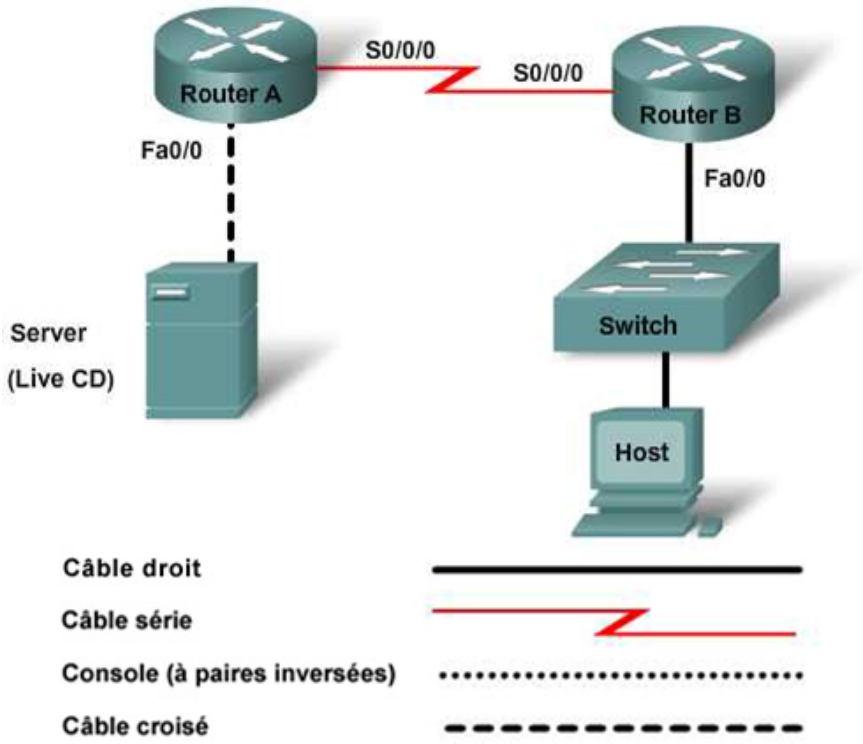
Travaux pratiques 1.2.2 : Capture et analyse du trafic réseau



Nom d'hôte	Adresse IP FA0/0	Masque de sous-réseau	Adresse IP S0/0/0	Masque de sous-réseau	Passerelle par défaut
RouterA	172.17.0.1	255.255.0.0	192.168.1.1 (**DCE**)	255.255.255.0	N/D
RouterB	192.168.3.1	255.255.255.0	192.168.1.2	255.255.255.0	N/D
Server	172.17.1.1	255.255.0.0			172.17.0.1
Switch					
Host	192.168.3.2	255.255.255.0			192.168.3.1

Objectifs

- Utiliser Wireshark pour capturer les paquets de données de protocole transitant par les réseaux
- Utiliser Wireshark pour analyser les paquets de données de protocole résultant de cette capture

Contexte / Préparation

Ces travaux pratiques concernent la configuration de base des routeurs Cisco 1841, ou d'autres routeurs équivalents, à l'aide de commandes Cisco IOS. Les informations de ces travaux pratiques s'appliquent à d'autres routeurs ; cependant la syntaxe des commandes peut varier. Le commutateur Cisco Catalyst 2960 est livré préconfiguré et nécessite uniquement l'attribution d'informations de sécurité de base pour être connecté à un réseau.

Ressources requises :

- Commutateur Cisco 2960, ou un autre commutateur équivalent
- Deux routeurs Cisco 1841, ou autres routeurs équivalents, équipés au minimum d'une interface série et d'une interface Fast Ethernet
- Deux PC Windows, dont un équipé d'un programme d'émulation de terminal. Premier PC utilisé en tant qu'hôte, second PC utilisé en tant que serveur
- 1 câble console avec connecteurs RJ-45/DB-9 pour configurer les routeurs
- 2 câbles droits Ethernet
- Un câble croisé Ethernet
- Accès à l'invite de commandes du PC
- Accès à la configuration réseau TCP/IP du PC

REMARQUE : assurez-vous que tous les routeurs, ainsi que le commutateur, ont été réinitialisés et vérifiez l'absence de configuration initiale. Si vous rencontrez des difficultés, reportez-vous à la procédure présentée à la fin de ces travaux pratiques. Des instructions concernant le commutateur et le routeur y sont présentées.

REMARQUE : Routeurs SDM – Si la configuration initiale (startup-config) est effacée dans un routeur SDM, le gestionnaire SDM ne s'affiche plus par défaut lors du redémarrage du routeur. Il est alors nécessaire de définir une configuration de base de routeur à l'aide des commandes IOS. Pour plus d'informations, adressez-vous à votre formateur.

Étape 1 : connexion des routeurs et configuration

a. Connectez les deux routeurs à l'aide d'un câble série. Le signal de synchronisation entre les deux routeurs est émis par le routeur A. Utilisez l'interface S0/0/0 sur les deux routeurs pour les connecter.

b. Utilisez le protocole RIP lors de la configuration des deux routeurs. Annoncez les réseaux appropriés sur chaque routeur.

c. En utilisant un câble croisé, connectez l'interface Fa0/0 du routeur A au serveur exécutant le CD Discovery Server Live.

d. Le routeur B utilise un câble droit, à partir de son interface Fa0/0, pour se connecter au commutateur via Fa0/1. Configurez les routeurs comme illustré dans le schéma de topologie ci-dessus.

Étape 2 : connexion de l'hôte au commutateur et configuration

Connectez l'hôte à relier au port de commutation Fast Ethernet Fa0/2. Configurez l'hôte comme illustré dans le schéma de topologie ci-dessus.

Étape 3 : utilisation d'une requête ping pour vérifier la connectivité

a. Pour vérifier si le réseau est correctement configuré, envoyez une requête ping au serveur à partir de l'hôte.

b. Si la requête ping échoue, vérifiez à nouveau les connexions et les configurations. Vérifiez si les câbles ne sont pas défectueux et si les connexions sont stables. Vérifiez les configurations de l'hôte, du serveur et du routeur.

