sous tension des périphériques

Mettez l'ordinateur et le routeur sous tension.

Tâche 2 : configuration de TeraTerm Web pour ouvrir une session en mode console avec le routeur

Étape 1 : démarrage de l'application TeraTerm Web

Dans la barre des tâches Windows, démarrez le programme TeraTerm Web en ouvrant le dossier TeraTerm Web et en ouvrant l'application TeraTerm Web (**`ttermpro`**).

Étape 2 : configuration de TeraTerm Web

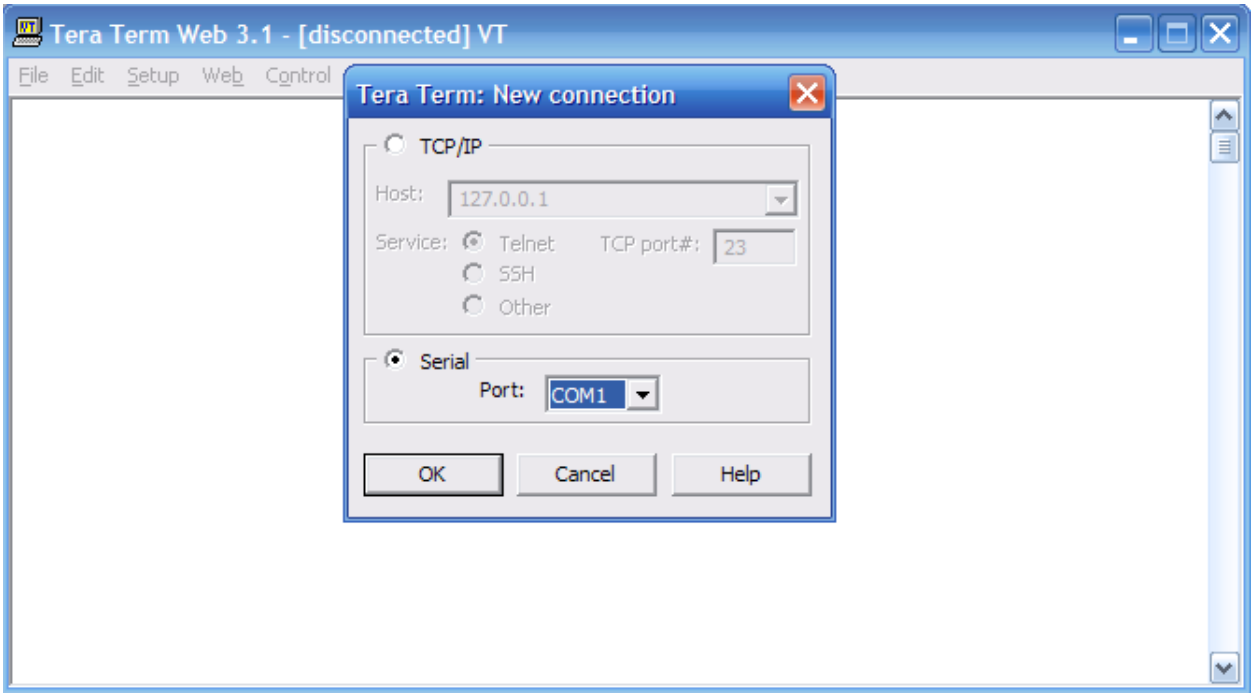


Figure 1. Fenêtre de configuration d'une connexion TeraTerm Web

Cliquez sur **File > New Connection**. Reportez-vous à la figure 1. Sélectionnez le port COM série approprié. Cliquez sur OK.

Lorsque la fenêtre de session TeraTerm Web s'affiche, appuyez sur la touche **Entrée**. Le routeur doit répondre. Cela indique que la connexion a été établie. En l'absence de connexion, procédez à un dépannage. Par exemple, vérifiez que le routeur est sous tension. Assurez-vous que le câble est bien connecté au port COM1 du PC et au port console du routeur. S'il n'y a toujours pas de connexion, demandez de l'aide au formateur.

Étape 3 : fermeture de TeraTerm Web

Lorsque vous avez terminé, fermez la session TeraTerm. Cliquez sur **File | Exit**. Lorsque vous êtes invité à enregistrer la session, cliquez sur **Yes**. Attribuez un nom à la session.

Étape 4 : reconnexion de la session TeraTerm Web

Rouvrez la session TeraTerm Web, comme indiqué à l'étape 1 de la tâche 2. Cette fois, cliquez sur **Cancel** lorsque la fenêtre New Description s'affiche (voir figure 1).

Cliquez sur **File > Open**. Sélectionnez la session enregistrée, puis cliquez sur **Open**. Employez cette technique pour reconnecter la session TeraTerm Web à un périphérique Cisco sans avoir à reconfigurer une nouvelle session.

Tâche 3 : remarques générales

Au cours de ces travaux pratiques, vous avez appris à établir une connexion console à un routeur Cisco. L'accès aux commutateurs Cisco s'effectue de façon analogue.

Tâche 4 : confirmation

Dessinez les connecteurs du câble de renversement et du câble droit. Comparez les différences au niveau des broches et soyez en mesure d'identifier les différents types de câbles.

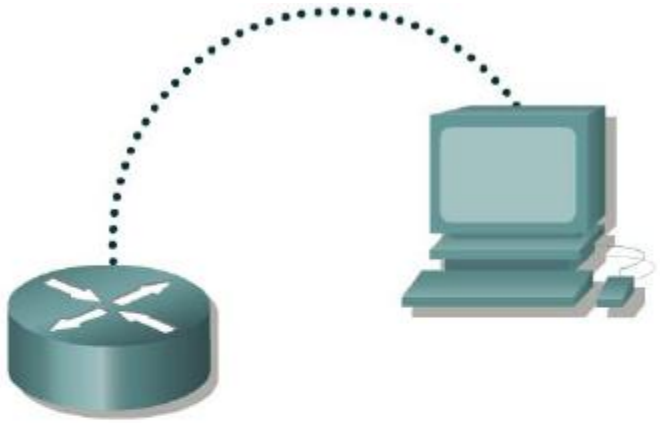
Tâche 5 : remise en état

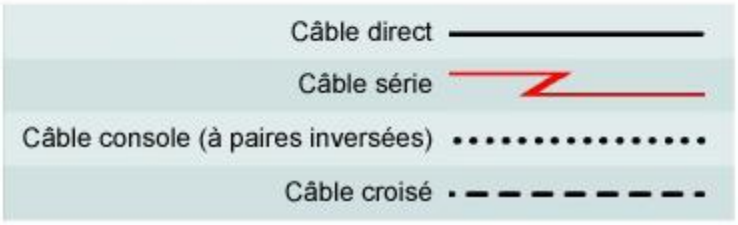
Sauf instructions contraires du formateur, mettez l'ordinateur hôte et le routeur hors tension. Retirez le câble de renversement.

Enlevez le matériel utilisé durant les travaux pratiques et préparez la salle pour le cours suivant.

Travaux pratiques 10.6.3 : établissement d'une session en mode console avec Minicom

Diagramme de topologie





Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Connecter un routeur et un ordinateur à l'aide d'un câble console
- Configurer Minicom pour ouvrir une session en mode console avec le routeur
- Exécuter des commandes de base

Contexte

Minicom est un programme d'émulation de terminal UNIX de type texte qui est comparable au programme HyperTerminal de Windows. Minicom peut être utilisé de plusieurs manières, par exemple, pour contrôler un modem ou accéder à un routeur Cisco via la connexion console série. Le système d'exploitation Linux ou UNIX est nécessaire.

Scénario

Installez un réseau similaire à celui du diagramme de topologie. Tout routeur doté de l'interface appropriée peut être utilisé. Vous pouvez utiliser les routeurs 800, 1600, 1700, 2500, 2600 ou une combinaison de ces routeurs. Les ressources nécessaires sont les suivantes :

- un ordinateur Linux/UNIX doté d'une interface et Minicom ;
- un routeur Cisco ;
- un câble console (de renversement) pour connecter la station de travail au routeur.

Tâche 1 : connexion d'un routeur et d'un ordinateur à l'aide d'un câble console

Étape 1 : configuration d'une connexion physique de base

Assurez-vous que l'ordinateur et le routeur Cisco sont sous tension. Connectez le câble console (de renversement) au port console du routeur. Connectez l'autre extrémité du câble au port COM1 du PC avec un adaptateur DB-9 ou DB-25.

Étape 2 : mise sous tension des périphériques

Mettez l'ordinateur et le routeur sous tension.

Tâche 2 : configuration de Minicom pour ouvrir une session en mode console avec le routeur

Étape 1 : démarrage de l'application Minicom en mode de configuration

Remarque : pour configurer Minicom, un accès racine (root) est nécessaire. Sur la ligne de commande Linux, démarrez **minicom** avec l'option **-s**. Minicom démarre en mode configuration :

```
[root]# minicom -s <ENTER>
```

Étape 2 : configuration de Minicom pour les communications série

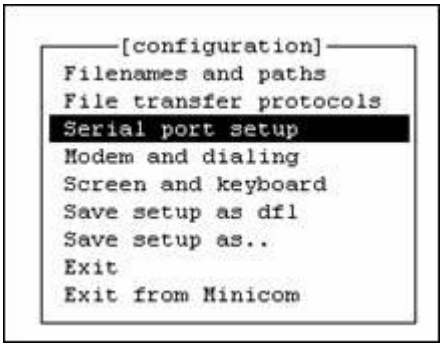


Figure 1. Fenêtre de configuration principale

Reportez-vous à la figure 1. Pour configurer le port série, parcourez la liste de configuration et sélectionnez **`Serial port setup`**. Appuyez sur **Entrée**.

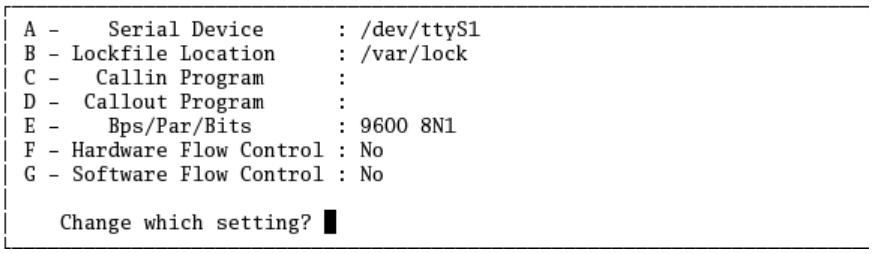


Figure 2. Fenêtre de configuration du port série

Reportez-vous à la figure 2. Utilisez la lettre en regard du champ pour modifier un paramètre. Les valeurs correctes sont indiquées dans le tableau 1.

Option	Champ	Valeur
A	Serial Device	/dev/ttyS0 for COM1 /dev/ttyS1 for COM2
E	Bps/Par/Bits	Bps- 9600 Par- None Bits- 8 Stop bits- 1 (ou sélectionnez l'option 'Q')
F	**Hardware Flow Control**	Toggle- No
G	**Software Flow Control**	Toggle- No

Tableau 1. Paramètres de port série

Pour revenir au menu Configuration, appuyez sur **Entrée** ou **ECHAP**.

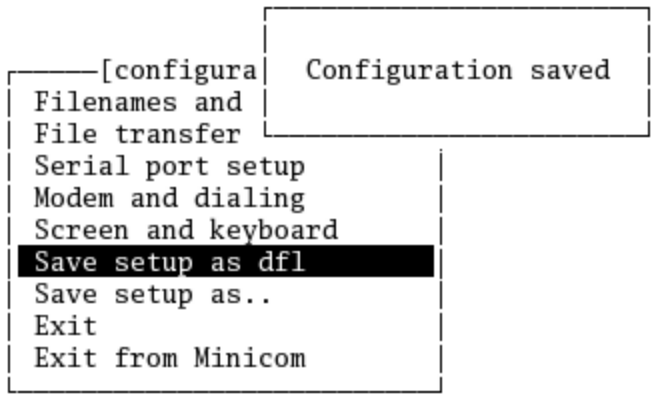


Figure 3. Fenêtre de configuration du port série

Reportez-vous à la figure 3. Sélectionnez **`Save setup as dfl`** (fichier par défaut). Les valeurs par défaut sont rechargées lors du redémarrage de Minicom.

Étape 3 : fermeture de Minicom

Lorsque vous avez terminé, fermez la session Minicom. Sélectionnez **`Exit from Minicom`**.

Étape 4 : redémarrage de la session Minicom

```
[root]# minicom <ENTER>
```

Lorsque la fenêtre de session s'affiche, appuyez sur la touche **Entrée**. Le routeur doit répondre. Cela indique que la connexion a été établie. En l'absence de connexion, procédez à un dépannage. Par exemple, vérifiez que le routeur est sous tension. Assurez-vous que le câble est bien connecté au port COM1 du PC et au port console du routeur. S'il n'y a toujours pas de connexion, demandez de l'aide au formateur.

Tâche 3 : exécution de commandes de base

Minicom est un utilitaire de communication série de type texte piloté par menus. Les commandes de base ne sont pas intuitives. Par exemple, les utilisateurs communiquent avec les périphériques distants dans la fenêtre de terminal. Toutefois, utilisez la combinaison **<CTRL> A** pour contrôler l'utilitaire. Pour obtenir de l'aide, appuyez sur **<CTRL> A**, puis sur **Z**.

```
                    Minicom Command Summary

          Commands can be called by CTRL-A <key>

               Main Functions                 Other Functions

| Dialing directory..D  run script (Go)....G | Clear Screen.......C
| Send files.........S  Receive files......R | cOnfigure Minicom..O
| comm Parameters....P  Add linefeed.......A | Suspend minicom....J
| Capture on/off.....L  Hangup.............H | eXit and reset.....X
| send break.........F  initialize Modem...M | Quit with no reset.Q
| Terminal settings..T  run Kermit.........K | Cursor key mode....I
| lineWrap on/off....W  local Echo on/off..E | Help screen........Z
|                                            | scroll Back........B

      Select function or press Enter for none.

             Written by Miquel van Smoorenburg 1991-1995
             Some additions by Jukka Lahtinen 1997-2000
             i18n by Arnaldo Carvalho de Melo 1998
```

Figure 4. Écran récapitulatif des commandes Minicom

Reportez-vous à la figure 4 pour consulter la liste des fonctions et des touches correspondantes. Pour quitter Minicom, appuyez sur **<CTRL> A,** suivi de **Q** ou **X**.

Tâche 4 : remarques générales

À travers ces travaux pratiques, vous avez appris à établir une connexion console à un routeur Cisco à l'aide de Minicom. L'accès aux commutateurs Cisco s'effectue de façon analogue.

Tâche 5 : remise en état

Sauf instructions contraires du formateur, mettez l'ordinateur hôte et le routeur hors tension. Retirez le câble de renversement.

Enlevez le matériel utilisé durant les travaux pratiques et préparez la salle pour le cours suivant.

10.7.1 : exercice d'intégration des compétences : planification d'un réseau et configuration d'une interface

Diagramme de topologie

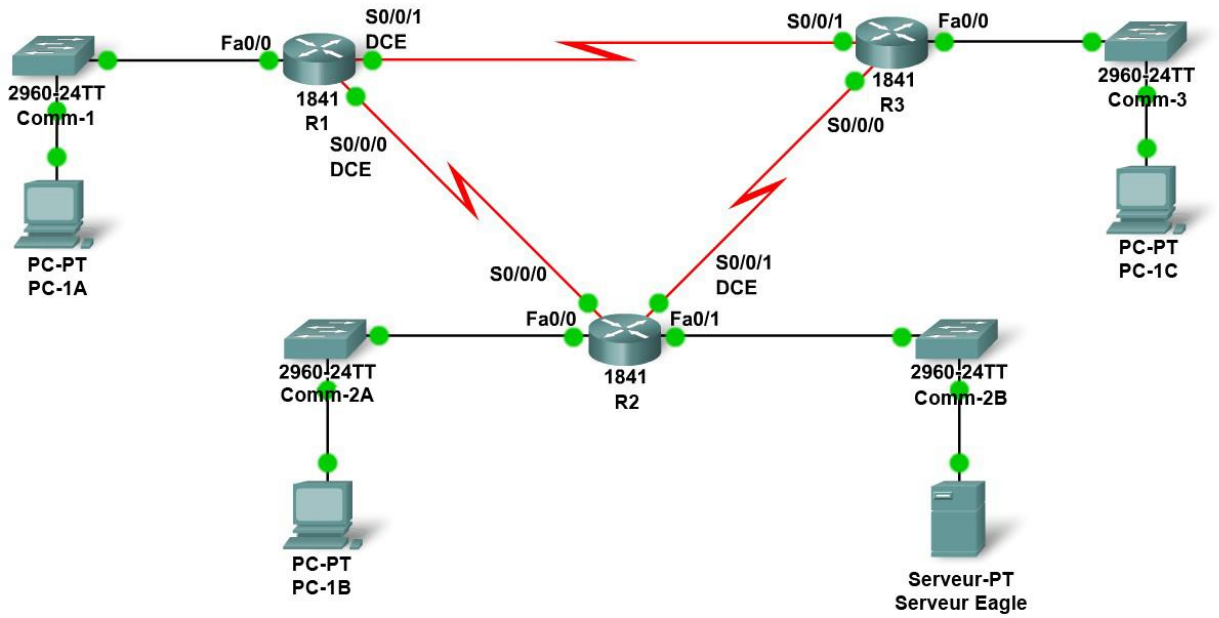


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	Fa0/0			N/A
	S0/0/0			N/A
	S0/0/1			N/A
R2	Fa0/0			N/A
	Fa0/1			N/A
	S0/0/0			N/A
	S0/0/1			N/A
R3	Fa0/0			N/A
	S0/0/0			N/A
	S0/0/1			N/A
PC -1A	La carte réseau			
PC -2A	La carte réseau			
PC -3A	La carte réseau			
Eagle_Server	La carte réseau			

Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Construire la topologie réseau
- Planifier les adresses IP
- Configurer les interfaces de routeur et de PC
- Tester le réseau

Contexte

Mettez en pratique vos compétences en matière de construction, de planification et de configuration de réseau. Les noms de périphériques et le routage ont déjà été configurés.

Tâche 1 : construction de la topologie réseau

Créez la topologie à l'aide des tableaux suivants et des périphériques présents dans le pool de périphériques.

Routeurs:

Nom d'hôte	Interface	Connecté à	Interface
R1	Fa0/0	SW-1	Fa0/1
R1	S0/0/0 (ETCD)	R2	S0/0/0
R1	S0/0/1 (ETCD)	R3	S0/0/1
R2	Fa0/0	SW-2A	Fa0/1
R2	S0/0/1 (ETCD)	R3	S0/0/0
R2	Fa0/1	SW-2B	Fa0/1
R3	Fa0/0	SW-3	Fa0/1

Commutateurs :

Nom d'hôte	Interface	Connecté à	Interface
SW-1	Fa0/2	PC -1A	FastEthernet
SW-2A	Fa0/2	PC -1B	FastEthernet
SW-2B	Fa0/2	Eagle_Server	FastEthernet
SW-3	Fa0/2	PC-1C	FastEthernet

Tâche 2 : création et attribution d'un modèle d'adressage

Vous êtes invité à utiliser l'espace d'adressage 192.168.1.0 /24. Sept réseaux complets sont nécessaires ; affectez les réseaux par ordre décroissant du nombre d'hôtes requis pour une utilisation efficace de l'espace d'adressage. Servez-vous des tableaux suivants pour créer un modèle d'adressage efficace :

Réseau local (LAN) :

Nom d'hôte	Interface	Nombre d'hôtes
R1	Fa0/0	60
R2	Fa0/0	10
	Fa0/1	30
R3	Fa0/0	7

Réseau étendu (WAN) :

Nom d'hôte	Adresse à affecter	Nombre d'hôtes
R1-R2	R1-Première adresse d'hôte	2
R1-R3	R1-Première adresse d'hôte	2
R2-R3	R2-Première adresse d'hôte	2

Attribuez les adresses IP en respectant les règles suivantes.

- Les PC utilisent la première adresse d'hôte du sous-réseau ; le serveur utilise l'avant-dernière adresse d'hôte de son sous-réseau.
- Tous les ports FastEthernet d'un routeur utilisent la dernière adresse d'hôte du sous-réseau concerné.
- La liaison R1-R2 utilisera le premier sous-réseau WAN, la liaison R1-R3 utilisera le second sous-réseau WAN et la liaison R2-R3 utilisera le troisième sous-réseau WAN. La fréquence d'horloge des interfaces ETCD de R1 et R2 doit être égale à 56 000.

Tâche 3 : configuration des interfaces

Configurez les interfaces des routeurs R1, R2 et R3, des PC et du serveur en fonction du modèle d'adressage présenté plus haut.

Tâche 4 : test de la connectivité

Assurez-vous que tous les PC sont en mesure d'envoyer une commande ping à leur passerelle, aux autres PC et au serveur.

Travaux pratiques 11.4.3.3 : constitution d'une documentation sur la latence d'un réseau avec ping

Schéma de la topologie

Objectifs pédagogiques

- Utiliser la commande **`ping`** pour documenter la latence du réseau.
- Calculer diverses statistiques à partir du résultat d'une capture de commande **`ping`**.
- Mesurer les effets de la latence à partir de datagrammes plus importants.

Contexte

Pour obtenir des statistiques de latence réseau réalistes, vous devez effectuer cet exercice sur un réseau actif. Vérifiez avec votre formateur s'il existe des restrictions de sécurité locales concernant l'utilisation de la commande **`ping`** sur le réseau.

L'ordinateur serveur de destination doit retourner des réponses ECHO, auquel cas la latence ne peut pas être calculée. Cette fonction est activée sur le pare-feu de certains ordinateurs. De plus, des réseaux privés bloquent les datagrammes ECHO de transit. Pour réaliser une expérience intéressante, choisissez une destination suffisamment distante. Par exemple, les destinations situées sur le même réseau local ou à quelques sauts peuvent retourner une faible latence non représentative. Soyez patient, et vous trouverez une destination appropriée.

L'objectif de ces travaux pratiques est de mesurer et d'évaluer la latence du réseau au fil du temps et à différentes périodes de la journée pour obtenir un échantillon représentatif de l'activité typique du réseau. Pour ce faire, il suffit d'analyser le délai de retour d'un ordinateur distant à l'aide de la commande **`ping`**.

L'analyse statistique du délai de retour s'effectuera à l'aide d'une application de feuille de calcul telle que Microsoft Excel. Les délais de retour, mesurés en millisecondes, seront résumés avec le calcul de la latence moyenne (moyenne), la valeur de latence située au centre de la gamme des points de latence (valeur médiane), ainsi qu'avec l'identification de la latence standard (valeur modale). L'annexe contient un graphique qui peut être soumis au formateur une fois terminé.

La latence sera également mesurée lors de l'augmentation de la taille du datagramme ICMP.

Scénario

Dans le graphique de topologie ci-dessus, le nuage de réseaux représente les périphériques et le câblage réseau entre l'ordinateur du participant et l'ordinateur-serveur de destination. Ce sont généralement ces périphériques qui génèrent une latence au niveau du réseau. Les ingénieurs réseau utilisent généralement des réseaux extérieurs à l'administration locale pour tester la connectivité vers les réseaux externes. La surveillance de la latence du chemin fournit une mesure de diligence administrative qui peut être utilisée dans la prise de décision lors de l'évaluation d'applications adaptées au déploiement d'un réseau étendu.

Cet exercice nécessite cinq jours de test. Chaque jour, trois tests seront effectués. Ces trois tests se répartiront de préférence le matin, en milieu de journée et en soirée. L'idée est de noter et de documenter les différences de latence qui surviennent à différentes périodes de la journée. Une fois terminé, nous disposerons de 15 ensembles de données.

Pour comprendre les effets de latence des diagrammes plus importants, les datagrammes ICMP seront envoyés avec des datagrammes de plus en plus importants et analysés.

Tâche 1 : utilisation de la commande `ping` pour documenter la latence du réseau.

Étape 1 : vérification de la connectivité entre l'ordinateur du participant et l'ordinateur-serveur de destination.

Pour vérifier la connectivité entre l'ordinateur du participant et l'ordinateur-serveur de destination, ouvrez une fenêtre de ligne de commande. Pour ce faire, cliquez sur Démarrer | Exécuter. Saisissez **cmd**, puis sélectionnez **OK**. Tentez d'envoyer une commande ping à une destination suffisamment distante, telle que `www.yahoo.com` :

```
C:\> ping -n 1 www.yahoo.com
Envoi d'une requête Ping sur www.yahoo-ht3.akadns.net [209.191.93.52] avec 32
octets de données :
Réponse de 209.191.93.52 : octets=32 temps=304 ms TTL=52
Statistiques Ping pour 209.191.93.5 :
      Paquets : Envoyés = 1, Reçus =      1, Perdus = 0 (perte 0%)
      Durée approximative des boucles en millisecondes :
      Minimum = 304ms, Maximum = 304ms , Moyenne = 304 ms
```

Utilisez la commande **ping /?** pour répondre aux questions suivantes :

Quelles sont les fonctions de l'option `-n` et de l'argument `1` ?

_____

_____

Quelle option et quel argument permettent de définir la taille par défaut sur 100 octets ? _____

Choisissez l'ordinateur-serveur de destination, puis indiquez son nom ici : _____

Utilisez la commande **ping** pour vérifier la connectivité avec la destination, puis indiquez les résultats obtenus :

Paquets envoyés	Paquets reçus	Paquets perdus

Si des paquets sont perdus, utilisez une autre destination, puis relancez le test.

Étape 2 : exécution d'un test de latence.

