TP3 : Couche Transport : Installation d'un serveur HTTP

Objectifs pédagogiques

- Explorer le mode Real-time de Packet Tracer
- Explorer la zone Logical Workplace
- Explorer le fonctionnement de Packet Tracer
- Connecter les périphériques
- Examiner la configuration d'un périphérique
- Analyser la configuration de travaux pratiques type
- Vue d'ensemble des périphériques

A fin d'arriver à ces objectifs, on doit réaliser les activités et la maquette

I. Les activités

I.1: Etablissement d'une session TCP (charger le fichier 4.2.5.2.pka)

TCP est un protocole orienté connexion. Avant d'informations, comme une page Web, peuvent être échangés, les pairs doit établir une connexion. Une connexion est établie par une poignée de main à trois voies où les numéros de séquence initiale pour les deux pairs sont envoyés et reçus. Lorsque l'échange est terminé, les pairs de change les segments TCP à mettre fin à la session correctement. L'activité précédente axée sur l'échange réel de segments TCP. Cette activité se concentrera sur l'établissement de connexion avant l'échange et la fin d'une session à la suite de l'échange.

Tâche 1: Configurer et exécuter la simulation

étape 1. Entrer simulation mode

Pour vérifier la connexion, cliquez sur le PC dans la zone de travail logique. Ouvrez le **Web Browser** sur le **Desktop**. Entrer 192.168.1.2 dans le champ URL et cliquez sur le bouton **Go**. La page web doit apparaître. Cliquez sur l'onglet **Simulation** pour entrer en mode de simulation

étape 2. définir les filters et la liste des événements

Nous voulons capturer uniquement les événements TCP. Dans la liste des événements **Event List Filters**, cliquez sur le bouton **Edit Filters**. Sélectionnez uniquement les événements TCP. Événements. Inclure les applications HTTP et Telnet .

étape 3. Demande une page web de PC

Restaurer la fenêtre du navigateur Web. Dans **Web Browser**, cliquez sur le bouton **Go** pour demander que la page web sera renvoyée. Réduire la fenêtre du navigateur simulé.

étape 4. exécution de simulation

Cliquez sur **Auto Capture / Play** . L'échange entre le PC et le serveur est animée et les événements sont ajoutés à **Event List**. Ces événements représentent la mise en place de la session TCP, la demande de la PC pour la page Web, le serveur d'envoi de la page Web en deux segments, le PC en reconnaissant la page web, et la fin de la session TCP. Une boîte de dialogue s'affiche, indiquant il ya des événements pas plus. Cliquez sur **OK** pour le fermer.

Tâche 2: Examiner les résultats

Étape1. Accès PDU spécifiques

Dans la section **Simulation Panel Event List** , la dernière colonne contient une case de couleur qui donne accès à des informations détaillées sur un événement. Cliquez sur la case de couleur dans la dernière colonne pour le premier événement. La fenêtre **PDU Information** s'ouvre.

Étape2. Examiner le contenu de la fenêtre PDU Information

Dans cette activité, nous allons nous concentrer uniquement sur les informations d'événement uniquement à la couche 4. Le premier onglet dans la fenêtre **PDU Information** contient des informations sur le PDU entrant et sortant en ce qui concerne le modèle OSI. Cliquez sur **Layer 4**: boîtes pour les deux couches les entrants et sortants et lire le contenu de la boîte et la description dans la case ci-dessous les couches. Faites attention au type de segment TCP. Cliquez sur **Outbound PDU Details**. Dans le segment TCP, notez le numéro de séquence initial.

Examiner les informations PDU pour les premiers événements TCP quatre de la même façon. Ces événements montrent la poignée de main à trois voies qui établit la session. Noter le type de segment TCP et le changement du nombre de séquence.

Examiner les informations PDU pour les événements TCP qui suivent l'échange principale HTTP de la même façon. Ces événements montrent la fin de session. Noter le type de segment TCP et le changement du nombre de séquence.

