

Guide d'utilisation de :

Création : 16/06/11

Auteur : David ROUMANET

Guide d'utilisation de l'analyseur réseau Wireshark Mise à jour : 19/05/2014



1. SOMMAIRE

1. SOMMAIRE	2
2. OBJET	4
3. PRÉREQUIS	5
3.1 CONNAISSANCES	5
2.2 Diefédence entre commutateur (switch) et rédéteur (hud)	
3.2 DIFFERENCE ENTRE COMMUTATEUR (SWITCH) ET REFETEUR (HUD)	
3.2.2 Commutateur	
5.2.2 Commutateur	
4. CAPTURES	7
4.1 Édition des préférences	7
4.2 Choisir les paramètres de capture	
4.2.1 Filtres de capture	9
4.2.2 Limitation de la taille des paquets	
4.2.3 Arrêt automatique sur seuil	
4.2.4 Captures circulaires	
4.3 Captures à distance	
4.3.1 Environnement Linux	
4.3.2 Environnement Microsoft	
4.4 CAPTURE SUR PLUSIEURS INTERFACES	
5. ANALYSES	14
5.1 I ECTURE DES TRAMES	14
5.1 1 Fenêtre de résumé	14
5.1.2 Fenêtre d'arborescence de protocole	
5.1.2 Fendire de vue des données	
5.1.5 Tenere de vue des données 5.1 A Réalages utiles	
5.1.4.1 Affichage horaire	
5.1.4.2 Choix des colonnes	15
5.2 ANALYSE RAPIDE	16
5.2.1 Expert Info Composite	16
5.2.2 Filtres d'affichage	17
5.2.2.7 titles d'affichage sur le granheur	19
5 3 ANALYSE NORMALE	20
5.3.1 Informations sur la canture	20
5 3 2 Rénartition des protocoles	20
5 3 3 Répartition des tailles de paquets	20
5.3.4 Conversations	22
5.5.7 Conversations	22
5.5 ANALYSE TEXTED IN FLUX TOP OUT UDP	24
5.6 ANALYSE GRAPHIOUE "TIME-SEQUENCE" (TOPTRACE)	
C DIAGNOSTIC	
6. DIAGNOSTIC	
6.1 Type de protocoles	
6.2 ARP	
6.3 PROTOCOLES TCP OU UDP	
6.3.1 DNS	
6.4 Erreurs générales	
6.4.1 Zero Window	
6.4.2 TCP Window Update	
6.4.3 TCP ZeroWindowViolation	
6.4.4 TCP ZeroWindowProbe	

6.4.5 Windows is full	
6.4.6 Bad Checksum IPv4	
6.4.7 Duplicate ACK	
6.4.8 Fast retransmit	
6.4.9 TCP Retransmission	
6.4.10 TCP Out-of-order	
6.4.11 TCP Previous segment lost	
6.4.12 BER error	
6.5 FLUX PARTICULIERS	
6.5.1 streaming	
6.5.2 Spanning-tree	
1 0	

2. OBJET

Le logiciel Wireshark (anciennement Ethereal) permet la capture et l'analyse de trames sur Ethernet.

Son utilité est indéniable pour contrôler le bon fonctionnement de réseau ou vérifier les trames transitant sur une interface d'un commutateur ou analyser les trafics inutiles ou ceux impactant les performances du réseau.

Voici un petit récapitulatif des capacités de Wireshark :

- Décoder les trames (niveau 2 et 3)
- Calculer le débit moyen sur la durée de la capture (Mbps)
- Tracer un graphe du trafic pour tout ou partie des flux capturés
- Afficher les temps de réponses des trames TCP (basé sur les acquittements)
- Indiquer les erreurs ou les alertes détectées (paquets perdus, retransmis, dupliqués...)
- Suivre un dialogue TCP (notamment HTTP)
- Donner les statistiques sur les tailles des trames réseaux
- Etc.

Pour cela, il suffit de l'installer sur un PC munit d'une interface réseau 100 Mbps ou plus et fonctionnant sous Windows ou Linux. La version décrite ici fonctionne sous Windows XP. Il s'agit de la version 1.6.

Récupérer la dernière version du programme sur le site <u>http://www.wireshark.org/</u>

Suivre les instructions d'installation (en particulier l'installation de WinPCAP s'il n'est pas déjà installé sur le poste).

Une fois l'installation terminée, le **poste** devient une **sonde** réseau prête à fonctionner.

3. PRÉREQUIS

Bien que Wireshark fonctionne sur de nombreux systèmes d'exploitation (Windows, Linux, ...), d'autres éléments sont à prendre en compte pour permettre une capture dans de bonnes conditions.

3.1 Connaissances

La connaissance des protocoles réseaux dans la théorie est un plus indéniable pour utiliser Wireshark.

Sans reprendre la description complète de TCP/IP, le schéma ci-dessous permet de lire l'état d'une connexion TCP (mode connecté du protocole IP).



Ce schéma permet de comprendre pourquoi un analyseur permet de trouver un problème réseau : en effet, les trames réseaux sont envoyés les unes après les autres mais un serveur ou un poste client reçoit également de nombreux autres flux. Les conversations ne sont donc pas continues dans le temps, comme le montre l'exemple ci-après. La machine « D » recevra plusieurs trames en provenance de « A », « B » et « C », que la couche « TCP » se chargera de remettre dans l'ordre.



3.2 Différence entre commutateur (switch) et répéteur (hub)

Le placement de la sonde est important et pourtant, le choix du matériel et du point de collecte reste une des raisons de l'échec d'une analyse.

Désormais, il n'y presque plus que des commutateurs sur les réseaux. Ils sont rapides et semblent ne pas perturber les captures de paquets. Malheureusement, l'avantage principal des commutateurs sur les répéteurs devient un inconvénient pour les analyses réseaux.

3.2.1 RÉPÉTEUR

Le répéteur est un équipement actif qui reçoit un signal sur un port et le renvoie sur ses autres ports.



Les paquets sont émis simultanément sur l'ensemble des ports et si plusieurs machines communiquent en même temps, les règles du protocole CSMA/CD s'appliquent.

3.2.2 COMMUTATEUR

Le commutateur est un équipement actif doté d'une intelligence lui permettant de transmettre les trames directement à destination d'un port, à la condition qu'il retrouve l'adresse Ethernet (aussi appelée adresse MAC) de la machine destinataire sur un de ces ports. Il fonctionne donc au niveau 2 du modèle OSI. Pour les autres trames, il fonctionne comme un simple répéteur (ne pouvant pas déterminer le port de destination) : cela est vrai pour les trames de broadcast notamment.



De ce fait, capturer le flux du port 3 en étant sur le port 5 n'est pas directement possible. Il existe plusieurs méthodes malgré tout :

- ▲ **Port mirroring** : le commutateur réplique toutes les trames valides du port à surveiller sur le port où est connectée la sonde.
- Network TAP : il s'agit d'une solution de duplication des trames. Un TAP passif consiste en une sorte de multiprise physique (4 ports RJ45) qui peut fonctionner en 10/100 Mbps full-duplex. Un TAP actif est un répéteur capable de monter jusqu'à 10 Gbps mais est très couteux.
- ▲ **ARP poisonning** : cette solution logicielle vient « tromper » le commutateur sur l'adresse MAC du destinataire. Cette solution n'est pas très propre en terme d'analyse.
- ARP flooding : cette solution consiste à saturer les tables ARP du commutateur pour l'obliger à broadcaster toutes les communications. Solution peu recommandable.

4. CAPTURES

La première opération est la capture de trames. Cependant il y a plusieurs cas possibles :

- Capture en temps réel de manière manuelle (l'utilisateur démarre et arrête la capture)
- Capture avec limitations automatiques (dans le temps ou sur la taille...)
- Capture sur une période donnée avec rotation (utilisation d'un « buffer » circulaire)
- Capture distante
- Capture sur plusieurs interfaces

D'autre part, il peut être utile de limiter les données capturées à celles qui sont en cause lors de l'analyse :

- Filtrage par protocoles
- Filtrage par adresses
- Limitation de la taille des paquets capturés

4.1 Édition des préférences

L'édition des préférences permet de choisir l'apparence de Wireshark mais aussi de choisir l'interface de capture à utiliser :

The V	Vireshark Network Analyz	zer								
e <u>E</u> di	it ⊻iew <u>G</u> o <u>C</u> apture A	nalyze Statistics	Help							
¥ 🖻	Eind Packet Find Ne⊻t Find Pre⊻ious	Ctrl+F Ctrl+N Ctrl+B	e.j	8 [8	•	۲	T	2	
er:	Mark Packet (toggle) Find Next Mark Find Previous Mark Mark <u>A</u> ll Packets Unmark All Packets	Ctrl+M Shift+Ctrl+N Shift+Ctrl+B				 Expr	ession.	. <u>c</u> lea	ar <u>A</u> pi	ы
8	Set Time Reference (toggle) Find Next Reference Find Previous Reference	Ctrl+T								
Ж	Preferences	Shift+Ctrl+P								

📶 Wireshark: Preferences		
🖃 User Interface	Capture	
Layout	Default interface:	\NPF_{E5E80F62-2D97-41F8-9382-F3D64A6B5AB9}
Columns		Generic dialup adapter: \Device\NPF_GenericDialupAdapt
Font	Interfaces:	Intel(R) PRO/100 VE Network Connection (Microsoft's Pa
Colors	Capture packets in promiscuous mode:	AT&T (Microsoft's Packet Scheduler) : \Device\NPF_{325
Printing	the data list of a solution is used times.	
Name Resolution	opdate list of packets in real time:	
Protocols	Automatic scrolling in live capture:	
	Hide capture info dialog:	
		QK Apply Cancel

Une fois les préférences modifiées, il est possible de procéder à notre première capture.

