Travaux Dirigés Architecture en couches, DNS et TCP

Exercice 1

Multiplexage et architecture en couches

Un utilisateur sur telesun.imag.fr (adresse IP 195.221.228.9) exécute un navigateur WWW pour accéder aux documents sur web.ensimag.fr (adresse IP 195.221.228.24). Au même instant, un autre utilisateur travaillant sur la même machine telesun utilise ssh pour travailler sur web.ensimag.fr.

Question 1. Faites un schéma qui présente l'architecture en couches des protocoles utilisés, les points de connexion avec les ports et adresses, et les chemins empruntés par

les données échangées au niveau de ces applications.

Exercice 2

Analyse de réponse DNS

Nous poursuivons l'étude de la capture de trafic étudiée lors du TD 1.

On s'intéresse à la réponse DNS qui se trouve dans la trame 4 (nous avions vu la requête DNS en trame 3), détaillée dans la figure 1. La réponse DNS rappelle la question, puis fournit 12 éléments de réponse, appelés RR, répartis en trois catégories.

Question 2. Rappelez ce que signifie RR dans le DNS, l'origine de la terminologie, et les

informations qu'ils peuvent contenir.

Question 3. Pourquoi y a-t-il 2 « Answers » et non pas une seule ?

Question 4. A quoi servent les 4 éléments de réponses classés « Authoritative nameservers » ? Dans quels cas seraient-ils utilisés ?

Question 5. Pourquoi y a-t-il des « Additional RR » ? Pourquoi ne pouvait-on fournir et trouver les informations correspondantes dans la catégorie au-dessus ?

<u>Question 6.</u> En revenant à la suite des échanges (trames 7 et suivantes) quel(s) élément(s) de réponse ont été réellement utilisés ?

En-tête TCP (1er aperçu)

On regarde maintenant l'en-tête TCP de la trame 8, en figure 2. Octets surlignés : en-tête IP.

Question 7. Repérez d'abord les octets correspondant aux différents champs (ports source et destination, numérotation des octets, longueur etc.). Indiquez ce que vaut chacun en hexadécimal.

Question 8. Pourquoi Wireshark écrit-il TCP dans la colonne Protocol de la trame 8 et HTTP pour la trame 10 ? Et que représente le http en minuscule qui apparaît au début de la colonne Info : « http > 50064 » ?

Ouestion 9. Où se trouvent les drapeaux? Comment y décode-t-on que les deux drapeaux SYN et ACK sont levés (et pas les autres)?

Question 10. Quel sera le numéro (absolu) du premier octet de la couche application (requête HTTP) qui sera envoyé par la machine 130.190.123.77?

Question 11. Que recouvre la longueur de 40 octets?

Réponse HTTP

Question 12. Comment le client DNS savait-il que la réponse contenue dans la trame 4 était bien une réponse à sa question posée en trame 3 (dans le dialogue complet, on voit que le client pose successivement deux questions, une pour web.ensimag.fr, l'autre pour www.ensimag.fr)? Et comment le navigateur de la machine 130.190.123.77 sait-il que la réponse du serveur « Not modified » en trame 12 correspond bien à sa requête en trame 10? Comparez ces deux mécanismes (entre la solution pour le DNS et celle pour HTTP).

Question 13. Vous pourrez étudier si vous le souhaitez les en-têtes TCP et HTTP de la trame 12 (figure 3).

No. Time	Source	Destination	Protocol	Info	
9 4.164252	130.190.123.77	195.221.228.2	TCP	50064 > http [AC	CK] Seq=1 Ack=1 Win=524280 L
10 4.164383	130.190.123.77	195.221.228.2	HTTP	GET / HTTP/1.1	
11 4.165886	195.221.228.24	130.190.123.7	TCP		CK] Seq=1 Ack=496 Win=6912 L
12 4.166390	Martin Colorest State of State of Color State of	130,190,123,7		HTTP/1.1 304 Not	The second secon
	130.190.123.77		AND DESCRIPTION OF THE PARTY OF		CK] Seq=496 Ack=151 Win=5242
14 4.166444	195.221.228.24	130.190.123.7	TCP	http > 50064 [FT	N. ACKI Seg=151 Ack=496 Win
4 (112	PERSONAL PROPERTY OF THE PROPE		The spirit of th	· management she	,
Frame 12: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits)					
Ethernet II, Src: Cisco_da:22:80 (00:25:84:da:22:80), Dst: Apple_20:c4:b0 (b8:8d:12:20:c4:b0)					
▶ Internet Protocol Version 4, Src: 195.221.228.24 (195.221.228.24), Dst: 130.190.123.77 (130.190					
▼ Transmission Control Protocol, Src Port: http (80), Dst Port: 50064 (50064), Seq: 1, Ack: 496,					
Source port: http (80)					
Destination port: 50064 (50064)					
[Stream index: 0]					
Sequence number: 1 (relative sequence number)					
[Next sequence number: 151 (relative sequence number)]					
Acknowledgment number: 496 (relative ack number)					
Header length: 32 bytes					
▶ Flags: 0x018 (PSH, ACK)					
Window size value: 54					
[Calculated window size: 6912]					
[Window size scaling factor: 128]					
D Checksum: Oxc75a [correct]					
D Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps					
D [SEQ/ACK analysis]					
∀ Hypertext Transfer Protocol					
D HTTP/1.1 304 Not Modified\r\n					
Date: Mon, 10 Sep 2012 09:38:01 GMT\r\n					
Server: Apache/2.2.3 (CentOS)\r\n					
Connection: close\r\n					
ETag: "554735-578-480bec9a4b980"\r\n					
\r\n					
firm 1/17					

