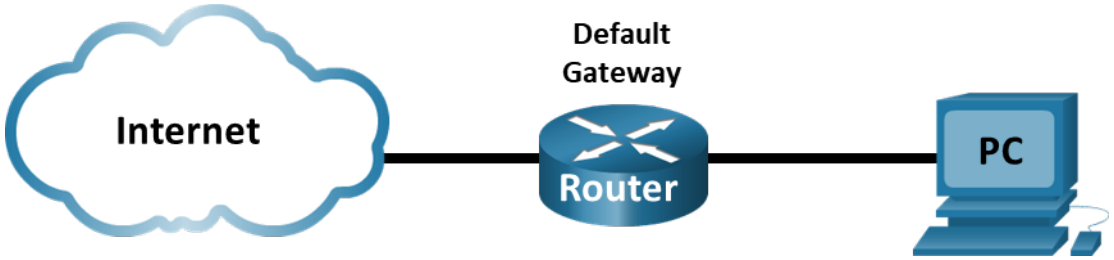
Travaux pratiques - Utiliser Wireshark pour examiner les trames Ethernet

Topologie



Objectifs

Partie 1 : Examiner les champs d'en-tête dans une trame Ethernet II

Partie 2 : Utiliser Wireshark pour capturer et analyser les trames Ethernet

Contexte/scénario

Lorsque des protocoles de couche supérieure communiquent entre eux, les données circulent dans les couches du modèle OSI (Open Systems Interconnection) et sont encapsulées dans une trame de couche 2. La composition des trames dépend du type d'accès aux supports. Par exemple, si les protocoles de couche supérieure sont TCP et IP et que l'accès aux supports est Ethernet, l'encapsulation des trames de couche 2 est Ethernet II. C'est généralement le cas pour un environnement de réseau local (LAN).

Lorsque vous étudiez les concepts de couche 2, il est utile d'analyser les informations d'en-tête des trames. Dans la première partie de ce TP, vous allez examiner les champs figurant dans une trame Ethernet II. Dans la deuxième partie, vous allez utiliser Wireshark pour capturer et analyser les champs d'en-tête de trame Ethernet II pour le trafic local et distant.

Ressources requises

- 1 PC (Windows avec accès à Internet et avec Wireshark installé)

Instructions

Partie 1 : Examiner les champs d'en-tête dans une trame Ethernet II

Dans la première partie, vous allez examiner les champs d'en-tête et le contenu d'une trame Ethernet II. Une capture Wireshark sera utilisée pour examiner le contenu de ces champs.

Étape 1: Consultez les descriptions et les longueurs des champs d'en-tête Ethernet II.

Préambule	Adresse de destination	Adresse source	Type de trame	Données	FCS
8 octets	6 octets	6 octets	2 octets	De 46 à 1 500 octets	4 octets

Étape 2: Examinez la configuration réseau de l'ordinateur.

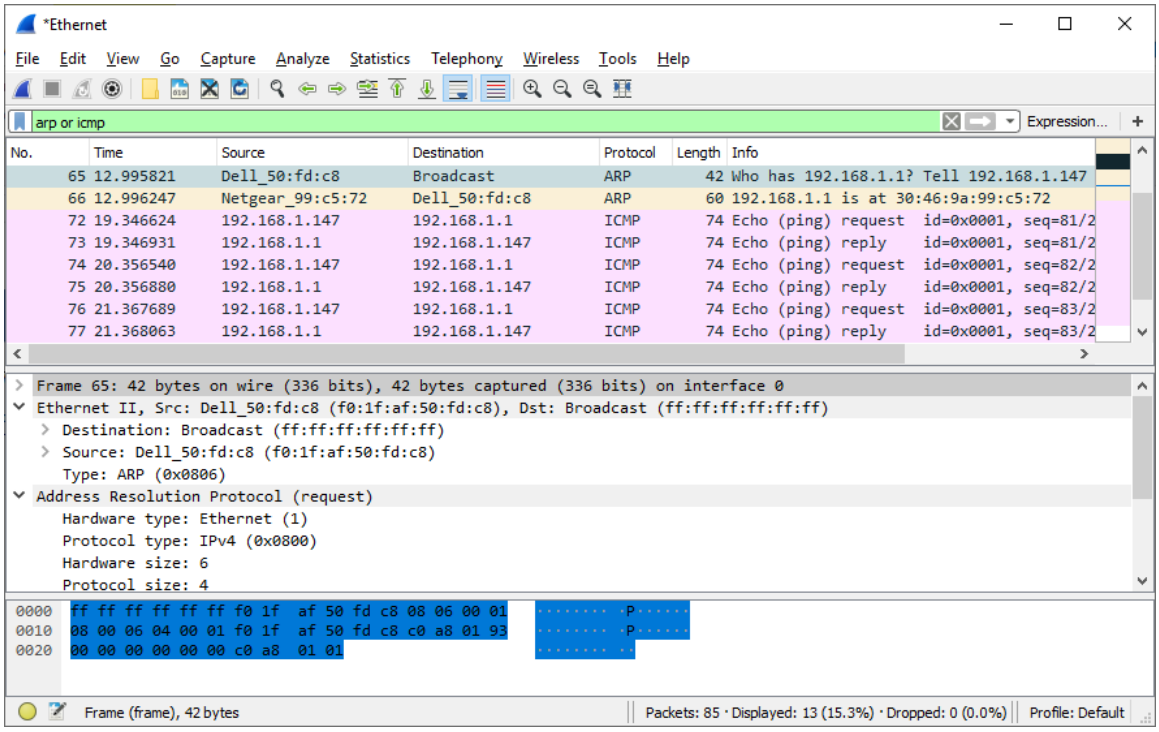
Dans cet exemple, l'adresse IP de l'hôte du PC est 192.168.1.147 et la passerelle par défaut a une adresse IP de 192.168.1.1.

```
C:\ ipconfig /all

Adaptateur Ethernet :

   Suffixe DNS propre à la connexion . :
   Description . . . . . . . . . . . : Connexion de réseau Intel(R) 82579LM Gigabit
   Physical Address. . . . . . . . .  : F0-1F-AF-50-FD-C8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80 : :58c 5:45 f 2:7 e5e:29c 2% 11 (Préféré)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147 (Préféré)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, September 6, 2019 11:08:36 AM
   Lease Expires . . . . . . . . . . : Saturday, September 7, 2019 11:08:36 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
<output omitted>
```

