ANNÉE 2023/2024

TP n° 2 : Outils pour les réseaux

NET4101

Ingénieur généraliste, 2ème année

Rédacteurs

Rémy Grünblatt
Maître de conférences
remy.grunblatt@telecom-sudparis.eu

Jehan Procaccia
Ingénieur systèmes et réseaux
jehan.procaccia@imtbs-tsp.eu

Équipe enseignante

Andrea Araldo
Maître de Conférences
andrea.araldo@telecom-sudparis.eu

Laurent Bernard
Directeur d'études
laurent.bernard@telecom-sudparis.eu

Franck Gillet
Ingénieur R&D — Plateforme
franck.gillet@telecom-sudparis.eu

Antoine Lavignotte
Directeur d'études
antoine.lavignotte@telecom-sudparis.eu

Objectifs de ce TP et compétences à acquérir

— Connaître les interfaces des matériels utilisés dans NET 4101
— Savoir se connecter aux équipements réseaux
— Configurer et utiliser un client SSH
— Connaître les outils et commandes de base de configuration réseau sous différents systèmes
— Mettre en œuvre une configuration réseau simple en ligne de commande
— Diagnostiquer et réparer des problèmes réseaux classiques
— Manipuler et utiliser wireshark

Important : Pour la réalisation de ce TP, vous devez récupérer une fiche avec des informations spécifiques à votre groupe de binôme auprès de votre chargé de TP.

Des outils, oui, mais pour quoi faire ?

L'informatique et les réseaux sont des disciplines *artisanales*. Quand on programme, quand on conçoit et déploie des réseaux, on n'est en général pas dans un contexte industriel de masse mais dans un contexte particulier, qui nécessite un certain *savoir-faire*. De la même manière qu'un bon cuisinier possède des couteaux bien affutés, des casseroles, des faitouts… pour faire du réseau, il est nécessaire de connaître (bien) et de savoir manipuler (mieux) un certain nombre d'outils. En bref, d'avoir différentes options pour diagnostiquer, débuguer, reconfigurer, *comprendre* ce que l'on manipule.

Avant de commencer à s'intéresser aux *logiciels*, nous allons cependant commencer par un rappel autour de l'environnement *matériel* de l'ingénieur systèmes et réseaux.

1 Environnement Matériel

Le but de cette partie est de vous familiariser avec la salle de TP que vous avez déjà vu à la première séance, ainsi qu'avec le matériel à disposition.

1.1 Organisation générale physique des salles

Deux salles de TP sont utilisées dans ce module, la b101 et la b109. Bien que leur organisation soit globalement commune, elles diffèrent les unes des autres par de petites variations, principalement physiques. Du point de vue logiciel, elles sont théoriquement identiques.

1.1.1 Postes

Les postes de chaque salle utilisent la distribution Linux Ubuntu 22.04. Au démarrage de la machine, une session s'ouvre automatiquement sans avoir besoin de rentrer de mot de passe, sous l'utilisateur virtuser. Vous n'êtes pas *root* (super-utilisateur) sur ces machines, mais vous n'avez pas besoin de l'être car la majorité de vos TPs se passeront dans des machines virtuelles « hébergées » par ces machines, machines dans lesquelles vous pourrez être *root*. Majoritairement, les machines virtuelles utiliseront la distribution Linux Ubuntu ou le système d'exploitation Windows.
L'utilisation de ces machines virtuelles permet de personnaliser l'environnement pour chaque TP, par exemple en proposant certains outils spécifiques, sans avoir besoin de reconfigurer les machines hôtes.

1.1.2 Câblage et réseau

Chaque poste possède deux cartes réseaux physiques, l'une intégrée à sa carte mère et l'autre ajoutée en sus, toutes deux connectées par bus PCI.

Information : Sous les systèmes d'exploitation basés sur Linux, il est possible d'utiliser respectivement les programmes `lspci`, `lsusb` et `lshw` pour lister les composants matériels sur le bus PCI, le bus USB, ou plus généralement obtenir les caractéristiques de l'ensemble des composants connectés à l'ordinateur. On peut par exemple utiliser `lshw -C network` pour se limiter aux cartes réseaux.