4.2 Choisir les paramètres de capture

Pour faire une **capture manuelle**, il suffit de cliquer sur l'icône "Start a new live capture" ou dans le menu, choisir [Capture] [Start]... il suffira ensuite d'arrêter la capture en cliquant sur l'icône à sa droite.



Cette option est intéressante pour tester le trafic et déterminer la quantité d'informations passant sur l'interface, cependant il est préférable de faire une capture automatisé.

Attention : la capture de trames sur un commutateur ne permet pas de voir tout le trafic mais seulement celui à destination du port ou se trouve la sonde. En général, le seul trafic visible est constitué de broadcast (Ethernet, TCP/IP, Netbios, IPX...)

Pour analyser le trafic utile en provenance ou à destination d'un équipement particulier, il est nécessaire d'activer une fonction de mirroring ou monitoring. Consulter la documentation du fabricant du commutateur pour plus d'informations. En dernier recours, il peut-être nécessaire d'intercaler un répéteur (hub) entre l'équipement et la sonde.

Commutateur Cisco : en mode config, taper la commande "monitor session 1 source..." puis "monitor session 1 destination ..."

Pour faire une **capture automatisée**, il faut cliquer sur l'icône "Show capture options..." ou dans le menu, choisir [Capture] [Options...] ou encore utiliser le raccourci-clavier [CTRL+K]



		Wire	eshark: Captu	re Options		
Capture						
Capture	Interface	Link-layer hea	der Prom. Mode	Snaplen [B] B	uffer [Mi	iB] Capture Filter ^
Connexion at fe80::306c:e0ce:7 fe80::306c:e0ce:7	u réseau local* 11 79c:691 79c:691	Ethernet	enabled	default	2	
Wi-Fi fe80:8541:1c3:dc 192.168.169.225	3f.fbb4	Ethernet	enabled	default	2	port 53
Connexion ré fe80:3d12:37e9:3 fe80:3d12:37e9:3	éseau Bluetooth Moc:7264 Moc:7264	Ethernet	enabled	default	2	
<						>
Capture on all inter	rfaces node on all interfa	aces				Manage Interfaces
Capture Filter: port	53					V Compile selected BPFs
Capture Files						Display Options
File:				Brow	vse	✓ Update list of packets in real time
Use <u>m</u> ultiple files		✓ Use pcap-ng fo	rmat			☑ <u>A</u> utomatically scroll during live capture
 Next file every 	1	megabyte(s)	V			✓ Hide capture info dialog
Ring buffer with	2	files				Name Resolution
Stop capture after	1	file(s)				Resolve MAC addresses
Stop Capture Automatic	ally After					Resolve <u>n</u> etwork-layer names
	packet(s)					✓ Resolve transport-layer name
	minute(s)	¥				✓ Use <u>e</u> xternal network name resolver
<u>H</u> elp						<u>Start</u> <u>C</u> lose

ut Pint récente le plupert des entiens e -i-- ć--....

Il est primordial que la capture se fasse en mode « promiscuous ». D'autre part, si le poste n'est pas très puissant, il est préférable de désactiver la case « Update list of packets in real time ».

4.2.1 FILTRES DE CAPTURE

Il est possible de ne capturer qu'un certain type de flux. En activant ce filtre, seule les trames réseaux répondant aux critères du filtre seront enregistrées dans Wireshark. Par exemple, le filtre port 53 permet de capturer seulement les paquets reçus et émis à destination du port TCP ou UDP 53 (ici, le protocole DNS). La couleur verte du champ indique que le filtre est valide. Ce filtre est différent du filtre d'affichage (qui est utilisable après la capture).

🗖 Wiresh	ark: Capture Filter	- 🗆 🛛
Edit	Filter	
	Ethernet type 0x0806 (ARP)	
	No Broadcast and no Multicast	
New	No ARP	
<u> ion</u>	IP only	
	IP address 192.168.0.1	
	IPX only	
	TCP only	≡
	UDP only	
	TCP or UDP port 80 (HTTP)	
Delete	HTTP TCP port (80)	
	No ARP and no DNS	
	Non-HTTP and non-SMTP to/from www.wireshark.org	
	Suppression OSPF/HSRP & STP	~
Properties	L	
Filter nam	e: Suppression OSPF/HSRP & STP	
Filter strin	g: not stp and not net 224.0.0.0 mask 255.255.255.240	
Help		⊆ancel

Il existe un certain nombre de filtres pré-définis (à titre d'exemple) mais il est tout à fait possible de créer les siens : la syntaxe autorise d'ailleurs l'utilisation de mots clés AND, OR, NOT...

4.2.2 LIMITATION DE LA TAILLE DES PAQUETS

L'analyse des trames se faisant généralement sur les premiers octets (les entêtes), il est utile de limiter la taille des paquets capturés à une taille maximum : pour cela, il suffit de cocher la case « Limit each packet to » et de choisir un nombre entre **60 octets** (minimum pour conserver l'entête TCP entier) et 512 (informations complémentaires pour des flux HTTP ou TNS par exemple).

Cela n'a aucune influence sur les statistiques concernant les tailles de trames puisque cette information est inscrite dans l'entête des trames Ethernet.

Dans les nouvelles versions (1.8 et supérieure) de Wireshark, il faut double-cliquer sur l'interface et la boite de dialogue suivante apparaît :

	Edit Interface Settings
Capture Interface:	Wi-Fi
IP address:	fe80::8541:1c3:dc3f:fbb4 172.16.11.67
Link-layer he Capture Limit eac Buffer size:	eader type: Ethernet v packets in promiscuous mode th packet to 65535 ÷ bytes mebibyte(s)
<u>C</u> apture Filt	eer:
Help	<u>U</u> K <u>C</u> ancel

4.2.3 ARRÊT AUTOMATIQUE SUR SEUIL

Il est possible de limiter la capture sur 3 critères :

- Nombre de paquets,
- Taille de la capture,
- Délai dans le temps.

Ces trois critères peuvent être combinés. Cet arrêt automatique permet de limiter le travail d'analyse plus tard et de ne pas écraser un événement important.

4.2.4 CAPTURES CIRCULAIRES

C'est le mode le plus intéressant, surtout si la sonde dispose d'un espace disque suffisant. En effet, les problèmes réseaux sont souvent fugitifs et lorsqu'un incident survient, le temps d'activer une capture ne permet pas de trouver l'origine du problème. D'un autre côté, une capture linéaire permet de remonter dans l'historique des trames capturées mais la manipulation d'un fichier unique et souvent de **taille imposante et difficile**. La capture circulaire résout ces problèmes :

Captur	e i iie(3)				
File:	D:\Audits\test			Browse	
🗹 Us	e <u>m</u> ultiple files				
📃 Ne	ext file every	1	Ŷ	megabyte(s)	~
🗹 Ne	ext file every	1	-	hour(s)	~
🗹 Rii	ng buffer with	24	\$	files	
🗌 St	op capture after	1	Ŷ	file(s)	

Dans l'exemple ci-dessus, Wireshark va créer 24 fichiers contenant chacun une heure de capture. Une fois la 24^{ème} heure écoulée, Wireshark va supprimer le premier fichier de la liste et va créer un nouveau fichier.



Avantages :

- Limiter le risque de dépassement de taille de disque,
- Conserver un historique sur 24 heures,
- Permettre la copie des fichiers intermédiaires (sauvegarde ou analyse sur autre poste),
- Localiser facilement un événement dans l'ensemble des fichiers.

Attention : la quantité de données capturées pouvant être très importante, il peut-être préférable de limiter chaque fichier à une taille comprise entre 5Mo et 20Mo afin de faciliter le travail d'analyse. En effet, l'utilisation des outils de Wireshark peut prendre beaucoup de temps sur un poste aux capacités limitées.

L'astuce pour déterminer le bon nombre de fichier pour effectuer la rotation est d'effectuer une première capture manuelle pour chronométrer combien de temps il faut pour remplir la taille choisie.

4.3 Captures à distance

Ce n'est pas uniquement lié à Wireshark mais aussi à WinPCAP dans les environnements Microsoft ou à l'utilisation de TShark via un tunnel SSH dans les environnements Linux.

4.3.1 ENVIRONNEMENT LINUX

La ligne de commande suivante (à adapter en fonction des filtres attendus) :

```
ssh -l root <remote host> tshark -w - not not tcp port 22 | wireshark -k
-i -
```

4.3.2 ENVIRONNEMENT MICROSOFT

Sur la machine distante, il faut créer un compte de service pour l'utilisation de « Remote Packet Capture » puis démarrer le service.

a	Gestion de l'ordinateur				
Fichier Action Affichage ?					
🗢 🏟 🙇 📰 📓 🗟	? 📷 🕨 💷 🔢				
Gestion de l'ordinateur (local)	Nom	Description	État	Type de démarrage	Ouvrir une sessi
Outils système	🤹 Remote Packet Capture Pro	Allows to ca		Manuel	.\David
Planificateur de taches	鵒 Requête du service VSS Mic	Coordonne		Manuel (Déclencher	Système local

Sur la machine locale, il faut déclarer la machine distante pour pouvoir accéder à ses interfaces. Cela se fait dans le menu [Capture] [Options...] (icône ())

Cliquer sur le bouton [Manage Interfaces] et choisir l'onglet « Remote Interfaces » puis cliquer sur le bouton [Add]. Il faut alors saisir les paramètres de la boite de dialogue (notamment choisir le port 2002 et cocher la case radio « Password Authentication »)

(Inter	rface Ma	nagement		- 🗆 🛛
Pipes Local Interfaces Remote Interfaces Host I 192.168.168.200	Inter Remote Interfaces Name rpcap://[192.168.168.200]:2	face Ma Wire Host: Port: Authent © Nul O Pas Usernar	nagement eshark: Remot 2002 Elication I authentication sword authentication ne:		C7BCEEF3D}
<u>A</u> dd [<u>D</u> elete		<u>O</u> K	ancel Apply	y <u>C</u> lose

L'interface distante est désormais visible dans la boite de dialogue habituelle.