Saisissez la commande qui enverra 100 requêtes ECHO à la destination :

_____

Utilisez la commande ping pour envoyer 100 requêtes ECHO à votre destination. Une fois terminé, copiez les réponses dans le Bloc-notes. Pour ouvrir le Bloc-notes, cliquez sur Démarrer | Programmes | Accessoires | Bloc-notes. Enregistrez le nom du fichier sous la forme *jour-echantillon#*.txt, où : *jour* = jour de l'exécution du test (1-5) et *échantillon#* = période de l'échantillon (1-3).

Vous pouvez également rediriger le résultat vers un fichier. Pour ce faire, ajoutez > *jour-échantillon#*.txt à la fin de la commande **ping** . REMARQUE : l'écran de la ligne de commande reste vierge jusqu'à la fin de la commande.

Tâche 2 : calcul de diverses statistiques à partir du résultat d'une capture de commande ping.

Étape 1 : envoi du fichier texte dans l'application de feuille de calcul Excel.

Si cela n'est pas déjà fait, démarrez Microsoft Excel. Sélectionnez Fichier | Ouvrir. Utilisez l'option Parcourir pour atteindre le répertoire qui contient le fichier texte. Sélectionnez le nom du fichier, puis cliquez sur Ouvrir. Pour formater un fichier texte et l'utiliser dans Excel, assurez-vous que toutes les valeurs numériques sont séparées du texte. Dans l'étape 1 de l'Assistant d'importation de texte, sélectionnez Largeur fixe. Dans l'étape 2, suivez les instructions dans la fenêtre afin de séparer les valeurs numériques des valeurs texte. Reportez-vous à la figure 1.

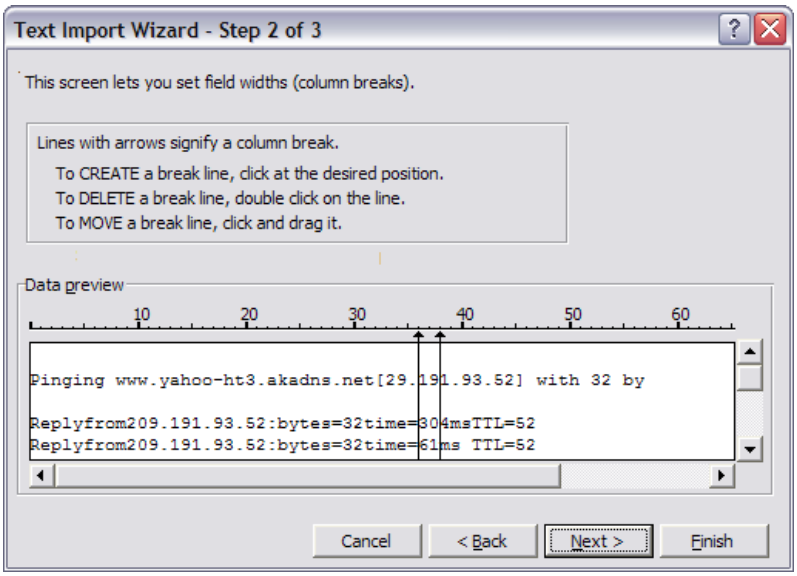


Figure 1. Assistant d'importation de texte Excel

Étape 2. Calcul des valeurs de latence moyenne, médiane et modale.

Une fois le formatage d'entrée satisfaisant, sélectionnez **Terminer**. Si la feuille de calcul possède des nombres dans plusieurs champs, corrigez manuellement les nombres. Une fois la feuille de calcul ouverte, formatez les colonnes de manière à les rendre plus lisibles. Une fois terminé, vous devriez disposer d'une feuille de calcul identique à celle de la figure 2.

	A	B	C	E	G	I
1				Octets	Retardez (ms	TTL
2	Réponse	de	209.191.93.52	32	304	52
3	Réponse	de	209.191.93.52	32	61	52
4	Réponse	de	209.191.93.52	32	56	52
5	Réponse	de	209.191.93.52	32	54	52
6	Réponse	de	209.191.93.52	32	65	52
7	Réponse	de	209.191.93.52	32	55	52

Figure 2. Feuille de calcul partielle correctement formatée.

Enregistrez le nombre de paquets abandonnés dans la colonne Paquets abandonnés de votre graphique. Les paquets abandonnés possèdent une valeur de latence importante et uniforme.

Les valeurs de latence doivent enfin être ordonnées (triées) lors du calcul des valeurs médiane et modale. Pour ce faire, utilisez les options de menu Données | Trier. Sélectionnez tous les champs de données. La figure 3 présente une feuille de calcul partielle sélectionnée et le menu Données | Trier ouvert. Si une ligne d'en-tête est sélectionnée, cochez la case d'option Ligne d'en-tête. Sélectionnez la colonne qui contient les valeurs de latence. Dans la figure 3, il s'agit de la colonne G. Cliquez sur OK une fois terminé.

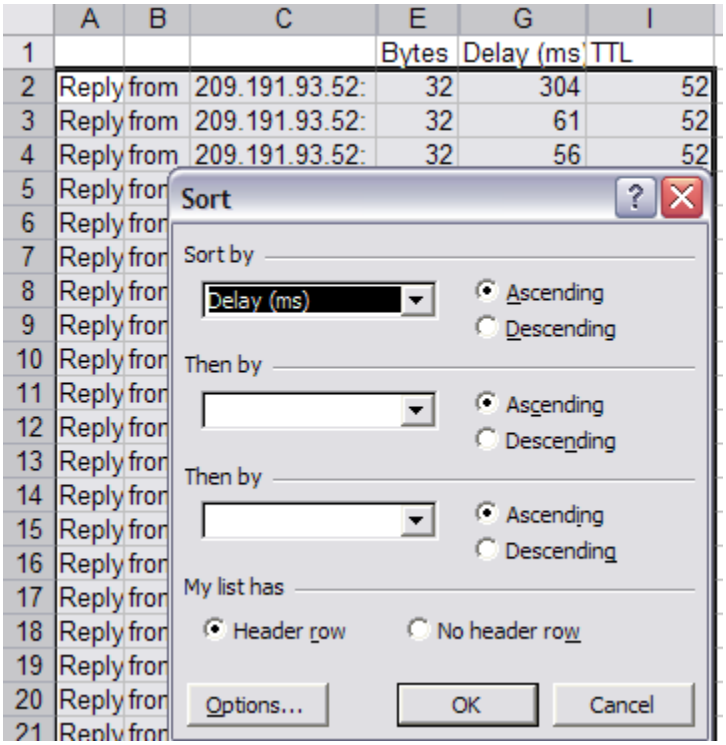


Figure 3. Tri de la colonne Latence.

La formule utilisée pour calculer la latence moyenne est la somme des latences divisée par le nombre de mesures. Dans l'exemple ci-dessus, il s'agit de la formule utilisée dans la cellule G102 : `=MOYENNE(G2:G101)`. Vérifiez si votre valeur moyenne correspond approximativement à la valeur affichée. Enregistrez ce nombre dans la colonne Moyenne de votre graphique.

La formule utilisée pour calculer la latence médiane (ou valeur de latence située au centre de la plage ordonnée) est similaire à la formule moyenne ci-dessus. La formule de la valeur médiane utilisée dans la cellule G103 est `=MEDIANE(G2:G101)`. Vérifiez si la valeur médiane est similaire à celle affichée au milieu de la plage de données. Enregistrez ce nombre dans la colonne Médiane de votre graphique.

La formule utilisée pour calculer la latence modale (ou valeur de latence la plus fréquente) est également similaire. La formule de la valeur modale utilisée dans la cellule G104 est `=MODE(G2:G101)`. Vérifiez si la valeur modale est la valeur la plus fréquente dans la plage de données. Enregistrez ce nombre dans la colonne Mode de votre graphique.

La nouvelle feuille de calcul peut être enregistrée ou abandonnée, le cas échéant, mais le fichier texte de données doit être conservé.

Tâche 3 : mesure des effets de latence à partir de datagrammes plus importants.

Pour déterminer si les diagrammes plus importants influent sur la latence, des requêtes ÉCHO de plus en plus importantes sont envoyées à la destination. Dans cette analyse, 20 datagrammes sont incrémentés de 100 octets par requête **`ping`**. Une feuille de calcul est créée avec les résultats de la réponse. Un graphique comparant la taille et la latence est également généré.

Étape 1 : exécution d'un test de latence de taille variable.

Le plus simple consiste à utiliser la commande de boucle FOR de Windows. La syntaxe est la suivante :

```
FOR /L %%variable IN (début,pas,fin) DO commande [paramètres]
```

L'ensemble est une séquence de chiffres allant de début à fin, incrémenté de pas. Ainsi (1,1,5) génère la séquence 1 2 3 4 5 et (5,-1,1) génère la séquence (5 4 3 2 1)

Dans la commande suivante, *`destination`* représente la destination. Saisissez la commande suivante :

`FOR /L %i IN (100,100,2000) DO ping -n 1 -l %i` ***`destination`***

Copiez le résultat dans le Bloc-notes, puis enregistrez le fichier sous le nom `variablesizedelay.txt`.

Pour rediriger le résultat vers un fichier, utilisez l'opérateur d'ajout de redirection **>>**, comme illustré ci-dessous. L'opérateur de redirection normal (**>**) écrase le fichier à chaque exécution de la commande ping et n'enregistre que la dernière réponse. REMARQUE : l'écran de ligne de commande reste vierge jusqu'à la fin de la commande :

`FOR /L %i IN (100,100,2000) DO ping -n 1 -l %i` ***`destination`*** **`>> variablesizedelay.txt`**

Le résultat d'une ligne est affiché ci-dessous. Les 20 réponses ont le même format :

```
C:\> FOR /L %i IN (100,100,2000) DO ping –n 1 –l %i www.yahoo.com

C:\> ping -n 1 -l 100 www.yahoo.com

Envoi d'une requête Ping sur www.yahoo-ht3.akadns.net [209.191.93.52]
avec 100 octets de données :
Réponse de 209.191.93.52 : bytes=100 time=383 ms TTL=52

Statistiques Ping pour 209.191.93.52 :
    Paquets : Envoyés = 1, Reçus = 1, Perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 383 ms, Maximum = 383 ms, Moyenne = 383 ms
```

Étape 2 : envoi du fichier texte dans l'application de feuille de calcul Excel.

Ouvrez le nouveau fichier texte dans Excel. Reportez-vous à la figure 4.

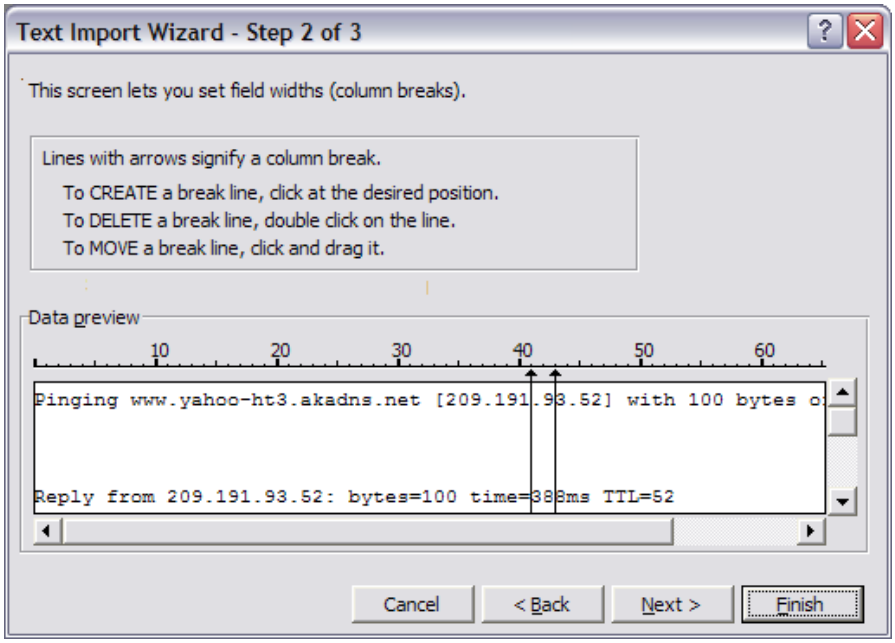
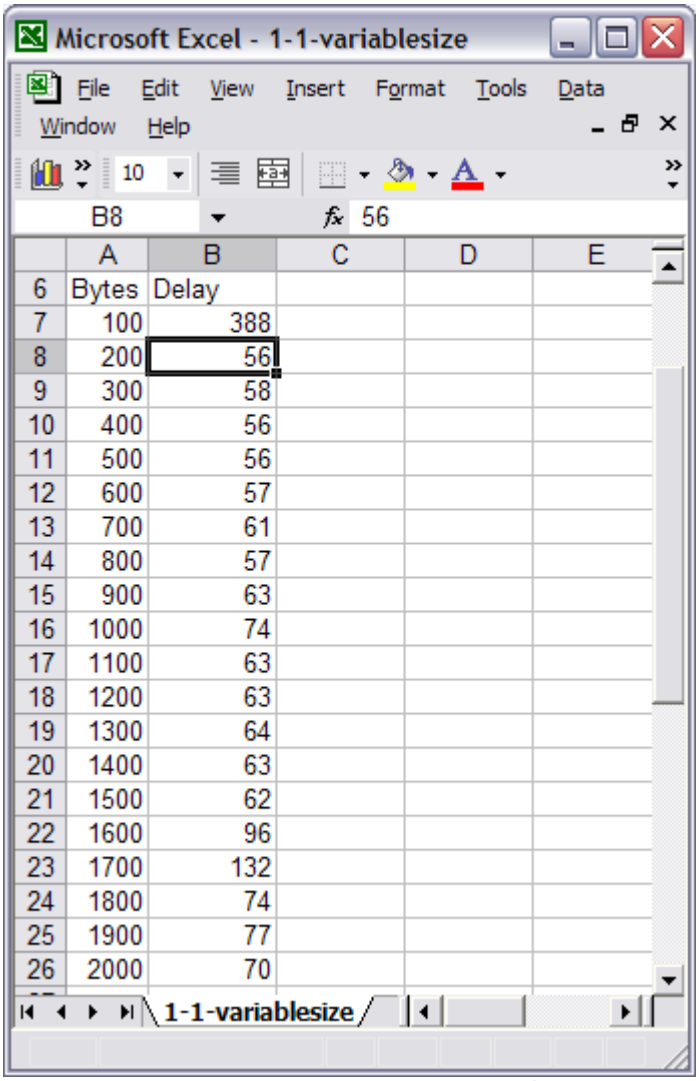


Figure 4. Assistant d'importation de texte Excel

La différence entre ce fichier et le fichier précédent se trouve au niveau du fichier de taille variable, qui possède bien plus d'informations que nécessaire.

Étape 3 : formatage de la feuille de calcul.

Nettoyez les données de la feuille de calcul, puis organisez-les en deux colonnes : Octets et Latence. Une fois terminé, la feuille de calcul doit être identique à celle de la figure 5.

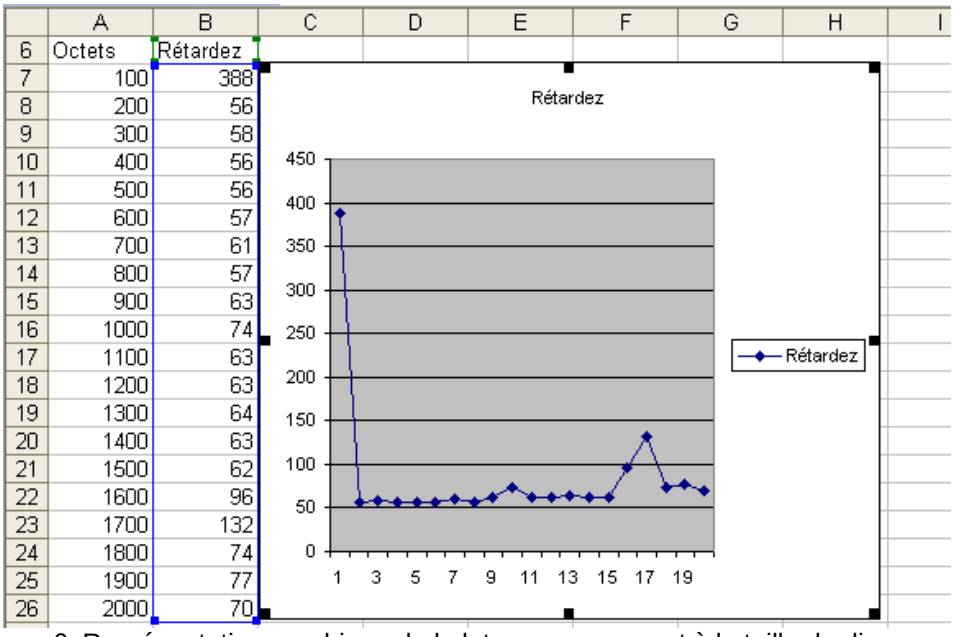


	A	B	C	D	E
6	Bytes	Delay			
7	100	388			
8	200	56			
9	300	58			
10	400	56			
11	500	56			
12	600	57			
13	700	61			
14	800	57			
15	900	63			
16	1000	74			
17	1100	63			
18	1200	63			
19	1300	64			
20	1400	63			
21	1500	62			
22	1600	96			
23	1700	132			
24	1800	74			
25	1900	77			
26	2000	70			

Figure 5. Feuille de calcul formatée.

Étape 3 : création d'un graphique de données.

Sélectionnez les données de la colonne Latence. Sélectionnez Insertion | Graphique. Vous pouvez utiliser différents types de graphique pour afficher les données de latence. Certains sont plus appropriés que d'autres. Un graphique se doit d'être clair, mais une place doit être laissée à la créativité individuelle. Le graphique de la figure 6 représente un graphique à courbes empilées.



	A	B
6	Octets	Rétardez
7	100	388
8	200	56
9	300	58
10	400	56
11	500	56
12	600	57
13	700	61
14	800	57
15	900	63
16	1000	74
17	1100	63
18	1200	63
19	1300	64
20	1400	63
21	1500	62
22	1600	96
23	1700	132
24	1800	74
25	1900	77
26	2000	70

Figure 6. Représentation graphique de la latence par rapport à la taille du diagramme.

Une fois terminé, enregistrez votre feuille de calcul et votre graphique, puis soumettez-les à votre formateur avec l'analyse de latence finale.

Que peut-on conclure au sujet de la latence lors de l'envoi de datagrammes plus importants sur le réseau ?

_____

_____

Tâche 4 : Remarques générales

La commande **`ping`** peut fournir des informations importantes sur la latence du réseau. Une analyse de latence attentive sur plusieurs jours et à différentes périodes de la journée peut informer l'ingénieur réseau de performances réseau changeantes. Par exemple, les périphériques réseau peuvent être saturés à certaines périodes de la journée, augmentant ainsi la latence du réseau. Dans ce cas, les transferts de données courantes doivent être programmés en dehors des périodes de pointe où la latence est moins importante. En outre, de nombreux utilisateurs utilisent des applications peer-to-peer telles que KaZaA et Napster. Lorsque ces applications de partage de fichiers sont actives, une quantité considérable de bande passante ne peut être utilisée par les applications vitales. Si des latences sont provoquées par des événements internes à l'entreprise, des outils d'analyse du réseau peuvent permettre d'en déterminer la source et de prendre les mesures appropriées. Lorsque la cause se situe dans des réseaux externes qui ne sont pas contrôlés par l'entreprise, s'abonner à un fournisseur de services Internet différent ou supplémentaire peut s'avérer judicieux.

Tâche 5 : confirmation

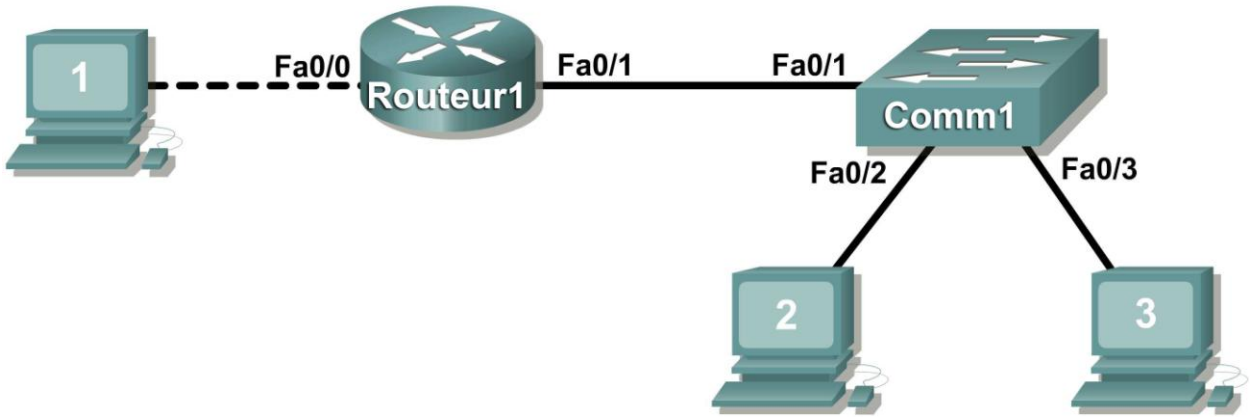
Si possible, téléchargez un fichier important et effectuez un test de latence séparé lors du téléchargement du fichier. Rédigez une analyse d'un ou deux paragraphes comparant ces résultats de latence à une mesure effectuée sans le téléchargement.

Annexe

NOM : _____				**Documentation de la latence du réseau**		
Adresse IP source : _____		**Adresse IP de destination :_____**		**TTL : _____**		
Analyse statistique de la latence du réseau avec des datagrammes de 32 octets						
Jour (1-5)	**Date (jj/mm/aaaa)**	**Heure (hh:mm)**	**VALEUR MOYENNE**	**VALEUR MÉDIANE**	**VALEUR MODALE**	**Paquets abandonnés**
1						
2						
3						
4						
5						

Travaux pratiques 11.5.1 : configuration de base d'un périphérique Cisco

Diagramme de topologie



Objectifs pédagogiques

- Définir les paramètres de configuration globale d'un routeur Cisco
- Configurer l'accès par mot de passe à un routeur Cisco
- Configurer les interfaces d'un routeur Cisco
- Enregistrer le fichier de configuration d'un routeur
- Configurer un commutateur Cisco

Contexte

Matériel	Qté	Description
Routeur Cisco	1	Inclus dans l'équipement de travaux pratiques CCNA
Commutateur Cisco	1	Inclus dans l'équipement de travaux pratiques CCNA
*Ordinateur (hôte)	1	Ordinateur de travaux pratiques
Câble console (de renversement)	1	Relie l'ordinateur hôte 1 au port console du routeur
Câble de croisement UTP de catégorie 5	1	Relie l'ordinateur hôte 1 à l'interface Fa0/0 de réseau local du routeur
Câble direct	3	Relie les ordinateurs hôtes au commutateur et le commutateur au routeur

Tableau 1. Équipement et matériel nécessaires pour ces travaux pratiques

Regroupez l'équipement et les câbles nécessaires. Pour configurer les travaux pratiques, vérifiez que vous disposez bien de l'équipement répertorié dans le tableau 1.

Les tâches de configuration courantes incluent la définition du nom d'hôte, des mots de passe et de la bannière MOTD.

La configuration des interfaces est extrêmement importante. En plus d'attribuer une adresse IP de couche 3, entrez une description du délai de dépannage des vitesses de connexion à destination.

Les modifications apportées à la configuration prennent immédiatement effet.

Elles doivent être enregistrées dans la mémoire NVRAM pour être conservées lors d'un redémarrage.

Il est également possible d'enregistrer ces modifications hors ligne dans un fichier texte à des fins d'audit ou dans le cadre d'un remplacement de périphérique.

La configuration d'un commutateur Cisco IOS s'apparente à la configuration d'un routeur Cisco IOS.

Scénario

Dans le cadre de ces travaux pratiques, les participants vont configurer des paramètres courants sur un routeur et un commutateur Cisco.
À partir de l'adresse IP 198.133.219.0/24, avec 4 bits empruntés pour les sous-réseaux, complétez le tableau ci-dessous avec les informations suivantes.

Astuce : renseignez le numéro de sous-réseau, puis l'adresse d'hôte. Il sera facile de calculer les paramètres des adresses en indiquant le numéro de sous-réseau en premier.

Nombre maximum de sous-réseaux : _____

Nombre d'hôtes utilisables par sous-réseau : _____

	Adresse IP :		Masque de sous-réseau :	
#	Sous-réseau	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion
0				

Avant de poursuivre, vérifiez vos adresses en compagnie du formateur. C'est lui qui attribuera les sous-réseaux.

