TP 11: Wireshark Lab sur les applications:

Basé sur : Computer Networks, A Top-down Approach, 8th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2020.

DHCP

Ce TP sur DHCP suppose que vous pouvez activer DHCP ... les commandes données ici supposent un PC-Windows.

Pour observer le fonctionnement de DHCP, vous allez effectuer les opérations suivantes:

- 1. Effectuez un *"ipconfig /release"* dans le fenêtre de commande. Cette commande relâche votre adresse IP, qui devrait devenir 0.0.0.0
- 2. Lancez Wireshark
- 3. Effectuez un "*ipconfig /renew*". Ca demandera une nouvelle adresse IP à votre serveur DHCP
- 4. Dès que une adresse a été allouée (verifiez avec "*ipconfig*"), effectuez un deuxième "*ipconfig /renew*".
- 5. Effectuez "ipconfig/release"
- 6. Réeffectuez "ipconfig /renew"
- 7. Stoppez Wireshark.

Filtrez les paquets DHCP, en entrant "dhcp" comme filtre. DHCP utilise les ports, 67 et 68. Sur d'anciennes versions de Wireshark, ça pourrait être le filtre « bootp » Vous devriez obtenir un trace du type :

📶 (Untitled) - Wireshark									
Eile	<u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> ap	oture <u>A</u> nalyze <u>S</u> tatistics <u>F</u>	<u>l</u> elp						
	e e	🕷 🛛 🗁 🖬 🗙	% ≛ ସ ♦	a 🖒 1	후 전 또		Θ, Ο, 🖻		
<u>F</u> ilter:	Ejlter: bootp Expression Clear Apply								
No. +	Time	Source	Destination	Protocol	Info			Ē	
	1 0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discove	er – Transaction	ID 0xe220d8c		
	3 0.996942	192.168.2.1	255.255.255.255	DHCP	DHCP Offer	 Transaction 	ID 0xe220d8c		
	4 0.997777	0.0.0.0	255.255.255.255	DHCP	DHCP Request	t - Transaction	ID 0xe220d8c		
-	5 U.9985UL	192.168.2.1	200.200.200.200	DHCP	DHCP ACK	 Inansaction Transaction 	ID UXE22008C		
	26 10.367574	192.168.2.1	255.255.255.255	DHCP	DHCP REQUEST	- Transaction	TD 0xb40714e		
	29 18.103802	192.168.2.145	192.168.2.1	DHCP	DHCP Release	e - Transaction	ID 0xfa73f6d		
	30 26.509019	0.0.0.0	255.255.255.255	DHCP	DHCP Discove	er – Transaction	ID 0xee71773		
	32 27.502890	192.168.2.1	255.255.255.255	DHCP	DHCP Offer	 Transaction 	ID 0xee71773		
	33 27.503705	0.0.0.0	255.255.255.255	DHCP	DHCP Request	t - Transaction	ID 0xee71773		
	34 27.004404	192.108.2.1	200.200.200.200	DHCP	DHEP ACK	- inansaction	10 Uxee/1//3		
							F	Ě	
Le Bo	otstran Protoc	กไ						I Al	
	Message type:	Boot Request (1)						1	
	Hardware type	Ethernet							
	Hardware sype. Hardware addre	ss length: 6							
	Haruware auure. Hong: A	ss rengen. o							
	Tups. V	• 0xp330d8c3							
	Concorde allones	. 0xezz0u8c3							
	Seconds erapse								
±	BOOTP TIAGS: U	xuuuu (unicast)	~ `						
	Citent IP addr	ess: 0.0.0.0 (0.0.0	.0)						
	Your (client)	IP address: 0.0.0.0	(0.0.0.0)						
	Next server IP	address: 0.0.0.0 (0.0.0.0)						
	Relay agent IP	address: 0.0.0.0 (0.0.0.0)						
	Client MAC add	ress: Netgear_61:8e	:6d (00:09:5b:61:8	3e:6d)					
	Server host na	me not given							
	Boot file name	not given							
	Magic cookie:	(ок)							
Ŧ	Option: (t=53,	l=1) DHCP Message T	ype = DHCP Discove	en					
÷	Option: (t=116	,l=1) DHCP Auto-Con	figuration						
+	Option: (t=€1,1=7) Client identifier								
E I	H option: (t=50, 1=4) Requested IP Address = 192.168.2.145								
E I	Option: (t=12,1=10) Host Name = "wingamailg"								
	Option: (t=60,	l=8) vendor class i	dentifier = "MSFT	5.0"					
(F)	Option: (t=55.)]=11) Parameter Red	uest List						
	End Ontion								
	Padding								
0020	tt ff 00 44 0	0 43 01 34 79 df	01 01 06 00 e2 20	D.C	.4 y				
0030		00000000000000000000000000000000000000	3e 6d 00 00 00 00	•••••	Га.т.				
0050									
0060									
0070									
0000				••••					
00a0	00 00 00 00 00		00 00 00 00 00 00 00					-	
Bootstr	Bootstrap Protocol (bootp), 300 bytes P: 50 D: 11 M: 0 Drops: 0 //								

