l'Institut Sino-Européen d'Ingénierie de l'Aviation – SIAE
Réseau Informatique

Travaux Pratiques

Année 2016

Guthemberg Silvestre
guthemberg.da-silva-silvestre@enac.fr

1 Introduction

Le réseau informatique est système réparti qui permet la connectivité de ses nœuds, comme les machines clients/serveurs, les commutateurs, les routeurs, entre autres. La connectivité d'un réseau est assurée par les liens physiques et logiques entes les nœuds. Les liens physiques sont constitués principalement de câbles et/ou de signaux envoyés entre des nœuds voisins, tandis que les liens logiques sont mis en place par les protocoles utilisés par les nœuds, comme l'Ethernet pour la communication entre pairs de nœuds voisins ou bien le protocole TCP pour la communication directe entre pairs de nœuds. Ces liens, physiques et logiques, ont une caractéristique commune qui est celle de permettre l'envoi des informations entre les nœuds qu'ils connectent.

Afin d'acquérir des connaissances fondamentales sur les concepts nécessaires pour la mise en œuvre de la connectivité d'un réseau informatique, nous allons construire ensemble pendant nos séances de travaux pratiques (TPs) notre propre réseau entre la Chine et la France. À l'aide d'outil de simulation Cisco Packet Tracer [1], notre but principal est d'avoir un réseau où tous les nœuds et leurs applications (e.g., le service Web/HTTP) sont connectés.

La Figure 1 représente le réseau global que nous allons mettre en œuvre.

Figure 1: La topologie réseau que nous allons mettre en œuvre pendant les séances de TPs.

Il s'agit de deux réseaux qui sont interconnectés par Internet. Chaque réseau est constitué des réseaux d'accès et d'un cœur (détaillé à posteriori lors les TPs sur IP, Internet Protocol, en Section 4). Les élèves doivent collaborer en équipes de deux personnes où chaque collègue s'occupera d'un réseau de la Figure 1.

Nous allons suivre la liste de TPs (avec l'outil Cisco Packet Tracer) suivante :

- Introduction à l'outil Cisco Packet Tracer, les applications et la mise en place d'un réseau local fonctionnel ;

- Les protocoles de transport : le multiplexage et la fiabilité de communications bout-à-bout (TCP/UDP) ;
- L'interconnections des réseaux avec l'Internet Protocol (IP) : le routage statique et le routage dynamique ;
- La couche liaison, les réseaux virtuels locaux (VLAN) et la traduction d'adresse (NAT) ;

2 Introduction à l'outil Cisco Packet Tracer, les applications et la mise en place d'un réseau local fonctionnel

2.1 Objectifs

Dans cette première séance de TPs, nous avons les objectifs suivants :

- Introduire l'usage de Cisco Packet Tracer [1] : un outil de simulation de systèmes connectés en réseau conçu par Cisco ;
- La mise en place des applications d'un réseau fonctionnel ;

2.2 Introduction à l'outil Cisco Packet Tracer

L'interface graphique (GUI) de l'outil Cisco Packet Tracer est très intuitive. L'outil nous permet de simuler d'une façon simple des topologies réseau diverses. Il nous offre la possibilité de :

- acquérir des compétences techniques dans le déploiement et la maintenance des équipements essentiels d'un réseau opérationnel, comme des routeurs, commutateurs, et même de serveur d'applications comme http ou bien e-mail ;
- simuler, visualiser, éditer, évaluer des réseaux informatiques ;
- partager une simulations en réseau afin de collaborer avec des collègues dans une topologie commune ;
- étudier les concepts d'une topologie complexe ;
- nous préparer à une certification Cisco (*e.g.*, CCNA, le *Cisco Certified Network Associate* de Cisco [1]) .

La Figure 2 représente cette GUI lors du démarrage de l'outil.
Nous avons mis en évidence deux parties cette GUI que nous allons utiliser souvent.

1. La première partie (située en bas à gauche de la GUI) nous permet d'ajouter des équipements/nœuds et les liens physiques d'une topologie réseau. Pour cela, il suffit de les sélectionner et de les faire glisser vers le milieu de la fenêtre ;
2. Au fur et à mesure que les éléments de la topologie sont ajoutés, nous pouvons les manipuler avec les fonctionnalités disponibles sur la partie droite de la fenêtre. Ces fonctionnalités nous permettent par exemple de sectionner un élément, l'effacer, de l'inspecter, ou bien d'ajouter des informations textuelles au schéma de la topologie ;

[1] `https://en.wikipedia.org/wiki/CCNA`

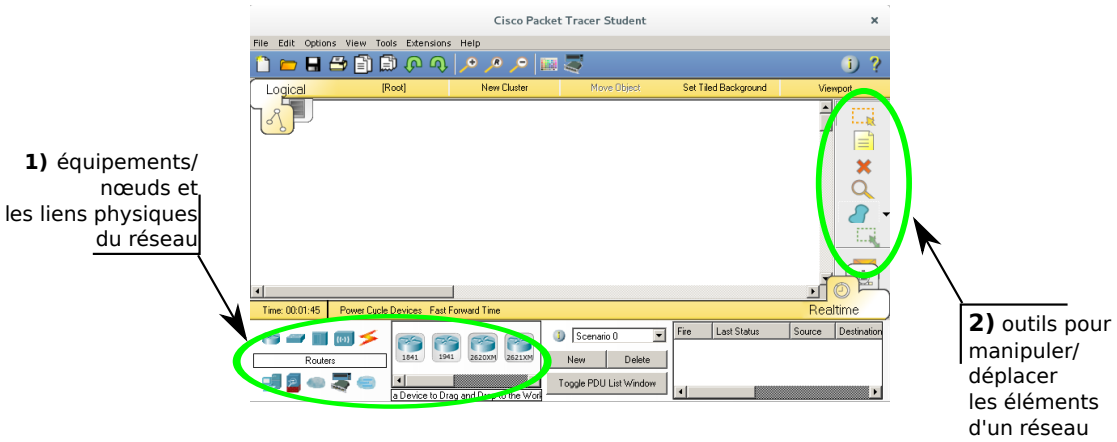


Figure 2: L'interface graphique d'outil Cisco Packet Tracer.

Afin de mieux montrer l'utilisation d'outil, nous allons décrire chaque étape de l'ajout et branchement d'un ordinateur portable au réseau local. Nous utiliserons le fichier qui est disponible sur le bureau de l'ordinateur.

1. lancez l'outil Cisco Packet Tracer, dont un raccourci se trouve sur le Bureau de votre ordinateur, puis ouvrez le fichier `siae_tp_reseau_informatique_PAYS.pkt`, où `PAYS` peut être `chine` ou `france`. Vous aurez une fenêtre similaire à celle de la Figure 3 ;

2. cliquez sur *End Devices* (dans la partie inférieur à gauche de la fenêtre, voir Figure 4) ;

3. choisissez un *Laptop-PT* en cliquant une fois sur ce type d'ordinateur de la liste d'ordinateurs disponible à droite (voir Figure 4) ;

4. faites glisser l'ordinateur choisi vers la topologie du réseau, comme il est représenté en Figure 4 ;

5. branchez le nouveau ordinateur d'usager au commutateur du réseau (dont le nom est `sw`) :

   (a) sélectionnez l'élément *Connections* (représenté en Figure 5) ;

   (b) choisissez le *Copper Straight-Through* puisque nous allons brancher un ordinateur portable à un commutateur (voir Figure 5) ;

   (c) cliquez sur le commutateur pour brancher une extrémité du câble et choisissez le port auquel le câble sera branché ;

   (d) cliquez sur l'ordinateur pour brancher l'autre extrémité du câble et choisissez le port auquel il sera branché (*e.g.*, FastEthernet0, voir Figure 5) ;

   (e) vérifiez si le câble est fonctionnel en observant si la couleur de points de deux extrémités du câble deviennent verts ;

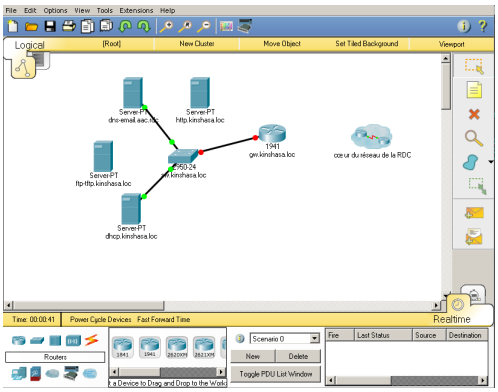


Figure 3: Notre topologie sur l'outil Cisco Packet Tracer.

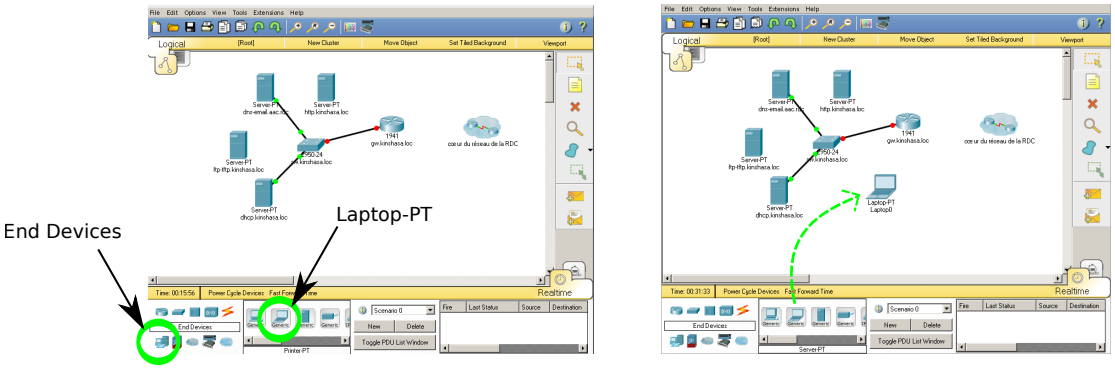


Figure 4: Ajout d'un ordinateur portable au réseau.

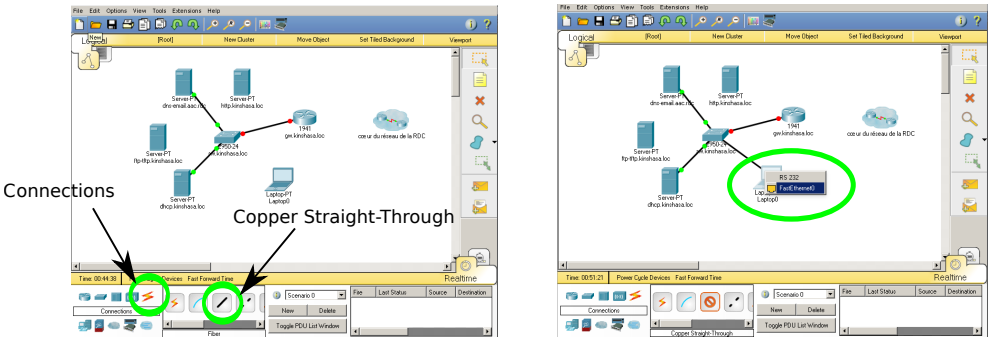


Figure 5: Branchement d'un câble entre le commutateur et l'ordinateur portable.

2.3 Les applications et la mise en œuvre d'un réseau local fonctionnel

Nous allons continuer à travailler la topologie précédente (qui est disponible sur le Bureau, *i.e.*, `siae_tp_reseau_informatique_PAYS.pkt`) afin d'installer un ensemble d'applications d'un réseau local. La Figure 6 représente le réseau local que nous souhaitons mettre en œuvre.

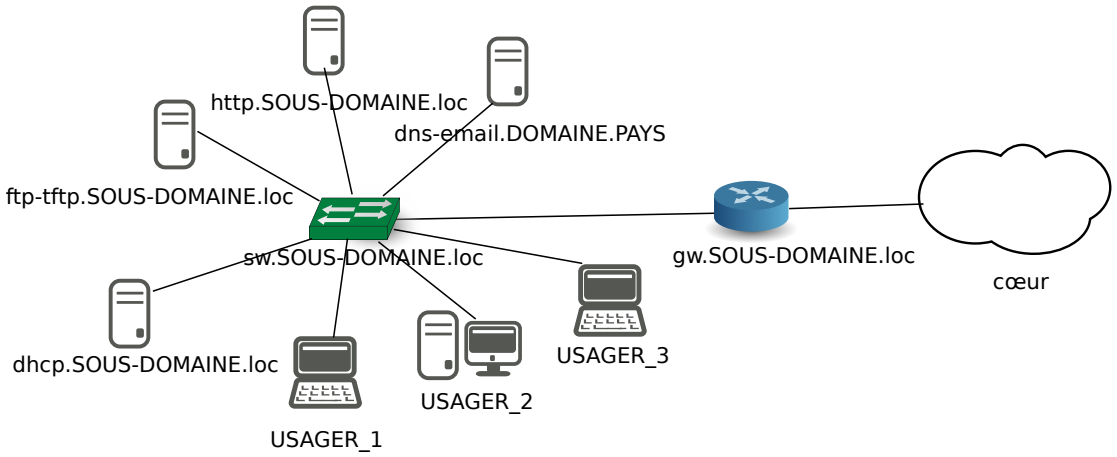


Figure 6: Réseau local à mettre en place.

Ce réseau est composé de :

- Quatre serveurs d'application : `dns-email`, `http`, `ftp-tftp`, et `dhcp`. Nous utiliserons des nœuds du type "*Server-PT*" (*Generic*), qui sont des *End Devices* de Cisco Paquet Tracer (pour plus d'informations, veuillez regarder la Figure 4 et 4) ;

- Trois ordinateurs d'usager (trois ordinateurs pour des usagers/clients est le nombre minimum), dont deux ordinateurs portables (rappelez-vous que un de ces deux portables a déjà été ajouté durant la Section 2.2) et une machine bureautique. Pour cela, nous utiliserons deux "*Laptop-PT*" et un "*PC-TP*", des *End Devices* de Cisco Paquet Tracer ;

- Un commutateur qui s'appelle `sw` (une abréviation de son mot en anglais *switch*) ;

- Un routeur ou passerelle qui s'appelle `gw` (une abréviation de son nom en anglais *gateway*) ;

Dans la prochaine section, nous allons choisir les noms, les e-mails et les mots de passes de nos trois usagers/clients. Ensuite, nous allons configurer chaque serveur puis les nœuds clients. La dernière étape du TP est de vérifier les applications à partir des usagers.

2.3.1 La création de la liste de clients de votre réseau d'accès

Veuillez remplir le Tableau 1 ci-dessous avec les informations de clients qui vont utiliser les trois ordinateurs/nœuds nous avons ajouté dans la section précédente. Vous trouverez des renseignements sur le modèle de création d'e-mail de votre réseau dans l'Appendice A.2.3 et A.2.4.

usager/log-in	**mot de passe**	**e-mail**

Table 1: Liste d'usagers du service d'e-mail de mon réseau.

Ce tableau nous sera très utile durant les TPs. Ce n'est pas nécessaire d'ajouter les nœuds de deux autres clients à ce moment des TPs. Vous pourra le faire proprement lors que vous serez dans la Section2.3.7.

2.3.2 Configuration du serveur DHCP

L'application DHCP est très utile dans un réseau local car elle permet aux nœuds des clients du réseau local d'obtenir automatiquement les informations nécessaires pour accéder aux application/services essentiels, notamment son identifiant réseau (l'adresse IP et le masque de sous-réseau), ainsi que l'identifiant réseau du serveur de noms (DNS) et de la passerelle (qui permet l'accès aux cœur du réseau et aux autres réseau externes).

Dans le fichier qui vous a été fourni (`siae_tp_reseau_informatique_PAYS.pkt`), le serveur DHCP est déjà configuré correctement et nous vous conseillons de ne pas le modifier. Afin de vérifier la configuration du serveur DHCP, veuillez cliquer sur le serveur DHCP dans le schéma du Cisco Paquet Tracer, puis choisir l'onglet "Services", et finalement cliquer sur "DHCP" sur le menu de gauche. La Figure 7 représente le contenu de la fenêtre qui s'ouvre une fois nous avons cliqué sur le serveur DHCP.

A gauche de la figure, nous avons la fenêtre de configuration du serveur. À droite, l'onglet de la même fenêtre qui nous permet de configurer les paramètres spécifiques de l'application/du service DHCP. Les principaux paramètres à vérifier sont :

- *Default Gateway* : la passerelle par défaut, il s'agit du nœud `gw`, le routeur vers le cœur du réseau ;

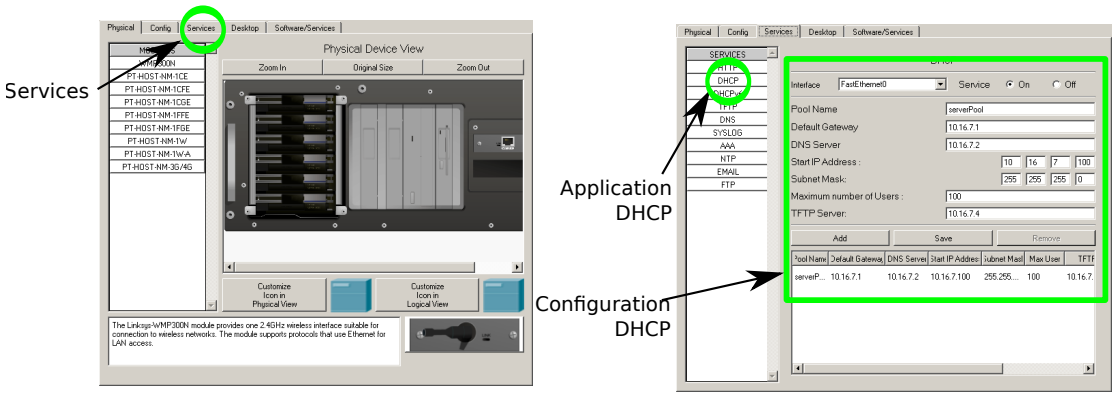


Figure 7: La vérification de la configuration de l'application DHCP. À gauche, nous avons la fenêtre de configuration du nœud, et à droite, l'onglet de la même fenêtre qui nous permet de configurer de l'application/service DHCP.