Tâche 1 : définition des paramètres de configuration globale d'un routeur Cisco

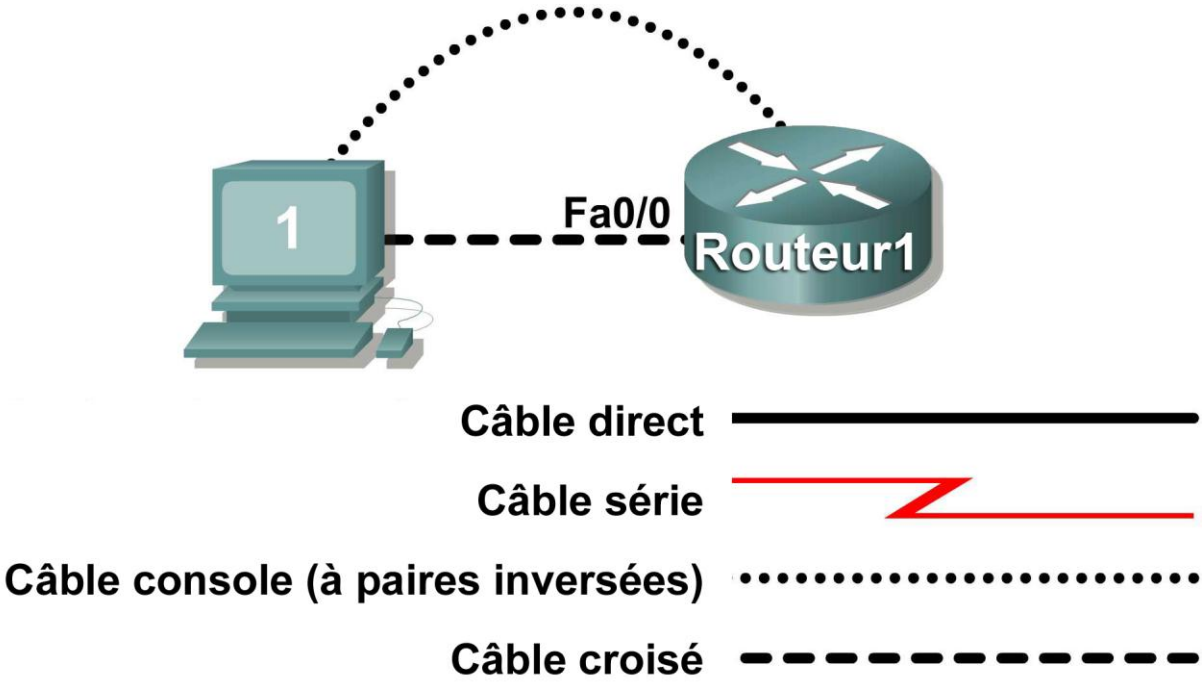


Figure 1. Câblage des travaux pratiques.

Étape 1 : connexion physique des périphériques

Reportez-vous à la figure 1. Connectez le câble console (ou de renversement) au port console du routeur. Connectez l'autre extrémité du câble au port COM1 de l'ordinateur hôte avec un adaptateur DB-9 ou DB-25. Reliez le câble de croisement à la carte réseau de l'ordinateur hôte et à l'interface Fa0/0 du routeur. Branchez un câble droit entre l'interface Fa0/1 du routeur et l'une des interfaces du commutateur (1-24).

Assurez-vous que l'ordinateur hôte, le commutateur et le routeur sont sous tension.

Étape 2 : connexion de l'ordinateur hôte au routeur via HyperTerminal

Dans la barre des tâches Windows, démarrez le programme HyperTerminal en cliquant sur Démarrer | Programmes | Accessoires | Communications | HyperTerminal.

Configurez HyperTerminal avec les paramètres appropriés :

Description de la connexion
Nom : **TP 11_2_11**
Icône : **au choix**

Connexion
Se connecter en utilisant : **COM1** (ou un port COM approprié)

Propriétés de COM1
Bits par seconde : **9600**

```
          Bits de données :    8
                  Parité :    Aucun
             Bits d'arrêt :    1
          Contrôle de flux :    Aucun
```

Lorsque la fenêtre de session HyperTerminal apparaît, appuyez sur la touche **Entrée** jusqu'à obtenir une réponse du routeur.

Si le terminal du routeur est en mode de configuration, sortez en tapant **NO**.

```
Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!
Router>
```

Lorsqu'il est en mode d'exécution privilégié et qu'une commande est mal libellée ou non reconnue, le routeur tente de la traduire en nom de domaine. Aucun serveur de domaines n'étant configuré, un délai d'attente devra être observé, le temps que la requête soit révolue. Ce délai peut varier de plusieurs secondes à plusieurs minutes. Pour ne pas attendre, appuyez simultanément sur les touches **<CTRL><MAJ>6**, relâchez-les, puis appuyez sur **x** :

```
Router>enabel
Translating "enabel"...domain server (255.255.255.255) %

Appuyez sur les touches <CTRL><MAJ>6, relâchez-les, et appuyez sur x


Name lookup aborted

Router>
```

Passez du mode d'exécution utilisateur au mode d'exécution privilégié :

```
Router> enable
Router#
```

Examinez un fichier de configuration intègre à l'aide de la commande d'exécution privilégiée **show running-config**. Si un fichier de configuration a été enregistré précédemment, il doit être supprimé. L'annexe 1 décrit la configuration par défaut d'un routeur. Selon le modèle et la version de l'IOS du routeur, votre configuration peut varier légèrement. Toutefois, elle ne doit pas comporter de mots de passe ni d'adresses IP configurés. Si votre routeur ne présente pas de configuration par défaut, demandez à votre formateur de supprimer la configuration.

Étape 3 : définition du paramètre de configuration globale hostname (nom d'hôte)

Quelles sont les deux commandes qui permettent de quitter le mode d'exécution privilégié ? _____
Quelle est la commande abrégée qui permet de passer en mode d'exécution privilégié ? _____

Examinez les différents modes de configuration pouvant être activés à l'aide de la commande **configure**. Dressez la liste des modes de configuration et leur description :

_____

_____

_____

_____

_____

_____

Passez du mode d'exécution privilégié au mode de configuration globale :

```
Router# configuration terminal
Router(config)#
```

Quelles sont les trois commandes qui permettent de quitter le mode de configuration globale et de repasser en mode d'exécution privilégié ?

_____

_____

Quelle est la commande abrégée qui permet de passer en mode de configuration globale ?

__ _____

Attribuez au périphérique le nom d'hôte (hostame) Router1 :

```
router(config)# hostname Router1
             Router1(config)#
```

Comment supprimer le nom d'hôte ?

_____

_____

Étape 4 : configuration de la bannière MOTD

Dans les réseaux de production, le contenu de la bannière peut avoir des conséquences juridiques importantes pour l'organisation. Par exemple, un tribunal peut considérer qu'un message amical du type « Bienvenue » autorise un pirate informatique à pirater un routeur. Une bannière doit comporter des informations sur l'autorisation, les sanctions en cas d'accès non autorisé, la journalisation des connexions et les lois applicables. La politique de la société en matière de sécurité doit figurer dans tous les messages affichés sous forme de bannière.

Créez une bannière MOTD appropriée. Seuls les administrateurs système de la société ABC bénéficient d'un droit d'accès. Tout accès non autorisé fera l'objet de poursuites et les paramètres de connexion seront enregistrés.

_____

_____

_____

_____

_____

_____

Examinez les différents modes de bannière utilisables. Dressez la liste des modes de bannière et leur description :

Router1(config)# banner ?

_____

_____

_____

_____

_____

_____

Choisissez un caractère de fin qui n'apparaîtra pas dans le texte du message. _____

Configurez la bannière MOTD La bannière MOTD s'affiche pour toutes les connexions avant l'invite d'ouverture de session. Utilisez le caractère de fin sur une ligne vide pour terminer la saisie MOTD :

```
Router1(config)# banner motd %
Enter TEXT message.  Faites-le suivre du caractère '%'
***Vous êtes connecté à un périphérique réseau d'ABC. L'accès n'est accordé
qu'aux administrateurs système actuels de la société ABC moyennant une
approbation écrite préalable. ***

*** Tout accès non autorisé fera l'objet de poursuites. ***

*** Les connexions sont systématiquement enregistrées. ***

%
Router1(config)#
```

Quelle est la commande de configuration globale qui permet de supprimer la bannière MOTD ?

_____

Tâche 2 : configuration de l'accès par mot de passe à un routeur Cisco

Les mots de passe d'accès sont définis pour le mode d'exécution privilégié et les points d'accès utilisateur tels que les lignes console, auxiliaires et virtuelles. Le mot de passe du mode d'exécution privilégié est le mot de passe le plus important, car c'est lui qui contrôle l'accès au mode de configuration.

Étape 1 : configuration du mot de passe du mode d'exécution privilégié

Cisco IOS prend en charge deux commandes permettant de définir l'accès au mode d'exécution privilégié. L'une de ces commandes, **enable password**, intègre une cryptographie faible et ne doit jamais être utilisée si la commande **enable secret** est disponible. La commande **enable secret** utilise un algorithme de hachage cryptographique MD5 très sûr. « Autant que l'on sache, il est impossible de récupérer un mot de passe enable secret en se basant sur le contenu d'un fichier de configuration (sauf dans le cas d'une intrusion classique dans un dictionnaire) », affirme-t-on chez Cisco. La protection par mot de passe repose sur l'algorithme du mot de passe et sur le mot de passe. . Dans les environnements de production, il est recommandé d'utiliser systématiquement des mots de passe forts. Ceux-ci se composent d'au moins neuf caractères, parmi lesquels figurent des lettres majuscules et minuscules, des chiffres et des symboles. Dans un environnement de travaux pratiques, nous utilisons des mots de passe faibles.

Attribuez au mot de passe du mode d'exécution privilégié la valeur **cisco**.

```
Router1(config)# enable secret cisco
Router1(config)#
```

Étape 2 : configuration du mode de passe de console

Attribuez au mot de passe d'accès à la console la valeur **class**. Le mot de passe de console régit l'accès de la console au routeur.

```
Router1(config)# line console 0
Router1(config-line)# password class
Router1(config-line)# login
```

Quelle est la commande qui permet de supprimer le mot de passe de console ? ____ _____

Étape 3 : configuration du mot de passe de ligne virtuelle

Attribuez au mot de passe d'accès à la ligne virtuelle la valeur **class**. Le mot de passe de ligne virtuelle contrôle l'accès au routeur via Telnet. Dans les toutes premières versions de Cisco IOS, il n'était possible de définir que cinq lignes virtuelles (0 à 4). Dans les versions récentes, ce chiffre est plus élevé. L'accès à cette ligne virtuelle est bloqué, sauf si vous avez défini un mot de passe Telnet.

```
Router1(config-line)# line vty 0 4
Router1(config-line)# password class
Router1(config-line)# login
```

Les commandes qui permettent de quitter le mode de configuration de ligne sont au nombre de trois :

Commande	Effet
	Vous fait repasser en mode de configuration globale.
	Vous quittez le mode configuration et repassez en mode d'exécution privilégié.

Exécutez la commande **exit**. Quelle est l'invite du routeur ? Quel est le mode ?
`Router1(config-line)# exit`

_____

_____

Exécutez la commande **end**. Quelle est l'invite du routeur ? Quel est le mode ?

_____

_____

Tâche 3 : configuration des interfaces d'un routeur Cisco

Toutes les interfaces câblées doivent contenir des informations sur la connexion. Sur les versions plus récentes de Cisco IOS, la description peut contenir au maximum 240 caractères.

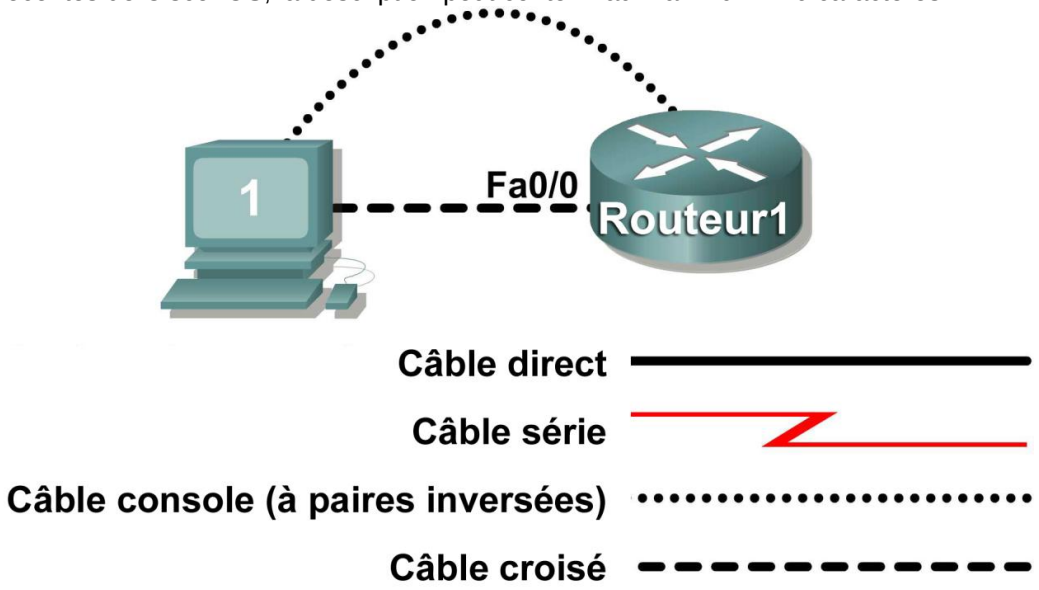


Figure 2. Topologie physique des travaux pratiques.

La figure 2 illustre une topologie réseau dans laquelle un ordinateur hôte est connecté au routeur Router1 par le biais de l'interface Fa0/0.

Inscrivez vos numéro et masque de sous-réseau :
La première adresse IP sert à configurer le réseau local de l'ordinateur hôte. Inscrivez la première adresse IP : _____

La dernière adresse IP sert à configurer l'interface fa0/0 du routeur. Inscrivez la dernière adresse IP :

_____

Étape 1 : configuration de l'interface fa0/0 du routeur

Décrivez brièvement les connexions du routeur Router1 :
Fa0/0 ->

_____

Appliquez la description à l'interface du routeur à l'aide de la commande de configuration d'interface (**description**) :

```
Router1(config)# interface fa0/0
Router1(config-if)# description Connexion à l'hôte 1 avec un câble de
croisement
Router1(config-if)# ip address masque d'adresse
Router1(config-if)# no shutdown
Router1(config-if)# end
Router1#
```

Recherchez l'interface à activer :

```
*Mar 24 19:58:590,602: %LINEPROTO-5-UPDOWN: Protocole de ligne sur l'interface
FastEthernet0/0, activée
```

Étape 2 : configuration de l'interface Fa0/1 du routeur

Décrivez brièvement les connexions du routeur Router1 :
Fa0/1 ->

_____

Appliquez la description à l'interface du routeur à l'aide de la commande de configuration d'interface (**description**) :

```
Router1(config)# interface fa0/1
Router1(config-if)# description Connexion au commutateur avec un câble direct
Router1(config-if)# ip address masque d'adresse
Router1(config-if)# no shutdown
Router1(config-if)# end
Router1#
```

Recherchez l'interface à activer :

```
*Mar 24 19:58:590,602: %LINEPROTO-5-UPDOWN: Protocole de ligne sur
l'interface FastEthernet0/1, activée
```

Étape 3 : configuration de l'ordinateur hôte

Configurez l'ordinateur hôte pour prendre en charge la connectivité sur le réseau local. Pour rappel, la fenêtre de configuration de réseau local est accessible via Démarrer | Panneau de configuration | Connexions réseau. Cliquez avec le bouton droit de la souris sur l'icône du réseau local, puis sélectionnez Propriétés. Mettez en surbrillance le champ Protocole Internet, puis sélectionnez Propriétés. Complétez les champs suivants :

Adresse IP : la première adresse d'hôte _____
Masque de sous-réseau : le masque de sous-réseau _____
Passerelle par défaut : l'adresse IP du routeur _____

Cliquez sur OK, puis sur Fermer. Ouvrez une fenêtre de terminal, puis vérifiez les paramètres réseau à l'aide de la commande **ipconfig**.

Étape 4 : vérification de la connectivité du réseau

Utilisez la commande **ping** pour vérifier la connectivité réseau avec le routeur. Si les réponses à la commande ping ne sont pas concluantes, dépannez la connexion :

Quelle est la commande Cisco IOS permettant de vérifier l'état de l'interface ? _____

Quelle est la commande Windows qui permet de vérifier la configuration d'un ordinateur hôte ?
_____

Quel est le type de câble de réseau local qu'il convient d'utiliser entre l'hôte 1 et le routeur Router1 ?
_____

Tâche 4 : enregistrement du fichier de configuration du routeur

Dans Cisco IOS, le stockage de la configuration en mémoire vive (RAM) correspond à la configuration en cours (running-config), tandis que le stockage de la configuration en mémoire vive non volatile (NVRAM) fait référence à la configuration initiale (startup-config). Pour la conserver lors des réamorçages ou des redémarrages, vous devez copier la configuration dans la mémoire vive non volatile (NVRAM). Toutefois, cela ne se produit pas automatiquement. La mémoire NVRAM doit être mise à jour manuellement après toute modification.

Étape 1 : comparaison des configurations RAM et NVRAM

Utilisez la commande **show** de Cisco IOS pour afficher les configurations RAM et NVRAM. La configuration s'affiche dans un écran à la fois. La ligne qui affiche " `-- more --` " indique qu'il y a davantage d'informations. La liste suivante décrit les fonctions des touches :

Touche	Description
<ESPACE>	Affiche la page suivante
<RETOUR>	Affiche la ligne suivante
Q	Quitter
<CTRL> c	Quitter

Écrivez une commande abrégée permettant d'afficher le contenu de la configuration NVRAM.
Affichez le contenu de la mémoire NVRAM. L'absence de résultat indique que la NVRAM ne contient pas de configuration enregistrée :

```
Router1# show startup-config
 startup-config is not present
Router1#
```

Affichez le contenu de la mémoire RAM.

```
Router1#show running-config
```

Répondez aux questions suivantes en fonction du résultat :

Quelle est la taille du fichier de configuration ? _____

Quel est le mot de passe « enable secret » ? _____

Votre bannière MOTD contient-elle les informations que vous avez saisies précédemment ?
_____

Vos descriptions d'interface contiennent-elles les informations que vous avez saisies précédemment ?
_____

Écrivez une commande abrégée pour afficher le contenu de la configuration RAM. _____

Étape 2 : enregistrement de la configuration RAM en mémoire NVRAM

Pour qu'une configuration puisse être utilisée lors du prochain redémarrage ou réinitialisation du routeur, elle doit être enregistrée en mémoire NVRAM. Enregistrez la configuration RAM en mémoire NVRAM :

```
Router1# copy running-config startup-config
Destination filename [startup-config]? <ENTRÉE>
Building configuration...
[OK]
Router1#
```

Écrivez une commande abrégée permettant de copier la configuration RAM dans la mémoire NVRAM.

_____

Examinez le contenu de la mémoire NVRAM, puis vérifiez que la configuration est identique à celle qui est enregistrée en mémoire RAM.

Tâche 5 : configuration d'un commutateur Cisco

Un commutateur Cisco IOS se configure (fort heureusement) de la même manière qu'un routeur Cisco IOS. Apprendre les commandes IOS est utile, car elles sont similaires à celles de nombreux périphériques et versions d'IOS différents.

Étape 1 : connexion de l'hôte au commutateur

Connectez le câble console (ou de renversement) au port console du commutateur. Assurez-vous que le commutateur est sous tension. Dans Hyperterminal, appuyez sur Entrée jusqu'à obtenir une réponse du commutateur.

Étape 2 : définition du paramètre de configuration globale hostname (nom d'hôte)

L'annexe 2 fournit un exemple de configuration par défaut. Selon le modèle et la version de l'IOS du routeur, votre configuration peut varier légèrement. Toutefois, aucun mot de passe ne doit avoir été configuré. Si votre routeur ne présente pas de configuration par défaut, demandez à votre formateur de supprimer la configuration.

Passez du mode d'exécution utilisateur au mode de configuration globale :

```
Switch> en
Switch# config t
Switch(config)#
```

Attribuez au périphérique le nom d'hôte (hostame) Switch1 :

```
Switch(config)# hostname Switch1
Switch1(config)#
```

Étape 3 : configuration de la bannière MOTD

Créez une bannière MOTD appropriée. Seuls les administrateurs système de la société ABC bénéficient d'un droit d'accès. Tout accès non autorisé fera l'objet de poursuites et les informations de connexion seront enregistrées.

Configurez la bannière MOTD. La bannière MOTD s'affiche pour toutes les connexions avant l'invite d'ouverture de session. Utilisez le caractère de fin sur une ligne vide pour terminer la saisie MOTD. Si vous avez besoin d'aide, examinez l'étape correspondante de la procédure de configuration d'une bannière MOTD.

```
Switch1(config)# banner motd %
```

Étape 4 : configuration du mot de passe du mode d'exécution privilégié

Attribuez au mot de passe du mode d'exécution privilégié la valeur **cisco**.

```
Switch1(config)# enable secret cisco
Switch1(config)#
```

Étape 5 : configuration du mode de passe de console

Attribuez au mot de passe d'accès à la console la valeur **class**.

```
Switch1(config)# line console 0
Switch1(config-line)# password class
Switch1(config-line)# login
```

Étape 6 : configuration du mot de passe de ligne virtuelle

Attribuez au mot de passe d'accès à la ligne virtuelle la valeur **class**. Il est possible de configurer 16 lignes virtuelles sur un commutateur Cisco IOS, de 0 à 15.

```
Switch1(config-line)# line vty 0 15
Switch1(config-line)# password class
Switch1(config-line)# login
```

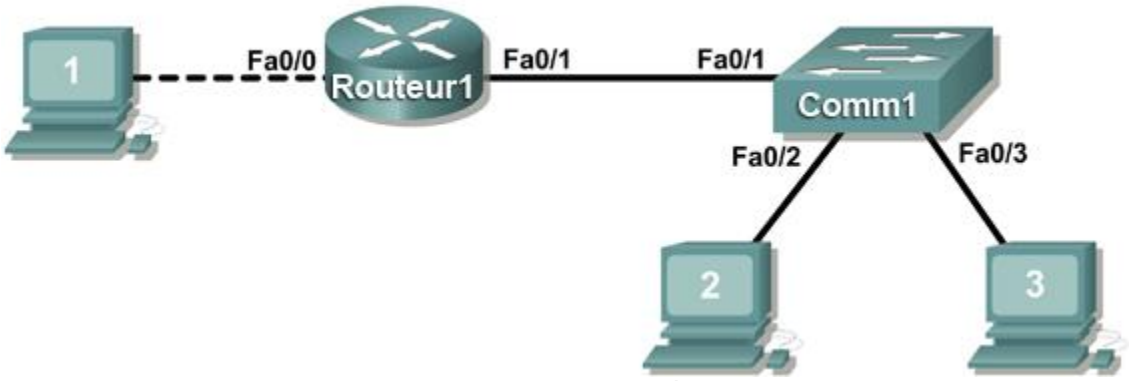


Figure 3. Topologie de réseau.

Étape 7 : configuration des interfaces

La figure 3 décrit la topologie d'un réseau, dans laquelle Router1 est connecté à l'interface Fa0/1 de Switch1. L'interface Fa0/2 de Switch1 est reliée à l'ordinateur hôte 2 et l'interface Fa0/3 est connectée à l'ordinateur hôte 3.

Décrivez brièvement les connexions du commutateur Switch1 :

Interface de Router1	Description
Fa0/1	
Fa0/2	
Fa0/3	

Appliquez les descriptions à l'interface du commutateur à l'aide de la commande de configuration d'interface **description** :

```
Switch1(config)# interface fa0/1
Switch1(config-if)# description Connexion à Router1
Switch1(config)# interface fa0/2
Switch1(config-if)# description Connexion à l'ordinateur hôte 2
Switch1(config)# interface fa0/3
Switch1(config-if)# description Connexion à l'ordinateur hôte 3
Switch1(config-if)# end
Switch1#
```

Étape 8 : enregistrement de la configuration RAM en mémoire NVRAM

Pour utiliser une configuration lors du prochain redémarrage ou réinitialisation du commutateur, vous devez l'enregistrer en mémoire NVRAM. Enregistrez la configuration RAM en mémoire NVRAM :

```
Switch1# copy run start
Destination filename [startup-config]? <ENTRÉE>
Building configuration...
[OK]
Switch1#
```

Examinez le contenu de la mémoire NVRAM, puis vérifiez que la configuration est identique à celle qui est enregistrée en mémoire RAM.

Tâche 6 : remarques générales

Lorsque vous maîtriserez ces commandes, vous serez vite capable de configurer un routeur ou un commutateur Cisco IOS. Si, dans un premier temps, il est normal de s'aider de notes pour configurer un périphérique, un ingénieur réseau professionnel n'a pas besoin d'« antisèche » pour effectuer des tâches de configuration courantes. Le tableau suivant répertorie les commandes traitées dans ces travaux pratiques :

Objectif	Commande
Passer en mode de configuration globale	**configure terminal** Exemple : Router> **enable** Router# configure terminal Router(config)#
Indiquer le nom du routeur	**hostname** *name* Exemple : Router(config)# **hostname Router1** Router(config)#
Définir un mot de passe chiffré pour empêcher tout accès non autorisé au mode d'exécution privilégié	**enable secret** *password* Exemple : Router(config)# **enable secret cisco** Router(config)#

Définir un mot de passe pour empêcher tout accès non autorisé à la console	**password** *password* **login** Exemple : Router(config)# **line con 0** Router(config-line)# **password class** Router(config-line)# **login** Router(config)#
Définir un mot de passe pour empêcher tout accès Telnet non autorisé. Lignes vty du routeur : 0 4 Lignes vty du commutateur : 0 15	**password** *password* **login** Exemple : Router(config)# **line vty 0 4** Router(config-line)# **password class** Router(config-line)# **login** Router(config-line)#
Configurer la bannière MOTD.	**Banner motd %** Exemple : Router(config)# **banner motd %** Router(config)#
Configurer une interface. L'interface du routeur est désactivée par défaut L'interface du commutateur est activée par défaut	Exemple : Router(config)# **interface fa0/0** Router(config-if)# **description** *description* Router(config-if)# **ip address** *masque d'adresse* Router(config-if)# **no shutdown** Router(config-if)#
Enregistrer la configuration en mémoire NVRAM.	**copy running-config startup-config** Exemple : Router# **copy running-config startup-config** Router#

Tâche 7 : confirmation

Il est souvent nécessaire et commode d'enregistrer le fichier de configuration dans un fichier texte hors ligne. Un moyen d'enregistrer le fichier de configuration est d'utiliser l'option Capturer du menu Transfert d'HyperTerminal.