Faites une capture d'écran et répondez aux questions suivantes :

- 1. DHCP utilise t'il UDP ou TCP ?
- 2. Faites un diagramme illustrant la séquence des quatre premiers paquets Discover/Offer/Request/ACK DHCP échangés entre client et server. Pour chaque paquet, indiquez la source (IP/port) et la destination. Ces ports seront-ils les mêmes si vous réeffectuer une trace ?
- 3. Quelle est l'adresse Ethernet de votre hôte ?
- 4. Quelle valeurs, dans le message DHCP discover, le différencient du message DHCP request ?
- 5. Quelle est la valeur du Transaction-ID dans chacun des 4 premiers paquets (Discover/Offer/Request/ACK) DHCP messages? Et dans le deuxième groupe ? Quelle est l'utilité du Transaction-ID?
- 6. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.
- 7. Quelle est l'adresse de votre serveur DHCP ?
- 8. Quelle adresse IP vous est proposée dans le message DHCP Offer ? Quels sont les messages qui contiennent cette adresse IP.
- 9. Dans la capture d'écrant donnée en exemple, il n'y a pas de relais entre l'hôte et le serveur DHCP. Quelles valeurs indiquent l'absence de relais ? Si c'est le cas chez vous, quelle est l'adresse du relais ?
- 10. Quel est l'objectif du masque dans le message DHCP offer.
- 11. Quel est l'objectif du « lease time ». Combien vaut-il dans votre cas ?
- 12. Quel est l'objectif du message DHCP release? Le serveur DHCP émet-il un accusé de réception au DHCP request du client ? Que se passerait-il si le DHCP release était perdu ?
- 13. Désactivez le filtre *bootp*. Y a-t-il eu des échanges ARP pendant l'échange DHCP. Si oui, pourquoi ?

DNS

NSLOOKUP

Dans ce TP, nous utiliserons largement l'outil *nslookup*, qui est actuellement disponible sur la plupart des plateformes Linux / Unix et Microsoft, en ligne de commande.

Dans son fonctionnement le plus basique, l'outil nslookup permet à l'hôte exécutant l'outil d'interroger un serveur DNS spécifié pour un enregistrement DNS. Le serveur DNS interrogé peut être un serveur DNS racine, un serveur DNS de domaine de premier niveau, un serveur DNS faisant autorité ou un serveur DNS intermédiaire. Pour accomplir cette tâche, nslookup envoie une requête DNS au serveur DNS spécifié, reçoit une réponse DNS de ce même serveur DNS et affiche le résultat.

Par exemple :

```
nslookup www.unice.fr
```

la réponse de cette commande fournit deux informations: (1) le nom et l'adresse IP du serveur DNS qui fournit la réponse; et (2) la réponse elle-même, qui est le nom d'hôte et l'adresse IP de www.mit.edu. Bien que la réponse provienne du serveur DNS local de l'Université polytechnique, il est fort possible que ce serveur DNS local ait contacté de manière itérative plusieurs autres serveurs DNS pour obtenir la réponse.