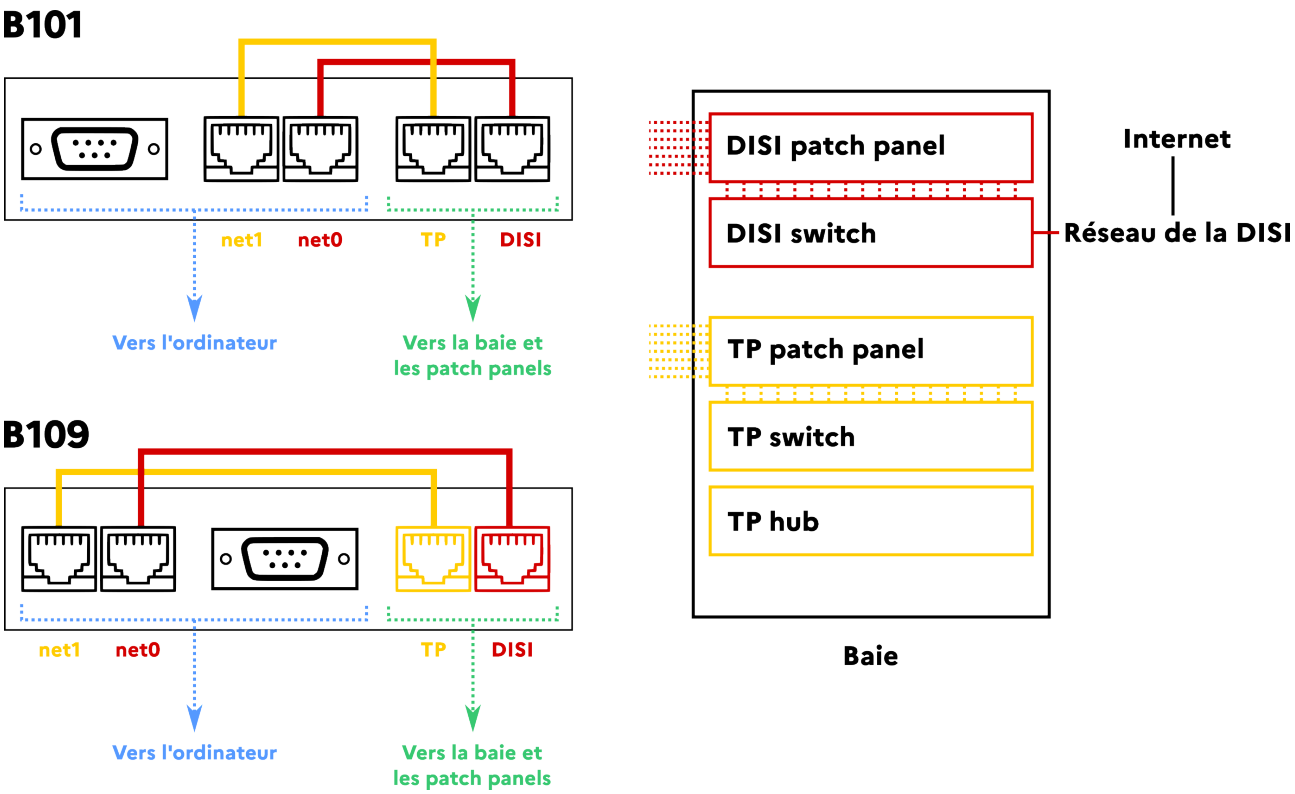


FIGURE 1 – Zoom sur le câblage des *patch panels* de bureau de la B101 et de la B109. Dans cette image, le réseau les câbles sont connectés au switch TP, mais on peut aussi décider de les relier au hub TP.

Pour chaque machine, chacune de ces cartes réseaux est connectée, par le biais de « *patch panel* » disponibles sur chaque bureau, à l'un des deux segment réseaux utilisé dans les salles : le segment réseau « DISI », sur lequel les machines sont connectées à un switch géré par la DISI, et sur lequel un routeur permet un accès à Internet (configuration automatique par DHCP), et un segment réseau « TP », commun aux deux salles, sur lequel les machines sont connectées à un hub. Un accès au port série de l'ordinateur peut également se faire via le *patch panel*, évitant de manipuler les unités centrales. Les configurations et branchements dans les salles B101 et B109 sont décrites par la figure 1.

Important : Il est important de rebrancher les câbles dans cette configuration à la fin des TPs, pour éviter aux suivants (e.g. potentiellement vous) de se retrouver face à une configuration inconnue. En cas de doutes, demandez nous !

Le nom de l'interface intégrée à la carte mère est nommée `net0`, et le nom de l'interface additionnelle est nommée `net1`.

1.2 Système d'exploitation hôte et Virtualbox

Dans le cadre des TPs, nous utiliserons principalement des machines virtuelles et des logiciels dans ces machines virtuelles. Ces machines virtuelles peuvent accéder aux périphériques de la machine hôte de différentes manières. On détaille ici les configurations les plus utilisées :

- **Cartes réseaux** : les cartes réseaux *virtuelles* de la machine *virtuelle* sont en général « bridgées » (ou « pontées ») avec les interfaces physiques de la machine hôte. Il s'agit de faire comme si un *switch* était présent en amont de l'interface physique, *switch* connecté à l'interface physique et à l'interface virtuelle. Du point de vue de l'extérieur (par exemple, du point de vue de la DISI), deux cartes réseaux sont visibles, notamment avec deux adresses MAC et deux adresses IP différentes.
- **Port série** : Le port série peut être utilisé au choix par l'hôte, au choix par une **unique** machine virtuelle. Attention : plusieurs machines virtuelles peuvent *techniquement* écrire dans le même port série, résultant alors en l'écriture de données incorrectes sur le port série. **Il faut bien faire attention à n'utiliser le port série que depuis une unique machine virtuelle ou uniquement depuis l'hôte**.

Pour accéder à la configuration d'une machine virtuelle, il suffit de sélectionner la machine virtuelle dans la fenêtre de VirtualBox et d'appuyer sur le bouton `Settings`.

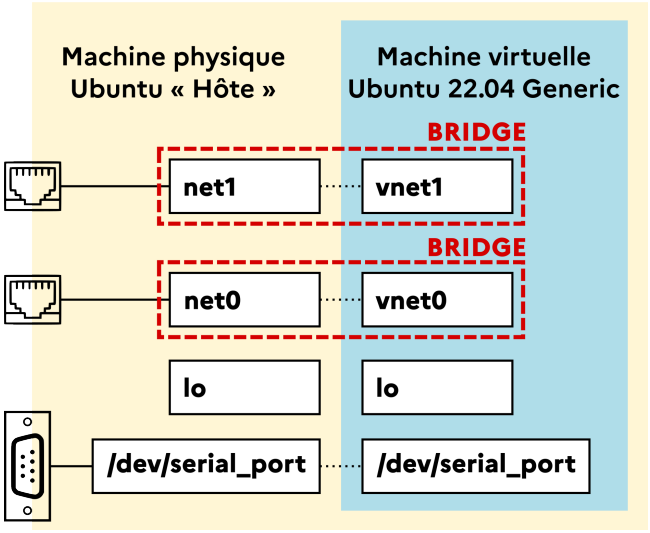


FIGURE 2 – Schéma logique de la machine virtuelle Ubuntu 22.04 Generic. Par défaut, la machine virtuelle possède deux interfaces ethernet, `vnet0` et `vnet1`, qui sont respectivement bridgées avec les interfaces ethernets de la machine hôte `net0` et `net1`, c'est-à-dire l'interface *généralement* connectée au segment réseau DISI et l'interface *généralement* connectée au segment réseau TP. Dans cette configuration, la machine virtuelle peut récupérer une adresse IP qui lui est propre en utilisant le protocole DHCP comme si elle était directement connectée au segment réseau DISI, via son interface net0. Le port série de l'hôte, `/dev/serial_port`, est exposé dans la machine virtuelle au chemin `/dev/serial_port`.