Notez que si vous utilisez le bouton **Reset Simulation** dans la fenêtre **Event List** , vous devrez retourner à la fenêtre du navigateur Web et appuyez sur **Go** de faire une nouvelle demande.

I.2: Numéros de ports TCP et UDP (charger le fichier 4.1.6.2.pka)

UDP et TCP sont des protocoles TCP / IP qui correspondent à la couche OSI 4, la couche transport. Les PDU pour UDP et TCP diffèrent sensiblement, mais ils partagent la notion de numéros de port. Segments contiennent les numéros de port qui permettent d'identifier le service demandé par le client à partir du serveur et les numéros de port générés par le client pour lequel le serveur doit répondre. En plus de numéros de port, le segment TCP contient également des numéros de séquence. Les numéros de séquence offrent une fiabilité en identifiant les segments manquants et en permettant le remontage des données d'application, en mettant les segments de retour ensemble dans le bon ordre.

Tâche 1: Configuration et exécution de simulation

étape 1. Entrer en simulation mode

Cliquer sur **Simulation** pour entrer en simulation mode.
.

étape 2. définir les filters et la liste des événements

Nous voulons capturer uniquement les événements DNS et HTTP. Dans la liste des événements **Event List Filters**, cliquez sur le bouton **Edit Filters**. Sélectionnez uniquement les événements HTTP et DNS .

étape 3. De PC, demande une page web de Server

Cliquer sur le PC dans logical workplace. Ouvre **Web Browser** sur **Desktop**.
Taper **udptcpexample.com** dans l'URL et cliquer sur **Go**. Réduire la fenêtre de simulateur.

étape 4. exécution de simulation

Cliquez sur **Auto Capture / Play** . L'échange entre le PC et le serveur est animée et les événements sont ajoutés à **Event List**. Ces événements représentent une demande de PC client d'un service DNS, suivie par une demande de la page Web, le serveur d'envoi de la page Web en deux segments, le PC en reconnaissant la page web. Une boîte de dialogue s'affiche, indiquant il y a pas plus des événements d'être capturés. Cliquez sur **OK** pour le fermer.

Tâche 2: Examiner les résultats

Étape1. Accès PDU spécifiques

Dans la section **Simulation Panel Event List** , la dernière colonne contient une case de couleur qui donne accès à des informations détaillées sur un événement. Cliquez sur la case de couleur dans la dernière colonne pour le premier événement. La fenêtre **PDU Information** s'ouvre.

Étape2. Examiner le contenu de la fenêtre PDU Information

Dans cette activité, nous allons nous concentrer uniquement sur les informations d'événement uniquement à la couche 4 et à la couche 7. Le premier onglet dans la fenêtre **PDU Information** contient des informations sur le PDU entrant et sortant en ce qui concerne le modèle OSI. Cliquez sur **Layer 4 et Layer 7**: boîtes pour les deux couches les entrants et sortants et lire le contenu de la boîte et la description dans la zone en dessous des couches. Notez que le serveur DNS utilise UDP et HTTP utilise le protocole TCP.

Faites attention aux numéros de port. Port 53 représente DNS, le protocole d'application qui associe de domaine noms avec des adresses IP. Port 80 HTTP représente le protocole d'application qui prend en charge les pages Web. L'autre port est généré par l'ordinateur client dans la gamme de numéros de port supérieur à 1023. Cliquez sur **Outbound PDU Details**. Dans le segment TCP, notez le numéro de séquence initial.

Examiner les informations PDU pour les autres événements de la même façon. Noter la modification de la source et numéros de port de destination (par UDP et TCP) et la variation du nombre de séquence (TCP pour seulement) que le segment suivant est rendu.

Notez que si vous utilisez le bouton **Reset Simulation** , vous devez également retourner à la fenêtre du navigateur et appuyez sur Entrée pour ré-émettre la demande de page Web. Cela vous permettra de re-capturer et d'animer le DNS et HTTP générés par paquets.