c. La requête ping a-t-elle abouti ? _____

Étape 4 : lancement de Wireshark

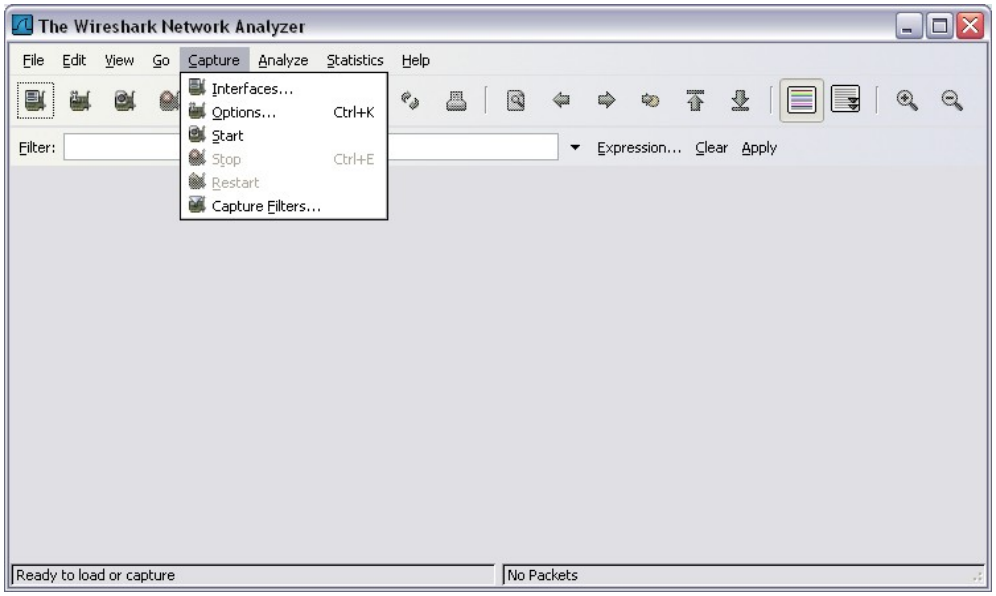
REMARQUE : vous pouvez télécharger Wireshark sur Internet à l'adresse www.wireshark.org, puis l'installer sur chaque hôte local. Vous pouvez également exécuter Wireshark à partir du CD Discovery Live. Demandez à votre formateur de vous indiquer la procédure la plus appropriée.

a. Si Wireshark s'exécute depuis l'hôte local, double-cliquez sur l'icône pour lancer l'application, et exécutez l'étape d. Si Wireshark s'exécute à partir du serveur Discovery, exécutez l'étape b.

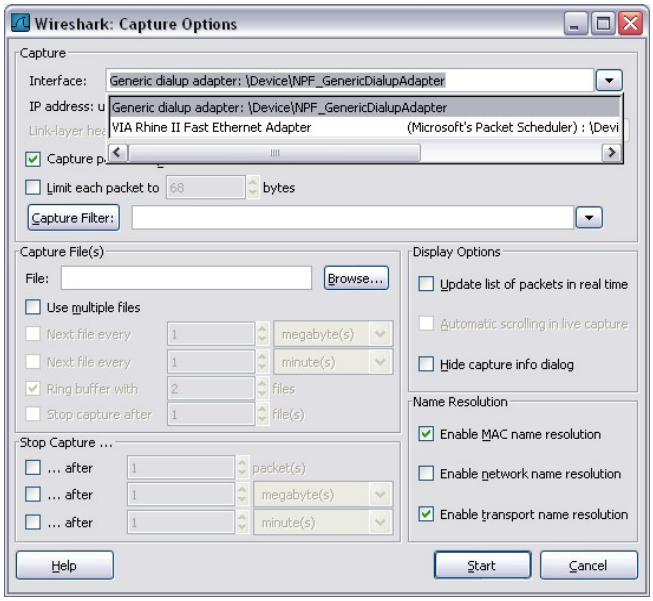
b. Sur le Bureau du serveur, dans le menu **K Start**, choisissez **Internet> Wireshark Network Analyzer**.

c. S'il n'est pas en cours d'exécution, lancez Wireshark. Si un mot de passe est demandé, entrez **discoverit**.

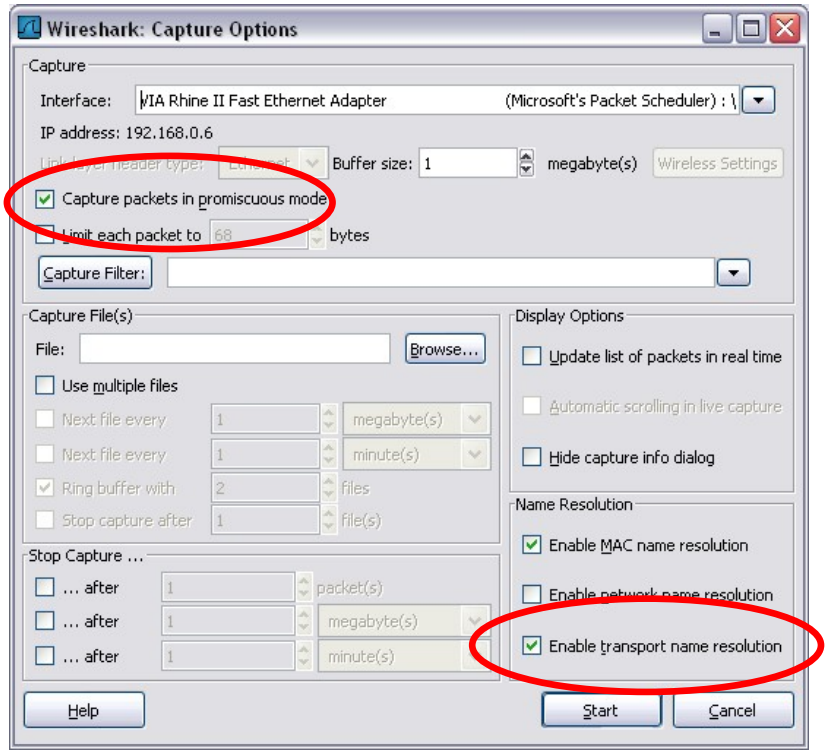
d. Pour lancer la capture des données, choisissez **Options** dans le menu **Capture**. La boîte de dialogue **Options** s'affiche et présente les paramètres et les filtres permettant de déterminer le volume de données capturées.



e. Vérifiez que Wireshark est configuré pour la gestion de l'interface. Dans la liste déroulante **Interface**, sélectionnez la carte réseau utilisée. En règle générale, il s'agit de la carte Ethernet du système.



f. D'autres options peuvent ensuite être définies. Examinons les deux options activées dans l'illustration suivante : Capture packets in promiscuous mode et Enable transport name resolution.



- **Activation de l'option Capture packets in promiscuous mode dans Wireshark**

  Si cette option n'est *pas activée*, seules les PDU (PDU) destinées à cet ordinateur sont capturées.

  Si cette option est activée, toutes les PDU destinées à cet ordinateur *ainsi que* celles détectées par la carte réseau de l'ordinateur situé sur le même segment de réseau, c'est-à-dire celles qui ont « transité » par la carte réseau mais qui ne sont pas destinées à l'ordinateur, sont capturées.

