Date :	NOM – Prénom :	TP n° /6
Lycée professionnel ***Pierre MENDÈS-FRANCE***	**Sujet de Travaux Pratiques**	**1ère SEN**
	PACKETTRACER : CRÉATION DE RÉSEAU VIRTUEL	

1ère Partie : Représentations du réseau

Objectifs pédagogiques :

- Exploration de l'interface de PacketTracer ;
- Recherche des composants clés utilisés pour placer des symboles de périphériques sur le lieu de travail logique ;
- Examen des périphériques qui peuvent être placés sur le lieu de travail logique et de leurs symboles ;
- Placement et connexion de périphériques ;
- Ajout de symboles de périphériques au lieu de travail logique ;
- Connexion de périphériques sur le lieu de travail logique à l'aide de la connexion automatique.

Présentation :

PacketTracer est un simulateur de réseau qui vous permet de créer une simulation de réseau, de configurer les périphériques dans le réseau, de tester le réseau et d'examiner le trafic du réseau. La première étape de création d'une simulation de réseau dans PacketTracer consiste à placer les périphériques sur le lieu de travail logique et à les connecter entre eux. PacketTracer utilise les symboles normalisés que l'on retrouve dans tous les schémas de réseaux informatiques.

1°) Tâche 1 : Exploration de l'interface de Packet Tracer

1.1°) Étape 1. « Lancer » le logiciel

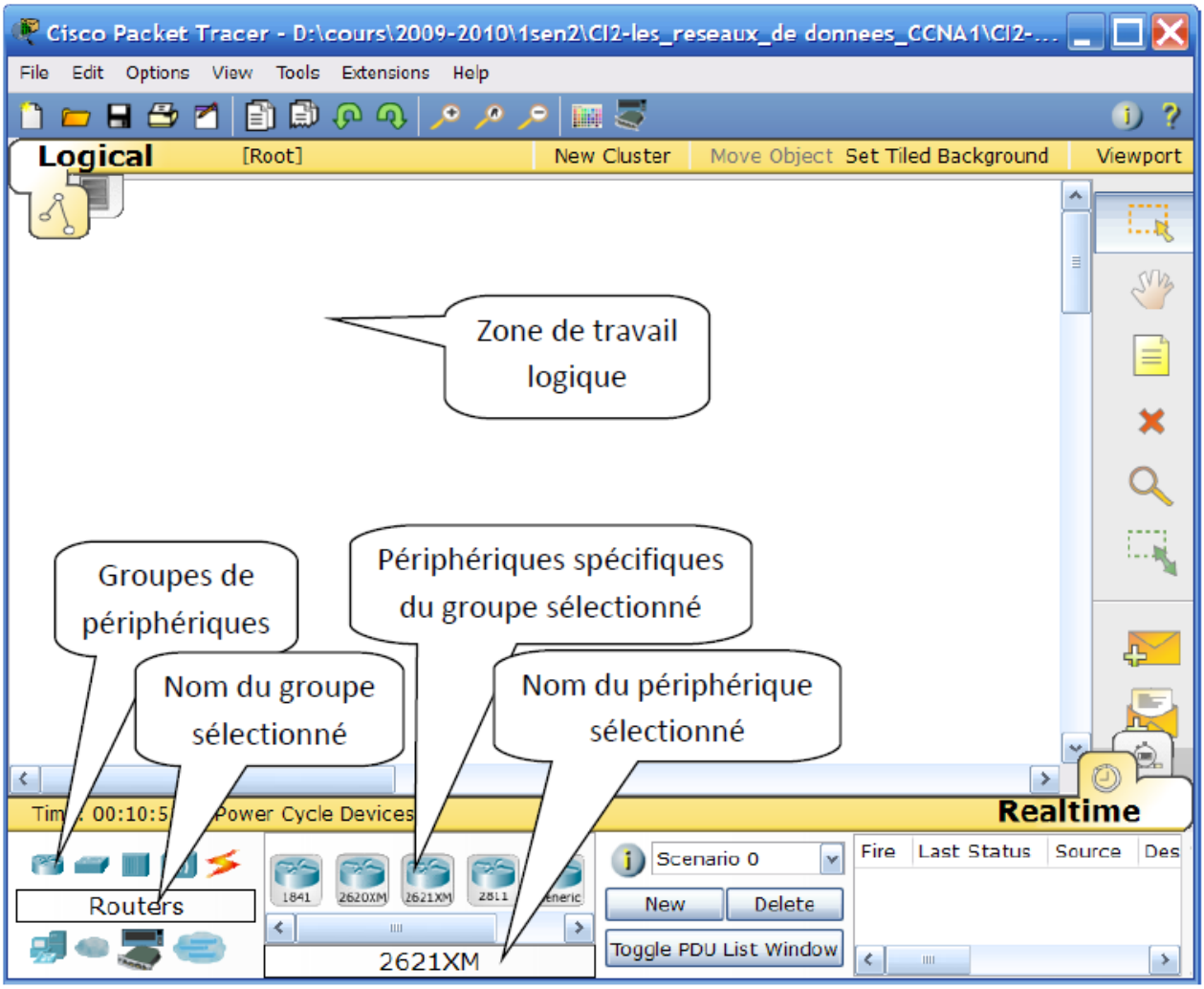
Ouvrir le logiciel « Packet Tracer »

1.2°) Étape 2. Zone de travai l logique

Lorsque PacketTracer démarre, il présente une vue logique du réseau en mode temps réel. La partie principale de l'interface de PacketTracer est le Lieu de travail logique. Il s'agit de la zone vierge étendue dans laquelle des périphériques peuvent être placés et connectés.