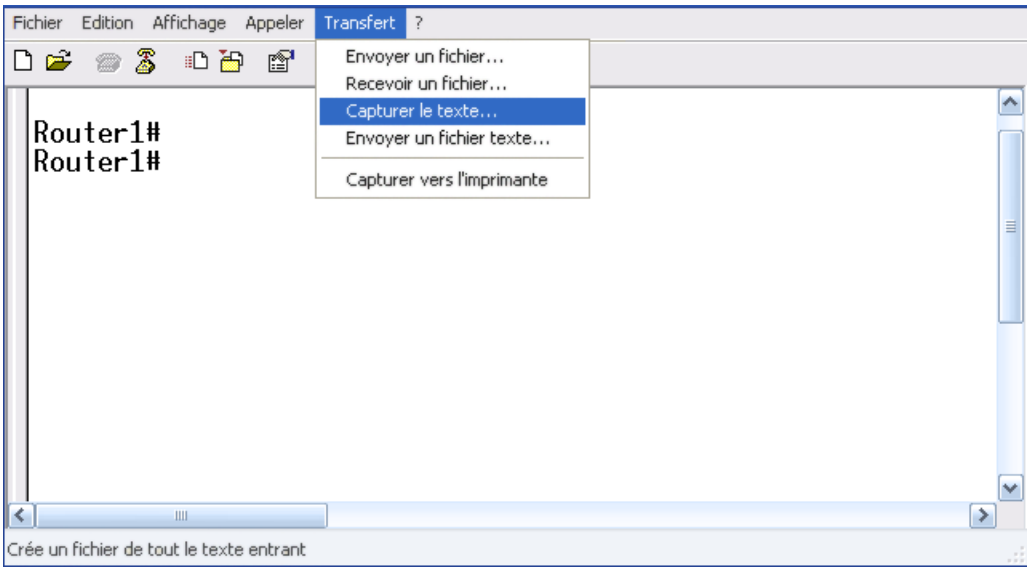


Figure 2. Option Capturer dans Hyperterminal.

Reportez-vous à la figure 2. Toutes les communications entre l'hôte et le routeur sont enregistrées dans un fichier. Vous pouvez modifier et enregistrer ce fichier. Vous pouvez également le modifier, le copier et le coller sur un routeur :

Pour lancer une capture dans HyperTerminal, sélectionnez l'option de menu Transfert | Capturer le texte. Entrez un chemin d'accès et un nom de fichier, puis sélectionnez Démarrer.

Exécutez la commande **show running-config**, puis appuyez sur la touche <ESPACE> jusqu'à ce que la configuration s'affiche dans sa totalité.

Arrêtez la capture. Sélectionnez l'option de menu Transfert | Capturer le texte | Arrêter.

Ouvrez le fichier texte et analysez le contenu. Supprimez les lignes qui ne correspondent pas à des commandes de configuration (par exemple, l'occurrence more). Corrigez manuellement les lignes qui ont été mélangées ou qui se trouvent au même endroit. Après avoir vérifié le fichier de configuration, mettez les lignes en surbrillance et sélectionnez le menu Edition | Copier dans le Bloc-notes. La configuration est alors enregistrée dans la mémoire de l'ordinateur hôte.

Pour importer le fichier de configuration, il est recommandé de TOUJOURS partir d'une configuration RAM intègre. Sinon, les commandes de configuration périmées risquent de survivre à une action de collage et produire des effets indésirables (ce que l'on appelle également la loi des conséquences inattendues) :

Suppression du fichier de configuration NVRAM :

```
Router1# erase start
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm] <ENTRÉE>
[OK]
Erase of nvram: complete
```

Réinitialisez le routeur :

```
Router1# reload
Proceed with reload? [confirm] <ENTRÉE>
```

Lorsque le routeur redémarre, passez en mode de configuration globale.

```
Router> en
Router# config t
Router(config)#
```

Cliquez avec le bouton droit de la souris dans la fenêtre d'HyperTerminal et sélectionnez Coller vers l'hôte. La configuration est rapidement importée sur le routeur. Prêtez une attention particulière aux messages d'erreur. Vous devez tous les lire et rectifier les erreurs.

Vérifiez la configuration en enregistrez-la en mémoire NVRAM.

Tâche 8 : remise en état

Avant de mettre le routeur et le commutateur hors tension, supprimez le fichier de configuration NVRAM sur chaque périphérique à l'aide de la commande **erase startup-config**.

Supprimez les éventuels fichiers de configuration sur les ordinateurs hôtes.

Sauf instruction contraire du formateur, rétablissez la connectivité réseau des ordinateurs hôtes, puis mettez-les hors tension. Enlevez le matériel utilisé durant les travaux pratiques et préparez la salle pour le cours suivant.

Annexe 1 : configuration d'un routeur Cisco IOS par défaut

```
Current configuration : 824 bytes
!
version 12,4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip cef
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Vlan1
 no ip address
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end
```

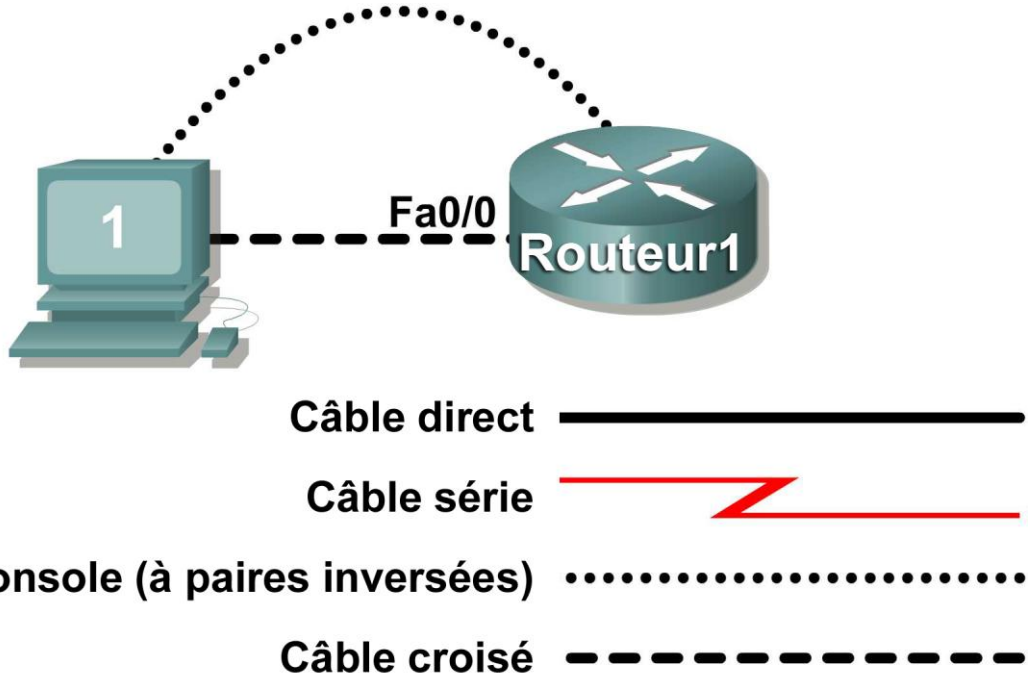
Annexe 2 : configuration d'un commutateur Cisco IOS par défaut

```
Current configuration : 1519 bytes
!
version 12,1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
ip subnet-zero
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
interface FastEthernet0/1
 no ip address
!
interface FastEthernet0/2
 no ip address
!
interface FastEthernet0/3
 no ip address
!
interface FastEthernet0/4
 no ip address
!
interface FastEthernet0/5
 no ip address
!
interface FastEthernet0/6
 no ip address
!
interface FastEthernet0/7
 no ip address
!
interface FastEthernet0/8
 no ip address
!
interface FastEthernet0/9
 no ip address
!
interface FastEthernet0/10
 no ip address
!
interface FastEthernet0/11
 no ip address
!
interface FastEthernet0/12
 no ip address
!
```

```
interface FastEthernet0/13
 no ip address
!
interface FastEthernet0/14
 no ip address
!
interface FastEthernet0/15
 no ip address
!
interface FastEthernet0/16
 no ip address
!
interface FastEthernet0/17
no ip address
!
interface FastEthernet0/18
 no ip address
!
interface FastEthernet0/19
 no ip address
!
interface FastEthernet0/20
 no ip address
!
interface FastEthernet0/21
 no ip address
!
interface FastEthernet0/22
 no ip address
!
interface FastEthernet0/23
 no ip address
!
interface FastEthernet0/24
 no ip address
!
interface GigabitEthernet0/1
 no ip address
!
interface GigabitEthernet0/2
 no ip address
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
ip http server
!
!
line con 0
line vty 5 15
!
end
```

Travaux pratiques 11.5.2 : gestion de la configuration d'un périphérique

Diagramme de topologie



Objectifs pédagogiques

- Configurer la connectivité réseau
- Enregistrer et restaurer une configuration Cisco IOS à l'aide de TFTP

Contexte

Matériel	Qté	Description
Routeur Cisco	1	Inclus dans l'équipement de travaux pratiques CCNA
Ordinateur (hôte)	1	Ordinateur de travaux pratiques
Câble console (de renversement)	1	Relie l'ordinateur hôte 1 au port console du routeur
Câble de croisement	1	Relie la carte réseau de l'hôte 1 à l'interface Fa0/1 du routeur Router1

Tableau 1. Équipement et matériel nécessaires pour ces travaux pratiques

Regroupez l'équipement et les câbles nécessaires. Pour configurer les travaux pratiques, vérifiez que vous disposez bien de l'équipement répertorié dans le tableau 1.

L'ordinateur hôte sera utilisé comme serveur TFTP. Ces travaux pratiques nécessitent l'utilisation du logiciel serveur SolarWinds TFTP. SolarWinds est une application TFTP gratuite pour Windows.

Scénario

Dans le cadre de ces travaux pratiques, les participants vont devoir configurer les paramètres courants d'un routeur Cisco, enregistrer la configuration sur un serveur TFTP, puis restaurer la configuration à partir d'un serveur TFTP.

Vous disposez de l'adresse 10.250.250.0/24, avec 6 bits utilisés pour les sous-réseaux. Utilisez le DERNIER sous-réseau. L'hôte 1 doit utiliser la PREMIÈRE adresse d'hôte autorisée, tandis que le routeur Router1 doit utiliser la DERNIÈRE :

Adresse IP : 10.250.250.0		Masque de sous-réseau :	
Sous-réseau	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion

Tâche 1 : configuration de la connectivité réseau

Étape 1 : connexion physique des périphériques

Examinez le diagramme de topologie. Connectez le câble console (ou de renversement) au port console du routeur et l'autre extrémité du câble au port COM 1 de l'ordinateur d'hôte à l'aide d'un adaptateur DB-9 ou DB-25. Assurez-vous que l'ordinateur hôte et le routeur sont sous tension.

Étape 2 : connexion logique des périphériques

À l'aide des paramètres IP fournis dans le scénario, configurez l'ordinateur hôte 1.

Étape 3 : connexion de l'ordinateur hôte au routeur via HyperTerminal

Dans la barre des tâches Windows, démarrez le programme HyperTerminal en cliquant sur Démarrer | Programmes | Accessoires | Communications | HyperTerminal.

Lorsque la fenêtre de session HyperTerminal s'affiche, appuyez sur la touche **Entrée** jusqu'à obtenir une réponse du routeur.

Étape 4 : configuration du routeur Router1

Configurez le routeur Router1. La configuration de Router1 comprend les tâches suivantes :

Tâche- reportez-vous à l'annexe 1 pour obtenir de l'aide sur les commandes
Spécifiez le nom du routeur- `Router1`
Spécifiez un mot de passe d'exécution privilégié chiffré- `cisco`
Spécifiez un mot de passe d'accès à la console- `class`
Spécifiez un mot de passe d'accès Telnet- `class`
Configurez la bannière MOTD.
Configurez l'interface Fa0/0 de Router1- définissez la description ; définissez l'adresse de couche 3 exécutez la commande **`no shutdown.`**

REMARQUE **N'ENREGISTREZ PAS LA CONFIGURATION EN MÉMOIRE NVRAM.

Étape 5 : vérification de la connectivité

Vérifiez la connectivité entre l'hôte 1 et Router1 :

```
Router1# ping 10 250 250 253

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10 250 250 253, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
Router1#
```

Tâche 2 : enregistrement et restauration d'une configuration Cisco IOS à l'aide de TFTP

Étape 1 : installation de l'application TFTP SolarWinds

Double-cliquez sur l'application TFTP SolarWinds pour lancer l'installation. Sélectionnez Next. Acceptez l'accord de licence et les paramètres par défaut. Une fois que SolarWinds a terminé l'installation, cliquez sur Finish.

Étape 2 : démarrage du serveur TFTP

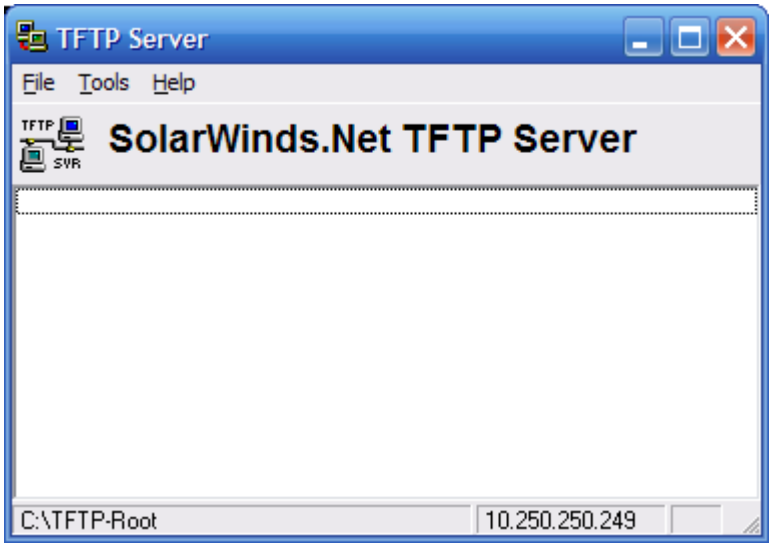


Figure 2. Fenêtre du serveur TFTP

Démarrez le serveur TFTP en sélectionnant Démarrer| Programmes | SolarWinds Free Tools | TFTP Server. La figure 2 illustre une fenêtre active du serveur TFTP.

Étape 3 : configuration du serveur TFTP

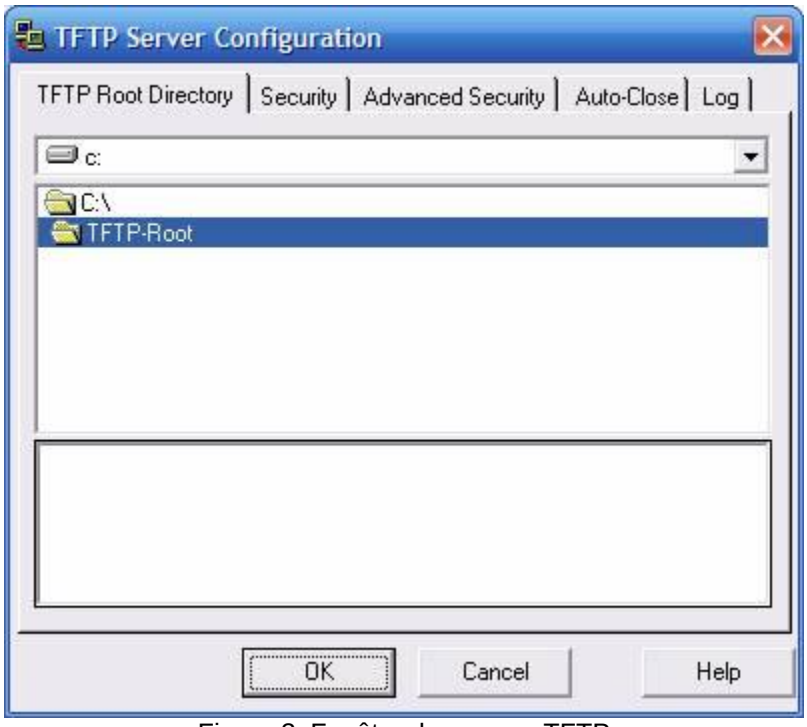


Figure 3. Fenêtre du serveur TFTP

Pour configurer le serveur TFTP, sélectionnez l'option de menu File | configure. Reportez-vous à la figure 3. Vérifiez les paramètres suivants :

Paramètre	Valeur
TFTP Root Directory:	TFTP-Root
Security	Transmit and Receive Files
Advanced Security	10 250 250 254 To 10 250 250 254
Auto-Close	Never
Log	Enable Log Requests to the Following File. Leave the default file.

Lorsque vous avez terminé, sélectionnez OK.

Étape 4 : enregistrement de la configuration de Router1 sur le serveur TFTP

Dans HyperTerminal, lancez un téléchargement TFTP sur le serveur TFTP :

```
Router1#copy running-config tftp:
Address or name of remote host []? 10.250.250.253
Destination filename [router1-confg]? <ENTRÉE>
!!
1081 bytes copied in 2.008 secs (538 bytes/sec)
Router1#
```

Vérifiez que le transfert a été correctement effectué. Ouvrez le fichier c:\Program Files\SolarWinds\Free Tools\TFTP-Server.txt. Le contenu doit être identique à ce qui suit :

```
3/25/2007 12:29 :Receiving router1-confg from  (10 250 250 254)
3/25/2007 12:29 :Received router1-confg from  (10 250 250 254), 1081 bytes
```

Vérifiez le fichier transféré. Utilisez Microsoft Word ou Wordpad pour examiner le contenu du fichier c:\TFTP-Root\router1-confg. Son contenu doit se présenter comme suit :

```
!
version 12,4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$D02B$AuX05n0HPT239yYRoQ0oE.
!
no aaa new-model
ip cef
!
interface FastEthernet0/0
 description connection to host1
 ip address 10 250 250 254 255.255.255.252
 duplex auto
 speed auto
```

```
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/1
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
ip http server
no ip http secure-server
!
control-plane
!
banner motd
*** PÃ‰RIPHÃ‰RIQUE RÃ‰SEAU DE LA SOCIÃ‰TÃ‰ ABC
****
*** Accès autorisé uniquement *****
*** La journalisation est activée ****
!
line con 0
 password class
 login
line aux 0
line vty 0 4
 password class
 login
!
scheduler allocate 20000 1000
End
```

Étape 5 : restauration de la configuration de Router1 à partir du serveur TFTP

Vérifiez que la mémoire NVRAM est vide, puis redémarrez Router1 :

```
Router1# show startup-config
 startup-config is not present
Router1# reload
Proceed with reload? [confirm] <ENTRÉE>
```

La connectivité doit être établie avec le serveur TFTP. L'interface fa0/0 du routeur Router1 doit être configurée avec une adresse IP, puis activée :

```
Router> enable
Router# conf t
Tapez les commandes de configuration (une par ligne).  Terminez avec CNTL/Z.
Router(config)# interface fa0/0
Router(config-if)# ip address 10 250 250 254 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)# exit

*Mar 25 16:43:030,095: %SYS-5-CONFIG_I: Configured from console by console
*Mar 25 16:43:040,967: %LINEPROTO-5-UPDOWN: Protocole de ligne sur
l'interface FastEthernet0/0, activée
```

Attribuez au routeur le nom d'hôte (hostname) TEST

```
Router(config-if)# exit
Router(config)#hostname TEST
Router(config-if)#end
TEST#
```

Vérifiez la connectivité à l'aide de la commande ping :

```
Router# ping 10 250 250 253
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10 250 250 253, timeout is 2 seconds:
.!!!!
Success rate is 80 percent(4/5), round-trip min/avg/max = 1/1/1ms
Router#
```

Téléchargez le fichier de configuration de Router1 depuis le serveur TFTP :

```
Router# copy tftp startup-config
Address or name of remote host []? 10.250.250.253
Source filename []? router1-confg
Destination filename [startup-config]? <ENTRÉE>
Accessing tftp://10 250 250 253/router1-confg...
Loading router1-confg from 10 250 250 253 (via FastEthernet0/0): !
[OK - 1081 bytes]

1081 bytes copied in 9.364 secs (115 bytes/sec)
Router1#
*Mar 25 16:55:260,375: %SYS-5-CONFIG_I: Configured from
tftp://10 250 250 253/router1-confg by console
Router1#
```

Examinez la configuration enregistrée en mémoire NVRAM pour vous assurer de la précision du transfert. La configuration doit être identique à celle indiquée à l'étape 4 de la tâche 1.

Réinitialisez le routeur et sélectionnez No à l'invite qui indique « Configuration has been modified ». La configuration précédente doit être restaurée et le routeur doit à présent avoir pour nom d'hôte « Router1 ».

Tâche 3 : remarques générales

TFTP offre un moyen rapide et efficace d'enregistrer et charger des fichiers de configuration Cisco IOS.

Tâche 4 : confirmation

À l'image du téléchargement d'un fichier de configuration, le système IOS peut également être stocké hors ligne pour une utilisation ultérieure. Pour trouver le nom de fichier IOS, exécutez la commande Cisco IOS **show version**. Le nom de fichier est surligné ci-dessous :

```
Router1# show version
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(10b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

Router1 uptime is 17 minutes
System returned to ROM by reload at 16:47:54 UTC Sun Mar 25 2007
System image file is "flash:c1841-advipservicesk9-mz.124-10b.bin"

This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to
import, export, distribute or use encryption. Importers, exporters,
distributors and users are responsible for compliance with U.S. and local
country laws. By using this product you agree to comply with applicable laws
and regulations. If you are unable to comply with U.S. and local laws, return
this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found
at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 1841 (revision 6,0) with 174 080K/22 528K bytes of memory.
Processor board ID FHK110918KJ
2 Serial(sync/async) interfaces
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
62 720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102

Router1#
```

Les commandes destinées à télécharger le fichier IOS sont identiques à celles utilisées pour télécharger le fichier de configuration :

```
Router1# copy flash tftp
Source filename []? c1841-advipservicesk9-mz.124-10b.bin
Address or name of remote host []? 10.250.250.253
Destination filename [c1841-advipservicesk9-mz.124-10b.bin]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!
22063220 bytes copied in 59.564 secs (370412 bytes/sec)
Router1#
```

Tâche 5 : remise en état

Avant de mettre le routeur hors tension, supprimez le fichier de configuration NVRAM si celui-ci était chargé. Utilisez la commande **erase startup-config**.

Supprimez le serveur TFTP SolarWinds de l'ordinateur hôte. Sélectionnez Démarrer | Panneau de configuration. Ouvrez Ajout/Suppression de programmes. Sélectionnez SolarWinds, puis Supprimer. Acceptez les paramètres par défaut.

Supprimez les éventuels fichiers de configuration sur les ordinateurs hôtes.

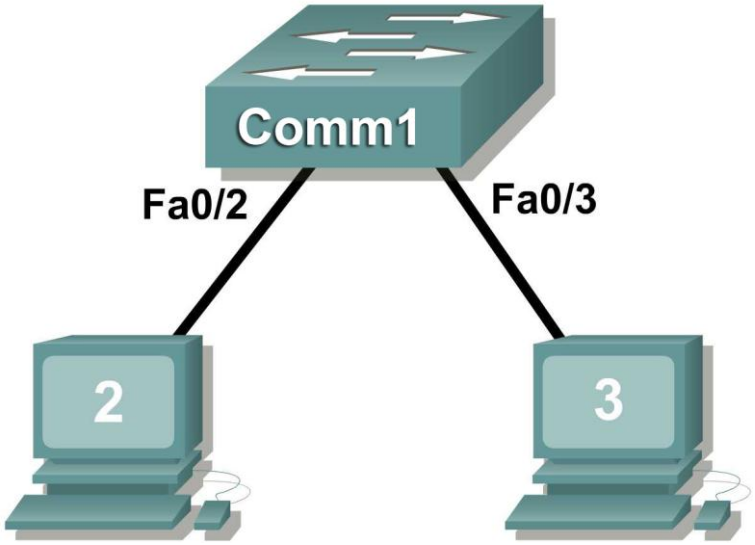
Sauf instruction contraire du formateur, rétablissez la connectivité réseau des ordinateurs hôtes, puis mettez-les hors tension. Enlevez le matériel utilisé durant les travaux pratiques et préparez la salle pour le cours suivant.

Annexe 1

Objectif	Commande
Passer en mode de configuration globale	**configure terminal** Exemple : Router> **enable** Router# configure terminal Router(config)#
Indiquer le nom du routeur	**hostname** *name* Exemple : Router(config)# **hostname Router1** Router(config)#
Définir un mot de passe chiffré pour empêcher tout accès non autorisé au mode d'exécution privilégié	**enable secret** *password* Exemple : Router(config)# **enable secret cisco** Router(config)#
Définir un mot de passe pour empêcher tout accès non autorisé à la console	**password** *password* **login** Exemple : Router(config)# **line con 0** Router(config-line)# **password class** Router(config-line)# **login** Router(config)#
Définir un mot de passe pour empêcher tout accès Telnet non autorisé. Lignes vty du routeur : 0 4 Lignes vty du commutateur : 0 15	**password** *password* **login** Exemple : Router(config)# **line vty 0 4** Router(config-line)# **password class** Router(config-line)# **login** Router(config-line)#
Configurer la bannière MOTD.	**Banner motd %** Exemple : Router(config)# **banner motd %** Router(config)#
Configurer une interface. L'interface du routeur est désactivée par défaut L'interface du commutateur est activée par défaut	Exemple : Router(config)# **interface fa0/0** Router(config-if)# **description** *description* Router(config-if)# **ip address** *masque d'adresse* Router(config-if)# **no shutdown** Router(config-if)#
Enregistrer la configuration en mémoire NVRAM.	**copy running-config startup-config** Exemple : Router# **copy running-config startup-config** Router#

Travaux pratiques 11.5.3 : configuration d'ordinateurs hôtes pour un réseau IP

Diagramme de topologie



Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Concevoir la topologie logique des travaux pratiques
- Configurer la topologie physique des travaux pratiques
- Configurer la topologie logique du réseau local (LAN)
- Vérifier la connectivité du réseau local

Contexte

Matériel	Qté	Description
Routeur Cisco	1	Inclus dans l'équipement de travaux pratiques CCNA
Commutateur Cisco	1	Inclus dans l'équipement de travaux pratiques CCNA
*Ordinateur (hôte)	3	Ordinateur de travaux pratiques
Câbles UTP droits de catégorie 5 ou supérieure	3	Relie le routeur Router1 et les ordinateurs hôtes 1 et 2 au commutateur Switch1

Tableau 1. Équipement et matériel pour ces travaux pratiques

Regroupez l'équipement et les câbles nécessaires. Pour configurer les travaux pratiques, vérifiez que vous disposez bien de l'équipement répertorié dans le tableau 1.