I.3: Analyse des couches Application et Transport (charger le fichier 4.6.1.3.pka)

La topologie partielle donnée; devrait être complétée.

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	**Fa0/0**	192.168.254.253	255.255.255.0	N/A
	S0/0/0	10.10.10.6	255.255.255.252	
R2-Central	**Fa0/0**	172.16.255.254	255.255.0.0	N/A
	S0/0/0	10.10.10.5	255.255.255.252	
S1-Central	**VLAN 1**	172.16.254.1	255.255.0.0	172.16.255.254
PC 1A	**NIC**	172.16.1.1	255.255.0.0	172.16.255.254

PC 1B	**NIC**	172.16.1.2	255.255.0.0	172.16.255.254
Eagle Server	**NIC**	192.168.254.254	255.255.255.0	192.168.254.253

Task 1: Compléter et tester la topologie

.

Le serveur a été remplacé. Configurez-le avec les paramètres suivants: Adresse IP 192.168.254.254, masque de sous réseau 255.255.255.0, la passerelle par défaut 192.168.254.253, DNS est activé, avec l'association des "eagle-server.example.com" (sans les guillemets) avec l'IP du serveur adresse, HTTP activé. Branchez Eagle Server au port Fa0 / 0 sur le routeur R1-ISP.

PC 1A a perdu son adresse IP. Configurez-le avec les paramètres suivants: Adresse IP 172.16.1.1, 255.255.0.0 Masque de sous réseau, passerelle par défaut 172.16.255.254 et serveur DNS 192.168.254.254. Connecter le PC 1A au port Fa0 / 1 du commutateur S1-Central.

Vérifiez votre travail en utilisant la rétroaction du Resultsbutton Check et l'onglet évaluation Articles. Test de la connectivité, en temps réel, en utilisant Ajout PDU SIMPLE pour tester la connectivité entre le PC 1A et le Eagle Server.

Notez que lorsque vous ajoutez un PDU simple, il apparaît dans la fenêtre Liste des PDU dans le cadre de «scénario 0». La première fois que vous émettez ce message ping, il sera considéré comme Échec **Failed** - c'est parce que le processus de ARP ce qui sera expliqué plus tard. Double cliquer sur le "feu" dans la fenêtre Liste des PDU, envoyer ce seul test de ping une seconde fois. Cette fois, il sera couronné de succès. Dans Packet Tracer, le terme «scénario» signifie une configuration spécifique d'un ou plusieurs paquets de test. Vous pouvez créer différents scénarios de paquets de test en utilisant le bouton **New**- par exemple scénario 0 pourrait en avoir un paquet de test à partir du PC 1A à Eagle Server; Scénario 1 pourrait tester les paquets entre 1B PC et les routeurs ... Vous pouvez supprimer tous les paquets de test dans un scénario particulier en utilisant le bouton **Delete**. Par exemple, si vous utilisez le **Delete Button** pour le scénario 0, le paquet de test, vous venez de créer entre le PC 1A et Eagle Server sera supprimé - s'il vous plaît le faire avant la prochaine tâche

Tâche 2: Découvrez Comment DNS, UDP, http et TCP travaillent ensemble

Passez du temps réel en mode simulation. Assurez-vous que l'événement filtre est configuré pour afficher DNS, UDP, HTTP, TCP et ICMP. Ouvrez un navigateur Web depuis le bureau de 1A. Tapez l'adresse URL eagle-server.example.com, appuyez sur Entrée, puis d'utiliser **Capture / Forward** Suivant dans **Event List** pour capturer l'interaction de DNS, UDP, HTTP et TCP.

