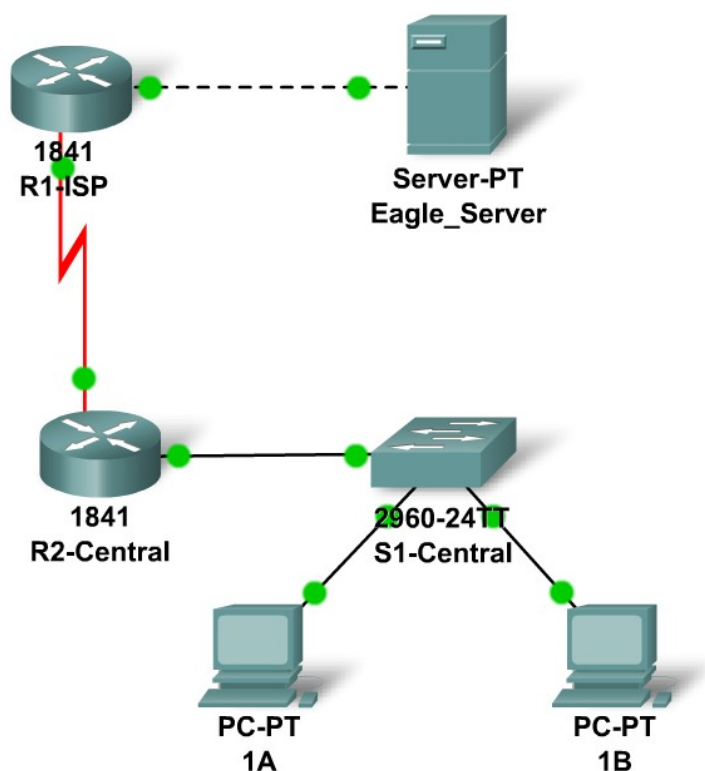


## 4.6.1 : Exercice d'intégration des compétences : Analyse des couches application et transport

### Schéma de topologie



### Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	Fa0/0	192.168.254.253	255.255.255.0	S/O
	S0/0/0	10.10.10.6	255.255.255.252	S/O
R2-Central	Fa0/0	172.16.255.254	255.255.0.0	S/O
	S0/0/0	10.10.10.5	255.255.255.252	S/O
S1-Central	VLAN 1	172.16.254.1	255.255.0.0	172.16.255.254
PC 1A	La carte réseau	172.16.1.1	255.255.0.0	172.16.255.254
PC 1B	La carte réseau	172.16.1.2	255.255.0.0	172.16.255.254
Eagle Server	La carte réseau	192.168.254.254	255.255.255.0	192.168.254.253

## Objectifs pédagogiques

- Configurer les hôtes et les services
- Connecter et configurer les hôtes et les services sur le modèle de réseau des travaux pratiques
- Analyser l'interaction entre DNS, UDP, HTTP et TCP
- Visualiser le fonctionnement de DNS, UDP, HTTP et TCP sur le modèle de réseau des travaux pratiques en mode Simulation

## Contexte

Tout au long de ce cours, vous allez utiliser une configuration de travaux pratiques type constituée de PC, de serveurs, de routeurs et de commutateurs réels dans l'optique d'apprendre des concepts liés aux réseaux. À la fin de chaque chapitre, vous construirez des parties de plus en plus importantes de cette topologie dans Packet Tracer et analyserez des interactions de protocoles de plus en plus complexes.

### Tâche 1 : réparation et test de la topologie

Le serveur a été remplacé. Il doit être mis sous tension. Configurez-le ensuite avec les paramètres suivants : adresse IP 192.168.254.254, masque de sous-réseau 255.255.255.0, passerelle par défaut 192.168.254.253, service DNS activé, en associant eagle-server.example.com à l'adresse IP du serveur, service HTTP activé. Reliez le serveur Eagle Server au port Fa0/0 du routeur R1-ISP avec un câble croisé.

Le PC 1A a perdu ses informations d'adresse IP. Configurez-le avec les paramètres suivants : adresse IP 172.16.1.1, masque de sous-réseau 255.255.0.0, passerelle par défaut 172.16.255.254 et serveur DNS 192.168.254.254. Reliez le PC 1A au port Fa0/1 du commutateur S1-Central avec un câble droit.

Vérifiez votre travail en vous basant sur les informations affichées par le bouton **Check Results** et l'onglet **Assessment Items**. Testez la connectivité en temps réel entre le PC 1A et le serveur Eagle Server en utilisant l'option ADD SIMPLE PDU.

Sachez que lorsque vous ajoutez une unité de données de protocole simple, elle apparaît dans la fenêtre PDU List en tant que partie intégrante du « Scenario 0 ». La première fois que vous émettrez ce message ping ponctuel, celui-ci échouera (libellé « **Failed** ») en raison du processus ARP, qui vous sera expliqué ultérieurement. Si vous double-cliquez sur le bouton « Fire » dans la fenêtre PDU List, ce message de test ping unique sera envoyé une deuxième fois. Cette fois, il aboutira. Dans Packet Tracer, le terme « scenario » représente une configuration spécifique d'un ou plusieurs paquets de test. Vous pouvez créer différents scénarios de paquet de test en utilisant le bouton **New**. Par exemple, Scenario 0 peut représenter un paquet de test entre le PC 1A et le serveur Eagle Server ; Scenario 1 peut correspondre à des paquets de test entre le PC 1B et les routeurs ; et ainsi de suite. Vous pouvez supprimer tous les paquets de test d'un scénario donné en utilisant le bouton **Delete**. Ainsi, si vous utilisez le bouton **Delete** pour Scenario 0, le paquet de test que vous venez de créer entre le PC 1A et le serveur Eagle Server sera supprimé (veillez à effectuer cette opération avant la prochaine tâche).

### Tâche 2 : analyse de l'interaction entre DNS, UDP, HTTP et TCP

Passez du mode Realtime au mode Simulation. Assurez-vous que le filtre d'événements (Event Filter) est défini de façon à afficher DNS, UDP, HTTP, TCP et ICMP. Ouvrez un navigateur Web à partir du Bureau de 1A. Tapez l'adresse URL du serveur eagle-server.example.com, appuyez sur Entrée, puis utilisez le bouton **Capture / Forward** dans la liste d'événements (**Event List**) pour capturer l'interaction de DNS, UDP, HTTP et TCP.

Vous pouvez examiner le paquet de deux façons différentes : en cliquant sur l'enveloppe du paquet lorsque celle-ci s'affiche dans l'animation ou en cliquant sur la colonne **Info** du paquet dès qu'il apparaît dans la liste d'événements (**Event List**). Visualisez cette animation et examinez le contenu des paquets (fenêtre **PDU Information, Inbound PDU Details, Outbound PDU Details**) pour chaque événement contenu dans la liste, particulièrement lorsque les paquets se trouvent au niveau du PC 1A ou du serveur Eagle Server. Si vous recevez le message « Buffer Full » (mémoire tampon saturée), cliquez sur le bouton **View Previous Events**. Bien que le traitement des paquets par le commutateur et les routeurs puisse encore vous paraître étranger, vous devriez être en mesure d'observer la façon dont DNS, UDP, HTTP et TCP interagissent en étudiant le traçage des paquets et en utilisant la fenêtre PDU Information pour les examiner de l'intérieur.

### Remarques générales

Êtes-vous en mesure de schématiser la séquence d'événements de protocoles impliqués dans la demande d'une page Web en utilisant une adresse URL ? Quels sont les points à risques ? Comparez et confrontez DNS et HTTP, puis UDP et TCP.