Scénario

Dans le cadre de ces travaux pratiques, les participants vont devoir créer un petit réseau, ce qui suppose de connecter des périphériques réseau et de configurer les ordinateurs hôtes pour une connectivité réseau de base. L'annexe ci-après fait office de référence pour la configuration du réseau logique.

Tâche 1 : conception de la topologie logique des travaux pratiques

1. Compte tenu de l'adresse IP `192.168.254.0/24` et des 5 bits utilisés pour les sous-réseaux, fournissez les informations suivantes :

   Nombre maximum de sous-réseaux : _____

   Nombre d'hôtes utilisables par sous-réseau : _____

	Adresse IP : 192.168.254.0		**Masque de sous-réseau :**	
#	**Sous-réseau**	**Première adresse d'hôte**	**Dernière adresse d'hôte**	**Diffusion**
0				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				

2. Avant de poursuivre, vérifiez vos adresses en compagnie du formateur. Le formateur attribuera un sous-réseau par participant ou équipe.

Tâche 2 : configuration de la topologie physique des travaux pratiques

Étape 1 : connexion physique des périphériques

1. Installez les périphériques réseau comme illustré dans la figure 1.

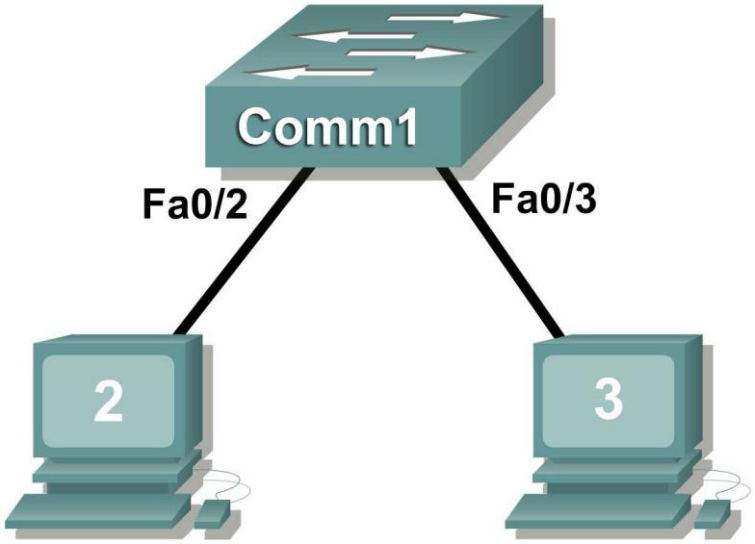


Figure 1. Installation du réseau

Est-il nécessaire d'utiliser un câble de croisement pour relier les ordinateurs hôtes au commutateur ? Justifiez votre réponse.

_____

_____

Si ce n'est déjà fait, mettez tous les périphériques sous tension.

Étape 2 : inspection visuelle des connexions réseau

Après avoir installé les périphériques réseau, prenez le temps de vérifier les connexions. C'est en faisant attention aux détails dès à présent que vous limiterez par la suite le temps passé à résoudre des problèmes de connectivité.

Tâche 3 : configuration de la topologie logique

Étape 1 : consignation des paramètres du réseau logique

1. Les ordinateurs hôtes utilisent les deux premières adresses IP du sous-réseau. Inscrivez les paramètres IP de chaque périphérique :

Périphérique	Sous-réseau	Adresse IP	Masque
Hôte 1			
Hôte 2			

Figure 2. Topologie logique

2. À partir des informations fournies dans la figure 2, indiquez l'adressage réseau IP pour chaque ordinateur :

Hôte 1	
Adresse IP	
Masque IP	

Hôte 2	
Adresse IP	
Masque IP	

Étape 2 : configuration de l'ordinateur hôte 1

1. Sur l'ordinateur 1, cliquez sur **Démarrer > Panneau de configuration > Connexions réseau**. Cliquez avec le bouton droit de la souris sur l'icône du réseau local, puis sélectionnez **Propriétés**. Sous l'onglet **Général**, sélectionnez **Protocole Internet (TCP/IP)**, puis cliquez sur le bouton **Propriétés**.

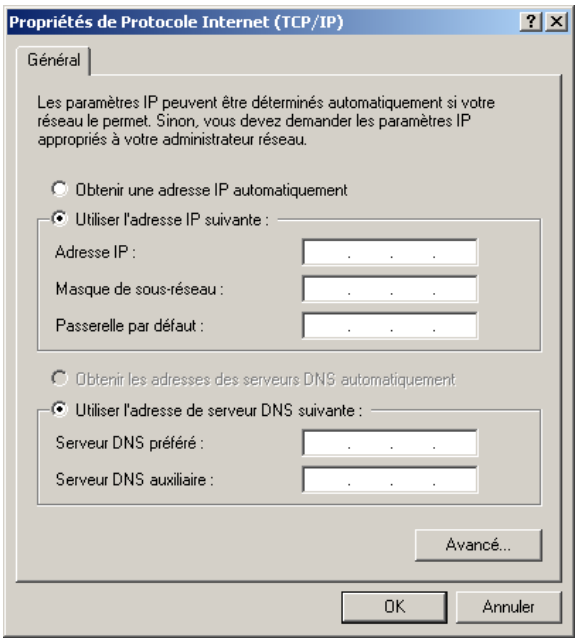


Figure 3. Paramètres d'adresse IP et de passerelle de l'hôte 1

2. Consultez les paramètres d'adresse IP et de passerelle de l'hôte 1 dans la figure 3.
3. Lorsque vous avez terminé, cliquez sur **OK**, puis sur **Fermer**. Il vous faudra peut-être redémarrer l'ordinateur pour enregistrer les modifications.
4. Vérifiez que l'hôte 1 est correctement configuré à l'aide de la commande **`ipconfig /all`**.

5. Consignez les résultats ci-dessous.

Paramètre	Valeur
Périphérique Ethernet	
Adresse physique	
Adresse IP	
Masque de sous-réseau	
Passerelle par défaut	

Étape 3 : configuration de l'hôte 2

1. Répétez l'étape 2 pour l'hôte 2 en utilisant les paramètres IP figurant dans le tableau complété à l'étape 1.
2. Vérifiez que l'hôte 1 est correctement configuré à l'aide de la commande **`ipconfig /all`**.
3. Consignez les résultats ci-dessous.

Paramètre	Valeur
Périphérique Ethernet	
Adresse physique	
Adresse IP	
Masque de sous-réseau	
Passerelle par défaut	

Tâche 4 : vérification de la connectivité du réseau

La connectivité réseau peut être vérifiée à l'aide d'une commande **`ping`** Windows.

1. Pour vérifier méthodiquement la connectivité avec chaque périphérique réseau, servez-vous du tableau suivant :

Origine	Destination	Adresse IP	Résultats de la requête ping
Hôte 1	Hôte 2		
Hôte 2	Hôte 1		

2. En cas d'échec à un test, prenez des mesures correctives pour établir la connectivité.

   Remarque : si vous n'obtenez pas de résultats en interrogeant les ordinateurs hôtes via la commande ping, désactivez provisoirement le pare-feu sur l'ordinateur et relancez le test. Pour désactiver un pare-feu Windows, cliquez sur **Démarrer > Panneau de configuration > Pare-feu Windows**, choisissez **Désactivé**, puis cliquez sur **OK**.

Tâche 5 : remarques générales

Analysez les problèmes de configuration physique ou logique rencontrés au cours de ces travaux pratiques. Assurez-vous d'avoir bien assimilé les procédures de configuration d'un ordinateur hôte Windows.

Tâche 6 : confirmation

Demandez à votre formateur ou à un autre participant d'introduire un ou deux problèmes dans votre réseau pendant que vous êtes occupé à une autre tâche ou que vous êtes absent de la salle de travaux pratiques. Les problèmes peuvent être d'ordre physique (câble UTP inapproprié) ou logique (adresse IP incorrecte). Pour résoudre les problèmes, procédez comme suit :

1. Faites une inspection visuelle minutieuse. Vérifiez que les voyants de liaison du commutateur Switch1 sont verts.
2. Servez-vous du tableau fourni à la tâche 3 ci-dessus pour identifier les problèmes de connectivité. Énumérez les problèmes :

   _____

   _____

   _____

   _____

   _____

3. Notez la ou les solutions que vous proposez :

   _____

   _____

   _____

   _____

   _____

4. Testez votre solution. Si la solution est concluante, notez-la. Si la solution est inefficace, poursuivez le dépannage.

   _____

   _____

   _____

   _____

   _____

Tâche 7 : remise en état

Sauf instruction contraire du formateur, rétablissez la connectivité réseau des ordinateurs hôtes, puis mettez-les hors tension. Enlevez le matériel utilisé durant les travaux pratiques et préparez la salle pour le cours suivant.

Annexe

Adressage de sous-réseaux pour le dernier octett — East Carolina University

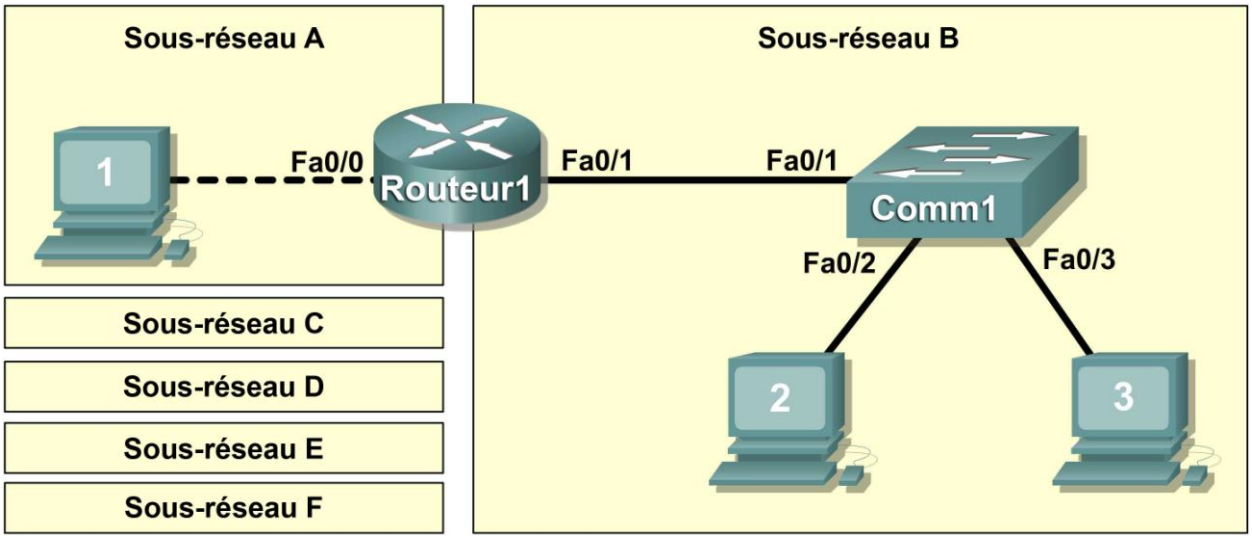
0 4 8 12 16 20 24 28 32 36 40 44 48 52 56 60 64 68 72 76 80 84 88 92 96 100 104 108 112 116 120 124 128 132 136 140 144 148 152 156 160 164 168 172 176 180 184 188 192 196 200 204 208 212 216 220 224 228 232 236 240 244 248 252						
.0						
(1 bit) 10000000	(2 bits) 11000000	(3 bits) 11100000	(4 bits) 11110000	(5 bits) 11111000	(6 bits) 11111100	
1 Sous-réseau, 126 hosts	3 Sous-réseaux, 62 hosts	7 Sous-réseaux, 30 hosts	15 Sous-réseaux, 14 hosts	32 Sous-réseaux, 6 hosts	63 Sous-réseaux, 2 hosts	
Masque - 128_{10}	Masque - 192_{10}	Masque - 224_{10}	Masque - 240_{10}	Masque - 248_{10}	Masque - 252_{10}	
.0 (.1 - 126)	**.0** (.1 - 62)	**.0** (.1 - 30)	**.0** (.1 - 14)	**.0** (.1 - 6)	**.0** (.1 - 2)	
					.4 (.5 - 6)	
				.8 (.9 - 14)	**.8** (.9 - 10)	
					.12 (.13 - 14)	
			.16 (.17 - 30)	**.16** (.17 - 22)	**.16** (.17 - 18)	
					.20 (.21 - 22)	
				.24 (.25 - 30)	**.24** (.25 - 26)	
					.28 (.29 - 30)	
		.0 (.1 - 62)			**.32** (.33 - 34)	
				.32 (.33 - 38)	**.36** (.37 - 38)	
			.32 (.33 - 46)			
					.40 (.41 - 42)	
				.40 (.41 - 46)	**.44** (.45 - 46)	
					.48 (.49 - 50)	
				.48 (.49 - 54)	**.52** (.53 - 54)	
					.56 (.57 - 58)	
			.32 (.33 - 62)			
					.60 (.61 - 62)	
				.56 (.57 - 62)		
					.64 (.65 - 66)	
				.64 (.65 - 78)	**.68** (.69 - 70)	
					.72 (.73 - 74)	
					.76 (.77 - 78)	
		.64 (.65 - 94)			**.80** (.81 - 82)	
				.80 (.81 - 94)	**.84** (.85 - 86)	
					.88 (.89 - 90)	
				.88 (.89 - 94)	**.92** (.93 - 94)	
					.96 (.97 - 98)	
				.96 (.97 - 110)	**.100** (.101 - 102)	
			.64 (.65 - 126)			
					.104 (.105 - 106)	
				.104 (.105 - 110)	**.108** (.109 - 110)	
					.112 (.113 - 114)	
				.112 (.113 - 118)	**.116** (.117 - 118)	
					.120 (.121 - 122)	
					.124 (.125 - 126)	
		.96 (.97 - 126)			**.128** (.129 - 130)	
				.120 (.121 - 126)	**.132** (.133 - 134)	
					.136 (.137 - 138)	
				.128 (.129 - 142)	**.140** (.141 - 142)	
					.144 (.145 - 146)	
			.128 (.129 - 158)			
					.148 (.149 - 150)	
				.144 (.145 - 158)	**.152** (.153 - 154)	
					.156 (.157 - 158)	
		.128 (.129 - 190)			**.160** (.161 - 162)	
				.160 (.161 - 174)	**.164** (.165 - 166)	
					.168 (.169 - 170)	
			.160 (.161 - 190)			
					.172 (.173 - 174)	
				.160 (.161 - 190)	**.176** (.177 - 178)	
					.180 (.181 - 182)	
				.176 (.177 - 190)	**.184** (.185 - 186)	
					.188 (.189 - 190)	
			.192 (.193 - 222)			
					.192 (.193 - 194)	
				.192 (.193 - 206)	**.196** (.197 - 198)	
					.200 (.201 - 202)	
				.192 (.193 - 222)	**.204** (.205 - 206)	
					.208 (.209 - 210)	
			.192 (.193 - 254)			
					.212 (.213 - 214)	
				.208 (.209 - 222)	**.216** (.217 - 218)	
					.220 (.221 - 222)	
			.224 (.225 - 254)			
					.224 (.225 - 226)	
				.224 (.225 - 238)	**.228** (.229 - 230)	
					.232 (.233 - 234)	
					.236 (.237 - 238)	
			.224 (.225 - 254)			
					.240 (.241 - 242)	
				.240 (.241 - 254)	**.244** (.245 - 246)	
					.248 (.249 - 250)	
				.248 (.249 - 254)	**.252** (.253 - 254)	

Adressage de sous-réseaux pour le dernier octett — East Carolina University

	(1 bit) 10000000 1 Sous-réseau, 126 hosts Masque - 128_{10}	(2 bits) 11000000 3 Sous-réseaux, 62 hosts Masque - 192_{10}	(3 bits) 11100000 7 Sous-réseaux, 30 hosts Masque - 224_{10}	(4 bits) 11110000 15 Sous-réseaux, 14 hosts Masque - 240_{10}	(5 bits) 11111000 32 Sous-réseaux, 6 hosts Masque - 248_{10}	(6 bits) 11111100 63 Sous-réseaux, 2 hosts Masque - 252_{10}
.0	**.0**	**.0** (.1- .62)	**.0** .1- .30)	.0 (.1- .14)	**.0** (.1- .6)	**.0** (.1- .2)
.4						**.4** (.5- .6)
.8					**.8** (.9- .14)	**.8** (.9- .10)
.12						**.12** (.13- .14)
.16				**.16** (.17- .30)	**.16** (.17- .22)	**.16** (.17- .18)
.20						**.20** (.21- .22)
.24					**.24** (.25- .30)	**.24** (.25- .26)
.28						**.28** (.29- .30)
.32			**.32** .33- .62)	**.32** (.33- .46)	**.32** (.33- .38)	**.32** (.33- .34)
.36						**.36** (.37- .38)
.40					**.40** (.41- .46)	**.40** (.41- .42)
.44						**.44** (.45- .46)
.48				**.48** (.49- .62)	**.48** (.49- .54)	**.48** (.49- .50)
.52						**.52** (.53- .54)
.56					**.56** (.57- .62)	**.56** (.57- .58)
.60						**.60** (.61- .62)
.64		**.64** (.65- .126)	**.64** (.65- .94)	**.64** (.65- .78)	**.64** (.65- .70)	**.64** (.65- .66)
.68						**.68** (.69- .70)
.72					**.72** (.73- .78)	**.72** (.73- .74)
.76						**.76** (.77- .78)
.80				**.80** (.81- .94)	**.80** (.81- .86)	**.80** (.81- .82)
.84						**.84** (.85- .86)
.88					**.88** (.89- .94)	**.88** (.89- .90)
.92						**.92** (.93- .94)
.96			**.96** (.97- .126)	**.96** (.97- .110)	**.96** (.97- .102)	**.96** (.97- .98)
.100						**.100** (.101- .102)
.104					**.104** (.105- .110)	**.104** (.105- .106)
.108						**.108** (.109- .110)
.112				**.112** (.113- .126)	**.112** (.113- .118)	**.112** (.113- .114)
.116						**.116** (.117- .118)
.120					**.120** (.121- .126)	**.120** (.121- .122)
.124						**.124** (.125- .126)
.128	**.128**	**.128** (.129- .190)	**.128** (.129- .158)	**.128** (.129- .142)	**.128** (.129- .134)	**.128** (.129- .130)
.132						**.132** (.133- .134)
.136					**.136** (.137- .142)	**.136** (.137- .138)
.140						**.140** (.141- .142)
.144				**.144** (.145- .158)	**.144** (.145- .150)	**.144** (.145- .146)
.148						**.148** (.149- .150)
.152					**.152** (.153- .158)	**.152** (.153- .154)
.156						**.156** (.157- .158)
.160			**.160** (.161- .190)	**.160** (.161- .174)	**.160** (.161- .166)	**.160** (.161- .162)
.164						**.164** (.165- .166)
.168					**.168** (.169- .174)	**.168** (.169- .170)
.172						**.172** (.173- .174)
.176				**.176** (.177- .190)	**.176** (.177- .182)	**.176** (.177- .178)
.180						**.180** (.181- .182)
.184					**.184** (.185- .190)	**.184** (.185- .186)
.188						**.188** (.189- .190)
.192		**.192** (.193- .254)	**.192** (.193- .222)	**.192** (.193- .206)	**.192** (.193- .198)	**.192** (.193- .194)
.196						**.196** (.197- .198)
.200					**.200** (.201- .206)	**.200** (.201- .202)
.204						**.204** (.205- .206)
.208				**.208** (.209- .222)	**.208** (.209- .214)	**.208** (.209- .210)
.212						**.212** (.213- .214)
.216					**.216** (.217- .222)	**.216** (.217- .218)
.220						**.220** (.221- .222)
.224			**.224** (.225- .254)	**.224** (.225- .238)	**.224** (.225- .230)	**.224** (.225- .226)
.228						**.228** (.229- .230)
.232					**.232** (.233- .238)	**.232** (.233- .234)
.236						**.236** (.237- .238)
.240				.240 (.241- .254)	**.240** (.241- .246)	**.240** (.241- .242)
.244						**.244** (.245- .246)
.248					**.248** (.249- .254)	**.248** (.249- .250)
.252						**.252** (.253- .254)

Travaux pratiques 11.5.4 : tests réseau

Diagramme de topologie



Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Concevoir la topologie logique des travaux pratiques
- Configurer la topologie physique des travaux pratiques
- Configurer la topologie logique du réseau local (LAN)
- Vérifier la connectivité du réseau local

Contexte

Matériel	Qté	Description
Routeur Cisco	1	Inclus dans l'équipement de travaux pratiques CCNA
Commutateur Cisco	1	Inclus dans l'équipement de travaux pratiques CCNA
*Ordinateur (hôte)	3	Ordinateur de travaux pratiques
Câbles UTP droits de catégorie 5 ou supérieure	3	Relie le routeur Router1 et les hôtes 1 et 2 au commutateur Switch1
Câble de croisement UTP de catégorie 5	1	Relie l'hôte 1 à Router1
Câble console (de renversement)	1	Relie l'hôte 1 à la console de Router1

Tableau 1. Équipement et matériel pour ces travaux pratiques

Regroupez l'équipement et les câbles nécessaires. Pour configurer les travaux pratiques, vérifiez que vous disposez bien de l'équipement répertorié dans le tableau 1.

Vous trouverez dans l'annexe ci-après la syntaxe de configuration Cisco IOS pour ces travaux pratiques.

Scénario

Dans le cadre de ces travaux pratiques, vous allez créer un petit réseau, ce qui suppose de connecter des périphériques et de configurer les ordinateurs hôtes pour une connectivité de base. SubnetA et SubnetB sont des sous-réseaux dont nous avons besoin. SubnetC, SubnetD, SubnetE et SubnetF sont des projets de sous-réseaux qui ne sont pas encore connectés au réseau.

Tâche 1 : conception de la topologie logique des travaux pratiques

À partir de l'adresse IP et du masque `172.20.0.0 / 24 (adresse / masque)`, concevez un modèle d'adressage IP qui remplisse les conditions suivantes :

Sous-réseau	Nombre d'hôtes
SubnetA	Comme illustré dans le diagramme de topologie
SubnetB	Entre 80 et 100
SubnetC	Entre 40 et 52
SubnetD	Entre 20 et 29
SubnetE	12
SubnetF	5

Remarque : commencez toujours par le sous-réseau qui compte le plus grand nombre d'hôtes pour terminer par celui qui en contient le moins. En l'occurrence, vous devez commencer par SubnetB et finir par SubnetA.

Étape 1 : conception du bloc d'adresses de SubnetB

Abordez la phase de conception du réseau logique en respectant les critères de SubnetB (le bloc d'adresses IP le plus grand). En utilisant des nombres binaires pour créer votre tableau de sous-réseaux, choisissez le premier bloc d'adresses prenant en charge SubnetB.

1. Dans le tableau suivant, indiquez les paramètres IP de SubnetB :

Adresse réseau	Masque	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion

2. Quel est le masque de bits en binaire ? _____

Étape 2 : conception du bloc d'adresses de SubnetC

Répondez aux critères de SubnetC, le prochain bloc d'adresses IP le plus grand. En utilisant des nombres binaires pour créer votre tableau de sous-réseaux, choisissez le prochain bloc d'adresses disponible prenant en charge SubnetC.

1. Dans le tableau suivant, indiquez les paramètres IP de SubnetC :

Adresse réseau	Masque	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion

2. Quel est le masque de bits en binaire ? _____

Étape 3 : conception du bloc d'adresses de SubnetD

Respectez les critères de SubnetD : le prochain bloc d'adresses IP le plus grand. En utilisant des nombres binaires pour créer votre tableau de sous-réseaux, choisissez le prochain bloc d'adresses disponible prenant en charge SubnetD.

1. Dans le tableau suivant, indiquez les paramètres IP de SubnetD :

Adresse réseau	Masque	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion

2. Quel est le masque de bits en binaire ? _____

Étape 4 : conception du bloc d'adresses de SubnetE

Respectez les critères de SubnetE : le prochain bloc d'adresses IP le plus grand. En utilisant des nombres binaires pour créer votre tableau de sous-réseaux, choisissez le prochain bloc d'adresses disponible prenant en charge SubnetE.

1. Complétez le tableau suivant à partir des informations d'adresse IP de SubnetE :

Adresse réseau	Masque	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion

2. Quel est le masque de bits en binaire ? _____

Étape 5 : conception du bloc d'adresses de SubnetF

Respectez les critères de SubnetF : le prochain bloc d'adresses IP le plus grand. En utilisant des nombres binaires pour créer votre tableau de sous-réseaux, choisissez le prochain bloc d'adresses disponible prenant en charge SubnetF.

