Jean-Claude CABIANCA Pascal BERTIN

BAC STI2D

Les Réseaux : Infrastructure, Protocoles et services, Modèles en couches

Document 1 : Présentation de la formation
Document 2 : Présentation CISCO CCNA Exploration
Document 3 : Les activités pratiques
Document 4 : Présentation du Live-DVD(CD) basé sur Ubuntu
Document 5 : Logiciel de capture de trames Ethernet

STI2D : SIN (Systèmes d'Information et Numérique)

Partie 3 : Les Réseaux

Présentation de la formation

Formateurs responsables :

Pascal Bertin (Lycée Borda – Dax)
Jean-Claude CABIANCA (Lycée Gaston Crampe – Aire sur Adour)

1 – Introduction

Afin d'étudier les réseaux en **STI2D**, nous proposons d'utiliser les ressources fournies par l'entreprise **CISCO** qui propose des certifications sur les réseaux.

Le format des ressources proposé repose sur un support multimédia : fiches de cours, animations, exercices, quiz en fin de chapitre, simulations. La plate-forme d'e-learning est accessible depuis une académie locale ou régionale CISCO, après inscription du stagiaire dans l'académie.

D'autre part, afin de pouvoir réaliser les **activités pratiques** associées à cette formation, nous proposons d'utiliser une salle d'ordinateurs standards sur lesquels fonctionnera une distribution **Linux** basée sur **Ubuntu 10.10** au travers d'un **Live CD** personnalisé.

Le **Live CD** contiendra tous les outils nécessaires pour l'étude des réseaux : les utilitaires standards (ipconfig, ping, traceroute, ipcalc, etc..) et un analyseur de trames **Wireshark**.

Une version **Live DVD** comportant les ressources **Cisco** «**CCNA Exploration Module 1**» et le simulateur de réseaux **Packet Tracer** sera aussi disponible.

2 – Les ressources

CISCO propose différentes certifications sur les réseaux. Notre formation s'appuiera sur la certification « **CCNA Exploration Module 1 : Notions de base sur les réseaux** ».

Pour pouvoir utiliser cette plateforme, il faudra disposer d'un compte chez **CISCO** (http://cisco.netacad.net), celui-ci sera attribué par les **académies locales** de Dax (Borda) ou d'Aire sur Adour (Gaston Crampe) par l'intermédiaire des formateurs. L'enseignant disposera des ressources mises en ligne et pourra passer s'il le désire la certification correspondante.

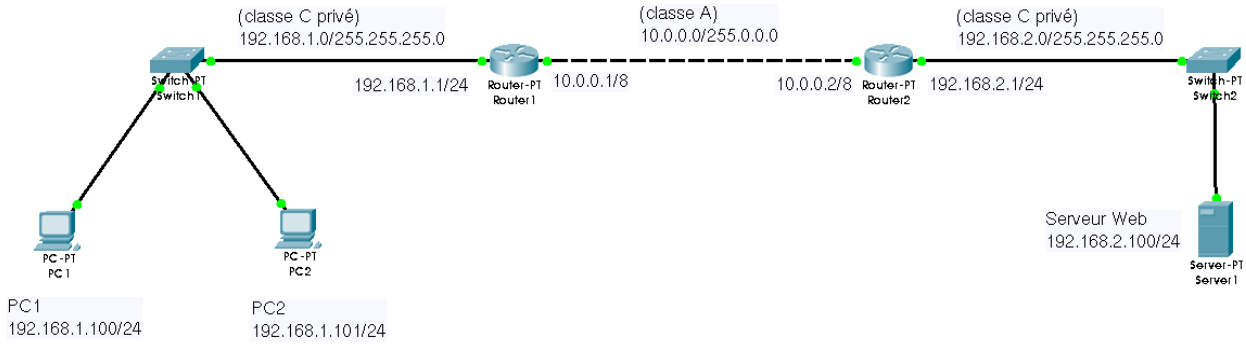
L'objectif de la formation n'est pas de passer cette certification qui demande au moins 40 Heures, mais il faudra que chaque stagiaire lise au moins les chapitres **2**, **3**, **5** et **9** afin de pouvoir réaliser les activités proposées.

3 – Les activités

Pour parcourir l'ensemble des activités pratiques, chaque centre de formation devra acquérir pour chaque pôle de formation, 2 routeurs **Linksys WRT54GL V1.1** et 1 adaptateur USB-Wifi **WUB54GC V3** (soit 10 routeurs et 5 adaptateurs USB-Wifi).

Les activités seront organisées par binôme, autour de l'infrastructure suivante :

A l'aide du matériel préconisé, nous nous limiterons au réseau WAN suivant :



4 – Déroulement de la formation

La formation sera organisée autour de la lecture des ressources **Cisco** (chapitres **2**, **3**, **5** et **9**) et de 4 activités pratiques (**TP1** à **TP4**) selon la chronologie suivante :

Activité 1 : Lecture et synthèse du chapitre **2** : «**Communication sur un réseau**».
Remarque : La lecture de ce chapitre est normalement réalisée avant de venir en formation.

Activité 2 : Réalisation des activités pratiques :
- **TP1** : Étude d'un réseau local (LAN)
- **TP2** : Configuration d'un réseau local (LAN)

Activité 3 : Lecture et synthèse du chapitre **3** : «**Fonctionnalité et protocoles des couches applicatives**».

Activité 4 : Réalisation de l'activité pratique **TP3** : Étude d'un réseau étendu (WAN**)**.

Activité 5 : Lecture et synthèse du chapitre **5** : «**Couche réseau OSI** ».

Activité 6 : Réalisation de l'activité pratique **TP4** : Étude d'un réseau WiFi (WLAN).

Activité 7 : Lecture et synthèse du chapitre **9** : «**Ethernet** ».

Activité 8 : Utilisation de **Packet Tracer** à l'aide du manuel de travaux pratiques **Cisco** :
- **1.7.1** : Présentation de Packet Tracer
- **2.7.1** : Analyse des paquets IP
- **3.5.1** : Configuration des hôtes et des services
- **4.6.1** : Analyse des couches application et transport
- **5.6.1 : R**outage des paquets IP

Activité 9 : Synthèse générale

CCNA EXPLORATION 1

PRESENTATION ET CONTENU

Notions de base sur les réseaux

Les cours de la Networking Academy sont conçus pour préparer les étudiants aux opportunités de carrière, à la formation continue et aux certifications reconnues au niveau mondial. Le programme, cohérent au niveau local, est délivré en ligne dans plusieurs langues et soutenu par un enseignement en classe et des travaux pratiques.

Le système robuste de données de Networking Academy traite près d'un million d'évaluations chaque mois. Les progrès, les résultats et les objectifs des étudiants sont mesurés continuellement et les offres du programme sont ajustées si nécessaires.

Ce cours présente l'architecture, la structure, les fonctionnalités, les composants et des modèles de réseaux Internet et autres réseaux informatiques. Il utilise les modèles en couches OSI et TCP pour examiner la nature et les rôles des protocoles et des services au niveau de l'application, du réseau, des liaisons de données et des couches physiques. Les principes et la structure de l'adressage IP, ainsi que les bases des concepts, supports et du fonctionnement Ethernet sont présentés. Ils constituent la base du cursus.

Les exercices Packet Tracer (PT) aident les participants à analyser le fonctionnement des protocoles et des réseaux et à développer des réseaux de petite taille dans un environnement simulé.
À l'issue du cours, les participants sont à même de construire des topologies de réseau local simples en appliquant les principes fondamentaux du câblage, d'effectuer des configurations de base sur les périphériques réseau tels que les routeurs et les commutateurs, et d'implémenter des systèmes d'adressage IP.

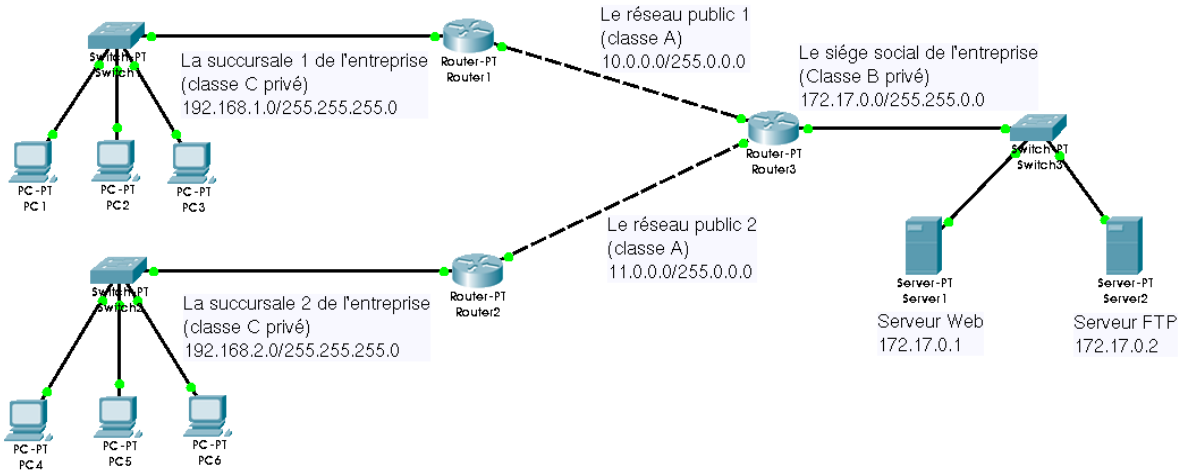
Connaissances requises : notions de base en informatique

STI2D - Tronc Commun (TC)
Groupe SIN (Systèmes d'Information et Numérique)

Les Réseaux : Etudes de cas / Travaux pratiques

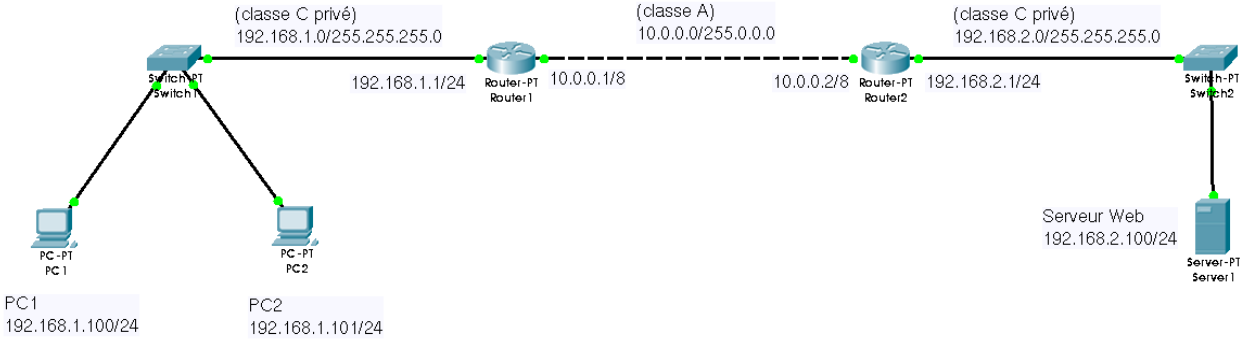
1 – Présentation

Dans cette série de TP, nous vous proposons une étude de cas. L'idée est de faire communiquer des réseaux locaux privés (LAN) distants, au travers de réseaux publics (WAN), selon l'exemple suivant :



Les réseaux publics pourront utiliser par exemple une liaison de type ADSL. Il faudrait rajouter au schéma ci-dessus des modems ADSL (ou modem/routeurs ADSL). Dans notre étude de cas, nous utiliserons une liaison de type Ethernet.