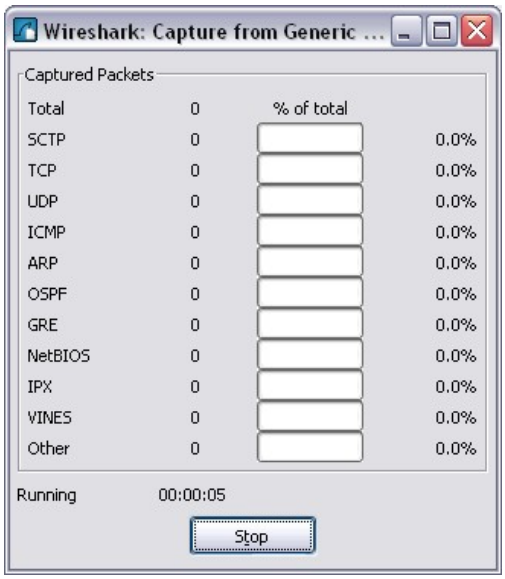
  REMARQUE : les résultats produits par Wireshark seront différents selon les périphériques intermédiaires utilisés pour la connexion au réseau (concentrateurs, commutateurs, routeurs).

- **Configuration de Wireshark pour la résolution de noms du réseau**

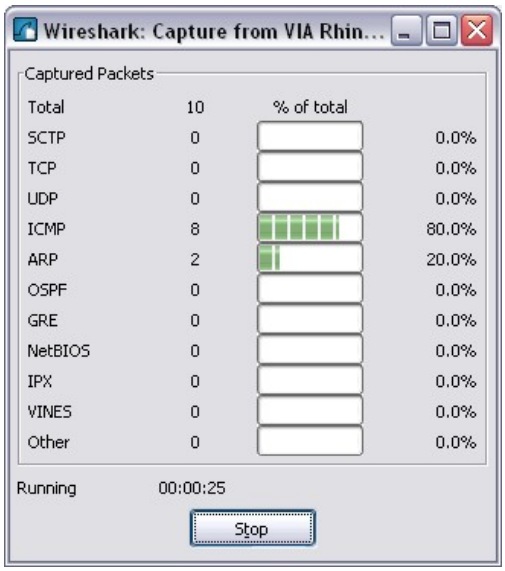
  Cette fonctionnalité permet de déterminer si les adresses réseau des PDU sont traduites en noms dans Wireshark. Malgré l'utilité de cette fonctionnalité, la résolution de noms ajoute généralement des PDU supplémentaires aux données capturées, ce qui peut causer une distorsion dans le processus d'analyse.

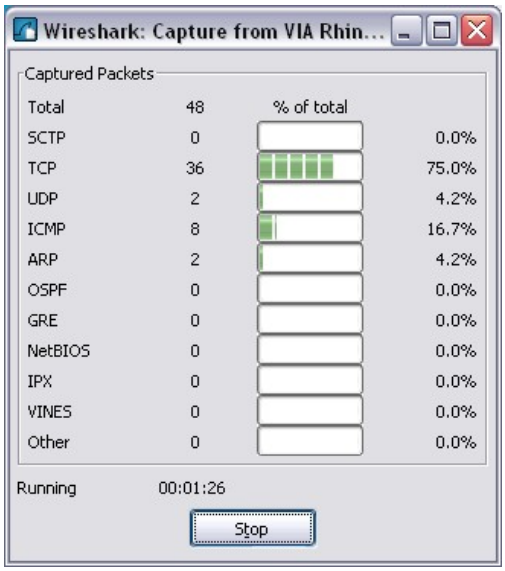
Cet écran contient également d'autres filtres de capture et d'autres paramètres de traitement.

- Cliquez sur le bouton **Start** pour lancer le processus de capture des données. Une boîte de dialogue s'affiche et présente l'évolution du processus.
- Créez le trafic à capturer. Lancez les commandes **`ping`** et **`tracert`** à partir de l'hôte et examinez les mises à jour de routage.



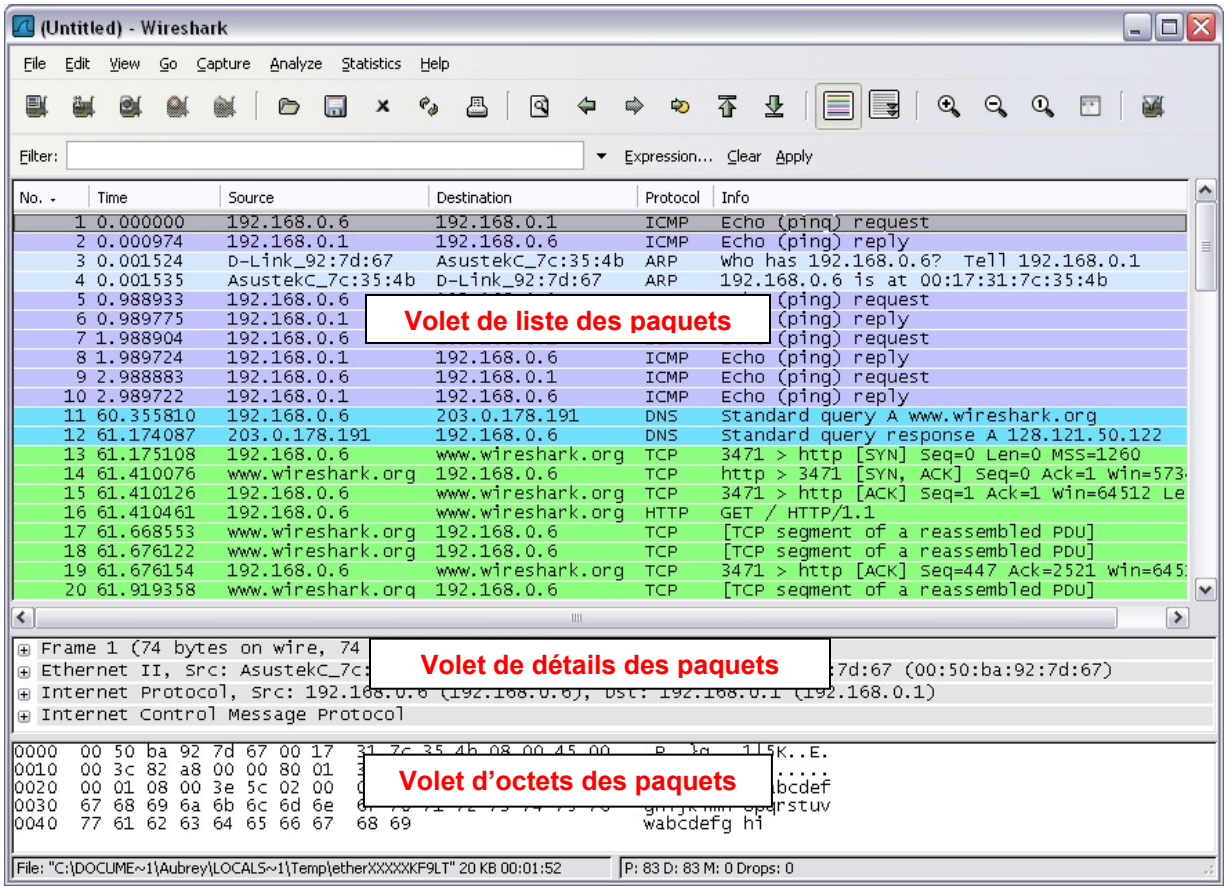
Le type et le nombre de PDU capturées sont renseignés dans la boîte de dialogue, au fur et à mesure de leur capture. Les boîtes de dialogue représentées ci-dessous illustrent un processus ping, suivi d'un accès à une page Web.