1.3°) Étape 3. Symboles de périphériques

La partie inférieure gauche de l'interface de PacketTracer, située sous la barre jaune, correspond à lapartie de l'interface que vous utilisez pour sélectionner et placer des périphériques dans le lieu de travail logique. La première zone dans la partie inférieure gauche contient des symboles qui représentent des groupes de périphériques. Lorsque vous déplacez le pointeur de la souris sur ces symboles, le nom du groupe s'affiche dans la zone de texte située au centre. Lorsque vous cliquez sur l'un de ces symboles, les périphériques spécifiques au groupe apparaissent dans la zone de droite. Lorsque vous pointez sur les périphériques spécifiques, une description de périphérique s'affiche dans la zone de texte située sous ces périphériques.



Les zones de PacketTracer

1.3.1°) Cliquez sur chacun des groupes et étudiez les différents périphériques disponibles, ainsi que leurs symboles. Compléter les tableaux suivants :

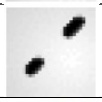
Groupe : généraliste :

Symbole groupe	Nom anglais	Nom français
	Routers	
	Switches	
	Hubs	
	Wireless Devices	
	Connections	
	End Devices	
	WAN emulation	
	Custom Made Device	
	Multiuser Connection	

Groupe : Wireless Devices :

Symbole groupe	Nom anglais	Nom français
	Acces point PT A N	

Groupe : Connections :

Symbole groupe	Nom anglais	Nom français
	Automatically choose connection type	
	console	
	Copper straight trough	
	Copper cross over	
	fiber	
	phone	
	coaxial	
	Serial DCE	
	Serial DTE	

Groupe : WAN emultion :

Symbole groupe	Nom anglais	Nom français
	cloud	
	DSL-modem-PT	
	Cable-modem-PT	

2°) Tâche 2 : ajout de périphériques au lieu de travail logique

2.1°) Étape 1. Sélection et placement de périphériques

Pour ajouter un périphérique, cliquez sur le symbole du périphérique désiré, puis pointez sur l'emplacement où vous voulez le placer dans la zone de travail logique (le pointeur se transforme en croix), puis cliquez. Recherchez et placez les périphériques suivants

- Le cloud
- Un modem ADSL
- Un switch 24 ports
- Un serveur
- Un PC de bureau
- Un PC portable
- Une imprimante réseau

2.2°) Étape 2. Connecter des périphériques à l'aide de la connexion automatique

Cliquez sur le symbole du groupe de connexions. Les symboles de connexion spécifiques représentent différents types de câbles qui peuvent être utilisés pour connecter des périphériques. Le premier type spécifique, la ligne en forme d'éclair doré, sélectionne automatiquement le type de connexion en fonction des interfaces disponibles sur les périphériques. Lorsque vous cliquez sur ce symbole, le pointeur ressemble à un connecteur de câble. Pour connecter deux périphériques, cliquez sur le symbole de connexion automatique, puis sur le premier périphérique et enfin sur le second périphérique. En commençant par le « cloud », connectez chaque périphérique en fonction de la logique de câblage.

Faire valider par le professeur

2ème Partie : Modèle OSI

Objectifs pédagogiques

- configuration IP
- serveur HTTP
- étude de la manière dont PacketTracer utilise le modèle OSI et les protocoles TCP/IP ;
- étude du traitement et du contenu des paquets.

Présentation :

En mode simulation de PacketTracer, des informations détaillées sur les paquets et leur traitement par des périphériques réseau peuvent être affichées. Les protocoles TCP/IP courants son modélisés dans PacketTracer, y compris les protocoles DNS, HTTP, TFTP, DHCP, Telnet, TCP, UDP, ICMP et IP. La manière dont ces protocoles sont utilisés par des périphériques réseau pour créer et traiter des paquets est affichée dans PacketTracer, à l'aide d'une représentation du modèle OSI. Le terme unité de données de protocole, ou PDU, correspond à une description générique des éléments identifiés comme des segments sur la couche transport, des paquets sur la couche réseau et des trames sur la couche liaison de données.

1°) Tâche 1 : Exploration de l'interface de PacketTracer

1.1°) Ouverture d'un fichier de simulation

Dans les fichiers ressources, ouvrir le fichier : « 2-modele-OSI.pka ». Ce fichier contient un schéma déjà saisi ainsi qu'une fenêtre « PT activity » qui reprend le texte de TP et qui permet de vérifier le travail réalisé.

1.2°) Étape 1. Étude des fichiers d'aide et des didacticiels

À partir du menu déroulant, choisissez Help->Contents. Une page Web s'ouvre. Dans la trame de gauche, choisissez Operating Modes->Simulation Mode. Si vous n'êtes pas encore familier avec le mode simulation, consultez la documentation relative à ce mode.

Traduire la partie suivante de la documentation :

« In Simulation Mode, you can watch your network run at a slower pace, observing the paths that packets take and inspecting them in detail. When you switch to Simulation Mode, the Simulation Panel will appear. You can graphically create PDUs to send between devices using the Add Simple PDU button and then pressing the Auto Capture / Play button to start the simulation scenario. The Event List window records (or "captures") what happens as your PDU propagates through the network. You can control the speed of the simulation by using the Play Speed Slider. Pressing the Auto Capture / Play toggle button again will pause the simulation. If you need greater control of the simulation, use Capture / Forward button to manually run the simulation forward one step in time. You can use the Back button to revisit a previous timeframe and view the events that occurred then."