Pour des raisons pratiques, nous nous limiterons au réseau WAN suivant :



2- Organisation

- **TP1 :** Etude d'un réseau local (LAN) *(Ctrl-clic pour ouvrir le lien)*
  - installation / câblage du réseau LAN
  - analyse des configurations existantes des éléments du réseau
  - tests de communication

- **TP2 :** Configuration d'un réseau local (LAN)
  - paramétrage des adresses IP des clients
  - tests de communication

- **TP3 :** Étude d'un réseau étendu (WAN)
  - installation / câblage du réseau WAN
  - analyse des configurations et paramétrages des éléments du réseau
  - tests de communication
  - analyse de trames

- **TP4 :** Réseau WiFi (WLAN)
  - installation / configuration de clés réseau Wifi
  - tests de communication

Nous avons choisi le système Live DVD basé sur Ubuntu car ils nous permet de réaliser les TP sans configuration préalable des ordinateurs.

Une documentation vous est proposée : Présentation du Live DVD basé sur Ubuntu 10.10 LTS

TP1 : Étude d'un réseau local (LAN)

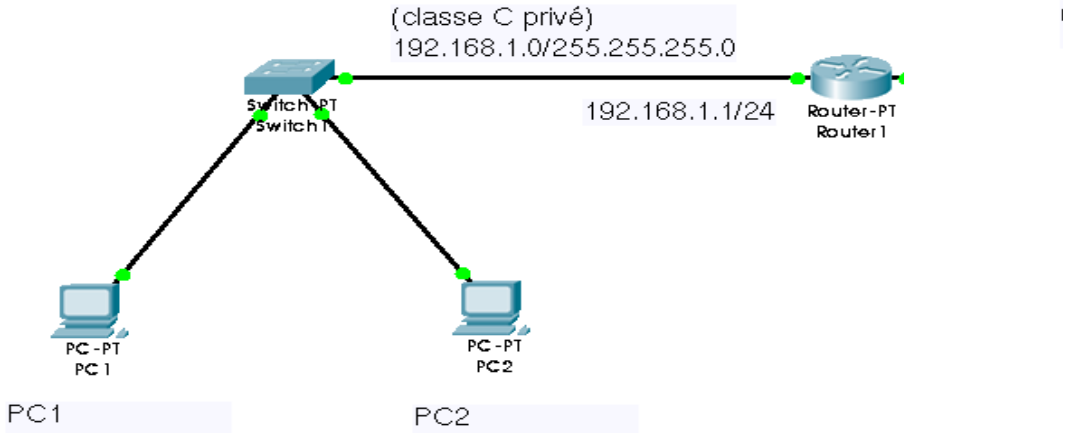
Objectifs :

- savoir câbler un réseau LAN
- reconnaître les fonctions remplies par les éléments d'un réseau
- relever et justifier la configuration des éléments d'un réseau
- tester la communication dans un réseau LAN et interpréter les résultats.

Matériel :

- 2 ordinateurs
- 1 routeur Lynksys WRT54GL
- 2 Live DVD basés sur Ubuntu (fournis par le formateur)
- câbles réseau

Schéma du réseau :



➔ Quelle est la fonction remplie par le routeur WRT54GL qui nous intéresse dans un réseau LAN ? *(voir éventuellement doc. Constructeur)*

➔ Réaliser le câblage de ce réseau.

➔ Faire démarrer *(booter)* les 2 ordinateurs sur les Live DVD Ubuntu. Configurer éventuellement le BIOS.

➔ A l'aide de la documentation Présentation du Live DVD basé sur Ubuntu 10.04 LTS *(page* 3 et 4*)*, relever et mettre dans le tableau suivant, les paramètres IP de chaque PC :

	PC1 (eth0)	PC2 (eth0)
Adresse MAC		
Adresse IP		
Masque de sous réseau		
Passerelle		

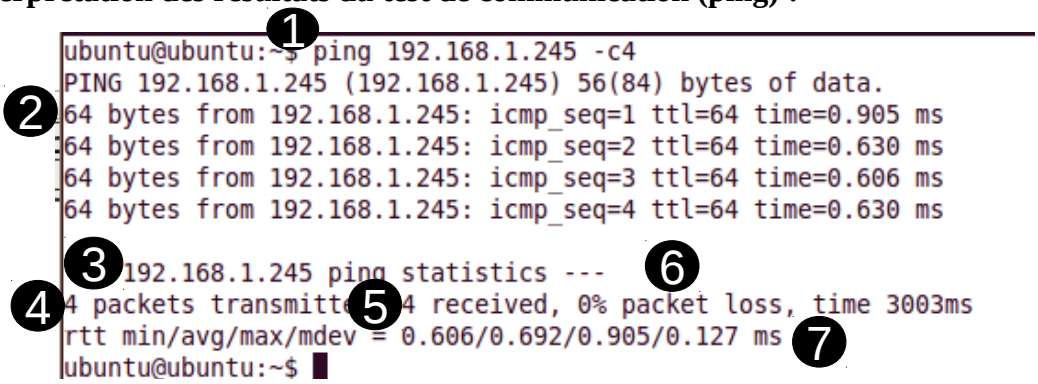
➔ Connaissant l'adresse IP de PC1, utiliser la commande ***ipcalc*** *(Cf. documentation page 7)* pour remplir le tableau suivant :

Note : pour lancer l'interface de commande en ligne (CLI), aller dans ***Application, Accessoires****, puis* ***Terminal***

Commande : *ipcalc @ip*	**PC1**
Adresse IP :	
Masque de sous réseau:	
Adresse du réseau :	
Adresse minimum d'un hôte :	
Adresse maximum d'un hôte :	
Adresse de broadcast :	
Nombre d'hôtes (2^8-2)	
Classe du réseau :	

➔ Utiliser la commande ***ping*** pour tester la communication entre PC1 et PC2, puis entre PC1 et le routeur 1, et enfin entre PC2 et le routeur 1.
2 possibilités :
- soit avec l'utilitaire **Système/Administration/Outils réseau**
- soit en ligne de commande , en tapant : ***ping @ip-destination -c4*** *(-c4 correspond à 4 paquets de données)*

Interprétation des résultats du test de communication (ping) :



➔ ***Champ 1*** : Adresse IP de l'ordinateur de destination
➔ ***Champ 2*** : Informations de réponse :
- octets : taille du paquet ICMP (64 octets, en général codes ASCII de l'alphabet)
- temps : délai écoulé entre la transmission et la réponse.

➔ ***Champ 3*** : Résumé des informations sur les réponses :
- TTL (Time To Live ou durée de vie) : valeur TTL par défaut du périphérique de DESTINATION, moins le nombre de routeurs dans le chemin. La valeur TTL maximale est **255**, mais pour les ordinateurs Windows plus récents, la valeur par défaut est **128**. La valeur TTL par défaut de Linux est réglée sur **64**.

➔ ***Champ 4*** : Paquets envoyés : nombre de paquets transmis. Par défaut 4.
➔ ***Champ 5*** : Paquets reçus : nombre de paquets reçus.
➔ ***Champ 6*** : Paquets perdus : différence entre le nombre de paquets envoyés et reçus.
➔ ***Champ 7*** : Informations sur le retard dans les réponses *(latence)*, mesurées en millisecondes.

TP2 : Configuration d'un réseau LAN

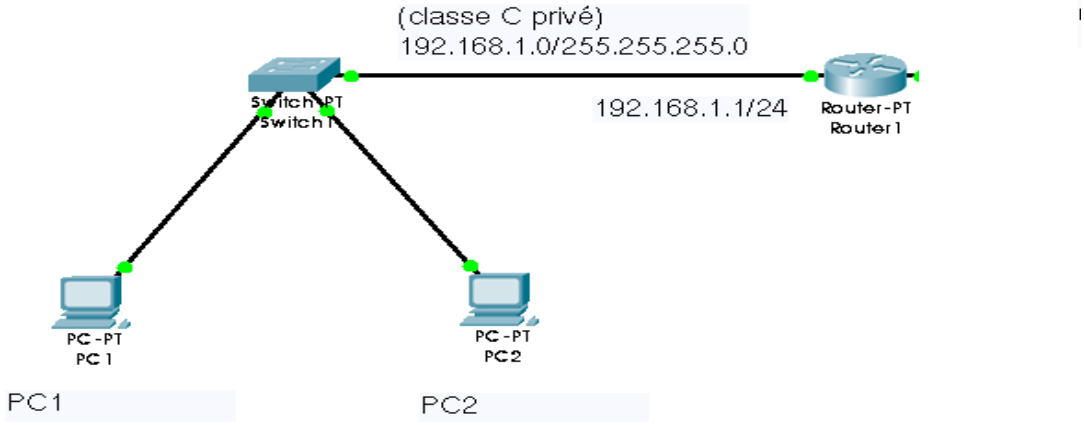
Objectifs :

- configurer un ordinateur en adresse IP fixe
- tester la communication dans un réseau LAN et interpréter les résultats.
- identifier un serveur DHCP et comprendre son fonctionnement.

