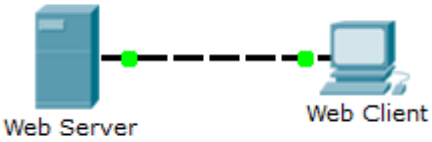
	**Réseaux** ***Analyse des modèles OSI et TCP/IP en action***	**BTS SN IR** ***S21***

Topologie du réseau à analyser :



Objectifs :

Partie 1 : Inspecter le trafic Web HTTP
Partie 2 : Afficher les éléments de la suite de protocoles TCP/IP

Remarque préliminaire :

Les réponses sont à inscrire dans les champs jaunis →[ ]
La taille du champ s'adapte automatiquement au nombre de caractères.

Contexte :

Cet exercice de simulation vise à fournir une base pour comprendre la suite de protocoles TCP/IP et sa relation avec le modèle OSI. Le mode Simulation vous permet d'afficher le contenu de données envoyé sur tout le réseau à chaque couche.

Au fur et à mesure de leur transmission sur le réseau, les données sont divisées en parties plus petites et sont identifiées, afin que ces parties puissent être réassemblées lorsqu'elles arrivent à destination. Chaque partie reçoit un nom spécifique (unité de données de protocole, PDU) et est associée à une couche spécifique des modèles OSI et TCP/IP. Le mode Simulation de Packet Tracer permet d'afficher chacune des couches et la PDU associée. Les étapes suivantes guident l'utilisateur tout au long du processus de demande d'une page Web à partir d'un serveur Web, à l'aide du navigateur Web disponible sur un PC client. Cela permet de visualiser le processus d'encapsulation.

PARTIE 1: CONSTRUIRE LE RÉSEAU

Avec les caractéristiques suivantes, construire le réseau à étudier.

- *Web serveur :* Nom : Web serveur
  Serveur DNS en IP statique: 192.168.1.254
- *Web client :* Nom : Web client
  IP statique : 192.168.1.1

PARTIE 2: INSPECTER LE TRAFIC WEB HTTP

Dans cette partie, vous allez utiliser le mode Simulation de Packet Tracer (PT) pour générer du trafic Web et examiner HTTP.

1. Passez du mode Realtime au mode Simulation.

*Le coin inférieur droit de l'interface de Packet Tracer comporte des onglets permettant de passer du mode **Realtime** au mode **Simulation**. Packet Tracer démarre toujours en mode **Realtime**, dans lequel les protocoles réseau fonctionnent avec des temporisations réalistes. Cependant, une fonctionnalité puissante de Packet Tracer 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.*

1.1. Cliquez sur l'icône du mode **Simulation** pour passer du mode **Realtime** au mode **Simulation**.
1.2. Manipulez le menu Event List et sélectionnez uniquement **HTTP** dans **Event List Filters**

2. Générez le trafic Web (HTTP).

*Le panneau de simulation (Simulation Panel) est actuellement vide. La liste des événements située en haut du panneau de simulation contient six colonnes. Les divers événements apparaissent dans cette liste au fur et à mesure de la génération et de l'acheminement du trafic. La colonne **Info** est utilisée pour examiner le contenu d'un événement.*

2.1. Cliquez sur **Web Client** dans le volet situé le plus à gauche.
2.2. Cliquez sur l'onglet **Desktop**, puis sur l'icône **Web Browser** pour ouvrir le programme.
2.3. Dans le champ URL, entrez **www.osi.local** et cliquez sur **Go**.

*Le mode Simulation étant basé sur les événements, vous devez utiliser le bouton **Capture/Forward** pour afficher les événements réseau.*

2.4. Cliquez à quatre reprises sur **Capture/Forward**. La liste des événements doit comporter quatre événements.
2.5. Accédez à la page du navigateur Web de Web Client. Constatez-vous un quelconque changement ?

➔ Un message s'affiche "You have successfully accessed the home page for Web Server."

3. Explorez le contenu du paquet HTTP.

3.1. Cliquez sur la première case en couleur située sous la colonne **Event List** > **Info**. Vous devrez peut-être développer le **panneau de simulation** ou utiliser la barre de défilement située directement sous la **liste d'événements**.

*La fenêtre **PDU Information at Device: Web Client** s'affiche. Cette fenêtre ne comporte que deux onglets, à savoir **OSI Model** et **Outbound PDU Details**, étant donné que la transmission n'en est qu'à son début. Trois onglets de plus s'afficheront au fur et à mesure que les événements seront examinés, avec l'ajout de l'onglet **Inbound PDU Details**. Pour le dernier événement du flux de trafic, seuls les onglets **OSI Model** et **Inbound PDU Details** s'affichent.*

3.2. Assurez-vous que l'onglet **OSI Model** est sélectionné. Sous la colonne **Out Layers**, vérifiez que la zone **Layer 7** est en surbrillance.
3.3. Quel est le texte affiché à côté de l'étiquette **Layer 7** ?

