Travaux pratiques - Utilisation de Wireshark pour l'examen de captures UDP

Topologie

Cette activité de TP mettra l'accent sur une capture UDP d'une session TFTP. Le PC doit disposer à la fois d'une connexion Ethernet et d'une connexion de console avec le commutateur S1.

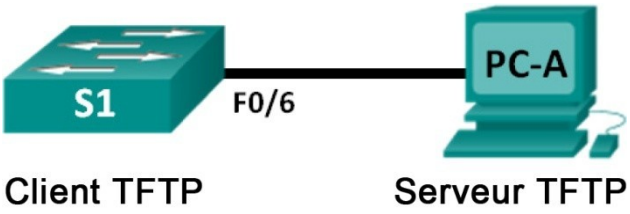


Table d'adressage (deuxième partie)

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
S1	VLAN 1	192.168.1.1	255.255.255.0	N/A
PC-A	Carte réseau	192.168.1.3	255.255.255.0	192.168.1.1

Objectif

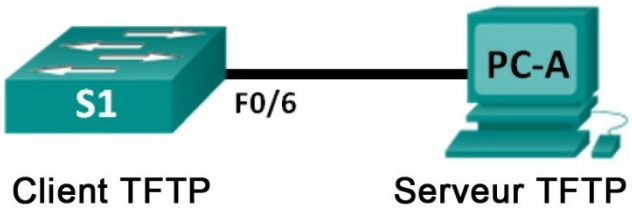
Identifier les champs d'en-tête UDP ainsi que les opérations UDP à l'aide de la capture de session TFTP de Wireshark

Contexte/scénario

Les deux protocoles de la couche transport TCP/IP sont le protocole TCP, défini dans le document RFC 761, et le protocole UDP, défini dans le document RFC 768. Les deux protocoles prennent en charge les communications du protocole de couche supérieure. Par exemple, TCP prend en charge la couche transport pour les protocoles HTTP (HyperText Transfer Protocol) et FTP, entre autres. UDP fournit notamment la prise en charge de la couche transport pour le système de noms de domaine (DNS) et TFTP.

Dans ce sujet de TP, vous utiliserez Wireshark pour capturer une session TFTP et examiner les champs d'en-tête UDP.

Étape 1: Installez cette topologie physique et préparez la capture TFTP.



a. Établissez une connexion de console et une connexion Ethernet entre PC-A et S1.

b. Configurez manuellement l'adresse IP sur le PC à la valeur 192.168.1.3. Il n'est pas obligatoire de définir la passerelle par défaut.

c. Configurez le commutateur. Attribuez l'adresse IP 192.168.1.1 à VLAN 1. Vérifiez la connectivité avec le PC en envoyant une requête ping à 192.168.1.3. Le cas échéant, procédez à un dépannage.

```
Switch> enable
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# host S1
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.1 255.255.255.0
S1(config-if)# no shut
*Mar  1 00:37:50.166: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Mar  1 00:37:50.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to up
S1(config-if)# end
S1# ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/203/1007 ms
```

d. Enregistrez la configuration en cours dans la mémoire NVRAM.

```
S1# copy run start
```

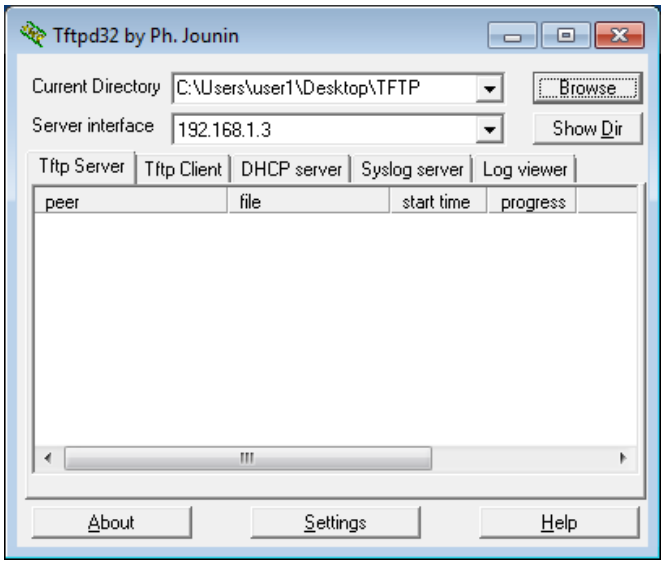
Étape 2: Préparez le serveur TFTP sur le PC.

a. S'il n'existe pas encore, créez un dossier sur le bureau de l'ordinateur appelé **TFTP**. Les fichiers du commutateur seront copiés à cet emplacement.

b. Démarrez **tftpd32** sur le PC.

c. Cliquez sur **Browse** (Parcourir) et remplacez le répertoire actuel par **C:\Users\user1\Desktop\TFTP** en remplaçant user1 par votre nom d'utilisateur.

