

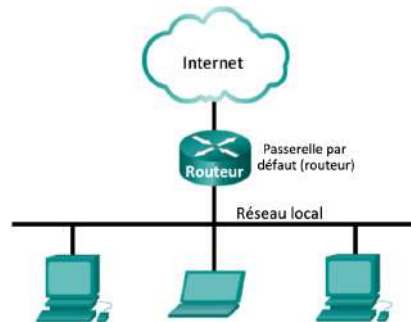
Nom : LAGUERRE
Prénom : Rithler
Université : UNITECH
Concentration : CyberSecurity
Cours : Architecture des Réseaux
Enseignante : Judith Soulamite Nouho Noutat



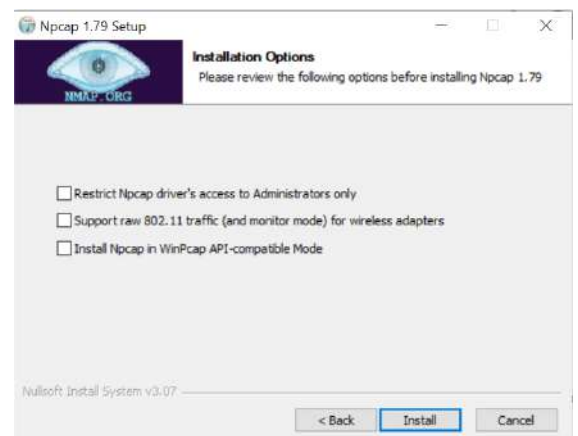
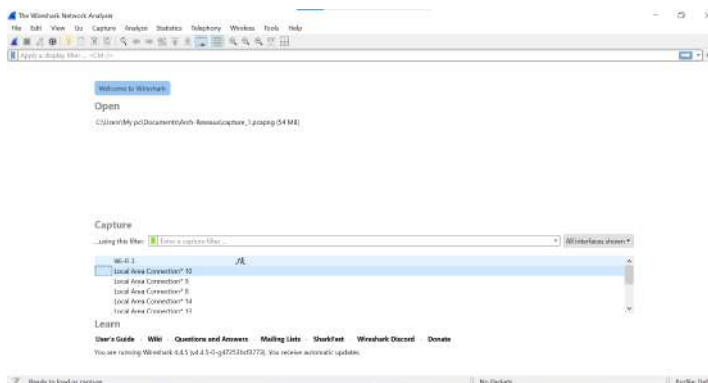
Compte rendu des travaux pratiques 1 et 2 du chapitre 1

Résumé du premier cours

Utilisation de Wireshark pour voir le trafic réseau

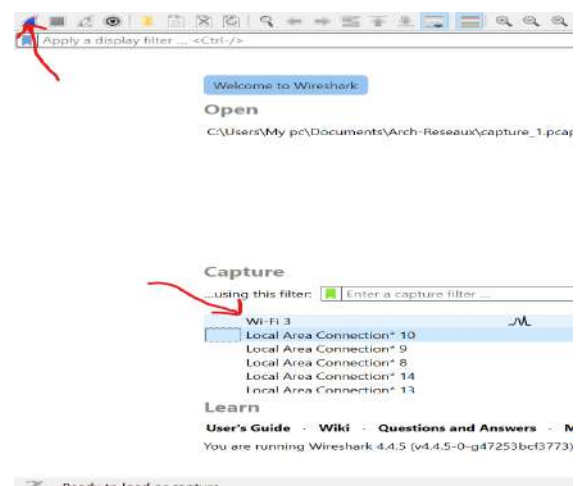


J'ai installé Wireshark sans difficulté sauf que mon interface paraît légèrement différent de celui décrit dans le document. Au cours de l'installation il m'a demandé d'installer Npcap contrairement à celui dans le document WinPcap pour capturer les paquets réseau.



Maintenant pour capturer et analyser les données ICMP locales avec Wireshark, j'ai récupéré mon IP et celui d'un autre utilisateur avec la commande **ipconfig/ all**.