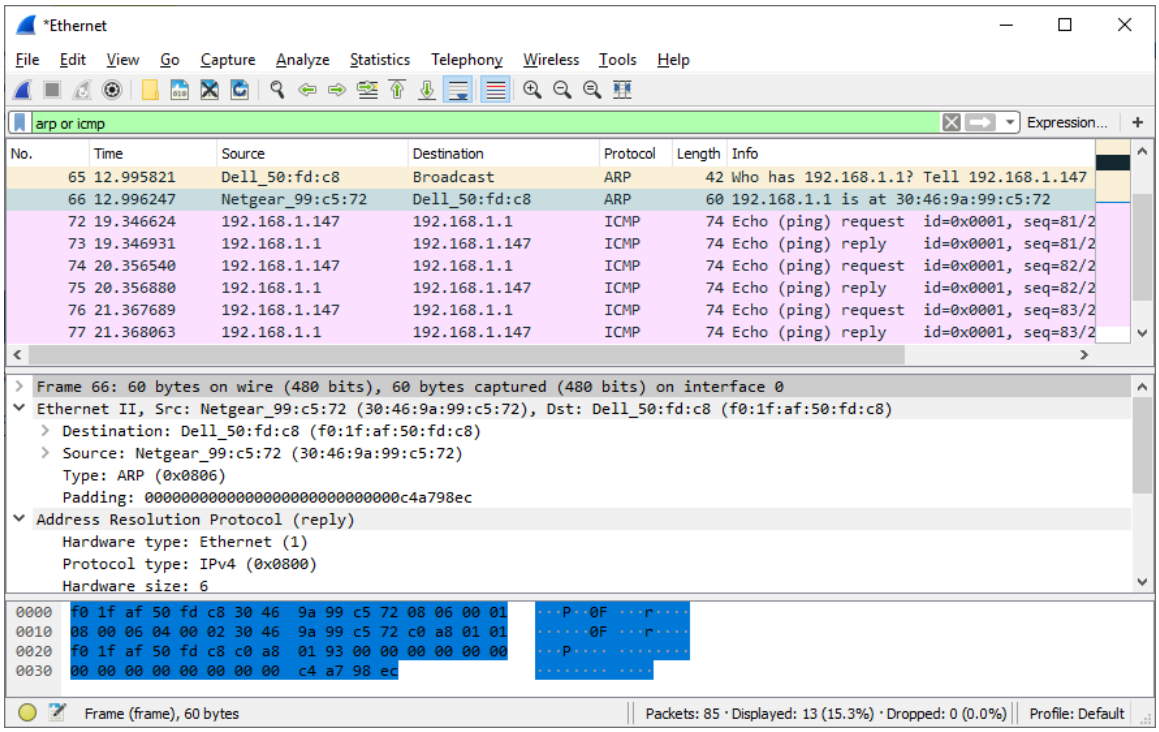
Étape 3: Examinez les trames Ethernet dans une capture Wireshark.