1.3°) Étape 2. Utilisation du mode temps réel

1.3.1°) Cliquez sur l'ordinateur du client Web. Choisissez l'onglet Desktop. Ouvrez le navigateur Web. Entrez l'adresse IP du serveur Web dans le navigateur, 192.168.1.254. Lorsque vous cliquez sur Go, une demande est envoyée au serveur Web.

1.3.2°) Expliquer ce qu'il vient de ce passer.

1.3.3°) Modifier l'adresse IP du serveur (172.17.7.252) et relancer une requête HTTP à la nouvelle adresse. Pourquoi cela ne fonctionne plus ? Modifier la configuration pour que cela fonctionne avec le serveur à cette adresse.

1.3.4°) Dans la configuration du serveur supprimer le service HTTP et refaire la

manipulation. Que ce passe-t-il ?

1.3.5°) Sans relancer le service HTTP, relancer une requête HTTPS sur l'adresse du serveur. Cela fonctionne t'il ? Pourquoi ?

1.3.6°) Donner la différence entre les protocoles HTTP et HTTPS.

1.3.7°) Replacer l'ensemble des configurations comme au début du TP (adresse IP, Services..)

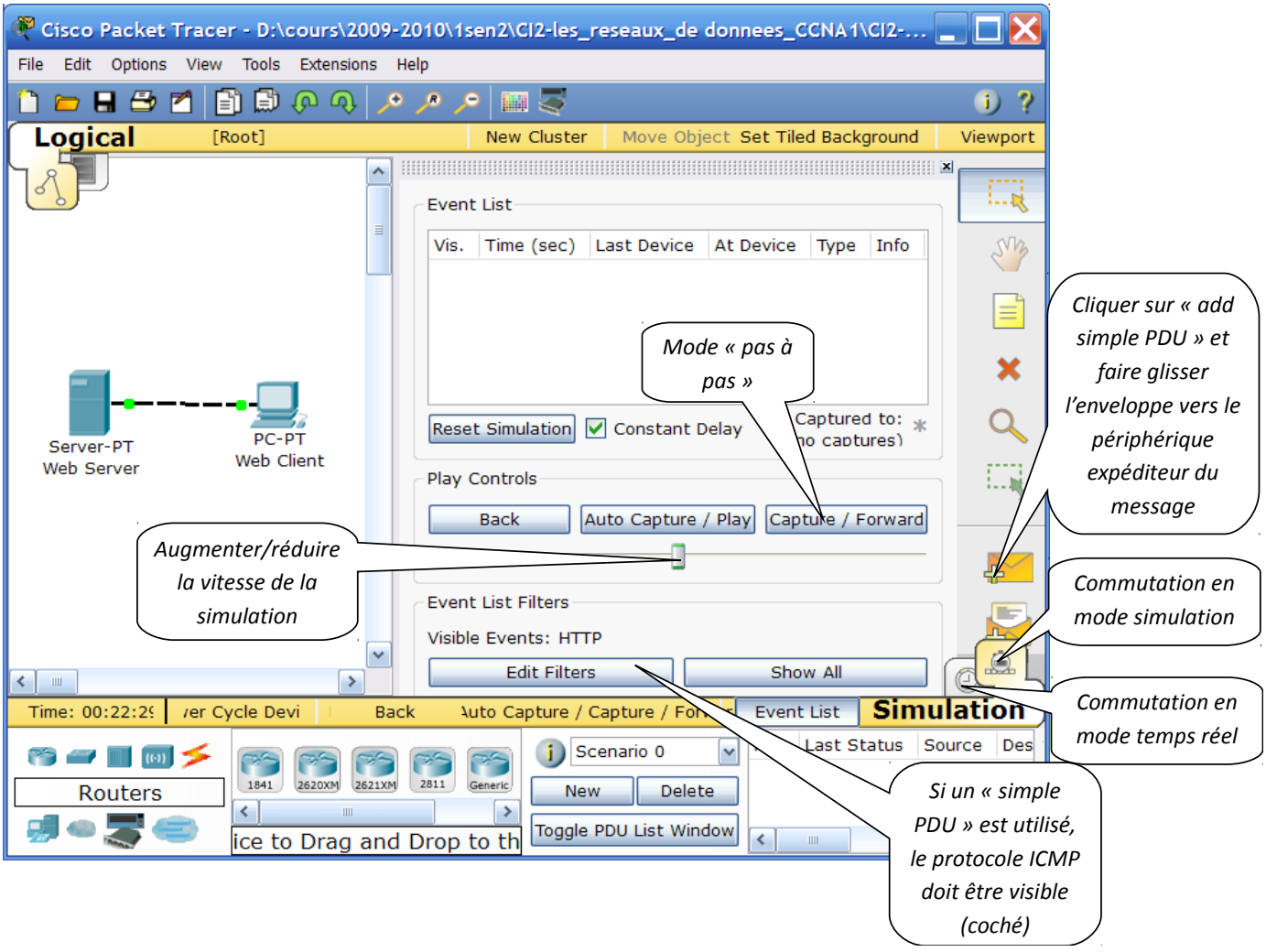
Faire valider par le professeur

2°) Tâche 2 : Examen du contenu et du traitement de paquet

2.1°) Étape 1. Passage du mode temps réel au mode simulation

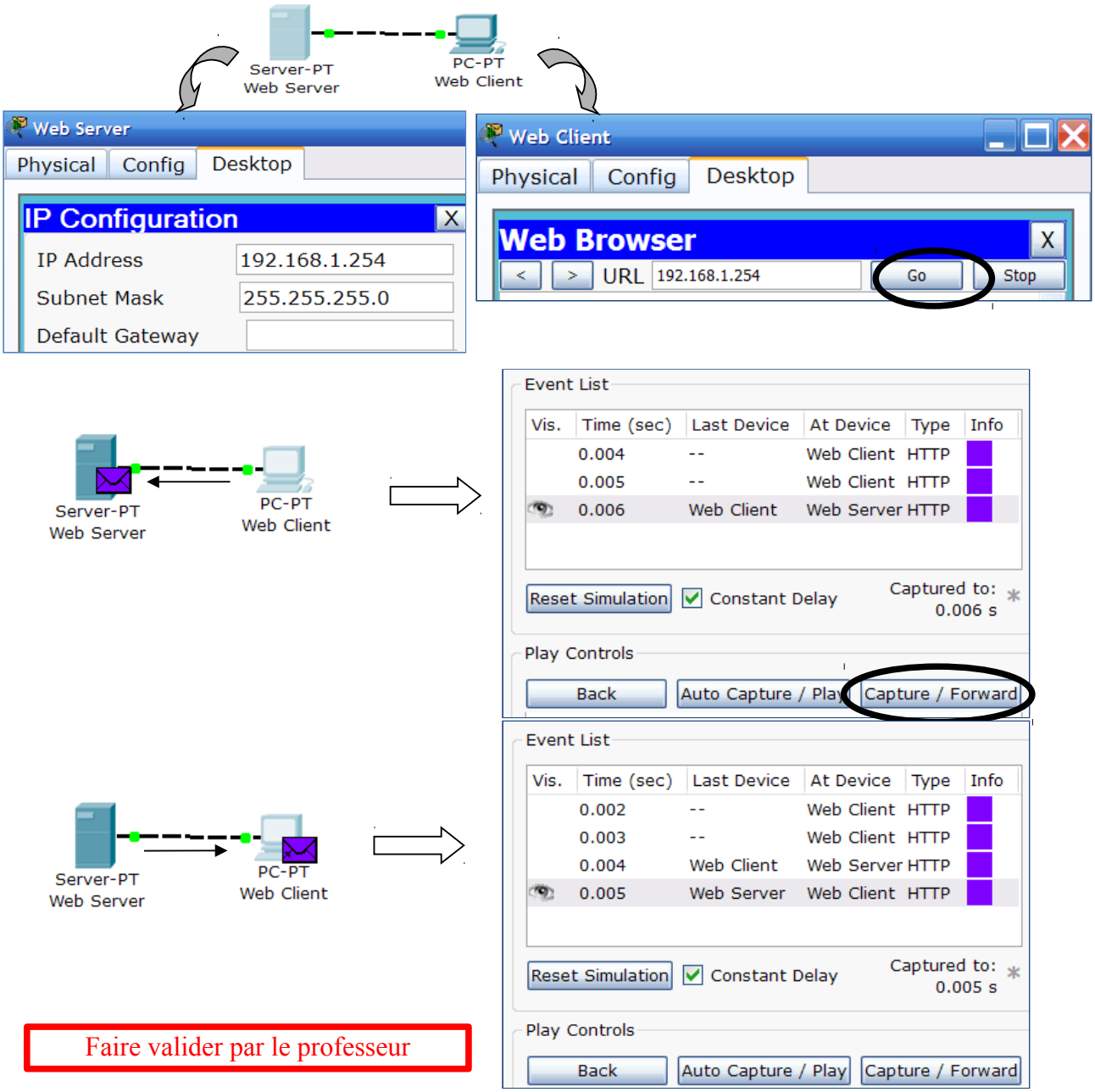
La partie inférieure droite de l'interface de PacketTracer comprend le commutateur mode temps réel/mode simulation. PacketTracer démarre toujours en mode temps réel, dans lequel les protocoles réseau fonctionnent avec des temporisations réalistes. Cependant, une fonctionnalité puissante de PacketTracer permet à l'utilisateur d'« arrêter le temps » en basculant vers le mode simulation. En mode simulation, les paquets sont affichés en tant qu'enveloppes animées, le temps est basé sur les événements et l'utilisateur peut parcourir les événements réseau.

=> Ce placer en mode simulation.



2.2°) Étape 2. Création d'un paquet et accès à la fenêtre PDU Information.

Réduisez la fenêtre de configuration du client Web. Le temps étant basé sur des événements dans la simulation, vous devez utiliser le bouton Capture/Forward pour afficher des événements réseau. Deux paquets apparaissent dans la liste d'événements et un œil apparaît à côté de l'un d'entre eux. Lorsqu'un œil apparaît à côté d'un paquet, cela signifie qu'il est affiché en tant qu'enveloppe sur la topologie logique. Recherchez le premier paquet dans Event List, puis cliquez sur le carré coloré dans la colonne Info. *Suivre le schéma ci-dessous.*