Information : La configuration des bridges de VirtualBox n'est pas visible dans les outils classiquement utilisés pour configurer les bridges sous Linux. En effet, VirtualBox utilise son propre module noyau pour implémenter son propre système de bridge, et il n'est donc pas possible de configurer le bridging entre machine virtuelle et hôte en utilisant par exemple le programme `ip` ou le programme `bridge`.

Question 1 : Lancez la machine virtuelle nommée "Ubuntu-22-04-Generic" et vérifiez qu'elle est fonctionnelle. Vérifiez qu'elle est notamment connectée à Internet en lançant un navigateur Web et en allant observer votre adresse IP telle que perçue par le site Web `https://monip.org/`. Comparez avec l'adresse IP obtenue en répétant la procédure sur la machine hôte. Que peut-on en déduire quant à la configuration réseau de cette machine ?

1.3 Équipements Cisco Catalyst 9200L (switchs) et Cisco ISR 4331 (routeurs)

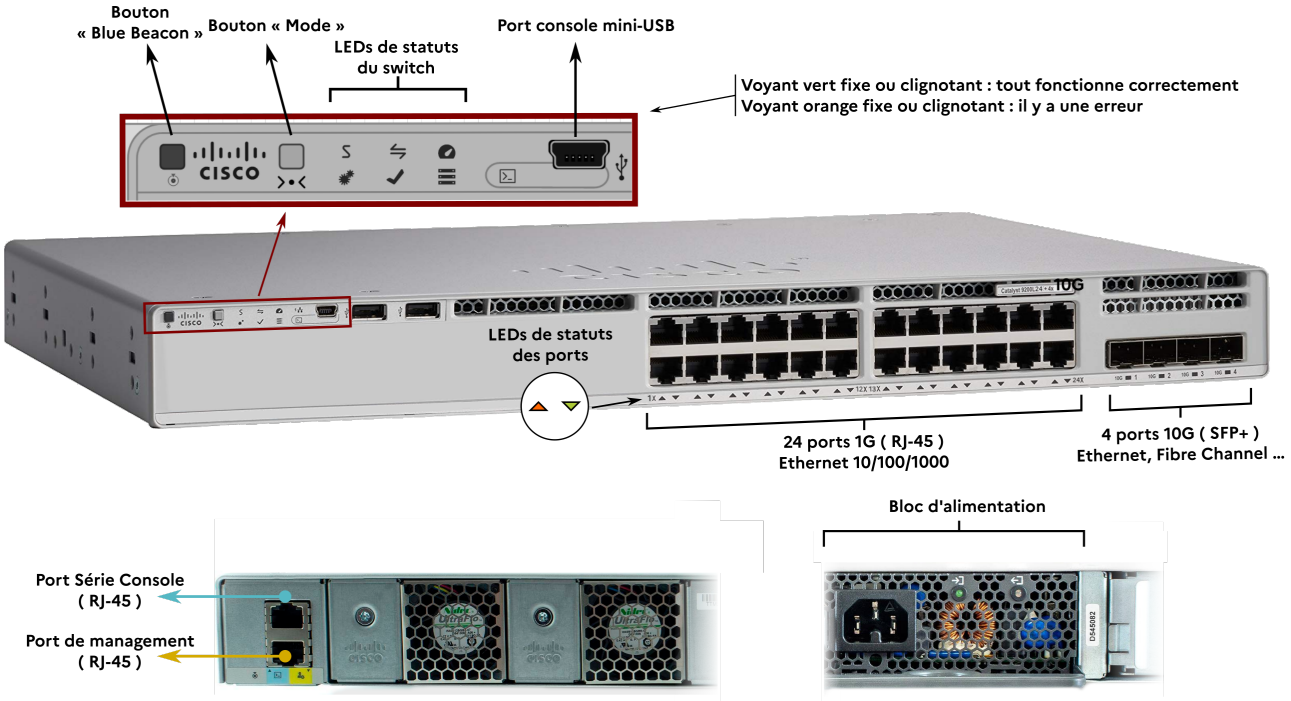


FIGURE 3 – Cisco Catalyst 9200L, l'un des switchs utilisés dans ce module

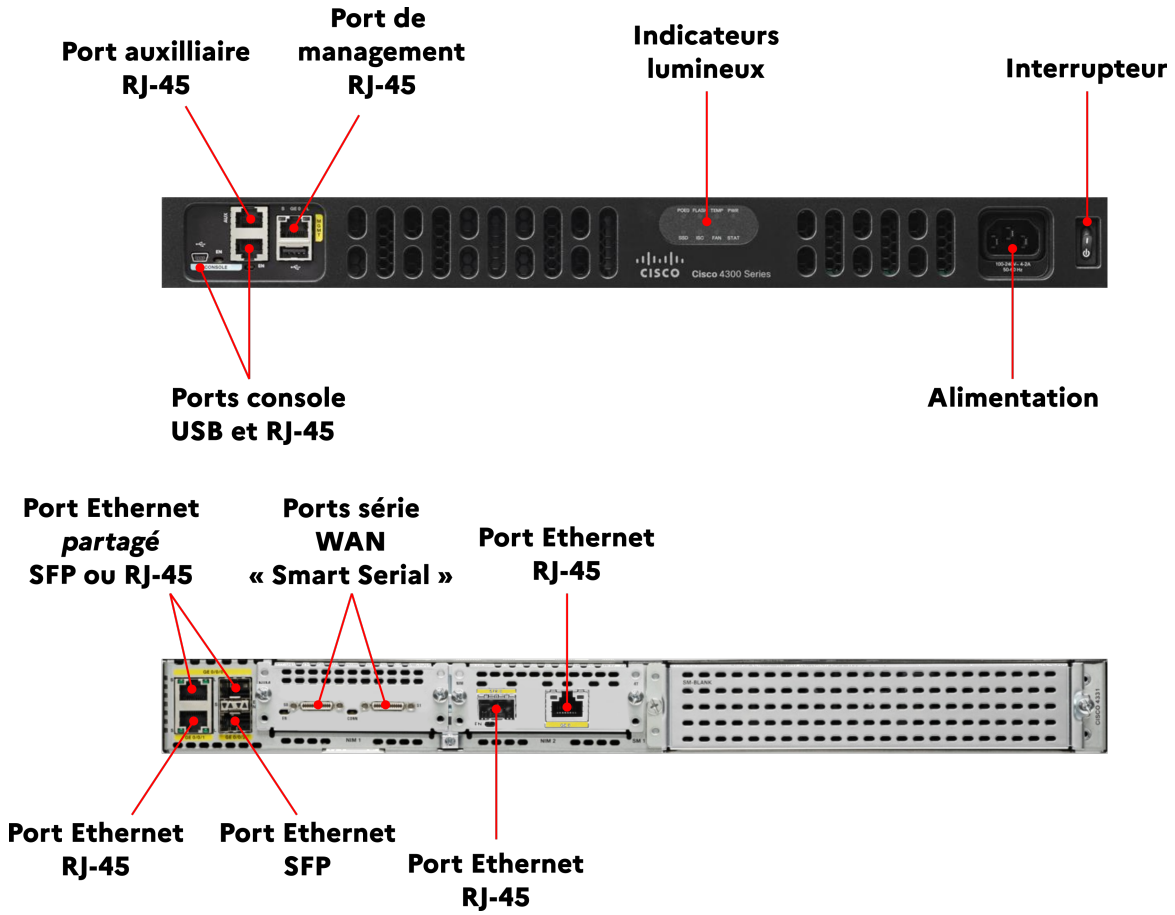


FIGURE 4 – Cisco ISR 4331, l'un des routeurs utilisés dans ce module

Attention : Lors de leur démarrage, les routeurs Cisco ISR 4331 font tourner leur ventilateur à la vitesse maximale pendant environ 7 minutes, ce qui a tendance à faire *beaucoup* de bruit. Il convient d'éviter de les redémarrer trop souvent pour le confort auditif de l'ensemble de la salle.

Question 2 : Vérifiez que votre routeur ISR 4331 est bien allumé et connecté sur son port console à votre machine. Utilisez le programme `minicom` (en terminal) pour vous connecter au routeur ISR 4331 par le biais de ce port console, ou le programme `Putty`, de manière graphique. Attention, effectuez bien cette manœuvre que dans la VM !
Pour vérifier que tout fonctionne bien, appuyez simplement sur la touche Entrée plusieurs fois, pour vérifier si une nouvelle ligne vous est proposée dans le shell Cisco.

Note : Pour les équipements Cisco, la configuration du port console est en général 9600-8-N-1 : 9600 bits par seconde, 8 bits de données (8) , pas de bit de parité (N), et 1 bit stop (1). Cette configuration est pré-enregistrée dans Putty et Minicom, mais d'autres équipements peuvent utiliser d'autres paramètres.

2 Outils logiciels

2.1 Linux

Note : Dans toutes cette section, les opérations se feront depuis la VM Ubuntu-22-04-Generic. Votre utilisateur `utilisateur` est sudoers et son mot de passe est `motdepasse`.