➔ rien ; The HTTP client sends a HTTP request to the server.

3.4. Quelles informations sont répertoriées dans les étapes numérotées directement sous les zones **In Layers** et **Out Layers** ?

➔ TCP Src Port : 1026, Dst Port : 80

3.5. Cliquez sur **Next Layer**. La couche 4 doit être en surbrillance. Quelle est la valeur **Dst Port** ?

➔ IP Header Src. IP : 192.168.1.1, Dest. IP : 192.168.1.254

3.6. Cliquez sur **Next Layer**. La couche 3 doit être en surbrillance. Quelle est la valeur **Dest. IP** ?

➔ Ethernet II Header 0060.47AC.4DEE >> 0001. 96A9.401D

3.7. Cliquez sur **Next Layer**. Quelles informations sont affichées au niveau de cette couche ?

➔ Port(s) :

3.8. Cliquez sur l'onglet **Outbound PDU Details**.

*Les informations répertoriées sous **PDU Details** reflètent les couches du modèle TCP/IP.*
***Remarque :** les informations affichées dans la section **Ethernet II** fournissent davantage de détails que celles qui figurent sous la zone Layer 2 de l'onglet **OSI Model**. L'onglet **Outbound PDU Details** fournit des informations plus descriptives et détaillées. Les valeurs figurant sous **DEST MAC** et **SRC MAC** dans la section **Ethernet II** de **PDU Details** apparaissent dans l'onglet **OSI Model** sous Layer 2, mais ne sont pas identifiées en tant que telles.*

3.9. Quelles sont les informations répertoriées à la fois dans la section **IP** de **PDU Details** et dans l'onglet **OSI Model** ? À quelle couche ces informations sont-elles associées ?

➔ L'adresse IP source et l'adresse IP destination. Elles correspondent à la couche 2 (Internet) dans le modèle TCP et à la couche 3 (Réseau) dans le modèle OSI.

3.10. Quelles sont les informations répertoriées à la fois dans la section **TCP** de **PDU Details**, et dans l'onglet **OSI Model**, et à quelle couche ces informations sont-elles associées ?

➔ Le port source et le port destination. Elles correspondent à la couche 3 (Transport) dans le modèle TCP et à la couche 4 (Transport) dans le modèle OSI.

3.11. Quelle est la valeur **Host** répertoriée dans la section **HTTP** de **PDU Details** ? À quelle couche ces informations sont-elles associées dans l'onglet **OSI Model** ?

➔ La valeur Host est www.osi.local. Elles sont associées à la couche 7 (Application) du modèle OSI

3.12. Cliquez sur la case en couleur suivante située sous la colonne **Event List** > **Info**. Seule la couche 1 est active (non grisée). Le périphérique prend la trame dans la mémoire tampon et la place sur le réseau.

3.13. Passez à la zone **Info** HTTP suivante dans la **liste des événements** et cliquez sur la case en couleur. Cette fenêtre contient à la fois **In Layers** et **Out Layers**. Notez la direction de la flèche juste sous la colonne **In Layers** ; elle pointe de **In Layers** vers **Out Layers**, indiquant le sens d'acheminement des informations. Faites défiler les différentes couches en observant les éléments précédemment affichés. La flèche située en haut de la colonne pointe vers la droite. Cela indique que le serveur renvoie maintenant les informations au client.

3.14. Lorsque vous comparez les informations affichées dans les colonnes **In Layers** et **Out Layers**, quelles différences remarquez-vous principalement ?

➔ Les adresses sources et destination (MAC et IP) ainsi que les ports sources et destination sont inversés.

3.15. Cliquez sur l'onglet **Outbound PDU Details**. Faites défiler l'écran jusqu'à la section **HTTP**. Quelle est la première ligne du message HTTP qui s'affiche.

➔ C'est : HTTP Data:Connection: close

3.16. Cliquez sur la dernière case en couleur dans la colonne **Info**. Combien d'onglets sont affichés avec cet événement et pourquoi ?

➔ Il y a 2 onglets qui sont affiché car le message vient de revenir au Web Client.

PARTIE 3: AFFICHER LES ÉLÉMENTS DE LA SUITE DE PROTOCOLES TCP/IP

Dans la Partie 3, vous allez utiliser le mode Simulation de Packet Tracer pour afficher et examiner quelques-uns des autres protocoles inclus dans la suite TCP/IP.

1. Afficher les événements supplémentaires

1.1. Fermez toutes les fenêtres d'information liées au protocole PDU.

1.2. Dans la section Event List Filters > Visible Events, cliquez sur Show All. Quels types d'événements supplémentaires sont affichés ?

➔ Il y a DNS et TCP.