4.4 Capture sur plusieurs interfaces

Les dernières versions de Wireshark permettent de capturer simultanément plusieurs interfaces : l'intérêt est de pouvoir tracer les flux en relation avec un service réseau d'une machine quelque soit son origine.

Les serveurs ont généralement plusieurs interfaces (parfois dédiés à la sauvegarde ou au NAS) mais aussi les postes de travail portable (Ethernet et Wi-Fi par exemple).

Pour cela, il suffit de sélectionner les interfaces à utiliser, dans le menu [Capture] [Interfaces...] ou bien en cliquant sur l'icône :

Ensuite il faut cocher les interfaces actives : la colonne de droite montre le nombre de paquets vus par seconde :

4	1	Wireshark: Capture Inte	rfaces		-	×
L	Device	Description	IP	Packets	Packets/s	
L	🔲 🔊 Connexion au réseau local* 11	Microsoft	fe80::306c:e0ce:779c:691	0	0	<u>D</u> etails
L	🗹 👰 Wi-Fi	Microsoft	fe80::8541:1c3:dc3f:fbb4	24	2	<u>D</u> etails
L	🔲 🔊 Connexion réseau Bluetooth	Microsoft	fe80::3d12:37e9:3f0c:7264	0	0	<u>D</u> etails
L	🔲 🔊 VirtualBox Host-Only Network	Sun	fe80::81f9:dad6:bc00:bd40	29	7	<u>D</u> etails
L	🗹 🔊 Ethernet	Realtek PCIe GBE Family Controller	fe80::c9e3:20bc:e850:6338	1	0	<u>D</u> etails
	<u>H</u> elp	<u>S</u> tart	Stop	<u>O</u> ptions	(lose

La lecture nécessite une petite manipulation pour créer une colonne affichant l'interface d'origine :

- 1. Déplier la couche physique dans la fenêtre « Packet Details »
- 2. Sélectionner le premier champ « Interface ID : »
- 3. Clic droit, choisir « Apply as Column »

*2 interfaces [Wireshark 1.10	7 (v1.10.7-0-g6b931a1 from master-1.10)] – 🗖 💌
<u>File Edit View Go</u> Capture <u>A</u> nalyze <u>Statistics</u> Telephony <u>T</u> ools	Internals <u>H</u> elp
◉ ◉ ∡ ≡ ∡ ⊨ ײ x ≈ <, + + • • 77 🕹	🗐 📴 Đ. Q. Q. 🖭 🖉 🕺 🏁 💢
Filter:	✓ Expression Clear Apply Save
IF No Time Protocol Source	Destination SrcPort DstPort Length Info
0 1252 10:33:49.06 MDNS 192.168.169.92	224.0.0.251 5353 5353 120 Standard guery response
0 1253 10:33:49.23 UDP 192.168.169.35	224.15.1.80 21115 10101 111 Source port: 21115 De
0 1254 10:33:49.26 UDP 192.168.169.35	224.15.1.80 21114 10101 111 Source port: 21114 De:
1 1255 10:33:49.85 NBNS 169.254.99.56	169.254.255.255 137 137 110 Registration NB MATRIX
0 1256 10:33:50.64 MDNS 192.168.169.35	224.0.0.251 5353 5353 733 Standard query response
1 1257 10:33:50.60 NBNS 169.254.99.56	169.254.255.255 137 137 110 Registration NB MATRIX
1 1250 10:33:51 35 NBNS 169.254.99.50	224.0.0.251 5555 5555 524 Standard query response 169 254 255 255 137 137 110 Penistration NB <01><01
1 1260 10:33:52.10 NBNS 169.254.99.56	169.254.255.255 137 137 110 Registration NB <01><0
<	
The second state is the second state of the second state is the se	
□ Frame 1258: 524 bytes on wire (4192 bits), 524 bytes ∧ Interface id: 1	0010 01 fe 68 07 00 00 ff 11 63 b5 a9 fe 63 38 e0 00h
Encapsulation type: Ethernet (1)	0020 00 fb 14 e9 14 e9 01 ea 78 35 00 00 84 00 00 00 x5
Arrival Time: May 19, 2014 10:33:50.641790000 Paris	0040 6c 65 20 70 72 6f 66 65 73 73 69 6f 6e 6e 65 6c le profe ss
[Time shift for this packet: 0.000000000 seconds]	0050 05 5f 65 70 69 6d 04 5f 74 63 70 05 6c 6f 63 61epim tc
Epoch Time: 1400488430.641790000 seconds	0070 65 72 76 69 63 65 73 07 5f 64 6e 73 2d 73 64 04 ervicesc
[Time delta from previous captured frame: 0.0352010	0080 5f 75 64 70 c0 31 00 0c 00 01 00 00 11 94 00 02udp.1
[Time delta from previous displayed frame: 0.035201	00a0 19 50 43 20 70 6f 72 74 61 62 6c 65 20 70 72 6f .PC port at
[Time since reference or first frame: 149.151119000	00b0 66 65 73 73 69 6f 6e 6e 65 6c 0c 5f 64 65 76 69 fessionn el
Frame Number: 1258	00d0 94 00 0e 0d 6d 6f 64 65 6c 3d 57 69 6e 64 6f 77mode 1=
Canture Length: 524 bytes (4192 bits)	00e0 73 c0 0c 00 21 80 01 00 00 078 00 0f 00 00 00 s!
[Frame is marked: False]	0100 39 39 03 32 35 34 03 31 36 39 07 69 6e 2d 61 64 99.254.1 6
[Frame is ignored: False]	0110 64 72 04 61 72 70 61 00 00 0c 80 01 00 00 78 dr.arpa
[Protocols in frame: eth:ip:udp:dns]	0120 01 02 01 02 01 03 01 33 01 33 01 35 01 30 01 358.3 .: 0130 01 38 01 45 01 43 01 42 01 30 01 32 01 33 01 45 .8.E.C.B .(
[Coloring Rule Name: TTL low or unexpected]	0140 01 39 01 43 01 30 01 30 01 30 01 30 01 30 01 30 .9.C.0.0.
[Coloring Rule String: (! ip.dst == 224.0.0.0/4 &&	0160 01 30 0
Ethernet II, Src: HewlettP_90:2f:cf (b4:b5:2f:90:2f:c	0170 00 78 00 02 c0 c9 c0 c9 00 01 80 01 00 00 00 78 .x
Internet Protocol Version 4, Src: 169.254.99.56 (169. Usen Datagnam Protocol Snc Pont, mdnc (5353). Det Pour	0190 00 10 fe 80 00 00 00 00 00 00 c9 e3 20 bc e8 50
B oser bacagram Prococor, Sic Port. muns (5555), Ost Po V	01a0 63 38 c0 0c 00 2f 80 01 00 00 11 94 00 09 c0 0c c8/*
💛 🌌 Interface id (frame.interface_id)	Packets: 1273 · D Profile: Default

5. ANALYSES

Une fois les captures effectuées, il est possible de faire le travail d'analyse. C'est la partie la plus complexe mais si les options de captures ont été judicieusement utilisées, ce travail ne sera pas trop long.

5.1 Lecture des trames

L'affichage de Wireshark se décompose en fenêtre qu'il est possible de redimensionner :

5.1.1 FENÊTRE DE RÉSUMÉ

Dans cette fenêtre, Wireshark affiche un résumé des informations : adresses (niveau 3 ou par défaut niveau 2), estampillage horaire, protocole et description succinte. La coloration permet de retrouver rapidement certains protocoles (broadcast, requêtes ARP, etc.) et elle est personnalisable dans le menu [View] [Coloring Rules...].

No.	-	Time	Source	Destination	Protocol	Info	^
	1557	2006-11-29 19:31:55.793332	00:09:6b:b0:da:be	ff:ff:ff:ff:ff	Intel A	Sequence: 3351399424, Sender ID 256, Tear	_
	1558	2006-11-29 19:31:55.835471	00:0b:db:8d:7d:11	ff:ff:ff:ff:ff:ff	ARP	Who has 10.196.22.67? Tell 10.196.23.23	
	1559	2006-11-29 19:31:56.196238	00:80:f4:00:64:07	00:80:f4:00:65:20	LLC	U, func=UI; DSAP 0x24 Individual, SSAP 0>	
	1560	2006-11-29 19:31:56.851720	00000000.000400222ed9	00000000.fffffffffffffffff	IPX SAP	General Response	
	1561	2006-11-29 19:31:56.852212	00000000.000400222ed9	00000000.ffffffffffffffff	IPX SAP	General Response	
	1562	2006-11-29 19:31:56.852648	00000000.000400222ed9	00000000.fffffffffffffffff	IPX SAP	General Response	
	1563	2006-11-29 19:31:56.853059	00000000.000400222ed9	00000000.fffffffffffffff	IPX SAP	General Response	
	1564	2006-11-29 19:31:56.862636	00:09:6b:b0:da:be	ff:ff:ff:ff:ff	Intel A	Sequence: 3368176640, Sender ID 256, Tear	
	1565	2006-11-29 19:31:57.317178	00:80:f4:00:64:05	00:80:f4:00:03:10	LLC	U, func=UI; DSAP 0x24 Individual, SSAP 0>	
	1566	2006-11-29 19:31:57.925888	00:09:6b:b0:da:be	ff:ff:ff:ff:ff	Intel A	Sequence: 3384953856, Sender ID 256, Tear	
	1567	2006-11-29 19:31:57.943504	10.196.22.86	10.196.22.54	TCP	[TCP Retransmission] 2733 > 502 [PSH, ACH	
	1568	2006-11-29 19:31:57.947756	00:80:f4:00:65:17	ff:ff:ff:ff:ff	ARP	Who has 10.196.22.86? Tell 10.196.22.54	
	1569	2006-11-29 19:31:57.947915	00:16:35:75:0e:4e	00:80:f4:00:65:17	ARP	10.196.22.86 is at 00:16:35:75:0e:4e	
	1570	2006-11-29 19:31:57.951050	10.196.22.54	10.196.22.86	TCP	502 > 2733 [RST] Seq=74468 Len=0	
	1571	2006-11-29 19:31:58.145842	10.196.22.86	10.196.22.54	TCP	2735 > 502 [SYN] Seq=0 Len=0 MSS=1460	
	1572	2006-11-29 19:31:58.149970	10.196.22.54	10.196.22.86	TCP	502 > 2735 [SYN, ACK] Seq=0 Ack=1 Win=409	
	1573	2006-11-29 19:31:58.150164	10.196.22.86	10.196.22.54	TCP	2735 > 502 [ACK] Seq=1 Ack=1 Win=17520 Le	
	1574	2006-11-29 19:31:58.150412	10.196.22.86	10.196.22.54	TCP	2735 > 502 [PSH, ACK] Seq=1 Ack=1 Win=175	
	1575	2006-11-29 19:31:58.180560	10.196.22.54	10.196.22.86	TCP	502 > 2735 [PSH, ACK] Seq=1 Ack=29 Win=4(
	1576	2006-11-29 19:31:58.181673	10.196.22.86	10.196.22.54	TCP	2735 > 502 [PSH, ACK] Seq=29 Ack=20 Win=:	-
	1577	2006-11-29 19:31:58.231942	10.196.22.54	10.196.22.86	TCP	502 > 2735 [PSH, ACK] Seq=20 Ack=57 Win=4	*
<				Ш		>	

