

TP6- TCP-IP-niveau 2



Présentation du TP:

Description du contexte/Mise en situation

professionnelle : Le technicien doit installer le système autoroutier et s'assurer du fonctionnement du système de supervision... se familiariser avec les commandes de test réseau et du logiciel d'analyse de trame "Wireshark" dans l'optique d'assurer la maintenance d'un réseau TCP-IP...

Problématique professionnelle : Il vous sera demandé de paramétrer 2 PCs pour paramétrer et échanger des données entre un client et un serveur TCP-IP. Visualiser les trames TCP-IP avec le logiciel "Wireshark". Utiliser les commandes de base en maintenance de réseau en utilisant l'éditeur de commande "CMD" de Windows Acquérir les connaissances de base sur le fonctionnement en couche (OSI) des réseaux TCP/IP.



Moyens et Ressources

- 2 ordinateurs + (connexion internet pour recherche documentaire)

- 1 boitier convertisseur + câbles associés
- 1 switch Ethernet + câbles associés
- logiciel « autoroute interactive »...

Niveau Taxonomique

🔀 1^{ére}

2

1

2^{de}

 $3 \boxtimes$

4

Tle T

Activités professionnelles :

- R5 Maintenance des réseaux informatiques
- D3 Gestion d'incidents
- R2 Installation et qualification

Compé	étences associés :	Connaissances associées :	Critères d'évaluation :	A NE =
C09	INSTALLER LES ÉLÉMENTS D'UN	 Architecture réseau 	 La configuration est réalisée 	
	SYSTÉME ÉLECTRONIQUE	– Modèles OSI/IP	- La mise en service est	
		- Protocoles usuels IPv4	réalisée	
C04	ANALYSER UNE STRUCTURE MATÈRIELLE ET LOGICIELLE	 Infrastructures matérielles et logicielles centralisées, décentralisées ou réparties 	 Les logiciels d'analyse et de tests sont utilisés selon les procédures de traitement d'incidents 	
		 Documents d'architecture métiers (synoptique, schéma de câblage, etc.) 	 Les indicateurs de fonctionnement sont interprétés 	
C10	EXPLOITER UN RÉSEAU INFORMATIQUE	 Méthodes de connexion à distance sur un équipement Lignes de commandes d'équipements 	 Les différents éléments d'un réseau ou d'un système à partir d'un schéma fourni sont identifiés 	
		 Les bonnes pratiques en sécurité informatique 	 La mise à jour des équipements (iOS, OS, logiciel,) est effectuée 	

NOM:	NOTE :	/20
Société S2IDidac - 84 rue Césaria Evora – 84350 C	OURTHEZON – France	

1 -Dans un premier temps, installez 2 PC (client et serveur TCP/IP) avec le logiciel « Réseau autoroute interactive ».





SZIDIDAC

Propriétés de : Protocole Internet versi	on 4 (TCP/IPv4)
Général	
Les paramètres IP peuvent être déten réseau le permet. Sinon, vous devez d appropriés à votre administrateur rése	ninés automatiquement si votre lemander les paramètres IP au.
Obtenir une adresse IP automation	quement
Utiliser l'adresse IP suivante :	
Adresse IP :	192 . 168 . 1 . 100
Masque de sous-réseau :	255.255.255.0
Passerelle par défaut :	
Obtenir les adresses des serveur	s DNS automatiquement
Utiliser l'adresse de serveur DNS	suivante :
Serveur DNS préféré :	
Serveur DNS auxiliaire :	
🔲 Valider les paramètres en quittar	Avancé
	OK Annuler

Paramétrez manuellement les 2 PC avec des adresses IPv4 en classe C.
 Notez ci-dessous les paramètres choisis.
 Désactivez les cartes réseau autres que celle que vous utilisez !

Pour obtenir le nom d'hôte de la machine, vous pouvez ouvrir un terminal en ligne de commande et taper la commande « hostname ». Sinon vous pouvez attendre de lancer le logiciel et utiliser la Boîte à outils

Machine	@ IPV4	Masque	@réseau Net ID	@hôte Host ID	Nom d'hôte
Serveur					
Client					

A quelles conditions les machines doivent elles répondrent pour communiquer entre elles :

- même @dresse réseau
- □ même @dresse hôte □ @dre
- @dresse réseau différente
 @dresse hôte différente

 $\triangleright 2$ -Installez les équipements et câblez le système,... Mettre sous tension les matériels.