- *DNS Server* : le serveur de noms (DNS) ;
- *Start IP Address* : il s'agit du premier identifiant réseau (l'adresse IP) que le serveur attribuera aux ordinateurs des usagers du réseau local ;
- *Subnet Mask* : le masque de sous-réseau des identifiants (IP) du réseau local ;
- *Maximum number of Users* : le nombre maximum d'usagers de ce serveur DHCP ;

2.3.3 Configuration du serveur de noms, l'application DNS

Le serveur de noms, le DNS, est essentiel pour le bon fonctionnement des services d'un réseau local. Il nous permet d'acceder aux services par les noms de nœuds au lieu de ses identifiant réseau. Par exemple, si nous souhaitons accéder au serveur Web de Google par un navigateur, ce sera beaucoup plus simple de rentrer et mémoriser le nom du serveur Web, `www.google.com`, que son identifiant, une adresse IP (*e.g.*, `216.58.210.238`). En effet, le serveur de nom, qui a été fourni aux client par le service DHCP, fera la traduction de de chaque nœud nœud vers l'identifiant réseau correspondant.

Afin de configurer l'application DNS du côté du serveur sur Cisco Packet Tracer pour votre réseau :

1. cliquez sur le serveur du réseau d'accès qui s'appelle `dns-email`, puis (a) sélectionnez l'onglet Services (veuillez revoir l'image de gauche de la Figure 7), et finalement (b) sélectionnez le service DNS dans le menu à la gauche. La Figure 8 représente la fenêtre de configuration du service DNS ;
2. (c) activez le service DNS en cochant l'option *ON* en haut de la fenêtre ;
3. (d) configurez/ajoutez les paramètres de votre serveur DNS tels quels sont décrits dans l'Appendice A.2.3;

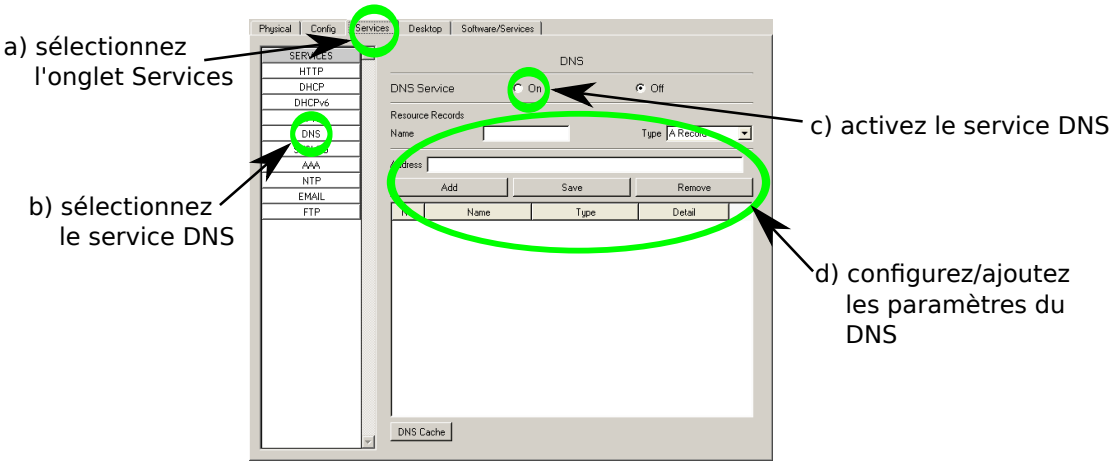


Figure 8: La fenêtre de configuration de l'application DNS sur le serveur.

2.3.4 Configuration du serveur d'email, les application SMTP et POP

L'application courrier électronique, ou simplement e-mail, est une des plus anciennes et populaires services qui fonctionne sur les réseaux informatiques. L'application e-mail offre deux services essentiels : l'envoi et la réception des messages électroniques. L'envoi de messages est assuré par un serveur *Simple Mail Transfer Protocol* (SMTP) tandis que la réception ou l'accès aux messages se fait par intermède d'un serveur de réception, dont les protocoles les plus utilisés sont le *Post Office Protocol—Version 3* (POP3), *l'Internet Mail Access Protocol* (IMAP) et *l'Hypertext Transfer Protocol* (HTTP).

Cisco Packet Tracer nous permet de configurer un serveur d'e-mail avec des implémentations simplifiés des services SMTP et POP. Afin de configurer le serveur, nous vous conseillons de suivre la liste d'étapes suivante :

1. cliquez sur le serveur du réseau d'accès qui s'appelle `dns-email`, puis (a) sélectionnez l'onglet Services, et finalement (b) sélectionnez le service EMAIL dans le menu à la gauche. La Figure 9 représente la fenêtre de configuration du serveur d'e-mail ;

2. (c) activez les services SMTP et POP du serveur d'e-mail en cochant les options *ON* en haut de la fenêtre ;

3. (d) configurez le nom de domaine et ajoutez les usagers de votre serveur d'e-mail tels quels sont décrits dans l'Appendice A.2.4 et listés par vous dans le Tableau 1;

2.3.5 Configuration du serveur web sur le réseau local (HTTP)

Le service web est le plus populaire qui existe sur Internet. Cette application utilise le protocole *Hypertext Transfer Protocol*, HTTP (ou HTTPS pour HTTP Secure). Un grand nombre de contenus sont diffusé en ligne par des serveurs web, du service de recherche de page de Google aux réseaux sociaux (Facebook, Twitter, *etc.*)

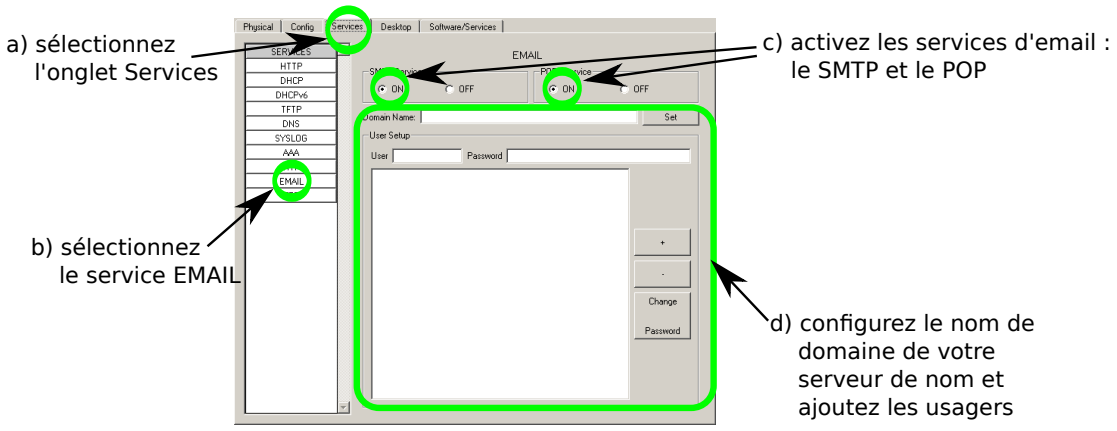


Figure 9: La fenêtre de configuration de l'application e-mail sur le serveur.

Afin de l'utiliser cette application pendant nos séances des TPs, nous allons configurer notre propre serveur sur Cisco Packet Tracer. Voici la recette à suivre :

1. branchez le serveur `http` au commutateur (qui s'appelle `sw`) du réseau local (pour vous rappelez comment brancher un câble, veuillez relire la Section 2.2) ;

2. vérifiez bien que les extrémités du câble qui lie le serveur web au commutateur sont vertes (cela veut dire qu'ils sont correctement liés au niveau logique) ;

3. cliquez sur le serveur du réseau d'accès qui s'appelle `http`, puis (a) sélectionnez l'onglet Services, et finalement (b) sélectionnez le service HTTP dans le menu à la gauche. La Figure 10 représente la fenêtre de configuration du serveur web ;

4. (c) activez les services HTTP et HTTPS du serveur web en cochant les options *ON* en haut de la fenêtre de configuration ;

5. (d) modifiez le contenu de la page principale de votre serveur web (en modifiant le fichier `index.html`). Vous pouvez ajouter un message personnalisé, par exemple, un message de bienvenue qui indique le réseau (la Chine ou la France) et votre nom. Après avoir fait les modifications sur le fichier, (e) n'oubliez pas de la sauvegarder ;

2.3.6 Configuration du serveur de fichier, les applications FTP et TFTP

Un serveur de fichiers est très important dans un réseau. Il sert à sauvegarder ou à partager des fichiers entre les clients du réseau. Afin de mettre en place un serveur de ce type sur notre réseau local/d'accès, nous allons utiliser les services FTP et TFTP du Cisco Packet Tracer. Voici la recette à suivre :

1. branchez le serveur `ftp-tftp` au commutateur (qui s'appelle `sw`) du réseau local (pour vous rappelez comment brancher un câble, relisez rapidement la Section 2.2) ;

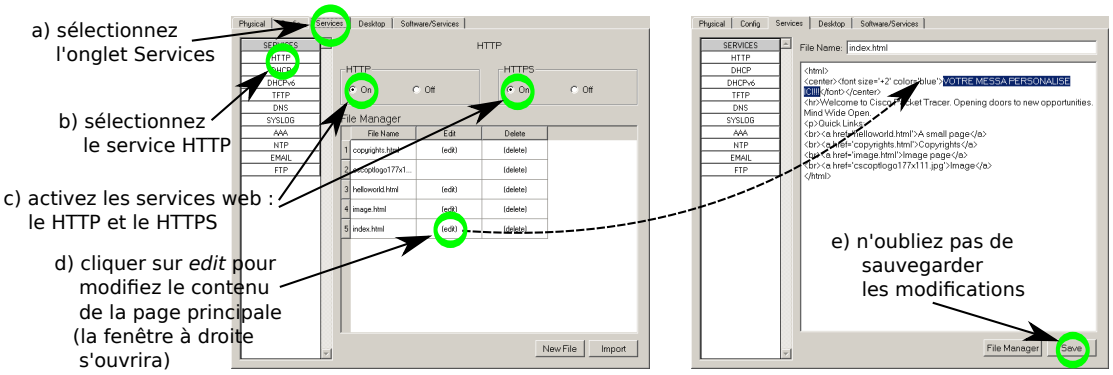


Figure 10: Les fenêtres de configuration du serveur web. A gauche, la configuration de paramètres globaux, et à droite, la modification du contenu de la page principale du serveur .

2. vérifiez bien que les extrémités du câble qui lie le serveur `ftp-tftp` au commutateur sont vertes (cela veut dire qu'ils sont correctement liés) ;

3. cliquez sur le serveur du réseau d'accès qui s'appelle `ftp-tftp`, puis sélectionnez l'onglet Services ;

4. sélectionnez le service FTP dans le menu à la gauche, et activez-le en cliquant sur l'option *ON* à droite . Notez que le service utilise un procédure d'authentification qui est déjà configurer avec un usager (`cisco`) et un mot de passe (`cisco`). Changez-les si vous le souhaitez. Tous en bas de cette fenêtre, vous avez une liste de fichiers actuellement partagés par le serveur FTP ;

5. sélectionnez le service TFTP dans le menu à la gauche, et activez-le en cliquant sur l'option *ON* à droite . Notez que ce service sera disponible sans authentification et que vous avez une liste de fichiers actuellement partagés par le serveur ;

Ce service, ainsi que les autres précédemment configurés, sera testé à partir des nœuds des clients.

2.3.7 Ajout et configuration des nœuds des clients/usagers du réseau d'accès/local

Nous avons jusqu'ici configuré l'ensemble de serveurs du notre réseau d'accès. Ces serveurs sont essentiels pour que notre réseau soit fonctionnel.

Maintenant nous allons ajouter et configurer des ordinateur pour les usagers du notre réseau d'accès. L'ajout de ces ordinateurs suivra la procédure discutée en Section 2.2. Nous vous recommandons d'ajouter un ordinateur ou poste de travail pour chaque usager qui a un compte d'e-mail sur le serveur `dns-email`. La liste d'usagers a été remplie par vous dans le Tableau 1 de la Section 2.3.4.

Pour chaque usager listé dans le Tableau 1 :

1. cliquez sur *End Devices* (dans la partie inférieur à gauche de la fenêtre) ;
2. choisissez en cliquant sur un type ordinateur disponible (par exemple, un ordinateur du type PC-PT ou bien Laptop-PT) ;
3. faites glisser vers la topologie du réseau l'ordinateur de votre choix, puis changez le nom de l'ordinateur par le nom d'usager qui l'appartient (il suffit de cliquer une fois sur le nom de l'ordinateur pour pouvoir le modifier) ;
4. branchez le nouveau ordinateur d'usager au commutateur du réseau (dont le nom est `sw`) :
   (a) sélectionnez l'élément *Connections* ;
   (b) choisissez le *Copper Straight-Through* puisque nous allons brancher un ordinateur à un commutateur ;
   (c) cliquez sur l'ordinateur pour brancher une extrémité du câble et choisissez le port auquel il sera branché (*e.g.*, FastEthernet0)
   (d) cliquez sur le commutateur pour brancher l'autre extrémité du câble et choisissez le port auquel le câble sera branché ;
   (e) vérifiez si le câble est fonctionnel en observant si les points verts de deux bouts du câble deviennent verts ;
5. configurez l'ordinateur d'usager par DCHP pour qu'il puisse accéder aux services du réseau :
   (a) cliquez sur l'image de l'ordinateur ajouté pour accéder à sa fenêtre de configuration ;
   (b) cliquez sur l'onglet *Desktop* afin d'accéder aux outils graphiques de cet ordinateur (voir Figure 11) ;
   (c) choisissez l'icône *IP Configuration* dans le *Desktop* ;
   (d) choisissez l'option *DHCP* seulement pour la partie "IP Configuration" [2] ;

2.3.8 Vérification du fonctionnement des services et des nœuds du réseau d'accès

La dernière étape de ces TPs sera la vérification de la des services du réseau d'accès. Afin de définir les nœuds de votre réseau d'accès qui feront partie de la vérification, remplissez le Tableau 2.

[2] Il s'agit de la partie de la fenêtre de configuration qui nous permet de configurer les paramètres d'IPv4 de la couche réseau, que nous allons étudier prochainement dans les cours. La deuxième partie nous permet de configurer les paramètres d'IPv6 qui ne nous intéresse pas à ce moment.

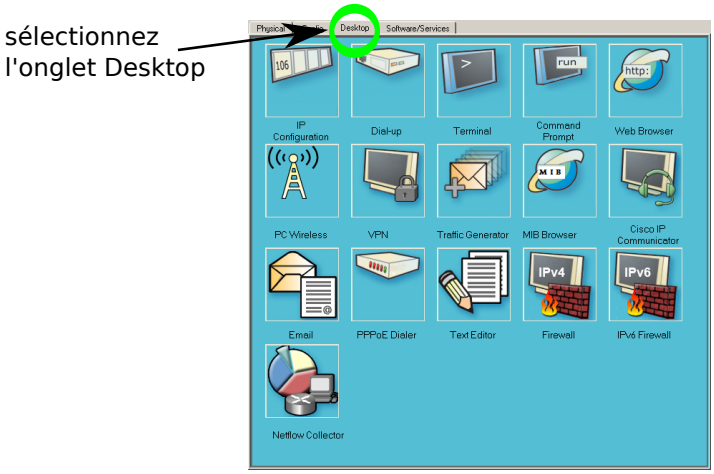


Figure 11: Le *Desktop* d'un ordinateur d'un client. Il contient des outils pour la configuration et l'accès aux applications du réseau .

Type du nœud	**Nom du nœud**
ORDINATEUR_USAGER_1	
ORDINATEUR_USAGER_2	
ORDINATEUR_USAGER_3	
SERVEUR_DE_NOMS	
SERVEUR_D_EMAIL	
SERVEUR_WEB	
SERVEUR_DE_FICHIERS (`ftp-tftp`)	

Table 2: Liste de nœuds du réseau d'accès qui feront partie de la vérification fonctionnelle.

Pour faire toutes les vérifications, nous allons utiliser les outils disponibles sur le *Desktop* d'un nœud d'un client (tous les nœuds doivent être listés dans Tableau 2). Afin d'accéder au *Desktop*, vous devez cliquer sur l'image d'un nœud d'un client, puis choisir l'onglet *Desktop*. Vous devez alors avoir la fenêtre représenté précédemment dans la Figure 11.

Vérification des configurations de l'ordinateur d'un usager

Cette vérification doit être faite pour chaque nœud client listé dans le Tableau 2.