1. Complétez le tableau suivant à partir des informations d'adresse IP de SubnetF :

Adresse réseau	Masque	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion

2. Quel est le masque de bits en binaire ? _____

Étape 6 : conception du bloc d'adresses de SubnetA

Respectez les critères de SubnetA : le plus petit bloc d'adresses IP. En utilisant des nombres binaires pour créer votre tableau de sous-réseaux, choisissez le prochain bloc d'adresses disponible prenant en charge SubnetA.

1. Dans le tableau suivant, indiquez les paramètres IP de SubnetA :

Adresse réseau	Masque	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion

2. Quel est le masque de bits en binaire ? _____

Tâche 2 : configuration de la topologie physique des travaux pratiques

Étape 1 : connexion physique des périphériques des travaux pratiques

1. Raccordez les périphériques réseau comme indiqué dans la figure 1. Tenez compte du câble de croisement requis entre l'hôte 1 et le routeur Router1.

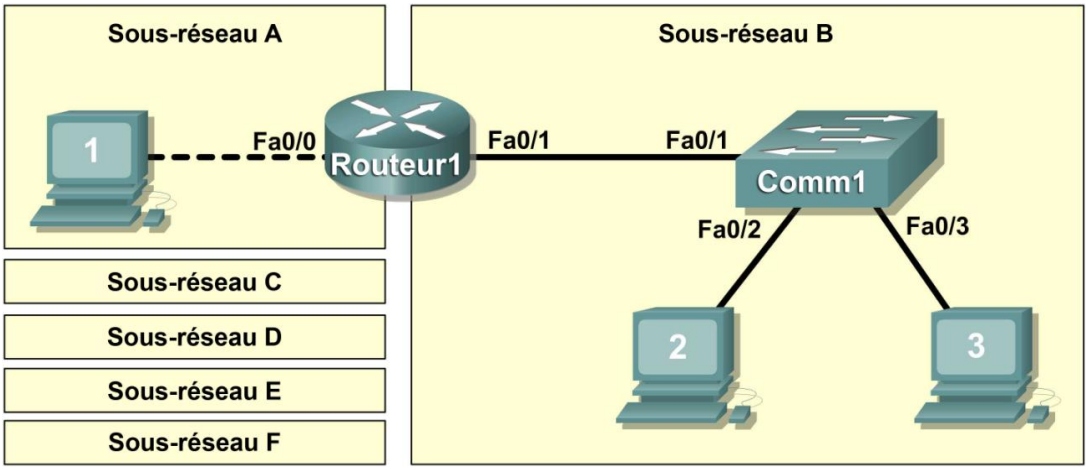


Figure 1. Installation du réseau

2. Si ce n'est déjà fait, mettez tous les périphériques sous tension.

Étape 2 : inspection visuelle des connexions réseau

Après avoir installé les périphériques réseau, prenez le temps de vérifier les connexions. C'est en faisant attention aux détails maintenant que vous limiterez par la suite le temps passé à dépanner les problèmes de connectivité de couche 1.

Tâche 3 : configuration de la topologie logique

Étape 1 : consignation des paramètres du réseau logique

Sur SubnetA, l'hôte 1 utilise la première adresse IP du sous-réseau. L'interface Fa0/0 de Router1 utilise la dernière adresse d'hôte. Sur SubnetB, les ordinateurs hôtes utilisent respectivement les première et deuxième adresses d'hôte du sous-réseau. L'interface Fa0/1 de Router1 utilise la dernière adresse d'hôte réseau.

Pour acheminer correctement les trames de couche 2 entre les périphériques du réseau local, le commutateur Switch1 n'a pas besoin d'une configuration de couche 3. L'adresse IP attribuée à Switch 1, interface VLAN 1, sert à établir une connectivité de couche 3 entre les périphériques externes et le commutateur. Sans adresse IP, les protocoles de couche supérieure tels que TELNET et HTTP ne peuvent pas fonctionner. L'adresse de passerelle par défaut permet au commutateur de répondre aux demandes de protocole émanant de périphériques de réseaux distants. Par exemple, l'adresse de la passerelle IP étend la connectivité de la couche 3 au-delà du sous-réseau B. Switch1 utilise l'avant-dernière adresse hôte.

Inscrivez les paramètres IP de chaque périphérique :

Périphérique	Sous-réseau	Adresse IP	Masque	Passerelle
Hôte 1				
Router1-Fa0/0				
Hôte 2				
Hôte 3				
Switch1				
Router1-Fa0/1				

Étape 2 : configuration des ordinateurs hôtes

1. Sur chaque ordinateur, à tour de rôle, cliquez sur **Démarrer > Panneau de configuration > Connexions réseau**. Cliquez avec le bouton droit de la souris sur l'icône du réseau local, puis sélectionnez **Propriétés**. Sous l'onglet **Général**, sélectionnez **Protocole Internet (TCP/IP)**, puis cliquez sur le bouton **Propriétés**.
2. Vérifiez que l'adresse IP de couche 3 de l'hôte 1 se trouve sur un sous-réseau différent de celui de l'hôte 2 et de l'hôte 3. Configurez chaque ordinateur hôte en utilisant les paramètres IP notés à l'étape 1.
3. Vérifiez que chaque ordinateur hôte est correctement configuré à l'aide de la commande **`ipconfig`** et complétez le tableau suivant :

Périphérique	Adresse IP	Masque	Passerelle par défaut
Hôte 1			
Hôte 2			
Hôte 3			

Étape 3 : Configuration du routeur Router1

1. Dans la barre des tâches Windows, démarrez le programme HyperTerminal en cliquant sur **Démarrer > Programmes > Accessoires > Communications > HyperTerminal**. Configurez HyperTerminal pour accéder au routeur Router1. La configuration de Router1 comprend les tâches suivantes :

Tâches (reportez-vous à l'annexe pour obtenir de l'aide sur les commandes)
Spécifiez le nom du routeur : `Router1`
Spécifiez un mot de passe d'exécution privilégié chiffré : `cisco`
Spécifiez un mot de passe d'accès à la console : `class`
Spécifiez un mot de passe d'accès Telnet : `class`
Configurez la bannière MOTD

Configurez l'interface Fa0/0 de Router1 : • définissez la description ; • définissez l'adresse de couche 3 ; • exécutez la commande **no shutdown.**
Configurez l'interface Fa0/1 de Router1 : • définissez la description ; • définissez l'adresse de couche 3 ; • exécutez la commande **no shutdown**.

2. Enregistrez la configuration en mémoire NVRAM.
3. Affichez le contenu de la mémoire RAM :
4. Inscrivez ci-dessous les spécifications de la configuration :

   Nom d'hôte : _____

   Mot de passe « enable secret » : _____

   Mot de passe d'accès à la console : _____

   Mot de passe d'accès Telnet : _____

   Bannière MOTD : _____
5. Affichez les paramètres de configuration de l'interface Fa0/0 : **show interface Fa0/0**

   État de FastEthernet 0/0 (up / down) : _____

   Protocole de ligne : _____

   Adresse MAC :_____
6. Affichez les paramètres de configuration de l'interface Fa0/1 : **show interface Fa0/1**

   État de FastEthernet 0/0 (up / down) : _____

   Protocole de ligne : _____

   Adresse MAC : _____
7. Affichez le récapitulatif des paramètres IP de chaque interface : **show ip interface brief**

```
Interface          IP-Address              OK? Method Status Protocol
FastEthernet0/0
FastEthernet0/1
```

8. Prenez des mesures correctives en cas de problème, puis effectuez un nouveau test.

Étape 4 : configuration du commutateur Switch1

1. Débranchez le câble console de Router1 pour le brancher sur Switch1.
2. Appuyez sur **Entrée** jusqu'à ce que vous receviez une réponse.

3. La configuration de Switch1 comprend les tâches suivantes :

Tâches (reportez-vous à l'annexe pour obtenir de l'aide sur les commandes)
Spécifiez le nom du commutateur- `Switch1`
Spécifiez un mot de passe d'exécution privilégié chiffré- `cisco`
Spécifiez un mot de passe d'accès à la console- `class`
Spécifiez un mot de passe d'accès Telnet- `class`
Configurez la bannière MOTD
Configurez l'interface Fa0/1 de Switch1 : définissez la description ;
Configurez l'interface Fa0/2 de Switch1 : définissez la description ;
Configurez l'interface Fa0/3 de Switch1 : définissez la description ;
Configurez l'adresse IP du VLAN 1 de gestion : • définissez la description ; • définissez l'adresse de couche 3 ; • exécutez la commande **`no shutdown`**.
Configurez l'adresse IP de la passerelle par défaut

4. Affichez le contenu de la mémoire RAM :
5. Inscrivez ci-dessous les spécifications de la configuration :

   Nom d'hôte : _____

   Mot de passe « enable secret » : _____

   Mot de passe d'accès à la console : _____

   Mot de passe d'accès Telnet : _____

   Bannière MOTD : _____

   Interface VLAN 1 : _____

   Adresse IP de la passerelle par défaut : _____
6. Affichez les paramètres de configuration de l'interface VLAN 1 : **`show interface vlan1`**

   État de VLAN 1 (up / down) : _____

   Protocole de ligne : _____

Tâche 4 : vérification de la connectivité du réseau

Étape 1 : vérification de la connectivité à l'aide de la commande `ping`

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.

1. Pour vérifier méthodiquement la connectivité avec chaque périphérique réseau, servez-vous du tableau suivant :

Origine	Destination	Adresse IP	Résultats de la requête ping
Hôte 1	Hôte local (127.0.0.1)		
Hôte 1	Adresse IP de la carte réseau		
Hôte 1	Passerelle (Router1, Fa0/0)		
Hôte 1	Router1, Fa0/1		
Hôte 1	Switch1		
Hôte 1	Hôte 2		
Hôte 1	Hôte 3		
Hôte 2	Hôte local (127.0.0.1)		
Hôte 2	Adresse IP de la carte réseau		
Hôte 2	Hôte 3		
Hôte 2	Switch1		
Hôte 2	Passerelle (Router1, Fa0/1)		
Hôte 2	Router1, Fa0/0		
Hôte 2	Hôte 1		
Hôte 3	Hôte local (127.0.0.1)		
Hôte 3	Adresse IP de la carte réseau		
Hôte 3	Hôte 2		
Hôte 3	Switch1		
Hôte 3	Passerelle (Router1, Fa0/1)		
Hôte 3	Router1, Fa0/0		
Hôte 3	Hôte 1		

2. Lorsqu'un test n'est pas concluant, faites le nécessaire pour établir la connectivité.

   Remarque : si vous n'obtenez pas de résultats en interrogeant les ordinateurs hôtes via la commande ping, désactivez provisoirement le pare-feu sur l'ordinateur et relancez le test. Pour désactiver un pare-feu Windows, cliquez sur **Démarrer > Panneau de configuration > Pare-feu Windows**, choisissez **Désactivé**, puis cliquez sur **OK**.

Étape 2 : vérification de la connectivité locale à l'aide de la commande tracert

1. Sur l'hôte 1, exécutez la commande tracert pour interroger les hôtes 2 et 3.
2. Notez les résultats :

   De l'hôte 1 à l'hôte 2 : _____

   De l'hôte 1 à l'hôte 3 : _____

Étape 3 : vérification de la connectivité de couche 2

1. Si ce n'est déjà fait, débranchez le câble console de Router1 pour le brancher sur Switch1.
2. Appuyez sur la touche **Entrée** jusqu'à obtenir une réponse de Switch1.
3. Exécutez la commande **`show mac-address-table`**. Cette commande permet d'afficher des entrées statiques (unité centrale) et dynamiques, ou acquises.
4. Dressez la liste des adresses MAC et des ports de commutation correspondants :

Adresse MAC	Port de commutation

5. Vérifiez qu'il existe trois adresses MAC acquises dynamiquement (une pour chaque interface : Fa0/1, Fa0/2 et Fa0/3).

Tâche 5 : remarques générales

Analysez les problèmes de configuration physique ou logique rencontrés au cours de ces travaux pratiques. Assurez-vous d'avoir bien compris les procédures destinées à vérifier la connectivité réseau.

Tâche 6 : confirmation

Demandez à votre formateur ou à un autre participant d'introduire un ou deux problèmes dans votre réseau pendant que vous êtes occupé à une autre tâche ou que vous êtes absent de la salle de travaux pratiques. Les problèmes peuvent être d'ordre physique (câble UTP inapproprié) ou logique (adresse IP ou passerelle incorrecte). Pour résoudre les problèmes, procédez comme suit :

1. Faites une inspection visuelle minutieuse. Vérifiez que les voyants de liaison du commutateur Switch1 sont verts.
2. Servez-vous du tableau fourni dans l'exercice 3 ci-dessus pour identifier les problèmes de connectivité. Énumérez les problèmes :

_____

_____

_____

_____

_____

3. Notez la ou les solutions que vous proposez :

_____

_____

_____

_____

_____

4. Testez votre solution. Si la solution est concluante, notez-la. Si la solution est inefficace, poursuivez le dépannage.

_____

_____

_____

_____

_____

Tâche 7 : remise en état

Sauf instruction contraire du formateur, rétablissez la connectivité réseau des ordinateurs hôtes, puis mettez-les hors tension.

Avant de mettre le routeur et le commutateur hors tension, supprimez le fichier de configuration NVRAM sur chaque périphérique à l'aide de la commande **`erase startup-config`**.

Retirez les câbles avec précaution et rangez-les soigneusement. Rebranchez les câbles qui ont été débranchés pour les besoins de ces travaux pratiques.

Enlevez le matériel utilisé durant les travaux pratiques et préparez la salle pour le cours suivant.

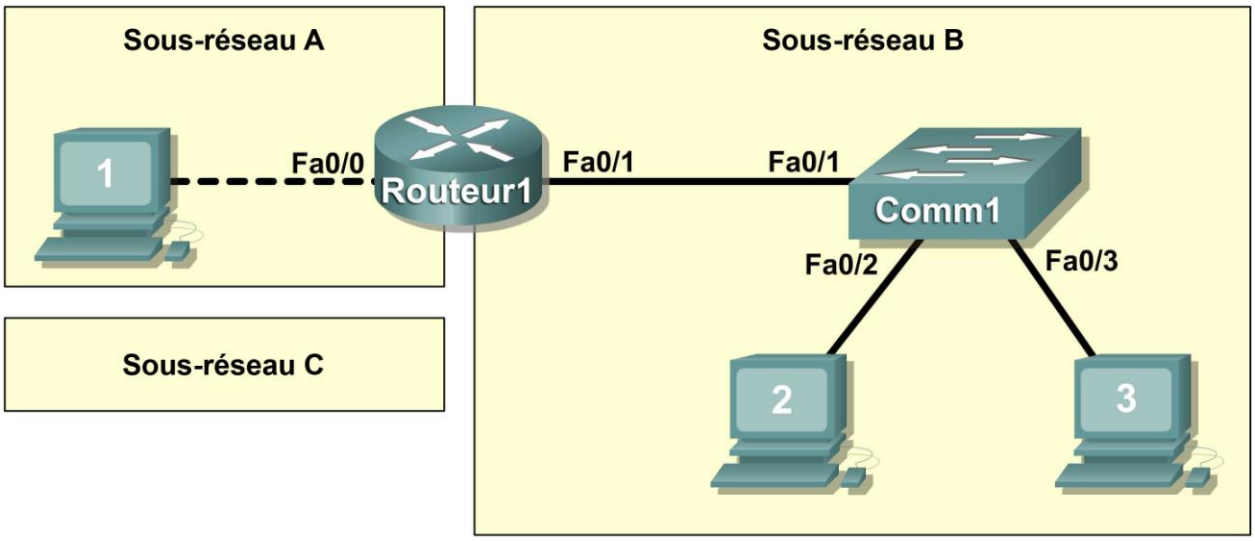
Annexe : liste des commandes Cisco IOS utilisées dans ces travaux pratiques

Objectif	Commande
Passer en mode de configuration globale	**configure terminal** Exemple : Router>**enable** Router# **configure terminal** Router(config)#
Spécifier le nom du périphérique Cisco	**hostname** *name* Exemple : Router(config)# **hostname Router1** Router(config)#
Spécifier un mot de passe chiffré pour empêcher tout accès non autorisé au mode d'exécution privilégié	**Enable secret** *mot de passe* Exemple : Router(config)# **enable secret cisco** Router(config)#
Définir un mot de passe pour empêcher tout accès non autorisé à la console	**password** *password* **login** Exemple : Router(config)# **line con 0** Router(config-line)# **password class** Router(config-line)# **login** Router(config)#
Spécifier un mot de passe pour empêcher tout accès Telnet non autorisé. Lignes vty du routeur : 0 4 Lignes vty du commutateur : 0 15	**password** *password* **login** Exemple : Router(config)# **line vty 0 4** Router(config-line)# **password class** Router(config-line)# **login** Router(config-line)#
Configurez la bannière MOTD.	**Banner motd** % Exemple : Router(config)# **banner motd** % Router(config)#
Configurer une interface de routeur. L'interface du routeur est DÉSACTIVÉE par défaut.	Exemple : Router(config)#**interface Fa0/0** Router(config-if)#**description** *description* Router(config-if)# **ip address** *masque d'adresse* Router(config-if)# **no shutdown** Router(config-if)#

L'interface du commutateur est ACTIVÉE par défaut (l'interface VLAN est DÉSACTIVÉE par défaut)	Exemple : `Switch(config)#`**`interface Fa0/0`** `Switch(config-if)#`**`description`** *`description`* `Switch(config)#`**`interface vlan1`** `Switch(config-if)#` **`ip address`** *`masque d'adresse`* `Switch(config-if)#`**`no shutdown`** `Switch(config-if)#`
Créer une passerelle IP par défaut pour le commutateur	`Switch(config)#`**`ip default-gateway`** *`adresse`*
Enregistrer la configuration en mémoire NVRAM.	**`copy running-config startup-config`** Exemple : `Router#`**`copy running-config startup-config`**

Travaux pratiques 11.5.5 : constitution d'une documentation du réseau avec des commandes d'utilitaire

Diagramme de topologie



Objectifs pédagogiques

- Concevoir la topologie logique des travaux pratiques
- Configurer la topologie physique des travaux pratiques
- Concevoir et configurer la topologie logique du réseau local
- Vérifier la connectivité du réseau local
- Consigner des informations sur le réseau

Contexte

Matériel	Qté	Description
Routeur Cisco	1	Inclus dans l'équipement de travaux pratiques CCNA
Commutateur Cisco	1	Inclus dans l'équipement de travaux pratiques CCNA
*Ordinateur (hôte)	3	Ordinateur de travaux pratiques
Câbles UTP droits de catégorie 5 ou supérieure	3	Relie le routeur Router1 et les hôtes 1 et 2 au commutateur Switch1
Câble de croisement UTP de catégorie 5	1	Relie l'hôte 1 à Router1
Câble console (de renversement)	1	Relie l'hôte 1 à la console de Router1

Tableau 1. Équipement et matériel des travaux pratiques Eagle 1

Regroupez l'équipement et les câbles nécessaires. Pour configurer les travaux pratiques, vérifiez que vous disposez bien de l'équipement répertorié dans le tableau 1.

Dans le cadre de ces travaux pratiques, les résultats du routeur et des hôtes seront copiés depuis les périphériques vers le Bloc-notes en vue d'être utilisés pour la consignation d'informations sur le réseau. Vous trouverez dans l'annexe 1 des tableaux dont vous pouvez vous servir pour y copier les résultats ou pour créer vos propres tableaux.

Scénario

Les informations sur le réseau constituent un outil très important pour l'organisation. Un réseau parfaitement décrit permet aux ingénieurs de gagner beaucoup de temps lorsqu'il s'agit de le dépanner ou de planifier son extension.

Dans le cadre de ces travaux pratiques, les participants vont devoir créer un petit réseau, ce qui suppose de connecter des périphériques réseau et de configurer les ordinateurs hôtes pour une connectivité réseau de base. Subnet A et Subnet B sont des sous-réseaux nécessaires dès à présent. Subnet C est un projet de sous-réseau qui n'est pas encore connecté au réseau.

Tâche 1 : configuration de la topologie logique du réseau local (LAN)

À partir de l'adresse IP 209.165.200.224 / 27 (adresse/masque), concevez un modèle d'adressage IP qui remplisse les conditions suivantes :

Sous-réseau	Nombre d'hôtes
Subnet A	2
Subnet B	Entre 2 et 6
Subnet C	Entre 10 et 12

Étape 1 : conception du bloc d'adresses de Subnet C

Abordez la phase de conception du réseau logique en respectant les critères de Subnet C, qui nécessite le bloc d'adresses IP le plus grand. En utilisant des nombres binaires pour créer votre tableau de sous-réseaux, choisissez le prochain bloc d'adresses disponible prenant en charge Subnet C.

Complétez le tableau suivant à partir des informations d'adresse IP de SubnetC :

Adresse réseau	Masque	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion

Quel est le masque de bits en binaire ? _____

Étape 2 : conception du bloc d'adresses de Subnet B

Respectez les critères de Subnet B : le prochain bloc d'adresses IP le plus grand. En utilisant des nombres binaires pour créer votre tableau de sous-réseaux, choisissez le premier bloc d'adresses prenant en charge Subnet B.

Complétez le tableau suivant à partir des informations d'adresse IP de Subnet B :

Adresse réseau	Masque	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion

Quel est le masque de bits en binaire ? _____

Étape 3 : conception du bloc d'adresses de Subnet A

Respectez les critères de Subnet A : le plus petit bloc d'adresses IP. En utilisant des nombres binaires pour créer votre tableau de sous-réseaux, choisissez le prochain bloc d'adresses disponible prenant en charge Subnet A.

Complétez le tableau suivant à partir des informations relatives aux adresses IP de Subnet A :

Adresse réseau	Masque	Première adresse d'hôte	Dernière adresse d'hôte	Diffusion

Quel est le masque de bits en binaire ? _____

Tâche 2 : configuration de la topologie physique des travaux pratiques

Étape 1 : connexion physique des périphériques des travaux pratiques

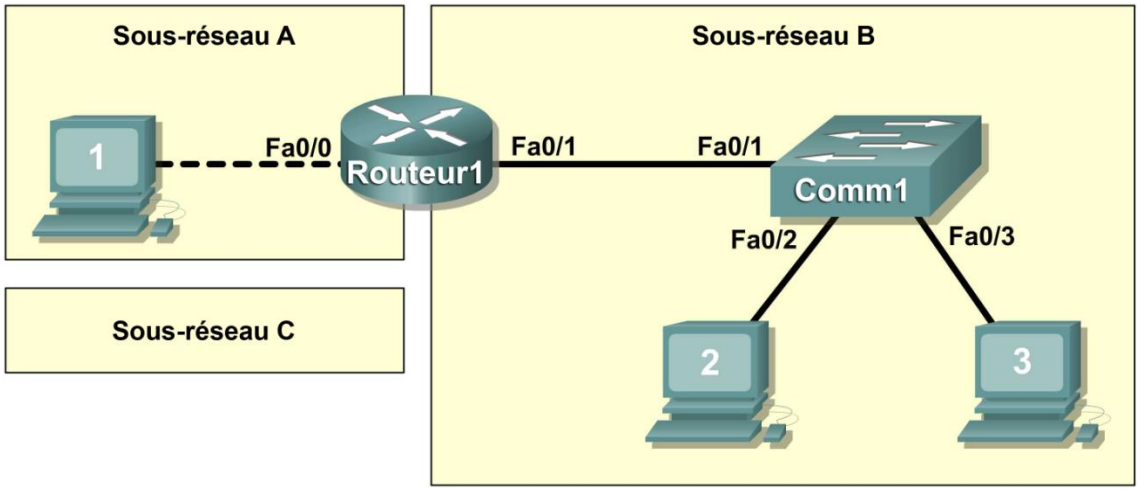


Figure 1. Installation du réseau

Raccordez les périphériques réseau comme indiqué dans la figure 1. Tenez compte du câble de croisement requis entre l'hôte 1 et le routeur Router1.

Si ce n'est déjà fait, mettez tous les périphériques sous tension.

Étape 2 : inspection visuelle des connexions réseau

Après avoir installé les périphériques réseau, prenez le temps de vérifier les connexions. C'est en faisant attention aux détails dès à présent que vous limiterez par la suite le temps passé à résoudre des problèmes de connectivité.

Tâche 3 : configuration de la topologie logique

Étape 1 : consignation des paramètres du réseau logique

Les ordinateurs hôtes utilisent les deux premières adresses IP du sous-réseau. Le routeur du réseau utilise la DERNIÈRE adresse d'hôte réseau. Inscrivez les paramètres IP de chaque périphérique :

Périphérique	Sous-réseau	Adresse IP	Masque	Passerelle
Router1-Fa0/0				
Hôte 1				
Router1-Fa0/1				
Hôte 2				
Hôte 3				
Switch1	N/A	N/A	N/A	N/A

Étape 2 : configuration des ordinateurs hôtes

Sur chaque ordinateur, à tour de rôle, sélectionnez Démarrer | Panneau de configuration | Connexions réseau. Identifiez l'icône du périphérique Connexion au réseau local. À l'aide du pointeur de la souris, mettez l'icône en surbrillance, cliquez avec le bouton droit de la souris, puis sélectionnez Propriétés. Mettez Protocole Internet (TCP/IP) en surbrillance, puis sélectionnez Propriétés.

Vérifiez que l'adresse IP de couche 3 de l'hôte 1 se trouve sur un sous-réseau différent de celui de l'hôte 2 et de l'hôte 3. Configurez chaque ordinateur hôte en utilisant les paramètres IP notés à l'étape 1.