Matériel :

- 2 ordinateurs
- 1 routeur Lynksys WRT54GL
- 2 Live DVD basés sur Ubuntu (fournis par le formateur)
- câbles réseau

Schéma du réseau :



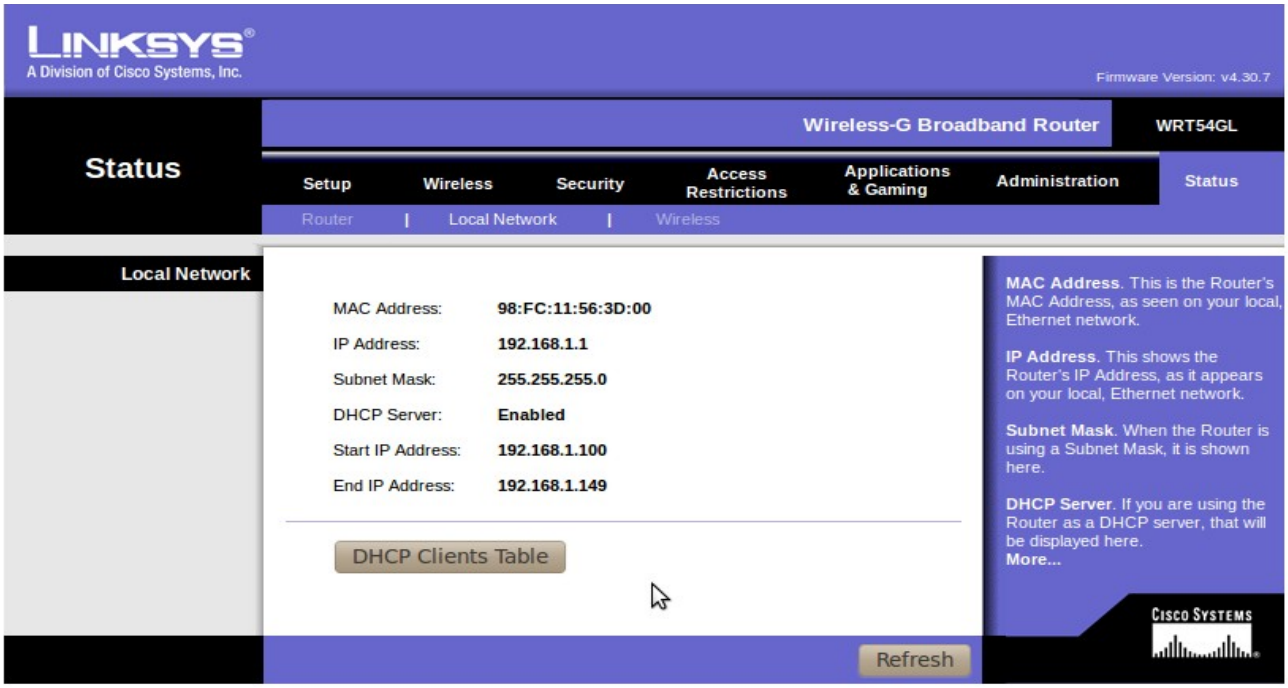
➔ Si cela n'a pas déjà été fait, vous devez câbler le réseau ci-dessus, et démarrer les ordinateurs PC1 et PC2 avec les Live DVD Ubuntu.

➔ Dans le navigateur FireFox, taper l'adresse IP du routeur 1 *(Nom d'utilisateur : admin, Mot de passe : admin)*. Vous accédez ainsi à l'interface d'administration du routeur.

➔ Observer les réglages du serveur DHCP : ***Setup / Network Setup / Network Address Server Settings (DHCP)***

➔ Vous allez maintenant visualiser la table des adresses attribuées par le serveur DHCP à vos ordinateurs PC1 et PC2 : ***Status /Local Network / DHCP Clients Table***

- ➔ Vérifier la correspondance entre l'adresse IP de vos ordinateurs clients et les adresses MAC des carte réseaux (on pourra utiliser la commande **ifconfig**).
- ➔ Quelle est la durée maximum d'un bail ?



D'après la figure ci-dessus :

- ➔ Combien d'adresses IP le serveur DHCP peut-il fournir ?
- ➔ A quelle carte réseau correspond l'adresse MAC ?

En conclusion :

- ➔ Quelle est la fonction supplémentaire que remplie le routeur Lynksys WRTG54GL ?

On désire maintenant configurer les ordinateurs avec des adresses IP fixes selon le plan suivant :

	PC1 (eth0)	PC2 (eth0)
Adresse IP	192.168.1.2	192.168.1.3
Masque de sous réseau	255.255.255.0	255.255.255.0
Passerelle	192.168.1.1	192.168.1.1

- ➔ Vérifier à l'aide de l'utilitaire **ipcalc** que les adresses choisies sont cohérentes.
- ➔ A l'aide de la documentation Présentation du Live DVD basé sur Ubuntu 10.10 *(page 4)*, configurer les adresses IP des 2 ordinateurs PC1 et PC2.
- ➔ Tester la communication entre ordinateurs et routeurs avec la commande ***ping***.

*Note : sous Windows, la commande **ping** est identique et la commande **ipcconfig / all** permet de connaître les paramètres réseaux de toutes les cartes réseaux de l'ordinateur (Ethernet , WiFi). Sous Linux il faut utiliser la commande **ifconfig***

TP3 : Étude d'un réseau WAN

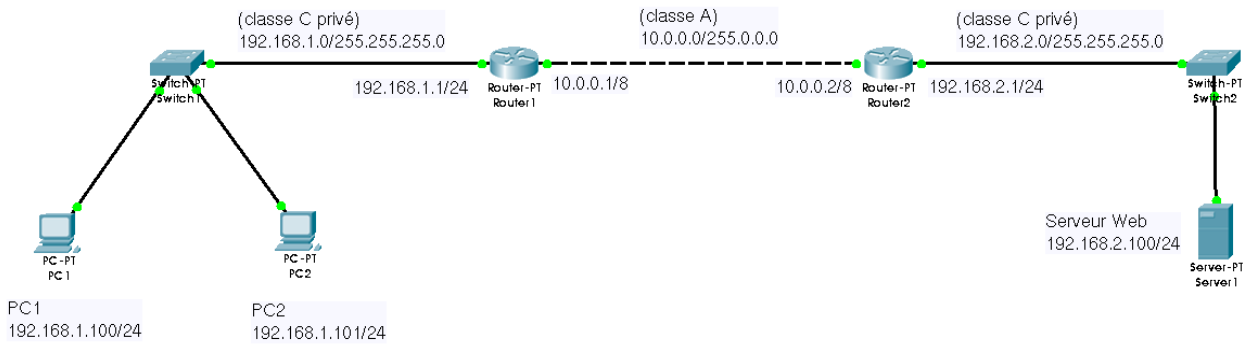
Objectifs :

- installer un réseau étendu
- reconnaître les fonctions remplies par les éléments d'un réseau
- relever et justifier la configuration des éléments d'un réseau
- tester la communication dans un réseau WAN et interpréter les résultats.
- Analyser des trames

Matériel :

- 3 ordinateurs (2 au moins)
- 2 routeur Lynksys WRTG54GL
- 3 Live DVD basés sur Ubuntu (fournis par le formateur)
- câbles réseaux

Schéma du réseau WAN à réaliser :



➔ Quelle fonction des routeurs WRTG54GL va-t-on utiliser pour réaliser un réseau étendu ?

➔ Réaliser le câblage du réseau WAN ci-dessus.

➔ Démarrer avec un Live DVD d'Ubuntu, l'ordinateur du LAN2 sur lequel sera implantée la fonction serveur Web.

➔ Vérifier la configuration IP du serveur Web. Vérifier à l'aide de l'utilitaire **ipcalc** que les adresses choisies pour le LAN2 sont cohérentes.

➔ Quelle est l'adresse de la passerelle ?

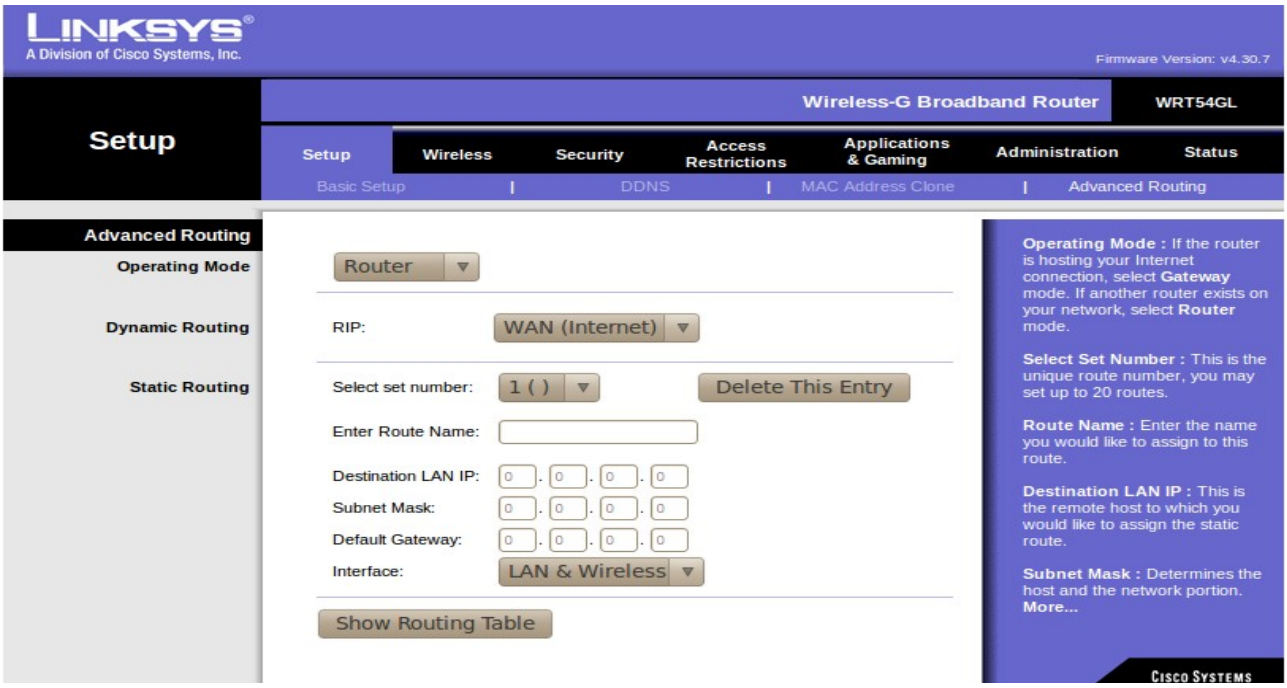
➔ Le formateur ayant au préalable configuré le routeur 2, tester la communication : de PC1 vers le routeur1, de PC1 vers le routeur2, puis de PC1 vers le serveur Web