Je Démarre wireshark et clique sur l'interface **Wi-Fi 3** car j'étais connecté non par câble Ethernet mais par le réseau WIFI. Ensuite comme vous voyez la flèche sur l'icône en haut à gauche de l'écran, on clique dessus pour démarrer la capture des données. Et taper icmp dans la zone Filter (Filtre) en haut de Wireshark et appuyez sur Entrée pour afficher uniquement les unités de données de protocole (PDU) (ping) ICMP.



ping IP de l'autre utilisateur que j'ai récupéré

C:\Users\My pc>ping 172.20.10.10

Pinging 172.20.10.10 with 32 bytes of data:
Reply from 172.20.10.10: bytes=32 time=3ms TTL=128
Reply from 172.20.10.10: bytes=32 time=4ms TTL=128
Reply from 172.20.10.10: bytes=32 time=3ms TTL=128
Reply from 172.20.10.10: bytes=32 time=4ms TTL=128

Ping statistics for 172.20.10.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 4ms, Average = 3ms

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF{...}

Ethernet II, Src: Intel_a5:73:91 (20:79:18:a5:73:91), Dst: Intel_50:f3:a2 (a0:d3:7a:50:f3:a2)

Destination: Intel_50:f3:a2 (a0:d3:7a:50:f3:a2)

Source: Intel_a5:73:91 (20:79:18:a5:73:91)

Type: IPv4 (0x0800)

[Stream index: 0]

Internet Protocol Version 4, Src: 172.20.10.5, Dst: 172.20.10.10

Internet Control Message Protocol

Remarque:

- 1- L'adresse MAC de la source correspond à l'interface de mon ordinateur et L'adresse MAC de la destination dans Wireshark correspond à l'adresse MAC du membre de votre équipe.
 - 2- de la destination dans Wireshark correspond à l'adresse MAC du membre de votre équipe.
 - 3- Mon ordinateur obtient l'adresse MAC de l'ordinateur de destination en utilisant le protocole ARP (Address Resolution Protocol)
- maintenant en envoyant une requête ping aux trois URL: a)

www.yahoo.com

IP : 69.147.92.12

MAC : 72:7a:55:04:9f:64

www.cisco.com

IP : 184.26.52.119

MAC : 72:7a:55:04:9f:64

www.google.com

IP : 172.217.15.196

MAC : 72:7a:55:04:9f:64

Frame 479: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF{...}

Ethernet II, Src: Intel_a5:73:91 (20:79:18:a5:73:91), Dst: 72:7a:55:04:9f:64 (72:7a:55:04:9f:64)

Destination: 72:7a:55:04:9f:64 (72:7a:55:04:9f:64)

Source: Intel_a5:73:91 (20:79:18:a5:73:91)

Type: IPv4 (0x0800)

[Stream index: 0]

Internet Protocol Version 4, Src: 172.20.10.5, Dst: 69.147.92.12

Internet Control Message Protocol

b) Pour les requêtes ping distantes L'adresse MAC n'est pas réelle.

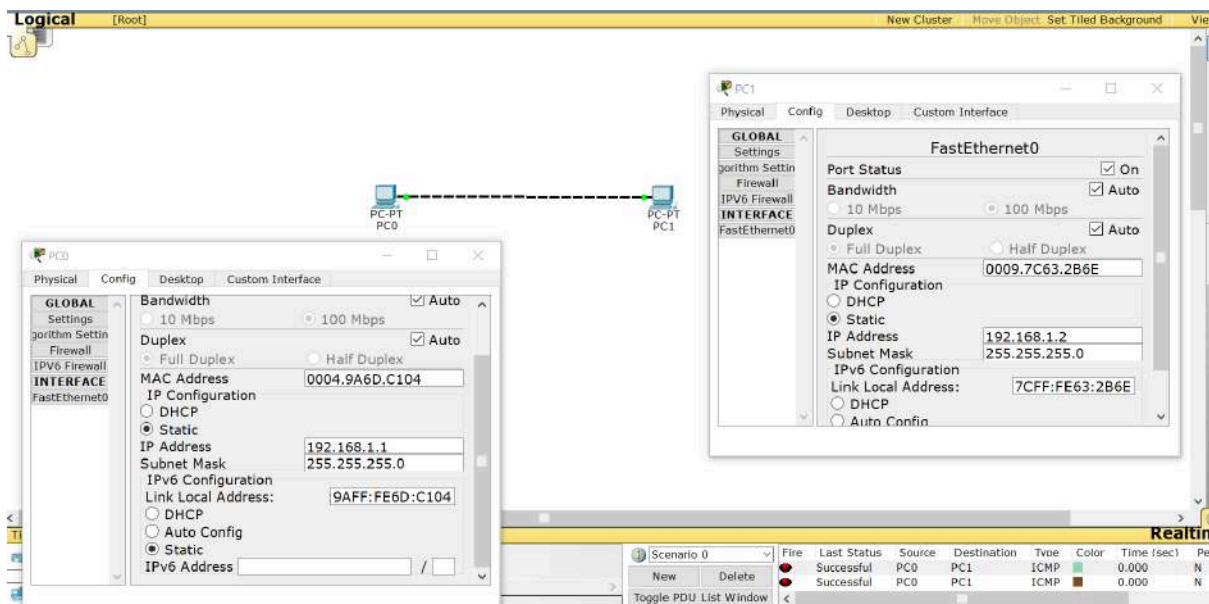
c) sur un réseau local, vous voyez les adresses MAC réelles des machines. Sur un réseau distant, vous ne voyez que l'adresse MAC du routeur.