Les captures d'écran de la capture Wireshark ci-dessous montrent les paquets générés par un ping émis depuis un PC hôte vers sa passerelle par défaut. Un filtre a été appliqué à Wireshark pour afficher les protocoles ARP et ICMP uniquement. ARP signifie protocole de résolution d'adresse. ARP est un protocole de communication utilisé pour déterminer l'adresse MAC associée à l'adresse IP. La session commence par une requête ARP pour l'adresse MAC du routeur de passerelle, suivie de quatre requêtes ping et réponses.

Cette capture d'écran met en évidence les détails du trame pour une requête ARP.



Cette capture d'écran met en évidence les détails du trame pour une réponse ARP.



Étape 4: Examinez le contenu d'en-tête Ethernet II d'une requête ARP.

Le tableau suivant prend la première trame dans la capture Wireshark et affiche les données présentes dans les champs d'en-tête Ethernet II.

Champ	Valeur	Description
Préambule	Non affichée dans la capture	Ce champ contient des bits de synchronisation traités par la carte réseau.
Adresse de destination Adresse source	Diffusion (ff:ff:ff:ff:ff:ff) NetGear_99:c 5:72 (30:46:9 a:99:c 5:72)	Les adresses de couche 2 pour la trame. La longueur de chaque adresse est de 48 bits, ou 6 octets, exprimés en 12 chiffres hexadécimaux, `de 0 à 9 et de A à F`. Le format suivant est courant : `12:34:56:78:9A:BC`. Les six premiers chiffres hexadécimaux indiquent le fabricant de la carte réseau, les six derniers chiffres hexadécimaux correspondent au numéro de série de la carte réseau. L'adresse de destination peut être une adresse de diffusion, qui ne contient que des 1, ou une adresse de monodiffusion. L'adresse source est toujours à monodiffusion.
Type de trame	0x0806	Pour les trames Ethernet II, ce champ contient une valeur hexadécimale qui permet d'indiquer le type de protocole de couche supérieure dans le champ de données. De nombreux protocoles de couche supérieure sont pris en charge par Ethernet II. Deux types de trame standard sont : Valeur Description `0x0800` IPv4 Protocol `0x0806` Protocole ARP (Address Resolution Protocol)
Données	ARP	Contient le protocole encapsulé de niveau supérieur. Le champ de données comprend entre 46 et 1 500 octets.

Champ	Valeur	Description
FCS	Non affichée dans la capture	Séquence de contrôle de trame, que la carte réseau utilise pour identifier les erreurs au cours de la transmission. La valeur est calculée par le dispositif d'envoi, englobant les adresses de trame, le type et le champ de données. Elle est vérifiée par le récepteur.

Quel élément est important en ce qui concerne le contenu du champ d'adresse de destination ?

Pourquoi l'ordinateur envoie-t-il une diffusion ARP avant d'envoyer la première requête ping ?

Quelle est l'adresse MAC de la source dans la première trame ?

Quel est l'ID du vendeur (OUI) du NIC source dans la réponse de l'ARP ?

À quelle partie de l'adresse MAC correspond l'identifiant OUI ?

Quel est le numéro de série de la carte réseau de la source ?

Partie 2 : Utiliser Wireshark pour capturer et analyser les trames Ethernet

Dans la deuxième partie, vous allez utiliser Wireshark pour capturer les trames Ethernet locales et distantes. Vous examinerez ensuite les informations contenues dans les champs d'en-tête de trame.

Étape 1: Déterminez l'adresse IP de la passerelle par défaut sur votre ordinateur.

Ouvrez une fenêtre d'invite de commandes et entrez la commande **ipconfig**.

Quelle est l'adresse IP de la passerelle par défaut de l'ordinateur ?

Étape 2: Commencez par capturer le trafic sur la carte réseau de votre ordinateur.

a. Ouvrez Wireshark pour lancez la capture des données.

b. Observez le trafic qui apparaît dans la fenêtre Packet List.

Étape 3: Filtrez Wireshark pour afficher uniquement le trafic ICMP.

Vous pouvez utiliser le filtre dans Wireshark pour bloquer la visibilité du trafic indésirable. Le filtre ne bloque pas la saisie de données indésirables ; il ne filtre que ce que vous voulez afficher à l'écran. Pour le moment, seul le trafic ICMP doit être affiché.

Dans la zone **Filter** (filtre) de Wireshark, saisissez **icmp**. La case devient verte si vous avez correctement tapé le filtre. Si la case est verte, cliquez sur **Apply** pour appliquer le filtre.

Étape 4: À partir de la fenêtre d'invite de commandes, envoyez une requête ping à la passerelle par défaut de votre ordinateur.

À partir de la fenêtre de commandes, envoyez une requête ping à la passerelle par défaut avec l'adresse IP que vous avez notée à l'étape 1.

Étape 5: Arrêtez la capture du trafic sur la carte réseau.

Cliquez sur l'icône **Stop Capturing Packets** pour arrêter la capture de trafic.

