Travaux pratiques 9.8.3 : Périphérique intermédiaire en tant que périphérique final

Schéma de topologie

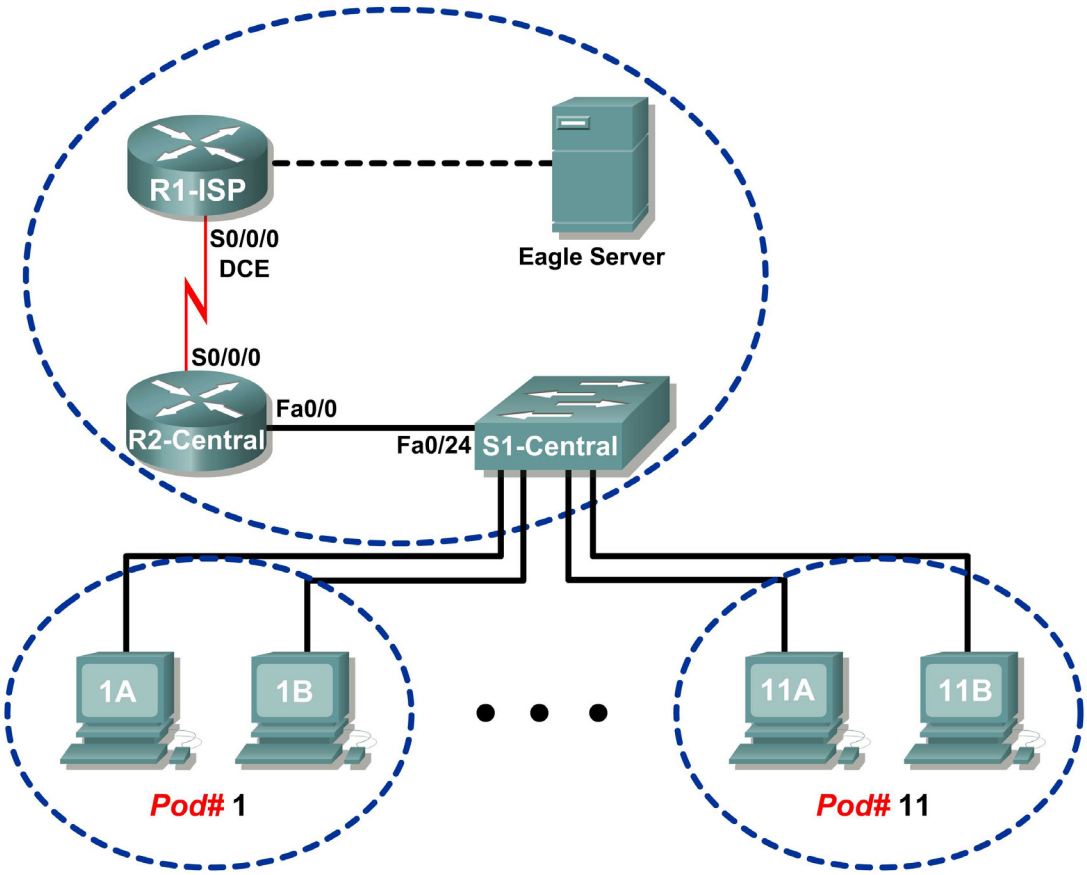

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0:	10.10.10.6	255.255.255.252	S/O
	Fa0/0	192.168.254.253	255.255.255.0	S/O
R2-Central	S0/0:	10.10.10.5	255.255.255.252	S/O
	Fa0/0	172.16.255.254	255.255.0.0	S/O
Eagle Server	S/O	192.168.254.254	255.255.255.0	192.168.254.253
	S/O	172.31.24.254	255.255.255.0	S/O
host*Pod#*A	S/O	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#*B	S/O	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	S/O	172.16.254.1	255.255.0.0	172.16.255.254

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Utiliser Wireshark pour capturer et analyser des trames provenant de nœuds réseau
- Examiner la provenance des trames dans un petit réseau

Contexte

Un commutateur permet de router des trames entre les périphériques réseau. En général, un commutateur n'est pas à l'origine de la trame transférée aux périphériques réseau. Il transmet plutôt efficacement la trame d'un périphérique à l'autre dans le réseau local.

Scénario

Wireshark permet de capturer et d'analyser les trames Ethernet. Si vous n'avez pas effectué le téléchargement de Wireshark sur l'ordinateur hôte pod, utilisez l'adresse URL ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter9/, fichier `wireshark-setup-0.99.4.exe`.