d) Wireshark ne voit que les paquets qui transitent par l'interface réseau où la capture est effectuée et au-delà du réseau local, seules les adresses MAC des routeurs intermédiaires sont visibles.

Packet Tracer

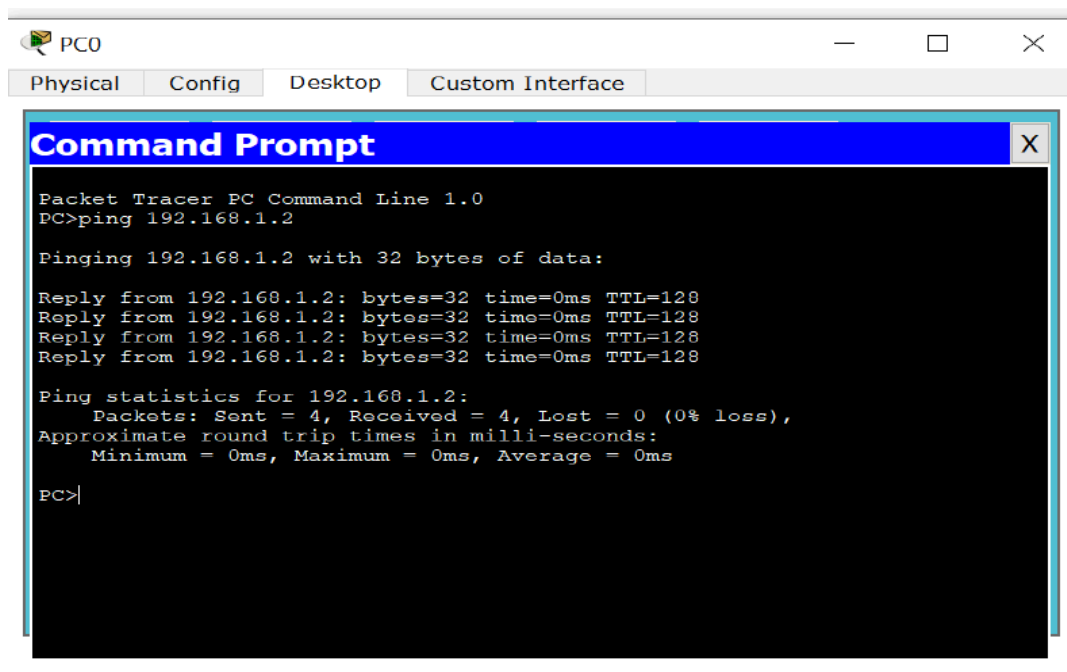
J'ai l'installer sans difficulté. et suivre les instruction dans le document

Dans la zone «IP Configuration», j'ai mis l'adresse 192.168.1.1 et le masque de sous-réseau 255.255.255.0 de même avec l'ordinateur de gauche mais je lui donne l'adresse 192.168.1.2 et le même masque de sous-réseau.