Étape 6: Examinez la première requête Echo (ping) dans Wireshark.

La fenêtre principale de Wireshark est divisée en trois sections : le volet Packet List (en haut), le volet **Packet Details** (au milieu) et le volet **Packet Bytes** (en bas). Si vous avez sélectionné la bonne interface pour la capture de paquets précédemment, Wireshark devrait afficher les informations ICMP dans le volet de la liste de paquets de Wireshark.

a. Dans le volet Packet List (section supérieure), cliquez sur la première trame répertoriée. **Echo (ping) request** (requête écho (ping)) devrait s'afficher en dessous de l'en-tête **Info**. La ligne doit maintenant être mise en surbrillance.

b. Examinez la première ligne du volet Packet Details (section centrale). Cette ligne affiche la longueur de la trame.

c. La deuxième ligne dans le volet Packet Details indique qu'il s'agit d'une trame Ethernet II. Les adresses MAC source et de destination sont également indiquées.

Quelle est l'adresse MAC de la carte réseau de l'ordinateur ?

Quelle est l'adresse MAC de la passerelle par défaut ?

d. Vous pouvez cliquer sur le signe plus grand que (>) au début de la deuxième ligne pour obtenir plus d'informations sur la trame Ethernet II.

Quel type de trame est affiché ?

e. Les deux dernières lignes figurant dans la section centrale fournissent des informations sur le champ de données de la trame. Notez que les données contiennent les informations d'adresse IPv4 de la source et de la destination.

Quelle est l'adresse IP source ?

Quelle est l'adresse IP de destination ?

f. Vous pouvez cliquer sur n'importe quelle ligne dans la section centrale pour mettre en surbrillance cette partie de la trame (hex et ASCII) dans le volet **Packet Bytes** (section inférieure). Cliquez sur la ligne **Internet Control Message Protocol** (protocole ICMP) dans la section centrale et examinez ce qui est mis en surbrillance dans le volet **Packet Bytes**.

Quelles sont les deux dernières lettres des octets mis en surbrillance ?

g. Cliquez sur la trame suivante dans la section supérieure et examinez une trame de réponse Echo. Notez que les adresses MAC source et de destination ont été inversées, car cette trame a été envoyée depuis le routeur de passerelle par défaut comme réponse au premier ping.

Quel périphérique et quelle adresse MAC s'affichent comme adresse de destination ?

Étape 7: Capturez des paquets pour un hôte distant.

a. Cliquez sur l'icône **Start Capture** (démarrer la capture) pour démarrer une nouvelle capture Wireshark. Une fenêtre contextuelle vous invite à enregistrer les précédents paquets capturés dans un fichier avant de démarrer une nouvelle capture. Cliquez sur **Continue without Saving** (continuer sans enregistrer).

b. Dans une fenêtre d'invite de commande, ping www.cisco.com.

c. Arrêtez la capture des paquets.

d. Examinez les nouvelles données dans le volet de la liste des paquets de Wireshark.

Dans la première trame de demande Echo (ping), quelles sont les adresses MAC source et de destination ?

Source:

Destination:

Quelles sont les adresses IP source et de destination figurant dans le champ de données de la trame ?

Source:

Destination:

Comparez ces adresses à celles que vous avez reçues à l'étape 6. La seule adresse qui a changé est l'adresse IP de destination. Pourquoi l'adresse IP de destination a-t-elle changé, alors que l'adresse MAC de destination est restée la même ?

Question de réflexion

Wireshark n'affiche pas le champ de préambule d'un en-tête de trame. Que contient le champ de préambule ?

Travaux pratiques - Utiliser Wireshark pour examiner les trames Ethernet

Topologie

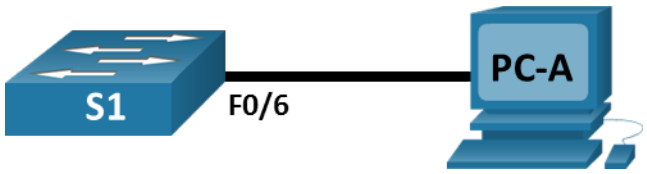


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
S1	VLAN 1	192.168.1.2	255.255.255.0	S/O
PC-A	Carte réseau	192.168.1.3	255.255.255.0	192.168.1.1

Objectifs

Partie 1: configurer des périphériques et vérifier la connectivité

Partie 2: afficher, décrire et analyser les adresses MAC Ethernet

Contexte/scénario

Chaque périphérique d'un réseau local Ethernet est identifié par une adresse MAC de couche 2. Celle-ci est attribuée par le fabricant et stockée dans le micrologiciel de la carte réseau. Ce TP présentera et analysera les composants d'une adresse MAC, ainsi que la façon dont vous pouvez collecter ces informations sur un commutateur et un ordinateur.