La vérification de la configuration de l'ordinateur du usager consiste à :

1. cliquez sur l'image de l'ordinateur d'usager pour accéder à sa fenêtre de configuration ;
2. cliquez sur l'onglet *Desktop* afin d'accéder aux outils graphiques de cet ordinateur (voir Figure 11) ;
3. choisissez l'icône *IP Configuration* dans le *Desktop* ;
4. vérifiez si les quatre champs de la partie "IP Configuration" sont dûment remplis (il s'agit des champs : *IP Addess, Subnet Mask, Defaukt Gateway,* et *DNS Server*) ;

Si tous les champs sont remplis, cela veut dire que l'ordinateur a été correctement configuré par le serveur DHPC et qu'il pourra se communiquer avec tous les nœuds du réseau local. Donc, vous pouvez tester le fonctionnement du serveur de noms (la prochaine étape de la procédure de vérification). Mais si un nœud n'a pas les quatre configuration ci-dessus dûment remplies n'est pas le cas de votre ordinateur d'un usager, veuillez vérifier si :

- le câble entre l'ordinateur et le commutateur est bien branché (des petits indicateurs ronds des extrémités du câble doivent être vertes) ;
- l'ordinateur utilise le DHCP pour accéder aux configuration IP automatiquement (la case DHCP doit être marquée dans la partie *IP Configuration* du *Desktop*) ;

Vérification du fonctionnement du serveur de noms, le DNS

Nous allons vérifier le fonctionnement du serveur de noms à partir d'un des nœuds client. pour vérifier chaque nom et alias des serveurs du Tableau 2, vous devez suivre les étapes de la recette suivante :

1. cliquez sur l'image de un des nœuds client pour accéder à sa fenêtre de configuration ;
2. cliquez sur l'onglet *Desktop* afin d'accéder aux outils graphiques de ce nœud (voir Figure 11) ;
3. choisissez l'icône *Command Prompt* dans le *Desktop*. Cela vous ouvrira une petite fenêtre noir dont le contenu est similaire à ceci :

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

Nous allons rentrer des commandes dans cette fenêtre *Command Prompt* (la fenêtre noir) pour tester le serveur DNS. Nous utiliserons l'outil `nslookup`, qu'il s'agit d'un client de l'application DNS qui nous permet d'envoyer des requêtes de résolution de noms ;

4. rentrez la commande `nslookup` dans la petite fenêtre :

```
Packet Tracer PC Command Line 1.0
PC>nslookup

Server:  [IP_DU_SERVEUR_DE_NOMS]
Address:  IP_DU_SERVEUR_DE_NOMS

>
```

si votre nœud est correctement configuré, nous voyons comme sortie de la commande l'identifiant du serveur DNS (IP_DU_SERVEUR_DE_NOMS). Dorénavant, nous sommes en mode interactif de la commande `nslookup` ;

5. rentrez "?" pour connaître les commandes disponibles d'outil `nslookup` :

```
>?
Commands:       identifiers are shown in uppercase,
                [] means optional)
NAME                    - print info about the host/domain NAME
                          using default server
NAME1 a.b.c.d           - as above, but use  server ip address
                          a.b.c.d
help or ?               - print info on common commands
set OPTION              - set an option
    set [no] recurse    - ask for recursive answer to query
    set [no] debug      - print debugging information
    timeout=X           - set initial time-out interval to X
                          milliseconds

>
```

il y a toute une liste d'options. Nous allons faire des requêtes de nom de serveurs (voir Tableau 2) ;

6. tapez le nom du serveur que vous souhaitez vérifier, par exemple, celui que correspond au SERVEUR_WEB dans le Tableau 2 :

```
>SERVEUR_WEB
Server:  [IP_DU_SERVEUR_DE_NOMS]
Address:  IP_DU_SERVEUR_DE_NOMS

Non-authoritative answer:
Name:    SERVEUR_WEB
Address:    IP_DU_SERVEUR_WEB


>
```

si la requête est réussie, nous avons l'identifiant (IP) du serveur comme sortie ;

7. le cas échéant, vérifiez aussi l'alias du serveur. Pour le SERVEUR_WEB, il s'agit de l'alias `www` :

```
>www
Server:  [IP_DU_SERVEUR_DE_NOMS]
Address:  IP_DU_SERVEUR_DE_NOMS

Non-authoritative answer:
Name:    SERVEUR_WEB
Address:    IP_DU_SERVEUR_WEB

Aliases:    SERVEUR_WEB


>
```

si la requête est réussie, nous avons l'identifiant (IP) de l'alias du serveur comme sortie ;

8. sortez de l'outil `nslookup` :

```
>exit
PC>
```

Si vous avez eu des erreurs pendant la vérification du serveur de noms, veuillez vérifier si :

- les câbles de l'ordinateur et du serveur sont bien branchés (en observant les extrémités des câbles qui doivent être vertes) ;
- l'ordinateur de l'usager est configuré avec le serveur de noms correct ;

- le service DNS est dûment configuré et actif (revoir la configuration du DNS en Section 2.3.3) ;

Vérification de l'envoie et de la réception d'e-mails

Une fois que nous avons constaté que le service de noms fonctionne normalement, nous pouvons vérifier le service d'e-mail. Nous allons utiliser les trois nœuds clients listés dans le Tableau 2 pour faire le teste.

Pour chaque pair de clients, veuillez suivre la procédure suivante :

1. cliquez sur l'image de l'ordinateur d'un usager pour accéder à sa fenêtre de configuration (voir Tableau 2 pour la liste de nœuds client disponibles) ;

2. cliquez sur l'onglet *Desktop* afin d'accéder aux outils graphiques de cet ordinateur (voir Figure 11) ;

3. choisissez l'icône *Email* dans le *Desktop*. Cela vous ouvrira une fenêtre dont le titre est *Configure Mail*, similaire à celle représentée par la Figure 12 ;

4. configurez la liste de paramètres demandés :

   (a) *Your Name* et *Email Address* : vous avez rempli ces informations dans le Tableau 1 ;

   (b) *Incoming Mail Server* et *Outgoing Mail Server* : il s'agit des serveurs SMTP et POP, dans notre cas, les deux tournent sur le même serveur, c'est-à-dire le SERVEUR_D_EMAIL du Tableau 2 ;

   (c) *User Name* et *Password* : ces deux champs correspondent au log-in et au mot de passe du Tableau 1 ;

5. sauvegardez la configurations en appuyant sur le bouton *Save*. En suite, vous verrez l'interface graphique intuitive (qui s'appelle *Mail Browser*) par laquelle vous pouvez envoyer et recevoir des e-mails ;

6. cliquez sur le bouton *Receive* pour recevoir les derniers messages (lors d'un clique de bouton, vous avez l'état des actions demandées dans une barre en bas de la fenêtre) ;

7. cliquez sur le bouton *Compose* (ou bien *Reply*) pour rédiger et envoyer un message à un autre client du Tableau 2 ;

En cas de problème, vous devez vérifier si :

- les câbles de nœuds client et du serveur d'e-mail sont bien branchés (en observant les extrémités des câbles qui doivent être vertes) ;

- le nœud du client est configuré avec les serveurs SMTP/POP (*Incoming Mail Server* et *Outgoing Mail Server*) ;

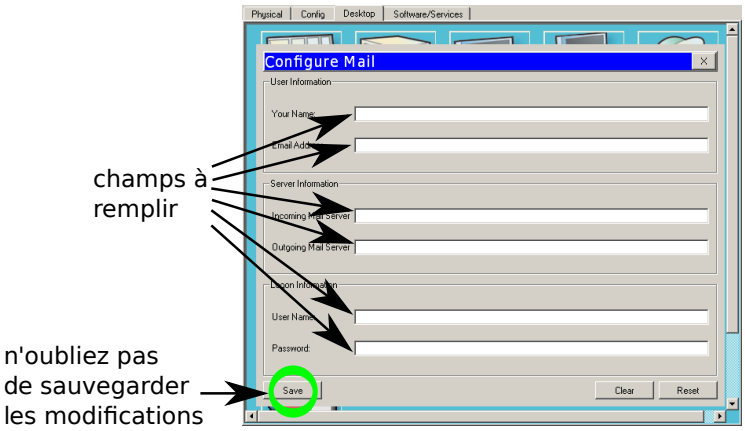


Figure 12: La fenêtre de configuration du client d'e-mail d'nu nœud client.

- les services SMTP et POP sont dûment configurés et actifs (revoir la configuration du serveur d'e-mails en Section 2.3.4), ainsi que le log-in et le mot de passe de celui qui souhaite envoyer/recevoir des messages ;

Teste d'accès au serveur Web

Cette vérification peut être faite à partir d'un nœud client du Tableau 2 à choisir. Voici la recette de vérification à suivre.

1. cliquez sur l'image du nœud client pour accéder à sa fenêtre de configuration ;
2. cliquez sur l'onglet *Desktop* afin d'accéder aux outils graphiques de ce nœud (voir Figure 11) ;
3. choisissez l'icône *Web Browser* dans le *Desktop*. Cela vous ouvrira une fenêtre du navigateur web de l'ordinateur ;
4. faites rentrez le nom du serveur web (celui que vous avez marqué comme SERVEUR_WEB dans le Tableau 2) ;
5. vérifiez si le contenu de la page correspond bien à celui que vous attendiez (rappel, vous l'avez probablement modifié durant les étapes de la Section 2.3.5) ;
6. vérifiez si le `HTTP Secure` est actif en essayant d'accéder l'URL `httpS://SERVEUR_WEB` au lieu de `http://SERVEUR_WEB` ;

Quelques pistes pour la corrections d'éventuels problèmes :

- vérifiez les états des câbles du nœud client et serveur;
- faites une vérification de la configuration du serveur (selon la Section 2.3.5) : est-ce que les services HTTP et HTTPS sont actifs ? Avez-vous modifié le contenu de la page principale (en modifiant le fichier `index.html`).

Vérification du serveur de fichiers

Cette vérification peut être faite à partir d'un nœud client du Tableau 2 à choisir.

Afin de vérifier le serveur de fichiers, nous allons tout d'abord créer un fichier qui s'appellera `fichier.txt`. Voici la recette pour créer ce fichier :

1. cliquez sur l'image du nœud client pour accéder à sa fenêtre de configuration ;
2. cliquez sur l'onglet *Desktop* afin d'accéder aux outils graphiques de cet ordinateur (voir Figure 11) ;
3. choisissez l'icône *Text Editor* dans le *Desktop*. Cela vous ouvrira une fenêtre avec un espace en blanc où vous devez écrire un message personnalisé ;
4. essayez de fermer le *Text Editor*;
5. si vous aviez écrit un message, vous aurez une fenêtre de dialogue que vous demandera si vous souhaitez sauvegardez vos modifications, choisissez "Save" ;
6. rentrez le `fichier.txt` comme nom du fichier à être sauvegardé ;

Maintenant que nous avons le fichier `fichier.txt` sur le nœud, veuillez suivre la liste étapes suivante afin de le télécharger sur le serveur de fichiers.

1. cliquez sur l'image de l'ordinateur de l'usager pour accéder à sa fenêtre de configuration ;
2. cliquez sur l'onglet *Desktop* afin d'accéder aux outils graphiques de ce nœud (voir Figure 11) ;
3. choisissez l'icône *Command Prompt* dans le *Desktop*. Cela vous ouvrira une petite fenêtre noir dont le contenu est similaire à ceci :

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

   Nous allons rentrer des commandes dans cette fenêtre *Command Prompt* (de couleur noire) pour vérifier le serveur de fichiers. Nous utiliserons l'outil `ftp`. Il s'agit d'un outil client pour l'application FTP ;

4. rentrez "`ftp SERVEUR_DE_FICHIERS`" dans le prompte, SERVEUR_DE_FICHIERS doit être remplacer par le nom du serveur de fichiers spécifié dans le Tableau 2 :

```
PC>ftp SERVEUR_DE_FICHIERS
Trying to connect...SERVEUR_DE_FICHIERS
Connected to SERVEUR_DE_FICHIERS
220- Welcome to PT Ftp server
Username:
```

si votre nœud est correctement configuré, nous voyons comme sortie un message de bienvenue du serveur de fichiers ;

5. faites rentrer le nom d'usager et mot de passe valide du service ftp. Par défaut, c'est `cisco` comme nom, et `cisco` comme mot de passe.

```
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

une fois que vous ayez fini l'authentification, vous rentrez en mode interactif de la commande `ftp` ;

6. rentrez "?" pour connaître les commandes disponibles par outil `ftp` :

```
ftp>?
          ?
          cd
          delete
          dir
          get
          help
          passive
          put
          pwd
          quit
          rename
ftp>
```

les options nous permettent de manipuler les fichiers sur le serveur, comme supprimer un fichier avec `delete` ou bien de récupérer un ficher avec l'option `get`;

7. tapez la commande `dir` pour avoir la liste de fichiers actuellement disponible sur le serveur ;

```
ftp>dir

Listing /ftp directory from SERVEUR_DE_FICHIERS
0    : asa842-k8.bin                                5571584
1    : c1841-advipservicesk9-mz.124-15.T1.bin       33591768
2    : c1841-ipbase-mz.123-14.T7.bin                13832032
3    : c1841-ipbasek9-mz.124-12.bin                 16599160
```

```
4    : c2600-advipservicesk9-mz.124-15.T1.bin          33591768
5    : c2600-i-mz.122-28.bin                           5571584
6    : c2600-ipbasek9-mz.124-8.bin                     13169700
7    : c2800nm-advipservicesk9-mz.124-15.T1.bi         50938004
8    : c2800nm-advipservicesk9-mz.151-4.M4.bin         33591768
9    : c2800nm-ipbase-mz.123-14.T7.bin                 5571584
10   : c2800nm-ipbasek9-mz.124-8.bin                   15522644
11   : c2950-i6q4l2-mz.121-22.EA4.bin                  3058048
12   : c2950-i6q4l2-mz.121-22.EA8.bin                  3117390
13   : c2960-lanbase-mz.122-25.FX.bin                  4414921
14   : c2960-lanbase-mz.122-25.SEE1.bin                4670455
15   : c2960-lanbasek9-mz.150-2.SE4.bin                4670455
16   : c3560-advipservicesk9-mz.122-37.SE1.bin         8662192
17   : pt1000-i-mz.122-28.bin                          5571584
18   : pt3000-i6q4l2-mz.121-22.EA4.bin                 3117390
ftp>
```

nous observons que le serveur contient déjà un ensemble de fichiers binaires (dont l'extension est `.bin`) ;

8. téléchargez le fichier (`fichier.txt`) vers le serveur de fichiers :

```
ftp>put fichier.txt

Writing file fichier.txt to SERVEUR_DE_FICHIERS:
File transfer in progress...

[Transfer complete - 18 bytes]

18 bytes copied in 0.015 secs (1200 bytes/sec)
ftp>
```

la sortie de la commande montre que un fichier vient d'être téléchargé sur le serveur avec succès. Nous avons aussi des informations sur sa taille (en octets) et du temps de téléchargement;

9. listez a nouveau le contenu du serveur de fichier :

```
ftp>dir

Listing /ftp directory from SERVEUR_DE_FICHIERS:
0    : asa842-k8.bin                                   5571584
1    : c1841-advipservicesk9-mz.124-15.T1.bin          33591768
2    : c1841-ipbase-mz.123-14.T7.bin                   13832032
3    : c1841-ipbasek9-mz.124-12.bin                    16599160
```

```
4    : c2600-advipservicesk9-mz.124-15.T1.bin          33591768
5    : c2600-i-mz.122-28.bin                           5571584
6    : c2600-ipbasek9-mz.124-8.bin                     13169700
7    : c2800nm-advipservicesk9-mz.124-15.T1.bin        50938004
8    : c2800nm-advipservicesk9-mz.151-4.M4.bin         33591768
9    : c2800nm-ipbase-mz.123-14.T7.bin                 5571584
10   : c2800nm-ipbasek9-mz.124-8.bin                   15522644
11   : c2950-i6q4l2-mz.121-22.EA4.bin                  3058048
12   : c2950-i6q4l2-mz.121-22.EA8.bin                  3117390
13   : c2960-lanbase-mz.122-25.FX.bin                  4414921
14   : c2960-lanbase-mz.122-25.SEE1.bin                4670455
15   : c2960-lanbasek9-mz.150-2.SE4.bin                4670455
16   : c3560-advipservicesk9-mz.122-37.SE1.bin         8662192
17   : fichier.txt                                     18
18   : pt1000-i-mz.122-28.bin                          5571584
19   : pt3000-i6q4l2-mz.121-22.EA4.bin                 3117390
ftp>
```

notez que le fichier (`fichier.txt`) maintenant fait partie de la liste de fichiers disponibles sur le serveur ;

10. sortez de l'outil `ftp` :