Lancez le logiciel sur les 2 PC, ouvrez une fenêtre « TCP/IP serveur –niveau 2 » sur l'un des PC et une fenêtre « TCP/IP client –niveau 2 » sur l'autre, la station et le panneau d'affichage ne sont pas indispensables dans ce TP...





Paramétrez et testez la communication TCP/IP, à l'ouverture de l'onglet les coordonnées du serveur doivent apparaitre...

1	Saisir le N⁰ de port	Coordonnées de serveur Adresse IP: 192.168.1.100 N de port: Enter n de port Nom: heriaud-PC
2	Attendre une connexion	Ouvrir la connexion
		Saisir le № de port

- Vérifiez l'adresse IP, le nom d'hôte et assurez-vous qu'il s'agit bien de l'adresse que vous avez configurée manuellement. Si ce n'est pas le cas il vous faudra identifier le problème et le résoudre !
- Pour cela vous disposez d'une Boite à outils en bas à droite de votre écran... Chaque bouton exécute une commande réseau de base.
- Pour les plus aguerris, vous pouvez ouvrir une fenêtre d'invite de commandes et taper les commandes manuellement...
- Pour les experts, vous pouvez ouvrir directement le CLI dans la barre des taches...

cmd	×	Arrêter

Si vous devez modifier l'adresse IP des machines, il vous faudra fermer et ouvrir la fenêtre pour prendre en compte la modification.

Renseignez le N° de port par exemple « 4000 » (cette valeur sera changée automatiquement pendant le processus de communication) et ouvrez une connexion avec le client, si vous rencontrez des difficultés : ouvrez le centre réseau et partage et contrôlez l'état du pare-feu !

Précisez pourquoi il est strictement interdit de paramétrer notre application dans la plage de ports 0 à 1023 ?

Autoriser les programmes à communiquer à travers le Pare-feu	Windows
Pour ajouter, modifier ou supprimer des programmes et des ports autorisés, cliquez	sur Modifier les
parametres.	

÷.

Nom	Domestique/entreprise (privé)	Public	1
Réseau Autoroute Interactive		2	L
🗹 Réseau de base	Y	7	
Routage et accès distant			
Serveur de sauvegarde mobile Acronis	₽	1	
Serveur de sauvegarde mobile Acronis		•	
Serveur de statut de sauvegarde mobile Acronis	₽	M	
Serveur de statut de sauvegarde mobile Acronis	V	1	
Service Accès réseau			ſ,
Service Bonjour		¥	1
Service Bonjour		2	
Service d'inscription de nom d'ordinateur Espace de c			
Service de partage réseau du Lecteur Windows Media			

Autoriser un autre programme...

Prompti

Modifiez les paramètres si nécessaire sur le serveur et sur le client...

.....

3-Une fois la connexion établie. Notez ci-dessous les coordonnées du client !

Coordonnées de c	client			
Adresse IP:		N de port:	Nom:	



Lorsque les protocoles de couche du modèle OSI sont encapsulés dans une trame de couche 2. La composition des trames dépend du type d'accès aux supports. Par exemple, si les protocoles de couche supérieure sont TCP et IP et que l'accès aux supports est Ethernet, l'encapsulation des trames de couche 2 est Ethernet II. Dans la première partie de ce TP, vous allez utiliser le logiciel Wireshark pour capturer et analyser les champs d'en-tête de trame Ethernet II. Mais avant, il vous faut vous familiariser avec les principaux protocoles du modèle OSI et le concept d'encapsulation. Vous répondrez aux questions ci-dessous pour assimiler ces concepts en vous aidant des fiches de synthèses (OSI, encapsulation, trame Ethernet, etc...) et de vos recherches sur internet.

- ✤ 4- Le modèle OSI se compose de ____ couches.
- Notez dans le tableau le nom de la couche correspondant au numéro...Placez dans le tableau les protocoles correspondant aux différentes couches :

MP3 - IP - HTTP - Ethernet - TCP/UDP - RS232 - SIP -

Identifiez les matériels ci-contre et les placer au niveau de la couche sur laquelle ils fonctionnent...