Vous pouvez examiner le paquet de deux manières: en cliquant sur l'enveloppe de paquet tel qu'il est affiché dans l'animation, ou en cliquant sur la colonne **info** de cette instance paquet comme il est répertorié dans **Event List**. faire cette animation et examiner le contenu de paquets (**PDU Information** Window, **Inbound PDU Details, Outbound PDU Details**) pour chaque événement de la liste des événements, surtout quand les paquets sont à PC 1A ou à l'Eagle Server. Si vous recevez un "tampon complète" message, cliquez sur le bouton **View Previous Events** . Alors que le traitement des paquets au niveau du commutateur et les routeurs ne peuvent pas faire sens pour vous encore, vous devriez être en mesure de voir comment DNS, UDP, HTTP, TCP et travailler ensemble en traçant les paquets et l'utilisation de la fenêtre Informations PDU à regarder "l'intérieur "entre eux.

Reflexion:

Pouvez-vous faire un schéma de la séquence d'événements protocolaires à suivre pour demander une page Web en utilisant une URL? Où pourrait les choses tournent mal? Comparer et contraster DNS et HTTP et UDP et TCP.

II. La maquette HTTP

Cette maquette a pour but de faire découvrir aux élèves l'intégration et le fonctionnement d'un serveur en local et a distance.

Capture de trames
Analyse des communications entre les divers équipements lors des échanges avec le serveur http
Mise en évidence du fonctionnement d'un serveur HTTP en local
Mise en évidence du fonctionnement d'un serveur HTTP à distance

Matériel nécessaire

Cette maquette est réalisable avec 2 commutateurs, 2 routeurs, 2 postes/commutateur et 1 serveur

Pré-requis

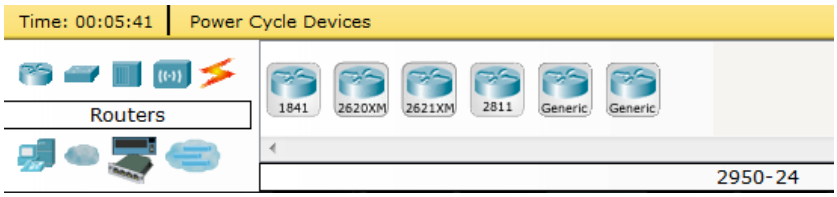
Les connaissances suivantes devront être maîtrisées afin de suivre cette procédure :

- Comprendre le modèle OSI
- Connaissances de l'environnement cisco
- Connaissance du protocole http
- Configuration d'un routeur Cisco

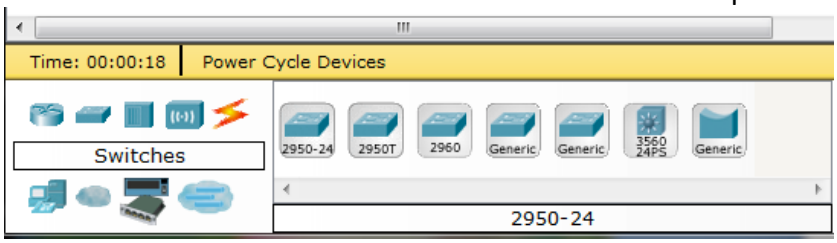
Mise en place

Matériel

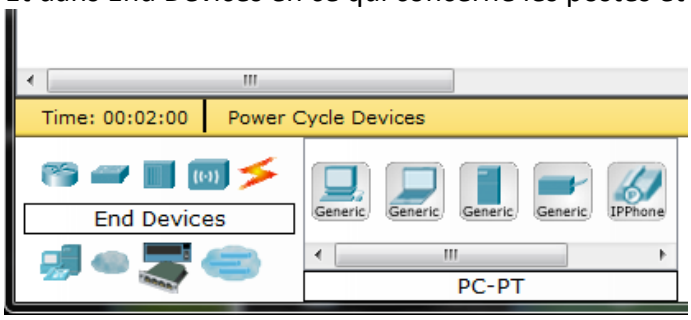
Le matériel nécessaire se situe dans le menu Routers pour sélectionner les routeurs Cisco.