Le serveur TFTP doit être similaire à celui-ci :



Notez que Current Directory (Répertoire actuel) indique l'utilisateur et l'interface du serveur (PC-A) avec l'adresse IP **192.168.1.3**.

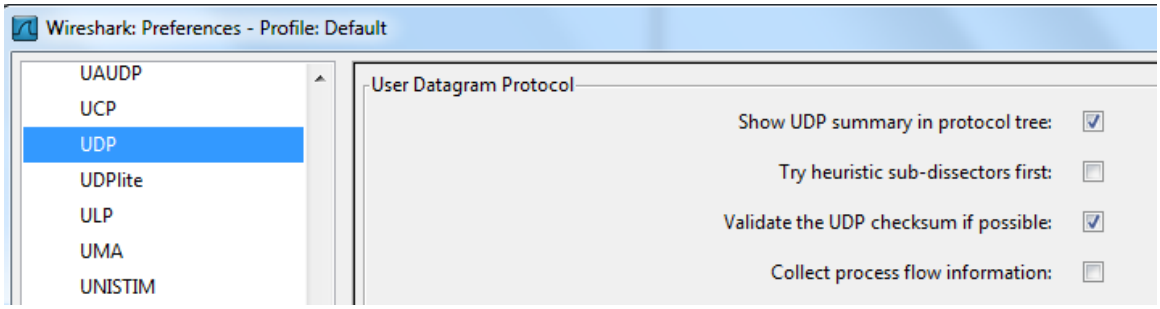
d. Testez la possibilité de copier un fichier en utilisant TFTP à partir du commutateur vers le PC. Le cas échéant, procédez à un dépannage.

```
S1# copy start tftp
Address or name of remote host []? 192.168.1.3
Destination filename [s1-confg]?
!!
1638 bytes copied in 0.026 secs (63000 bytes/sec)
```

Si vous voyez que le fichier a été copié, vous êtes prêt à passer à l'étape suivante. Si le fichier n'a pas été copié, procédez à un dépannage. Si vous obtenez l'erreur **%Error opening tftp (Permission denied)**, vérifiez d'abord que votre pare-feu ne bloque pas le protocole TFTP et que vous effectuez la copie vers un emplacement pour lequel votre nom d'utilisateur dispose des autorisations appropriées, comme l'ordinateur de bureau.

Étape 3: Capturer une session TFTP dans Wireshark

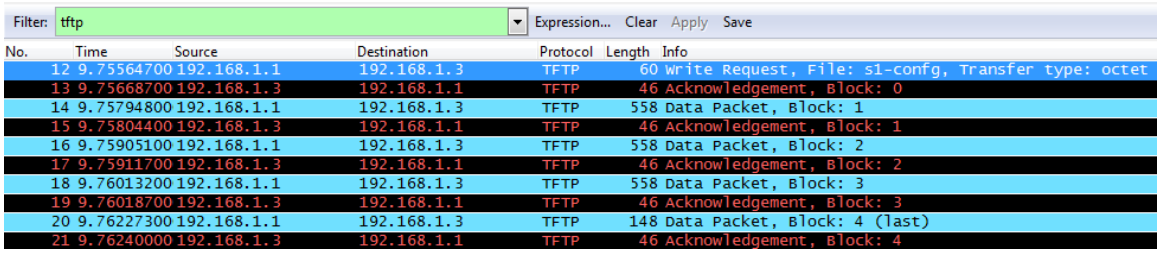
a. Ouvrez Wireshark. À partir du menu **Edit** (Edition), choisissez **Preferences** (Préférences) et cliquez sur le signe (+) pour développer **Protocols** (Protocoles). Faites défiler vers le bas, puis sélectionnez **UDP**. Activez la case à cocher **Validate the UDP checksum if possible** (Valider la somme de contrôle UDP si possible) et cliquez sur **Apply** (Appliquer). Cliquez ensuite sur **OK**.



b. Démarrez une capture Wireshark.