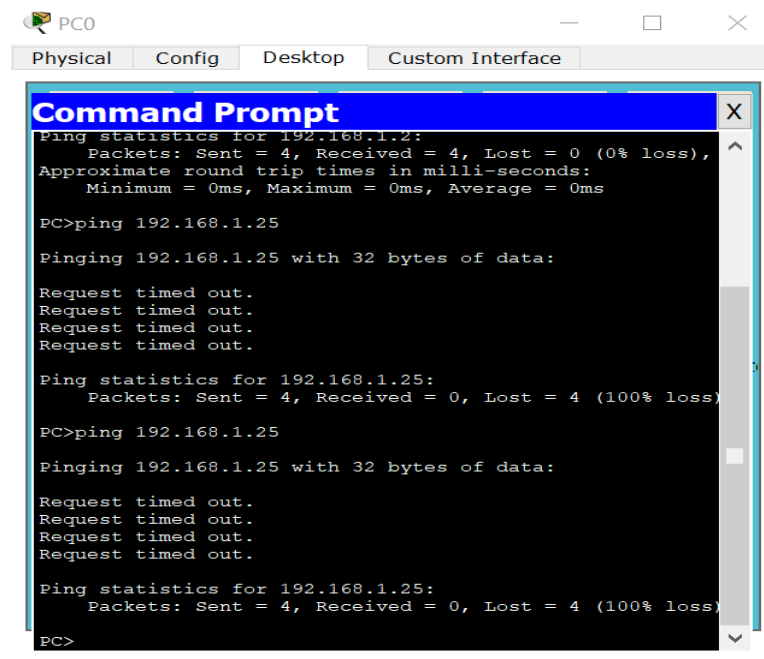


en un seul clic je peux accéder a une fenêtre pour avoir accès à l'onglet Desktop ensuite pour cliquer sur l'invite de commande.

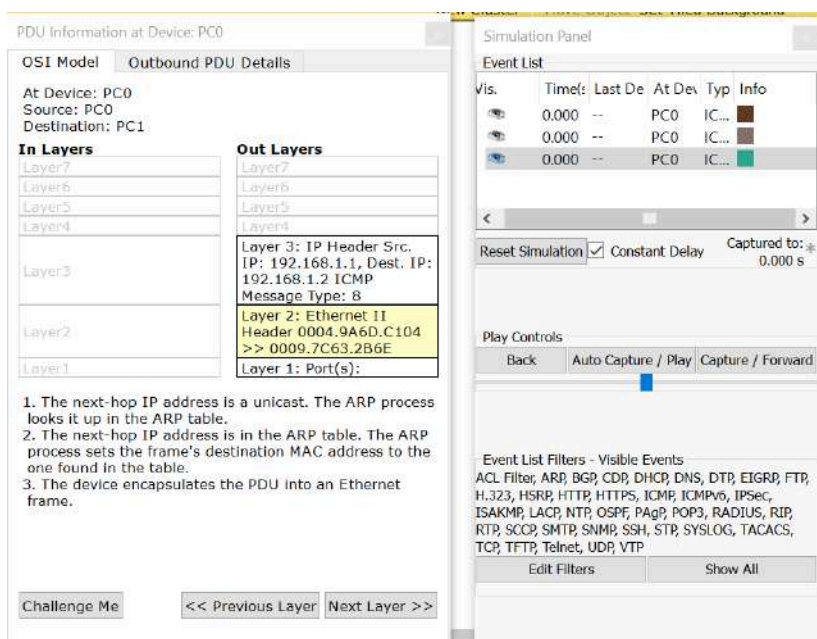
En envoyant la commande «ping» à l'autre ordinateur en indiquant son adresse : ping 192.168.1.2 :



maintenant un «ping» à un ordinateur qui n'est pas sur le réseau : ping 192.168.10.25
Effectivement Aucun ordinateur n'a répondu aux quatre «ping».



pour la partie Simulation et détail sur un paquet, même si je filtre HTTP ça ne marche pas pour envoyer le message alors je laisse avec **show all**.



pour cet interface je vois que c'est par rapport à celui du document TP2.

OSI Model

Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19 bytes
PREAMBLE: 101010...1011		DEST MAC: 0009.7C63.2B6E	SRC MAC: 0004.9A6D.C104	
TYPE: 0x800	DATA (VARIABLE LENGTH)			FCS: 0x0

IP

0	4	8	16	19	31 bits
4	THI	DSCP:	TI: 28		
ID: 0x28		0x0	0x0		
TTL: 255	PRO: 0x1	CHKSUM			
SRC IP: 192.168.1.1					
DST IP: 192.168.1.2					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

ICMP

0	8	16	31 bits
TYPE:	CODE:	CHECKSUM	
ID: 0x20	SEQ NUMBER:		