Sous Linux, quelques commandes permettent d'interagir avec le système pour gérer et configurer le réseau. Certains programmes prennent cependant la main sur la configuration du réseau, auquel cas utiliser ces commandes pour modifier la configuration n'aura probablement pas l'effet escompté. En effet, le programme, fonctionnant très souvent sous la forme d'un démon logiciel, écrasera votre configuration manuelle ou interférera avec vos actions. Parmi ces programmes, on peut noter un programme bien connu : **NetworkManager**. NetworkManager est utilisé notamment sous Ubuntu, il permet de gérer et de configurer les connexions filaires et sans fils en utilisant une interface graphique (mais il fonctionne aussi en ligne de commande).

Important : Il convient donc de s'assurer que les interfaces que l'on configure « manuellement » ne sont pas déjà configurées automatiquement par des programmes comme NetworkManager, pour éviter de se faire marcher dessus par ces *démons logiciels*.

Information : Par défaut, sur la **VM Ubuntu-22.04-Generic**, NetworkManager est configuré pour utiliser `DHCP` sur l'interface `vnet0`, et ne configure pas l'interface `vnet1`. Pour empêcher NetworkManager de configurer ces interfaces, il suffit, en utilisant l'interface graphique de NetworkManager accessible dans votre barre d'état (en haut à droite dans la VM), de supprimer ces connexions.

Connaître la configuration réseau

Question 3 : Dans un terminal, lancez les commandes `ip address`, `ip link`, `ip neighbour`, `ip route`. En se basant sur le nom des sous-commandes, de la sortie de ces commandes, et éventuellement du manuel, à quoi servent chacune de ces sous-commandes ?

Question 4 : Avec quelle(s) commande(s) mentionnée à la question précédente, et sur quelle(s) machine(s) est-il possible de retrouver les adresses visibles dans la question 1 ?

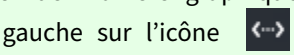
Question 5 : À quoi correspondent les options `-4` et `-6` du programme `ip` lorsques utilisées avec les sous-commandes `neighbor`, `route`, ou `address`, e.g. `ip -6 <sous-commande>` ?

Une partie de la configuration réseau de votre machine est contenue dans les fichiers suivants :
- `/etc/resolv.conf` : il s'agit des serveurs DNS utilisés par la majorité des applications du système. On peut y lire des lignes du type `nameserver <ADRESSE IP>` où `<ADRESSE IP>` est l'adresse IP du serveur DNS utilisé ;
- `/etc/hostname` : il s'agit du nom d'hôte de la machine ;
- `/etc/hosts` : il s'agit d'une liste de noms d'hôtes qui sont « résolus » statiquement, sans passer par des requêtes DNS.