```
ftp>quit

Packet Tracer PC Command Line 1.0
PC>221- Service closing control connection.
PC>
```

Voici quelques consignes que peuvent vous aider a corriger des éventuels problèmes pendant la vérification du serveur de fichier.

- vérifiez si les câbles des nœuds sont bien branchés (en observant les extrémités des câbles qui doivent être vertes) ;
- assurez-vous que le service FTP sur le serveur est dûment configuré et actif (revoir la configuration du FTP en Section 2.3.6) ;
- en cas de problème d'authentification, vérifiez si l'usager et le mot de passe du côté du serveur sont ceux que vous avez tapez (par défaut, utilisez `cisco` comme client, et aussi `cisco` pour le mot de passe) ;

3 La couche transport et l'analyse de trafic

3.1 Objectifs

Un protocole réseau définit les règles de communication entre les nœuds, les processus ou les couches qui souhaitent échanger de données. Pour mieux comprendre le comportement/fonctionnement des protocoles réseaux, nous pouvons recourir à **la capture passive** de données échangées par ces protocoles. La capture passive de données est faite à l'aide d'outils ou d'équipements qui peuvent récupérer des paquets (ou bien, le terme générique PUDs *Protocol Data Unit*) sans interférer dans le comportement du protocole.

Dans ces TPs, nous allons utiliser Cisco Packet Tracer pour capturer les paquets des communications de notre réseau local/d'accès. A partie des paquets capturés, nous allons faire une analyse du trafic en fonctions des informations de chaque paquet, ainsi que des flux de données échangées.

Les objectifs du TP sont :

- apprendre comment nous pouvons capturer des paquets en Cisco Packet Tracer;
- analyser le trafic capturé sur un réseau ;
- étudier le fonctionnement des protocoles réseaux, et en particulier les services offert par la couche transport aux applications ;
- identifier les différences entre les deux principaux protocoles de transport utilisés sur Internet, UDP et TCP ;

3.2 La capture de trafic avec un *Sniffer*

Depuis la version de Cisco Packet Tracer (6.2), lancée en 2015, nous pouvons utiliser un équipement qui capture de données des communications échangées sur les réseaux informatiques. Cet outil s'appelle *Sniffer* et il fait partie des *End Devices* de Cisco Packet Tracer. *Sniffer* nous permet de :

- capturer les données binaires d'un lien physique ;
- désencapsuler et interpréter les données capturées selon leurs en-têtes et les couches réseaux correspondantes ;
- afficher les détails des paquets (ou bien, *Protocol Data Units*, PDUs, le terme générique) qu'il a été capable d'interpréter ;

Le *Sniffer* disponible sur Cisco Packet Tracer a deux ports. Néanmoins il est important de remarquer qu'*il n'est capable de capturer que les données d'entrées d'un seul port à la fois.*

Pour ajouter un *Sniffer* :

1. cliquez sur *End Devices* (dans la partie inférieur à gauche de la fenêtre) ;
2. choisissez l'équipement *Sniffer* dans la liste à droite et faites-le glisser vers la topologie du réseau l'ordinateur de votre choix, puis donnez-le un nom qui représente la trafic ou le lien que vous aller capturer ;
3. branchez le nouveau *Sniffer* au milieu de deux nœuds dont le trafic nous intéresse et vérifiez bien que le lien est actif (faites attention aux câbles, du type droit, *straight* en anglais, ou croisé, *crossover*) ;

Figure 13 représente un *Sniffer* (appelé `mon_trafic`) qui a été branché entre un serveur (`mon serveur`) et un commutateur.

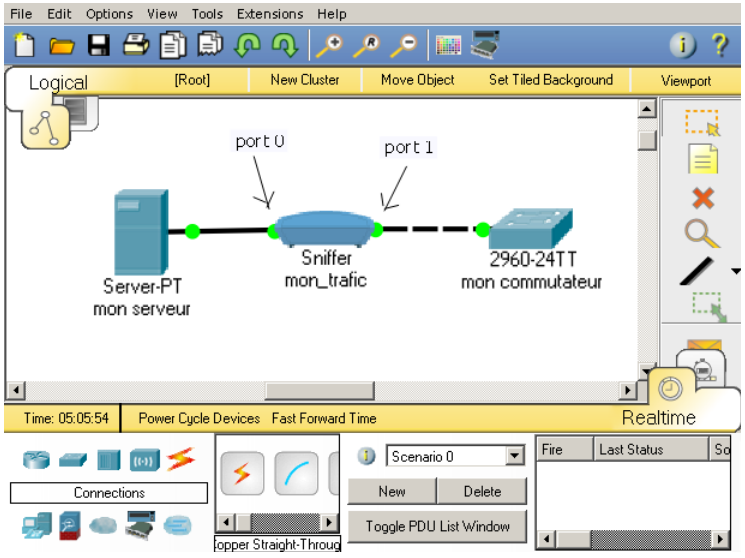


Figure 13: Le *Sniffer* capture le trafic d'entrée sur seulement un de ses deux ports (au choix).

Nous devons cliquer sur le *Sniffer* afin de le configurer. La configuration du *Sniffer* peut être faite de la façon décrite dans la Figure 14.

Par exemple, si nous souhaitons capturer le trafic qui sort du serveur vers le commutateur, nous devons activer la capture sur le "port 0". Afin de capturer seulement le trafic des certains services réseau, nous devons filtrer les données capturées selon les protocoles que nous intéressent. Dans ces TPs, nous allons nous intéresser au trafic des protocoles que nous avons étudié, notamment les protocoles de la couche application et de la couche transport. Pour rendre notre analyse plus intéressante, nous allons aussi observer l'identifiant réseau de la couche réseau des paquets capturés, c'est-à-dire, son adresse IP.

3.2.1 Une méthodes d'analyse de trafic

Nous allons analyser le trafic en utilisant deux méthodes complémentaires : l'analyse de paquets et l'analyse de flux.

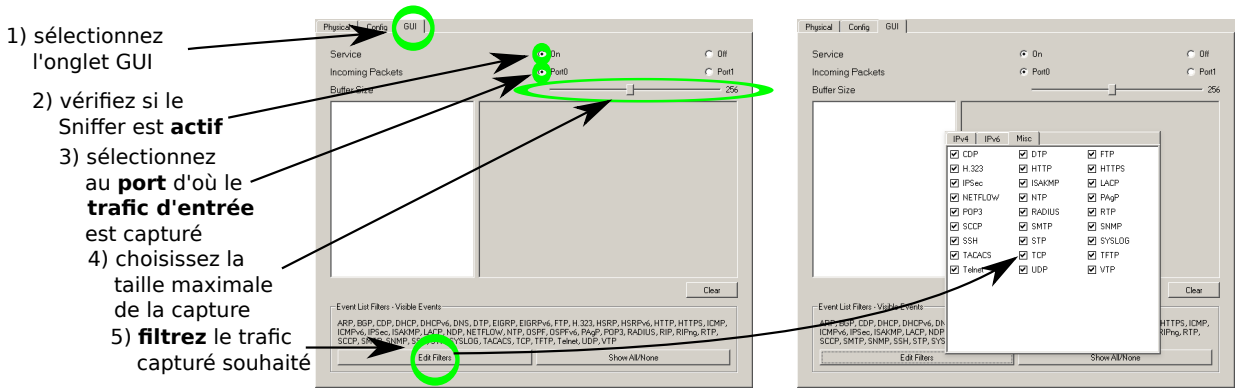


Figure 14: L'interface de configuration du *Sniffer*. A gauche, nous avons la configuration générale, et à droite, la configuration des filtres de la capture.

L'analyse de paquets consiste à analyser les données de chaque paquet capturé. Alors pour chaque paquet, nous allons observer un ensemble d'informations afin de mieux comprendre le fonctionnement des protocoles, notamment ceux des couches application, transport et réseau. Les informations qui vont particulièrement nous intéresser sont : l'IP (identifiant réseau) de la source (ou émetteur), le port de la source, l'IP de la destination (ou destinataire), le port de la destination, le protocole de transport, les indicateurs de la couche transport (le cas échéant), et l'application (le cas échéant). Veuillez noter que nous allons nous intéresser **exclusivement** au trafic qui contient des informations de la couche transport (*i.e.*, UDP et TCP).

Pour analyser le trafic en forme de flux, nous allons agréger les informations des paquets capturés. Cette agrégation d'informations se fera en fonction de cinq informations clés des paquets : l'IP de la source, le port de la source, l'IP de la destination, le port de la destination, et le protocole de transport. Cela veut dire qu'**un flux est l'agrégation des paquets capturés qui ont en commun ces cinq informations**. Par exemple, si nous avons capturé trois paquets qui ont en commun ces informations, ils forment un seul flux, et donc au moment de l'analyse, ils seront représentés par une seul ligne au lieu de trois (une par paquet).

3.2.2 L'analyse de trafic réseau et étude des protocoles

Nous allons capturer et analyser du trafic réseau afin de mieux comprendre le fonctionnement des protocoles réseaux, notamment les protocoles des couches application et transport.

La capture sera faite en utilisant de *Sniffers* qui seront branchés entre les nœuds dont le trafic nous intéresse. Nous vous conseillons de nommer les *Sniffers* selon les nœuds auxquels ils sont branchés et le sens du trafic capturé. Par exemple, si vous avez un *Sniffer* branché entre le serveur `http` et le commutateur `sw` et vous souhaitez observer le trafic qui vient du serveur vers le commutateur, alors nous vous recommandons d'appeler ce *Sniffer* de `http-sw`.

Pour l'analyse de paquets capturés, vous devez utiliser le Tableau 3 et le Tableau 4. Le Tableau 3 sert à analyser chaque paquet du trafic capturé. Vous allez remplir les lignes de ce tableau à partir des informations des *Sniffers* déployés. Le deuxième tableau, Tableau 4, sera utilisé pour l'analyse des flux de paquets. Chaque ligne de ce tableau sera écrite à partir de l'agrégation des informations notées dans le Tableau 3.

Nous vous recommandons d'analyser le trafic des événements suivants :

1. L'envoie d'une requête de configurations d'un nœud client au serveur DHCP ;
2. L'envoie d'une requête de résolution de nom vers le serveur DNS en utilisant l'outil `nslookup` ;
3. L'envoie d'un e-mail ;
4. La réception d'un e-mail ;
5. L'accès à une page web ;
6. Le téléchargement d'un fichier du serveur *ftp* ;

Pour chaque événement, veuillez remplir les tableaux (Tableau 3 et Tableau 4) en précisant l'événement et les déploiements des *Sniffers*.

Événement : _____

Liste de noms de *Sniffers* : _____

# Paquet	**Source**		**Destination**		**Protocole de transport**	**Indicateurs (*flags*)**	**Application**
	IP	port	IP	port			

Table 3: Tableau d'analyse de paquets du trafic capturé.

Événement : _____

Liste de noms de *Sniffers* : _____

# Flux	**Identifiant du flux**					**Quantité de Paquets**
	Source IP	Src port	Destination IP	Dst port	Transport	

Table 4: Tableau d'analyse de flux du trafic capturé.

3.3 La capture de trafic réseau en mode simulation

Cisco Packet Tracer offre une autre fonctionnalité de capture de paquets qui s'appelle *Simulation Mode*. Le mode simulation nous permet de capturer et visualiser au fur et à mesure paquets des communications en cours. Ainsi comme le *Sniffer*, nous pouvons filtrer le trafic afin de capturer et analyser un sous-ensemble de paquets qui nous intéresse. Une différence importante en relation *Sniffer*, c'est que en mode simulation nous observons l'ensemble des échanges du réseau simulé. Cela veut dire que selon la quantité de nœuds de la topologie, une capture peut être ralentie à cause d'une consommation importante de ressources par le simulateur Cisco Packet Tracer.

La Figure 15 représente l'interface de Cisco Packet Tracer en mode simulation et la Figure 16 la même interface "en action".

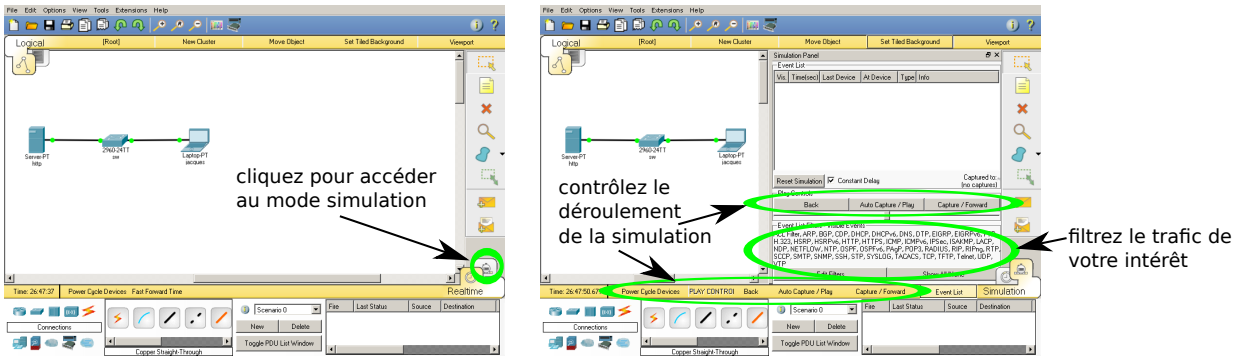


Figure 15: Cisco Packet Tracer en mode simulation. A gauche, le bouton qui nous permet de changer de mode, et à droite les paramètres de contrôle et filtrage de trafic d'une simulation.

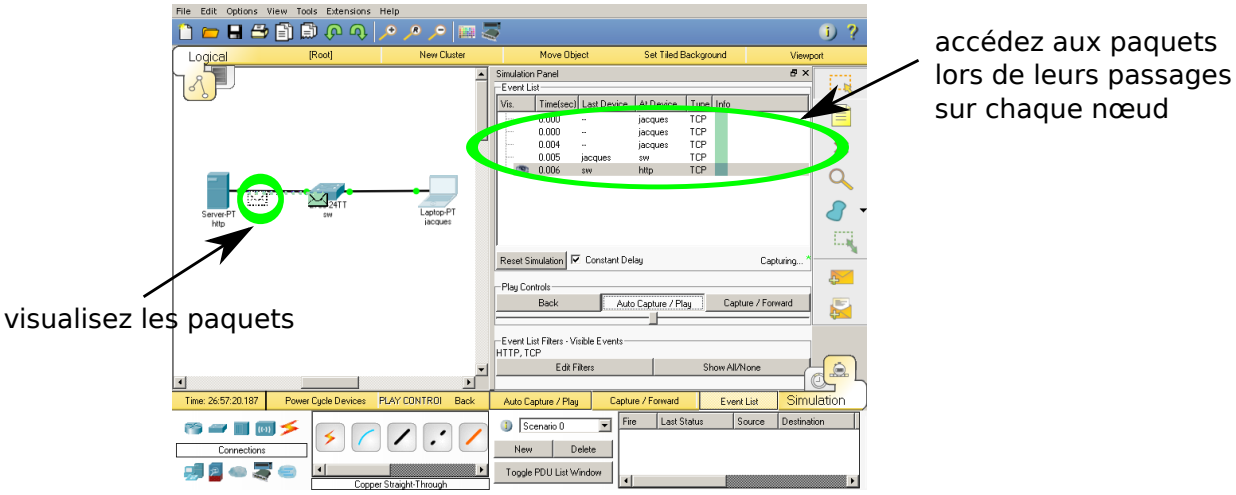


Figure 16: L'usage de Cisco Packet Tracer en mode simulation.

Pour cette partie des TPs, nous vous demandons de réaliser deux tâches à l'aide du mode simulation de Cisco Packet Tracer :

1. faites tourner (au moins) deux simulations, une d'un trafic UDP et autre du trafic TCP de votre choix (à partir de la liste d'événements proposé dans la Section 3.2.2) et remplissez les tableaux (Tableau 3 et Tableau 4) en fonction du trafic capturé en mode simulation ;

2. pour chaque trafic de paquets analysé, dessinez un diagramme similaire à celui de la Figure 17 en précisant le temps de *round to trip* (RTT) ;

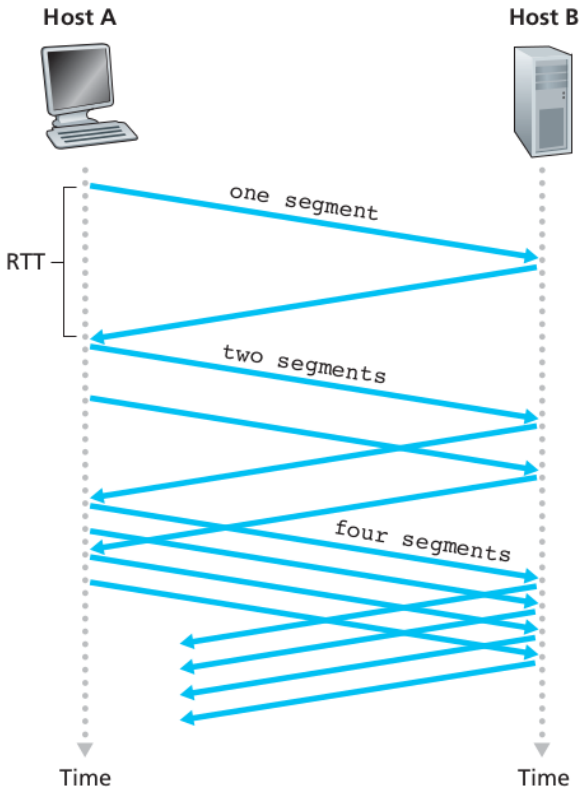


Figure 17: Diagramme d'échange de paquets en ordre chronologique et le temps de RTT.

4 La couche réseau et l'interconnexion des réseaux de la Chine

4.1 Objectifs

Ce TP nous permettra de mettre en pratique nos connaissances du protocole IP sur Cisco Packet Tracer. Les objectifs des TPs sont :

- comprendre l'interconnexion de réseaux avec le protocole IP ;
- mettre en place un plan d'adressage ;
- configurer un routeur Cisco en utilisant le terminal ;
- apprendre le routage par l'ajout de routes statiques ;
- vérification de l'interconnexion du réseau avec les commandes `ping` et `traceroute` ;

4.2 Les réseaux à interconnecter

Nous allons interconnecter deux réseau d'accès par le cœur de notre réseau en utilisant quatre routeur. La Figure 18 représente le réseau à mettre en place. Le plan d'adressage du réseau est détaillé dans l'Appendice A.

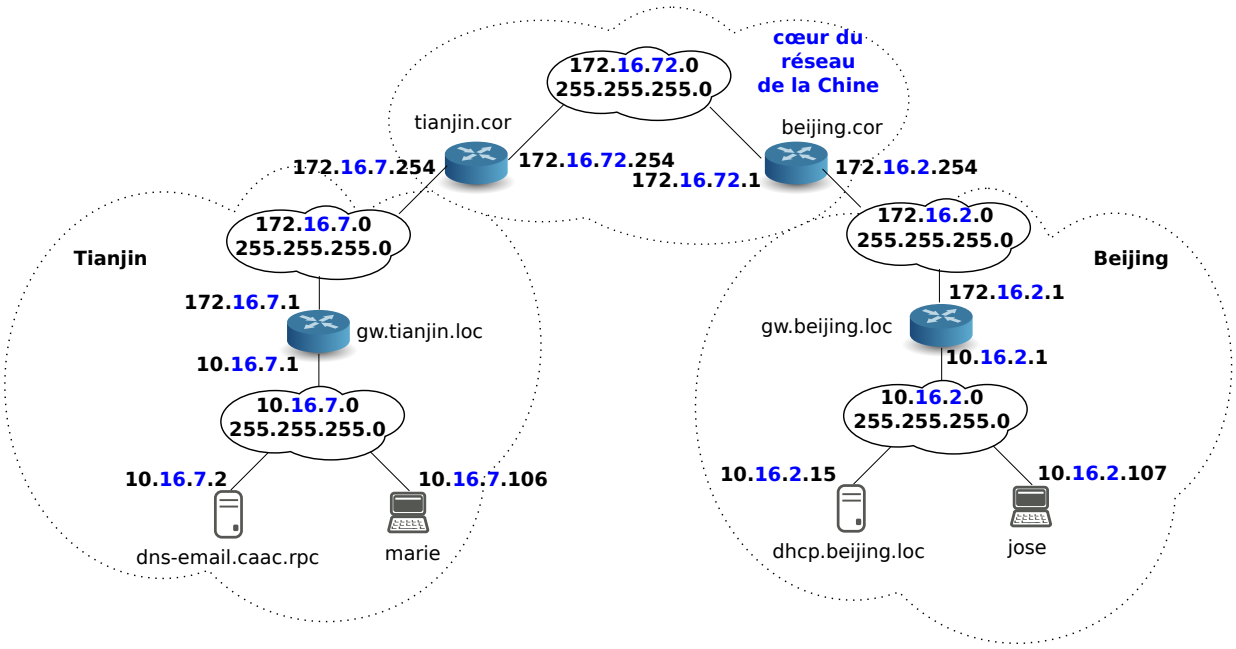


Figure 18: Réseau à mettre en place.

Chaque routeur du réseau à mettre en place doit avoir au moins quatre interfaces, deux interfaces du type *Gigabit Ethernet* et deux autres du type *Fast Ethernet*.

4.3 L'accès à la console de configuration du routeur

Veuillez suivre la procédure suivante pour accéder à la console du routeur à partir d'un ordinateur d'usager.

1. Vérifiez si votre routeur a bien quatre interfaces requises. Si cela n'est pas le cas, vous pouvez créer votre propre routeur avec les interfaces demandées à partir du routeur du type *Routeur-PT-Empty*;

2. Afin de configurez les routeurs de la Figure 18, vous devez d'abord brancher un câble du type console entre le port RS 232 de l'ordinateur d'un usager et le port console du routeur :

   (a) choisissez le câble du type console (Figure 19);

   (b) branchez l'ordinateur (port RS 232) d'un usager au port console du routeur (Figure 19);

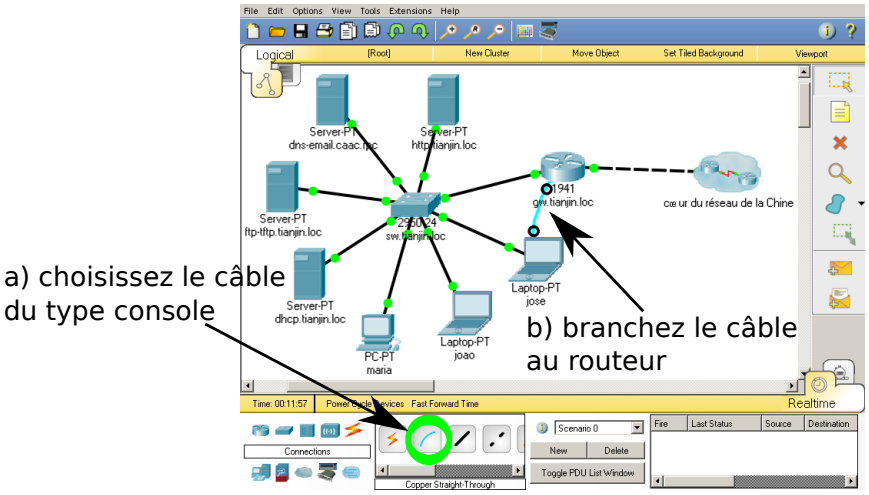


Figure 19: Brancher un câble au console du routeur.

3. Accédez à la console de configuration de votre routeur par le *Terminal* de l'ordinateur d'usager :

   (a) cliquez sur l'ordinateur pour accéder à sa fenêtre de configuration l'ordinateur d'usager ;

   (b) choisissez l'onglet *Desktop*, puis cliquez sur *Terminal* (Figure 20) ;

   (c) validez les paramètres d'accès à la console du routeur en cliquant sur *OK* (Figure 20). En suite, vous devez avoir accès à une fenêtre similaire à celle de la Figure 21 ;

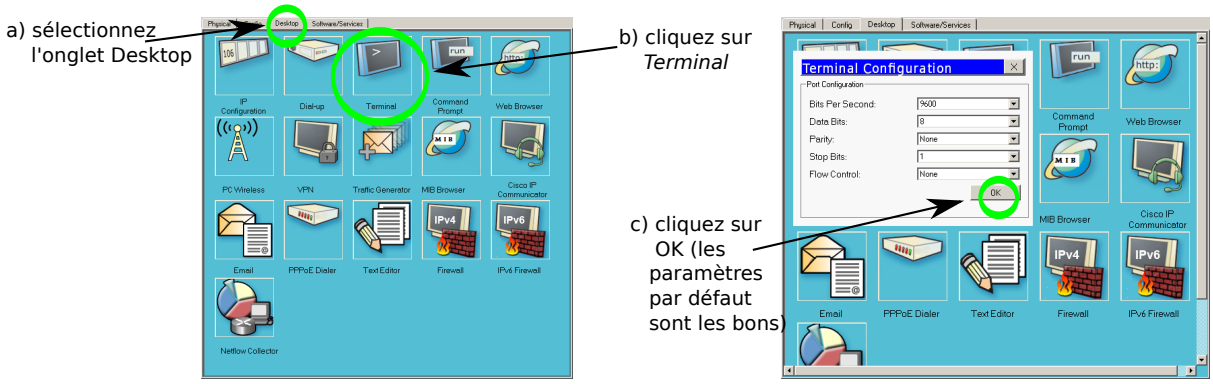


Figure 20: Le *Terminal* de l'ordinateur (client) nous permet d'accéder à la console du routeur.

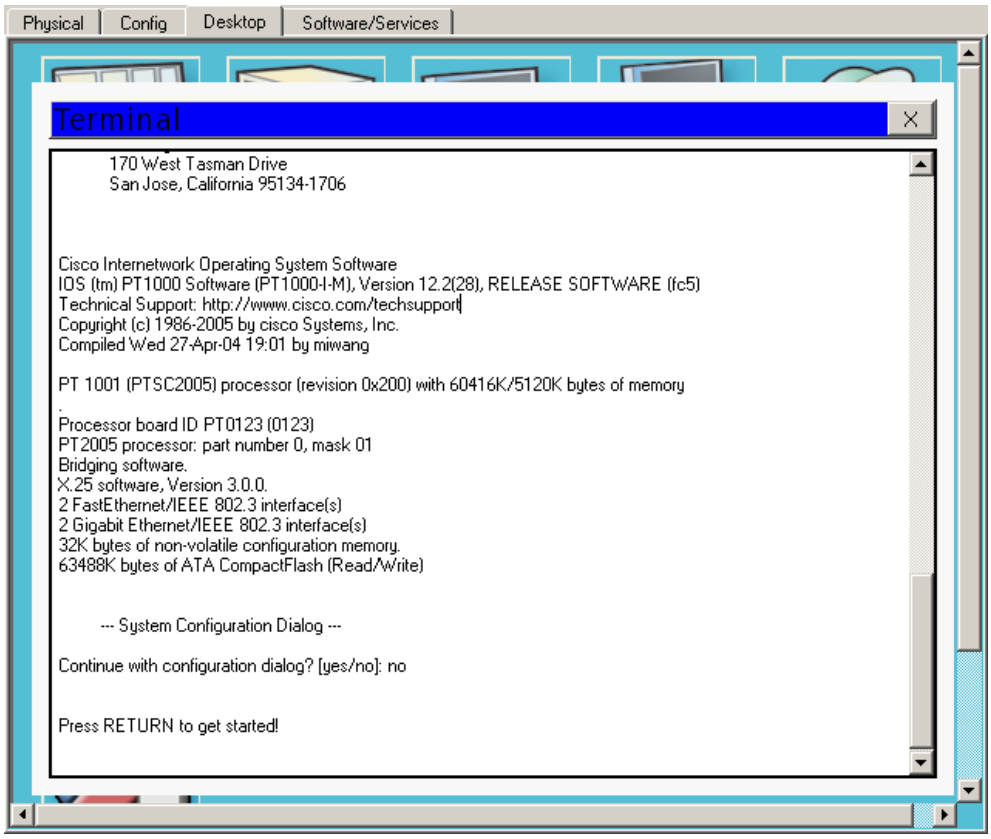


Figure 21: La fenêtre de la console du routeur.

4.4 Introduction à la modification de la configuration global d'un routeur (le changement du nom de l'hôte)

Nous allons maintenant changer le nom du routeur *gw.tianjin.loc* par la console [3] :

1. si le routeur vous propose la question de configuration par dialogue (copiée ci-bas), choisissez `no` afin d'accéder directement à sa console du routeur, puis tapez entrer ;