A partir de cette vue, il est possible de marquer des paquets : menu [Edit] [Mark packet (toggle)] ou séquence clavier [CTRL]+[M]. Cela permet lors d'une sauvegarde ou d'un export de limiter le nombre de trames sauvegardés.

5.1.2 FENÊTRE D'ARBORESCENCE DE PROTOCOLE

Cette fenêtre détaille le paquet sélectionné dans la fenêtre de résumé : la trame est décomposée de manière hiérarchique, du plus bas niveau (frame) jusqu'au niveau du protocole le plus élevé connu par Wireshark.

ame 1 (80 bytes on wire, 80 bytes captured)					
ernet II, Src: 00:16:35:75:0e:4e (00:16:35:75:0e:4e), Dst: 00:80:f4:00:65:17 (00:80:f4:00:65:17)					
Destination: 00:80:f4:00:65:17 (00:80:f4:00:65:17)					
Source: 00:16:35:75:0e:4e (00:16:35:75:0e:4e)					
Гуре: IP (0×0800)					
ernet Protocol, Src: 10.196.22.86 (10.196.22.86), Dst: 10.196.22.54 (10.196.22.54)					
ansmission Control Protocol, Src Port: 2733 (2733), Dst Port: 502 (502), Seq: 0, Ack: 0, Len: 26					
:a (26 bytes)					
iernet Protocol, Src: 10.196.22.86 (10.196.22.86), Dst: 10.196.22.54 (10.196.22.54) unsmission Control Protocol, Src Port: 2733 (2733), Dst Port: 502 (502), Seq: 0, Ack: 0, Len: 26 :a (26 bytes)					

5.1.3 FENÊTRE DE VUE DES DONNÉES

Cette fenêtre affiche les données brutes : chaque champ sélectionné dans la fenêtre d'arborescence de protocole et indiqué en inverse vidéo dans cette fenêtre. L'inverse est possible aussi. De plus, la barre d'état affiche également le type de donnée sélectionnée.

0000 0010 0020 0030	00 : 00 ff ff	1e 30 b2 ff	0b 03 04 b7	72 7e 3b dd	e5 40 04 00	28 00 01 00	00 80 a7 02	1c 06 b8 04	23 e9 0e 04	11 ba 86 ec	ee 0a 00 01	d7 9d 00 01	08 f8 00 04	00 a2 00 02	45 0a 70	00 9d 02		. 0	~.(.@	*	≠ 	E).				 	
	/pe (eth.	type	e), 2	bytes	5					Pac	æts:	9410	6 Disj	playe	d: 94	16 M	arke	d: 0 L	oad tim	ne: I	0:00	.218	Profi	le: De	efault			.:
	alertes (menu [Analyze] [Expert Info Composite]. BLEU = Chats, JAUNE = Warning, ROUGE = Errors																											

5.1.4 RÉGLAGES UTILES

Pour améliorer la lisibilité des trames dans la vue de résumé, voici deux réglages intéressants :

5.1.4.1 Affichage horaire

Dans le menu [View] [Time Display Format], choisir la représentation temporelle la plus pratique :

- Time Of Day (CTRL+ Alt + 2) permet un estampillage horaire permettant de comparer l'heure d'arrivée d'une trame avec un événement lié (appui d'un bouton, trame d'alerte SNMP, etc.)
- Second Since beginning of Capture (CTRL + Alt + 3) permet de mesurer le temps depuis le démarrage de la capture. L'affichage dans la colonne time est moins large, permettant ainsi de se positionner plus facilement dans les trames.
- Second since Previous... affiche le délai entre les trames : cette représentation est utile pour mesurer le délai de réponse à une trame ou lors d'échange de flux (calcul de latence).

Dans ce même menu, il est intéressant de limiter le nombre de décimales affichées (une résolution au centième de seconde sera généralement suffisant) pour limiter la largeur de la colonne « Time ».

5.1.4.2 Choix des colonnes

Dans le menu [Preferences], choisir l'onglet « Columns » ajouter les colonnes « Src Port » et « Dest Port »

4	Wireshark: Preferences - Profile: Default – 🗖	×
 User Interface Layout Columns Font and Colors Capture Filter Expressions Name Resolution Printing Protocols Statistics 	[The first list entry will be displayed as the leftmost column - Drag and drop entries to change column order] Displayed Title Field type Image: Time Time (format as specified) Image: Time (format as specified) Image: Time Time (format as specified) Image: Time Time (format as specified) Image: Time Time (format as specified) Image: Time Time (format as specified) Image: Time Time (format as specified) Image: Time Time (format as specified) Image: Time Time (format as specified) Image: Time Time (format as specified) Image: Time Time (format as specified) Image: Time Time (format as specified) Image: Time Time (format as specified) Image: Time Time (format as specified) Image: Time Time (format as specified) Image: Time (format as specified) Image: Time Time (format as specified) Image: Time (format as specified) Image: Time Time (format as specified) Image: Time (format as specified) Image: Time Time (format as specified) Image: Time (format as specified) Image: Time Time (format as specified) Image: Time (format as specified) Image: Time (format as specified) Image: Time (format as specified) Image: Time (format as specified) Image: Time (format as specified) Image: Time (format as specified) Image: Time (form	
<u>H</u> elp	QK Apply Car	cel

5.2 Analyse rapide

Pour obtenir rapidement des indications concernant les erreurs dans la capture, il faut utiliser le module expert.

5.2.1 EXPERT INFO COMPOSITE

Ce module est accessible via le menu [Analyze] [Expert Info Composite]. Il permet une analyse rapide (bien que ce soit l'analyse la plus complexe).

	186 from Arunk-1.6)] 📃 🗖 🛛 🔤
Ele Edit View Go Capture Analyze Statistics Telephony Tool	ls Internals Help
📑 🛃 🎒 🚳 🗎 📄 🕻 🖾 Display Filters	: 🗏 🗐 🔍 🔍 🥨 🖉 🕅 🛸 🕅
Filter:	Expression Gear Apply
Apply as Column	Dubud bank tak
1747 192 721477 He presses a Silver	APP 60 who has 10 157 248 1
1748 192, 833186 De	ARP 60 Who has 10.157.248.1
1749 192, 904050 Ci 🗹 Enabled Protocols Shif	ft+Ctrl+E ARP 60 who has 10.157.0.5?
1750 192.918315 Or 28 Decode As	ARP 60 who has 10.157.255.1;
1751 193.096390 Di	ARP 60 who has 10.157.255.2:
1752 193.146456 Ci	ARP 60 who has 10.157.0.5?
1753 193.196412 10 Eollow TCP Stream	250 SSDP 175 M-SEARCH * HTTP/1.1
1754 193.296555 On Eolow UDP Stream	ARP 60 who has 10.157.255.2
1755 193. 330389 10 Eolow SSL Stream	78 ICMP 60 Echo (ping) request
1756 193.334198 10 🌻 Expert Info Composite	78 TCP 62 ansott - Im-1 > blackj.
1757 193.334385 10 1758 102 248002 10 Conversation Filter	78 ICP 60 ansort-IM-1 > DIack].
1750 102 249010 10 157 249 162 10 15	7 355 179 TCD 1214 BINU: Cd II_IU: D Frd
1760 193 348790 10 157 248 162 10 15	7.255.178 TCP 1314 ansoft-lm-1 > blackj.
1761 193.348808 10.157.248.162 10.15	7.255.178 TCP 1314 ansoft -]m-1 > blackj.
	2
 ⊨ Frame 1/36: 62 bytes on whre (496 bits), 62 f Ethernet II, Src: Dell_11:ee:d7 (00:1c:23:11: □ Destination: HewlettP_72:e5:28 (00:1e:0b:72: Address: HewlettP_72:e5:28 (00:1e:0b:72:e5) 	ytes captured (496 61ts) :ee:d7), Dst: HewlettP_72:e5:28 (00:1e:0b:72:e5:28) 25:28)
0 = IG bit: I	Individual address (unicast)
0 = LG bit: 0	5lobally unique address (factory default)
Source: Dell_11:ee:d7 (00:1c:23:11:ee:d7)	->
Address: Dell_11:ee:d/ (UU:10:23:11:ee:d/	() Individual address (unicast)
- ic bit: a	llulviuual auuress (unicast) llohally unique address (factory default)
Type: TP (0x0800)	stobality unique audress (ractory derault)
Internet Protocol Version 4. Src: 10.157.248.	.162 (10.157.248.162), Dst: 10.157.255.178 (10.157.255
Transmission Control Protocol, Src Port: anso	oft-lm-1 (1083), Dst Port: blackjack (1025), Seg: 0, L
,	,
2	
<u> </u>	>
0000 00 1e 0b 72 e5 28 00 1c 23 11 ee d7 08 0	0 45 00r.(#E.
UULU UU SU 03 /E 40 00 80 06 E9 ba 0a 9d 18 a 0020 ff h2 04 3h 04 01 a7 h8 0e 86 00 00 00 0	12 Ua 90 .U.~03
0030 ff ff b7 dd 00 00 02 04 04 ec 01 01 04 0	12
Type (eth.type), 2 bytes Packets: 9416 Displa	yed: 9416 Marked: 0 Load time: 0:00,218 Profile: Default

Chaque trame va être analysée et les drapeaux (flags) ainsi que les numéros de séquences seront suivis. Le résultat est trié en 5 catégories :

- **ERRORS** : les problèmes réels comme des pertes de données. L'impact est donc visible.
- **WARNINGS**: les problèmes potentiels comme les trames malformées ou les BER.
- NOTES : les problèmes légers comme les retransmissions suspectées
- CHAT : le suivi des sessions (SYNchronisation, ReSeT, etc.)
- Details : est une vue des 4 catégories précédentes permettant de trier les données par type.