➔ Remplir le tableau suivant :

	PC1 (eth0)	PC2 (eth0)	Serveur Web
Adresse MAC			
Adresse IP			
Masque sous réseau			
Passerelle			

Configurations des routeurs :

➔ Visualiser la configuration des routeurs 1 et 2 : ***Firefox / @ip routeur / Setup / Advanced Routing***



➔ Expliquer le mode de fonctionnement et le choix du protocole de routage

Table de routage :

➔ Visualiser les tables de routage des routeurs 1 et 2 : ***Show Routing Table***

Routeur1:

Routing Table Entry List Refresh

Destination LAN IP	Subnet Mask	Gateway	Interface
192.168.2.0	255.255.255.0	10.0.0.2	WAN (Internet)
192.168.1.0	255.255.255.0	0.0.0.0	LAN & Wireless
10.0.0.0	255.0.0.0	0.0.0.0	WAN (Internet)
0.0.0.0	0.0.0.0	10.0.0.2	WAN (Internet)

Close

➔ Interpréter cette table de routage :

- pour une communication vers le réseau 192.168.2.0 , la trame sera envoyée vers la passerelle 10.0.0.2 dont l'interface est le port Internet (WAN)
- pour une communication vers le réseau 192.168.1.0, il n'y a pas de passerelle puisque c'est le réseau interne (LAN)
- pour une communication sur le réseau WAN, pas de passerelle.
- pour une communication vers tout autre réseau (0.0.0.0), la trame est envoyée vers la passerelle 10.0.0.2 côté port Internet (WAN)

➔ De la même façon interpréter la table de routage du routeur2.

➔ Analyser une route de PC1 vers le Serveur Web: depuis **PC1**, **Système / Administration / Outils réseau / onglet Traceroute** , puis taper l'adresse: ***192.168.2.100***

➔ Interpréter les résultats obtenus.

- ➔ A quoi correspondent les sauts ?
- ➔ Vous pouvez également exécuter cette commande en ligne de commande (mode Terminal):
  traceroute @ip_destination

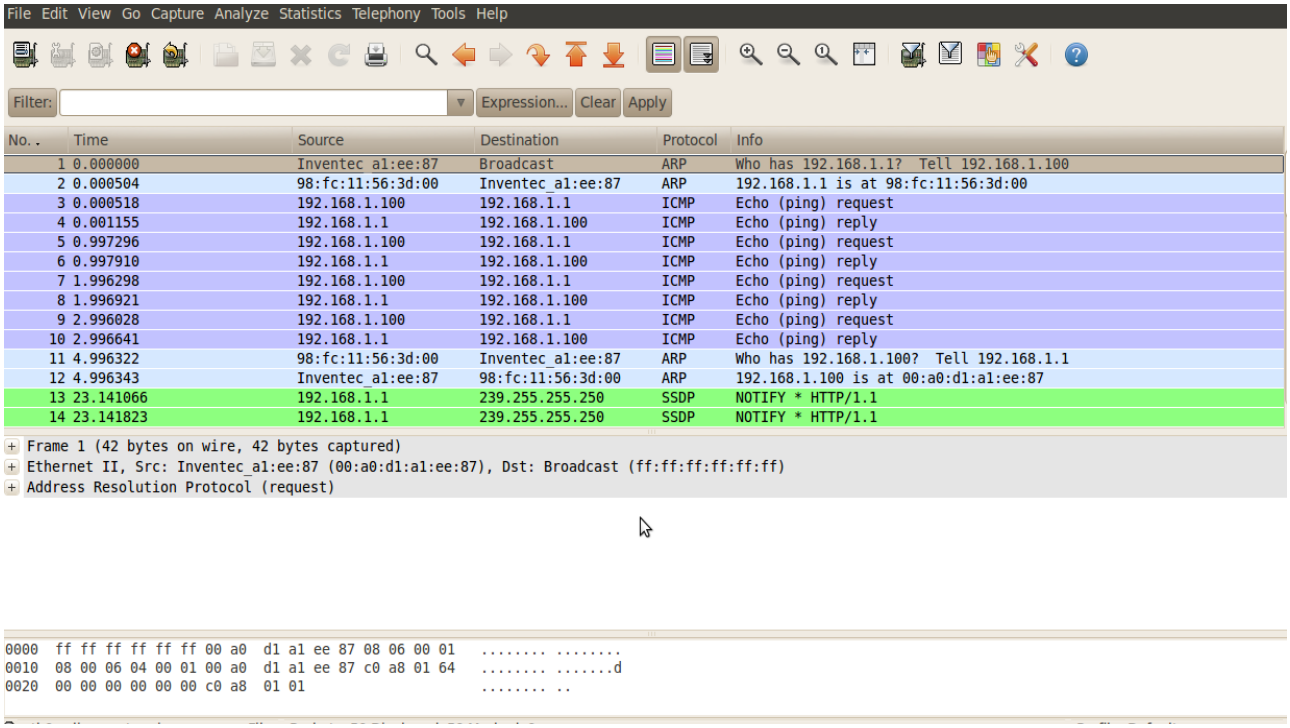
Note : sous Windows, la commande équivalente à ***traceroute*** *est :* ***tracert @ip*** *(ou adresse internet)*

Analyse de trames avec Wireshark:

Capture associée à la commande ping :

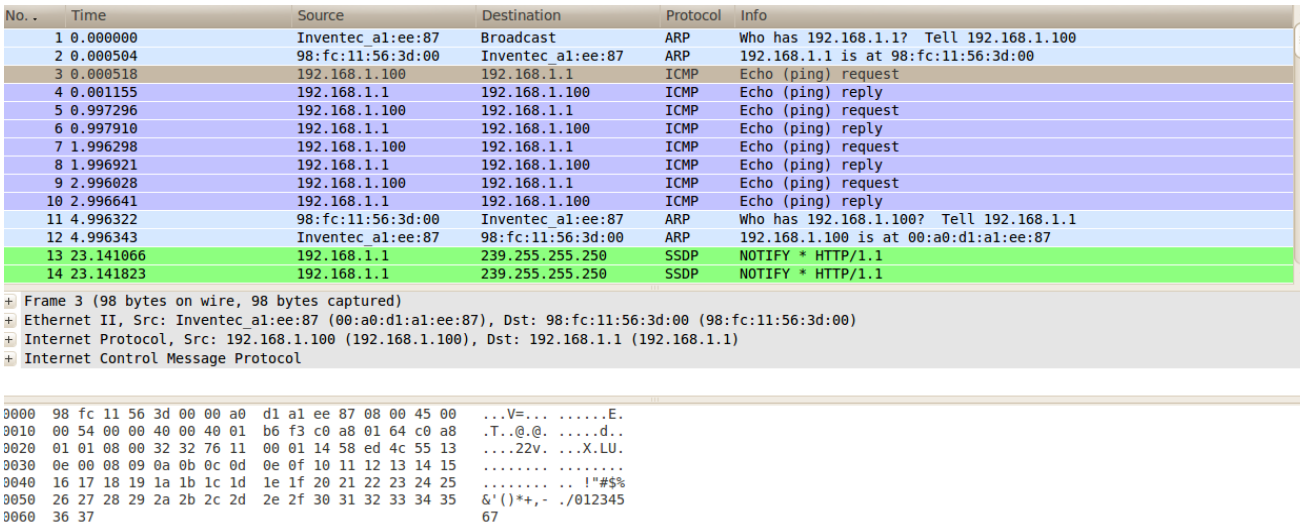
- ➔ Lire le document annexe concernant **Wireshark** (Cf. documentation Logiciel de capture Ethernet : Wireshark)
  En déduire le filtre permettant de visualiser uniquement les trames émises et reçus par l'adresse IP de PC1 (192.168.1.2)
- ➔ il faut lancer Wireshark par l'interface de commande en ligne (CLI).
  Rappel: **Application, Accessoires**, puis **Terminal.**
  Taper : ***sudo wireshark*** *(Cf. doc. Live DVD Ubuntu - page7)*
- ➔ lancer une capture en utilisant l'interface d'analyse : ***eth0***
- ➔ en mode terminal, envoyer une requête ICMP ***(ping)*** vers le Routeur1 :
  ping 192.168.1.1 -c4 *(-c4 correspond à 4 paquets de données)*

Lors d'une toute première communication, on obtient une capture similaire à celle-ci:



- ➔ Ligne 1 : justifier l'adresse Source et l'adresse Destination
- ➔ Ligne 2 : justifier l'adresse Source et l'adresse Destination
- ➔ Dans la fenêtre du milieu, on retrouve la trame de la première ligne. A quoi correspond ff:ff:ff:ff:ff:ff ?
- ➔ Dans la fenêtre du bas, retrouver le code hexadécimal des adresses Source et Destination.
- ➔ Pourquoi la communication commence-t-elle par une requête ARP ?