Ces entrées supplémentaires jouent divers rôles au sein de la suite TCP/IP. Si le protocole ARP (Address Resolution Protocol) est indiqué, il recherche des adresses MAC. Le protocole DNS est chargé de la conversion d'un nom (par exemple, www.osi.local) en adresse IP. Les événements TCP supplémentaires sont responsables de la connexion, de la configuration des paramètres de transmission et de la déconnexion des sessions de communication entre les périphériques. Il existe actuellement plus de 35 protocoles possibles (types d'événements) disponibles pour la capture dans Packet Tracer.

1.3. Cliquez sur le premier événement DNS dans la colonne **Info**. Examinez les onglets **OSI Model** et **Outbound PDU Details**, et observez le processus d'encapsulation. Pendant que vous examinez l'onglet **OSI Model** avec la zone **Layer 7** en surbrillance, une description de ce qui se passe s'affiche directement sous **In Layers** et **Out Layers** (« 1. Le client DNS envoie une requête DNS au serveur DNS. »). Il s'agit d'informations très utiles pour mieux comprendre ce qui se produit durant le processus de communication.

1.4. Cliquez sur l'onglet **Outbound PDU Details**. Quelles informations sont répertoriées dans la zone **NAME:** de la section **DNS QUERY** ?

➔ C'est : www.osi.local

1.5. Cliquez sur la dernière case en couleur **Info DNS** dans la liste des événements. Quel périphérique est affiché ?

➔ C'est : Web Client ; 1.6. 192.168.1.254 ; 1.7. 4. The TCP connection is successful.
5. The device sets the connection state to ESTABLISHED ; 1.8. 4. The device sets the connection state to CLOSING.

1.6. Quelle est la valeur indiquée en regard de la **zone ADDRESS:** de la section **DNS ANSWER** de l'onglet **Inbound PDU Details** ?

1.7. Recherchez le premier événement **HTTP** de la liste, et cliquez sur la case en couleur de l'événement **TCP** situé juste après. Mettez en surbrillance **Layer 4** sur l'onglet **OSI Model**. Dans la liste numérotée située directement sous **In Layers** et **Out Layers**, quelles sont les informations affichées sous les points 4 et 5 ?

Entre autres tâches, TCP gère la connexion et la déconnexion du canal de communication. Cet événement particulier indique que le canal de communication est à l'état ESTABLISHED.

1.8. Cliquez sur le dernier événement **TCP**. Mettez en surbrillance **Layer 4** sur l'onglet **OSI Model**. Examinez les étapes répertoriées directement sous **In Layers** et **Out Layers**. Quel est le rôle de cet

événement, sur la base des informations fournies dans le dernier élément de la liste (il doit s'agir du point 4) ?

PARTIE 4: SYNTHESE

Cette simulation a illustré un exemple de session Web entre un client et un serveur sur un réseau local (LAN). Le client envoie des requêtes à des services spécifiques s'exécutant sur le serveur. Le serveur doit être configuré de manière à écouter sur des ports spécifiques en cas de requête du client.

➢ Sur la base des informations collectées durant la capture dans Packet Tracer, compléter les informations du tableau suivant.

	Requête HTTP	***Requête DNS***	***Requête TCP***
N° de port écouté par le Serveur Web			
	80	53	80
N° de port écouté par le Client WEB			
	1028	1027	1027
Protocole TCP mis en œuvre			
	HTTP	DNS	TCP
Nbre de couches du modèle OSI concernées lors d'une communication ***Web serveur <-> Web client***			
	5	5	5
Couche du modèle TCP/IP associée			
	7	7	4

➢ Ré-ouvrir (File/Open) le modèle packet tracer.
➢ En reprenant la démarche de la Partie 2/Question 2, rendre visible tous les protocoles et effectuer une requête ping du Web client vers le Web serveur
➢ Compléter les informations dans le tableau ci-dessous pour chaque ***Web serveur <-> Web client*** requête mise en œuvre.

Commande **ping** du Web client vers Web serveur	
Adresse IP du Web client	192.168.1.1
Adresse IP du Web serveur	192.168.1.254
1ère Requête ***Web serveur <-> Web client*** *mise en œuvre*	
Nom du protocole	ICMP
N° de port écouté par le Serveur Web	53
N° de port écouté par le Client WEB	1028
Nbre de couches du modèle OSI concernées lors d'une communication Web serveur <-> Web client	1
Protocole TCP mis en œuvre	ICMP
Couche du modèle TCP/IP associée	2 (Internet)
2ième Requête ***Web serveur <-> Web client*** *mise en œuvre*	
Nom du protocole	ICMP
N° de port écouté par le Serveur Web	53
N° de port écouté par le Client WEB	1028
Nbre de couches du modèle OSI concernées lors d'une communication Web serveur <-> Web client	1
Protocole TCP mis en œuvre	ICMP
Couche du modèle TCP/IP associée	2 (Internet)