Le matériel nécessaire ce situe dans le matériel Switchs pour le commutateur



Et dans End Devices en ce qui concerne les postes et le serveur



Proposition de plan d'adressage

Le plan d'adressage proposé dans cette procédure est défini ci-dessous :

Le premier poste et le serveur sont sur le réseau 192.168.1.0/24
Le second sur le réseau 192.168.0.0/24
La connexion entre les routeurs est sur un réseau bloqué 10.0.0.0/30

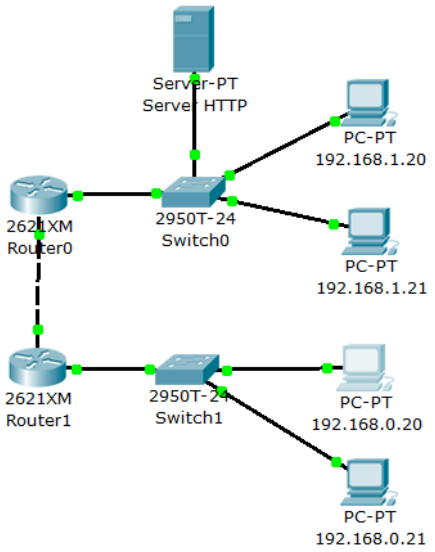
Procédure pas à pas

La maquette est réalisée en 2 étapes :

- La première consiste à réaliser la maquette a proprement parler.
- La seconde à configurer les postes et voir le comportement des paquets sur un réseau

Etape 1

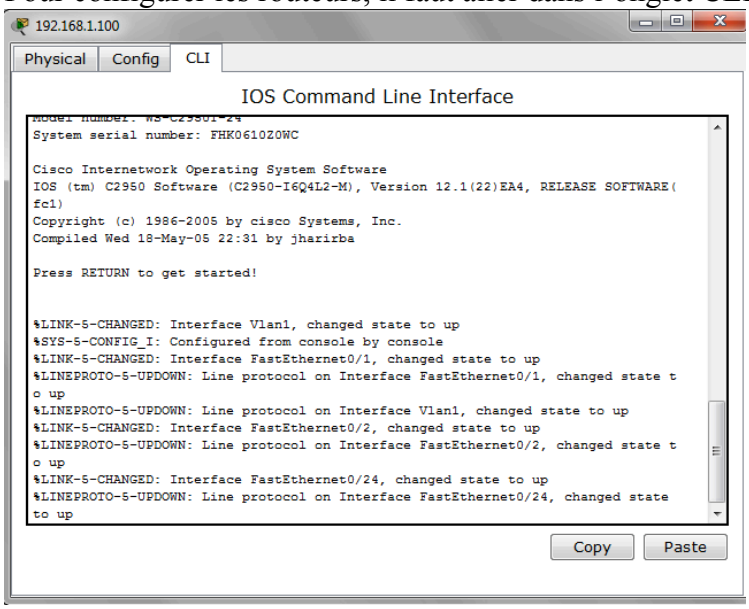
La première étape consiste à mettre en place l'architecture réseau ci-dessous.
La maquette se compose de commutateurs sur lesquels sont branchés 2 postes chacun, 2 routeurs reliant les 2 ensembles Switch/Postes et d'un Serveur relié sur un des Switch.



Etape 2

La 2e étape correspond à la configuration des postes :

Pour configurer les routeurs, il faut aller dans l'onglet CLI du matériel.