Note: On pourra visualiser la table ***arp*** *à l'aide de la commande* ***arp****. On pourra enlever une entrée à cette table en tapant :* ***sudo arp -d @ip****.*



No.	Time	Source	Destination	Protocol	Info
1	0.000000	Inventec_a1:ee:87	Broadcast	ARP	Who has 192.168.1.1? Tell 192.168.1.100
2	0.000504	98:fc:11:56:3d:00	Inventec_a1:ee:87	ARP	192.168.1.1 is at 98:fc:11:56:3d:00
3	0.000518	192.168.1.100	192.168.1.1	ICMP	Echo (ping) request
4	0.001155	192.168.1.1	192.168.1.100	ICMP	Echo (ping) reply
5	0.997296	192.168.1.100	192.168.1.1	ICMP	Echo (ping) request
6	0.997910	192.168.1.1	192.168.1.100	ICMP	Echo (ping) reply
7	1.996298	192.168.1.100	192.168.1.1	ICMP	Echo (ping) request
8	1.996921	192.168.1.1	192.168.1.100	ICMP	Echo (ping) reply
9	2.996028	192.168.1.100	192.168.1.1	ICMP	Echo (ping) request
10	2.996641	192.168.1.1	192.168.1.100	ICMP	Echo (ping) reply
11	4.996322	98:fc:11:56:3d:00	Inventec_a1:ee:87	ARP	Who has 192.168.1.100? Tell 192.168.1.1
12	4.996343	Inventec_a1:ee:87	98:fc:11:56:3d:00	ARP	192.168.1.100 is at 00:a0:d1:a1:ee:87
13	23.141066	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
14	23.141823	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1

```
+ Frame 3 (98 bytes on wire, 98 bytes captured)
+ Ethernet II, Src: Inventec_a1:ee:87 (00:a0:d1:a1:ee:87), Dst: 98:fc:11:56:3d:00 (98:fc:11:56:3d:00)
+ Internet Protocol, Src: 192.168.1.100 (192.168.1.100), Dst: 192.168.1.1 (192.168.1.1)
+ Internet Control Message Protocol
```

```
0000  98 fc 11 56 3d 00 00 a0  d1 a1 ee 87 08 00 45 00   ...V=... ......E.
0010  00 54 00 00 40 00 40 01  b6 f3 c0 a8 01 64 c0 a8   .T..@.@. .....d..
0020  01 01 08 00 32 32 76 11  00 01 14 58 ed 4c 55 13   ....22v. ...X.LU.
0030  0e 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                             67
```

- ➔ Lignes 3 à 10 : expliquer le déroulement de la requête ICMP
- ➔ Dans la fenêtre du milieu, dérouler chaque Item, puis à l'aide de ce que vous avez vu dans le cours CISCO, essayez de comprendre un maximum d'éléments.
- ➔ Quelles sont les données envoyées ?

Serveur Web (protocole HTTP):

- ➔ depuis un ordinateur du réseau LAN1, lancer un navigateur Web, et saisir dans la barre d'adresse, l'adresse IP du serveur Web du LAN2 pour accéder au cours Cisco,
- ➔ Depuis le serveur lui même, quelle autre adresse que 192.168.2.100 peut-on saisir ?
- ➔ Depuis PC1, avec WireShark, lancer une analyse de trame d'échange entre PC1 et le serveur Web lors de la navigation.
- ➔ Analyser la partie HTTP de la trame,

Administration à distance:

Beaucoup d'appareils intègrent des fonctions d'administration à distance. C'est le cas du Linksys WRT54G.

- ➔ Depuis un ordinateur du réseau LAN1, lancer un navigateur Web, et saisir l'adresse IP du Routeur2.
- ➔ Vous devez voir apparaître la fenêtre du routeur Lynksys. *(user=admin + mdp =password)*

TP4 : Réseau sans fil (WLAN)

Objectifs :

- installer et configurer un réseau WiFi
- reconnaître les fonctions remplies par les éléments d'un réseau
- tester la communication dans un réseau WLAN et interpréter les résultats.

Matériel :

- 3 ordinateurs (2 au moins)
- 2 routeur Lynksys WRTG54GL
- 3 Live DVD basés sur Ubuntu (fournis par le formateur)
- câbles réseaux
- clés réseaux WiFi WUSB54GC

➔ Dans un réseau WiFi, comment se comporte le routeur1 ? C'est une fonction de plus remplie par le routeur Linksys WRT54GL

➔ Comment appelle-t-on ce type de réseau WiFi ?

➔ Depuis le PC1 du LAN1, dans Firefox, accéder à la page d'administration du Routeur1. Relever les paramètres WiFi du point d'accès dans **Status/Wireless**

➔ En navigant dans les différents onglets, remplir le tableau suivant :

Paramètres WLAN	wlan0
Type de réseau WiFi (Ad-hoc / Infrastructure)	
SSID	
Adresse MAC de l'interface réseau WiFi	
Filtrage MAC	
Type de Cryptage	

➔ Après avoir relevé l'adresse MAC de la clé WiFi qui vous a été fournie, la connecter à PC2 *(débrancher le câble réseau de PC2)*.

➔ Configurer le SSID de la clé WiFi pour qu'elle se connecte au point d'accès Routeur1 *(Cf. documentation page 4 et 5)*

➔ Un symbole en haut à droite de l'écran, doit vous indiquer que la connexion WiFi est établie.

➔ Relever l'adresse IP de la clé WiFi,

➔ Effectuer les tests de communication en WiFi entre PC2 et le point d'accès,

➔ Afin de valider le fonctionnement, depuis PC2, accéder au cours Cisco sur le serveur Web du LAN2.

Présentation du Live DVD basé sur Ubuntu 10.10

1 . Introduction à Ubuntu

Ubuntu est une distribution **GNU/Linux** qui réunit stabilité et convivialité. Elle s'adresse aussi bien aux particuliers qu'aux professionnels, débutants ou confirmés qui souhaitent disposer d'un système d'exploitation libre et sécurisé.
Ubuntu-fr.org est un site francophone dédié à la distribution Ubuntu. Ce site a été créé bénévolement par des passionnés de logiciels libres qui croient en cette distribution et adhèrent au message qu'elle véhicule : « humanité ».
Pour accéder à toute la documentation d'Ubuntu, il suffit de taper l'URL suivante : **http://doc.ubuntu-fr.org/**

Remarque : Linux est diffusé sous licence GPL. Il s'agit d'une licence qui impose à l'auteur de diffuser aussi le code de son programme.

2 . Contenu du Live DVD d'Ubuntu

Celui-ci est réalisé à partir de la distribution **Ubuntu 10.10** (version stable d'Octobre 2010). Il est personnalisé pour l'**enseignement des réseaux** à destination des professeurs de **STI2D**. Le DVD proposé comporte :

- Les outils nécessaires à l'étude des réseaux : **ifconfig**, **traceroute**, **nmap**, **ipcalc**, **tshark**, **gftp**, **open- ssh**, **wireshark**, etc. ;
- Les outils fournis par **Cisco** :
  - Un logiciel de simulation : **Packet Tracer** (/usr/local/PacketTracer5/packettracer) ;
  - les cours du module **CCNA Exploration 4.0** : **« Notions de base sur les réseaux »** accessibles en local à l'adresse **http://localhost** ;
- La suite Bureautique **OpenOffice.org 3.2** ;
- Un logiciel de création de diagrammes **SYSML** : **Topcased** (/usr/local/Topcased-
- 4.3.0/eclipse) ;
- Un logiciel de réalisation de diagrammes (réseaux, circuits électriques, etc.) : **DIA**.

Remarque : Une version CD existe à l'intention des élèves ne contenant pas les outils fournis par Cisco.

3 . Conditions d'utilisation du Live DVD

Cisco est une entreprise informatique américaine qui est le leader mondial des réseaux. Elle propose plusieurs programmes de cours et formation, adaptés à la variété des niveaux des différents acteurs de **Cisco** : professionnels, partenaires, employés, étudiants.
Le format des cours repose sur un support multimédia généré par CISCO : fiches de cours, animations, exercices, quiz en fin de chapitre. La plate-forme d'e-learning est accessible depuis une académie locale ou régionale Cisco, après **inscription du stagiaire dans l'académie**.

Pour utiliser ce DVD, il sera impératif de disposer d'un compte dans une académie Cisco.

4 . Présentation du Live DVD d'Ubuntu

4.1 : Démarrage du Live DVD

Si votre poste de travail ne démarre pas automatiquement sur le DVD, il faut au démarrage du poste de travail, accéder au **setup** (touche sup ou F1 ou F2) et choisir le lecteur de DVD comme premier périphérique de démarrage (First boot device).

4.2 : Aperçu

Une fois démarré, **Ubuntu** n'a rien de déroutant même pour les habitués de **Windows**. L'interface est composée de deux parties :

- Le **bureau**, qui contient une icône : un dossier avec des exemples de fichiers ;
- Les deux **tableaux de bord** : ce sont les deux barres en haut et en bas de l'écran.
  - Celle du **haut** permet de lancer des logiciels à partir des différents menus ou icônes. Le menu "**Applications**" correspond au menu "démarrer" de Windows;
  - La barre du **bas** correspond à la barre des tâches de Windows. C'est ici qu'apparaissent les fenêtres ouvertes.

Remarque : L'utilisateur par défaut se nomme **ubuntu** avec un mot de passe **vide**.

Une vidéo disponible sur **youtube**, vous présente un peu plus en détail le bureau d'Ubuntu :

http://www.youtube.com/watch?v=emEvDTHiz2Y&feature=player_embedded#!

4.3 : Menus

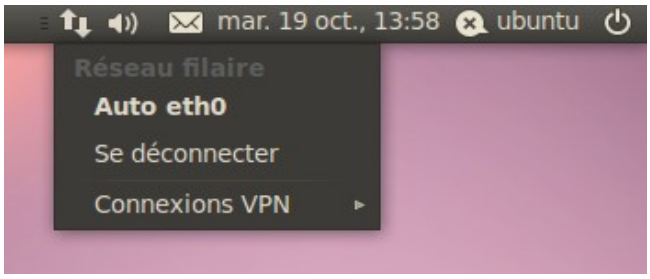
La barre du haut comporte **3 menus** :

- menu "**Applications**" correspondant au menu "démarrer" de Windows ;
- menu "**Raccourcis**" permettant d'accéder à tous les systèmes de fichiers du poste de travail ;
- menu "**Systèmes**" permettant d'accéder aux « Préférences » et à l' « Administration » du poste de travail.