```
Continue with configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>
```

2. ça y est, vous êtes en mode usager (*user EXEC mode* de la *commande line interface*, CLI, des équipements Cisco). Pour vérifier les commandes disponibles dans le mode usager, donc non privilégié, tapez `?` dans la console et vous devez avoir la sortie de commande suivante :

```
Router>?
Exec commands:
  <1-99>      Session number to resume
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
Router>
```

[3] Une introduction aux modes de configuration des équipements Cisco est disponible en ligne `http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-3_2_JA/command/reference/i1232cr/cr32cli.html`

pour l'instant, nous allons nous intéresser à la commande `enable` qui va nous permettre d'accéder au mode privilégié (*Privileged EXEC Mode*) de configuration du routeur ;

3. rentrez la commande `enable` puis `?` pour avoir la liste de commandes disponibles en mode privilégié ;

```
Router>enable
Router#?
Exec commands:
  <1-99>      Session number to resume
  auto        Exec level Automation
  clear       Reset functions
  clock       Manage the system clock
  configure   Enter configuration mode
  connect     Open a terminal connection
  copy        Copy from one file to another
  debug       Debugging functions (see also 'undebug')
  delete      Delete a file
  dir         List files on a filesystem
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  erase       Erase a filesystem
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  mkdir       Create new directory
  more        Display the contents of a file
  no          Disable debugging informations
  ping        Send echo messages
  reload      Halt and perform a cold restart
  resume      Resume an active network connection
  rmdir       Remove existing directory
  send        Send a message to other tty lines
  setup       Run the SETUP command facility
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
  undebug     Disable debugging functions (see also
              'debug')
  write       Write running configuration to memory,
              network, or terminal
```

```
Router#
```

deux commandes vont nous intéresser d'avantage pour la configuration du nom, les commandes `show` et `configure terminal` ;

4. tapez `show ?` pour avoir les options d'utilisation de la commande ;

```
Router#show ?
  aaa                 Show AAA values
  access-lists        List access lists
  arp                 Arp table
  cdp                 CDP information
  class-map           Show QoS Class Map
  clock               Display the system clock
  controllers         Interface controllers status
  crypto              Encryption module
  debugging           State of each debugging option
  dhcp                Dynamic Host Configuration Protocol status
  file                Show filesystem information
  flash:              display information about flash: file system
  flow                Flow information
  frame-relay         Frame-Relay information
  history             Display the session command history
  hosts               IP domain-name, lookup style, nameservers,
  interfaces          Interface status and configuration
  ip                  IP information
  line                TTY line information
  logging             Show the contents of logging buffers
  login               Display Secure Login Configurations and Stat
  ntp                 Network time protocol
  policy-map          Show QoS Policy Map
  privilege           Show current privilege level
  processes           Active process statistics
  protocols           Active network routing protocols
  queue               Show queue contents
  queueing            Show queueing configuration
  running-config      Current operating configuration
  sessions            Information about Telnet connections
  snmp                snmp statistics
  ssh                 Status of SSH server connections
  standby             standby configuration
  startup-config      Contents of startup configuration
  tcp                 Status of TCP connections
  tech-support        Show system information for Tech-Support
```

```
  terminal         Display terminal configuration parameters
  users            Display information about terminal lines
  version          System hardware and software status
Router#show
```

à partir de cette longue liste d'options, nous allons choisir `running` pour vérifier la configuration courante du routeur (rappel, utilisez `TAB` après avoir tapé une partie de la commande pour la compléter);

5. faites rentrer `show running-config` pour vérifier la configuration actuelle du routeur :

```
Router#show running-config
Building configuration...

Current configuration : 649 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
no ip cef
no ipv6 cef
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet2/0
 no ip address
 duplex auto
```

```
 speed auto
 shutdown
!
interface GigabitEthernet3/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
end


Router#
```

nous observons que le routeur s'appelle actuellement *Router*;

6. pour changer le nom du routeur, nous devons d'abord accéder au mode de configuration global du routeur. Pour cela, à partir du mode privilégié, tapez la commande `configure terminal` :

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

7. faites rentrez le nom que vous souhaitez pour votre routeur à l'aide de la commande `hostname` puis tapez `end` pour sortir du mode de configuration global et revenir au mode privilégié ;

```
Router(config)#hostname gw.tianjin.loc
gw.tianjin.loc(config)#end
gw.tianjin.loc#
```

```
%SYS-5-CONFIG_I: Configured from console by console

gw.tianjin.loc#
gw.tianjin.loc# exit
gw.tianjin.loc>
```

nous pouvons remarquer que le prompt de la console du routeur a changé, nous avons le nom de l'hôte que vous voulions. Pour sortir du mode privilégié, rentrez `exit`. Vous pouvez constater le changement du nom de l'hôte aussi par la sortie de la commande `show running-configuration`;

Vous devez changer le nom de tous les routeurs de la Figure 18. Vous devez aussi rajouter et configurer le nom du router du réseau d'accès du réseau du Beijing, le `gw.beijing.loc`.

4.5 La configuration des adresses IP des interfaces des routeurs

Nous allons configurez les interfaces des routeurs selon la topologie décrite dans la Figure 18 (faites attention aux particularités du réseau de votre pays, spécifiées dans l'Appendice A). Nous devons configurez tous les interfaces nécessaires à la mise en place de notre topologie.

Les étapes suivantes correspondent à la configuration de l'interface `FastEthernet 0/0` du routeur `gw.tianjin.loc`. Cette interface est branchée au commutateur `sw.tianjin.loc` du réseau local/ d'accès.

1. Accédez au mode de configuration de l'interface à partir du mode usager;

```
gw.tianjin.loc>
gw.tianjin.loc>enable
gw.tianjin.loc#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
gw.tianjin.loc(config)#interface FastEthernet 0/0
gw.tianjin.loc(config-if)#
```

2. Activez l'interface (rappelez-vous, les interfaces des routeurs Cisco sont désactivés par défaut);

```
gw.tianjin.loc(config-if)#no shutdown

gw.tianjin.loc(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

la couleur qui représente l'état de l'interface sur le câble passera de rouge à vert ;

3. Configurez l'adresse IP de l'interface :

```
gw.tianjin.loc(config-if)#ip address 10.16.7.1 255.255.255.0
```

nous avons rentré l'adresse IP et le masque de sous-réseau ;

4. Vérifiez la configuration de votre interface avec la commande `ping` vers le serveur de noms, DNS (rappel, nous sommes toujours en mode de configuration de l'interface) :

```
gw.tianjin.loc(config-if)#do ping 10.16.7.2

Type escape sequence to abort.
Sending 5,100-byte ICMPEchos to 10.16.7.2,timeout is 2seconds:
.!!!!
Success rate is 80 percent(4/5),round-trip min/avg/max=0/0/0ms

gw.tianjin.loc(config-if)#
```

   cette commande `ping` envoie des messages ICMP `echo request` vers le serveur de noms qui fait partie du même sous-réseau de cette interface du notre routeur. Si le taux de réussite de la commande (indiqué à la dernière ligne de sa sortie de la commande) est supérieur à 0, votre configuration a été bien faite, si non, veuillez vérifier si le câble est branché, sont état (les couleurs des cercles aux extrémités du câble) et si les configurations de l'adresse IP et du masque de sous-réseau sont correctes ;

5. Configurez le serveur de noms dans votre routeur puis vérifiez si vous arrivez à l'utiliser avec la commande `ping` :

```
gw.tianjin.loc(config-if)#exit
gw.tianjin.loc(config)#ip name-server 10.16.7.2
gw.tianjin.loc(config)#do ping www
Translating "www"...domain server (10.16.7.2)
Type escape sequence to abort.
Sending 5,100-byte ICMPEchos to 10.16.7.3,timeout is 2seconds:
.!!!!
Success rate is 80 percent(4/5),round-trip min/avg/max=0/0/0ms

gw.tianjin.loc(config)#
```

   tout d'abord, nous sommes sortis du mode de configuration de l'interface pour revenir au mode de configuration global (commande `exit`). En suite, nous avons fait rentrer l'adresse IP du serveur de noms par la commande `ip name-server 10.16.7.2`. Finalement, nous avons utilisé la commande `ping` vers le nom `www` pour vérifier notre configuration. Un taux de réussite supérieur à 0 confirme le bon fonctionnement de notre configuration.

Vous devez vous inspirer de la configuration de cette interface afin de configurer les autres interfaces des routeurs de la Figure 18.

4.6 La configuration des routes statiques pour assurer la connectivité des réseau locaux/d'accès

Cette étape du TP nous permettra d'avoir enfin un réseau interconnecté, où tous les nœuds de deux réseau d'accès pourrons se communiquer.

Pour cela, nous allons ajouter toutes routes statiques nécessaires à chaque routeur. Ces routes doivent tenir compte de l'ensemble de réseaux de la Figure 18 ainsi que des lien physiques que les interconnectes.

La liste de étapes suivante décrit l'ajout de routes statiques sur le routeur `gw.tianjin.loc`.