Information : Pour afficher des fichiers en ligne de commande sous linux, on utilise le programme `cat`, par exemple `cat /etc/foo/bar`.

Modifier la configuration réseau

Pour modifier la configuration d'une machine sous Linux, plusieurs options s'offrent à nous :
- On pourra modifier certains paramètres en éditant les fichiers de configurations manuellement, par exemple `/etc/hostname`, `/etc/resolv.conf` ou encore `/etc/NetworkManager/NetworkManager.conf`.
- On pourra utiliser des programmes graphiques ou en ligne de commande pour faire ces modifications de manière *programmatique* :
  1. Si l'interface est gérée par NetworkManager, on pourra utiliser `nmcli` en ligne de commande, ou l'interface graphique de NetworkManager ;
  2. Si on a supprimé la gestion des interfaces par NetworkManager, on pourra utiliser le programme `ip`, qui permet de gérer les interfaces, les adresses, les routes, et d'en modifier la configuration (en plus de la consulter, comme vu précédemment). **C'est cette option qui sera privilégiée dans ce TP.**

Information : Pour modifier de manière graphique les connexions sur la VM *Ubuntu-22.04-Generic*, il suffit d'effectuer un clic gauche sur l'icône  (en haut à droite, dans la barre d'outils), puis `Modifiez les connexions`, puis double-cliquer sur `Connexion filaire 1` (interface `vnet0`) ou `Connexion filaire 2` (interface `vnet1`) pour éditer ses paramètres.

Question 6 : Dans la VM, utilisez `sudo ip link set down <INTERFACE>` pour placer l'interface `vnet0` (virtuelle) bridgée avec l'interface (physique) `net0` dans son état `down`. Vérifiez que le changement a bien été pris en compte en utilisant la commande `ip link`.

Pour réactiver l'interface, il suffit de remplacer `down` par `up` (mais ce n'est pas nécessaire à cette étape du TP)

Information : La syntaxe pour modifier des paramètres réseaux avec `ip` peut sembler compliquée au premier abord. N'hésitez pas à utiliser le manuel (commande `man`) pour consulter des exemples sur l'utilisation d'`ip` ! Par exemple, on pourra utiliser `man ip`, `man ip link`, `man ip route` ou `man ip address`, puis chercher la section `EXAMPLES` (située à la fin de la page de manuel) en tapant `/EXAMPLES` pour se déplacer directement vers la section.

Question 7 :

1. Lancez la commande `ip -4 route` et observez les routes actuellement installées sur votre machine.
2. Ajoutez ensuite l'adresse IPv4 (telle que mentionnée sur votre fiche) à l'interface virtuelle `vnet1` en utilisant la commande `sudo ip address add <ADRESSE>/<MASQUE> dev <INTERFACE>`.

   ⚠ Pour éviter les collisions, merci d'utiliser l'adresse mentionnée sur la fiche que vous avez reçu au démarrage du TP ⚠

   Si vous avez fait une erreur sur l'adresse et que celle ci a été ajoutée à l'interface, ré-utilisez la commande précédente et remplacez `add` par `del` pour supprimer l'adresse de l'interface
3. Ré-itérez la commande `ip -4 route`. Qu'observez vous ?
4. Vérifiez que la machine possédant l'adresse IP `10.13.37.254` répond bien aux pings, avec la commande `ping 10.13.37.254`, puis chargez la page web `http://10.13.37.254/`, et notez le *flag* affiché sur votre fiche de réponse.

Question 8 : Arrivez vous à ping l'adresse `88.99.105.147` depuis votre VM ? Est-ce logique ?

Question 9 : Sur le réseau `10.13.37.0/24`, un routeur connecté à Internet est disponible à l'adresse `10.13.37.254`. Ajoutez une route par défaut en utilisant l'adresse de ce routeur avec la commande `sudo ip route add default via 10.13.37.254`.
Pour modifier les DNS utilisés par votre VM, éditez le fichier `/etc/resolv.conf` avec un éditeur de texte (e.g. `sudo gedit /etc/resolv.conf`) et faites faites-y figurer la ligne `nameserver 157.159.10.28`, en haut du fichier.)
Utilisez ensuite un navigateur web (ou le programme `curl`) pour vérifiez avec quelle IP vous sortez sur Internet, toujours en utilisant le service web `https://monip.org`. Notez cette IP sur votre fiche de réponse.

Question 10 : Arrivez vous désormais à ping l'adresse `88.99.105.147` depuis votre VM ? Est-ce logique ? Utilisez `traceroute 88.99.105.147` pour observer le chemin pris par les paquets.

2.2 Cisco

Note : Dans toutes cette section, on suppose que l'on est connecté par le port série aux équipements CISCO. Cette connexion peut se faire depuis l'hôte, depuis une VM Ubuntu, ou depuis une VM Windows.

La CLI Cisco n'est pas la CLI Linux ou la CLI Windows. Ainsi, son fonctionnement est différent, et on n'aura a priori pas accès aux utilitaires que l'on a l'habitude d'utiliser sur ces systèmes, même si *sous le capot*, Cisco IOS XE (utilisé par les ISR, mais pas par les switchs) utilise Linux…

La CLI Cisco se caractérise par plusieurs niveaux de privilèges dont un résumé est disponible sur la figure 1.

À tout instant, dans la CLI Cisco, il est possible d'utiliser le point d'interrogation « `?` » pour lister les commandes disponibles dans le terminal. Pour naviguer dans la sortie d'une commande Cisco, on peut utiliser les flèches directionnelles ou la barre espace pour faire défiler plus rapidement les commandes.