5 . Configuration du réseau avec Ubuntu

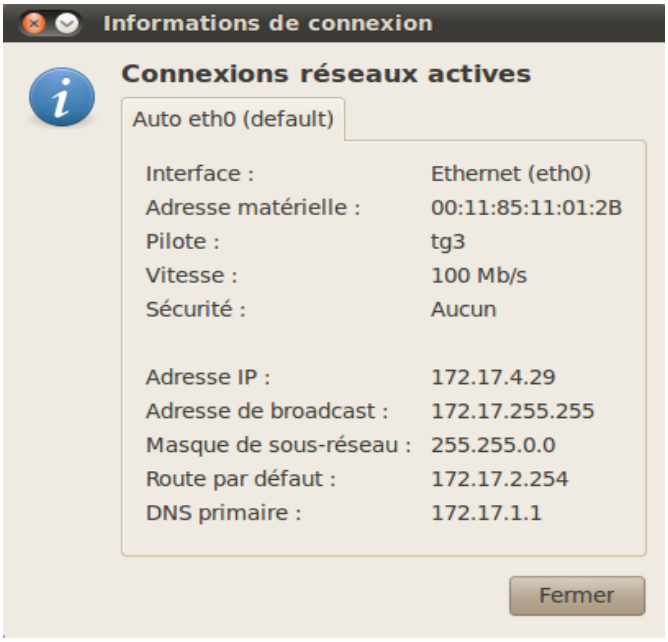
5.1 : Introduction

La configuration du réseau sous Ubuntu se fait grâce à l'utilitaire **Network Manager** et il prend la forme d'une applet, une petite icône située **à droite**, dans **le tableau de bord du haut**.



5.2 : Voir l'état des réseaux actuellement connectés

Lorsque vous êtes connecté à un ou plusieurs réseaux, **Network Manager** peut vous en indiquer les caractéristiques. Pour ce faire, faites un **clic-droi**t sur l'applet de **Network Manager** et sélectionnez l'entrée de menu **Informations de connexions**.
Pour chacune des connexions actives, un onglet est proposé selon le nom de la connexion. Affichez l'onglet de votre choix pour obtenir des informations à propos de la connexion en cours.



5.3 : Configurer des nouveaux réseaux ou modifier des réseaux existants

Pour configurer des réseaux, que ce soit l'ajout de nouveaux réseaux ou la modification de réseaux existants, faites un **clic-droit** sur l'applet de **Network Manager** et sélectionnez l'entrée de menu **Modification des connexions**.

- Pour **modifier une connexion existante**, ouvrez d'abord l'onglet correspondant au type de connexion à créer (filaire, sans fil, connexion mobile, VPN ou DSL). Puis, appuyez sur le bouton **Modifier** : une interface identique à celle de l'ajout d'une nouvelle connexion s'ouvre, mais avec certains champs d'informations pré-remplis. Modifiez les informations de votre choix, puis appuyez sur le bouton **Appliquer** pour que les changements soient pris en compte ;

- Pour **ajouter une nouvelle connexion**, ouvrez d'abord l'onglet correspondant au type de connexion à créer (filaire, sans fil, connexion mobile, VPN ou DSL). Puis, appuyez sur le bouton **Ajouter** : une interface vous permet de saisir les informations relatives à votre connexion réseau. Saisissez les informations de votre nouvelle connexion, puis appuyez sur le bouton **Appliquer** pour ajouter votre nouvelle connexion à la liste de celles disponibles.

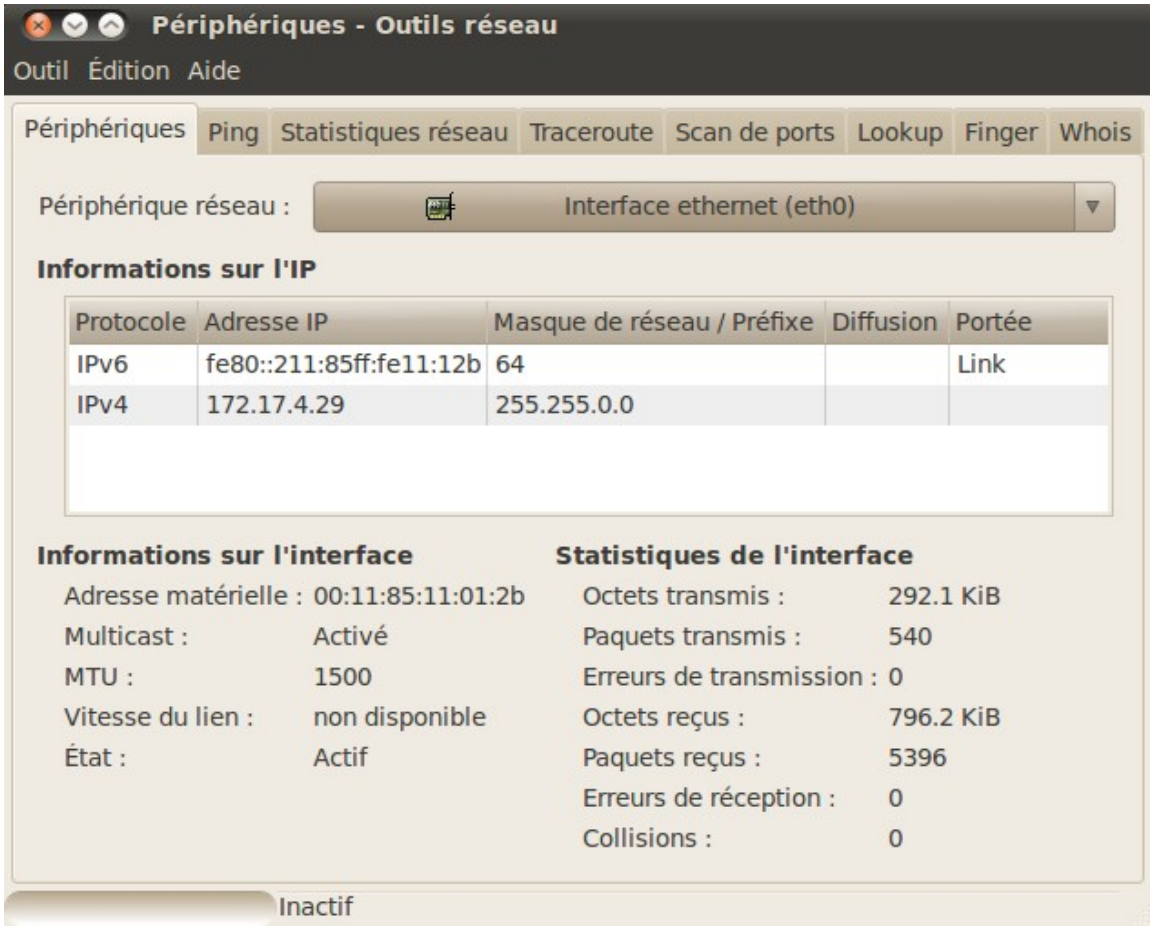
5.4 : Modifier les paramètres IP pour la saisie d'une adresse manuelle

Vous pouvez **paramétrer manuellement l'adresse IP** attribuée à votre ordinateur. Pour paramétrer une connexion devant avoir une adresse IP fixe (au moment de créer une nouvelle connexion ou en modifiant une connexion existante) :

- Rendez-vous dans l'onglet **Paramètres IPv4** de l'interface de gestion de votre connexion ;
- Dans le champ **Nom de la connexion**, entrez un nom unique significatif pour votre connexion ;
- Dans le menu déroulant **Méthode**, choisissez la méthode **Manuel** ;
- À la droite du cadre **Adresses**, appuyez sur le bouton Ajouter ;
- Dans le cadre **Adresses**, inscrivez l'adresse IP, le masque de sous-réseau et (accessoirement) la passerelle par défaut que doit utiliser votre connexion ;
- Dans le champ **Serveurs DNS**, inscrivez la ou les adresses des serveurs DNS que doit utiliser votre connexion. Séparez les adresses multiples par une virgule ;
- Dans le champ **Domaine de recherche**, inscrivez le domaine dans lequel votre connexion doit rechercher automatiquement des adresses, si tel est le cas ;
- Appuyez sur le bouton **Appliquer**, pour appliquer les changements.

6 . Utilitaires réseaux

Les utilitaires réseaux tels que **ping**, **traceroute** etc. peuvent être utilisés en mode graphique. Pour cela il faut passer par le menu **Système/Administration/Outils réseau**.



- Onglet « **Périphériques** » : Permet de sélectionner l'interface réseau (lo, eth0, etc.) et d'afficher les informations la concernant ;
- Onglet « **Ping** » : Permet de tester la connectivité réseau vers une autre machine à l'aide de la commande ping ;
- Onglet « **Statistiques réseau** » : Permet d'obtenir des informations réseaux sur la table de routage et sur les protocoles actifs ;
- Onglet «**Traceroute**» : Permet d'obtenir la route empruntée pour atteindre une machine distante ;
- Onglet «**Scan de ports**» : Permet de lister les ports ouverts sur la machine spécifiée ;
- Onglet «**Lookup**» : Permet de récupérer le nom ou l'adresse Ip de la machine spécifiée ;
- Onglet «**Finger**» : Permet d'obtenir des informations sur les utilisateurs du système ;
- Onglet «**Whois**» : Permet de récupérer le propriétaire d'un **nom de domaine**.

7 . Utilisation de Wireshark

Lorsqu'on lance **Wireshark** depuis le menu **Applications**, les interfaces réseaux ne sont pas disponibles. Il faut donc le lancer en ligne de commande avec les droits administrateur.

Faire **Applications/Accessoires/Terminal** et saisir la commande : **sudo wireshark** ou **gksudo wireshark**.

L'utilisation de **Wireshark** est détaillée dans le **document 5**.

Remarque : On peut aussi utiliser en mode commande l'application **tshark** (par exemple : **sudo tshark -i eth0**) qui correspond à **Wireshark** sans interface graphique. Pour connaître les interfaces valides faire **ifconfig** (équivalent à **ipconfig** sous Windows).

8 . Utilitaire ipcalc

ipcalc est un utilitaire en **ligne de commande** permettant de fournir de manière simple les informations IP d'un hôte.
Les diverses options permettent d'indiquer quelles informations seront affichées par **ipcalc** sur la sortie standard. Il est possible d'indiquer plusieurs options. Il faut toujours fournir une adresse IP sur laquelle travailler. La plupart des opérations ont également besoin d'un masque réseau ou d'un préfixe **CIDR**.