N°	Couche OSI	Protocole	Matériel	
7			Ordinateur	
6	Présentation			
5		SIP		
4				
3				and the second sec
2				X
1				

Suivant la couche sur laquelle transitent les données, elles sont souvent nommées différemment (bit, paquet, trame, segment), complétez le tableau ci-dessous !

N°	Couche du modèle OSI	Nom
4	Transport	
3	Réseau	
2	Liaison	
1	1 Physique Bi	

Les étapes validées, vous pouvez lancer le logiciel « Wireshark » dans la fenêtre en bas à droite… (Vous pouvez le lancer sur le client et le serveur).

Lancer capture des trames





Vous devez voir apparaitre un écran semblable à celui-ci, divisé en trois fenêtres :

- 1. Les échanges entre le serveur et le client...
- 2. Le détail des informations d'une trame suivant la couche du modèle OSI (trame physique, Ethernet, paquet et segment... (cliquez sur le triangle pour obtenir le détail).
- 3. La trame complète en hexadécimal. (Ces informations sont surlignées en bleu suivant la sélection de la couche du modèle OSI).

🖸 Con	nexion au réseau lo	cal			
Fichier	Editer Vue A	ller Capture Analyser	Statistiques Telephonie Wire	less Outils A	Aide
	🧕 💿 🔝 🛅	🗙 🖸 । ९. 🗢 🔿 🕾	7 🞍 📃 🗏 🔍 🍳 🍳 🖳	E	
tcp					🗶 📑 👻 Expression.
No.	Time	Source	Destination	Protocol	Length Info
F	3 0.000370	192.168.1.100	192.168.1.101	TCP	66 54145 → 52516 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
	4 0.001441	192.168.1.101	192.168.1.100	ТСР	66 52516 → 54145 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
	5 0.001636	192.168.1.100	192.168.1.101	TCP	54 54145 → 52516 [ACK] Seq=1 Ack=1 Win=65700 Len=0
	6 0.102281	192.168.1.100	192.168.1.101	TCP	106 54145 → 52516 [PSH, ACK] Seq=1 Ack=1 Win=65700 Len=52 🥢
	7 0.119895	192.168.1.101	192.168.1.100	TCP	60 52516 → 54145 [FIN, ACK] Seq=1 Ack=53 Win=525568 Len=0
	8 0.120048	192.168.1.100	192.168.1.101	TCP	54 54145 → 52516 [ACK] Seq=53 Ack=2 Win=65700 Len=0
	9 0.120192	192.168.1.100	192.168.1.101	TCP	54 54145 → 52516 [FIN, ACK] Seq=53 Ack=2 Win=65700 Len=0
L	10 0.121028	192.168.1.101	192.168.1.100	TCP	60 52516 → 54145 [ACK] Seq=2 Ack=54 Win=525568 Len=0
> Fra ≥ Eth ≥ Int	me 3: 66 bytes ernet II, Src: ernet Protocol	on wire (528 bits), AsustekC_19:a8:44 (c Version 4, Src: 192.	66 bytes captured (528 bit 8:60:00:19:a8:44), Dst: He 168.1.100. Dst: 192.168.1.	s) on interfa wlettP_5b:27: 101	ce θ 4e (ac:e2:d3:5b:27:4e)
▷ Tra	nsmission Cont	ol Protocol, Src Por	t: 54145, Dst Port: 52516,	Seq: 0, Len:	0
		·			
0000	ac e2 d3 5b 27	4e c8 60 00 19 a8	44 08 00 45 00 ····['N·`·	· · D · · E ·	
0010	00 34 07 d5 40	00 80 06 6e d5 c0	a8 01 64 c0 a8 ·4··@···r	n····d·· 🧉	
0020	01 65 d3 81 cd	24 cd 6a 8e 67 00	00 00 00 80 02 ∙e···\$·j·	g	
0030	20 00 ce 83 00	00 02 04 05 b4 01	03 03 02 01 01		
0040	04 02				

En vous aidant de la fiche de synthèse « Trame Ethernet » et de l'exemple page suivante, identifiez les différents champs de la trame et complétez le tableau page suivante. Attention, les champs « préambule et CRC sont absents » de la capture !