🗖 NET	Tw4x322 Intel(R) PR	tO/Wireless 3945ABG Netv	vork Connect	ion [Wireshar	k 1.6.0 (S∀N Re	v 37592 from	/trunk-1.6)]		- • ×
<u>Eile</u> (<u>E</u> dit ⊻iew <u>G</u> o <u>C</u>	apture <u>A</u> nalyze <u>S</u> tatistic	s Telephony	<u>T</u> ools <u>I</u> ntern	nals <u>H</u> elp				
		🖻 🖬 🗙 🎜 占	🔍 🔶	🔶 🐔 😫		$ \oplus $	0, 🖭 🎬 🔟 畅 🐝 1	B	
Filter:					Expression	Clear Appl	У		
No.	Time	Source	De	estination		Protocol L	ength Info		VI 🔼
	381 24.170789	207.200.96.134	1	92.168.40.49)	нттр	1514 Continuation or nor	1-HTTP traffic	
	382 24.287141	192.168.40.49	2	07.200.96.13	14	тср	54 abr-secure > http [[ACK] Seq=1 Ack=294921 Win=5840	0 Len
	383 24.356178	207.200.96.134	1	92.168.40.49	,	HTTP	1514 Continuation or nor	1-HTTP traffic	
	384 24.357252	207.200.96.134	1	92.168.40.49	,	НТТР	1514 Continuation or nor	1-HTTP traffic	
	385 24.357375	192.168.40.49	2	07.200.96.13	34	TCP	54 abr-secure > http [[ACK] Seq=1 Ack=297841 Win=2920	0 Len
	386 24.357916	207.200.96.134	1	92.168.40.49	,	HTTP	1514 Continuation or nor	1-HTTP traffic	
	387 24.358895	207.200.96.134	1	92.168.40.49	,	HTTP	1514 Continuation or nor	1-HTTP trattic	-l. 70
	388 4.358984	192.168.40.49	2	07.200.96.13	14	ICP HTTP	54 [ICP Zerowindow] at	pr-secure > nttp [ACK] Seq=1 AC	CK=30
	389 0.091/80	192.168.40.49		09.85.229.10	12	TCD	continuation of Nor	Formatine charine (Martonmeu Packet	4 60.5
	291 25 29191	203.85.223.102	1	92.108.40.49	2	TCP	E4 [TCB Keen-Alivel ht	seq-1 ACK-2 WHH-118 CEN-0 SCE-3	T DRE
	392 25.39 050	192 168 40 49	📶 Wireshar	k: 110 Expert Ir	nfos				3 = 20
	393 25.957217	192.168.40.49							Ack
	394 26.023848	209.85.146.104	Errors: 1 (1	1) Warpipge: 4	(31) Notes: 9.(1	(Chate: 3)	(30) Details: 110		
	395 26.024541	289.85.146.104	Enors, r (r	ry warnings. r	(31) 140003. 7 (loy crides, or			
2			No	 Severity 	Group	 Protocol 	 Summary 	•	
				336 Note	Sequence	TCP	Duplicate ACK (#3)		
🗄 Fra	ame 388: 54 byt	es on wire (432 bit		338 Note	Sequence	TCP	Duplicate ACK (#4)		
🗄 Eth	hernet II, Src:	IntelCor_80:04:04		340 Note	Sequence	TCP	Duplicate ACK (#5)		
± Int	ternet Protocol	Version 4, Src. 19		342 Note	Sequence	TCP	Duplicate ACK (#6)		
🗄 Tra	ansmission Cont	rol Protocol, Src 🤇		343 Warn	Sequence	TCP	Fast retransmission (suspected	3)	
				364 Warn	Sequence	TCP	Zero window		
				365 Chat	Sequence	TCP	Window update	I	
				366 Chat	Sequence	TCP	window update		
				300 Viarn	Sequence	CIE impag	Malformed Dasket (Evention of	an word)	
1				391 Note	Sequence	TCP	Keep-üliye	(correa)	
				392 Warp	Sequence	TCP	Zero window		
				·	-				
			Help					Close	
1								7000	
									_
1									
0000	00 17 c5 5e 72	f7 00 1c bf 80 04	04 08 00	45 00	۸r				
0010	00 28 31 8c 40	0 00 80 06 b0 1b c0	a8 28 31	cf c8 ,(1.	.e(1				
0030	00 00 f8 19 00) 00	05 IG CO			•			
1									
📕 📕 File	e: "C:\DOCUME~1\RC	UMANE1\LOCALS~1\Te	Packets: 682	Displayed: 682 M	larked: 0 Dropped	:0		Profile: Default	

En cliquant sur une erreur, le module affiche la trame dans le programme principal.

Attention : les onglets du module d'analyse expert indiquent le nombre de types d'erreurs reconnus. En cliquant sur l'onglet, chaque type d'erreur est affiché de manière condensé : il suffit d'explorer l'arborescence pour pouvoir afficher les trames.

Attention : le module d'analyse est une aide précieuse mais il ne permet pas un diagnostic à 100%. J'ai eu dans certains cas (protocole TNS d'Oracle) des messages « TNS unreassembled packets » qui étaient finalement dus à la multiplicité de requêtes simultanées : Wireshark n'est pas capable de différencier les différencies requêtes

Parfois, Wireshark affiche un résultat erroné ou considère presque toute les trames en erreurs. Le cas le plus classique est celui de l'erreur « Bad Checksum IPv4 ». Dans ce cas, il est utile de vérifier que l'interface Ethernet matériel est correctement configurée et éventuellement, désactiver l'option « Checksum offloading ».

D'autres outils permettent l'analyse des protocoles utilisés et les temps de réponses ou bande passante.

5.2.2 FILTRES D'AFFICHAGE

Wireshark permet de filtrer en temps réel l'affichage des trames. Cela peut-être utile pour n'afficher que les flux en provenance d'une machine, suivre les échanges d'une machine en particulier ou lire les informations d'un protocole en particulier.

Filt	er: ip.a	ddr==10.157.248.	162	Expression.	Clear	Apply	
No.		Time	Source	Destination	Protocol	Length	Info
	3884	312.129378	10.157.248.162	10.157.255.179	NSPI	154	NspiBind requ
	3887	312.320258	10.157.248.162	10.157.255.179	TCP	60	trim > blackj
	4044	320.989137	10.157.248.162	10.157.255.179	NSPI	202	NspiDNToEph r
	4 0 4 5	321.003297	10.157.248.162	10.157.255.179	NSPI	186	NspiGetProps
	4046	321.005631	10.157.248.162	10.157.255.179	NSPI	282	NspiGetProps

L'expression est valide lorsque le champ est coloré en vert. Exemples de filtres classiques :

ip.addr == a.b.c.d	Afficher l'ensemble des flux de/vers l'adresse IP a.b.c.d (ou nom FQDN)
ip.addr == a.b.c.d/r	Il est également possible de fournir une plage IP (notation /24 par exemple)
ip.addr != a.b.c.d	Afficher toutes les trames sauf celles de/vers a.b.c.d
ip.src eq a.b.c.d	Autres variantes : ip.src et ip.dest pour choisir le sens du flux et eq, ne, gt
ip.dst gt a.b.c.d	
tcp.port == nnnn	Afficher les trames correspondantes au protocole TCP n°nnnn

Mots clés :

,	==	Equal
,	!=	Not Equal
,	>	Greater Than
,	<	Less Than
,	>=	Greater than or Equal to
,	<=	Less than or Equal to
	, , , , ,	, == , != , > , < , < , >= , <=

Il y a aussi des filtres rapides :

Pour afficher tous les flux SSL, il est possible de taper directement 'SSL' dans la barre de saisie du filtre.

Filter:	ssl		Expres	sion Clear A	Apply	
No.	Time	Source	Destination	Protocol	Length	Info
	3 3.546412	192.168.40.49	195.47.241.4	SSL	302	Continuation Data
	7 5.521439	192.168.40.49	195.47.241.4	SSL	302	Continuation Data
	9 5.796824	192.168.40.49	195.47.241.4	SSL	206	Continuation Data

ssl	Flux de navigation sécurisé HTTPS ou SSL
dns	Requête de résolution de nom (DNS, port 53 UDP et TCP)
http	Flux de navigation (port 80 TCP)
imap	Flux de messagerie (port 143 TCP)
arp	Requête ARP (protocole de résolution d'adresse, couche 2 du modèle OSI)
stp	Protocole Spanning-Tree (protocole de niveau 2 pour les commutateurs)

Certains protocoles nécessitent un peu plus de connaissance : n'afficher que les trames DHCP sur une capture, implique de savoir que DHCP est une option de BOOTP. Le filtre s'exprime comme suit :

bootp.option.type == 53

5.2.3 FILTRES D'AFFICHAGE SUR LE GRAPHEUR

Les filtres précédemment vus, sont également utilisables dans la fenêtre d'analyse graphique.

