## 2023/2024

## Travaux Pratiques N°2 : Mode simulation, Modèle OSI et capture des PDU

**But :** Capture et suivi des PDUs des différents couches du modèle OSI Capture des Requêtes/Réponses HTTP

Topologie : La topologie est composée d'un PC relié directement à un serveur, à l'aide d'un câble croisé.



## Table d'adressage :

Device	Interface	IP Address	Mask	Default Gateway
PC0	Fa0	10.10.10.2	255.255.255.0	
Server0	Fa0	10.10.10.2	255.255.255.0	

1- Configurer les adresses IP de PC0 et Server0 et tester leurs connectivités.

2- Vérifier que le serveur Web est actif (HTTP on), en cliquant sur le serveur

Cliquer sur le serveur  $\rightarrow$  Choisir l'onglet **Services** : HTTP doit être On

Server0											
Physical Config Se	ervices Desktop	Custom Inter	face								
SERVICES		HTTP									
HTTP											
DHCP	НТТР		HTTPS								
DHCPv6	On C	Off	On O	Off							
SYSLOG	DNS File Manager										
AAA	File Name	Edit	Delete								
NTP	1 convrights html	(edit)	(delete)								
EMAIL	r copyrights.nem	(cuit)	(delete)	_							
FTP	2 cscoptlogo177x		(delete)								
	3 helloworld.html	(edit)	(delete)								
	4 image.html	(edit)	(delete)								
	5 index.html	(edit)	(delete)								
			New File	Import							

3- Editer le fichier index.html, en cliquant sur (edit). Le système vous donne la possibilité de le modifier.

4- Pour capturer le trafic réseau il faut basculer vers le mode simulation. Les onglets de bas à droite permettent le basculement entre le Mode *Realtime* et *Simulation*.



5- Dans ce TP on s'intéresse qu'au trafic HTTP. Pour cela nous devons décocher tous le trafic relatifs aux autres protocoles.

- Passer en mode simulation en liquant sur l'onglet Simulation
- La liste des événements visibles (Visible Events) comprend tous les protocoles
- Cliquer sur le bouton **Show All/None** pour désélectionner tous les protocoles
- Cliquer sur le bouton Edit Filters  $\rightarrow$  Choisir l'onglet *Misc* et cocher HTTP
- A ce stade seule le trafic HTTP sera capturé

Simulation Panel					ē×	
Event List						· 🤻
Vis. Time(sec)	Last Device	At Device	Туре І	nfo		
						×
						Q
				Cant	urad tau u	
Reset Simulation	Constant [	)elay		(no ca	aptures)	÷
Play Controls						
Back	Au	uto Capture /	Play	Capture / Fo	rward	<del>4</del> -
Event List Filters ACL Filter, ARP, BC HSRP, HSRPv6, HT NTP, OSPF, OSPFv SSH, STP, SYSLOG	: - Visible Events 3P, CDP, DHCP, I TTP, HTTPS, ICM 6, PAgP, POP3, 5, TACACS, TCP,	DHCPv6, DNS, P, ICMPv6, IP RADIUS, RIP, TFTP, Telnet,	, DTP, EIG Sec, ISAk , RIPng, F UDP, VTF	RP, EIGRPv6, FT MP, LACP, NDP, I RTP, SCCP, SMTP,	TP, H.323, NETFLOW, SNMP,	
Ed	it Filters		S	how All/None		
					(	
						a second second second
				Event List	Simu	liauon

- 6- Cliquer sur PC0  $\rightarrow$  Choisir l'onglet **Web Browser**  $\rightarrow$  Dans URL taper 10.10.10.1
- 7- Cliquer sur *Capture / Forward* pour passer d'une trame à l'autre, jusqu'à l'arrêt des échanges. En principe quatre PDU seront générés.

		*	Simulatior	Panel					₽×
	(		Event Li	st					
			Vis.	Time(sec)	Last Device	At Device	Туре	Info	
10 10 10 2/24	10.10.10.1/24	=		0.002		PC0	HTTP		
10.10.2224		-		0.003		PC0	HTTP		
				0.004	PC0	Server0	HTTP		
PC-PT	Server		9	0.005	Server0	PC0	HTTP		
			Reset Sir	nulation) 📝 htrols Back	Constant Dela	y Capture / Plan	/	Captur	Captured to: * 436,849 s

- 8- Vous pouvez revenir au Web Browser pour voir la page index.html envoyée par le serveur
- 9- Cliquer sur le PDU généré par le PCO : Requête HTTP

## Choisir le **deuxième** PDU $\rightarrow$ Cliquer sur le carré **bleu** Basculer entre **OSI Model** et **Outband** PDU **Details**

- 10- Dans Outband PDU dtails s'affichera les PDUs relatifs à chaque couche du modèle TCP/IP
  - Couche Liaison : Trame Ethernet II
  - Couche Réseau : Paquet IP
  - Couche Transport : Segment TCP
  - Couche Application : Requête HTTP