Γ		1	Nombre d'octets	:		
	8	6	6	2	46 à 1500	4
	Préambule	Adresse Destination	Adresse Source	Ether Type	Données	CRC

Format de la trame Ethernet V2



EXEMPLE :

🙇 Co	nnexion au	réseau local									- • •
Fichie	r Editer	Vue Aller Captu	re Analyser	Statistiques	Telephonie	Wireless	Outils	Aide			
	1		⇔ ⇔ 🕾	₸ 🕹 🔲 (🗐 🔍 Q	् 🎹					
📙 tcp										🗶 🛁 💌 E	xpression +
No.	Time	Source		Destin	ation		Protocol	Length Info			
	3 0.00	0370 192.168	.1.100	192.3	168.1.101		TCP	66 54145 → 52516	[SYN]	Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1	
	4 0.00	1441 192.168	.1.101	192.1	168.1.100		TCP	66 52516 → 54145	[SYN,	ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SA	CK_PERM=1
	5 0.00	1636 192.168	.1.100	192.3	168.1.101		TCP	54 54145 → 52516	[ACK]	Seq=1 Ack=1 Win=65700 Len=0	
	6 0.10	2281 192.168	.1.100	192.3	168.1.101		TCP	106 54145 → 52516	[PSH,	ACK] Seq=1 Ack=1 Win=65700 Len=52	
	7 0.11	9895 192.168	.1.101	192.3	168.1.100		TCP	60 52516 → 54145	[FIN,	ACK] Seq=1 Ack=53 Win=525568 Len=0	
	8 0.12	0048 192.168	.1.100	192.3	168.1.101		TCP	54 54145 → 52516	[ACK]	Seq=53 Ack=2 Win=65700 Len=0	
	9 0.12	0192 192.168	.1.100	192.3	168.1.101		TCP	54 54145 → 52516	[FIN,	ACK] Seq=53 Ack=2 Win=65700 Len=0	
L	10 0.12	1028 192.168	.1.101	192.3	168.1.100		TCP	60 52516 → 54145	[ACK]	Seq=2 Ack=54 Win=525568 Len=0	
▷ Fr ▲ Et	ame 3: 60 hernet II	bytes on wire (, Src: AsustekC	528 bits), 19:a8:44 (c	66 bytes ca	ptured (52 a8:44), Ds	8 bits) o t: Hewlet	n inter tP_5b:2	face 0 7:4e (ac:e2:d3:5b:27:4e))		
Þ	Source:	AsustekC_19:a8:44	1 (c8:60:00):19:a8:44)	:40)						
5 T-	Type: IF	V4 (0x0800)	C 400	100 1 100	D-+- 400 4	CO 4 404					
	cernet Pr	otocol version 4	, SFC: 192.	168.1.100,	UST: 192.1	0516 510					
	ansmissic	on Control Protoco	DI, SPC POR	τ: 54145, D	st Port: 5	2516, Seq	: 0, Lei	1:0			
0000 0010 0020 0030 0040	ac e2 d 00 34 0 01 65 d 20 00 c 04 02	3 5b 27 4e c8 60 7 d5 40 00 80 06 3 81 cd 24 cd 6a e 83 00 00 02 04	00 19 a8 6e d5 c0 8e 67 00 05 b4 01	44 08 00 45 a8 01 64 c0 00 00 00 80 03 03 02 01	00 ···[a8 ·4·· 02 ·e·· 01 ···	'N•` •••D @••• n••• •\$•j ∙g••	E ·				
0	Etherne	t (eth), 14 bytes								Paquets: 909 · Affichés: 8 (0.9%)	Profile: Default

Préambule	@ destination	@ source	Type de trame	données	crc
Exemple	ac:e2:d3:5b:27:4e	c8:60:00:19:a8:44	0800	46 à 1500	
Votre capture 1					
Votre capture 2					

- Dans la fenêtre (1) sélectionnez la première ligne TCP... Dans la fenêtre (2) sélectionnez Ethernet II, et complétez le tableau ci-dessus avec les informations présentes sur votre capture...
- Dans la fenêtre (1) sélectionnez la deuxième ligne TCP... Dans la fenêtre (2) sélectionnez Ethernet II, et complétez le tableau ci-dessus avec les informations présente sur votre capture...
- Quelles adresses utilise « Ethernet » pour communiquer sur un réseau LAN (@destination et @source) ?