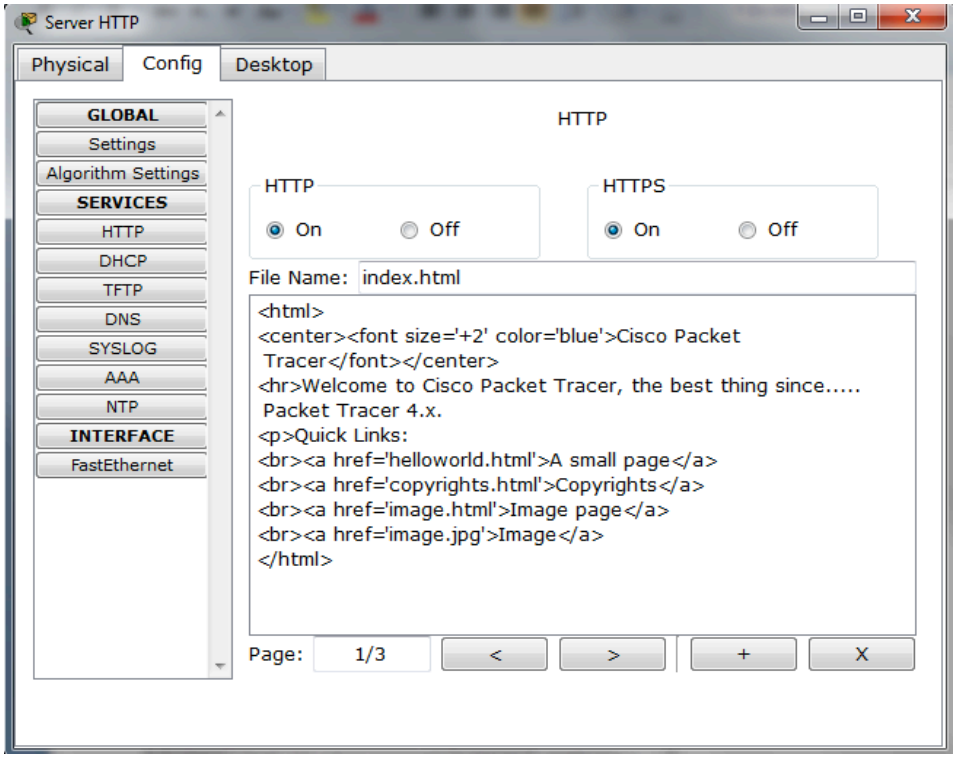
On entre les adresses voulus dans les interfaces du routeur :
enable : pour prendre la main sur l'équipement
show ip interface brief : permet de voir l'état de no interfaces
configure terminale : pour entrer dans le mode de configuration
interface vlan1 : pour entrer les paramètres de l'interface vlan1
no shutdown : pour être sur que l'interface n'est pas down.
ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz: pour y renseigner une adresse ip (x : ip,y : masque, z : passerelle)
exit : permet de revenir un cran en arrière dans le menu.

De plus, il faut renseigner les routes non connectées directement à la machine (voir ci-dessous)

ip route xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz, ici, pour le routeur1 :
ip route 192.168.1.0 255.255.255.0 10.0.0.1
exit
show ip route : pour voir les route existantes.
Ci-dessous, pour le routeur1 :

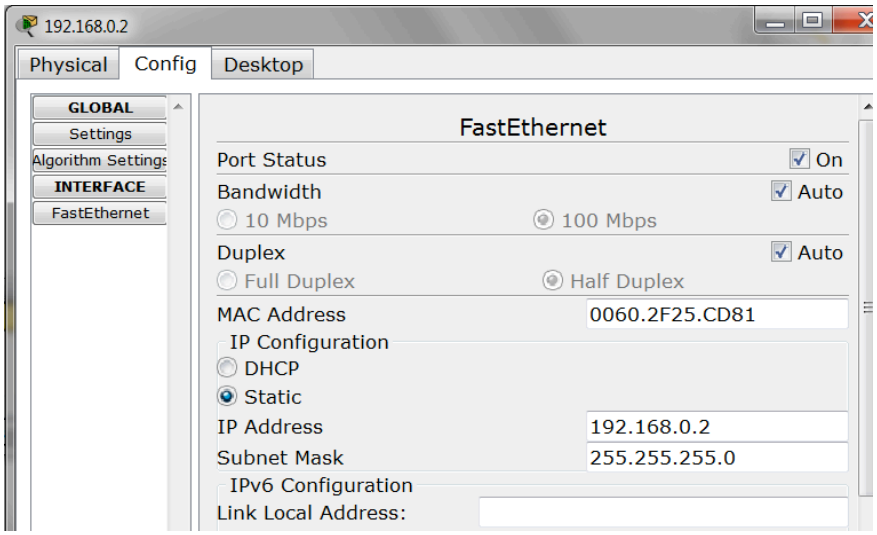
```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inte
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, FastEthernet0/0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
S    192.168.1.0/24 [1/0] via 10.0.0.1
Router#
```

Pour configurer le serveur, sur l'équipement aller dans l'onglet Config et l'option http et activer les services http et HTTPS.