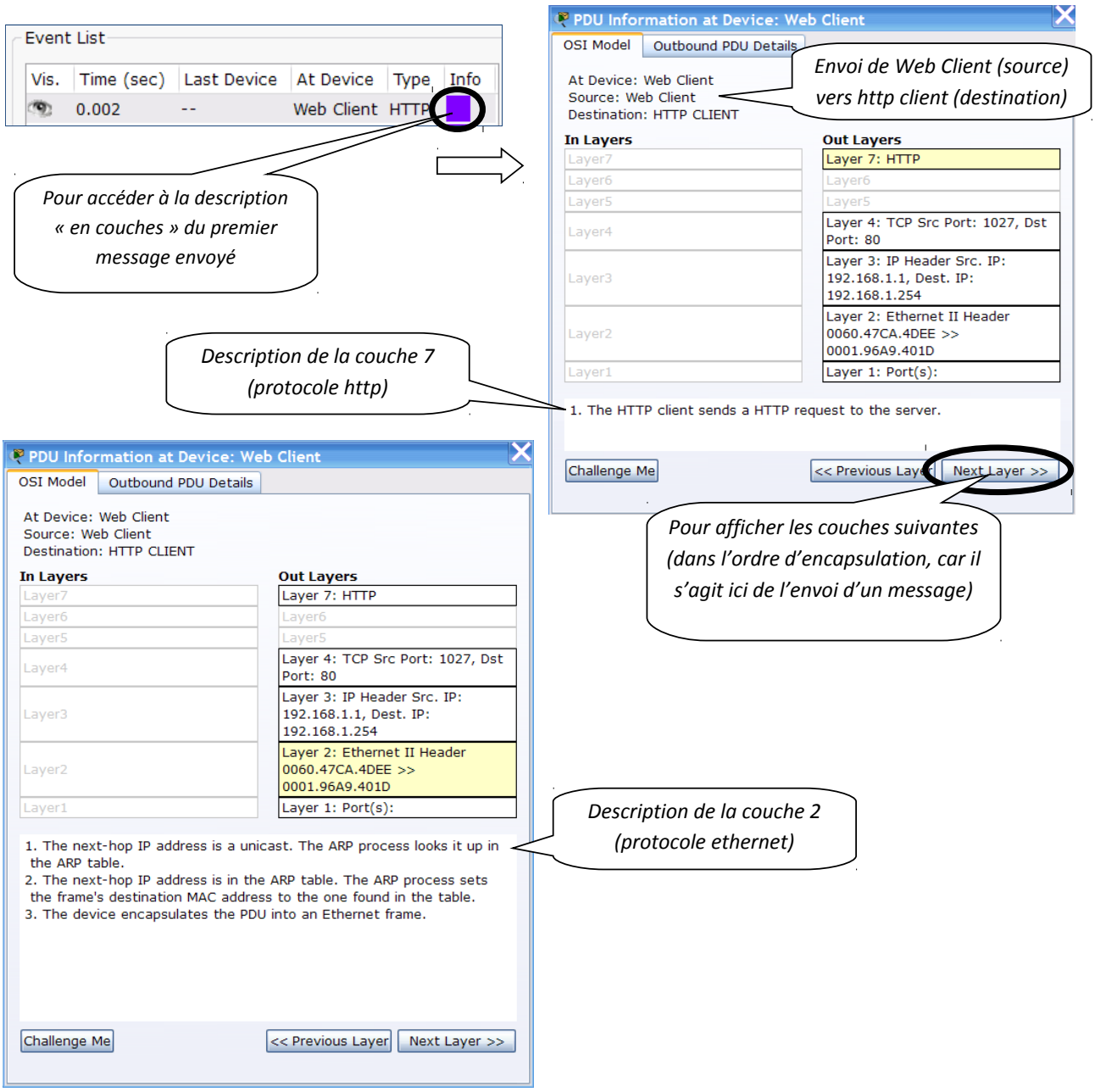


Faire valider par le professeur

2.3°) **<u>Étape 3. Analyse des algorithmes de périphérique dans l'affichage OSI Model</u>**

Lorsque vous cliquez sur le carré Info d'un paquet dans la liste d'événements ou équivalent (*voir le schéma ci-dessous)*, vous cliquez sur une enveloppe de paquet affichée sur la topologie logique ; la fenêtre « PDU Information » apparaît. Le modèle OSI organise cette fenêtre. Dans le cas du premier paquet affiché, notez que la demande HTTP (à la couche 7) est ensuite encapsulée successivement aux couches 4, 3, 2 et 1. Si vous cliquez sur ces couches, l'algorithme utilisé par le périphérique (dans ce cas, l'ordinateur) est affiché. Observez ce qui se produit à chaque couche ; il en sera question pendant la majeure partie du reste de ce TP.

2.3.1°) Définir ce qu'est le modèle OSI
2.3.2°) Donner le nom et le rôle de chaque couche. Faire un schéma représentant les couches.
2.3.3°) Le modèle TCP/IP n'utilise que 4 couches. Donner lesquels.