Dans ces travaux pratiques, vous allez envoyer une requête ping vers l'ordinateur hôte pod du voisin.

Inscrivez l'adresse IP et la connexion du port sur S1-Central pour l'ordinateur hôte pod du voisin.

Adresse IP : _____ Numéro de port de S1-Central : _____

Tâche 1 : utilisation de Wireshark pour capturer et analyser des trames provenant de nœuds réseau

Étape 1 : configuration de Wireshark pour les captures de paquets

Configurez Wireshark.

1. Cliquez sur **Capture > Options**.
2. Sélectionnez l'interface qui correspond au LAN.
3. Cochez la case pour mettre à jour la liste de paquets en temps réel.
4. Cliquez sur **Démarrer**.

Ceci permet de commencer la capture des paquets. Plus de 200 captures vont être probablement effectuées, ce qui rend l'analyse un peu fastidieuse. La communication Telnet entre l'ordinateur hôte pod et S1-Central est facile à filtrer.

Étape 2 : utilisation du client Telnet de Windows pour accéder à S1-Central

S1-Central a été configuré avec 11 comptes de participants, `ccna1` à `ccna11`. Pour fournir l'accès à chaque participant, utilisez l'ID d'utilisateur qui correspond à votre pod. Par exemple, utilisez `ccna1` pour les ordinateurs hôtes sur pod 1. Sauf indication contraire de votre formateur, le mot de passe est `cisco`.

1. Dans le terminal Windows, exécutez la commande **`telnet`** *`adresse IP de destination`*:

   C:/> **`telnet 172.16.254.1`**

2. Indiquez le nom d'utilisateur et le mot de passe appropriés (**`cisco`**).
   L'invite de S1-Central doit être retournée, `S1-Central#`.

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Étape 3 : effacement de la table d'adresses MAC

1. Examinez la table d'adresses MAC du commutateur avec la commande **`show mac-address-table`**. Outre plusieurs entrées (CPU) statiques, les entrées dynamiques de la table d'adresses doivent être nombreuses.
2. Pour effacer les entrées dynamiques de la table d'adresses MAC, utilisez la commande **`clear mac-address-table dynamic`**.
3. Répertoriez les entrées dynamiques de l'adresse MAC :

Adresse MAC	Port de commutation

4. Ouvrez une deuxième fenêtre de terminal. Envoyez une requête ping à l'adresse IP de votre voisin, qui a été consignée auparavant.

   C:>\ **ping –n 1** *adresse IP*

5. L'adresse MAC de cet ordinateur doit être ajoutée de façon dynamique dans la table d'adresses MAC de S1-Central
6. Répertoriez à nouveau les entrées dynamiques de l'adresse MAC :

Adresse MAC	Port de commutation

   Quelle conclusion peut-on tirer de la manière dont un commutateur obtient des informations sur les adresses MAC associées aux interfaces du commutateur ?

   _____

   _____

7. Fermez la capture Wireshark.

   La capture est analysée à l'étape suivante.

Tâche 2 : analyse de la provenance des trames dans un petit réseau

Étape 1 : analyse d'une session Telnet avec S1-Central

1. Sélectionnez l'un des paquets de la session Telnet. Dans le menu Wireshark, cliquez sur **Analyze | Follow TCP Stream**. Une fenêtre de contenu du flux affiche du texte ASCII par défaut. Si le nom d'utilisateur et le mot de passe ne sont pas visibles, basculez vers HEX Dump.
2. Vérifiez le nom d'utilisateur et le mot de passe saisis.
   Nom d'utilisateur : _____ Mot de passe : _____
3. Fermez la fenêtre du contenu du flux.

Étape 2 : analyse les résultats de la commande `show mac-address-table`

1. Ouvrez le Bloc-notes. Les données capturées sont transférées vers Bloc-notes pour l'analyse. Il se peut qu'il y ait de nombreux paquets capturés.

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

2. Dans le volet Packet List supérieur de Wireshark, faites défiler la liste vers le bas jusqu'à la requête ICMP capturée. Si la fenêtre Packet Byte inférieure de Wireshark n'est pas visible, cliquez sur **View > Packet bytes**.