Pour y accéder, il suffit de ce rendre dans le menu [Statistics] [IO Graph]. Pour retrouver un débit en bits, il est préférable de modifier l'unité de l'échelle de l'axe Y (Y Axis).

- En cochant le bouton [GraphX] on active la couleur de graphique voulue
- En cliquant sur le bouton [Filter:] d'une ligne, on peut sélectionner un filtre existant
- En choisissant le style « Line », « Dot », « FBar », les événements s'affiche sous forme de lignes continues, de point ou de lignes verticales



Il est ainsi possible de mettre en relation un changement de débit avec un buffer mémoire saturé (gestion de congestion), des problèmes de retransmission ou d'autres messages d'erreurs.

tcp.analysis.zero_window	Trame de gestion de congestion (zero window)
tcp.analysis.duplicate_ack	Trame de gestion de retransmission
expert.message	Trame correspondante à une alerte dans le système expert composite de Wireshark

5.3 Analyse normale

La qualification d'un réseau nécessite de pouvoir déterminer l'utilisation de celui-ci. Cela inclut l'utilisation de la bande passante, les protocoles présents ainsi que leur proportion, les temps de latence, la répartition des tailles de paquets, etc.

5.3.1 INFORMATIONS SUR LA CAPTURE

Wireshark affiche les informations sur le fichier de capture avec notamment le débit moyen lors de la capture. Pour cela, il faut aller dans le menu [Statistics] [Summary].

📶 Wireshark: Sun	mary			- 🗆 🛛
File Name: Length: Format: Packet size limit:	D:\Audits) 2389415 t Wireshark 65535 byt	Merpins_automa bytes /tcpdump/ lit ;es	ates\Merpins_panne_19-315' opcap	9-13.pcap
Time First packet: Last packet: Elapsed:	2006-11-2 2006-11-2 00:10:00	29 19:30:50 29 19:40:51		
Capture Interface: Dropped packets: Capture filter:	unknown unknown unknown			
Display				
Display filter: Marked packets:	none O			
Traffic		Captured	Displayed	
Between first and l	ast packet	600,908 sec		
Packets		18067		
Avg. packets/sec		30,066		
Avg. packet size		116,000 bytes		
Bytes		2100319		
Avg. bytes/sec		3495,242		
Hvg. Mbic/sec		0,020		
		⊆lose		

La durée de capture, ainsi que les dates de début et de fin sont indiquées de manière claire.

5.3.2 RÉPARTITION DES PROTOCOLES

Wireshark est capable de donner la répartition des protocoles sur une capture. Dans ce cas, plus la capture est grande, plus elle sera significative.

Dans le menu [Statistics], sélectionner [Protocol Hierarchy] :



Wireshark analyse alors l'ensemble des trames et fournit une table donnant le pourcentage d'utilisation sur le nombre totale de trame : ainsi le pourcentage de la sous-catégorie « Malformed Packet » sous « Transparent Network Substrate Protocol » se rapporte bien à la totalité des trames de la capture.

Wireshark: Protocol Hierarchy Statistics		-	_	-	-		-	🛛
Display file	r: none							
Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets B	ind Bytes E	ind Mbit/s 🔼
🗏 Frame	100.00 %	9416	100.00 %	948524	0.012	0	0	0.000
Ethernet	100.00 %	9416	100.00 %	948524	0.012	0	0	0.000
Address Resolution Protocol	59.57 %	5609	35,51 %	336806	0.004	5609	336806	0.004
Data	4.33 %	408	5.39 %	51160	0.001	408	51160	0.001
Logical-Link Control	20.03 %	1886	13.28 %	125959	0.002	0	0	0.000
Datagram Delivery Protocol	5.87 %	553	3.50 %	33180	0.000	0	0	0.000
Zone Information Protocol	5.87 %	553	3.50 %	33180	0.000	553	33180	0.000
Cisco Discovery Protocol	0.21 %	20	0.72 %	6855	0.000	20	6855	0.000 📃
Spanning Tree Protocol	13.33 %	1255	8.36 %	79316	0.001	1255	79316	0.001
Dynamic Trunking Protocol	0.24 %	23	0.15 %	1426	0.000	23	1426	0.000
NetBIOS	0.18 %	17	0.32 %	3076	0.000	0	0	0.000
SMB (Server Message Block Protocol)	0.18 %	17	0.32 %	3076	0.000	0	0	0.000
SMB MailSlot Protocol	0.18 %	17	0.32 %	3076	0.000	0	0	0.000
Microsoft Windows Browser Protocol	0.18 %	17	0.32 %	3076	0.000	17	3076	0.000
VLAN Trunking Protocol	0.03 %	3	0.03 %	297	0.000	3	297	0.000
Internetwork Packet eXchange	0.15 %	14	0.17 %	1652	0.000	0	0	0.000
Service Advertisement Protocol	0.15 %	14	0.17 %	1652	0.000	14	1652	0.000
Data	0.01 %	1	0.02 %	157	0.000	1	157	0.000
DEC DNA Routing Protocol	1.43 %	135	0.85 %	8100	0.000	135	8100	0.000
Internet Protocol Version 4	13.22 %	1245	43. <mark>41 %</mark>	411721	0.005	0	0	0.000
🖃 User Datagram Protocol	5.56 %	524	7.11 %	67444	0.001	0	0	0.000
Data	3.30 %	311	2.44 %	23144	0.000	311	23144	n.nnn 💌
Help								⊆lose

Il n'est – hélas – pas possible de copier les informations contenues dans cette fenêtre, ni même, les trier par colonnes.

5.3.3 RÉPARTITION DES TAILLES DE PAQUETS

Wireshark est capable d'afficher la répartition des paquets par taille. Dans le menu [Statistics], choisir [Packet Length...]

Une fenêtre s'affiche permettant de filtrer sur quels éléments la répartition doit être calculée : il n'est pas nécessaire de remplir le champ...

📶 Wireshark: Packet Length Stats Tree 🖃 🗆 🔀
Eilter:
Create Stat Cancel

En cliquant sur le bouton [Create Stat], Wireshark ouvre une fenêtre contenant la répartition demandée par tranche.

Comme pour la répartition hiérarchique de protocoles, il n'est – hélas – pas possible de copier les informations contenues dans cette fenêtre, ni même, les trier par colonnes.

2	🛿 Packet Length				- 🗆 🛛
	Topic / Item	Count	Rate	Percent	
	😑 Packet Length	18067	0,030066		
	0-19	0	0,000000	0,00%	
	20-39	0	0,000000	0,00%	
	40-79	6413	0,010672	35,50%	
	80-159	8173	0,013601	45,24%	
	160-319	3457	0,005753	19,13%	
	320-639	20	0,000033	0,11%	
	640-1279	4	0,000007	0,02%	
	1280-2559	0	0,000000	0,00%	
	2560-5119	0	0,000000	0,00%	
	5120-	0	0,000000	0,00%	
			Class		
			lose		

5.3.4 CONVERSATIONS

Wireshark est capable de montrer les conversations durant la capture, menu [Statistics] [Conversations].

Conversations	: Merpins_panne	-19-3159-1	3.pcap					-0
thernet: 119 E	ibre Channel EDD	T IPv4: 40 1	PX: 4 1X	TA SCTP TCP: 3	Token Ring LID	P: 44 WIAN NCP	RSVP	
				IPv4 Conversat	ions	The start start	110011	
Address A	Address B	Packets *	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	7 ^
10.196.22.54	10.196.22.86	16127	1946278	8183	1327740	7944	618538	
10.196.22.31	10.196.22.86	272	34162	135	15130	137	19032	=
10.196.22.31	10.196.23.255	24	2760	24	2760	0	0	
10.196.22.133	10.196.23.255	19	2407	19	2407	0	0	
10.196.6.33	10.196.22.86	6	1722	3	210	3	1512	
10.196.22.87	10.196.23.255	5	611	5	611	0	0	
10.196.22.86	10.196.23.255	4	519	4	519	0	0	
10.196.22.85	10.196.23.255	4	519	4	519	0	0	
10.196.22.83	10.196.23.255	3	276	3	276	0	0	
10.196.23.27	10.196.23.255	2	486	2	486	0	0	
10.196.22.88	10.196.23.255	2	335	2	335	0	0	
10.196.22.134	10.196.23.255	2	335	2	335	0	0	
10.196.23.15	10.196.23.255	2	496	2	496	0	0	
10.196.22.117	139.160.126.198	1	90	0	0	1	90	~
				⊆ору				
Name resolution	n							
				⊆lose				
					_			

Les onglets permettent de choisir le type d'adressage (Ethernet, IPX, Ipv4) et même par protocoles (TCP ou UDP).

Il est possible de trier les données par colonnes (en cliquant sur le titre de la colonne une fois ou deux fois pour changer l'ordre) et de copier le résultat dans le presse-papier (bouton [Copy]. La troisième et la quatrième colonne (Packets et Bytes) sont respectivement la somme des colonnes 'Packets A->B + Packet B->A' et 'Bytes A->B + Bytes B->A'.

5.4 Analyse graphique de flux

Cet outil permet d'afficher de manière graphique les échanges entre les différentes machines. Pour y accéder, il suffit de choisir dans le menu [Statistics] [Flow Graph...] Un filtre s'affiche pour déterminer les options du graphique puis (après avoir cliqué sur [OK]) la fenêtre des flux s'ouvre.