2.4°) **<u>Étape 4. Unités de données de protocole entrantes et sortantes</u>**

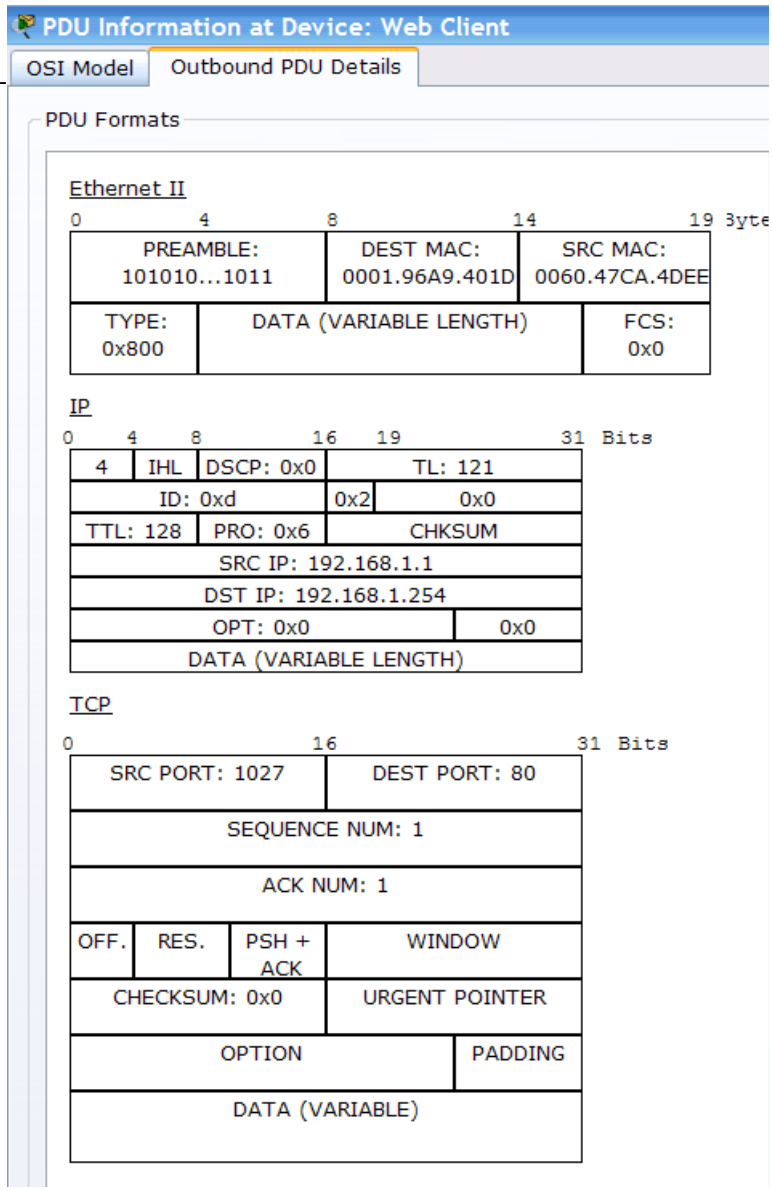
Lors de l'ouverture de la fenêtre PDU Information, l'affichage par défaut est « OSI Model ». Cliquez maintenant sur l'onglet « Outbound PDU Details ». Faites défiler l'affichage jusqu'au bas de cette fenêtre. À cet emplacement, vous apercevez que le protocole HTTP (la demande de page Web qui a démarré cette série d'événements) est encapsulé sous forme de données dans un segment TCP, qui à son tour est encapsulé dans un paquet IP, lui-même encapsulé dans une trame Ethernet, elle-même transmise sous forme de bits sur le support. Si un périphérique constitue le premier périphérique impliqué dans une série d'événements, les paquets qui se trouvent à ce périphérique ne disposent que d'un onglet Outbound PDU Details (Outbound = correspond à un envoi) ; si un périphérique est le dernier périphérique dans une série d'événements, les paquets qui se trouvent à ce périphérique ne disposent que d'un onglet Inbound PDU Details (Inbound = correspond à une réception).

En général, vous apercevez les détails d'unités de données de protocole sortantes et entrantes, qui fournissent des informations sur la manière dont Packet Tracer modélise ce périphérique.

2.4.1°) Expliquer le mot *encapsulation* à partir du schéma "Encapsulation.jpg".

2.5°) Étape 5. Traçage de paquet : animations de flux de paquets

Lors de la première animation de paquets, vous capturez les paquets, comme dans un analyseur de protocole. Ainsi, le bouton Capture/Forward signifie « Capturer » un ensemble d'événements à la fois. Parcourez la demande de page Web pas à pas. Notez que vous affichez uniquement les paquets associés à HTTP, mais que d'autres protocoles, tels que TCP et ARP, possèdent également des paquets qui ne sont pas affichés. Lors de votre capture de paquets, vous pouvez ouvrir la fenêtre PDU Information à n'importe quel moment. Parcourez la totalité de l'animation, jusqu'à ce que le message « No More Events » apparaisse. Familiarisez-vous avec ce processus de traçage de paquet en exécutant à nouveau l'animation, en analysant les paquets, en prévoyant ce qui doit se passer ensuite et en analysant vos prévisions.



2.5.1°) Modifier l'adresse MAC du PC « web client » en « *EEEE.EEEE.EEEE* » et rechercher dans la trame Ethernet ou apparaît cette adresse.

2.5.2°) Cette adresse MAC apparaît elle dans les protocoles IP, TCP ou HTTP ? Pourquoi ?

Faire valider par le professeur

3ème Partie : Création d'un petit réseau

Objectifs pédagogiques :

- identification correcte des câbles à utiliser sur le réseau ;
- câblage physique d'un réseau d'égal à égal ;
- vérification de la connectivité de base sur chaque réseau.

Matériel nécessaire :

- 2 ordinateurs
- 1 câble RJ45 croisé
- 2 câbles RJ45 droit.
- 1 concentrateur ou 1 commutateur.

Simulation avec Packet tracer

1°) **Tâche1 : Création d'un réseau d'égal à égal**

1.1°) Ouvrir le fichier « 3-creation-petit-reseau.pka »

1.2°) Lire la première puis la deuxième page de présentation de la fenêtre PT-Activity.

1.3°) Packet tracer permet, comme on l'a vu précédemment, de vérifier le travail effectué.

=> Cliquer sur le bouton « Check result » pour voir ou vous en êtes.

=> Comme vous n'avez rien branché le résultat doit être :

This activity is incomplete, please try again.