Nom du mode	État de la CLI	Utilisation
User exec	Router> Switch>	Mode dans lequel on se connecte généralement aux équipments. Permet d'exécuter des commandes de base de type `ping`. Utiliser `logout` pour se déconnecter.
Privileged exec	Router# Switch#	Pour passer dans ce mode, utiliser `enable` depuis le mode *user exec*. Pour le quitter, utiliser `disable`. Permet d'afficher la configuration de l'équipement avec e.g. `show running-config`, de redémarrer la machine, de débuguer…
Global configuration	Router#(config) Switch#(config)	Pour passer dans ce mode, utiliser `configure terminal` depuis le mode *privileged exec*. Pour le quitter, utiliser `exit` ou `<Ctrl>+z`. Permet d'éditer la configuration de l'équipement, de ses interfaces…

TABLE 1 – Vue d'ensemble des différents modes de la ligne de commande Cisco

Exemple de passage d'un niveau de privilège à l'autre

```
Router>
Router>?
Exec commands:
  access-profile   Apply user-profile to interface
  app-hosting      Application hosting
  [. . .]
Router>enable
Router#
Router#?
Exec commands:
  access-profile   Apply user-profile to interface
  access-session   Access-session options for eEdge                                  Cette commande
  ↪  n'était pas disponible en mode user exec !
  app-hosting      Application hosting
  [. . .]
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#exit
```

Note : Sauf mention contraire, les mots de passes utilisés pour « protéger » l'accès au mode privileged exec ou au terminal virtuel est toujours `int`.

Connaître la configuration réseau

Pour connaître la configuration d'un équipement cisco (notamment un routeur), on utilise la commande `show` qui permet de consulter l'état courant de cet équipement.

Question 11 : À partir de quel niveau de privilège la commande `show running-config` est elle disponible ? À quoi sert cette commande ?

Question 12 : Quel est l'uptime et le numéro de version de votre routeur ? Indice : `show v?`.

Question 13 : À quoi sert la commande `show ip interface brief` ? Quel est son principal intérêt par rapport à la commande `show interfaces` ?

Modifier la configuration réseau

Pour modifier la configuration d'un équipement Cisco, il est nécessaire d'avoir recours au terminal de configuration (mode « Global configuration »). La syntaxe à utiliser dans ce terminal est la même que celle visible dans la sortie de `show running-config`. Par exemple, on peut voir dans la sortie de `show running-config` une ligne du type `hostname routeur-XX`. Dans le terminal de configuration, il suffira donc de taper la commande `hostname routeur-YY` pour changer ce nom de machine vers `routeur-YY`.

Information : Les commandes Cisco peuvent être abrégées lorsqu'il n'y a pas d'ambiguïté sur ce qu'elles désignent. Par exemple, au lieu de taper `configure terminal`, on pourra taper `conf t` car il n'existe pas d'autre commande que `configure` commençant par `conf`, et il n'existe pas d'autre sous-commande que `terminal` commençant par `t`.

Certaines options de configurations, par exemple celles liées aux interfaces, possèdent des sous-options de configuration, qui sont visible dans la sortie de `show run` car elles présentent une indentation :

Exemple d'option de configuration avec sous-configuration

```
!
interface GigabitEthernetX/Y/Z
 no ip address
 shutdown
 negotiation auto
!
```

Pour modifier les sous-options de configuration, il faut utiliser le nom de l'option principale, par exemple `interface GigabitEthernetX/Y/Z`, qui va permettre d'entrer un terminal de configuration spécifique à cette option, à la manière de la commande `conf term` (mode `interface configuration`) :

```
routeur-ABCD(config)#interface GigabitEthernetX/Y/Z
routeur-ABCD(config-if)#!On configure de la manière souhaitée. . .
routeur-ABCD(config-if)#exit
routeur-ABCD(config)#
```

Dans la sortie de `show running-config`, on peut voir certaines lignes préfixées du mot-clef `no`, par exemple `no ip http server`. Ce préfixe sert à désactiver la fonctionnalité, par exemple ici la présence d'un serveur web de configuration hébergé sur le routeur. Pour réactiver l'option, il suffit de taper `ip http server` (sans le `no`).

Question 14 : Débranchez votre ordinateur du segment réseau TP, et branchez là sur un switch Catalyst 9200L lui même branché sur le segment réseau TP. Par défaut, le switch Catalyst 9200L devrait être dans un mode d'opération de « switching » simple, et il ne devrait pas y avoir de configuration du switch à effectuer. Vérifiez que vous arrivez toujours à pinguer l'adresse `10.13.37.254`.

Question 15 : Activez ensuite l'une des interfaces Ethernet de votre routeur, puis configurez l'adresse IP de votre fiche sur cette interface. Pour configurer l'adresse IP, utilisez, en mode configuration d'interface, la commande `ip address` (utilisez le `?` pour la suite). Vous brancherez ensuite cette interface sur le switch, permettant ainsi et à votre routeur, et à votre machine d'être connectée au même segment réseau « TP ». Lorsque c'est fait, pinguez l'adresse de votre routeur depuis votre VM (ou l'adresse de votre VM depuis votre routeur) pour vérifier que tout est bien configuré.

Question 16 : Connectez une interface de votre routeur au segment réseau DISI, configurez cette interface en dhcp client (`ip address dhcp` en mode de configuration d'interface), et vérifiez que vous récupérez bien une IP sur le réseau de la DISI. Tentez ensuite de pinguer une adresse bien connue.

SSH : Se connecter à une machine ou un équipement distant

SSH est un logiciel (et un protocole) permettant de se connecter à des machines distantes de manière sécurisée.

Question 17 : Depuis la VM Ubuntu-22-04-Generic, connectez vous à votre routeur en utilisant le protocole réseau `ssh`. Cette connexion peut se faire avec la commande suivante : `ssh <UTILISATEUR>@<ADRESSE IP ou NOM D'HÔTE>`. Le nom d'utilisateur est `thd` et le mot de passe est `mdp`.

Question 18 : Vérifiez que votre invite de commande sur le routeur, exposée par la connexion SSH, fonctionne de la même manière que par la connexion série (`enable`, ...). Relancez la commande `show running-config`. Que remarquez vous sur la vitesse d'affichage de la sortie ?