- Cliquez sur le bouton **Stop** pour terminer le processus de capture des données. La fenêtre principale s'affiche.

  Cette fenêtre principale de Wireshark est constituée de trois volets.



- Le volet de liste PDU (ou des paquets), situé dans la partie supérieure de la fenêtre, présente une synthèse de chaque paquet capturé. En cliquant sur les paquets affichés dans ce volet, vous contrôlez les éléments affichés dans les deux autres volets.
- Le volet de détails PDU (ou des paquets), situé dans la partie centrale de la fenêtre, présente en détail le paquet sélectionné dans le volet de liste des paquets.
- Le volet d'octets PDU (ou des paquets), situé dans la partie inférieure de la fenêtre, affiche les données réelles (en notation hexadécimale, représentant le format binaire réel) du paquet sélectionné dans le volet de liste des paquets, et met en surbrillance le champ sélectionné dans le volet de détails des paquets.

Volet de liste des paquets

Chaque ligne du volet de liste des paquets correspond à une unité de données de protocole ou à un paquet de données capturées. Si vous sélectionnez une ligne dans ce volet, des détails supplémentaires s'affichent automatiquement dans le volet de détails des paquets et dans le volet d'octets des paquets. L'exemple ci-dessus présente les PDU qui ont été capturées lors de l'utilisation de l'utilitaire ping et de l'accès au site http://www.Wireshark.org. Le paquet numéro 1 est sélectionné dans ce volet.

Volet de détails des paquets

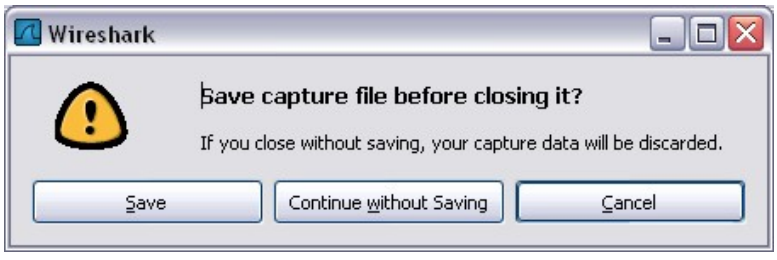
Le volet de détails des paquets présente les détails du paquet actuellement sélectionné dans le volet de liste des paquets. Ce volet affiche les protocoles et les champs de protocole du paquet sélectionné. L'arborescence des protocoles et des champs du paquet qui s'affiche peut être développée ou réduite.

Volet d'octets des paquets

Le volet d'octets des paquets présente les données du paquet actuellement sélectionné dans le volet de liste des paquets, dans un style appelé « hexdump ». Ce volet n'est pas examiné en détail dans le cadre de ces travaux pratiques. Toutefois, lorsqu'une analyse plus approfondie est requise, les informations affichées dans ce volet peuvent s'avérer très pratiques pour examiner les valeurs binaires et le contenu des unités de données de protocole.

Les informations capturées pour les PDU des données peuvent être enregistrées dans un fichier. Ce fichier peut être ouvert dans Wireshark à des fins d'analyse future, sans qu'il soit nécessaire de capturer à nouveau le même trafic de données. Les informations affichées lors de l'ouverture d'un fichier de capture sont identiques à celles de la capture initiale.

Lorsque vous fermez une fenêtre de capture de données, ou quittez Wireshark, un message s'affiche pour vous demander si les PDU capturées doivent être enregistrées.



Cliquez sur **Continue without Saving** pour fermer le fichier ou quitter Wireshark sans enregistrer les données capturées affichées.

Étape 5 : commande ping pour la capture des unités de données de protocole

a. Lancez Wireshark.

b. Configurez les options de capture tel que décrit à l'étape 4, et lancez le processus de capture.

c. À partir de la ligne de commande de l'hôte, envoyez une requête ping à l'adresse IP du serveur à l'autre extrémité de la topologie. Dans cet exemple, envoyez une requête ping au CD Discovery Server Live, en utilisant la commande **`ping 172.17.1.1`**.

d. Après la réponse d'écho positive de la requête ping dans la fenêtre de ligne de commande, arrêtez la capture de paquets.

Étape 6 : examen du volet de liste des paquets

a. Le volet de liste des paquets de Wireshark doit se présenter comme suit :

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_79:f3:80	CDP/VTP/DTP/PAgP/UDLD	CDP	Device ID: ROUTER_A Port ID: FastEthernet0/0
2	4.959859	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
3	5.555085	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
4	5.555108	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
5	6.557116	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
6	6.557137	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
7	7.557337	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
8	7.557359	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
9	8.557088	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
10	8.557111	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
11	10.557548	Intel_56:98:68	Cisco_79:f3:80	ARP	Who has 172.17.0.1? Tell 172.17.1.1
12	10.558224	Cisco_79:f3:80	Intel_56:98:68	ARP	172.17.0.1 is at 00:0d:28:79:f3:80

b. Dans les paquets de la liste, examinez les paquets 3 à 10.

c. Dans la liste des paquets de votre ordinateur, localisez les paquets équivalents. Il se peut que les chiffres soient différents.

d. Dans la liste de paquets de Wireshark, répondez aux questions suivantes :

1) Quel est le protocole utilisé par l'utilitaire ping ? _____

2) Quel est le nom complet du protocole ? _____

3) Quels sont les noms des deux messages ping ? _____ et _____

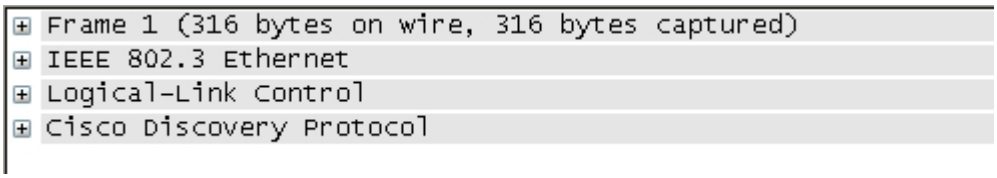
4) Les adresses IP d'origine et de destination affichées correspondent-elles à votre réponse ? _____

5) Pourquoi ?