Time	192.168.40.49 212.27.4 209.85.146.132	0.240 209.85.229.9 10.1.19.26	5 209.85.14 209.85.229.100	Comment
15.057	(1700)	HTTP/1.1 200 OK (t	1900	HTTP: HTTP/1.1 200 OK (text/html)
15.057	(3722)	radius-dynauth > ht	(co)	TCP: radius-dynauth > http [ACK] Se
15.058	(3733)	[TCP Out-Of-Order]	(00)	TCP: [TCP Out-Of-Order] [TCP segm
15.058	(3/22)	[TCP Dup ACK 4493#1	(du)	TCP: [TCP Dup ACK 4493#1] radius-
15.059	[]CP Retransmission		(100)	TCP: [TCP Retransmission] [TCP segr
15.059	[TCP Dup ACK 4463 # 8			TCP: [TCP Dup ACK 4463#8] dcsoftv
15.091	(1700)	[TCP Retransmission		TCP: [TCP Retransmission] [TCP segr
15.091	(1790)	[TCP Dup ACK 4493#2		TCP: [TCP Dup ACK 4493#2] radius-
15.092	(1790)	[TCP Retransmission	(80)	TCP: [TCP Retransmission] [TCP segr
15.092	(1790)	[TCP Dup ACK 4493#3	(00)	TCP: [TCP Dup ACK 4493#3] radius-
15.093	Ignored Unknown Rec			TLSv1: Ignored Unknown Record
15.093	[TCP Dup ACK 4463#9			TCP: [TCP Dup ACK 4463#9] dcsoftv
15.093	Standard query resp	3)		DNS: Standard query response CNAM
15.094	vhd > http [SYN] Sg			TCP: vhd > http [SYN] Seq=0 Win=6
15.096	Standard query resp	3)		DNS: Standard query response CNAM
15.097	(3803)	soniqsync > http [S		. TCP: soniqsync > http [SYN] Seq=0 l
15.101	(3800)	http > pwgpsi [ACK]	(80)	TCP: http > pwgpsi [ACK] Seq=1 Ad
	< III		>	

L'échelle de temps est verticale (ascenseur à droite) tandis que les échanges sont affichés entre les machines de manière horizontale.

L'outil propose également une sauvegarde en mode texte (bouton [Save As])

L'intérêt de cet outil devient clair lorsqu'il est utilisé après un filtre. Il permet ainsi de lire les échanges dans le temps de manière pédagogique comme dans l'exemple ci-dessous pour une requête DNS :

5	capture_	wireshark_type.pcap - Graph Analysis		
	Time	192.168.40.49 212.27.40.240	Comment	^
	33.982	Standard query AAAA	DNS: Standard query AAAA www.gstatic.com	
	34.009	Standard guery resp	DNS: Standard query response CNAME gstatic.l.google.com A	

Les chiffres en grisés et entre parenthèses sur le graphique correspondent aux numéros de ports (UDP ou TCP).

5.5 Analyse texte d'un flux TCP ou UDP

Il existe une option qui permet de reconstituer un flux dans Wireshark. Cette option est particulièrement intéressante pour afficher un flux web au format HTTP par exemple. Il faut d'abord cliquer sur une trame correspondante au flux à analyser. Ensuite, dans le menu [Analyze] choisir [Follow TCP stream].

📶 Intel(R) 82567V-2 Gigabit Network Connection [Wireshark 1.6.0 (SVN Rev 37592 from /trunk-1.6)]
Eile Edit View Go Capture Analyze Statistics Telephony Iools Internals <u>H</u> elp
$\blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \square X \textcircled = [0, + +] \odot \overline{7} \textcircled = [0] \blacksquare \oplus Q \bigcirc \overline{7} \blacksquare \blacksquare \blacksquare \blacksquare H $
Filter: tcp.stream eq 4 Expression Clear Apply
Pinter (tcpartelm eq.4
Eind Save As Print ASCII EBCDIC Hex Dump C C Arrays @ Raw
Help Filter Out This Stream
0000 00 17 c5 5e 72 f2 00 25 11 5e 9a 80 08 00 45 00 ^r % .^E. 0010 03 f6 41 1c 40 00 80 06 00 00 c0 a8 a8 c8 d1 55 ^RU 0020 92 68 c5 85 00 50 73 d9 e9 20 1f f3 7a 65 01 8 .hPsGE T /langu 0030 01 00 d1 17 00 00 47 45 54 20 2f 6c 61 6e 67 75 GE T /langu 0040 61 67 65 5f 74 6f 6f 6c 73 3f 68 6c 3d 66 72 20 age_tool s?hl=fr 0050 48 54 54 50 2f 21 20 2f 0 48 6f 72 74 25 20 artr /l + Nett
File: "C:\Users\parents\AppData\Loca\Tem Packets: 55 Displayed: 26 Marked: 0 Dropped: 0 Profile: Default

Le flux apparaît avec deux couleurs :

- ▲ En rouge : le flux envoyé par le client vers le serveur
- A En bleu : la réponse du serveur à la requête du client

Grâce à cet outil, il est possible de lire quel navigateur web a été utilisé pour effectuer la requête (champ 'user-agent') ainsi que les options négociées.

En général, la réponse du serveur commence par 'HTTP/1.1 200 OK'.

A noter : la même option existe pour les flux UDP. Cliquer sur [Analyze] [Follow UDP stream]. Cela peut-être utilisé sur un flux SSDP ou DNS.

5.6 Analyse graphique "Time-Sequence" (tcptrace)

Cet outil graphique permet de voir rapidement la forme des échanges pour un flux sélectionné :



Ce graphe est une succession de traits noirs et de lignes bleues. Il est possible de zoomer dans ce graphe en cliquant sur le bouton du milieu de la souris. L'axe horizontal représente le temps tandis que l'axe vertical représente le numéro de séquence (en nombre relatif à la première trame).

Cette fonction est issue de l'outil tcptrace, disponible à l'adresse <u>http://www.tcptrace.org/</u> dont le fonctionnement est totalement décrit : l'outil s'avère cependant extrêmement complet et sa lecture reste difficile pour un néophyte.

Il est possible de se déplacer dans le graphique ainsi que d'effectuer des zooms. Pour cela, il faut une souris avec 3 boutons, le bouton de milieu servant pour zoomer (en cliquant sur celui-ci). Le déplacement se fait en tenant le bouton droit de la souris enfoncée tout en déplaçant celle-ci.
En enfonçant la touche [CTRL] et en appuyant sur le bouton droit, une loupe apparaît, permettant de grossir une zone particulière du graphique.
Enfin, les touches de raccourcis suivantes permettent les mêmes actions :
[CTRL] + [-] dézoomer
[CTRL] + [+] zoomer (sur les PC portables sans pavé numérique : [CTRL] + [Shift] + [+])
[Espace]permet de cliquer sur un segment graphique et de le retrouver dans la fenêtre principale des trames Wireshark.

Cette fonction est très complète et permet de suivre la conversation de manière graphique et ainsi de détecter des variations dans le temps ou des modifications de fenêtre.



La flèche **bleue** montre la hauteur du trait vertical noir (en forme de 'l') : il s'agit d'une trame envoyé (du premier au dernier octet, dont la hauteur représente l'écart du nombre de séquences).

La flèche **rouge** montre le temps écoulé entre l'émission des trames et la trame d'acquittement reçue.

La courbe la plus basse qui suit les traits verticaux noirs correspond à la réceptions des trames d'acquittement (ACK) du destinataire. La forme de la courbe ainsi constituée indique le débit : une courbe plutôt verticale montre un débit élevé tandis qu'une tendance horizontale montre un débit faible.

L'autre courbe bleue (au-dessus de la première courbe) correspond au mécanisme de fenêtre TCP (windows) : plus elle est haute, plus la quantité de trames à émettre avant un acquittement est importante.

6. **DIAGNOSTIC**

L'intérêt d'utiliser Wireshark est de faire de l'analyse réseau ou encore de l'audit : cet outil permet de contrôler les trames d'un flux et de les afficher.

Mais sans connaissance des protocoles affichés, les informations données par Wireshark ne sont pas facilement interprétables.

Cette partie est donc une aide au diagnostic, pour faciliter l'utilisation des nombreuses fonctions de Wireshark. Je n'ai pas la prétention de tout connaître et je souhaite rester humble : j'ai ajouté cette partie d'abord pour moi-même...

6.1 Type de protocoles

Depuis plusieurs années, le protocole IP s'est généralisé : il devrait donc être **rare** de rencontrer d'autres protocoles. Le passage par l'outil [Statistics] [Protocol Hierarchy] est donc une étape obligatoire :

Wireshark: Protocol Hierarchy Statistics							- 0	X
Displ	ay filter: no	ne						
Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packet	s End By	tes End
= Frame	100,00 %	34	100,00 %	3749	0,001		D	0
Ethernet	100,00 %	34	100,00 %	3749	0,001		0	0
Internet Protocol Version 6	29,41 %	10	52,3 <mark>9 %</mark>	1964	0,001		0	0
User Datagram Protocol	29,41 %	10	52,3 <mark>9 %</mark>	1964	0,001		0	0
Hypertext Transfer Protocol	23,53 %	8	44,89 %	1664	0,001		8 1	664
DHCPv6	5,88 %	2	8,00 %	300	0,000		2	300
Internet Protocol Version 4	70,59 %	24	47,61 %	1785	0,001		0	0
🗆 User Datagram Protocol	8,82 %	3	10,96 %	411	0,000		0	0
Domain Name Service	5,88 %	2	4,27 %	160	0,000		2	160
NetBIOS Datagram Service	2,94 %	1	6,70 %	251	0,000		0	0
SMB (Server Message Block Protocol)	2,94 %	1	6,70 %	251	0,000		0	0
SMB MailSlot Protocol	2,94 %	1	6,70 %	251	0,000		0	0
Microsoft Windows Browser Protocol	2,94 %	1	6,70 %	251	0,000		1	251
Transmission Control Protocol	61,76 %	21	<mark>36</mark> ,65 %	1374	0,000	1	5	998
Simple Mail Transfer Protocol	8,82 %	3	6,46 %	242	0,000		3	242
Internet Message Access Protocol	2,94 %	1	2,11 %	79	0,000		1	79
Hypertext Transfer Protocol	2,94 %	1	1,47 %	55	0,000	(0	0
Malformed Packet	2,94 %	1	1,47 %	55	0,000		1	55
								Þ
Help								lose

Dans la figure ci-dessus, il n'y a que 2 protocoles majeurs présents : IPv6 et IPv4. 100% des trames capturées sont de type Ethernet :

- ▲ 30% environ de type IPv6
- ▲ 70% environ de type IPv4

Si le réseau audité ne fonctionne pas en IPv6, il y a une partie de la bande passante qui est utilisée de manière inutile.