Exemple :

ipcalc 192.168.1.1/255.255.255.0

Address:	192.168.1.1	11000000.10101000.00000001. 00000001
Netmask:	255.255.255.0 = 24	11111111.11111111.11111111. 00000000
Wildcard:	0.0.0.255	00000000.00000000.00000000. 11111111
=>		
Network:	192.168.1.0/24	11000000.10101000.00000001. 00000000
HostMin:	192.168.1.1	11000000.10101000.00000001. 00000001
HostMax:	192.168.1.254	11000000.10101000.00000001. 11111110
Broadcast:	192.168.1.255	11000000.10101000.00000001. 11111111
Hosts/Net:	254	Class C, Private Internet

Logiciel de capture de trames Ethernet : WIRESHARK

1 . Introduction

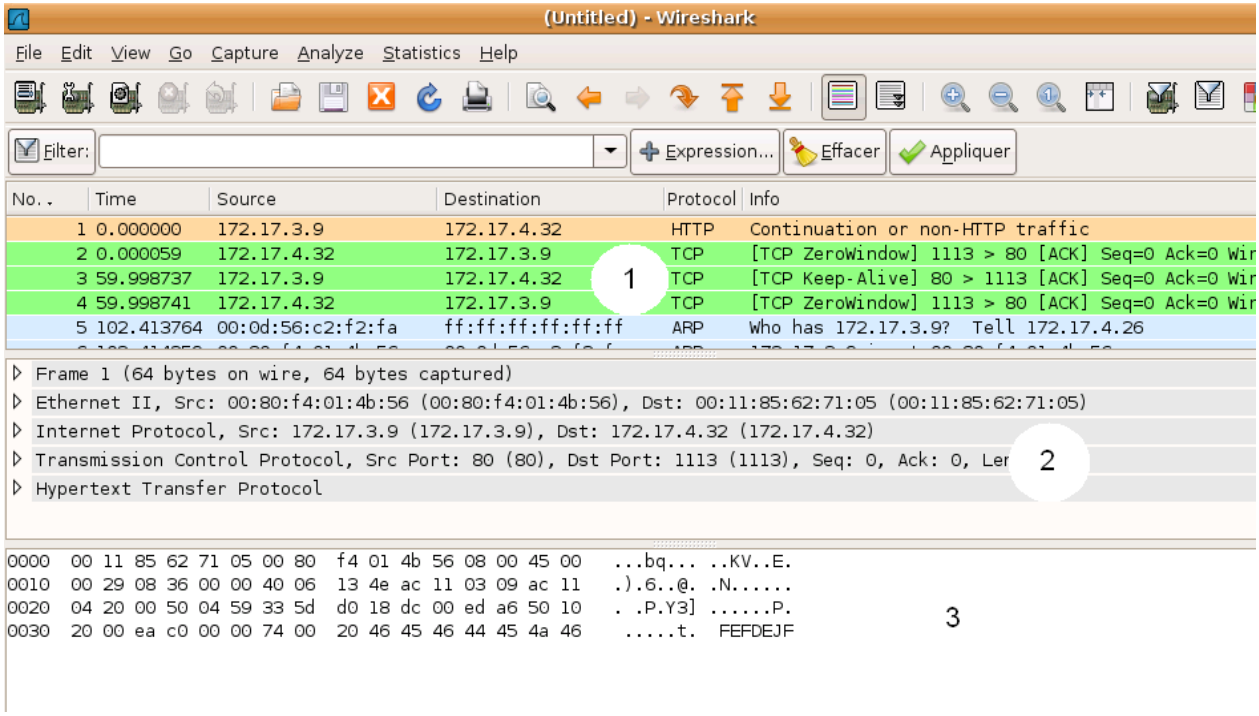
Pour pouvoir analyser finement le trafic réseau, il existe des **logiciels de capture de trames** qui sont des outils qui permettent de récupérer les paquets qui passent physiquement sur un réseau (quelque soit la destination de ces paquets).

Il existe un outil sous licence GNU qui permet de faire cela et qui permet d'interpréter la structure des paquets, cela de façon graphique. Cet outil se nomme **Wireshark**. Avant juin 2006, **Wireshark** répondait au nom d'**Ethereal**.
Wireshark utilise la librairie **Libpcap** et la syntaxe des **filtres** est similaire à celle de la commande Unix **tcpdump**.

Le guide de l'utilisateur est disponible à l'adresse suivante :
http://www.wireshark.org/docs/wsug_html_chunked/.

2 . Interface principale

La fenêtre principale de **Wireshark** comporte trois volets :



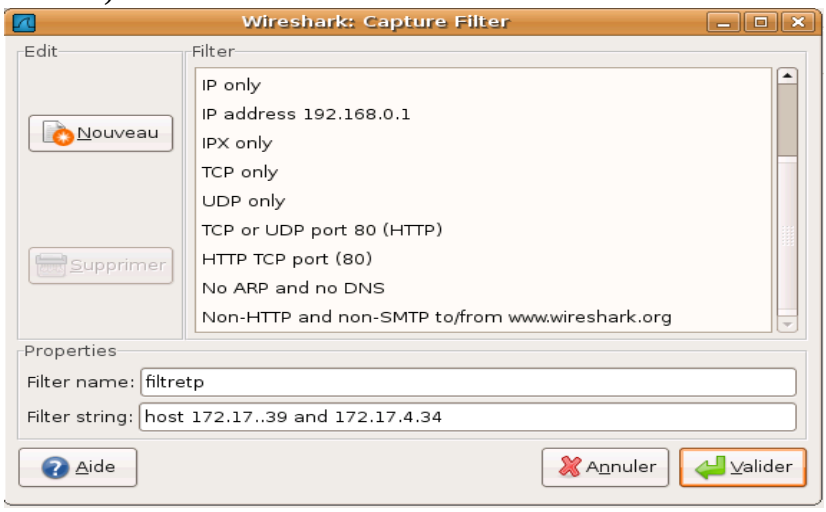
- Le volet **1** permet de recenser **l'ensemble des paquets capturées**. Sont spécifiés **l'émetteur** de la trame, le **destinataire** de la trame et le **protocole réseau** mis en œuvre;
- Le volet **2** permet de visualiser la **pile des protocoles** employés dans le **paquet** sélectionné dans le premier volet;
- Le volet **3** permet de visualiser **l'ensemble du paquet capturée** au format **hexadécimal** et la traduction **ASCII** correspondante.

3 . La capture de trames

Les 2 **étapes** permettant la **capture** de **trames** sont les suivantes :

3.1 : Définition d'un filtre de capture

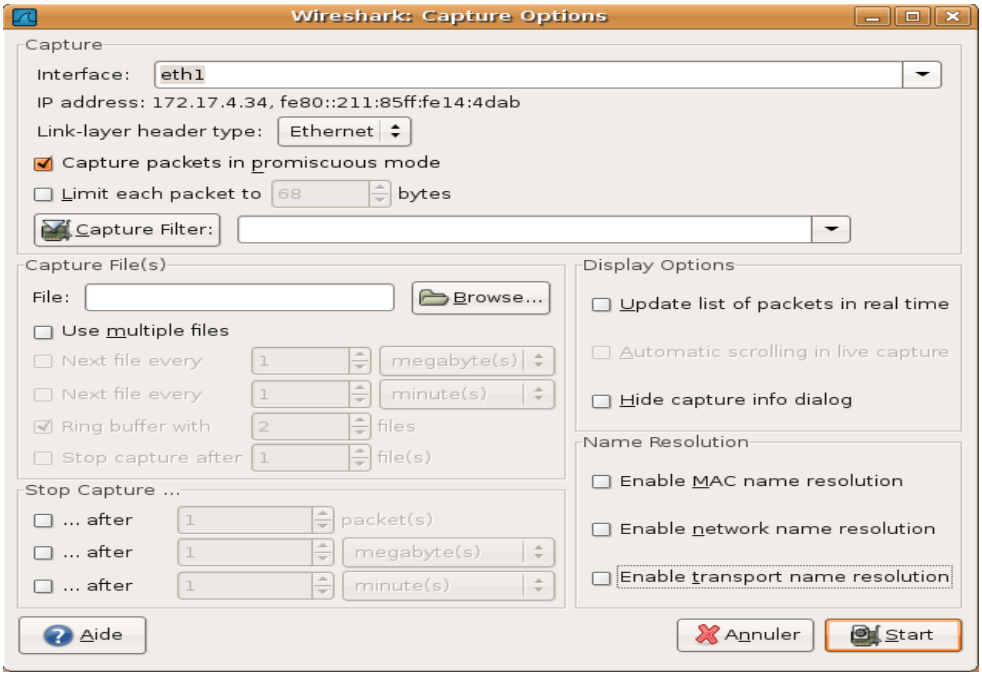
La définition d'un **filtre de capture** (*Menu Capture – Capture Filters*) permet de **cibler** les **trames** à **acquérir** en spécifiant les **protocoles voulus**, les **adresses désirées**.
La **fenêtre** permettant d'établir les **filtres de captures** (*la syntaxe des filtres est identique à celle de* ***tcpdump*** *cf. annexe* ***1***) est la suivante :



Le **nom du filtre** et sa **syntaxe** sont à **spécifier** en premier. Le fait de **cliquer** sur **Nouveau** permet la **sauvegarde** du **filtre** défini.
Si par exemple, on veut observer **uniquement** les **trames échangées** entre les **postes 172.16.2.28** et **172.16.2.9**, le **filtre** à appliquer est **host 172.16.2.28 and host 172.16.2.9**.