Vérifiez que chaque ordinateur hôte est correctement configuré à l'aide de la commande **`ipconfig /all`**. Consignez les informations dans l'annexe 1, Consignation d'informations sur le réseau.

Étape 3 : configuration du routeur Router1

Dans la barre des tâches Windows, démarrez le programme HyperTerminal en cliquant sur Démarrer | Programmes | Accessoires | Communications | HyperTerminal. Configurez HyperTerminal pour accéder au routeur Router1. La configuration de Router1 comprend les tâches suivantes :

Tâche
Spécifiez le nom du routeur- `Router1`
Spécifiez un mot de passe d'exécution privilégié chiffré- `cisco`
Spécifiez un mot de passe d'accès à la console- `class`
Spécifiez un mot de passe d'accès Telnet- `class`
Configurez la bannière MOTD.

Configurez l'interface Fa0/0 de Router1- définissez la description ; définissez l'adresse de couche 3 exécutez la commande **no shutdown**.
Configurez l'interface Fa0/1 de Router1- définissez la description ; définissez l'adresse de couche 3 exécutez la commande **no shutdown.**

Enregistrez la configuration en mémoire NVRAM.

Affichez le contenu de la mémoire RAM :

Copiez le résultat de la configuration dans le tableau de configuration de Router1, dans l'annexe 1.

Copiez le résultat des commandes **show interface fa0/0** et **show interface fa0/1** dans les tableaux de configuration des interfaces de Router1, dans l'annexe 1.

Copiez le résultat de la commande **show ip interface brief** dans le tableau de configuration des adresses IP de Router1, dans l'annexe 1.

Étape 4 : configuration du commutateur Switch1

Débranchez le câble console de Router1 pour le brancher sur Switch1. Appuyez sur Entrée jusqu'à ce que vous receviez une réponse. La configuration de Switch1 comprend les tâches suivantes :

Tâche
Spécifiez le nom du commutateur- Switch1
Spécifiez un mot de passe d'exécution privilégié chiffré- cisco
Spécifiez un mot de passe d'accès à la console- class
Spécifiez un mot de passe d'accès Telnet- class
Configurez la bannière MOTD.
Configurez l'interface Fa0/1 de Switch1- définissez la description
Configurez l'interface Fa0/2 de Switch1- définissez la description
Configurez l'interface Fa0/3 de Switch1- définissez la description

Affichez le contenu de la mémoire RAM :

Copiez le résultat de la configuration dans le tableau de configuration de Switch1, dans l'annexe 1.

Copiez le résultat de la commande **show mac address-table** dans la table d'adresses MAC de Switch1, dans l'annexe 1.

Tâche 4 : vérification de la connectivité du réseau

Étape 1 : vérification de la connectivité à l'aide de la commande ping

La commande ping permet de vérifier la connectivité sur le réseau. Il est très important de disposer d'une connectivité sur tout le réseau. En cas d'échec, une mesure corrective doit être prise.

**REMARQUE : si vous n'obtenez pas de résultats en interrogeant les ordinateurs hôtes via la commande ping, désactivez provisoirement le pare-feu sur l'ordinateur et relancez le test. Pour désactiver un pare-feu Windows, sélectionnez Démarrer | Panneau de configuration | Pare-feu Windows, choisissez Désactivé, puis OK.

Pour vérifier méthodiquement la connectivité avec chaque périphérique réseau, servez-vous du tableau ci-dessous. Lorsque le test n'est pas concluant, faites le nécessaire pour établir la connectivité :

Origine	Destination	Adresse IP	Résultats de la requête ping
Hôte 1	Hôte local (127.0.0.1)		
Hôte 1	Adresse IP de la carte réseau		
Hôte 1	Passerelle (Router1, Fa0/0)		
Hôte 1	Router1, Fa0/1		
Hôte 1	Hôte 2		
Hôte 1	Hôte 3		
Hôte 2	Hôte local (127.0.0.1)		
Hôte 2	Adresse IP de la carte réseau		
Hôte 2	Hôte 3		
Hôte 2	Passerelle (Router1, Fa0/1)		
Hôte 2	Router1, Fa0/0		
Hôte 2	Hôte 1		
Hôte 3	Hôte local (127.0.0.1)		
Hôte 3	Adresse IP de la carte réseau		
Hôte 3	Hôte 2		
Hôte 3	Passerelle (Router1, Fa0/1)		
Hôte 3	Router1, Fa0/0		
Hôte 3	Hôte 1		

Étape 2 : vérification de la connectivité locale à l'aide de la commande `tracert`

Outre le test de la connectivité, la commande tracert peut également être utilisée comme testeur de débit rudimentaire pour obtenir une référence. Autrement dit, dans le cas d'un trafic minimum, les résultats de tracert peuvent être comparés aux périodes de fort trafic. Les résultats peuvent être utilisés pour justifier des mises à niveau d'équipement ou de nouveaux achats.

À partir de l'hôte 1, exécutez la commande tracert pour interroger Router1, l'hôte 2 et l'hôte 3. Consignez les résultats de la commande Tracert de l'hôte 1 (annexe A).

À partir de l'hôte 2, exécutez la commande tracert pour interroger l'hôte 3, Router1 et l'hôte 1. Consignez les résultats de la commande Tracert de l'hôte 2 (annexe A).

À partir de l'hôte 3, exécutez la commande tracert pour interroger l'hôte 2, Router1 et l'hôte 1. Consignez les résultats de la commande Tracert de l'hôte 3 (annexe A).

Tâche 5 : consignation d'informations sur le réseau

Compte tenu des tâches accomplies jusqu'à présent, vous penserez probablement qu'il ne reste plus rien à faire. En effet, le réseau est configuré (physique et logique), testé, et le résultat des commandes a été enregistré dans les tables.

La dernière étape de la procédure de consignation d'informations sur le réseau consiste à organiser les résultats. Au cours de cette étape, demandez-vous quels seront les besoins potentiels dans six mois ou un an. Exemple :

À quel moment le réseau a-t-il été créé ?
À quel moment les informations sur le réseau ont-elles été consignées ?
A-t-il fallu surmonter des difficultés importantes ?
Quelle est la personne qui a effectué la configuration (un talent pareil doit être suivi à la trace) ?
Quelle est la personne qui a consigné les informations (un talent pareil doit être suivi à la trace) ?

Les réponses à ces questions doivent être insérées dans la documentation, éventuellement sous la forme d'une lettre d'accompagnement.

Veillez à inclure les informations suivantes :
une copie de la topologie physique ;
une copie de la topologie logique.

Organisez ces informations de façon professionnelle, puis soumettez-les à votre formateur.

Tâche 6 : remarques générales

Analysez les problèmes de configuration physique ou logique rencontrés au cours de ces travaux pratiques. Assurez-vous d'avoir bien compris les procédures destinées à vérifier la connectivité réseau.

Tâche 7 : confirmation

Demandez à votre formateur ou à un autre participant d'introduire un ou deux problèmes dans votre réseau pendant que vous êtes occupé à une autre tâche ou que vous êtes absent de la salle de travaux pratiques. Les problèmes peuvent être d'ordre physique (câbles branchés sur le commutateur) ou logique (adresse IP ou passerelle incorrecte).

Servez-vous des informations sur votre réseau pour procéder au dépannage et remédier aux problèmes :

1. Faites une inspection visuelle minutieuse. Vérifiez que les voyants de liaison du commutateur Switch1 sont verts.

2. Servez-vous des informations sur votre réseau pour comparer la configuration actuelle à la configuration théorique :

   _____
   _____
   _____
   _____
   _____

3. Notez la ou les solutions que vous proposez :

   _____
   _____
   _____
   _____
   _____

4. Testez votre solution. Si la solution est concluante, notez-la. Si la solution est inefficace, poursuivez le dépannage.

   _____
   _____
   _____
   _____
   _____
   _____

Tâche 8 : remise en état

Sauf instruction contraire du formateur, rétablissez la connectivité réseau des ordinateurs hôtes, puis mettez-les hors tension.

Avant de mettre le routeur et le commutateur hors tension, supprimez le fichier de configuration NVRAM sur chaque périphérique à l'aide de la commande **`erase startup-config`**.

Retirez les câbles avec précaution et rangez-les soigneusement. Rebranchez les câbles qui ont été débranchés pour les besoins de ces travaux pratiques.

Enlevez le matériel utilisé durant les travaux pratiques et préparez la salle pour le cours suivant.

Annexe 1- Consignation d'informations sur le réseau

Tables d'hôtes créées à l'étape 2 de la tâche 3 :

Configuration réseau hôte 1	
Nom d'hôte	
Routage IP activé	
Carte Ethernet	
Description	
Adresse physique	
Adresse IP	
Masque de sous-réseau	
Passerelle par défaut	

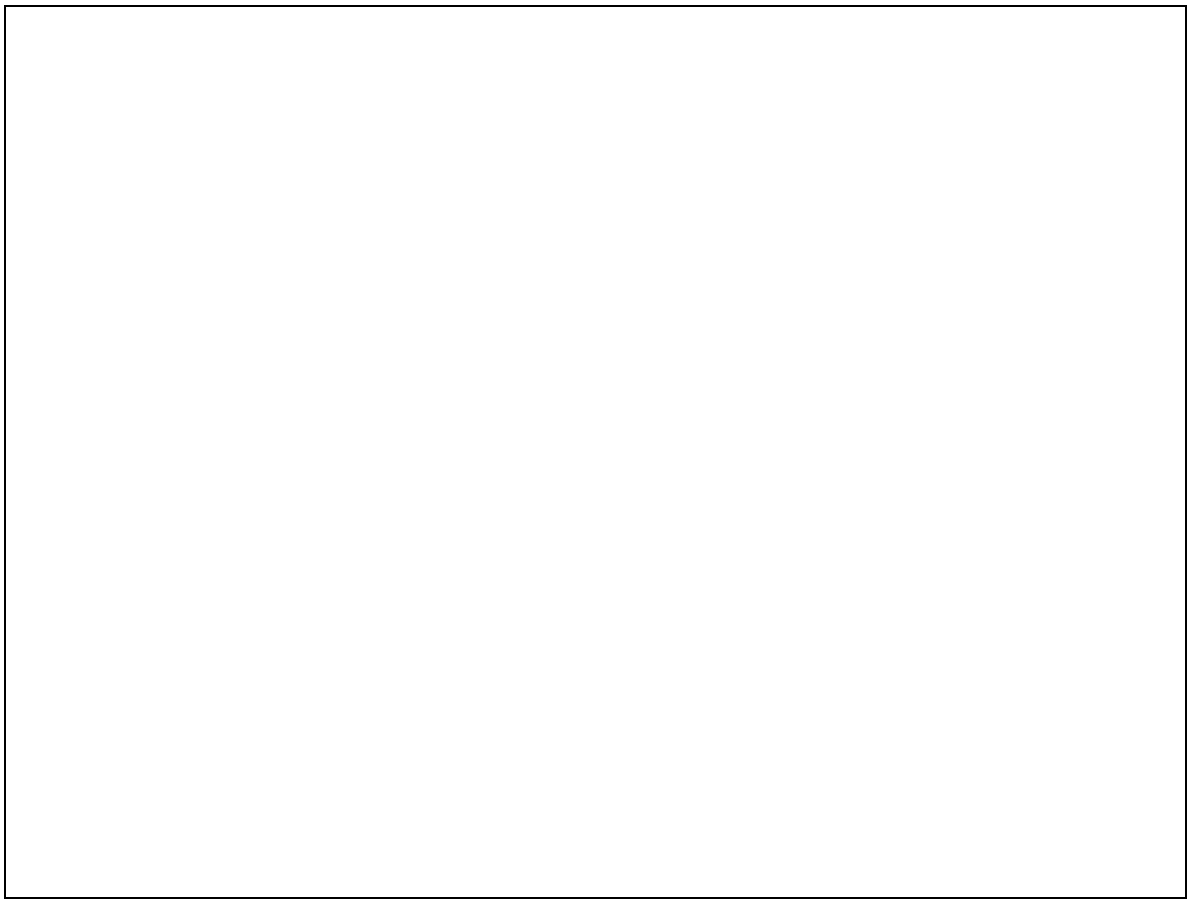
Configuration réseau hôte 2	
Nom d'hôte	
Routage IP activé	
Carte Ethernet	
Description	
Adresse physique	
Adresse IP	
Masque de sous-réseau	
Passerelle par défaut	

Configuration réseau hôte 3	
Nom d'hôte	
Routage IP activé	
Carte Ethernet	
Description	
Adresse physique	
Adresse IP	
Masque de sous-réseau	
Passerelle par défaut	

Configuration de Router1 effectuée à l'étape 3 de la tâche 3 :

Configuration de Router1

Configuration de l’interface Fa0/0 de Router1 effectuée à l’étape 3 de la tâche 2 :



Configuration de l’interface fa0/1 de Router1 effectuée à l’étape 3 de la tâche 3 :

Configuration des adresses IP de Router1 effectuée à l’étape 3 de la tâche 3 :

Configuration de Switch1 effectuée à l’étape 4 de la tâche 3 :

Table d’adresses MAC de Switch1, tâche 3, étape 4 :

Résultats de la commande Traceroute de l’hôte 1, tâche 4, étape 2 :

Résultats de la commande Traceroute de l’hôte 2, tâche 4, étape 2 :

Résultats de la commande Traceroute de l’hôte 3, tâche 4, étape 2 :

Travaux pratiques 11.5.6 : étude de cas finale : analyse de datagramme avec Wireshark

Objectifs pédagogiques

À l'issue de cet exercice, les participants seront en mesure de montrer comment effectuer les opérations suivantes :

- Construire un segment TCP et décrire les champs du segment
- Construire un paquet IP et décrire les champs du paquet
- Construire une trame Ethernet II et décrire les champs de la trame
- Décrire le contenu d'une REQUÊTE ARP et d'une RÉPONSE ARP

Contexte

Ces travaux pratiques nécessitent deux fichiers de paquets capturés et Wireshark, analyseur de protocole réseau. Téléchargez les fichiers suivants sur le serveur Eagle, puis installez Wireshark sur votre ordinateur, si ce n'est déjà fait :

- eagle1_web_client.pcap (décrit)
- eagle1_web_server.pcap (référence uniquement) ;
- wireshark.exe.

Scénario

Cet exercice décrit la séquence de datagrammes créés et transmis au sein d'un réseau entre un client Web (PC_client) et un serveur Web (eagle1.example.com). C'est en maîtrisant l'insertion séquentielle de paquets sur le réseau que les participants pourront logiquement traiter les pannes. Pour plus de concision et de clarté, le bruit des paquets réseau a été omis dans les captures. Avant d'exécuter un analyseur de protocole réseau sur un réseau qui appartient à un tiers, veillez à vous procurer une autorisation écrite.

La figure 1 illustre la topologie de ces travaux pratiques.

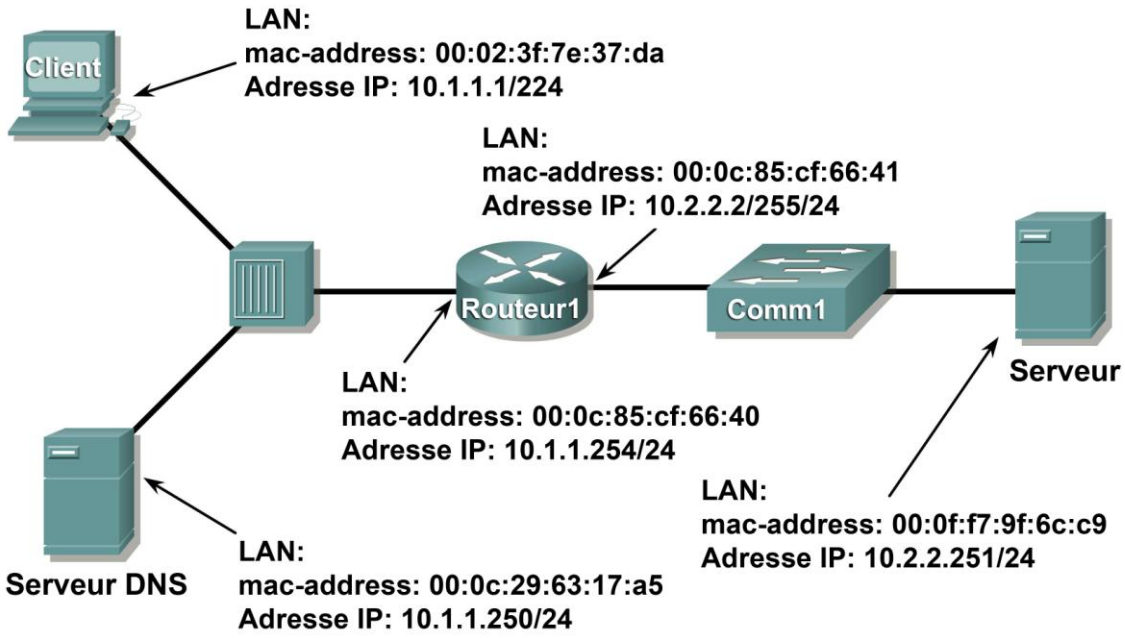


Figure 1. Topologie de réseau

Les paramètres de configuration IP et le contenu de la mémoire cache ARP sont affichés à l'aide des outils de ligne de commande Microsoft ®. Reportez-vous à la figure 2.

```
C: > ipconfig / all
Windows IP Configuration
Ethernet adapter Local Area Connection:
     Connection-specific DNS Suffix  . :
     Description . . . . . . . . . . . : Intel(R) PRO/1000 MT
                                         Network Connection
     Physical Address. . . . . . . . . : 00:02:3f:7e:37:da
     Dhcp Enabled. . . . . . . . . . . : No
     IP Address. . . . . . . . . . . . : 10.1.1.1
     Subnet Mask . . . . . . . . . . . : 255.255.255.0
     Default Gateway . . . . . . . . . : 10.1.1.254
     DNS Servers . . . . . . . . . . . : 10.1.1.250
C: > arp –a
No ARP Entries Found
C: >
```

Figure 2. État initial du réseau sur le PC Client.

Comme l'indique la figure 3, on active un client Web et on saisit l'URL eagle1.example.com. Cela permet d'établir une communication avec le serveur Web et de capturer les paquets.

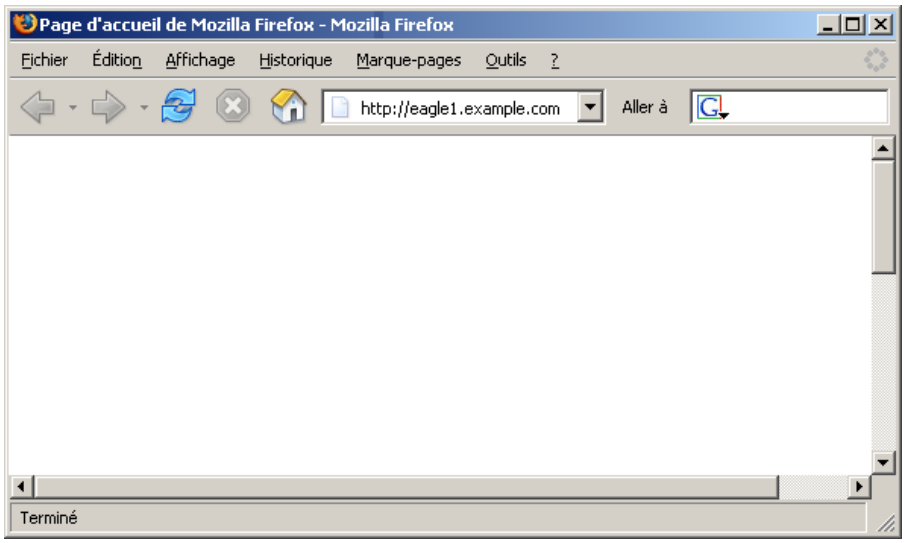


Figure 3. Navigateur Web sur le PC Client.

Tâche 1 : préparation des travaux pratiques

Étape 1 : démarrage de Wireshark sur votre ordinateur

Reportez-vous à la figure 4 pour visualiser les différences par rapport à l'affichage par défaut. Désactivez `Main toolbar`, `Filter toolbar` et `Packet Bytes`. Vérifiez que `Packet List` et `Packet Details` sont activés. Pour éviter toute traduction automatique des adresses MAC, désélectionnez `Name Resolution` pour `MAC layer` et `Transport Layer`.

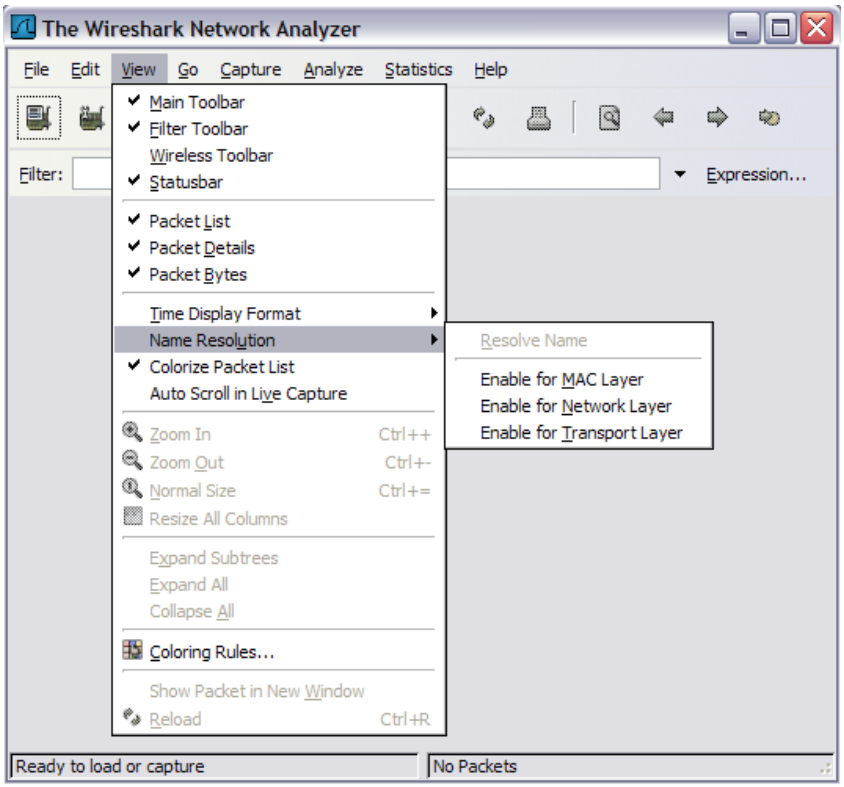


Figure 4. Modifications de l'affichage par défaut de Wireshark.

Étape 2 : importation de la capture du client Web, `eagle1_web_client.pcap`

Un écran similaire à la figure 5 apparaît. Plusieurs menus et sous-menus déroulants sont disponibles. Vous distinguez également deux fenêtres de données distinctes. La fenêtre supérieure de Wireshark répertorie tous les paquets capturés. La fenêtre du bas contient les détails des paquets. Dans la fenêtre du bas, chaque ligne contient une case à cocher ; ☒ indique la présence d'informations supplémentaires.

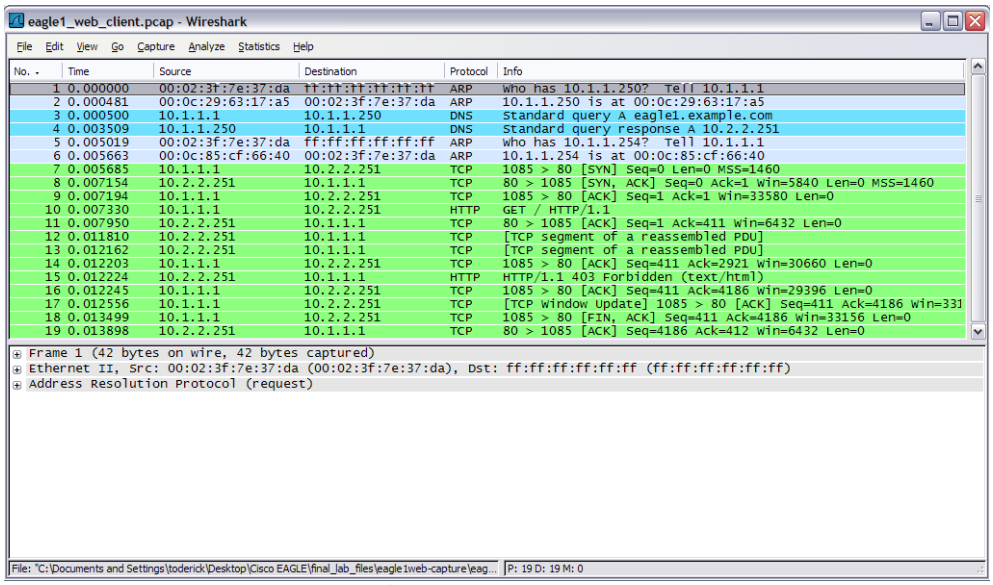


Figure 5. Wireshark après le chargement du fichier eagle1_web_client.pcap.

Tâche 2 : analyse du flux de données transitant par le réseau

Étape 1 : analyse du fonctionnement de la couche transport

Lorsque PC_Client construit le datagramme pour une connexion avec eagle1.example.com, celui-ci transite par les différentes couches réseau. À chaque couche, des informations d'en-tête importantes sont ajoutées. Cette communication ayant pour origine un client Web, le protocole de la couche transport est TCP. Observez le segment TCP illustré dans la figure 6. PC_Client crée une adresse de port TCP interne dans la communication 1085. Le port 80 sur le serveur Web est identifié. De même, le système crée un numéro d'ordre en interne. Des données fournies par la couche application sont incluses. Certaines informations n'étant pas connues de PC_Client, elles doivent être obtenues via d'autres protocoles réseau.

