

Compte-rendu de TP réseau

Wireshark et HTTP

Table des matières

Réponses aux questions.....	1
Exercice 1 : nslookup.....	1
Exercice 2 : codage des caractères.....	1
Exercice 3 : codage des adresses IPv4.....	2
Exercice 4 : capture réseau.....	2
Exercice 5 : couche applicative.....	2
Exercice 6 : pile protocolaire.....	3
Bilan.....	4

Réponses aux questions

Exercice 1 : nslookup

Nous commençons ce TP en utilisant la commande nslookup pour trouver l'adresse IP associé au nom www.blagnac.fr.

```
C:\Users\Pack>nslookup www.blagnac.fr
Serveur : mabbox.bytel.fr
Address: fe80::5e03:39ff:fe29:cbb4

Réponse ne faisant pas autorité :
Nom : www.blagnac.fr
Address: 5.44.162.145
```

Figure 1: Résultat de nslookup www.blagnac.fr

Nous pouvons voir l'adresse IP de cette machine est : 5.44.162.145.

Exercice 2 : codage des caractères

Voici un tableau ASCII Hexa :

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	\$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

Figure 2: Tableau ASCII Hexa. Source : https://www.fil.univ-lille1.fr/~wegrzyno/portail/Info/Doc/HTML/seq7_codage_caracteres.html
Voici le séquence Hexa correspondant a www.blagnac.fr :

77 77 77 2E 62 69 61 67 6E 61 63 2E 66 72

Exercice 3 : codage des adresses IPv4

Nous allons transformer l'IP obtenue à l'exercice 1 grâce au site : <https://www.browserling.com/tools/ip-to-hex>

05.2c.a2.91 (0x052ca291)

Figure 3: Adress 5.44.162.145 en hexa

Exercice 4 : capture réseau

29 1.910301	fe80::f12f:ecc3:695...	fe80::5e03:39ff:fe2...	DNS	94 Standard query 0x0002 A www.blagnac.fr
30 1.911011	fe80::5e03:39ff:fe2...	fe80::f12f:ecc3:695...	DNS	110 Standard query response 0x0002 A www.blagnac.fr A 5.44.162.145
31 1.915198	fe80::f12f:ecc3:695...	fe80::5e03:39ff:fe2...	DNS	94 Standard query 0x0003 AAAA www.blagnac.fr
32 1.991988	fe80::5e03:39ff:fe2...	fe80::f12f:ecc3:695...	DNS	160 Standard query response 0x0003 AAAA www.blagnac.fr SOA ns1.prododomaines.com

Figure 4: Résultat de la capture de nslookup www.blagnac.fr par Wireshark

Exercice 5 : couche applicative

1)

0000	5c 03 39 29 cb b4 d0 27 88 86 15 bb 86 dd 60 0d	\.9)....'.....^.
0010	2b 91 00 28 11 40 fe 80 00 00 00 00 00 00 f1 2f	+..(.@..../
0020	ec c3 69 58 ca 6f fe 80 00 00 00 00 00 00 5e 03	..iX.o.....^.
0030	39 ff fe 29 cb b4 fd 05 00 35 00 28 70 d8 00 02	9..)-...-5.(p...
0040	01 00 00 01 00 00 00 00 00 00 03 77 77 77 07 62www.b
0050	6c 61 67 6e 61 63 02 66 72 00 00 01 00 01	lagnac.f r.....

Figure 5: Octets du message n°29 de la capture de l'exercice précédent

Nous pouvons voir que le messages à bien été envoyé en ASCII car nous retrouvons a peu près la même suite qu'a l'exercice 2 (Exception sur les . qui ont été remplacé par des -).

2)

0000	d0 27 88 86 15 bb 5c 03 39 29 cb b4 86 dd 60 00	.'.....\ 9)....^.
0010	00 00 00 38 11 40 fe 80 00 00 00 00 00 00 5e 03	...8.@.....^.
0020	39 ff fe 29 cb b4 fe 80 00 00 00 00 00 00 f1 2f	9..)-...../
0030	ec c3 69 58 ca 6f 00 35 fd 05 00 38 7b d6 00 02	..iX-o-5...8{...
0040	81 80 00 01 00 01 00 00 00 00 03 77 77 77 07 62www.b
0050	6c 61 67 6e 61 63 02 66 72 00 00 01 00 01 c0 0c	lagnac.f r.....
0060	00 01 00 01 00 00 00 8d 00 04 05 2c a2 91,.,.

Figure 6: Octets du message n°30

Nous pouvons voir la séquence de l'exercice 3 à la fin du message réponse.

3) Lorsque nous analysons les différences entre les deux requêtes (n°29 et n°31 sur la capture de l'exo 4), la première chose qui change est le type. En effet, sur la première requête, le type est « A » et pour la seconde c'est « AAAA ». En regardant la page Wikipédia du protocole DNS, nous pouvons voir que le type A permet d'obtenir l'adresse IPV4 du nom de machine et le type AAAA permet d'obtenir l'IPV6.

Exercice 6 : pile protocolaire

```
> Frame 29: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{8C14CAFA-DF2F-4F11-85A3-306A42EFCFC7}, id 0
> Ethernet II, Src: HonHaiPr_86:15:bb (d0:27:88:86:15:bb), Dst: HuaweiTe_29:cb:b4 (5c:03:39:29:cb:b4)
> Internet Protocol Version 6, Src: fe80::f12f:ecc3:6958:ca6f, Dst: fe80::5e03:39ff:fe29:cbb4
> User Datagram Protocol, Src Port: 64773, Dst Port: 53
> Domain Name System (query)
```

Figure 7: Pile réseau de la première requête.

1) Nous pouvons voir que le protocole DNS se base sur le protocole UDP.

2) Le serveur DNS écoute sur le port 53

3) L'adresse IP du serveur DNS est fe80::5e03::39ff::fe29::cbb4.

```

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : Realtek PCIe GbE Family Controller
Adresse physique . . . . . : D0-27-88-86-15-BB
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6. . . . . : fd5c:339:29cb:b400:f12f:ecc3:6958:ca6f(préfér  )
Adresse IPv6 temporaire . . . . . : fd5c:339:29cb:b400:6514:4fa3:1ac1:ebad(pr  f  r  )
Adresse IPv6 de liaison locale. . . . : fe80::f12f:ecc3:6958:ca6f%11(pr  f  r  )
Adresse IPv4. . . . . : 192.168.1.127(pr  f  r  )
Masque de sous-r  seau. . . . . : 255.255.255.0
Bail obtenu. . . . . : jeudi 29 avril 2021 23:58:18
Bail expirant. . . . . : samedi 1 mai 2021 14:59:44
Passerelle par d  faut. . . . . : 192.168.1.1
Serveur DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 181413768
DUID de client DHCPv6. . . . . : 00-01-00-01-25-97-B5-13-D0-27-88-86-15-BB
Serveurs DNS. . . . . : fe80::5e03:39ff:fe29:cbb4%11
                        192.168.1.1
                        fe80::5e03:39ff:fe29:cbb4%11
NetBIOS sur Tcpip. . . . . : Activ  

```

Figure 8: Partie du résultat de `ipconfig /all`

Nous pouvons voir que l'adresse du serveur DNS est la même.

Bilan

Dans ce TP, nous avons vu les bases du protocole DNS. Nous avons vu les informations envoyées dans les deux types de requêtes effectuées par la commande nslookup grâce à Wireshark. Ces informations sont envoyées en ASCII.