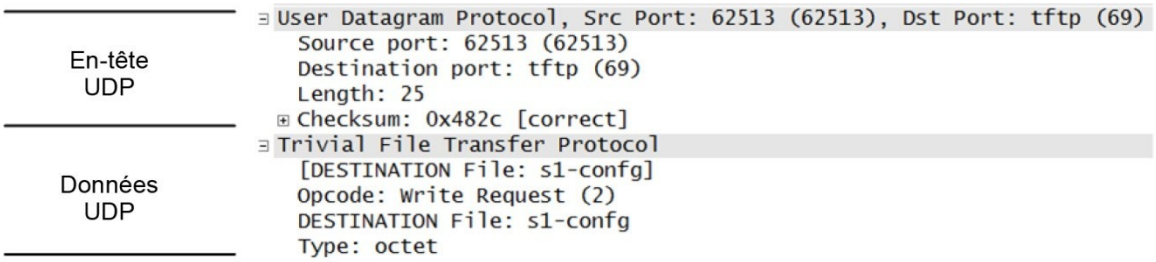
c. Exécutez la commande **copy start tftp** sur le commutateur.

d. Arrêtez la capture Wireshark.

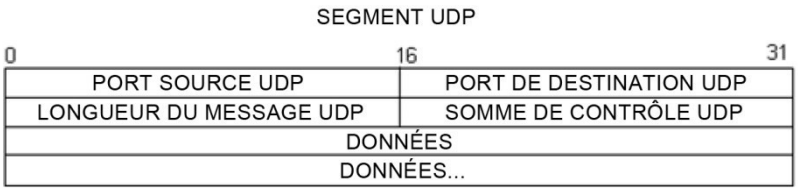


e. Définissez le filtre sur **tftp**. Les informations affichées doivent être similaires à celles figurant ci-dessus : Ce transfert TFTP permet d'analyser les opérations UDP de la couche transport.

Des informations UDP détaillées sont disponibles dans le volet de détails des paquets Wireshark. Sélectionnez le premier datagramme UDP à partir de l'ordinateur hôte, et déplacez le pointeur de la souris vers le volet de détails des paquets. Il peut s'avérer nécessaire de modifier le volet de détails des paquets et de développer l'enregistrement UDP en cliquant sur la zone de développement du protocole. Le datagramme UDP développé doit être semblable au schéma ci-dessous.



La figure ci-dessous représente un schéma de datagramme UDP. Les informations d'en-tête sont peu nombreuses par rapport au datagramme TCP. De même que pour le protocole TCP, chaque datagramme UDP est identifié par les ports source et de destination UDP.



À l'aide de la capture Wireshark du premier datagramme UDP, renseignez les informations concernant l'en-tête UDP. La somme de contrôle est une valeur hexadécimale (base 16), identifiée par le code 0x précédent :

Adresse IP source	
Adresse IP de destination	
Numéro du port source	
Numéro du port de destination	
Longueur du message UDP	
Somme de contrôle UDP	

De quelle manière UDP vérifie-t-il l'intégrité du datagramme ?

Examinez la première trame renvoyée par le serveur tftpd. Complétez les informations sur l'en-tête UDP :

Adresse IP source	
Adresse IP de destination	
Numéro du port source	
Numéro du port de destination	
Longueur du message UDP	
Somme de contrôle UDP	

```
⊟ User Datagram Protocol, Src Port: 58565 (58565), Dst Port: 62513 (62513)
    Source port: 58565 (58565)
    Destination port: 62513 (62513)
    Length: 12
  ⊞ Checksum: 0x8372 [incorrect, should be 0xa385 (maybe caused by "UDP checksum offload"?)]
⊟ Trivial File Transfer Protocol
    [DESTINATION File: s1-confg]
    Opcode: Acknowledgement (4)
    Block: 0
```

Remarque : le datagramme UDP de retour possède un port de source UDP différent. Toutefois, ce dernier sert au transfert TFTP restant. Étant donné que la connexion n'est pas fiable, seul le port source d'origine utilisé pour commencer la session TFTP sert à gérer le transfert TFTP.

Notez également que la somme de contrôle UDP est incorrecte. Ceci provient très probablement du déchargement de la somme de contrôle UDP. Pour plus d'informations sur la raison de cet événement, effectuez une recherche sur « UDP checksum offload » (Déchargement de la somme de contrôle).

Nettoyage

Sauf indication contraire de votre formateur :

1) Supprimez les fichiers qui ont été copiés sur votre ordinateur.
2) Supprimez les configurations sur S1.
3) Supprimez l'adresse IP manuelle du PC et restaurez la connectivité Internet.