_____

Étape 7 : examen du volet de détails des paquets

a. Sélectionnez (mettez en surbrillance) le premier paquet de requête d'écho de la liste. Le volet de détails des paquets doit se présenter comme suit :



b. Cliquez sur chacun des quatre signes **+** pour développer les informations. Le volet de détails des paquets doit se présenter comme suit :

```
Frame 1 (316 bytes on wire, 316 bytes captured)
    Arrival Time: Aug 12, 2007 16:26:56.565057000
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 316 bytes
    Capture Length: 316 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:llc:cdp:data]
    [Coloring Rule Name: Routing]
    [Coloring Rule String: hsrp || eigrp || ospf || bgp || cdp || vrrp || gvrp || igmp || ismp]
IEEE 802.3 Ethernet
  Destination: CDP/VTP/DTP/PAgP/UDLD (01:00:0c:cc:cc:cc)
  Source: Cisco_79:f3:80 (00:0d:28:79:f3:80)
    Length: 302
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
  Control field: U, func=UI (0x03)
    Organization Code: Cisco (0x00000c)
    PID: CDP (0x2000)
Cisco Discovery Protocol
    Version: 2
```

Comme vous pouvez le constater, les détails de chaque section et de chaque protocole peuvent être développés.

c. Développez l'arborescence pour faire défiler les informations. À ce niveau du cours, il est normal que vous ne compreniez pas toutes les informations affichées. Prenez note des informations que vous reconnaissez.

d. Localisez les deux types différents : Source et Destination.

Pourquoi sommes-nous en présence de deux types ?

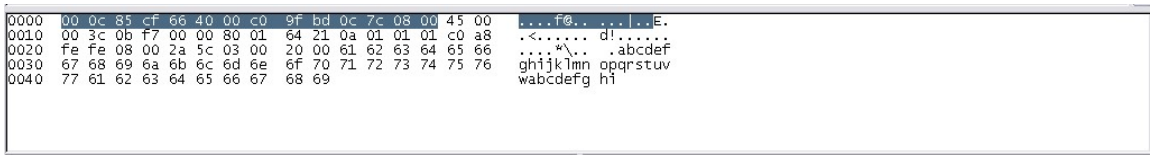
_____

Quels sont les protocoles de la trame Ethernet ?

_____

e. Sélectionnez une ligne dans le volet de détails des paquets (volet central). Notez que tout ou partie des informations du volet d'octets des paquets sont également mises en surbrillance.

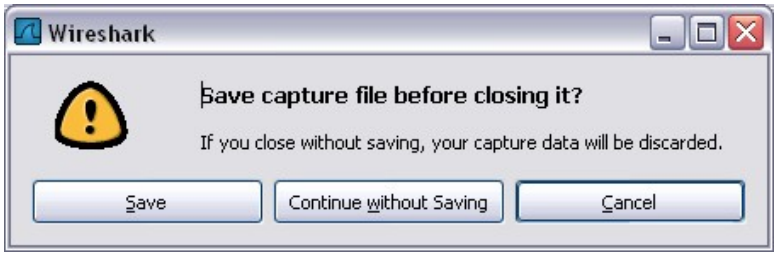
Par exemple, si la seconde ligne (+ Ethernet II) est mise en surbrillance dans le volet de détails, le volet d'octets met automatiquement les valeurs correspondantes en surbrillance.



Cet exemple affiche les valeurs binaires qui représentent ces informations dans l'unité de données de protocole. À ce niveau du cours, il n'est pas nécessaire de comprendre ces informations en détail.

f. Dans le menu **File**, sélectionnez **Close**.

g. Cliquez sur **Continue without Saving** lorsque la boîte de message suivante s'affiche :



Étape 8 : exécution d'une capture d'unité de données de protocole dans FTP

a. Si Wireshark est toujours en cours d'exécution depuis les étapes précédentes, lancez la capture de paquets en cliquant sur l'option **Start** dans le menu **Capture** de Wireshark.

b. Sur la ligne de commande de votre hôte, tapez **ftp 172.17.1.1**. Une fois la connexion établie, tapez **anonymous** comme nom d'utilisateur.

c. Une fois la session ouverte, tapez **get /pub/Discovery_1/document_1** et appuyez sur la touche **Entrée**. N'oubliez pas d'insérer un espace après **get**. Cette commande permet de lancer le téléchargement du fichier depuis le serveur ftp. Le résultat doit être similaire à celui-ci :

```
C:\> ftp 172.17.1.1
Connected to 172.17.1.1
220 Welcome to The CCNA-Discovery FTP service.
ftp> get /pub/Discovery_1/document_1
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for pub/Discovery_1/document_1
<73 bytes>.
226 File send OK.
ftp: 73 bytes received in 0.03Seconds 2.35Kbytes/sec.
```

d. Une fois le fichier téléchargé, tapez **quit**.

```
ftp> quit
221 Goodbye.

C:\>
```

e. Arrêtez la capture des unités de données de protocole dans Wireshark.

Étape 9 : examen du volet de liste des paquets

a. Agrandissez le volet de liste des paquets de Wireshark et faites défiler les PDU de la liste.

b. Localisez et consignez les PDU associées au téléchargement de fichier. Il s'agit des unités de données de protocole provenant du protocole de couche 4 TCP, et du protocole de couche 7 FTP.

c. Identifiez les trois groupes de PDU associés au transfert de fichier. Le premier groupe est associé à la phase d'ouverture de session et de connexion au serveur. Citez quelques exemples de messages échangés au cours de cette phase.

d. Localisez et citez des exemples de messages échangés au cours de la seconde phase, correspondant à la demande de téléchargement et au transfert de données.

e. Le troisième groupe de PDU correspond à la fermeture de session et à la déconnexion. Citez quelques exemples de messages échangés au cours de ce processus.

f. Localisez des échanges TCP récurrents dans le processus FTP. Quelle est la fonctionnalité TCP correspondante ?

Étape 10 : examen du volet de détails des paquets et du volet d'octets des paquets

a. Sélectionnez (mettez en surbrillance) un paquet dans la liste associée à la première phase du processus FTP. Examinez les détails du paquet dans le volet de détails des paquets.

b. Quels sont les protocoles encapsulés dans la trame ?

_____

c. Mettez en surbrillance les paquets contenant le nom d'utilisateur et le mot de passe. Examinez la section mise en surbrillance dans le volet d'octets des paquets. Que nous indique-t-elle sur la sécurité de ce processus d'ouverture de session FTP ?

_____

d. Mettez en surbrillance un paquet associé à la seconde phase. Dans l'un des volets, localisez le paquet contenant le nom de fichier. Quel est le nom de fichier de l'élément téléchargé ?

_____

e. Quand vous avez terminé, fermez le fichier Wireshark sans l'enregistrer.