	🗆 @ MAC	: [] @IP		@ Postale	
٠	Les adresses IP interv	iennen	t-elles dar	ns le process	sus de communication Eth	ernet sur le réseau LAN ?
		E	NON			
•	Indiquez quel protoco	ole est v	véhiculé d	ans ce type	de trame :	
•	Ouvrir Boîte à outils	puis	Configur	ation des cartes	ou alors ouvrir le CLI	C::>
Qu	elle commande doit-on	n saisir	pour obte	nir les adres	ses IP et MAC ? :	



Identifiez les cartes réseaux de votre serveur et de votre client, relevez les adresses IP et MAC.

	@ MAC	@ IP
Serveur		
Client		

Vous pouvez valider cette étape en comparant la conformité des adresses obtenues avec le CLI et celles obtenues avec Wireshark.



Il semblerait que Wireshark connaisse le constructeur de la carte réseau ?

- # Ethernet II, Src: AsustekC_19:a8:44 (c8:60:00:19:a8:44), Dst: HewlettP_5b:27:4e (ac:e2:d3:5b:27:4e)
 - Destination: HewlettP_5b:27:4e (ac:e2:d3:5b:27:4e)
 Source: AsustekC_19:a8:44 (c8:60:00:19:a8:44)
 - Type: IPv4 (0x0800)
- Identifiez et notez la partie de l'adresse MAC correspondant au constructeur, recherchez sur les sites Coffer ou MAC Vendor Lookup... Complétez le tableau ci-dessous !

	@ MAC constructeur	Constructeur
Serveur		
Client		

- Relancez une capture Wireshark pour vider l'écran (sur le serveur et le client) :
 - Arrêtez la capture...
 - Modifiez éventuellement le filtre (tcp)...
 - Relancez la capture....

Continue without Saving

Envoyez un message du serveur vers le client : Message Jai tout compris t

- Arrêtez la capture...
- Dans la fenêtre (1) sélectionnez la première ligne TCP... Dans la fenêtre (2) sélectionnez « Internet Protocol Version 4 ». En vous aidant de la fiche de synthèse « Paquet IP » et de l'exemple page suivante, identifiez les différents champs du paquet IP et complétez le tableau page suivante.



	Connexion au réseau loc	al			
Fich	nier Editer Vue All	ler Capture Analyser	Statistiques Telephonie Wireless	Outils	Aide
	🔳 🧷 🙆 🛄 🔜 🕅	x 🗈 Q 🚗 🔿 🖘			
	tcp				Expression
No.	Time	Source	Destination	Protocol	Length Info
	1 0.000000	AsustekC_19:a8:44	Broadcast	ARP	42 Who has 192.168.1.101? Tell 192.168.1.100
	2 0.000527	HewlettP_5b:27:4e	AsustekC_19:a8:44	ARP	60 192.168.1.101 is at ac:e2:d3:5b:27:4e
_	3 0.000569	192.168.1.100	192.168.1.101	TCP	66 56501 → 52007 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
	4 0.001639	192.168.1.101	192.168.1.100	TCP	66 52007 → 56501 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
	5 0.001734	192.168.1.100	192.168.1.101	TCP	54 56501 → 52007 [ACK] Seq=1 Ack=1 Win=65700 Len=0
	6 0.102135	192.168.1.100	192.168.1.101	TCP	107 56501 → 52007 [PSH, ACK] Seq=1 Ack=1 Win=65700 Len=53
	7 0.143070	192.168.1.101	192.168.1.100	TCP	60 52007 → 56501 [ACK] Seq=1 Ack=54 Win=65536 Len=0
	8 0.156074	192.168.1.101	192.168.1.100	TCP	60 52007 → 56501 [FIN, ACK] Seq=1 Ack=54 Win=65536 Len=0
	9 0.157139	192.168.1.100	192.168.1.101	TCP	54 56501 → 52007 [ACK] Seq=54 Ack=2 Win=65700 Len=0
	10 0.157243	192.168.1.100	192.168.1.101	TCP	54 56501 → 52007 [FIN, ACK] Seq=54 Ack=2 Win=65700 Len=0
Ľ	11 0.158284	192.168.1.101	192.168.1.100	TCP	60 52007 → 56501 [ACK] Seq=2 Ack=55 Win=65536 Len=0
	Frame 3: 66 bytes o	on wire (528 bits),	66 bytes captured (528 bits) o	n interf	face 0
	Ethernet II, Src: A	AsustekC_19:a8:44 (c	8:60:00:19:a8:44), Dst: Hewlet	tP_5b:27	7:4e (ac:e2:d3:5b:27:4e)
4	Internet Protocol \	/ersion 4, Src: 192.	168.1.100, Dst: 192.168.1.101		
	0100 = Vers	ion: 4			
	0101 = Head	ler Length: 20 bytes	(5)		
	Differentiated S	Services Field: 0x00	(DSCP: CS0, ECN: Not-ECT)		
	Total Length: 52	2			
	Identification:	0x08b1 (2225)			
	Flags: 0x4000, D	Oon't fragment			
	0 0000 0000 0	0000 = Fragment offs	et: 0		
	Time to live: 12	28			
	Protocol: TCP (6	5)			
	Header checksum:	0x6df9 [validation	disabled]		
	[Header checksum	<pre>status: Unverified</pre>]		
	Source: 192.168.	1.100			
	Destination: 192	2.168.1.101			
	Transmission Contro	ol Protocol, Src Por	t: 56501, Dst Port: 52007, Seq	: 0, Len	1: 0
000	00 ac e2 d3 5b 27	4e c8 60 00 19 a8 4	14 08 00 <mark>45 00</mark> ···['N·` ···D	· · E ·	
001	10 00 34 08 b1 40	00 80 06 6d f9 c0 a	a8 01 64 c0 a8 ·4··@··· m···	·d··	
002	20 01 65 dc b5 cb	27 6c e9 0d 3c 00 0	00 00 00 80 02 <u>•</u> e···'1· ·<··		
003	20 00 a8 t9 00	00 02 04 05 b4 01 0	03 03 02 01 01		
004	0 04 02				