Figure 3. Détail trame 12: réponse HTTP

Destination | Protocol Info No. | Time Source Standard query 0x9e63 A web.ensimag.fr 3 0.004187 130.190.123.77 193.54.188.33 DNS ▼ Domain Name System (response) [Request In: 3] [Time: 0.003031000 seconds] Transaction ID: 0x9e63 ▶ Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 2 Authority RRs: 4 Additional RRs: 6 ▽ Queries ▼ web.ensimag.fr: type A, class IN Name: web.ensimag.fr Type: A (Host address) Class: IN (0x0001) D web.ensimag.fr: type CNAME, class IN, cname web-ensimag.imag.fr D web-ensimag.imag.fr: type A, class IN, addr 195.221.228.24 ▼ Authoritative nameservers D imag.fr: type NS, class IN, ns isis.imag.fr D imag.fr: type NS, class IN, ns dns.inria.fr D imag.fr: type NS, class IN, ns ns2.nic.fr D imag.fr: type NS, class IN, ns imag.imag.fr ▼ Additional records D dns.inria.fr: type A, class IN, addr 193.51.208.13 D ns2.nic.fr: type A, class IN, addr 192.93.0.4 D ns2.nic.fr: type AAAA, class IN, addr 2001:660:3005:1::1:2 D imag.imag.fr: type A, class IN, addr 129.88.30.1 D imag.imag.fr: type AAAA, class IN, addr 2001:660:5301:le::101 D isis.imag.fr: type A, class IN, addr 129.88.32.24 4 6000 b8 8d 12 20 c4 b0 00 25 84 da 22 80 08 00 45 00 .7....?. ...6.1..

0010 01 37 15 ad 00 00 3f 11 e9 a5 c1 36 bc 21 82 be 0020 7b 4d 00 35 c5 5a 01 23 8f 7d 9e 63 81 80 00 01 {M.5.Z.# .}.c... 0030 00 02 00 04 00 06 03 77 65 62 07 65 6e 73 69 6dw eb.ensim

Figure 1. Détail trame 4 : réponse DNS

intro_IRC_10sep12_ex_Web_bis [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)] Elle Edit View Go Capture Analyze Statistics Telephony Tools Internals Help Q Q Q F 10、每日日本 BRXSB Filter: Expression... Clear Apply No. Time Source Destination Protocol Info Standard query response CNAME www-ensimag.imag.fr CNAME we 6 0.029449 193.54.188.33 130.190.123.77 DNS 50064 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSV 7 4.160316 130.190.123.77 195.221.228.24 TCP N. ACK] Seq=0 Ack=1 Win=575/2 Len=0 MSS=14 8 4.164126 50064 > http [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=6250 9 4.164252 130.190.123.77 195.221.228.24 TCP מדדע אל פכל וכל 201 דל בלו חמו חבו בפלאו א חו D Frame 8: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) D Ethernet II, Src: Cisco_da:22:80 (00:25:84:da:22:80), Dst: Apple_20:c4:b0 (b8:8d:12:20:c4:b0) 1 130, 190, 123, 77 (130, 190, 123, Transmission Control Protocol, Src Port: http (80), Dst Port: 50064 (50064), Seq: 0, Ack: 1, Len: 0 Source port: http (80) Destination port: 50064 (50064) [Stream index: 2] Sequence number: 0 (relative sequence number) Acknowledgement number: 1 (relative ack number) Header length: 40 bytes D Flags: Ox12 (SYN, ACK) Window size value: 5792 [Calculated window size: 5792] D Checksum: 0x7d88 [correct] ♥ Options: (20 bytes) Maximum segment size: 1460 bytes TCP SACK Permitted Option: True D Timestamps: TSval 8478111, TSecr 625068780 No-Operation (NOP) D Window scale: 7 (multiply by 128) 0000 b8 8d 12 20 c4 b0 00 25 84 da 22 80 08 00 8 .. " ... 0010 00 50 c3 90 le 2c e9 3a 37 b8 bc 77 a0 12 16 a0 7d 88 00 00 02 04 05 b4 04 02 08 0a 00 81 .P..., .:7..w.. 0020 0030 .} 0040 5d 9f 25 41 ca ec 01 03 03 07].%A....

O Internet Protocol V... Packets: 78 Displayed: 78 Marked: 0 Load time: 0:00.079

Figure 2. Détail trame 8 : TCP SYNACK.

Exo1 1) Part Petto: 80 Part 88h : 22 Telesur. mag. fr ueb. ensimag. fr Apache sehd 5002 HTTP 8844 5001 80 HTTP 8841

7CP meltiplosogy TCP

IP 22 195.221.228.24 V donulliplex. Ethernet

Cthernet Ethernet Ethernet 2) RR: ressource record: Données suregrations dans le DNS Moss le forme non + option + valeur telesur imag. fr A 195.221.223.9 (IP du rom BNS)

imag. fr NS ns. imag. fr (namo sendeur => plusieurs sendeurs
regroupés pour frabilités)

ensimag. fr CNAME telesur. imag. fr (alleas) 3) On pose la prestion sur un alias Rop 1 -> Nous donne le rom canonique Ropl _ noos donne l'adresse IP 4) Les 4 éléments réponses nont les noms serveuxs Ils seraient utilisés pour avoir une réponse d'autorité et non du cache 5) Ce sont des enrogretments supplémentaires (cache) Lo On a desoitement l'IP au lieu de separse une recharche de von