1. Rentrez en mode de configuration global (à partir du mode usager), puis tapez `ip ?` afin de lister les options de configuration globales de la commande `ip` :

```
gw.tianjin.loc>enable
gw.tianjin.loc#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
gw.tianjin.loc(config)#ip ?
  access-list        Named access-list
  cef                Cisco Express Forwarding
  default-network    Flags networks as candidates for default
                     routes
  dhcp               Configure DHCP server and relay parameters
  domain             IP DNS Resolver
  domain-lookup      Enable IP Domain Name System hostname
                     translation
  domain-name        Define the default domain name
  flow-export        Specify host/port to send flow statistics
  forward-protocol   Controls forwarding of physical and
                     directed IP broadcasts
  ftp                FTP configuration commands
  host               Add an entry to the ip hostname table
  name-server        Specify address of name server to use
  nat                NAT configuration commands
  route              Establish static routes
  ssh                Configure ssh options
  tcp                Global TCP parameters
gw.tianjin.loc(config)#ip
```

   nous allons utiliser le paramètre `route` pour rentrer les routes statiques de notre réseau ;

2. Vérifiez les paramètres de la commande `ip route`, puis ajoutez les routes nécessaires à joindre tous les autres réseaux :

```
gw.tianjin.loc(config)#ip route ?
  A.B.C.D  Destination prefix
gw.tianjin.loc(config)#ip route 172.16.72.0 ?
  A.B.C.D  Destination prefix mask
gw.tianjin.loc(config)#ip route 172.16.72.0 255.255.255.0 ?
  A.B.C.D           Forwarding router's address
  Ethernet          IEEE 802.3
  FastEthernet      FastEthernet IEEE 802.3
  GigabitEthernet   GigabitEthernet IEEE 802.3z
  Loopback          Loopback interface
  Null              Null interface
  Serial            Serial
.loc(config)#ip route 172.16.72.0 255.255.255.0 172.16.7.254
.loc(config)#ip route 172.16.2.0 255.255.255.0 172.16.7.254
.loc(config)#ip route 10.16.2.0 255.255.255.0 172.16.7.254
gw.tianjin.loc(config)#
```

notez que la commande a comme paramètres le préfixe du réseau à être ajouté, son masque de sous-réseau et la passerelle qui amène à ce réseau. Nous avons ajouté au fur et à mesure les réseaux intermédiaires qui amènent au réseau du Beijing de la Figure 18.

3. Listez la nouvelle table de routage du routeur :

```
gw.tianjin.loc(config)#end
gw.tianjin.loc#show ip route
Codes:C-connected, S-static, I-IGRP, R-RIP, M-mobile, B-BGP
      D-EIGRP, EX-EIGRP external, O-OSPF, IA-OSPF inter area
      N1-OSPF NSSA external type1,N2-OSPF NSSA external type2
      E1-OSPF external type 1, E2-OSPF external type 2, E-EGP
      i-IS-IS, 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 not set

     10.0.0.0/24 is subnetted, 2 subnets
S       10.16.2.0 [1/0] via 172.16.7.254
C       10.16.7.0 is directly connected, FastEthernet0/0
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.2.0 [1/0] via 172.16.7.254
C       172.16.7.0 is directly connected, GigabitEthernet2/0
```

```
S        172.16.72.0 [1/0] via 172.16.7.254
gw.tianjin.loc#
```

4. Listez la configuration finale du routeur :

```
gw.tianjin.loc#show running-config
Building configuration...

Current configuration : 850 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname gw.tianjin.loc
!
!
no ip cef
no ipv6 cef
!
!
ip name-server 10.16.7.2
!
!
interface FastEthernet0/0
 ip address 10.16.7.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet2/0
 ip address 172.16.7.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet3/0
 no ip address
```

```
 duplex auto
 speed auto
 shutdown
!
ip classless
ip route 10.16.2.0 255.255.255.0 172.16.7.254
ip route 172.16.2.0 255.255.255.0 172.16.7.254
ip route 172.16.72.0 255.255.255.0 172.16.7.254
!
ip flow-export version 9
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
end

gw.tianjin.loc#
```

4.7 Configuration des nœuds du réseau du Beijing et vérification de connectivité avec le réseau de Tianjin

Afin de déployer le réseau d'accès du Beijing pour la vérification, nous allons :

1. Ajouter un commutateur au réseau d'accès du Beijing et y brancher le routeur d'accès ;

2. Configurer un serveur DHCP pour le réseau du Beijing (pour cela, vous pouvez faire copier/coller du serveur DHCP de Tianjin, puis changer son adresse IP statique et la plage d'adresse à attribuer aux usagers);

3. Déplacer un des usagers du réseau de Tianjin vers le réseau du Beijing, ainsi cet usager pourra envoyer un e-mail aux autres usager pour les informer que le réseau du Beijing et les réseau intermédiaires du cœur du réseau sont fonctionnels ;

Pour vérifier la connectivité entre les nœuds de deux réseaux, vous devez :

1. Utiliser la commande `traceroute` (*e.g.*, `traceroute NŒUD_CIBLE`, où le nœud cible appartient au réseau distant) pour vérifier si le chemin est correctement configuré. Si

vous n'arrivez pas à rejoindre l'autre réseau, veuillez vérifier la table de routage des nœuds où l'envoie de réponse aux messages du `traceroute` s'arrêtent;

2. La vérification finale sera par l'envoie d'e-mails d'usager branché au réseau du Beijing vers ses collègues du réseau de Tianjin ;

5 Une introduction au routage dynamique avec le protocole RIP

5.1 Objectifs

Ces TPs consistent à finaliser le déploiement du cœur du réseau de chaque pays et de les interconnectés. A la fin de la séance, nous devrons être capables d'envoyer d'e-mails d'un pays à l'autre.

Les objectifs des TPs sont :

- étudier la mise en place d'un protocole de routage ;
- comprendre la configuration et le fonctionnement de RIPv2 ;
- interconnecter des réseaux simulés par le réseau (réel) local de la salle ;

Pour illustrer l'interconnexion par le réseau local (réel), nous avons utiliser l'exemple des réseaux de deux pays : la France et la Chine. Dans notre exemple, nous souhaitons brancher deux routeurs : le routeur `toulouse.cor`en France au routeur `tianjin.cor` en Chine. Ce branchement sera mis en œuvre par une fonctionnalité de Packet Tracer et utilisera la liaison local réelle pour l'échange de données entre les réseaux de deux pays. Lors de la configuration de ce branchement, nous supposerons le cas de figure où le réseau français (*le demandeur*) sollicite le branchement au réseau chinois (*le destinataire*).

5.2 La mise en place des liens physiques et logiques du cœur du réseau

Cette étape consiste à finaliser le déploiement physique du cœur du réseau et de configurer localement l'adresse IP de chaque interface et sa respective masque de sous-réseau. Les informations sur l'adressage IP à être utilisé sont décrites dans l'Appendice A de cache documents de TPs.

L'objectif ici est d'assurer **la connectivité locale** de tous les routeurs du cœur du réseau. Voici la procédure à suivre pour chaque :

1. Effacez toutes les routes statiques qui vous avez ajouté manuellement auparavant;
2. Branchez toutes les liaisons physiques (les câbles) vers les routeurs voisins;
3. Configurez l'adresse et masque de sous-réseau pour chaque interface (ces informations sont détaillées dans les appendices) ;
4. Vérifiez la connectivité local avec les routeurs voisins en utilisant la commande `ping` ;

5.3 La configuration du protocole RIPv2 et la mise en place de la connectivité globale

Une fois que vous avez vérifié que chaque routeur est capable de joindre tous ses voisins (par `ping`), nous pouvons mettre en place le protocole de routage RIPv2 pour assurer la connectivité globale. Dès que le protocole de routage sera dûment configuré sur tous les routeurs (du cœur du réseau et du réseau d'accès), les routeurs pourrons diffuser leurs informations locales aux autres routeurs. Les échanges d'informations par RIPv2 permettront les routeurs de remplir leurs tables de routage automatiquement et surtout d'assurer une connectivité globale.

Pour configurer le RIPv2 sur les routeurs, vous devez utiliser les commandes suivantes sur la console des routeurs Cisco :

```
enable
conf t
router rip
version 2
no auto-summary
network 172.16.0.0
network 172.31.0.0
network 10.0.0.0
default-information originate
```

Les commandes représentent :

- `enable` : nous passons au mode privilégié ;
- `conf t` : pour accéder au mode de configuration globale ;
- `router rip` : nous permet de passer au mode de configuration du routeur pour configurer le protocole RIP ;
- `version 2` : nous choisissons la version 2, la plus récente, du protocole RIP ;
- `network 172.16.0.0`: nous déclarons un premier préfixe qui correspond à un ensemble de réseaux dont la porté est à l'échelle d'un pays (veuillez consulter l'Appendice A pour plus de détails) ;
- `network 172.31.0.0`: nous déclarons un deuxième préfixe qui correspond à un autre ensemble de réseaux dont la porté est à l'échelle d'un pays (veuillez consulter l'Appendice A pour plus de détails) ; ;
- `network 10.0.0.0` : nous déclarons tous les réseau d'accès avec un seul préfixe ;
- `default-information originate` : cela sert à créer des routes par défaut dans le RIP (pour les routeur aux extrémités du réseau) ;
- `end` : nous finalisons la configuration et nous revenons au mode privilégié ;

5.4 La vérification du fonctionnement du protocole RIPv2

Afin de vérifier le fonctionnement du protocole RIPv2, vous devez déployer un nouveau réseau d'accès (cela sera le troisième) au réseau de votre pays et essayer de vous communiquer avec les deux autres réseau existants.

Pour cela, nous vous conseillons de :

1. Choisir le réseau local de deux villes qui sont aux extrémités du réseau d'un pays (voir la Figure 34) ;

2. Ajouter et configurer le routeur du nouveau réseau d'accès ;

3. Ajouter un commutateur à ce nouveau réseau auquel seront branchés les équipement du réseau d'accès ;

4. Déployer un serveur DHCP au nouveau réseau choisi (voir l'appendice de votre pays pour connaître les paramètres d'adressage IP) ;

5. Déplacer un de vos usagers de votre premier réseau d'accès déployé vers le nouveau réseau d'accès de votre choix ;

6. Vérifier la connectivité globale avec les commandes `ping` et `traceroute` (essayez de corriger des erreurs éventuels) ;

7. **Envoyer un e-mail à partir de l'usager du nouveau réseau d'accès aux autres usagers du réseau du pays** afin de leur annoncer que la connectivité globale fonctionne proprement ;

5.5 La mise en place de la connectivité entre les deux pays

Pour conclure les TPs sur le routage, nous allons interconnecté les réseau de deux pays. Nous vous conseillons d'utiliser **les routeurs du cœur du réseau de Tianjin et de Toulouse**, c'est à dire que nous allons brancher un lien logique entre ces deux routeurs à travers un réseau qui nous appellerons d'Internet. Pour cela, nous allons utiliser une fonctionnalité du Cisco Packet Tracer que nous permet de "brancher" des réseaux des ordinateur différents par le réseau local de la salle de TP.

Nous décrivons la procédure à faire de la façon suivante :

1. Pour le réseau destinataire, le réseau chinois, configurez les paramètre d'accès à Cisco Packet Tracer par le réseau local réel (voir Figure 22) ;

2. Pour le destinataire (réseau chinois), vérifiez, et modifiez si nécessaire, les configurations qui permettent l'accéder au Cisco Packet Tracer par le réseau local réel (voir Figure 23) ;

3. Encore du côté chinois, le destinataire de la demande de branchement, accédez au menu qui nous permet de configurer la visibilité de ports des équipements qui seront disponibles pour un branchement par une connexion à travers du réseau local réel (voir Figure 24) ;

4. Choisissez les ports des équipements qui seront visibles/disponibles au demander de branchement par le réseau local réel (voir Figure 25) ;

5. A partir du réseau de la France, nous ajoutons un élément de connexion, le *Multiuser Connection*, qui nous permet de nous connecter aux réseau de la Chine (voir Figure 26) ;

6. Remplissez du côté du réseau de France, le demandeur, les paramètre nécessaire pour nous brancher au réseau du côté de la Chine (voir Figure 27). Le réseau qui a été sollicité du côté français apparaît du côté de la Chine avec le nom que nous avons indiqué, Internet (voir Figure 28);

7. Du côté du demandeur de branchement, le réseau français, cliquez sur nuage qui représente le réseau créé, ainsi nous pouvons voir les ports des équipement qui sont visibles/disponibles du côté de la Chine (voir Figure 29). Le réseau qui a été créé et branché en France apparaît du côte français (veuillez voir Figure 30) et du côté de la Chine ;

8. Configurez la connectivité local du lien physique que vous venez de créer. Dès que cela sera fait, le protocole RIPv2 mettra à jour les tables de routages de routeurs de deux pays afin d'assurer la connectivité globale;

9. Vérifiez la connectivité globale de deux réseaux par `ping`, `traceroute` et finalement par l'envoie d'e-mail du réseau d'un pays à l'autre ;

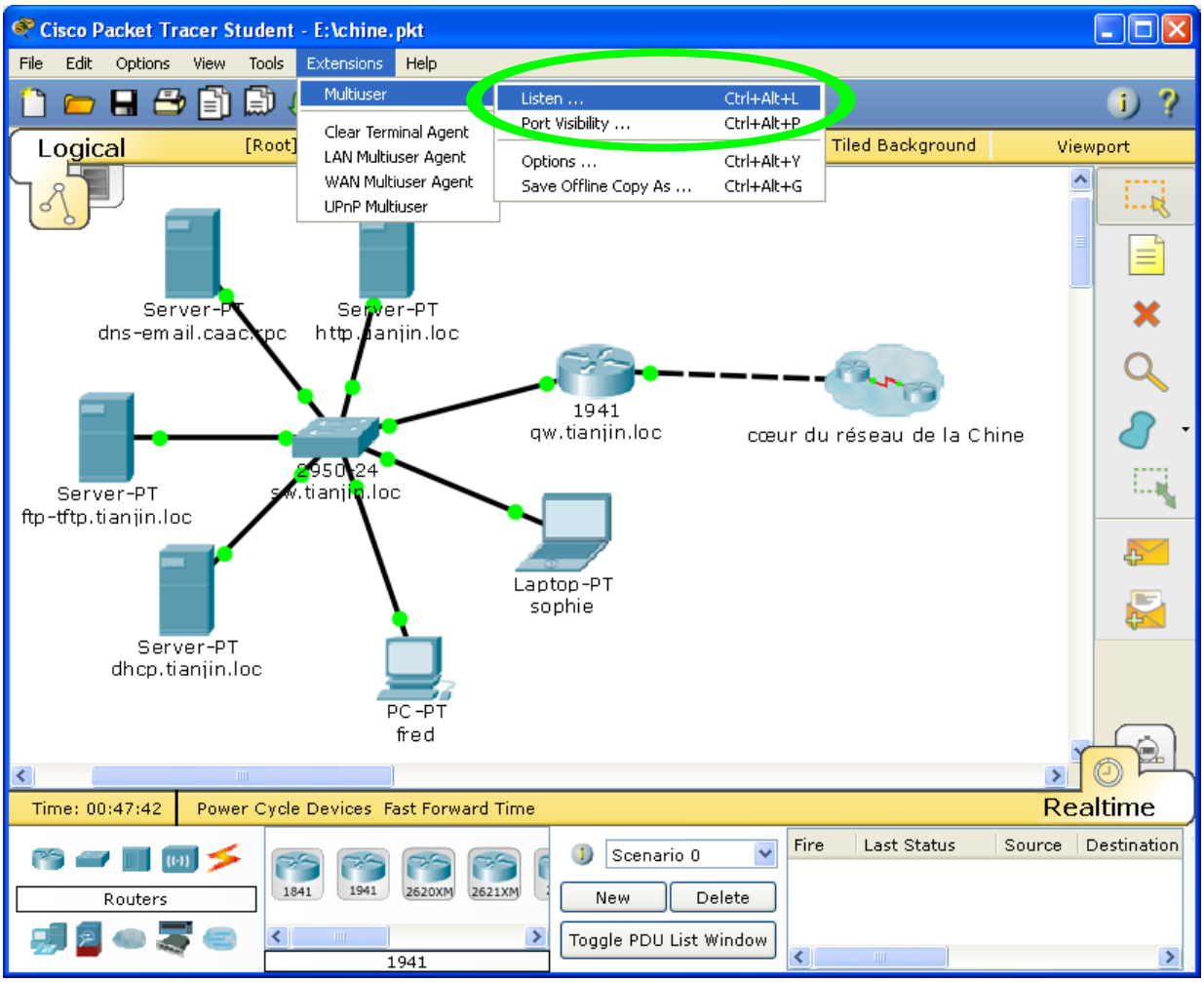


Figure 22: Nous devons choisir l'option *Listen* afin de configurez les paramètre d'accès à Cisco Packet Tracer par le réseau local de la salle. Dans ce exemple, nous souhaitons que le réseau chinois accepte de connections demandées par le réseau local.

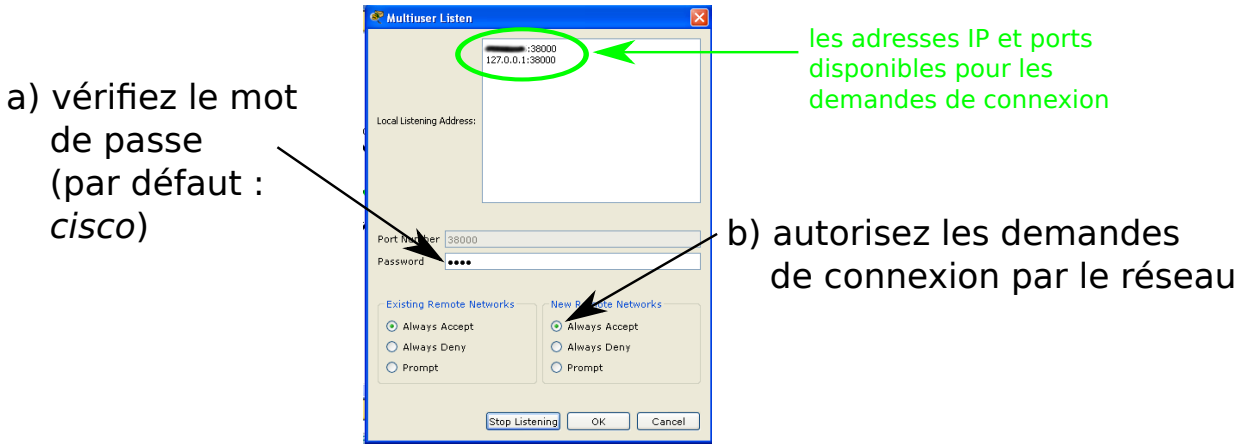


Figure 23: Cette fenêtre nous permet de configurer les paramètres du destinataire, dans notre cas, la Chine. Veuillez vérifier, et modifier si nécessaire, les configurations qui permettent l'accès au Cisco Packet Tracer par le réseau local de la salle. Cet image nous montre le choix du port 38000. Les demandes de connections d'un nœud distant seront toujours acceptées sur ce port et les adresses du lien local et *localhost*.