Vous allez câbler les équipements comme illustré dans la topologie. Ensuite, vous configurerez le commutateur et l'ordinateur pour qu'ils correspondent à la table d'adressage. Vous vérifierez vos configurations en testant la connectivité réseau.

Une fois que les périphériques auront été configurés et que la connectivité du réseau aura été vérifiée, vous utiliserez différentes commandes pour récupérer les informations des périphériques afin de répondre à des questions sur l'équipement de votre réseau.

Remarque:Les commutateurs utilisés sont des modèles Cisco Catalyst 2960 équipés de Cisco IOS version 15.2(2) (image lanbasek9). D'autres commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le

modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier par rapport à ceux qui est indiqué dans les travaux pratiques.

Remarque: vérifiez que les paramètre des commutateurs a été effacée et qu'ils ne présentent aucune configuration initiale. En cas de doute, demandez à votre formateur.

Ressources requises

- 1 commutateur (Cisco 2960 équipé de Cisco IOS version 15.2(2) image lanbasek9 ou similaire)
- 1 ordinateur (Windows équipés d'un programme d'émulation de terminal tel que Tera Term)
- Câble de console pour configurer le commutateur Cisco via les ports de console
- Câbles Ethernet conformément à la topologie

Instructions

Partie 3 : Configurer les périphériques et vérifier la connectivité

Dans cette partie, vous configurerez la topologie du réseau et les paramètres de base, tels que les adresses IP de l'interface et le nom du périphérique. Pour connaître le nom du périphérique et les informations liées aux adresse, reportez-vous à la topologie et à la table d'adressage.

Étape 1: Câblez le réseau conformément à la topologie indiquée.

a. Connectez les périphériques conformément à la topologie et effectuez le câblage nécessaire.

b. Mettez sous tension tous les périphériques de la topologie.

Étape 2: Configurez l'adresse IPv4 du PC.

a. Configurez l'adresse IPv4, le masque de sous-réseau et l'adresse de la passerelle par défaut pour PC-A

b. À partir de l'invite de commandes de PC-A, envoyez une requête ping à l'adresse du commutateur.

Les requêtes ping ont-elles abouti ? Expliquez votre réponse.

c. Fermez la fenêtre d'invite de commandes.

Étape 3: Configurez les paramètres de base du commutateur.

Au cours de cette étape, vous configurerez le nom et l'adresse IP du périphérique, et désactiver la recherche DNS sur le commutateur.

a. Accédez au commutateur par la console et passez en mode de configuration globale.

```
Switch> enable
```



```
Switch# configure terminal
Entrez les commandes de configuration, une par ligne.  Terminez par CNTL/Z.
Switch(config)#
```

b. Attribuez un nom d'hôte au commutateur selon la table d'adressage.

```
Switch(config)# hostname S1
```

c. Désactivez la commande de recherche DNS.

```
S1(config)# no ip domain-lookup
```

d. Configurez et activez l'interface SVI pour VLAN 1.

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
*Mar 1 00:07:59.048: %SYS-5-CONFIG_I: Configured from console by console
```

Étape 4: Vérifiez la connectivité du réseau.

Envoyez une requête ping à l'adresse du commutateur du PC-A

Les requêtes ping ont-elles abouti ?

Partie 4 : Afficher, décrire et analyser les adresses MAC Ethernet

Chaque périphérique d'un réseau LAN Ethernet possède une adresse MAC attribuée par le fabricant et stockée dans le micrologiciel de la carte réseau. Les adresses MAC Ethernet ont une valeur binaire de 48 bits. Elles sont affichées à l'aide de six groupes de caractères hexadécimaux généralement séparés par un tiret, deux points ou un point. Dans l'exemple suivant, la même adresse MAC est affichée selon les trois différent méthodes de notations :

00-05-9A-3C-78-00 00:05:9 A:3C: 78:00 0005.9A3C.7800

Remarque: les adresses MAC sont également appelées adresses physiques, adresses matérielles ou adresses matérielles Ethernet.

Vous émettrez des commandes pour afficher les adresses MAC sur un ordinateur et un commutateur, et analyser les propriétés de chacune.

Étape 1: Analysez l'adresse MAC de la carte réseau de PC-A.

Avant d'analyser l'adresse MAC sur PC-A, examinez un exemple provenant de la carte réseau d'un autre ordinateur. Vous pouvez exécuter la commande **ipconfig /all** pour afficher l'adresse MAC de vos cartes réseau. Vous trouverez un exemple des résultats affichés ci-dessous. Lorsque vous utilisez la commande **ipconfig /all**, notez que les adresses MAC sont appelées adresses physiques. Si on lit l'adresse MAC de gauche à droite, les six premiers caractères hexadécimaux se rapportent au fournisseur (le fabricant) de ce périphérique. Ces six premiers caractères hexadécimaux (3 octets) sont également appelés OUI (Organizationally Unique Identifier). Ce code de 3 octets est attribué au fournisseur par l'IEEE.

Pour trouver le fabricant, utilisez les mots-clés ***normes IEEE OUI*** pour trouver un outil de recherche OUI sur Internet ou accédez à http://standards-oui.ieee.org/oui.txt pour trouver les codes fournisseurs OUI enregistrés. Les six derniers caractères correspondent au numéro de série de la carte réseau attribué par le fabricant.

a. En utilisant le résultat de la commande **ipconfig /all** , répondez aux questions suivantes:

```
C:\ ipconfig /all
<output omitted>
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . . : Intel(R) 82577LC Gigabit Network Connection
   Physical Address. . . . . . . . . : 5C-26-0A-24-2A-60
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . .: fe80::b 875:731 b:3c7b:c0b 1% 10 (Préféré)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147 (Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, September 6, 2019 11:08:36 AM
   Lease Expires . . . . . . . . . . : Saturday, September 7, 2019 11:08:36 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
<output omitted>
```

Quelle est la partie qui correspond au OUI de l'adresse MAC de ce périphérique ?

Dans l'adresse MAC de ce périphérique, quelle est la partie qui correspond au numéro de série ?

Dans l'exemple ci-dessus, recherchez le nom du fabricant de cette carte réseau.

b. À partir de l'invite de commandes sur PC-A, exécutez la commande **ipconfig /all** et identifiez la partie OUI de l'adresse MAC pour la carte réseau de PC-A.

Identifiez la partie correspondant au numéro de série dans l'adresse MAC pour la carte réseau de PC-A.

Identifiez le nom du fabricant de la carte réseau de PC-A.

Étape 2: Analysez l'adresse MAC de l'interface F0/6 de S1.

Vous pouvez utiliser diverses commandes pour afficher les adresses MAC du commutateur.

a. Accédez à S1 via la console et utilisez la commande **show interfaces vlan 1** pour trouver les informations d'adresse MAC. Voyez l'exemple ci-dessous. Utilisez le résultat généré par votre commutateur pour répondre aux questions.

```
S1# show interfaces vlan 1
Vlan1 is up, line protocol is up
  Hardware is EtherSVI, address is 001b.0c6d.8f40 (bia 001b.0c6d.8f40)
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:14:51, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     34 packets output, 11119 bytes, 0 underruns
     0 output errors, 2 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Quelle est l'adresse MAC pour VLAN1 sur S1?

Quel est le numéro de série MAC pour VLAN 1?

Quel est l'OUI pour VLAN 1 ?

Selon cet OUI, quel est le nom du fournisseur?

Que signifie «bia»?

Pourquoi le résultat affiche-t-il deux fois la même adresse MAC ?

b. Une autre manière d'afficher l'adresse MAC sur le commutateur est d'utiliser la commande **show arp**. Utilisez la commande **show arp** pour collecter les informations d'adresse MAC. Cette commande mappe l'adresse de couche 2 à l'adresse de couche 3 correspondante. Voyez l'exemple ci-dessous. Utilisez le résultat généré par votre commutateur pour répondre aux questions.

```
S1# show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.1.2 - 001b.0c6d.8f40 ARP Vlan1
Internet 192.168.1.3 0 5c26.0a24.2a60 ARP Vlan1
```

Quelles adresses de couche 2 s'affichent sur S1 ?

Étape 3: Affichez les adresses MAC sur le commutateur.

Exécutez la commande **show mac-address-table** sur S1. Voyez l'exemple ci-dessous. Utilisez le résultat généré par votre commutateur pour répondre aux questions.

```
S1# show mac address-table
          Mac Address Table
-------------------------------------------


Vlan Mac Address Type Ports
---- ----------- -------- -----
 All 0100.0ccc.cccc STATIC CPU
 All 0100.0ccc.cccd STATIC CPU
 All 0180.c200.0000 STATIC CPU
 All 0180.c200.0001 STATIC CPU
 All 0180.c200.0002 STATIC CPU
 All 0180.c200.0003 STATIC CPU
 All 0180.c200.0004 STATIC CPU
 All 0180.c200.0005 STATIC CPU
```

```
 All 0180.c200.0006 STATIC CPU
 All 0180.c200.0007 STATIC CPU
 All 0180.c200.0008 STATIC CPU
 All 0180.c200.0009 STATIC CPU
 All 0180.c200.000a STATIC CPU
 All 0180.c200.000b STATIC CPU
 All 0180.c200.000c STATIC CPU
 All 0180.c200.000d STATIC CPU
 All 0180.c200.000e STATIC CPU
 All 0180.c200.000f STATIC CPU
 All 0180.c200.0010 STATIC CPU
 All ffff.ffff.ffff STATIC CPU
   1 5c26.0a24.2a60 DYNAMIC Fa0/6
Total Mac Addresses for this criterion: 21
```

Le commutateur a-t-il affiché l'adresse MAC de PC-A ? Si vous répondez oui, précisez sur quel port.