Information : Savoir accéder à une machine « distante » est important, que ce soit pour l'utilisation des ressources de cette machine, pour le diagnostic de problèmes réseaux, ou tout simplement pour expérimenter l'envoi et la réception de données à travers Internet. SSH est la méthode préférentielle pour l'administration des équipements réseaux : la connexion console / série ne devrait être qu'une solution de secours / de configuration initiale !

Tshark et Wireshark : observer et analyser le trafic réseau

Les outils Wireshark (graphique) et Tshark (en CLI) permettent d'observer et d'analyser le trafic réseau passant sur les interfaces résaux de la machine sur laquelle ils sont exécutés.

Pour pouvoir capturer ce trafic, il est nécessaire d'avoir des droits super-utilisateurs : on imagine très bien quels problèmes de confidentialité pourraient se présenter si l'on laissait n'importe quel utilisateur capturer le trafic des autres utilisateurs de la machine. En général, sous Linux, ces droits super-utilisateurs peuvent être obtenus en utilisant les commandes `su` (**s**witch **u**ser), qui demande le mot de passe de l'utilisateur que l'on souhaite utiliser, ou `sudo` (**s**witch **u**ser and **do**), qui demande le mot de passe de l'utilisateur actuel.

Une autre manière de permettre la capture est d'attribuer une fois pour toute le bit SUID au binaire utilisé (tcpdump, tshark, ...) ce qui permettra à n'importe quel utilisateur, même non super-utilisateur.

Question 19 : Dans votre VM, lancez Wireshark et familiarisez vous avec son interface. Celle-ci est aussi représentée sur la figure 5.

Question 20 : Lancez une capture sur l'ensemble des interfaces connues de Wireshark : sélectionnez `any` dans le panneau de sélection de l'interface (partie jaune sur la figure 5, puis lancez la capture en appuyant sur le bouton  :

Lancez ensuite les commandes suivantes sur votre VM :

- `wget -4 http://telecom-sudparis.eu/`
- `wget -6 http://telecom-sudparis.eu/`
- `dig telecom-sudparis.eu`
- `dig telecom-sudparis.eu @8.8.8.8`

Connectez vous sur votre routeur en ssh et lancez quelques commandes (tout en gardant la capture active).

Stoppez ensuite cette capture en appuyant sur  .

Information : Pour changer d'interface quand on vient de stopper une capture, il suffit de cliquer sur l'icône  et de sélectionner la nouvelle interface.

Question 21 : Dans cette capture, quel(s) protocole(s) observez vous ? On pourra utiliser le menu `Statistiques > Hiérarchie des protocoles` pour obtenir cette information.

Question 22 : Quelles adresses IPv4 sont visibles dans la capture ? On pourra utiliser `Statistiques > IPv4 Statistics`. Prenez une adresse au hasard, et utilisez la commande `whois <ADRESSE-IP>` pour obtenir plus d'informations à son propos. Quel organisme possède cette adresse IP ?