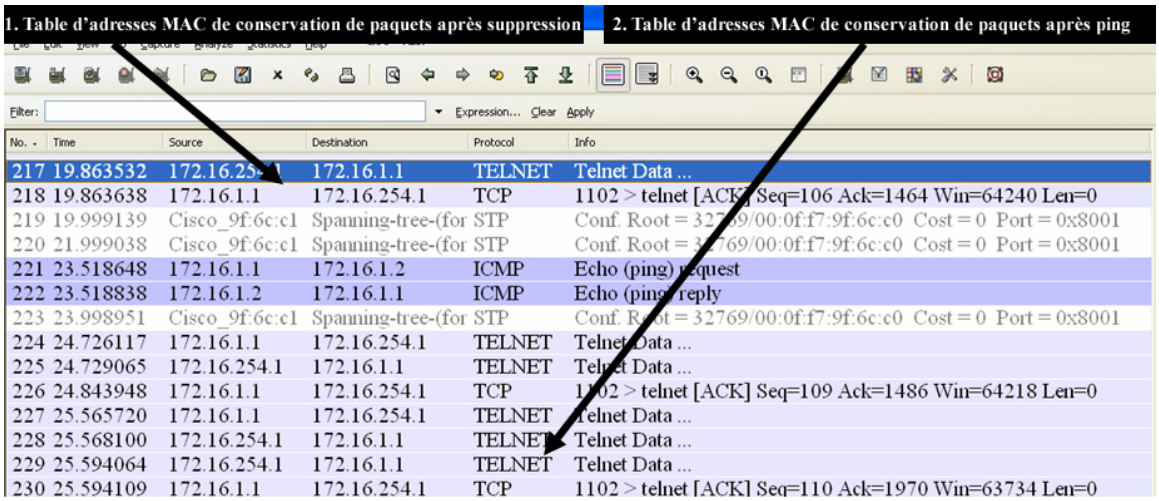

Figure 1. Capture Wireshark de Telnet

Reportez-vous à la figure 1, les résultats partiels de la capture Wireshark :

1 Sélectionnez le dernier paquet de données Telnet provenant de S1-Central avant la commande **`ping`**. Ensuite, sélectionnez l'octet de paquet correspondant. Cliquez avec le bouton droit sur l'octet de paquet et cliquez sur **Copier > Texte seulement**. Dans Bloc-notes, cliquez sur **Édition > Coller**. Les mappages dynamiques doivent être semblables aux résultats suivants :

```
{_lEMaNL;RPC          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000f.f79f.6cc0    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0010.a47b.015f    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 5
S1-Central#
```

3. Notez l'adresse MAC et le numéro de port affichés dans les résultats. Le port du commutateur correspond-il à votre ordinateur hôte pod ? _____

Adresse MAC	Type	Port

Pourquoi le mappage de l'ordinateur hôte pod figure-t-il encore dans la table d'adresses MAC, même après avoir été supprimé ? _____

_____

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

❷ Sélectionnez le dernier paquet de données Telnet immédiatement après la réponse ping. Ensuite, sélectionnez l'octet de paquet correspondant. Cliquez avec le bouton droit sur l'octet de paquet et cliquez sur **Copier > Texte seulement**. Dans Bloc-notes, cliquez sur **Édition > Coller**. Le texte doit être semblable à l'opération Coller suivante :

```
{_lEPaNM;VP          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000f.f79f.6cc0    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0010.a47b.015f    DYNAMIC     Fa0/1
   1    0016.76ac.a76a    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 6
S1-Central#
```

4. Notez l'adresse MAC et le numéro de port pour le deuxième type dynamique affiché dans les résultats. Le port du commutateur correspond-il à l'ordinateur hôte pod de votre voisin ?

_____

Adresse MAC	Type	Port

Tâche 3 : remarques générales

La capture Wireshark d'une session Telnet entre un ordinateur hôte pod et S1-Central a été analysée pour indiquer la manière dont un commutateur obtient des informations dynamiques sur les nœuds auxquels il est directement connecté.

Tâche 4 : confirmation

Wireshark permet de capturer et d'analyser une session Telnet entre l'ordinateur hôte pod et le commutateur Cisco. Utilisez l'option du menu Wireshark **Analyze > Follow TCP Stream** pour afficher l'ID d'utilisateur et le mot de passe de connexion. Quel est le niveau de protection du protocole Telnet ? Comment sécuriser davantage la communication avec les périphériques Cisco ?

_____

_____

_____

_____

_____

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Tâche 5 : nettoyage

Wireshark a été installé sur l'ordinateur hôte pod. Si vous souhaitez désinstaller Wireshark, cliquez sur **Démarrer > Panneau de configuration**. Ouvrez **Ajout ou suppression de programmes**. Sélectionnez Wireshark et cliquez sur **Supprimer**.

Supprimez tout fichier créé sur l'ordinateur hôte pod au cours des travaux pratiques.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques et préparez la salle pour le cours suivant.

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.