La commande

nslookup -type=NS unice.fr

demandant spécifiquement les DNS liés à unice.fr.

A noter que nslookup peut également être exécuté en mode interactif (il suffit d'exécuter nslookup sans argument, et vous aurez un « prompt », et il faut alors entrer des commandes).

On notera également que sur Windows, les commandes

```
ipconfig /displaydns
ipconfig /flushdns
```

permettent d'afficher les DNS et également de les effacer de la configuration.

Explorer DNS avec Wireshark

- Utilisez ipconfig pour vider le cache DNS de votre hôte.
- Ouvrez votre navigateur et videz le cache de votre navigateur.
- Ouvrez Wireshark et entrez «ip.addr == your_IP_address» dans le filtre, où vous obtenez votre_IP_address avec ipconfig. Ce filtre supprime tous les paquets qui ne proviennent ni ne sont destinés à votre hôte.
- Démarrez la capture de paquets dans Wireshark.
- Avec votre navigateur, visitez la page Web: http://www.ietf.org
- Arrêtez la capture de paquets.
- Recherchez la requête DNS et les messages de réponse. Sont-ils envoyés via UDP ou TCP?
- Quel est le port de destination du message de requête DNS? Quel est le port source du message de réponse DNS?
- À quelle adresse IP le message de requête DNS est-il envoyé? Utilisez ipconfig pour déterminer l'adresse IP de votre serveur DNS local. Ces deux adresses IP sont-elles identiques?
- Examinez le message de requête DNS. De quel «type» de requête DNS s'agit-il? Le message de requête contient-il des «réponses»?
- Examinez le message de réponse DNS. Combien de «réponses» sont fournies? Que contient chacune de ces réponses?
- Considérez le paquet TCP SYN envoyé par votre hôte. L'adresse IP de destination du paquet SYN correspond-elle à l'une des adresses IP fournies dans le message de réponse DNS?
- Cette page Web contient des images. Avant de récupérer chaque image, votre hôte émet-il de nouvelles requêtes DNS?

Jouons maintenant avec nslookup.

- Démarrez la capture de paquets.
- Faites un nslookup sur www.mit.edu
- Arrêtez la capture de paquets.

Vous devriez obtenir une trace qui ressemble à ce qui suit:

🚺 (Untitled) - Wireshark							
<u>File E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze Statistics	Help					
	🕷 🕞 🖬 🗙	% 🕹 🍳 🗢	🕈 🔊 🔂 🖉				
Eilter: ip.addr == 192.168.2.145							
No Time	Source	Destination	Protocol Info	E			
1 0.000000	192.168.2.145	192.168.1.1	DNS Standard query	PTR 1.1.168.192.in-addr.ar			
3 0.013858	192.168.2.145	192.168.1.1	DNS Standard query	A www.mit.edu.myhome.weste			
4 0.074954	192.168.1.1	192.168.2.145	DNS Standard query	response			
5 0.084591 6 0.140633	192.168.2.145	192.168.1.1	DNS Standard query DNS Standard query	A www.mit.edu response A 18.7.22.83			
1	<u>.</u>						
⊕ Destination:	LinksysG_45:90:a8 (00:0c:41:45:90:a8)		-			
Source: Netg Trans. ID (0)	ear_61:8e:6d (00:09:	5b:61:8e:6d)					
Type: IP (UX	J800) col src• 197 168 7	145 (107 168 7 145)	Det: 107 168 1 1 (107	169 1 1)			
	Protocol. Src Port:	1565 (1565). Dst Por	t: domain (53)	.100.1.1)			
🗆 Domain Name Sy	Domain Name System (Juery)						
[Response In	: 6]						
Transaction	ID: 0×0003						
🗷 Flags: 0x0100 (Standard query)							
Questions: 1	Questions: 1						
Answer RRS:	Answer RRs: 0						
Additional R	AUTHOFITY KKS: U						
□ □ Oueries							
□ www.mit.edu: type A, class IN							
Name: ww	w.mit.edu						
Туре: А	(Host address)						
Class: I	N (0×0001)			x			
र							
0000 00 00 41 45	90 a8 00 09 5b 61	8e 6d 08 00 45 00	AE [a.mE. 9sí B	<u>~</u>			
0020 01 01 06 10		00 03 01 00 00 01					
	00 00 03 77 77 77 01 00 01	03 6d 69 74 03 65	w ww.mit.e				
HIE: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXa01796" 713 Bytes 00:00:(] P: 6 D: 6 M: 0 Drops: 0							