3.2 : Définition des options de capture

Une fois le filtre établi, cliquer sur **Capture Options** (*menu Capture*). La fenêtre suivante apparaît :



Plusieurs critères peuvent être spécifiés :

- **Interface** : *permet de sélectionner l'interface physique (carte réseau, …) à partir de laquelle la capture va être effectuée;*
- **Capture filter** : *permet d'établir un filtre de capture (syntaxe tcpdump) ou d'appliquer un filtre sauvegardé (voir précédemment);*
- **Enable MAC name resolution** : *permet de spécifier (si sélectionné) que les adresses Ethernet n'apparaîtront pas sous la forme nn-nn-nn-nn-nn-nn mais avec le nom de l'interface MAC (nom de carte réseau par exemple).*

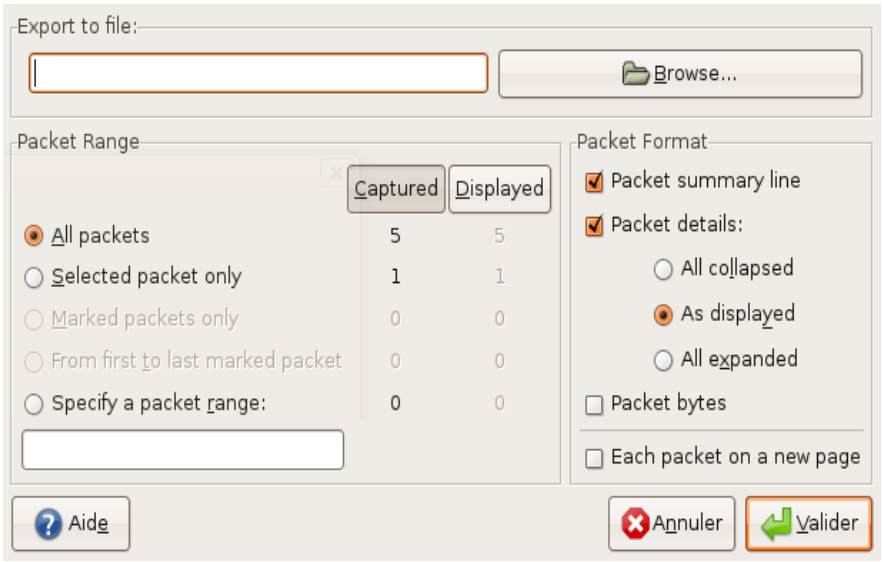
Décocher les options du groupe « **Name Resolution** » et cliquer sur **Start** pour lancer la **capture**.

4 . Analyse et sauvegarde des trames

Une fois les captures effectuées, il est possible de faire le travail d'analyse.

Wireshark offre de nombreuses possibilités d'analyse de haut-niveau. Ces fonctionnalités sont accessibles par le menu [Statistiques] (Summary, Protocol Hierarchy, ...).

Vous pouvez enregistrer les informations capturés dans le format "Wireshark/tcpdump/ - libcap" pour une analyse ultérieure avec Wireshark : [File] – [Save As...]. Les informations peuvent être exportées dans un format texte, incluant une mise en forme simple qui correspond à peu près à l'arborescence affiché dans la fenêtre "Packet Details".



5 . Les filtres

5.1 : Introduction

Dans un réseau Ethernet sous IP, les informations circulent sous forme de **datagrammes**, c'est-à-dire de paquets encapsulant les données à transmettre.

Il y a deux sortes de filtres. Les filtres à la **capture** et les filtres à l'**affichage**. Ces filtres n'ont pas la même syntaxe. La syntaxe des filtres à la capture est la même que les filtres utilisés pour la commande **tcpdump**.

Quand aux filtres à l'affichage, la syntaxe est une syntaxe propriétaire à **Wireshark**. La section présente donne des exemples pour ces deux types de filtres.

5.2 : Filtres de capture

Ne seront gardés que les paquets pour lesquels le filtre est vrai. Les filtres se décomposent en 3 parties :

- le **protocole** qui peut être **arp**, **ether**, **fddi**, **icmp**, **ip**, **ip6**, **link**, **ppp**, **radio**, r**arp**, **slip**, **tcp**, **tr**, **udp** ou **wlan** ;
- la **direction** qui peut être **src** (source) ou **dst** (destination) ;
- un **champ** qui peut être **host**, **net** ou **port** suivi d'une valeur.

Les opérateurs **and** (ou **&&**), **or** (ou ||) et **not** (ou **!**) peuvent être utilisés pour combiner des filtres.

Voici quelques exemples de filtres de capture :

Filtre	Fonction
host 172.16.0.1 and tcp	ne conserve que les paquets TCP à destination ou en provenance de la machine 172.16.0.1
udp port 53	ne conserve que les paquets UDP en provenance ou en destination du port 53
udp port 53 and dst host 172.16.0.1	ne conserve que les paquets UDP en provenance ou en destination du port 53 à destination de la machine 172.16.0.1
tcp dst port 80 and dst host 172.16.0.1 and src net 172.16.0.0 mask 255.255.255.0	ne conserve que les paquets TCP en destination de la machine 172.16.0.1 sur le port 80 et en provenance des machines du réseau 172.16.0/24

En **annexe 1**, vous trouverez tous les types de filtres de **capture** compatibles **TCPDUMP**.

5.3 : Filtres d'affichage

Les filtres d'affichage sont un peu plus fin que ceux de la capture. Seuls les paquets pour lesquels l'expression du filtre est vraie seront gardés. Les expressions sont basées sur les champs disponibles dans un paquet. Le simple ajout d'un champ veut dire que l'on garde le paquet si ce champ est disponible.

Maintenant, on peut aussi utiliser les opérateurs ==, **!**=, >, <, >= et <= pour comparer les champs avec des valeurs. Les expressions ainsi fabriquées peuvent être combinées avec les opérateurs **&&** (pour un et logique), || (pour un ou logique), ^^ (pour le ou exclusif) et **!** pour la négation.

L'usage des parenthèses est possible.

Voici quelques exemples de champs disponibles :

Champ	Type	Signification
ip.addr	adresse IPv4	adresse IP source ou destination
ip.dst	adresse IPv4	adresse IP destination
ip.flags.df	booléen	Drapeau IP, ne pas fragmenter
ip.flags.mf	booléen	Drapeau IP, fragments à venir
ip.ttl	entier non signé sur 8 bits	Time to live
http.request	booléen	requête HTTP
http.response	booléen	réponse HTTP
icmp.code	entier non signé sur 8 bits	numéro du code d'une commande ICMP
icmp.type	entier non signé sur 8 bits	numéro du type d'une commande ICMP

Voici quelques exemples de filtres d'affichage :

Filtre	Signification
ip.addr == 172.16.0.100	tous les paquets IP en provenance ou à destination de la machine 172.16.0.100
(ip.addr >= 172.16.0.100) && (ip.addr <= 172.16.0.123)	tous les paquets IP en provenance ou à destination des machines comprises entre l'adresse IP 172.16.0.100 et l'adresse IP 172.16.0.123 (comprises)

6 . Conclusion

Remarque : Si vous n'avez pas d'interface graphique, vous pourriez être intéressé par "**TShark**" qui est une version en ligne de commande de **Wireshark**. **TShark** supporte les mêmes fonctionnalités que **Wireshark**.

Par exemple : **#tshark -i eth1 host 192.168.1.10**

Annexe 1 : Les filtres de capture (TCPDUMP)

Command Line Options			
`-A`	Print frame payload in ASCII	`-q`	Quick output
`-c <count>`	Exit after capturing **count** packets	`-r <file>`	Read packets from **file**
`-D`	List available interfaces	`-s <len>`	Capture up to **len** bytes per packet
`-e`	Print link-level headers in the capture dump	`-S`	Print absolute TCP sequence numbers
`-F <file>`	Use **file** as the filter expression	`-t`	Don't print timestamps
`-G <n>`	Rotate the dump file every **n** seconds	`-v[v[v]]`	Print more verbose output
`-i <iface>`	Specifies the capture interface	`-w <file>`	Write captured packets to **file**
`-K`	Don't verify TCP checksums	`-x`	Print frame payload in hex
`-L`	List data link types for the interface	`-X`	Print frame payload in hex and ASCII
`-n`	Don't convert addresses to names	`-y <type>`	Specify the data link type
`-p`	Don't capture in promiscuous mode	`-Z <user>`	Drop privileges from root to **user**

Capture Filter Primitives	
`[src|dst] host <host>`	Matches a host as the IP source, destination, or either
`ether [src|dst] host <ehost>`	Matches a host as the Ethernet source, destination, or either
`gateway host <host>`	Matches packets which used **host** as a gateway
`[src|dst] net <network>/<len>`	Matches packets to or from an endpoint residing in **network**
`[tcp|udp] [src|dst] port <port>`	Matches TCP or UDP packets sent to/from **port**
`[tcp|udp] [src|dst] portrange <p1>-<p2>`	Matches TCP or UDP packets to/from a port in the given range
`less <length>`	Matches packets less than or equal to **length**
`greater <length>`	Matches packets greater than or equal to **length**
`(ether|ip|ip6) proto <protocol>`	Matches an Ethernet, IPv4, or IPv6 protocol
`(ether|ip) broadcast`	Matches Ethernet or IPv4 broadcasts
`(ether|ip|ip6) multicast`	Matches Ethernet, IPv4, or IPv6 multicasts
`type (mgt|ctl|data) [subtype <subtype>]`	Matches 802.11 frames based on type and optional subtype
`vlan [<vlan>]`	Matches 802.1Q frames, optionally with a VLAN ID of **vlan**
`mpls [<label>]`	Matches MPLS packets, optionally with a label of **label**
`<expr> <relop> <expr>`	Matches packets by an arbitrary expression

Protocols		
`arp`	`ip6`	`slip`
`ether`	`link`	`tcp`
`fddi`	`ppp`	`tr`
`icmp`	`radio`	`udp`
`ip`	`rarp`	`wlan`

TCP Flags	
`tcp-urg`	`tcp-rst`
`tcp-ack`	`tcp-syn`
`tcp-push`	`tcp-fin`

Modifiers
! or `not`
`&&` or `and`
`||` or `or`

Examples	
`udp dst port not 53`	All UDP not bound for port 53
`host 10.0.0.1 && host 10.0.0.2`	All packets between these hosts
`tcp dst port 80 or 8080`	All packets to either TCP port

ICMP Types		
`icmp-echoreply`	`icmp-routeradvert`	`icmp-tstampreply`
`icmp-unreach`	`icmp-routersolicit`	`icmp-ireq`
`icmp-sourcequench`	`icmp-timxceed`	`icmp-ireqreply`
`icmp-redirect`	`icmp-paramprob`	`icmp-maskreq`
`icmp-echo`	`icmp-tstamp`	`icmp-maskreply`