Questions de réflexion

1. Les diffusions sont-elles possibles au niveau de la couche 2 ? Si oui, quelle serait l'adresse MAC ?
2. Pourquoi faut-il connaître l'adresse MAC d'un appareil ?

Travaux pratiques - Utiliser Wireshark pour examiner les trames Ethernet

Topologie

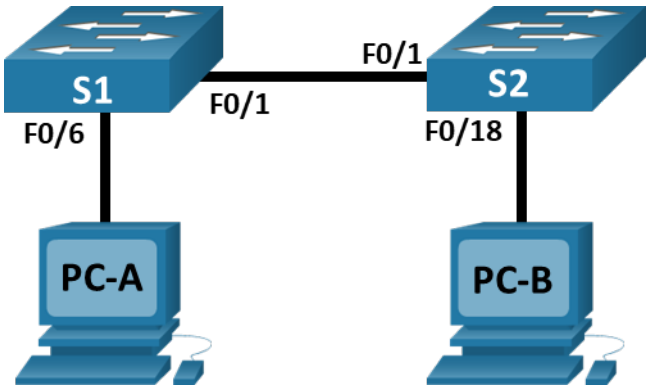


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
S1	VLAN 1	192.168.1.11	255.255.255.0
S2	VLAN 1	192.168.1.12	255.255.255.0
PC-A	Carte réseau	192.168.1.1	255.255.255.0
PC-B	Carte réseau	192.168.1.2	255.255.255.0

Objectifs

Partie 1 : concevoir et configurer le réseau

Partie 2 : analyser la table d'adresses MAC du commutateur

Contexte/scénario

La fonction d'un commutateur LAN de couche 2 est de fournir des trames Ethernet aux périphériques hôtes du réseau local. Le commutateur enregistre les adresses MAC d'hôte qui sont visibles sur le réseau, et associe ces adresses MAC à ses ports de commutateur Ethernet. On dit de ce processus qu'il consiste à construire la table d'adresses MAC. Lorsqu'un commutateur reçoit une trame d'un ordinateur, il examine les adresses MAC source et de destination de la trame. L'adresse MAC source est enregistrée et associée au port de commutateur dont elle est issue. L'adresse MAC de destination est ensuite recherchée dans la table

d'adresses MAC. Si elle y figure, la trame est transférée via le port de commutateur correspondant à l'adresse MAC. Si l'adresse MAC est inconnue, la trame est diffusée à partir de tous les ports de commutateur, excepté celui dont elle provient. Il est important d'examiner et de comprendre la fonction d'un commutateur et la manière dont il transmet les informations sur le réseau. La manière dont un commutateur fonctionne a des conséquences pour les administrateurs réseau dont le travail est d'assurer une communication réseau sécurisée et homogène.

Les commutateurs sont utilisés pour relier les ordinateurs des réseaux locaux et leur fournir des informations. Les commutateurs fournissent des trames Ethernet aux périphériques hôtes identifiés par les adresses MAC de la carte réseau.

Dans la première partie, vous allez créer une topologie avec plusieurs commutateurs au moyen d'un trunk reliant les deux commutateurs. Dans la partie 2, vous allez envoyer des requêtes ping à différents appareils et observer comment les deux commutateurs créent leurs tables d'adresses MAC.

Remarque:Les commutateurs utilisés sont des modèles Cisco Catalyst 2960 équipés de Cisco IOS version 15.2(2) (image lanbasek9). D'autres commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent différer de ceux indiqués dans les travaux pratiques.

Remarque: vérifiez que les paramètre des commutateurs a été effacée et qu'ils ne présentent aucune configuration initiale. En cas de doute, contactez votre formateur.

Ressources requises

- 2 commutateurs (Cisco 2960 équipés de Cisco IOS version 15.2(2) image lanbasek9 ou similaires)
- 2 ordinateurs (Windows équipés d'un programme d'émulation de terminal tel que Tera Term)
- Câbles de console pour configurer les appareils Cisco IOS via les ports de console
- Câbles Ethernet conformément à la topologie

Remarque: les interfaces FastEthernet sur les commutateurs Cisco 2960 sont à détection automatique et un câble Ethernet droit peut être utilisé entre les commutateurs S1 et S2. Si vous utilisez un autre modèle de commutateur Cisco, un câble Ethernet croisé pourrait être nécessaire.

Instructions

Partie 1 : Construire et configurer le réseau

Étape 1: Câblez le réseau conformément à la topologie.

Étape 2: Configurez les PC hôtes.