Étape 11 : exécution d'une capture de PDU dans HTTP

a. Lancez la capture de paquet. Si Wireshark est toujours en cours d'exécution depuis les étapes précédentes, lancez la capture de paquets en cliquant sur l'option **Start** dans le menu **Capture** de Wireshark.

REMARQUE : les options de capture ne doivent pas être définies si vous avez effectué les étapes précédentes de ces travaux pratiques.

b. Lancez l'exécution d'un navigateur Web sur l'ordinateur exécutant Wireshark.

c. Entrez l'adresse IP du serveur Discovery 172.17.1.1 dans la barre d'adresse. Une fois la page Web téléchargée, arrêtez la capture de paquets dans Wireshark.

Étape 12 : examen du volet de liste des paquets

a. Agrandissez le volet de liste des paquets de Wireshark et faites défiler les PDU de la liste.

b. Localisez et identifiez les paquets TCP et HTTP associés à la page Web téléchargée.

c. Notez la similitude entre cet échange de message et l'échange FTP.

Étape 13 : examen du volet de détails des paquets et du volet d'octets des paquets

a. Dans le volet de liste des paquets, mettez en surbrillance un paquet HTTP dont la colonne **Info** comporte la mention **(text/html)**.

b. Dans le volet de détails des paquets, cliquez sur le signe **+** affiché en regard de la mention **Line-based text data : html**. En développant ces informations, quels sont les éléments affichés ?

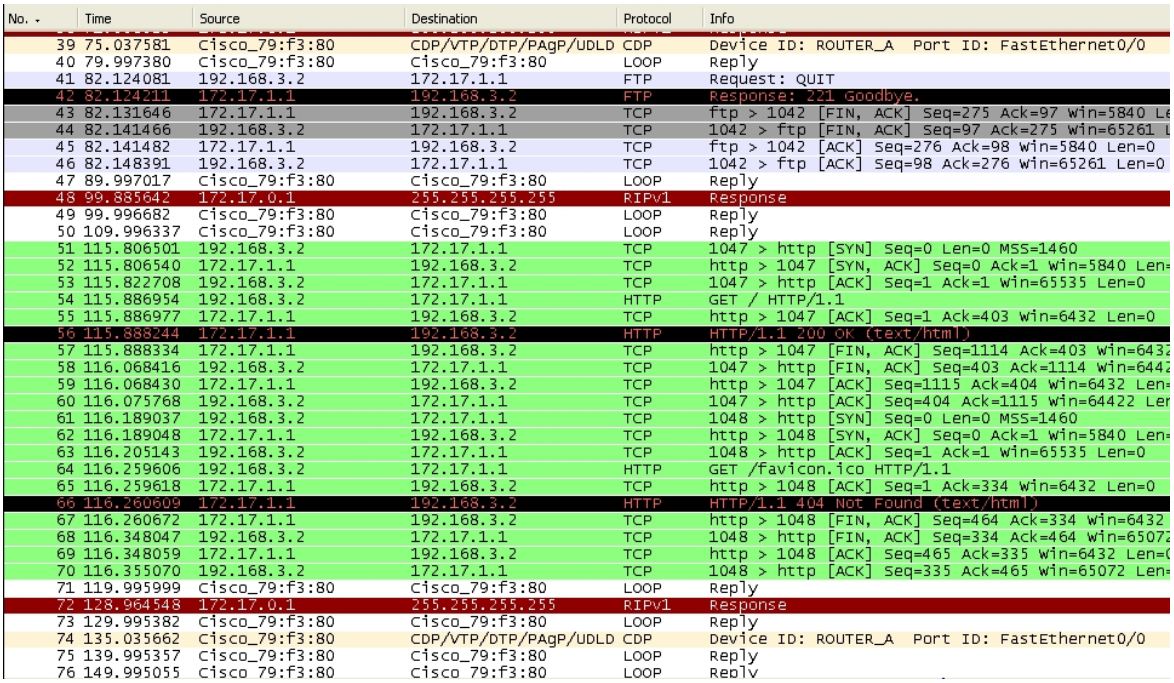
_____

c. Examinez la section mise en surbrillance dans le volet d'octets. Cette section présente les données HTML véhiculées par le paquet.

d. Quand vous avez terminé, fermez le fichier Wireshark sans l'enregistrer.

Étape 14 : analyse de la capture

a. Examinez la capture ci-dessous et notez les différents protocoles utilisés dans ce réseau.