Nous voyons dans la capture d'écran ci-dessus que nslookup a en fait envoyé trois requêtes DNS et reçu trois réponses DNS. Dans le cadre de cette tâche, en répondant aux questions suivantes, ignorez les deux premiers ensembles de requêtes / réponses, car ils sont spécifiques à nslookup et ne sont normalement pas générés par des applications Internet standard. Vous devriez plutôt vous concentrer sur les derniers messages de requête et de réponse.

- Quel est le port de destination du message de requête DNS? Quel est le port source du message de réponse DNS?
- À quelle adresse IP le message de requête DNS est-il envoyé? Est-ce l'adresse IP de votre serveur DNS local par défaut?
- Examinez le message de requête DNS. De quel «type» de requête DNS s'agit-il? Le message de requête contient-il des «réponses»?
- Examinez le message de réponse DNS. Combien de «réponses» sont fournies? Que contient chacune de ces réponses?
- Fournissez une capture d'écran.

Maintenant, répétez l'expérience précédente, mais émettez plutôt la commande:

nslookup –type = NS mit.edu remplacer par dig nslookup www.aiit.or.kr bitsy.mit.edu

HTTP

1. L'interaction de base HTTP GET / réponse

Commençons notre exploration de HTTP en téléchargeant un fichier HTML très simple, très court et ne contenant aucun objet incorporé. Procédez comme suit:

- 1. Démarrez votre navigateur Web.
- 2. Démarrez Wireshark, Entrez «tcp port http» dans la fenêtre de spécification du filtre d'affichage.
- 3. Attendez un peu plus d'une minute puis commencez la capture de paquets Wireshark.
- 4. Entrez ce qui suit dans votre navigateur : <u>http://www.i3s.unice.fr/~deneire/test.html</u> vous devriez avoir un résultat simple
- 5. Arrêtez la capture de paquets Wireshark.