Les valeurs inscrites dans les tableaux sont celles de l'écran donné en exemple ci-dessus, les élèves peuvent avoir des valeurs différentes !

0	1	2	3	4	5	6	7	8	9	1 0	1	1 2	1 3	1 4	1 5	1 6	1 7	1 8	1 9	2 0	2 1	2 2	2 3	2 4	2 5	2 6	2 7	2 8	2 9	3 0	3 1
L																															
									0	ptio	ns lf	۹ (év	entu	Jelle	es)											Во	urra	ige			
																Don	nées	S													

Quel est le codage par défaut de la trame ?

 \Box h : hexadécimal \Box d : décimal \Box b : binaire

Convertissez les informations hexadécimales (@IP destination et @ IP source) en décimal !

	hexadécimal	décimal
@ IP source		
@ IP destination		

Quelles adresses (@destination et @source) sont utilisées dans un paquet ?

@ MAC
 @ IP
 @ Postale

Vérifiez les valeurs obtenues dans le tableau avec les @ du serveur et du client !

Evor

Relancez une capture Wireshark pour vider l'écran (sur le serveur et le client) :

• Arrêtez la capture...

SZIDIDAC

- Modifiez éventuellement le filtre (tcp)...
- Relancez la capture.... Continue without Saving

Envoyez un message du serveur vers le client : Message ca y est j'ai tout compris ! Envoyer le message

Arrêtez la capture...

- Dans la fenêtre (1) sélectionnez la première ligne TCP ayant un longueur supérieure à 0 (Len=0)...
- Dans la fenêtre (2) sélectionnez « Transmission Control Protocol », En vous aidant de la fiche de synthèse « Segment TCP » et de l'exemple page suivante, identifiez les différents champs du segment et complétez le tableau suivant.