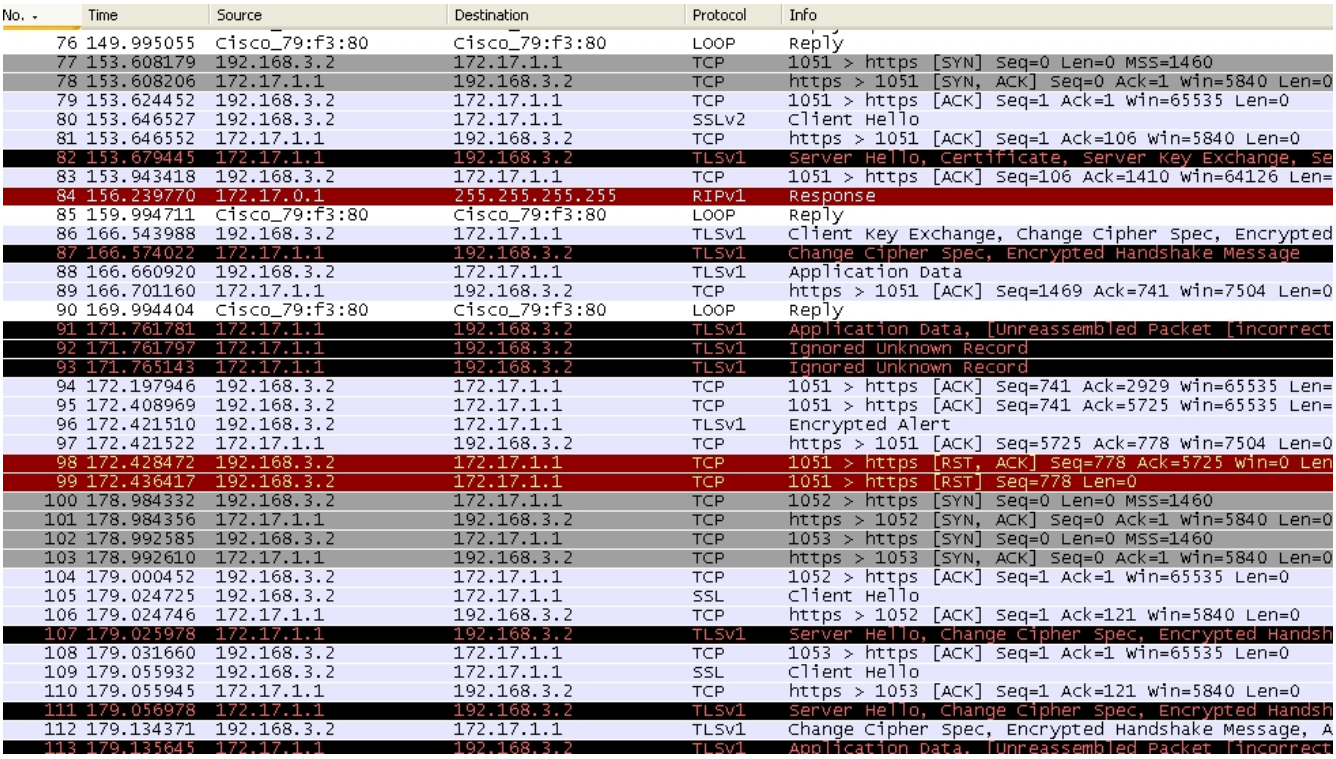


No.	Time	Source	Destination	Protocol	Info
39	75.037581	Cisco_79:f3:80	CDP/VTP/DTP/PAgP/UDLD	CDP	Device ID: ROUTER_A Port ID: FastEthernet0/0
40	79.997380	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
41	82.124081	192.168.3.2	172.17.1.1	FTP	Request: QUIT
42	82.124211	172.17.1.1	192.168.3.2	FTP	Response: 221 Goodbye.
43	82.131646	172.17.1.1	192.168.3.2	TCP	ftp > 1042 [FIN, ACK] Seq=275 Ack=97 Win=5840 Le
44	82.141466	192.168.3.2	172.17.1.1	TCP	1042 > ftp [FIN, ACK] Seq=97 Ack=275 Win=65261 L
45	82.141482	172.17.1.1	192.168.3.2	TCP	ftp > 1042 [ACK] Seq=276 Ack=98 Win=5840 Len=0
46	82.148391	192.168.3.2	172.17.1.1	TCP	1042 > ftp [ACK] Seq=98 Ack=276 Win=65261 Len=0
47	89.997017	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
48	99.885642	172.17.0.1	255.255.255.255	RIPv1	Response
49	99.996682	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
50	109.996337	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
51	115.806501	192.168.3.2	172.17.1.1	TCP	1047 > http [SYN] Seq=0 Len=0 MSS=1460
52	115.806540	172.17.1.1	192.168.3.2	TCP	http > 1047 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=
53	115.822708	192.168.3.2	172.17.1.1	TCP	1047 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
54	115.886954	192.168.3.2	172.17.1.1	HTTP	GET / HTTP/1.1
55	115.886977	172.17.1.1	192.168.3.2	TCP	http > 1047 [ACK] Seq=1 Ack=403 Win=6432 Len=0
56	115.888244	172.17.1.1	192.168.3.2	HTTP	HTTP/1.1 200 OK (text/html)
57	115.888334	172.17.1.1	192.168.3.2	TCP	http > 1047 [FIN, ACK] Seq=1114 Ack=403 Win=643
58	116.068416	192.168.3.2	172.17.1.1	TCP	1047 > http [FIN, ACK] Seq=403 Ack=1114 Win=644
59	116.068430	172.17.1.1	192.168.3.2	TCP	http > 1047 [ACK] Seq=1115 Ack=404 Win=6432 Len=
60	116.075768	192.168.3.2	172.17.1.1	TCP	1047 > http [ACK] Seq=404 Ack=1115 Win=64422 Len
61	116.189037	192.168.3.2	172.17.1.1	TCP	1048 > http [SYN] Seq=0 Len=0 MSS=1460
62	116.189048	172.17.1.1	192.168.3.2	TCP	http > 1048 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=
63	116.205143	192.168.3.2	172.17.1.1	TCP	1048 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
64	116.259606	192.168.3.2	172.17.1.1	HTTP	GET /favicon.ico HTTP/1.1
65	116.259618	172.17.1.1	192.168.3.2	TCP	http > 1048 [ACK] Seq=1 Ack=334 Win=6432 Len=0
66	116.260609	172.17.1.1	192.168.3.2	HTTP	HTTP/1.1 404 Not Found (text/html)
67	116.260672	172.17.1.1	192.168.3.2	TCP	http > 1048 [FIN, ACK] Seq=464 Ack=334 Win=6432
68	116.348047	192.168.3.2	172.17.1.1	TCP	1048 > http [FIN, ACK] Seq=334 Ack=464 Win=6507
69	116.348059	172.17.1.1	192.168.3.2	TCP	http > 1048 [ACK] Seq=465 Ack=335 Win=6432 Len=
70	116.355070	192.168.3.2	172.17.1.1	TCP	1048 > http [ACK] Seq=335 Ack=465 Win=65072 Len=
71	119.995999	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
72	128.964548	172.17.0.1	255.255.255.255	RIPv1	Response
73	129.995382	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
74	135.035662	Cisco_79:f3:80	CDP/VTP/DTP/PAgP/UDLD	CDP	Device ID: ROUTER_A Port ID: FastEthernet0/0
75	139.995357	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
76	149.995055	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply

b. Citez les protocoles utilisés dans le réseau présenté ci-dessus.

_____

c. Examinez la capture suivante.