=> Vérifier dans « assessment items » qu'il n'y a encore rien de correct.

2°) **Tâche2 : Identification des câbles utilisés dans un réseau**

2.1°) Lire la troisième page de la fenêtre PT-Activity.

2.2°) Choisir le bon câble.

2.3°) Faire la connexion en mode manuel, avec le bon câble,

2.3.1°) Cliquer sur le bouton « Check result » pour voir ou vous en êtes. Y a t'il des choses correctes ?

2.3.2°) Pour voir la différence de comportement du simulateur faire la connexion en mode manuel avec le mauvais câble. Y a t'il un moyen de repérer que l'on utilise le mauvais câble ? Cliquer sur le bouton « Check result » . Y a t'il des choses correctes ?

3°) **Tâche3 : Configuration d'adresses et test**

3.1°) Lire la troisième page de la fenêtre PT-Activity.

3.2°) Faire les activités de la tâche 3 sur le simulateur **et sur les ordinateurs**.

3.3°) Après avoir configuré l'@IP et avant de taper la commande « ping », vérifier cette @IP en tapant « ipconfig » dans la fenêtre de commande.

3.4°) Observer le résultat de la commande « ping ». Le dialogue est-il possible ?

À la fin de cette tâche, votre taux de réalisation devrait être de 100%.

Faire valider par le professeur

4°) **Tâche4 : Ajout d'un commutateur**

- Modifier le câblage de manière à connecter PC1 et PC2 par l'intermédiaire d'un commutateur (utiliser les bons câbles).
- Depuis le PC2, faire un ping de PC1. Assurez vous que le dialogue soit possible.
- Ajouter PC3 et PC4 (sur PacketTracer uniquement) et leur attribuer les @IP 192.168.1.4 et 192.168.1.5. Vérifier ces adresses avec la commande ipconfig.

- Attendre que le commutateur fasse l'auto-apprentissage des adresses MAC des PC qui lui sont connectés (connexions en vert).
- Passer du mode temps réel au mode simulation.
- Faire « Edit Filters » et ne conserver que le protocole ICMP (commande ping).
- Envoyer des PDU simples entre les différent PC et vérifier leur bonne réception.
- Observer le cheminement des PDU.

5°) **Tâche5 : Différence entre commutateur et concentrateur**

- Remplacer le commutateur par un concentrateur.
- Rétablir les connexions entre les 4 PC.
- Placez-vous en simulation, avec le protocole ICMP uniquement.
- Envoyer des PDU simples entre es différent PC et vérifier leur bonne réception.
- Observer le cheminement des PDU.

Conclusion :

- Quelle différence y a t'il entre un commutateur et un concentrateur ?
- Pourquoi on préfère utiliser un commutateur (switch) plutôt qu'un concentrateur (hub).

Faire valider par le professeur

6°) **Tâche6 : Test de communication**

- Passer du mode simulation au mode temps réel.

Modifier l'@IP du PC2 : @IP= 172.17.107.100 – masque ss réseau : 255.255.0.0
Modifier l'@IP du PC3 : @IP= 172.17.107.101 – masque ss réseau : 255.255.0.0
Envoyer des PDU entres les PC et vérifier quels PC peuvent dialoguer entre eux.
Compléter le tableau ci-dessous (la communication est elle possible ?) :

Nom Adresse IP Masque sous réseau	PC1 192.168.1.2 255.255.255.0	PC2 172.17.107.100 255.255.0.0	PC3 172.17.107.101 255.255.0.0	PC4 192.168.1.5 255.255.255.0
PC1 192.168.1.2 255.255.255.0				
PC2 172.17.107.100 255.255.0.0				
PC3 172.17.107.101 255.255.0.0				
PC4 192.168.1.5 255.255.255.0				

4ème Partie : Affichage d'un PDU

Objectifs pédagogiques :

- capture d'un ping d'une invite de commandes d'un ordinateur ;
- exécution de la simulation et capture du trafic ;
- examen du trafic capturé ;
- capture d'une demande Web à l'aide d'une URL depuis un ordinateur ;
- exécution de la simulation et capture du trafic ;
- examen du trafic capturé.

Présentation :

Wireshark permet de capturer et d'afficher l'ensemble du trafic réseau entrant et sortant sur l'ordinateur sur lequel il est installé via une interface réseau. Le mode simulation de Packet Tracer capture l'ensemble du trafic réseau qui traverse la totalité du réseau mais prend en charge un nombre limité de protocoles uniquement. Pour reproduire aussi fidèlement que possible la réalité, nous allons utiliser un réseau constitué d'un ordinateur directement relié à un serveur Web, capturer un ping envoyé au serveur depuis l'invite de commandes de l'ordinateur et effectuer une demande de page Web à l'aide d'une URL.

RQ : Au début de cette tâche, votre taux de réalisation devrait être complet. Les périphériques sont configurés et l'objectif de cet exercice est d'examiner le flux de trafic entre des périphériques.

1°) Tâche 1 : capture d'un ping depuis une invite de commandes d'un ordinateur.

1.1°) Étape 1. Exécution de la simulation et capture du trafic.

- Ouvrir le fichier « 4-affichage-pdu.pka »

Dans la partie inférieure droite de l'interface de Packet Tracer figure le commutateur mode temps réel/mode simulation.

- Cliquez sur le mode Simulation.
- Cliquez sur l'ordinateur.
- Choisissez l'onglet Desktop
- Ouvrez l'invite de commandes.
- Entrez la commande ping 192.168.1.2, qui est l'adresse IP du serveur.