Étape 3: Initialisez et redémarrez les commutateurs, le cas échéant.

Étape 4: Configurez les paramètres de base pour chaque commutateur.

a. Configurez le nom du périphérique conformément à la topologie.

b. Configurez l'adresse IP figurant dans la table d'adressage.

c. Attribuez le mot de passe **cisco** à la console et au vty.

d. Attribuez **class** comme mot de passe d'exécution privilégié.

Partie 2 : Analyser la table d'adresses MAC du commutateur

Un commutateur acquiert les adresses MAC et génère la table d'adresses MAC à mesure que les périphériques réseau établissent la communication sur le réseau.

Étape 1: Notez les adresses MAC des périphériques réseau.

a. Ouvrez une invite de commandes sur PC-A et PC-B, et tapez **ipconfig /all**.

Quelles sont les adresses physiques des adaptateurs Ethernet ?

Adresse MAC de PC-A :

Adresse MAC de PC-B:

b. Accédez aux commutateurs S1 et S2 par le biais de la console et tapez la commande **show interface F0/1** sur chaque commutateur.

Sur la deuxième ligne du résultat de la commande, quelles sont les adresses matérielles (ou adresses rémanentes [bia])?

Adresse MAC Fast Ethernet 0/1 de S1:

Adresse MAC Fast Ethernet 0/1 de S2:

Étape 2: Affichez la table d'adresses MAC du commutateur.

Accédez au commutateur S2 par le biais de la console et affichez la table d'adresses MAC, à la fois avant et après avoir exécuté les tests de communication réseau au moyen de requêtes ping.

a. Établissez une connexion console à S2 et passez en mode d'exécution privilégié.

b. En mode d'exécution privilégié, tapez la commande **show mac address-table** et appuyez sur Entrée.

```
S2# show mac address-table
```

Même s'il aucune communication réseau n'a été lancée sur l'ensemble du réseau (c-à-d., aucune utilisation de requêtes ping), il est possible que le commutateur ait acquis les adresses MAC à partir de sa connexion à l'ordinateur et à l'autre commutateur.

La table d'adresses MAC contient-elle des adresses MAC ?

Quelles adresses MAC sont enregistrées dans la table ? À quels ports de commutateur sont-elles associées et à quels périphériques appartiennent-elles ? Ignorez les adresses MAC qui sont associées au processeur.

Si vous n'avez pas noté les adresses MAC des périphériques réseau à l'étape 1, comment pouvez-vous savoir à quels périphériques les adresses MAC appartiennent, en utilisant uniquement le résultat de la commande **show mac address-table** ? Cela fonctionne-t-il dans tous les scénarios ?

Étape 3: Effacez la table d'adresses MAC de S2 et réaffichez la table d'adresses MAC.

a. En mode d'exécution privilégié, tapez la commande **clear mac address-table dynamic** et appuyez sur **Entrée**.

```
S1# clear mac address-table dynamic
```

b. Ressaisissez rapidement la commande **show mac address-table**.

La table d'adresses MAC contient-elle l'une des adresses de VLAN 1? D'autres adresses MAC sont-elles répertoriées ?

Attendez 10 secondes, tapez la commande **show mac address-table** et appuyez sur Entrée. La table d'adresses MAC contient-elles de nouvelles adresses ?

Étape 4: À partir de PC-B, envoyez une requête ping aux périphériques du réseau et examinez la table d'adresses MAC du commutateur.

a. À partir de PC-B, ouvrez une invite de commandes et tapez **arp -a**.

Sans compter les adresses de multidiffusion ou de diffusion, combien de paires d'adresses IP vers MAC de périphériques ont été acquises par ARP ?

b. À partir de l'invite de commandes de PC-B, envoyez des requêtes ping à PC-A, S1 et S2.

Tous les périphériques ont-ils reçu des réponses positives ? Dans le cas contraire, vérifiez votre câblage et vos configurations IP.

c. À partir d'une connexion console à S2, entrez la commande **show mac address-table**.

Le commutateur a-t-il ajouté des adresses MAC supplémentaires à la table d'adresses MAC ? Si oui, quelles adresses et quels périphériques ?

d. À partir de PC-B, ouvrez une invite de commandes et retapez arp -a.

Le cache ARP de PC-B contient-il des entrées supplémentaires pour tous les périphériques réseau auxquels des requêtes ping ont été envoyées ?

Question de réflexion

Sur les réseaux Ethernet, les données sont envoyées aux périphériques selon leur adresse MAC. Pour ce faire, les commutateurs et les ordinateurs génèrent de manière dynamique des caches ARP et des tables d'adresses MAC. Avec seulement quelques ordinateurs sur le réseau, ce processus semble assez facile. Quelles difficultés peut-on rencontrer sur les réseaux plus importants ?