No.	Time	Source	Destination	Protocol	Info
76	149.995055	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
77	153.608179	192.168.3.2	172.17.1.1	TCP	1051 > https [SYN] Seq=0 Len=0 MSS=1460
78	153.608206	172.17.1.1	192.168.3.2	TCP	https > 1051 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
79	153.624452	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
80	153.646527	192.168.3.2	172.17.1.1	SSLv2	Client Hello
81	153.646552	172.17.1.1	192.168.3.2	TCP	https > 1051 [ACK] Seq=1 Ack=106 Win=5840 Len=0
82	153.679445	172.17.1.1	192.168.3.2	TLSv1	Server Hello, Certificate, Server Key Exchange, Se
83	153.943418	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=106 Ack=1410 Win=64126 Len=
84	156.239770	172.17.0.1	255.255.255.255	RIPv1	Response
85	159.994711	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
86	166.543988	192.168.3.2	172.17.1.1	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted
87	166.574022	172.17.1.1	192.168.3.2	TLSv1	Change Cipher Spec, Encrypted Handshake Message
88	166.660920	192.168.3.2	172.17.1.1	TLSv1	Application Data
89	166.701160	172.17.1.1	192.168.3.2	TCP	https > 1051 [ACK] Seq=1469 Ack=741 Win=7504 Len=0
90	169.994404	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
91	171.761781	172.17.1.1	192.168.3.2	TLSv1	Application Data, [Unreassembled Packet [incorrect
92	171.761797	172.17.1.1	192.168.3.2	TLSv1	Ignored Unknown Record
93	171.765143	172.17.1.1	192.168.3.2	TLSv1	Ignored Unknown Record
94	172.197946	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=741 Ack=2929 Win=65535 Len=
95	172.408969	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=741 Ack=5725 Win=65535 Len=
96	172.421510	192.168.3.2	172.17.1.1	TLSv1	Encrypted Alert
97	172.421522	172.17.1.1	192.168.3.2	TCP	https > 1051 [ACK] Seq=5725 Ack=778 Win=7504 Len=0
98	172.428472	192.168.3.2	172.17.1.1	TCP	1051 > https [RST, ACK] Seq=778 Ack=5725 Win=0 Len
99	172.436417	192.168.3.2	172.17.1.1	TCP	1051 > https [RST] Seq=778 Len=0
100	178.984332	192.168.3.2	172.17.1.1	TCP	1052 > https [SYN] Seq=0 Len=0 MSS=1460
101	178.984356	172.17.1.1	192.168.3.2	TCP	https > 1052 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
102	178.992585	192.168.3.2	172.17.1.1	TCP	1053 > https [SYN] Seq=0 Len=0 MSS=1460
103	178.992610	172.17.1.1	192.168.3.2	TCP	https > 1053 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
104	179.000452	192.168.3.2	172.17.1.1	TCP	1052 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
105	179.024725	192.168.3.2	172.17.1.1	SSL	Client Hello
106	179.024746	172.17.1.1	192.168.3.2	TCP	https > 1052 [ACK] Seq=1 Ack=121 Win=5840 Len=0
107	179.025978	172.17.1.1	192.168.3.2	TLSv1	Server Hello, Change Cipher Spec, Encrypted Handsh
108	179.031660	192.168.3.2	172.17.1.1	TCP	1053 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
109	179.055932	192.168.3.2	172.17.1.1	SSL	Client Hello
110	179.055945	172.17.1.1	192.168.3.2	TCP	https > 1053 [ACK] Seq=1 Ack=121 Win=5840 Len=0
111	179.056978	172.17.1.1	192.168.3.2	TLSv1	Server Hello, Change Cipher Spec, Encrypted Handsh
112	179.134371	192.168.3.2	172.17.1.1	TLSv1	Change Cipher Spec, Encrypted Handshake Message, A
113	179.135645	172.17.1.1	192.168.3.2	TLSv1	Application Data, [Unreassembled Packet [incorrect

d. Quels sont les deux protocoles répertoriés dans cette capture et qui ne l'étaient pas dans la capture précédente ?

_____

e. Comparez la première capture de l'étape 14 avec la seconde capture. Quelle est la différence majeure entre les protocoles HTTP et HTTPS ?

_____

_____

Étape 15 : Remarques générales

Comment les modèles de couche OSI et TCP/IP sont-ils représentés dans les données de réseau capturées fournies par Wireshark ?

_____

_____

_____

Effacement et rechargement du commutateur

Dans la plupart des travaux pratiques de CCNA Discovery, il est nécessaire de commencer avec un commutateur non configuré. L'utilisation d'un commutateur déjà configuré peut produire des résultats imprévisibles. Les instructions suivantes permettent de préparer le commutateur avant d'effectuer les travaux pratiques pour que les options de configuration précédentes ne créent pas d'interférence. Elles sont fournies pour les commutateurs des gammes 2900 et 2950.

a. Passez en mode d'exécution privilégié à l'aide de la commande **enable**. Si un mot de passe vous est demandé, entrez **class** (si cela ne fonctionne pas, demandez de l'aide au formateur).

```
Switch>enable
```

b. Supprimez le fichier d'informations de la base de données VLAN.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?[Enter]
Delete flash:vlan.dat? [confirm] [Enter]
%Error deleting flash:vlan.dat (No such file or directory)
```

c. Supprimez de la mémoire vive non volatile (NVRAM) le fichier de configuration initiale du commutateur.

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
Erase of nvram: complete
```

d. Vérifiez que les informations VLAN ont été supprimées.

e. Redémarrez le logiciel à l'aide de la commande **reload.**

1) En mode d'exécution privilégié, entrez la commande **reload** :

```
Switch#reload
System configuration has been modified. Save? [yes/no]:
```

2) Tapez **n**, puis appuyez sur **Entrée**.

```
Proceed with reload? [confirm] [Enter]
Reload requested by console.
Would you like to enter the initial configuration dialog? [yes/no]:
```

3) Tapez **n**, puis appuyez sur **Entrée**.

```
Press RETURN to get started! [Enter]
```

Effacement et rechargement du routeur

a. Passez en mode d'exécution privilégié à l'aide de la commande **enable**.

```
Router>enable
```

b. À l'invite du mode d'exécution privilégié, entrez la commande **erase startup-config**.

```
Router#erase startup-config
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

c. Appuyez sur **Entrée** pour confirmer.

```
Erase of nvram: complete
```

d. En mode d'exécution privilégié, entrez la commande **reload**.

```
Router#reload
System configuration has been modified. Save? [yes/no]:
```


e. Tapez **n**, puis appuyez sur **Entrée**.

```
Proceed with reload? [confirm]
```

f. Appuyez sur **Entrée** pour confirmer.

```
Reload requested by console.
Would you like to enter the initial configuration dialog? [yes/no]:
```

g. Tapez **n**, puis appuyez sur **Entrée**.

```
Press RETURN to get started!
```

h. Appuyez sur **Entrée**.

Configuration IOS de base du routeur SDM pour afficher le gestionnaire SDM

Si la configuration initiale (startup-config) est effacée sur un routeur SDM, le gestionnaire SDM ne s'affiche plus par défaut au redémarrage du routeur. Vous devez créer une configuration de base comme suit : Pour plus d'informations sur la configuration et l'utilisation de SDM, reportez-vous au guide de démarrage rapide du gestionnaire SDM (SDM Quick Start Guide) :

http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/quick/guide/SDMq7.html

a. Définissez l'adresse IP de l'interface Fa0/0 du routeur.

```
Router(config)#interface Fa0/0
Router(config-if)#ip address 10.10.10.1 255.255.255.248
Router(config-if)#no shutdown
```

b. Activez le serveur HTTP/HTTPS du routeur, à l'aide des commandes Cisco IOS suivantes :

```
Router(config)#ip http server
Router(config)#ip http secure-server
Router(config)#ip http authentication local
```

c. Créez un compte utilisateur avec un niveau de privilège défini sur 15 (activez les privilèges).

```
Router(config)#username <nom d'utilisateur> privilege 15 password 0
<mot de passe>
```

d. Configurez SSH et Telnet pour la session locale et un niveau de privilège défini sur 15.

```
Router(config)#line vty 0 4
Router(config-line)#privilege level 15
Router(config-line)#login local
Router(config-line)#transport input telnet
Router(config-line)#transport input telnet ssh
Router(config-line)#exit
```