	Outbour	nd PDU Det	ails							S	t Tiled Back	kground			V	/iewport
PDU Forma	ats									hulatio	n Panel					5
									*	vent	ist					
Etherne	<u>et II</u>									is.	Time(sec)	Last Device	At Device	Туре	Info	
0	4		8		1	4	1	9 Byt 7			0.002		PC0	HTTP		
	PREAMBL 101010 1	.E: 011	DE	ST MAC: 2493-281	32	SRC 0009.7	C83 3596				0.003		PC0	HTTP		
	1010101	.011	0000.	2,2,7,5,2,20	52	0005.7	003.3350		=		0.004	PC0	Server0	HTTP		
TYP 0x8	PE: 300	DATA (	VARIAE	BLE LENG	GTH)		FCS: 0x0		-	9	0.005	Server0	PC0	нттр		
	4	8	1	16 19			3:	l Bits	в							
	4 IHL ID: L: 128	B DSCP: 0x3a PRO: 0 SR	0x0 0x6 C IP: 10	0x2	TL CH	L: 119 0x0 HKSUM	3	l Bits	3	eset S	mulation) 🔽	Constant Dela	у			Captured to 436.849
0 4 TTL	4 IHL ID: L: 128	8 DSCP: 0x3a PRO: 0 SR DS	0x0 0x6 C IP: 10 T IP: 10	0x2 0.10.10.2 0.10.10.1	ті СН 2	L: 119 0x0 HKSUM	3	l Bits	3	eset S	mulation) 📝	Constant Dela	У			Captured to 436.849
	4 IHL ID: L: 128	8 DSCP: 0x3a PRO: C SR DS OPT: 0	0x0 0x6 C IP: 10 T IP: 10 x0	0x2 0.10.10.2 0.10.10.1	TL CH 2 1	.: 119 0x0 HKSUM	3. 0x0	l Bits	3	eset S	mulation 🔽	Constant Dela	y Casturo (Play	. )[	Capture	Captured to 436.849
	4 IHL ID: L: 128	8 DSCP: 0x3a PRO: 0 SR DS OPT: 0 DATA (	0x0 0x6 C IP: 10 T IP: 10 x0	0×2 0.10.10.2 0.10.10.1 BLE LENG	TL CH 2 1 STH)	.: 119 0x0 HKSUM	3: 0x0	l Bits	3	eset S lay Co	mulation) 👽 ntrols Back	Constant Dela	y Capture / Play	/	Capture	Captured to 436.849 : / Forward
	4 IHL ID: L: 128 RC PORT:	8 DSCP: 0 0x3a PRO: 0 SR DS OPT: 0 DATA ( 1037	0x0 0x6 C IP: 10 T IP: 10 x0 (VARIAE	16 19 0x2 0.10.10.2 0.10.10.1 BLE LENG	TL CH 2 1 5TH) 2 5TH ()	_: 119 0x0 HKSUM	0x0 Bits	l Bits	3	eset S lay Co vent1	mulation) 👽 ntrols Back ist Filters - Vie	Constant Dela	y Capture / Play	/	Capture	Captured to 436.849 : / Forward

11- Refaire la même chose avec le **quatrième** PDU, pour voir la Réponse HTTP du serveur.

12- Refaire la même chose avec le troisième paquet.

- Visualiser le Inbound PDU Details
- Visualiser le Outband PDU Details
- Le champ Data de chaque PDU contient le PDU de la couche supérieure, par exemple Data du paquet IP contient le segment TCP

	Tabau								Simulat	on Panel					
DSI Model	Inpour	nd PDU Deta		Outbound P	DU Detai	s			Event	List			-		
- PDU Form	ats							— II	Vis.	Time(sec)	Last Device	At Device	Туре	Info	
										0.002		PC0	HTTP		
Etherne	et II									0.003		PC0	HTTP		
0	4		8		14		19 Byte			0.004	PCO	Server0	HIIP		
	PREAME 101010	BLE: .1011	DI 0006	EST MAC: 5.2A93.2832	2 000	RC MAC: 9.7C83.3596	5			0.005	ServerU	PCU	HIIP		
TYF 0x8	PE: 800	DATA	(VARIA	ABLE LENGT	H)	FCS: 0x0		=							
<u>IP</u> 0	4	8		16 19			31 Bits		Reset	Simulation	Constant Dela	ıy		Cap	otured to 436.849
4	IHL	DSCP:	0x0		TL: 11	9									
	ID:	: 0x3a		0x2	0	×0									
ТТ	L: 128	PRO:	0x6		CHKSU	м	_		Play	Controls					
		SR	C IP: 1	10.10.10.2						Back	Auto	Capture / Pla	y	Capture / F	orward
		DS	ST IP: 1	10.10.10.1											
		OPT: (	0x0			0x0									
		DATA	(VARIA	BLE LENGT	H)					un etter an	the market				
TCP									HTTP	List Hiters - Vi	sidie Events				
ICF										Edit Fil	ters		Shov	v All/None	
0			16		31	l Bits									
	RC PORT	: 1037	'	DEST PORT	: 80										
S				• 1		1									
s		SEQUENC						-					-		Cir
S		SEQUENC				1							E	vent List	<b>3</b> 11
S		SEQUENC	"	11		1	۱.			Seures D	ationtion	Tune	Color	Vent List	Deric