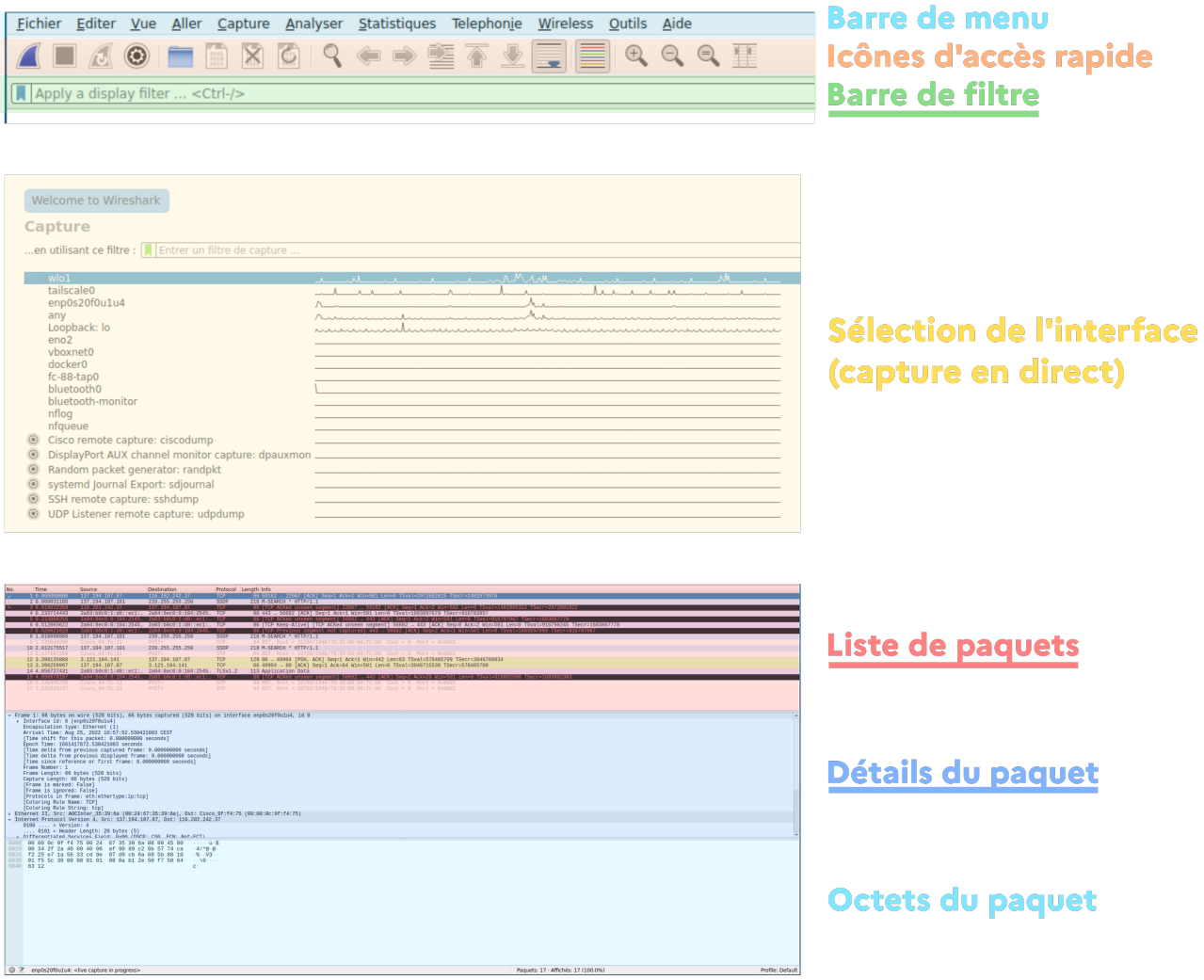


FIGURE 5 – Vue d'ensemble de l'interface graphique de Wireshark. Les parties soulignées sont les plus importantes. Au lancement de wireshark (appelé sans arguments), il est possible de sélectionner une interface pour effectuer une capture locale « en direct ». Il est aussi possible d'ouvrir un fichier de capture (de type `.pcap` ou `.pcapng`) pour une analyse « hors-ligne »

Question 23 : Dans la capture, beaucoup de paquets sont des paquets du protocole SSH car c'est celui que vous avez utilisé pour vous connecter à la machine distante. Tapez le filtre `not ssh` dans la barre de filtre. Qu'observez vous ?

Testez ensuite les filtres suivants :

- `tcp.dstport == 80`
- `tcp.srcport == 80`
- `http`
- `udp.port == 53`

Question 24 : Relancez une capture live sur l'interface `vnet1`, puis utilisez le filtre `arp.dst.proto_ipv4 == 1.2.3.4`. Toutes les 20 secondes environ, vous devriez voir un nouveau paquet de type arp. Ouvrez les détails de l'un des paquets, et notez la valeur du champ `Sender MAC Address`, qui fait partie de la trame, sur votre fiche de réponse.

Attention : Wireshark capture le trafic au niveau de l'interface réseau, avant même que le pare-feu de la machine n'entre en jeu. Ainsi, si un pare-feu logiciel (comme nftables) bloque le trafic sur une machine, il est tout de même possible d'observer le trafic arriver sur l'interface avec ces outils.

2.3 Windows

Le système d'exploitation Windows est bien moins intéressant pour l'ingénieur et l'ingénieur réseau que les systèmes d'exploitation Linux, BSD, ou même OSX. En effet, la majorité des serveurs liés à Internet (Web, DNS, …) fonctionnent sous Linux, la totalité des super-calculateurs fonctionnent sous Linux, les équipements réseaux fonctionnent presque tous sur des systèmes d'exploitation basés sur Linux, Android est basé sur Linux…

Cependant, Windows est très largement utilisé sur les postes utilisateurs dans certains champs d'application (santé, bureautique, …), et l'administration de ces postes va souvent de pair avec l'utilisation de serveurs sous Windows. Il est donc important de se familiariser avec l'environnement Windows, ce que l'on va donc faire dans cette partie.

Note : Dans toutes cette section, les opérations se feront depuis la VM Windows10Generic. Dans sa configuration initiale, cette VM ne possède qu'une seule interface (virtuelle) bridgée avec l'interface physique `net1` (qui est classiquement reliée au segment réseau TP).

Connaître et modifier la configuration réseau

Outre les applications graphiques de Windows comme le « Centre Réseau et Partage » permettant d'afficher la configuration réseau sous Windows, l'invite de commande Windows est intéressante car elle permet de centraliser l'ensemble des informations liées à la configuration réseau de Windows.

Question 25 : Ouvrez un invite de commande PowerShell (en cherchant Powershell dans la barre de menu Windows, et en le lançant **en administrateur** en cliquant droit dessus, `Lancer comme administrateur`). Il est aussi possible d'utiliser l'invite de commande `cmd`, de même, en mode administrateur. Testez les commandes `ipconfig /all`, `winver`, `arp -a`. À quoi servent ces commandes ? De même pour la commande `netsh interface ipv4 show config`

Interface Graphique Pour accéder à la configuration IP de votre carte ethernet virtuelle sous Windows, il est nécessaire d'effectuer un clic droit sur le bouton  de la barre de tâche Windows (en bas à droite).

Il faut ensuite cliquer sur `Ouvrir les paramètres réseau et Internet`, puis `Centre Réseau et partage` et enfin `Modifier les paramètres de la carte`, puis `Protocole Internet Version 4 (TCP/IPv4)` et cliquer sur `Propriétés`.

Par défaut, l'interface est configurée pour « obtenir une adresse IP automatiquement » et « obtenir les adresses des serveurs DNS automatiquement », c'est-à-dire en utilisant DHCP.

Console Pour modifier la configuration IP de l'interface nommée `<INTERFACE>` dans la sortie de la commande `netsh interface ipv4 show config`, il est possible d'utiliser en console la commande suivante :

```
C:\Users\user> netsh interface ipv4 set address name="<INTERFACE>" static <ADRESSE> <MASQUE> <PASSERELLE>
```

Pour repasser l'interface en configuration automatique via DHCP, il est possible de changer les arguments de la commande :

```
C:\Users\user> netsh interface ipv4 set address name="<INTERFACE>" source=dhcp
```

Question 26 : Configurez la VM pour utiliser la configuration IP mentionnée sur votre fiche, et configurez le serveur DNS pour pointer vers `157.159.10.28` (sans configuration de serveur dns auxiliaire). Vérifiez que vous avez bien accès à Internet.

Question 27 : Vérifiez que la machine possédant l'adresse IP `10.13.37.254` répond bien aux pings, avec la commande `ping 10.13.37.254`, puis chargez la page web http://10.13.37.254/ dans chrome, et notez le *flag* affiché sur votre fiche de réponse.

Question 28 : Utilisez la commande `tracert` pour afficher le chemin emprunté par les paquets pour atteindre l'adresse `8.8.8.8`.