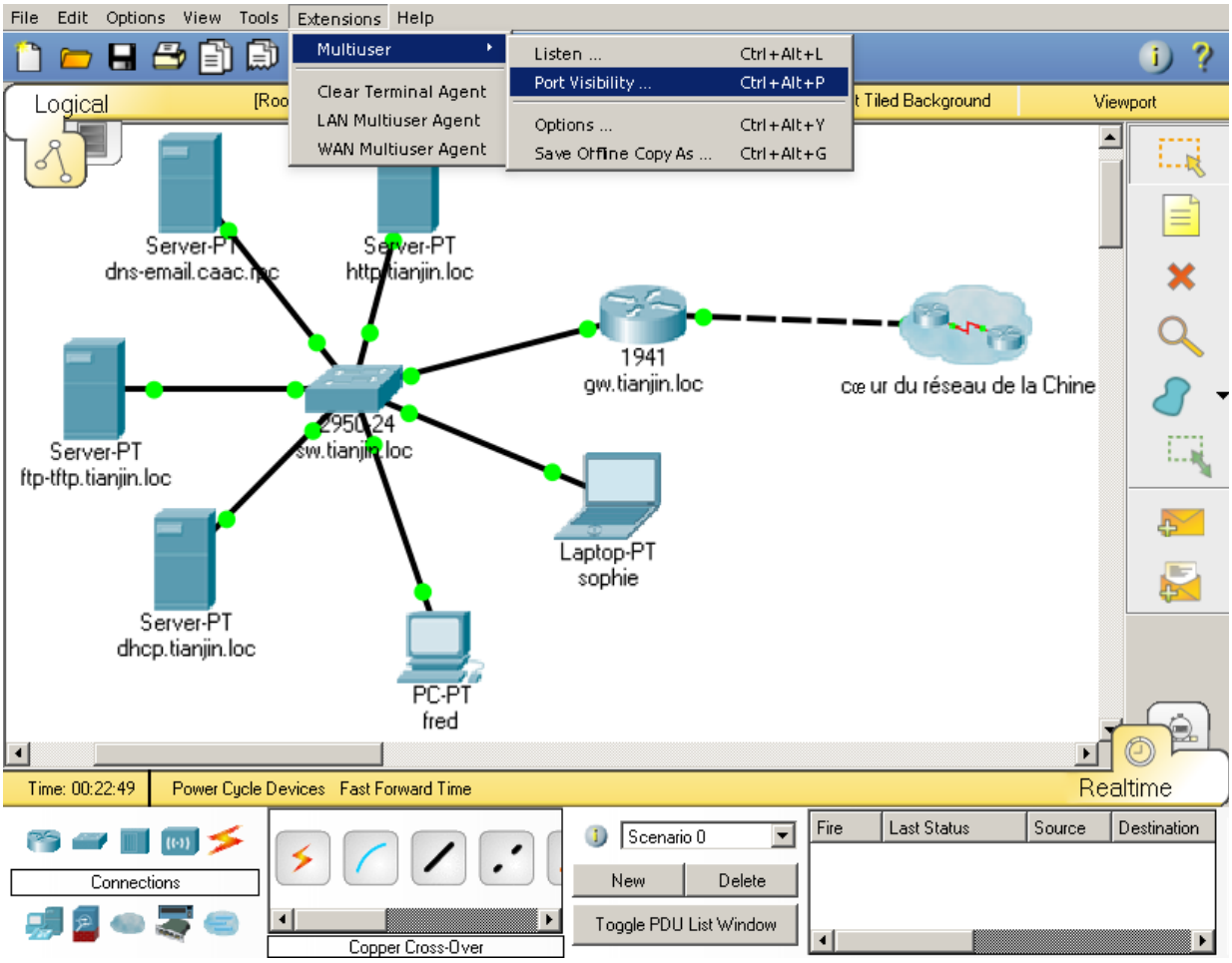


Figure 24: Configurez la visibilité de ports des équipements par le réseau local de la salle. Ceci doit être fait su côté du destinataire, par exemple, sur le réseau chinois.

sélectionnez les ports des équipements que vous souhaitez laisser visible à l'extérieur (partagés). Par exemple, le port Serial2/0 du routeur du cœur du réseau chinois à Tianjin.

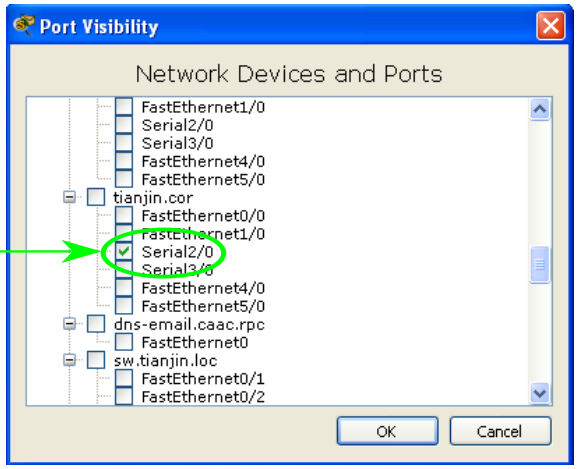


Figure 25: Choisissez les ports des équipements qui seront visibles/partagés par le réseau local de la salle. Ceci doit être lancé sur le destinataire de la connexion, dans notre exemple, le réseau chinois.

sélectionnez l'élément *Multiuser Connection* et faites-le glisser vers votre topologie

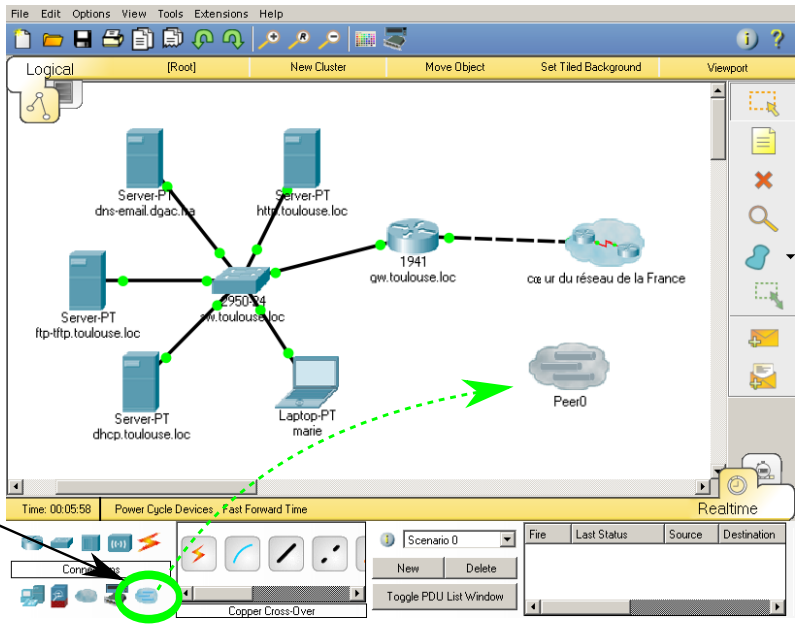


Figure 26: A partir du réseau de France, nous ajoutons un élément qui nous permet de nous connecter aux réseau de la Chine.

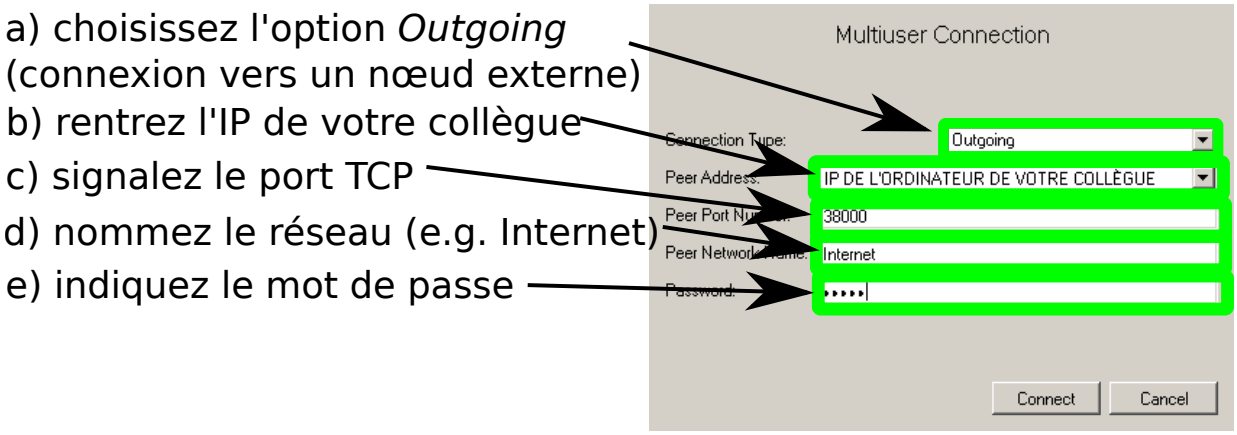


Figure 27: Nous remplissons du côté du réseau de France les paramètre nécessaire pour nous connecter et créer un réseau du côté de la Chine.

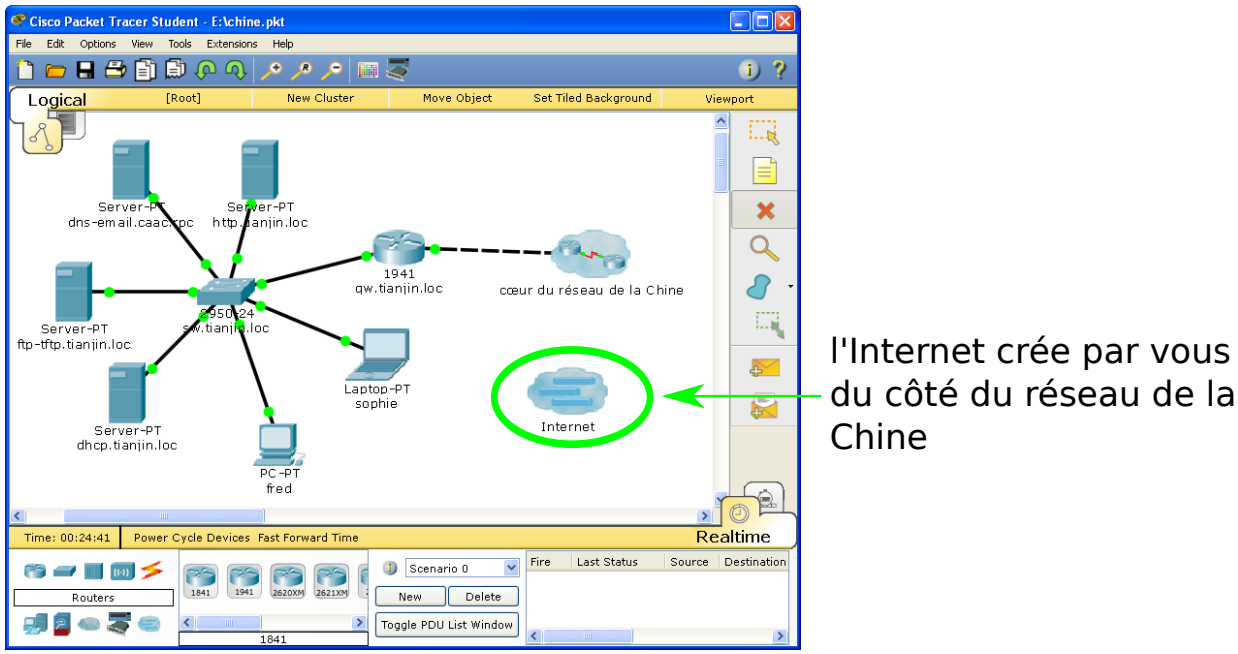


Figure 28: Le réseau qui a été créé du côté français apparaît du côté de la Chine avec le nom que nous avons indiqué, Internet.

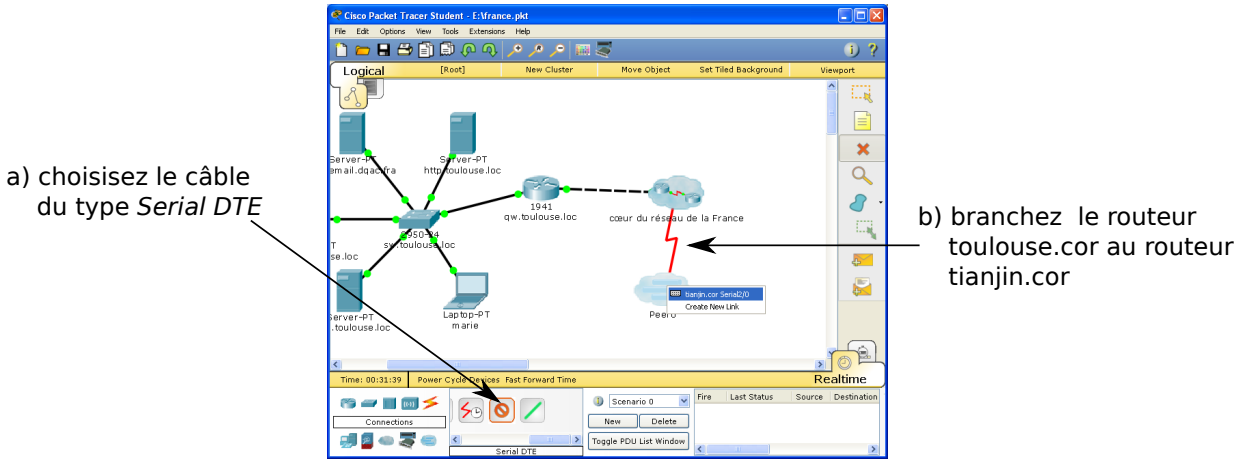


Figure 29: Quand nous cliquons sur le réseau créé, nous pouvons voir les ports des équipement qui sont visibles/partagés du côté de la Chine.

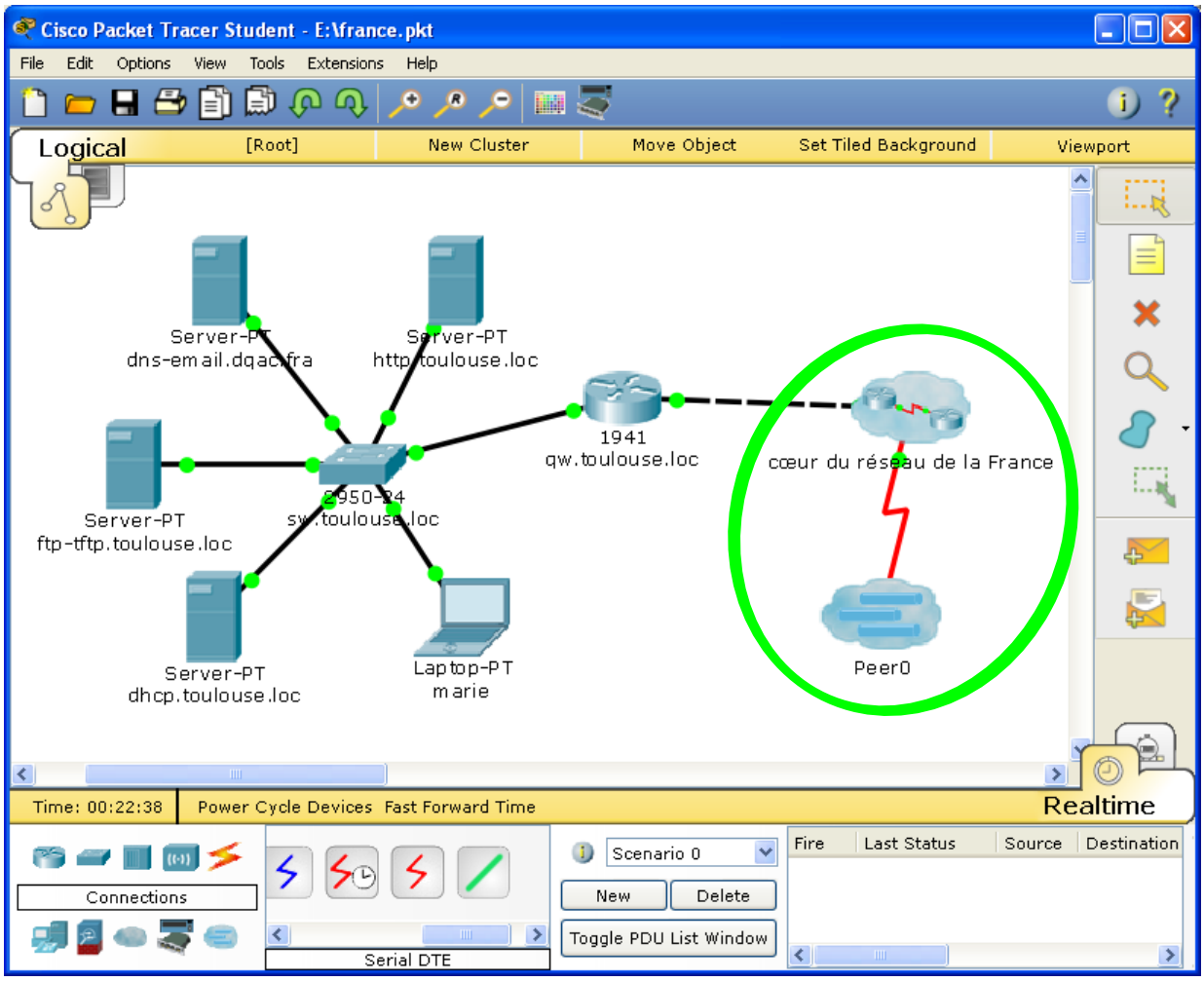


Figure 30: Le réseau créé apparaît du côte français.