No.	Time	Source	Destination	Protocol	Length Info
-	1 0.000000	192.168.1.100	192.168.1.101	TCP	66 50903 → 52631 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
	2 0.000879	192.168.1.101	192.168.1.100	TCP	66 52631 → 50903 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
	3 0.001016	192.168.1.100	192.168.1.101	TCP	54 50903 → 52631 [ACK] Seq=1 Ack=1 Win=65700 Len=0
	4 0.101533	192.168.1.100	192.168.1.101	TCP	115 50903 → 52631 [PSH, ACK] Seq=1 Ack=1 Win=65700 Len=61
	5 0.105092	192.168.1.101	192.168.1.100	TCP	60 52631 → 50903 [FIN, ACK] Seq=1 Ack=62 Win=65536 Len=0
	6 0.105209	192.168.1.100	192.168.1.101	TCP	54 50903 → 52631 [ACK] Seq=62 Ack=2 Win=65700 Len=0
	7 0.105328	192.168.1.100	192.168.1.101	TCP	54 50903 → 52631 [FIN, ACK] Seq=62 Ack=2 Win=65700 Len=0
L	8 0.105855	192.168.1.101	192.168.1.100	TCP	60 52631 → 50903 [ACK] Sea=2 Ack=63 Win=65536 Len=0
Fra	me 4: 115 byte	s on wire (920 bits), 1	15 bytes captured (920 b	oits) on inter	face 0
⊳ Eth	ernet II. Src:	AsustekC 19:a8:44 (c8:	60:00:19:a8:44), Dst: He	wlettP 5b:27:	4e (ac:e2:d3:5b:27:4e)
⊳ Int	ernet Protocol	Version 4, Src: 192.16	8.1.100, Dst: 192.168.1	.101 -	
⊿ Tra	nsmission Cont	rol Protocol, Src Port:	50903, Dst Port: 52631	Seq: 1, Ack:	1, Len: 61
	Source Port: 5	0903			
	Destination Po	rt: 52631			
	[Stream index:	01			
	TCP Segment L	en: 61]			
	Sequence numbe	r: 1 (relative seque	nce number)		
	Next sequence	number: 62 (relativ	e sequence number)]		
	Acknowledgment	number: 1 (relative	ack number)		
	0101 = He	ader Length: 20 bytes (5)		
⊳	Flags: 0x018 (PSH. ACK)			
	Window size va	lue: 16425			
	[Calculated wi	ndow size: 65700]			
	[Window size s	caling factor: 4]			
	Checksum: 0xa0	9b [unverified]			
	[Checksum Stat	us: Unverified]			
	Urgent pointer	: 0			
⊳	[SEO/ACK analy	sisl			
⊳	[Timestamps]	,			
	TCP pavload (6	1 bytes)			
Dat	a (61 bytes)	,,			
0000	ac of d2 Eb 7	7 40 58 60 00 10 58 44	08 00 45 00		
0000	ac ez us so z	0 00 80 06 74 9a c0 a8	01 64 c0 28 ce c0	+d	
0020	01 65 c6 d7 c	d 97 ba df 46 df 90 59	3b fe 50 18 ·e····	E · · Y: · P ·	
0030	40 29 a0 9b 0	0 00 00 01 00 00 00 ff	ff ff ff 01 (a) · · · ·		
0040	00 00 00 00 00	0 00 00 06 01 00 00 00	25 6d 65 73	····%mes	
0050	73 61 67 65 3	a 20 63 61 20 79 20 65	73 74 20 6a sage: ca	y est j	
0060	27 61 69 20 7	4 6f 75 74 20 63 6f 6d	70 72 69 73 'ai tout	compris	
0070	20 21 0b		1.		

Les valeurs inscrites dans les tableaux sont celles de l'écran donné en exemple ci-dessus, les élèves peuvent avoir des valeurs différentes !

0	1	2	3	4	5	6	7	8	9	1 0	1 1	1 2	1 3	1 4	1 5	1 6	1 7	1 8	1 9	2 0	2 1	2 2	2 3	2 4	2 5	2 6	2 7	2 8	2 9	3 0	3 1
Op	otior	ıs IP	' (év	enti	uelle	es)																	Во	urra	age						
Do	nné	es																													
						h	: he	exad	écin	nal		(1 : d	écin	nal				b:1	bina	ire										



Convertissez les informations hexadécimales (port destination et port source) en décimal !

					décima	ıl					
Port source											
Port destina	tion										
* *	Vérifiez les va Comment cla	aleurs o assifierie	btenues dar ez-vous les p	ns le tab orts sou	ileau avec le urce et desti	s @ du s nation ?	serveur	et du client !			
	Port source :		🗆 réservé		enregistré	C	∃ dynar	nique ou priv	é		
	Port destinat	ion :	□ réservé		enregistré	Γ	🗆 dynar	nique ou priv	é		
<u>Synthèse :</u>											

▶ 6- Vous noterez dans les cases appropriées sur le schéma, les informations suivantes :

- Le protocole utilisé :
- IP / TCP / Ethernet
- Les informations d'entête :
- @ MAC / N° Port / @IP
- Le format des données :
- Trame / Segment / Paquet





Vous venez de terminer votre TP avec succès, pensez à rétablir les paramètres par défaut du pare-feu et réactiver les cartes réseau des machines.... Bravo !!!