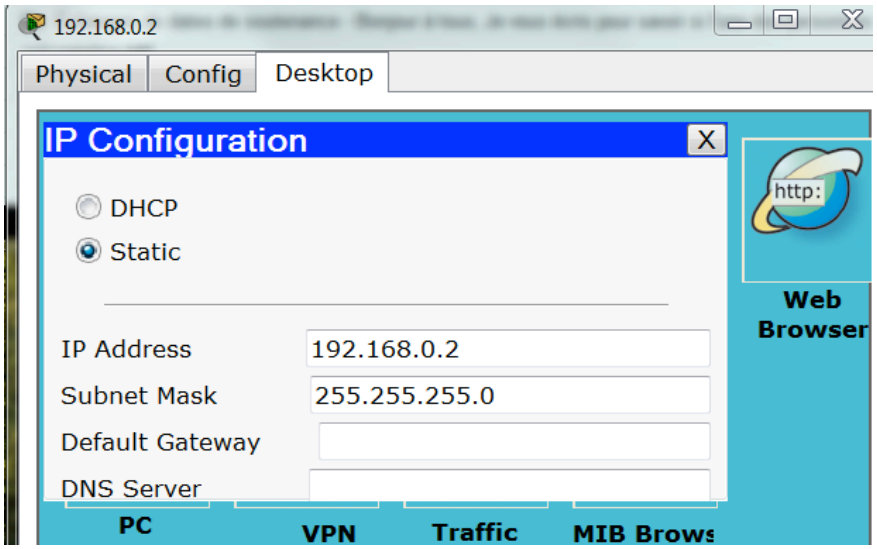


Il est possible de personnaliser la page en modifiant le code HTML présent.

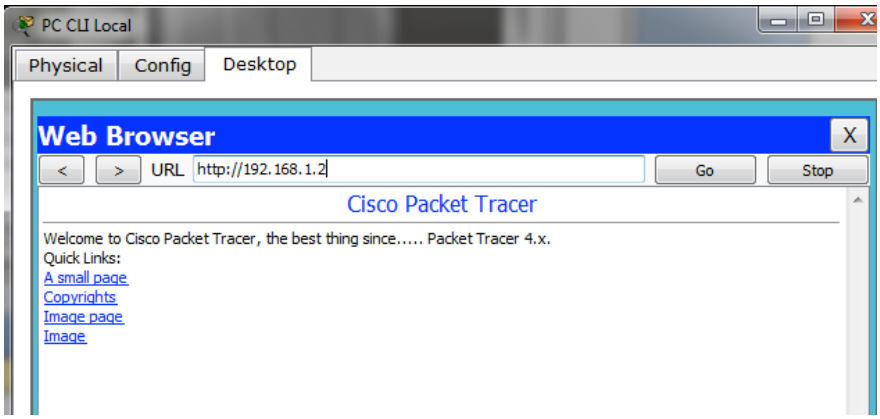
Pour configurer un poste il faut cliquer sur le poste choisi et modifier son adresse dans l'écran interface



Il est aussi possible de faire la modification en « mode graphique » à l'écran « desktop »



On peut vérifier la connexion http avec le serveur en allant dans le Web browser et en renseignant l'adresse de celui-ci :



Améliorations

Les améliorations réalisables sont listées ci-dessous :

Il est possible d'accroitre le réseau.
Il est possible d'activer d'autres services sur le serveur ou implémenter d'autres serveurs.
Il est aussi possible de combiner plusieurs maquettes entre elles avec l'outil MultiUsers

Résumé de Travail à Faire :

- Les activités
- La maquette HTTP