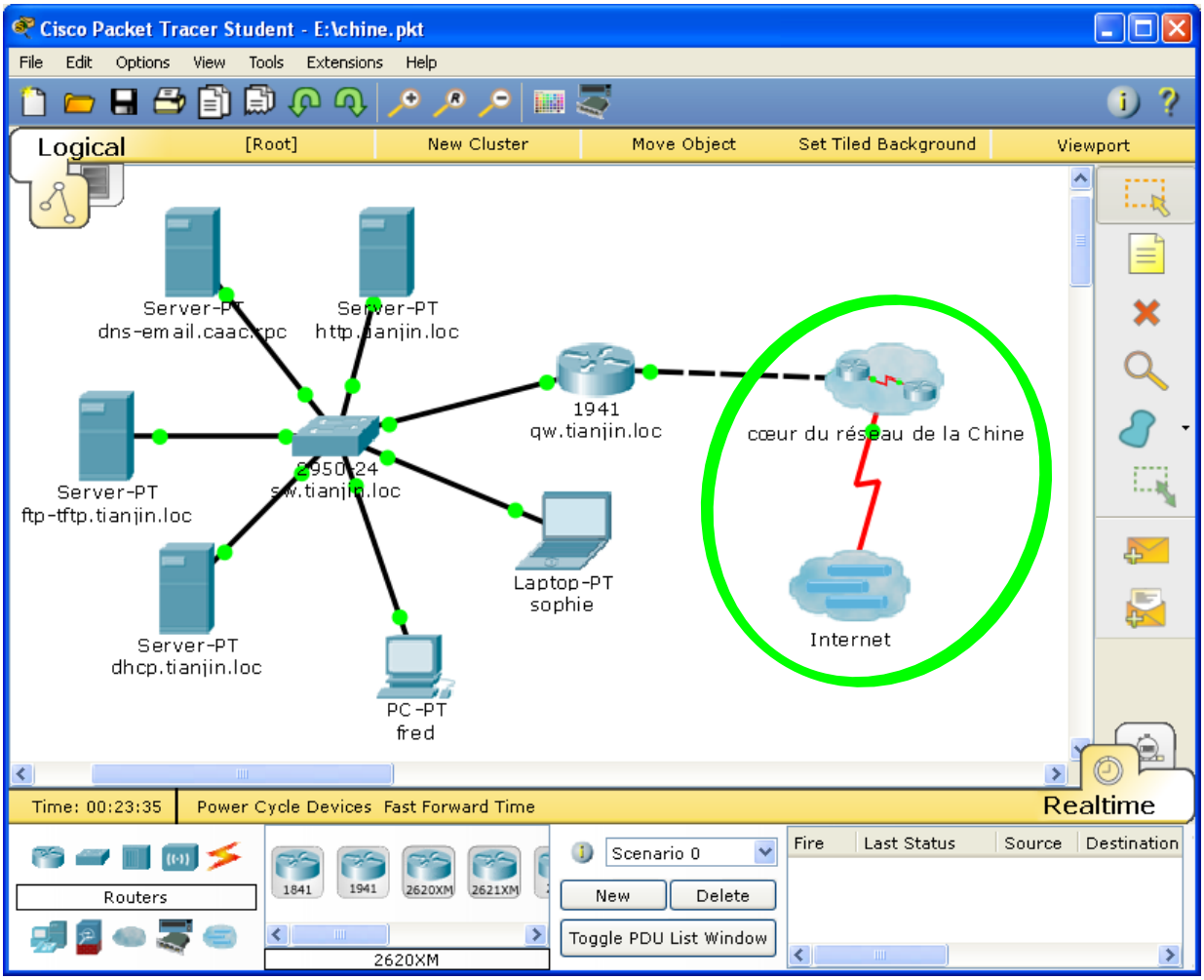


Figure 31: Le réseau créé en France apparaît du côté chinois.

A
Notre Réseau de la République Populaire de Chine

Le réseau de la République Populaire de Chine (RPC) que nous allons mettre en œuvre pendant nos séances des TPs est composé d'un cœur et de plusieurs réseaux d'accès (réseaux locaux). Nous détaillons ici la topologie et le plan d'adressage de ces deux réseau ainsi que les services/applications de nom et d'e-mail pour l'ensemble du réseau de la Chine.

A.1 Le cœur du réseau de la Chine

A.1.1 La topologie

Le cœur du réseau relie 12 villes de la Chine, représentées dans la Figure 33. Chaque ville a son propre routeur, représenté par son identifiant numérique sur la carte [4].

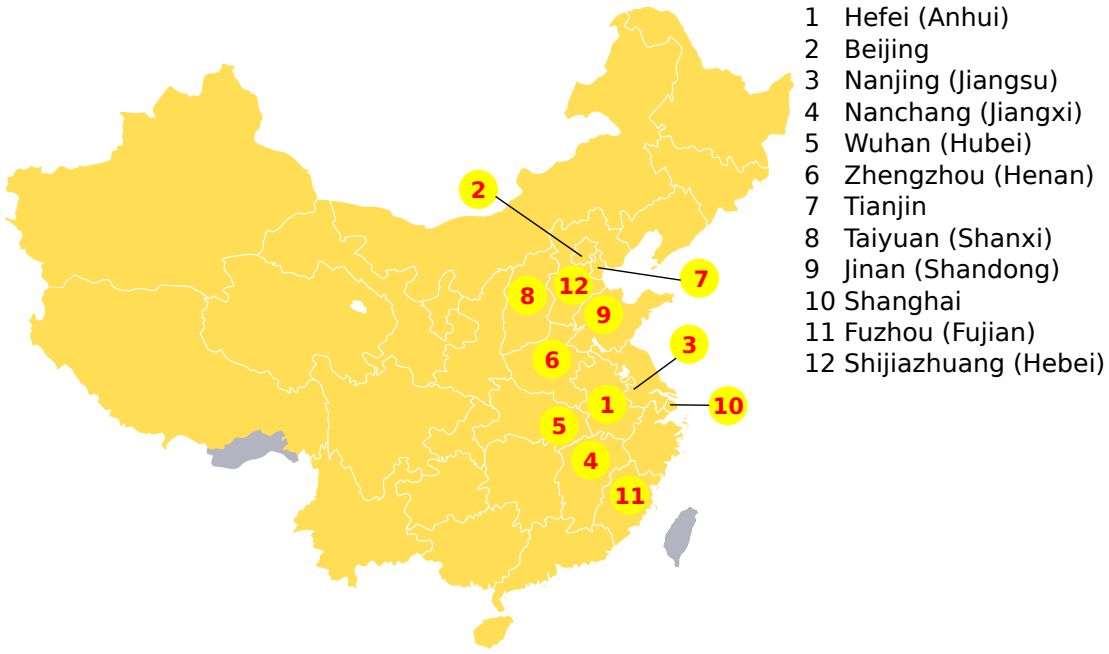
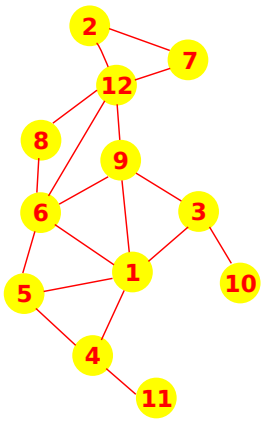


Figure 33: Les routeurs de chaque ville du cœur du réseau de la Chine.

Afin de relier les routeurs du cœur entre eux, nous supposons que chaque pair de villes voisines a un lien physique (par exemple, il y a un lien physique entre les routeurs du cœur du réseau de Beijing et Tianjin). La Figure 34 représente tous les routeurs du cœur du réseau de la Chine reliés par de liens physiques.

[4]Source : By ASDFGH - Own work, Public Domain, `https://commons.wikimedia.org/w/index.php?curid=18573908`



1 Hefei (Anhui)
2 Beijing
3 Nanjing (Jiangsu)
4 Nanchang (Jiangxi)
5 Wuhan (Hubei)
6 Zhengzhou (Henan)
7 Tianjin
8 Taiyuan (Shanxi)
9 Jinan (Shandong)
10 Shanghai
11 Fuzhou (Fujian)
12 Shijiazhuang (Hebei)

Figure 34: Une représentation logique du cœur du réseau de la Chine.

A.1.2 Le plan d'adressage

Le plan d'adressage est défini de la façon suivante :

- Adresse du réseau : 172.16.**XY**.0, où **XY** est formé de la juxtaposition de deux identifiants (listés dans la Figure 33) de villes voisines, dont le **X** est toujours le plus grand entre les deux identifiants. Par exemple, l'adresse du réseau du lien physique entre Beijing et Tianjin sera le 172.16.**72**.0, car 7, l'identifiant de Tianjin, vient d'abord pour être plus grand que celui de Beijing, 2 ;
- Masque de sous-réseau : 255.255.255.0 ;
- Les adresses des routeurs du même réseau (entre pairs de routeurs) : Nous utiliserons le premier adresse, 1, pour le routeur de la ville avec l'identifiant le plus petit et le dernier, 254, pour celui avec l'identifiant le plus grand. Par exemple, pour le réseau entre Beijing et Tianjin, nous aurons l'adresse 172.16.72.1 pour le routeur du côté du Beijing et 172.16.72.254 pour celui du côté de la ville de Tianjin ;

A.2 Réseaux d'accès de la Chine

A.2.1 La topologie

Un réseau de d'accès doit avoir au moins la topologie représenté en Figure 35. Cette topologie représente le réseau d'accès avec trois serveurs d'application (`tftp-ftp`, `http` et `dhcp`), un client (`fred`), un commutateur et un routeur qui joue le rôle de passerelle vers le cœur du réseau. Chaque nœud a un nom dont la partie VILLE devra être remplacée par le nom de la ville correspondante du réseau d'accès.

Un réseau d'accès particulier sera celui de la ville de Tianjin car nous ajouterons à ce réseau un serveur avec deux application pour l'ensemble du réseau de la Chine : l'e-mail et le DNS. La topologie du réseau d'accès de la ville de Tianjin est représenté dans la Figure 36.

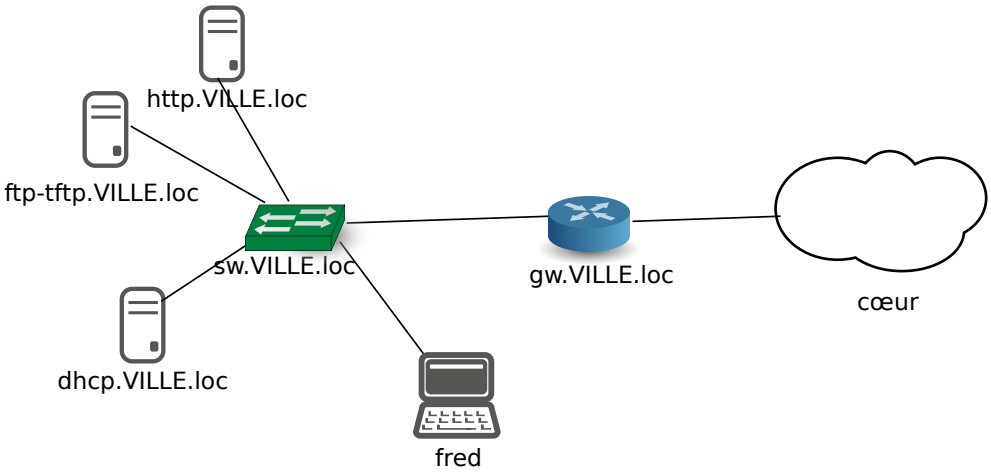


Figure 35: Le réseau d'accès type de la Chine.

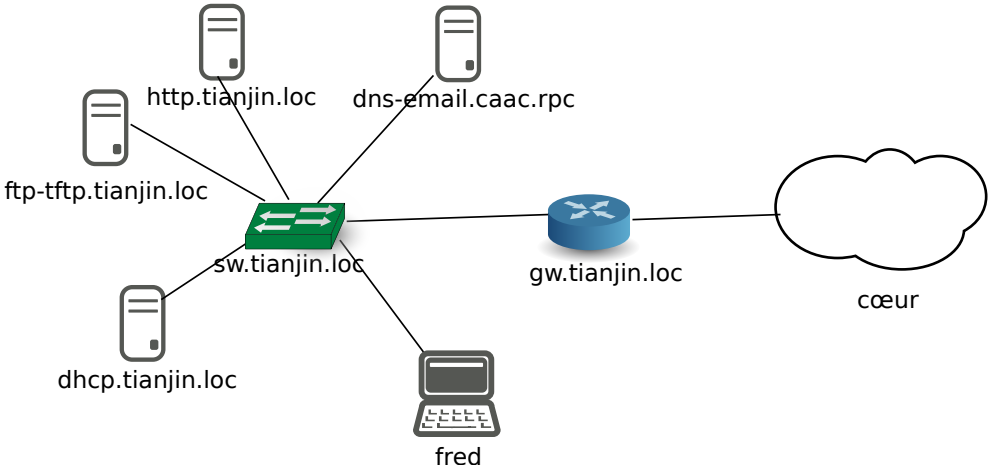


Figure 36: Le réseau d'accès de la ville de Tianjin, où il y a les services/applications d'e-mail et DNS pour l'ensemble du réseau de la Chine.

A.2.2 Le plan d'adressage

Le plan d'adressage de ce réseau suit les recommandations suivantes :

- Adresse du réseau d'accès : 10.16.**X**.0, où **X** est l'identifiant de la ville (listé en Figure 33). Par exemple, le réseau d'accès de la ville Tianjin sera 10.16.7.0 ;
- Adresse du réseau vers le cœur du réseau : 172.16.**X**.0, où **X** est l'identifiant de la ville(listé en Figure 33). Par exemple, le réseau entre la passerelle de la ville Tianjin et le cœur sera 172.16.7.0 ;
- Masque de sous-réseau : 255.255.255.0 pour le réseau d'accès et aussi pour le réseau entre la passerelle et le routeur voisin du cœur;

- Les adresses des routeurs du même réseau (entre pairs de routeurs) : Nous utiliserons le premier adresse de chaque réseau, 1, pour les deux interfaces la passerelle. Par exemple, les adresses du routeur qui sert de passerelle pour le réseau d'accès de la ville de Tianjin seront 10.16.7.1 et 172.16.7.1;

A.2.3 Liste de noms et d'identifiants réseau (les adresses IP) pour l'application/service DNS

Nous avons trois principaux types de nom de domaine pour le réseau de la Chine :

- Nom de domaine local : qui est formé du nom de la ville puis le suffixe `.loc` (le nom du domaine local). Par exemple, pour le réseau local de la ville de Tianjin, nous aurons le nom de domaine suivant : `tianjin.loc` ;

- Nom de domaine pour le cœur du réseau : chaque router à un nom qui fait partie du domaine `.cor` (le nom du domaine du cœur du réseau). Lorsque nous parlons du routeur du cœur du réseau installé à Tianjin, son nom sera `tianjin.cor` ;

- Notre nom de domaine pour tout le réseau de la Chine: il s'agit d'un domaine global `caac.rpc` qui nous utiliserons pour créer notre service/application d'e-mail, à être installé sur le réseau local de la ville de Tianjin.

Le Tableau 5 contient les paramètres nécessaires pour configurer le serveur de noms (DNS) de la Chine sur Cisco Packet Tracer.

Cette liste de paramètres est compatible avec l'implémentation de l'application DNS de Cisco Packet Trace. Certaines fonctionnalités, comme l'hiérarchie des serveurs de noms et `MX`, ne sont pas disponible sur la version (6.2, Student Version) utilisée pendant la rédaction de ce document.

A.2.4 Liste de paramètre pour l'application/service d'email

La configuration du serveur d'e-mail pour le réseau de la Chine est très simple. Nous avons besoin de faire rentrer deux types de paramètres :

1. Domain Name : `caac.rpc` ;

2. Setup User : il faut rentrer un *username*/nom et un *password*/mot de passe pour chaque usager qui pourra envoyer et recevoir e-mails. Par exemple, si nous ajoutons l'usager "fred" (avec un mot de passe "fred"), son e-mail sera fred@caac.rpc. Nous vous conseillons d'ajouter au moins trois usagers ;

Nom du serveur	**Type de paramètre**	**Détails**
ftp-tftp.tianjin.loc	A Record	10.16.7.14
dhcp.tianjin.loc	A Record	10.16.7.15
gw.tianjin.loc	A Record	10.16.7.1
sw.tianjin.loc	A Record	10.16.7.20
http.tianjin.loc	A Record	10.16.7.3
www.tianjin.loc	CNAME	`http.tianjin.loc`
www	CNAME	`http.tianjin.loc`
dns-email.caac.rpc	A Record	10.16.7.2
dns	CNAME	`dns-email.caac.rpc`
caac.rpc	NS Record	`dns-email.caac.rpc`
caac.rpc	A Record	10.16.7.2
caac.rpc	SOA	*Primary Server Name* : `dns-email.caac.rpc` *Mail Box* : `dns-email.caac.rpc` *Expiry Time* : 1209600 *Refresh Time* : 172800 *Retry Time* : 900 *Minimum TTL* : 3600

Table 5: Paramètres du serveur de noms de la Chine.

References

[1] *Cisco packet tracer.* `https://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html`, 02 2015.