Votre fenêtre Wireshark doit ressembler à la fenêtre illustrée

•	 Display Ethernet: en8 (tcp port http) 							
	📕 🙋 🔘 📘	। 🛅 🖹 🤇	🔶 🍝 🖀 有	<u>↓</u>				
📙 htt	р				X			
No.	Time	Source	Destination	Protocol	Lengtr Info			
	7 0.028424	192.168.2.24	134.59.130.2	HTTP	692 GET /~deneire/test.html HTTP/1.1			
-	11 0.056652	Time (format as specified)	192.168.2.24	HTTP	71 HTTP/1.1 200 OK (text/html)			
	16 0.985719	192.168.2.24	192.168.2.5	HTTP	150 GET /device HTTP/1.1			
	18 1.015065	192.168.2.5	192.168.2.24	HTTP/XML	340 HTTP/1.0 200 OK			
	27 4.143673	192.168.2.24	17.253.109.201	HTTP	183 GET / HTTP/1.1			
	29 4.160076	17.253.109.201	192.168.2.24	HTTP	780 HTTP/1.1 200 OK (text/html)			
h Er	Since 7, 602 between view (SE26 between sections) (SE26 between sections) and a							
> F1	hornot TT Srci Ann	Wire (5550 bits), 09	2 bytes captured (55	shows 61.68.56 (14.0c.76.61.b9.5b)			
P EL	ternet II, Src: App	ciep 4 Erc: 102 169	2 24 Det: 124 E0 12	enox2_01:00:30 (14:00:/0:01:08:50/			
	ansmission Control	Drotocol Erc Dort: E	2.24, DSL: 134.39.13	Cogi 1 Acki 1	Long 626			
	anshission control	etecel	7707, DSt PUTL: 00,	Seq: 1, ACK: 1,	Len: 020			
Р	percext fransfer Pr	010001						
0000	14 0c 76 61 b8 5k	a8 20 66 2e 25 df	08 00 45 00	. f &E.				
0010	02 a6 00 00 40 00	40 06 00 00 c0 a8	02 18 86 3b ····@·	a				
0020	82 02 e1 a7 00 50	4e 6c 59 19 d8 db	52 7b 80 18 ·····P	NÎLY···R{··				
0030	08 04 cd 96 00 00	0 01 01 08 0a 25 3c	4b 45 cb 21 ·····	••••% <ke•!< td=""><td></td><td></td></ke•!<>				
0040	e2 7e 47 45 54 20	2f 7e 64 65 6e 65	69 72 65 2f ~GET	/~ deneire/				
0050	74 65 73 74 2e 68	3 74 6d 6c 20 48 54	54 50 2f 31 test.h	tm L HTTP/1				
0000	Ze 31 00 0a 48 01	13 74 30 20 77 77 8 65 20 66 72 0d 0a	43 6f 6e 6e - sunic	e fru Conn				
0080	65 63 74 69 6f 6e	3a 20 6b 65 65 70	2d 61 6c 69 ection	: keep-ali				
0090	76 65 0d 0a 43 61	63 68 65 2d 43 6f	6e 74 72 6f ve··Ca	ch e-Contro				
00a0	6c 3a 20 6d 61 78	3 2d 61 67 65 3d 30	0d 0a 55 70 l: max	-a ge=0 · · Up				
00b0	67 72 61 64 65 20	49 6e 73 65 63 75	72 65 2d 52 grade-	In secure-R				
00c0	65 71 75 65 73 74	73 3a 20 31 0d 0a	55 73 65 72 equest	s: 1 User				
00d0	2d 41 67 65 6e 74	3a 20 4d 6f 7a 69	6c 6c 61 2f -Agent	: Mozilla/				
00e0	35 Ze 30 20 28 40	1 01 03 09 66 74 6T	73 08 30 20 5.0 (M 20 58 20 31 Totol	ac intosh; Ma c OS X 1				
0010			20 50 20 51 Intet	HU C US A 1				
	Hypertext Transfer Protocol: Protocol: Protocol Packets: 34 · Displayed: 6 (17.6%) · Dropped: 0 (0.0%) • Profile: Default							

L'exemple de la figure 1 montre dans la fenêtre de liste des paquets que deux messages HTTP ont été capturés: le message GET et le message de réponse du serveur à votre navigateur. La fenêtre du contenu des paquets affiche les détails du message sélectionné (dans ce cas, le message HTTP OK). En examinant les informations contenues dans HTTP GET et les messages de réponse, répondez aux questions suivantes. Lorsque vous répondez aux questions suivantes, vous devez imprimer les messages GET et de

- 1. Votre navigateur exécute-t-il la version 1.0 ou 1.1 de HTTP? Quelle version de HTTP le serveur exécute-t-il?
- 2. Quelles langues (le cas échéant) votre navigateur indique-t-il qu'il peut accepter le serveur?
- 3. Quelle est l'adresse IP de votre ordinateur? Du serveur?
- 4. Quel est le code d'état renvoyé par le serveur à votre navigateur?
- 5. Quand le fichier HTML que vous récupérez a-t-il été modifié pour la dernière fois sur le serveur?
- 6. Combien d'octets de contenu sont renvoyés à votre navigateur?
- 7. En inspectant les données brutes dans la fenêtre de contenu des paquets, voyezvous des en-têtes dans les données qui ne sont pas affichés dans la fenêtre de liste des paquets? Si oui, nommez-en un.