Lorsque vous appuyez sur la touche Entrée, quatre requêtes d'écho ICMP sont effectuées.

- Réduisez la fenêtre de configuration de l'ordinateur.

Deux paquets apparaissent dans la liste des événements Event List, la première requête d'écho ICMP et une requête ARP requise pour résoudre l'adresse IP du serveur avec l'adresse MAC de son matériel.

- Cliquez sur le bouton Auto Capture / Play pour exécuter la simulation et capturer des événements.
- Visualisez les « enveloppes » en même temps que les événements dans la list (Event List) et que le déroulement de la commande Ping dans l'invite de commande.
- Une fois que la commande Ping est terminé (les quatre paquets sont envoyés et reçus) re-cliquez sur le bouton Auto Capture / Play pour stopper la simulation.

1.1.1°) Comptez le nombre d'événement créés par cette commande.

Pour ne pas mélanger les PDU, les événements correspondant à chaque PDU sont repérés par une couleur.

1.1.2°) Combien d'événements sont utiles pour le quatrième paquet ? Intègre t'il des commande ARP ?

1.1.3°) Idem pour les deuxième et troisième paquet ?

1.1.4°) A votre avis pourquoi le premier est décomposé en plusieurs partie et comporte t'il des

commande ARP ? *Vous pouvez cliquer sur l'icône « info » pour visualisez les couches couvertes par les commande ARP et ICMP.*

- Dans l'invite de commande, relancer une deuxième fois la commande ping 192.168.1.2
- Analysez une nouvelle fois les événements dans chaque paquet

1.1.5°) Comporte t'elle des commande ARP ? Pourquoi ?

Faire valider par le professeur

1.2°) Étape 2. Examen du trafic capturé.

- Recherchez de nouveau le premier paquet dans Event List,
- Cliquez sur le carré coloré dans la colonne Info.

La fenêtre PDU Information s'ouvre. Le modèle OSI organise cette fenêtre. Dans le cas du premier paquet affiché, notez que la requête d'écho ICMP (à la couche 3) est encapsulée à la couche 2. Si vous cliquez sur chacune de ces couches, l'algorithme utilisé par le périphérique (dans ce cas, l'ordinateur) est affiché.

- Étudiez ce qui se passe sur chaque couche sur les deux première lignes.

Lors de l'ouverture de la fenêtre PDU Information, l'affichage par défaut est OSI Model.

- Cliquez maintenant sur l'onglet Outbound PDU Details.

En faisant défiler l'affichage jusqu'au bas de cette fenêtre, vous constaterez que la requête d'écho ICMP est encapsulée sous forme de données dans un paquet IP.

- Recherchez le premier paquet ARP dans Event List.
- Cliquer sur « info »
- Cliquez maintenant sur l'onglet Outbound PDU Details.

1.2.1°) Noter les adresse IP et MAC de la sources et de la destinations.
1.2.2°) « Qui parle » à « qui » ?

- Recherchez le deuxième paquet ARP dans Event List.
- Cliquez maintenant sur l'onglet Inbound PDU Details.

1.2.3°) Y a t'il une différence entre le « Outbound PDU Details » de la commande précédente (le premier paquet ARP) et le « Inbound PDU Details » de ce deuxième paquet ? Pourquoi ?

- Toujours dans ce deuxième paquet ARP, cliquez maintenant sur l'onglet Outbound PDU Details.

1.2.4°) Noter les adresse IP et MAC de la sources et de la destinations.
1.2.5°) « Qui parle » à « qui » ?
1.2.6°) Qu'apporte cette deuxième commande ARP ?

- Recherchez maintenant le troisième paquet ARP dans Event List.
- Cliquez sur l'onglet Inbound PDU Details.

1.2.7°) Noter les adresse IP et MAC de la sources et de la destinations.
1.2.8°) Conclure sur le rôle des commandes ARP.

Faire valider par le professeur

2°) <u>Tâche 2 : capture d'une demande Web à l'aide d'une URL à partir d'un ordinateur.</u>

2.1°) Étape 1. Exécution de la simulation et capture du trafic.

- Cliquez sur l'ordinateur
- Ouvrez le navigateur Web et entrez www.exemple.com dans le navigateur

Lorsque vous cliquez sur Go, une requête est envoyée au serveur Web.

- Réduisez la fenêtre de configuration du client Web. Un paquet apparaît dans la liste des événements, une requête DNS requise pour résoudre l'URL avec l'adresse IP du serveur.
- Cliquez sur le bouton Auto Capture / Play pour exécuter la simulation et capturer des événements.

- Faire la même manipulation sur deux ordinateurs réels et capturer les même trames DNS avec Wireshark

2.2°) Étape 2. Examen du trafic capturé.

- Examinez les informations d'unités de données de protocole concernant les événements dans cet échange dans Packet Tracer
- Examinez les informations d'unités de données de protocole concernant les événements dans cet échange dans Wireshark
- Comparez Wireshark et Packet Tracer et différenciez-les.

Faire valider par le professeur

Travail supplementaire :

5ème Partie : Analyse d'un paquet IP

Objectifs pédagogiques :

- réalisation de la topologie ;
- ajout d'unités de données de protocole simples en mode temps réel ;
- analyse d'unités de données de protocole en mode simulation ;
- familiarisation avec le modèle de configuration de travaux pratiques standard.

Travail à faire :

- Ouvrir le fichier « 4-affichage-pdu.pka »
- Suivre les instructions données dans la fenètre « PT Activity »

Faire valider par le professeur