Il n'y a pas de numéro d'accusé de réception. Pour que ce segment puisse atteindre la couche réseau, la connexion TCP en trois étapes doit être établie.

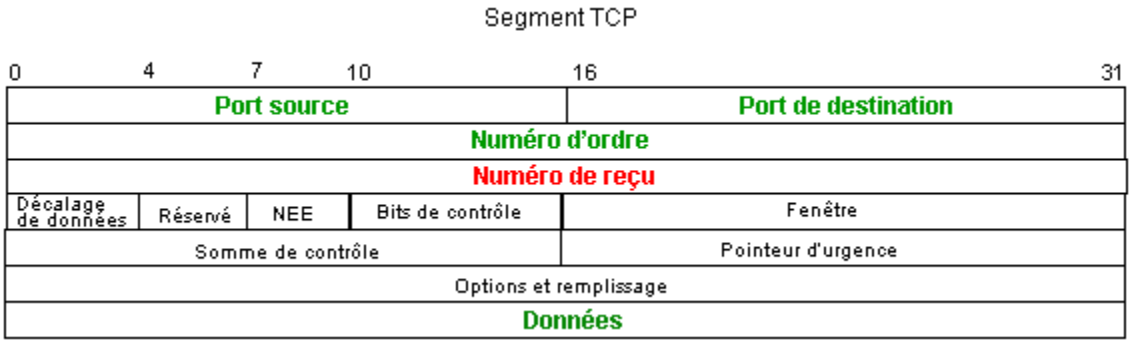


Figure 6. Champs du segment TCP.

Étape 2 : analyse du fonctionnement de la couche réseau

Au niveau de la couche réseau, le paquet IPv4 (IP) comporte plusieurs champs renseignés. Reportez-vous à la figure 7. Par exemple, le paquet version (IPv4) est connu, tout comme l'adresse IP source.

eagle1.example.com est la destination de ce paquet. L'adresse IP correspondante doit être identifiée via DNS (Domain Name Services). Tant que le datagramme de la couche supérieure n'a pas été reçu, les champs associés aux protocoles de couche supérieure sont vides.

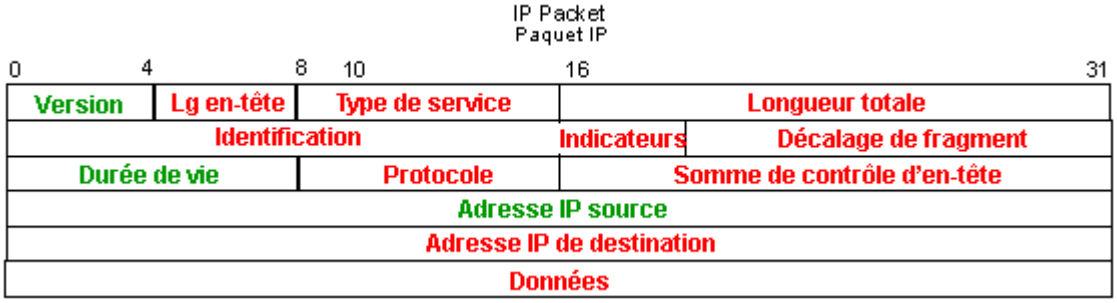


Figure 7. Champs du paquet IP.

Étape 3 : analyse du fonctionnement de la couche liaison de données

Avant d'être inséré sur le support physique, le datagramme doit être encapsulé à l'intérieur d'une trame. Reportez-vous à la figure 8. Si PC_Client connaît l'adresse MAC source, il doit en revanche trouver l'adresse MAC de destination.

Celle-ci doit être identifiée.

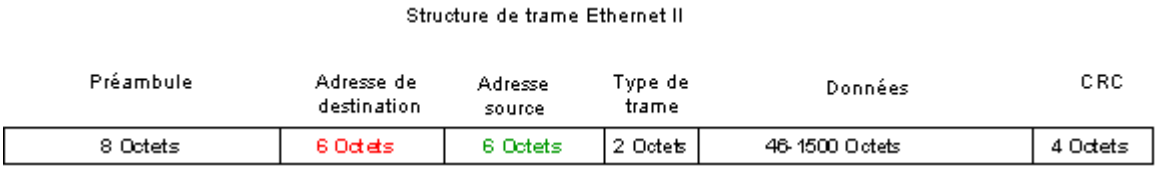


Figure 8. Champs d'une trame Ethernet II

Tâche 3 : analyse des paquets capturés

Étape 1 : analyse des étapes parcourues par le flux de données

Une analyse des informations manquantes s'avèrera utile pour suivre les étapes parcourues par les paquets capturés :

a. Le segment TCP ne peut pas être construit, car le champ d'accusé de réception est vide. Une connexion TCP en trois étapes doit d'abord être établie avec eagle1.example.com.

b. La connexion TCP en trois étapes n'est pas possible, car PC_Client ne connaît pas l'adresse IP de eagle1.example.com. Il faut donc que PC_Client envoie une requête DNS au serveur DNS.

c. Le serveur DNS ne peut pas être interrogé, car l'adresse MAC du serveur DNS n'est pas connue. Le protocole ARP est diffusé sur le réseau local pour identifier l'adresse MAC du serveur DNS.

d. L'adresse MAC du serveur eagle1.example.com est inconnue. Le protocole ARP est diffusé sur le réseau local pour identifier l'adresse MAC de destination du serveur eagle1.example.com.

Étape 2 : analyse de la requête ARP

Reportez-vous à la liste de paquets Wireshark n°1. La trame capturée est une requête ARP (Address Resolution Protocol). Le contenu de la trame Ethernet II s'affiche si vous cochez la case située dans la deuxième ligne de la fenêtre Packet Details. Il est possible d'afficher le contenu de la requête ARP en cliquant sur la ligne ARP Request dans la fenêtre Packet Details.

1. Quelle est l'adresse MAC source de la requête ARP ? _____

2. Quelle est l'adresse MAC de destination de la requête ARP ? _____

3. Quelle est l'adresse IP inconnue dans la requête ARP ? _____

4. Quel est le type de la trame Ethernet II ? _____

Étape 3 : examen de la réponse ARP

Reportez-vous à la liste de paquets Wireshark n°2. Le serveur DNS a envoyé une réponse ARP.

1. Quelle est l'adresse MAC source de la réponse ARP ? _____
2. Quelle est l'adresse MAC de destination de la requête ARP ? _____
3. Quel est le type de la trame Ethernet II ? _____
4. Quelle est l'adresse IP de destination dans la réponse ARP ? _____
5. Après observation du protocole ARP, que pouvez-vous déduire d'une adresse de requête ARP et d'une adresse de destination de réponse ARP ?
   _____
   _____
   _____
6. Pourquoi le serveur DNS n'a pas envoyé de requête ARP pour l'adresse MAC du PC_Client ?
   _____
   _____

Étape 4 : analyse de la requête DNS

Reportez-vous à la liste de paquets Wireshark n°3. PC_Client a envoyé une requête DNS au serveur. En vous aidant de la fenêtre Packet Details, répondez aux questions suivantes :

1. Quel est le type de la trame Ethernet II ? _____
2. Quel est le protocole de la couche transport, et quel est le numéro de port de destination ?
   _____

Étape 5 : analyse de la réponse à la requête DNS

Reportez-vous à la liste de paquets Wireshark n°4. Le serveur DNS a envoyé une réponse à PC_Client. En vous aidant de la fenêtre Packet Details, répondez aux questions suivantes :

1. Quel est le type de la trame Ethernet II ? _____
2. Quel est le protocole de la couche transport, et quel est le numéro de port de destination ?
   _____
3. Quelle est l'adresse IP du serveur eagle1.example.com ? _____
4. L'un de vos collègues, administrateur de pare-feu, vous demande s'il y a une raison de ne pas empêcher l'entrée de tous les paquets UDP sur le réseau interne. Quelle est votre réponse ?
   _____
   _____
   _____
   _____

Étape 6 : analyse de la requête ARP

Reportez-vous aux listes de paquets Wireshark n°5 et 6. PC_Client a envoyé une requête ARP à l'adresse IP 10.1.1.254.

1. Cette adresse IP est-elle différente de l'adresse IP du serveur eagle1.example.com ? Expliquez.
   _____
   _____

Étape 7 : analyse de la connexion TCP en trois étapes

Reportez-vous aux listes de paquets Wireshark n°7, 8 et 9. Ces captures décrivent la connexion TCP en trois étapes entre PC_Client et eagle1.example.com. Au départ, seul l'indicateur TCP SYN est associé au datagramme transmis par PC_Client, (numéro d'ordre 0). eagle1.example.com répond avec les indicateurs TCP ACK et SYN avec 1 accusé de réception et 0 séquence. Dans la liste de paquets, une valeur est inconnue : **MSS=1460**. Il s'agit de la taille maximale d'un segment. Lorsqu'un segment TCP est transporté sur IPv4, la valeur de MSS correspond à la taille maximale d'un datagramme IPv4 moins 40 octets. Cette valeur est envoyée au début de la connexion. C'est également à ce moment que les fenêtres dynamiques TCP sont définies.

1. Si la valeur initiale de séquence TCP du PC_Client est égale à 0, pourquoi le serveur eagle1.example a-t-il répondu avec un accusé de réception de 1 ?
   _____
   _____

2. Dans eagle1.example.com, à la ligne n°8, que signifie la valeur 0x04 d'indicateur IP ?
   _____

3. Lorsque le PC_Client termine la connexion TCP en 3 étapes (ligne n° 9 dans la fenêtre Packet List de Wireshark), quels sont les états des indicateur TCP renvoyés à eagle1.example.com ?
   _____

Tâche 4 : analyse finale

Étape 1 : résultats de Wireshark par rapport au processus

Il a fallu neuf datagrammes transmis entre PC_Client, le serveur DNS, la passerelle et eagle1.example.com pour que PC_Client obtienne suffisamment de paramètres pour envoyer la requête initiale à eagle1.example.com. La liste de paquets Wireshark n°10 montre que PC_Client a envoyé une requête GET.

1. Indiquez le numéro de la fenêtre Packet List de Wireshark qui satisfait à chacune des entrées manquantes suivantes :

   a. Le segment TCP ne peut pas être construit, car le champ d'accusé de réception est vide. Une connexion TCP en trois étapes doit d'abord être établie avec eagle1.example.com. _____

   b. La connexion TCP en trois étapes n'est pas possible, car PC_Client ne connaît pas l'adresse IP de eagle1.example.com. Il faut donc que PC_Client envoie une requête DNS au serveur DNS. _____

   c. Le serveur DNS ne peut pas être interrogé, car l'adresse MAC du serveur DNS n'est pas connue. Le protocole ARP est diffusé sur le réseau local pour identifier l'adresse MAC du serveur DNS. _____

   d. L'adresse MAC permettant à la passerelle d'atteindre eagle1.example.com est inconnue. Le protocole ARP est diffusé sur le réseau local pour découvrir l'adresse MAC de destination de la passerelle. _____

2. La ligne n° 11 de la fenêtre Packet List de Wireshark est un accusé de réception du serveur eagle1.example.com à la demande GET du PC_Client (ligne n° 10 de la fenêtre Packet List de Wireshark).

3. Les listes de paquets Wireshark n°12, 13 et 15 affichent des segments TCP transmis par eagle1.example.com. Les listes n°14 et 16 sont des datagrammes ACK transmis par PC_Client.

4. Pour vérifier les datagrammes ACK, sélectionnez la liste de paquets n°14. Ensuite, faites défiler l'écran jusqu'au bas de la liste détaillée, puis développez la trame [SEQ/ACK]. À quel datagramme du serveur eagle1.example.com le datagramme ACK de la ligne n° 14 de la fenêtre Packet List de Wireshark répond-il ? _____

5. PC_Client transmet la liste n°17 à eagle1.example.com. Analysez les paramètres de la trame [analyse SEQ/ACK]. À quoi sert ce datagramme ? _____

6. Lorsque PC_Client a terminé, les indicateurs TCP ACK et FIN sont transmis et figurent dans la liste de paquets Wireshark n°18. eagle1.example.com répond avec un datagramme TCP ACK et met fin à la session TCP.

Étape 2 : utilisation du flux TCP de Wireshark

L'analyse du contenu des paquets est parfois fastidieuse et peut vous amener à faire des erreurs. Wireshark intègre une option qui construit le flux TCP dans une fenêtre distincte. Pour utiliser cette fonctionnalité, sélectionnez d'abord un datagramme TCP dans la fenêtre Packet List de Wireshark. Ensuite, sélectionnez les options de menu Wireshark Analyze | Follow TCP Stream. Une fenêtre similaire à la figure 9 s'affiche à l'écran.

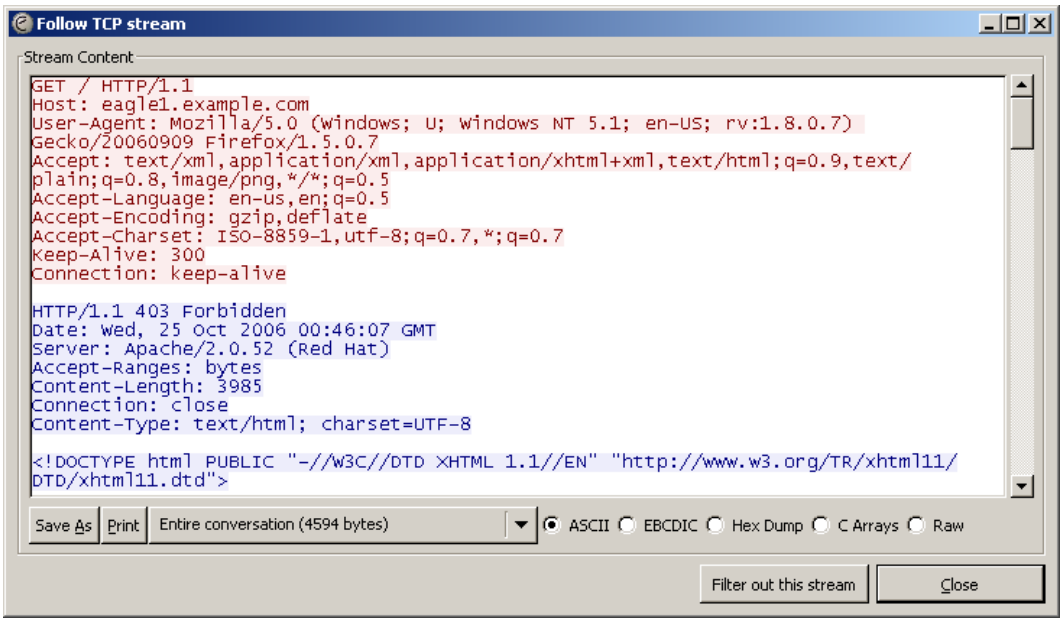


Figure 9. Aperçu de la fenêtre de flux TCP.

Tâche 5 : conclusion

L'utilisation d'un analyseur de protocole est souvent un outil d'apprentissage efficace pour assimiler les éléments importants qui constituent la communication réseau. Dès lors que l'administrateur réseau s'est familiarisé avec les protocoles de communication, ce même analyseur de protocole peut devenir un outil de dépannage efficace en cas de panne réseau. Par exemple, plusieurs raisons peuvent empêcher un navigateur Web de se connecter à un serveur Web. Un analyseur de protocole désignera les requêtes ARP et DNS infructueuses, ainsi que les paquets non reconnus.

Tâche 6 : résumé

Au cours de cet exercice, le participant a compris comment un client et un serveur Web communiquent. Les protocoles en arrière-plan, notamment DNS et ARP, sont utilisés pour combler les parties manquantes des paquets IP et des trames Ethernet. Pour qu'une session TCP puisse démarrer, la connexion TCP en 3 étapes doit créer un chemin d'accès fiable et fournir aux deux extrémités communicantes les paramètres d'en-tête TCP d'origine. Au final, la session TCP est détruite de façon ordonnée, dès lors que le client émet un indicateur TCP FIN.

11.6.1 : projet d'intégration des compétences : configuration et test de votre réseau

Diagramme de topologie

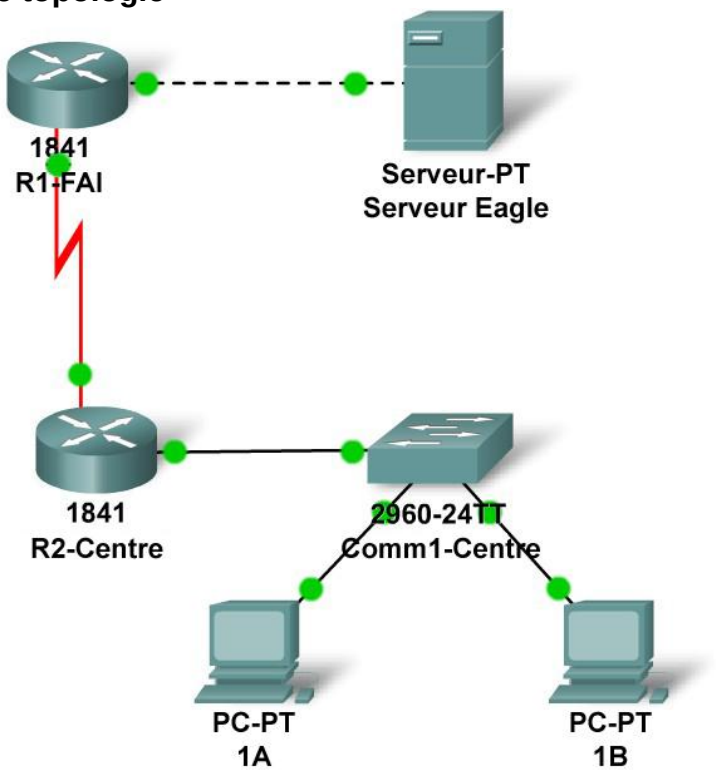


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	Fa0/0			N/A
	S0/0/0			N/A
R2-Central	Fa0/0			N/A
	S0/0/0			N/A
PC 1A	La carte réseau			
PC 1B	La carte réseau			
Serveur Eagle	La carte réseau			

Objectifs pédagogiques

- Construire, tester et configurer l'ensemble du réseau des travaux pratiques
  - Intégration des compétences acquises tout au long du cours
- Analyser les événements dans les opérations suivantes :
  - Demande de page Web (DNS, ARP, HTTP, TCP, IP, Ethernet, HDLC) ;
  - Suivi de l'acheminement vers le serveur Web (DNS, UDP, ARP, ICMP, IP, Ethernet, HDLC).

Contexte

Dans ce cours, vous avez approfondi vos compétences en matière de planification, de construction, de configuration et de test de réseau. Vous avez également assimilé des concepts liés aux protocoles réseau et aux algorithmes de périphériques. Voici le moment de tester vos connaissances : vous devez effectuer un exercice en moins de 30 minutes (près de 100 composants configurables, même si certains sont relativement simples).

Tâche 1 : planification

Utilisez la topologie de travaux pratiques de type Exploration pour planifier le modèle d'adressage IP :

- deux routeurs 1841 équipés d'une carte d'interface WIC-2T installée dans le logement de droite (l'une nommé R1-ISP, reliée à R2-Central par la connexion WAN ETCD, et l'autre reliée à S1-Central via la connexion LAN Fa0/0) ;
- un commutateur 2960TT (S1-Central) ;
- deux PC appelés 1A et 1B ;
- un serveur nommé Eagle_Server.

Notez bien que les noms complets ET les noms d'hôtes doivent être configurés exactement à l'identique pour tous les périphériques, et que les chaînes (noms, mots de passe, bannières) doivent être généralement tapées en stricte conformité avec ces instructions pour permettre une notation fiable.

On vous a attribué le bloc d'adresses IP 192.168.3.0 /24. Vous devez configurer les réseaux existants et prévoir les besoins ultérieurs.

Les attributions de sous-réseaux sont les suivantes :

- 1er sous-réseau, réseau local existant des participants, jusqu'à 28 hôtes (Fa0/0 sur R2-Central, connecté à Fa0/24 sur S1-Central) ;
- 2ème sous-réseau, futur réseau local des participants, jusqu'à 28 hôtes (pas encore mis en œuvre) ;
- 3ème sous-réseau, réseau local existant du fournisseur de services Internet (ISP), jusqu'à 14 hôtes (Fa0/0 sur R1-ISP) ;
- 4ème sous-réseau, futur réseau local du fournisseur de services (ISP), jusqu'à 7 hôtes (pas encore mis en œuvre) ;
- 5ème sous-réseau, réseau étendu (WAN) existant, liaison point à point (S0/0/0 sur R1-ISP et S0/0/0 sur R2-Central).

Les affectations d'adresses IP sont les suivantes :

- Pour le serveur, configurez la deuxième adresse IP utilisable la plus élevée sur le sous-réseau LAN du fournisseur de services Internet (ISP).
- Pour l'interface Fa0/0 du routeur R1-ISP, configurez l'adresse IP utilisable la plus élevée sur le sous-réseau LAN du fournisseur de services Internet (ISP).
- Pour l'interface S0/0/0 du routeur R1-ISP, configurez l'adresse utilisable la plus élevée sur le sous-réseau WAN existant.
- Pour l'interface S0/0/0 du routeur R2-Central, utilisez l'adresse utilisable la plus basse sur le sous-réseau WAN existant.
- Pour l'interface Fa0/0 du routeur R2-Central, utilisez l'adresse utilisable la plus élevée sur le sous-réseau LAN existant des participants et connectez-la à l'interface Fa0/24 du commutateur S1-Central.
- Pour les hôtes 1A et 1B, utilisez les deux premières adresses IP (les deux adresses utilisables les plus basses) du sous-réseau LAN existant des participants et connectez-les aux interfaces Fa0/1 et Fa0/2 du commutateur S1-Central.
- Pour l'interface de gestion du commutateur, utilisez la deuxième adresse utilisable la plus élevée sur le sous-réseau des participants.

Tâche 2 : construction et configuration du réseau

Construisez le réseau en veillant à effectuer les connexions comme indiqué. Configurez les deux routeurs, le commutateur, le serveur et les deux PC.

Configurez les routeurs par le biais de l'interface de ligne de commande (CLI) pour mettre en pratique vos compétences. La configuration des routeurs doit inclure la gestion interne (nom complet, nom d'hôte, mots de passe, bannière), les interfaces (Fast Ethernet et série) et le routage (route statique sur R1-ISP, route par défaut sur R2-Central). Les mots de passe de connexion suivants doivent tous être « cisco » (sans guillemets) : enable secret, console et Telnet. Les bannières doivent indiquer **Ceci est le routeur de travaux pratiques R1-ISP. Les bannières doivent indiquer **Ceci est le routeur de travaux pratiques R2-ISP. Accès autorisé uniquement.**

Les interfaces doivent être configurées comme indiqué dans la section d'adressage IP précédente ; utilisez une fréquence d'horloge de 64 000 sur l'interface S0/0/0 de R1-ISP. La route statique du routeur R1-ISP doit pointer vers le sous-réseau LAN existant des participants via l'adresse IP de l'interface série du routeur R2-Central ; la route statique du routeur R2-Central doit être une route statique par défaut qui pointe vers l'adresse IP de l'interface série du routeur R1-SP. Chaque fois que vous configurez un périphérique Cisco IOS, veillez à enregistrer votre configuration.

Sur le commutateur, configurez le nom complet, le nom d'hôte, la bannière (**Ceci est le commutateur de travaux pratiques S1-Central. Accès autorisé uniquement.**), les mots de passe de connexion permettant l'accès (mots de passe enable secret, console et Telnet ayant tous pour valeur « cisco »), ainsi que l'interface de gestion (int vlan1). Chaque fois que vous configurez un périphérique Cisco IOS, veillez à enregistrer votre configuration.

Pour les hôtes 1A et 1B, outre la configuration IP, configurez-les de sorte qu'ils utilisent les services DNS. Pour le serveur, activez les services DNS, utilisez le nom de domaine eagle-server.example.com, puis activez les services HTTP.

Pendant que vous travaillez, utilisez le bouton « Check Results » pour identifier les composants qu'il reste à configurer. Si vous tenez à vous exercer davantage, utilisez le bouton « Reset Activity » et reprenez la configuration à zéro en vous chronométrant.

Tâche 3 : tests et analyses

Il est recommandé de tester la connectivité par le biais des commandes ping et Telnet et d'examiner les tables de routage. Dès lors que vous êtes assuré du bon fonctionnement de votre réseau, veillez à enregistrer vos configurations sur les périphériques Cisco IOS. Ensuite, mettez hors tension puis sous tension les périphériques avant de réinitialiser le réseau. En mode simulation, demandez une page Web page en faisant en sorte que les protocoles suivants figurent dans la liste d'événements : DNS, HTTP, Telnet, TCP, UDP, ICMP, ARP. Examinez les paquets à mesure qu'ils sont traités par les périphériques pour étudier le comportement des protocoles, et plus particulièrement la façon dont IP intervient dans toutes les opérations. De même, soyez attentif aux algorithmes utilisés par les hôtes, les commutateurs et les routeurs. Expliquez l'ensemble du processus à un collègue. Débranchez et rebranchez les périphériques pour réinitialiser le réseau. En mode simulation, exécutez la commande traceroute sur l'un des PC pour interroger le serveur. Observez les réponses ICMP. Expliquez à nouveau le processus à un collègue.

remarques générales

Établissez un parallèle entre les processus observés dans la tâche 3 et le schéma de protocoles TCP/IP. Vos compétences en matière de modélisation de réseaux dans Packet Tracer vous seront très utiles dans les cours suivants.