Il est également possible de contrôler le fonctionnement de ces protocoles avec l'outil [IO Graph] : les filtres sont alors basés sur le champ type de la trame Ethernet.



6.2 ARP

Le protocole ARP permet la résolution de l'adresse Ethernet une adresse IP. Généralement, une machine n'a qu'une seule adresse IP mais il y a des exceptions, notamment, le routeur (parfois nommé « passerelle par défaut »).

Il est donc fréquent lorsque les caches sont vides, de rencontrer deux trames ARP (demande et réponse).

Time	Protocol	Source	Destination	SrcPort	DstPort	Length	Info		
11:02:42.26	ARP	HonHaiPr_a6:de:2d	Acrosser_15:e3:05			42	2 Who has 17	2.16.11.254?	Tell 172.16.11.93
11:02:42.26	ARP	Acrosser_15:e3:05	HonHaiPr_a6:de:2d			5(5 172.16.11.	254 is at 00:	02:b6:15:e3:05

Il faut cependant surveiller que pour une même adresse IP, on ne trouve pas plusieurs adresses Ethernet, ce qui révélerait un problème (sécurité, duplication d'adresse IP, etc). Wireshark est capable de vous montrer le cas d'une adresse dupliquée.

14:33:18.33 ARP Dell_8b:8f:43 Broadcast 60 Gratuitous ARP for 192.168.0.120 (Reply) 14:33:23.58 ARP Dell_8a:78:cb Broadcast 60 Gratuitous ARP for 192.168.0.120 (Reply) (duplicate use of 192.168.0.120 detected!)

Le cas ci-dessus montre des requêtes ARP « gratuites » : ce type de requête est émise au démarrage d'un système afin de vérifier que son adresse IP n'est pas déjà utilisée.

6.3 **Protocoles TCP ou UDP**

L'analyse de protocoles TCP ou UDP implique une bonne connaissance de leur fonctionnement... elle exige aussi une bonne connaissance de l'environnement dans lequel s'effectue l'analyse. Les performances réseaux dépendent également de la configuration des systèmes d'exploitation.

6.3.1 DNS

L'analyse des requêtes DNS permet de vérifier que les machines du réseau s'adressent au bon serveur DNS. En effet, un DNS externe peut répondre moins rapidement ou ne pas répondre sur les adresses locales. Un DNS inexistant ralentira les réponses au début de l'application : en effet, une fois le cache renseigné, la machine n'interroge plus le DNS.

Un problème de performance uniquement au lancement d'une application doit faire suspecter un problème de DNS.

Filter:	dns			Expression	. Clear App	oly					
No.		Time	Source	Destination	Protocol	Length	Info				VLAN
		REF	192.168.40.49	8.5.7.2	DNS	80	Standard	query	PTR 2.7.5.8.1	Mark Dasket (teggle)	
	4	2.001013	192.168.40.49	8.8.8.8	DNS	80	Standard	query	PTR 8.8.8.8.1	Mark Packet (toggle)	
	5	2.094662	8.8.8.8	192.168.40.49	DNS	124	Standard	query	response PTR	Ignore Packet (toggle)	
	6	2.098018	192.168.40.49	8.8.8.8	DNS	92	Standard	query	A www.lci.com	Set Time Reference (toggle)	> [
	7	4.094412	192.168.40.49	8.8.8.8	DNS	71	Standard	query	A www.lci.com	Mapually Recolve Address	
	8	4.594815	8.8.8.8	192.168.40.49	DNS	87	Standard	query	response A 15	Manually Resolve Address	
										Apply as Filter	- • II
										Prepare a Filter	II
										Conversation Filter	II
										Colorize Conversation	
								_		CCTD	

Dans cet exemple, la requête DNS part pour la destination 8.5.7.2... puis 2 secondes plus tard, la même requête est exécutée vers 8.8.8.8 qui répond presque instantanément.

L'utilisation conjointe d'un filtre « DNS » ainsi que le marquage de la référence de temps sur la première requête (bouton droit sur la trame, choisir [Set the reference]) permet de mesurer le délai de réponse du serveur DNS.

6.4 Erreurs générales

Il existe plusieurs catégories d'erreurs et d'avertissements à surveiller. Pour cela, la première action est de lancer l'outil d'analyse [Analyze] [Expert Info Composite]

rrors: 0 (0)	Warnings: 4 (117)	Notes: 31 (333) Chats: 134 (666)	Details: 1	116	
iroup •	Protocol 4	Summary	•	Count	
Sequence	TCP	Previous segment lost (commo	n at captur	re	
Sequence	ТСР	Fast retransmission (suspected)			
Sequence	ТСР	Window is full			2
Sequence	ТСР	Zero window			8
	-				

Les onglets sont classés de gauche (les erreurs les plus graves) à droite.

6.4.1 ZERO WINDOW

Ce type d'erreur signifie qu'une application sur la machine concernée est saturée et refuse de recevoir d'autres trames. Pour cela, elle réduit la fenêtre TCP à zéro.

On peut également voir ce type de problème avec la fonction graphique [Statistics] [TCP stream graph] [Windows Scaling Graph] : en reliant les points verticalement on obtient une droite qui chute rapidement.

TCP Graph 35:	Intel(R) 825	67V-2	2 Gig	abit	Netw	ork Con	necti	on 192.1	.68.168	3.200:	5143	2 ->	207.2	200.96.	134:80	-						• ×
Windowsize [bytes]	1										Wind	dow S	Scalir	ng Gra	aph								
	_ .		•		•					•		•								•		•	
	••			•	·	•	•		·	•			•	•	• •	٠	٠	• .	•		٠	• •	·
60000	• •						•		٠			٠	•			•		• .					•
00000	••	•							•	•		٠		•			•	۰.					
-		·	·						•	•	·	•		٠			٠						
	. •	·	·	•	·	•			•		·	•				·	٠		·	•			
50000		٠	٠	·	•	·	•		•		·		•	•	•••	•	٠	•	·	•	·	• •	
	••	٠	٠	٠	٠	·	•		•		·		•	•	• •		٠	•••	·	٠	·	• •	
-		٠	٠	٠	٠	·	•		•••	•	٠			•	• •			••••	·	٠	·		•
	. •		٠	·	٠		•		•	•	•	•			• •			• •	·	٠	·	. •	•
40000 —					•	•	•		. ·	·		•			• •			• .	•	•	·	·	•
	•				•	·	•		· ·	·		•	•	·	• •	•		۰.			•	• •	•
-						•			•	•		٠	•	•		·	•						•
	•	•	•			٠			•	•	•	٠	·	٠		·	٠	•					
30000 —		·	·	·		·			•	•	·	·	·	٠		·	٠	• •	•	•			
	••	·	·	·	·	·	•		•		·		·	٠			٠	• •		•	•		
-	••	٠	٠	·	·		•		•	٠	٠			•	• •	•	٠	• •		٠	·	• •	
	٠.	٠	٠	٠	٠		•	•	• •	٠	٠				• •	•	٠	• •		٠	·	• •	•
20000 —	•	٠		٠	٠	٠	·	•	· ·	•	٠				• •	٠	•			٠	·	• •	·
				·	٠	·		•	· ·	•	٠				• •	·				٠	·	• •	•
-			·		•	٠	·	•	· ·		٠	٠			• •	٠			•	٠	·	• •	•
10000	••		·			·	·	•	· ·				·	•	· ·				•	•	•	• •	•
10000	••		•			٠	·	•	•				•	•	• •		•		•	•			•
-	••	•	٠					•	•	·				٠			•		٠				
	••	٠	٠	·	Ţ.				•	٠	•			٠	• •		•	•	•				•
	••	•	•	· ·	÷	÷	•		•	•	-1	÷		•		•	•			÷	•	• •	
		10		20		30	40		50	60		70	1	80	90	, ' ·	100	110	12	n '	130	140	150
		2.		_,																-	Ti	me [s]	

Les raisons d'une erreur « Zero Window » sont multiples mais une surcharge de la machine émettrice est à envisager : trop de processus, CPU trop lente, application avec un buffer trop petit... ou parfois, certains programmes de streaming audio (type radio en ligne).

Un autre moyen d'analyser lorsque surviennent ces erreurs sont d'ajouter un filtre dans le module [IO Graph] :

Wireshark IO Graphs: Intel(R) 82567V-2 Gigabit Network Connection		
		200
145.0s 150.0s 155.0s 160.0s 165.0s 170.0s 175.0s		
		111 × 1
Graph1 Color Filter:	Style: Line 🔻	Tick interval: 0.1 sec
Graph 2 Color Filter: expert.message	Style: FBar 💌	Pixels per tick: 2
Graph 3 Color Filter:	Style: Line 💌	Y Axis
Graph 4 Color Filter:	Style: Line 💌	Unit: Packets/Tick 💌
Graph 5 Color Filter:	Style: Line 💌	Scale: Auto 💌
Help Copy		Save Close

Le mécanisme de ZeroWindow est généralement suivi d'un message TCP Window Update.

6.4.2 TCP WINDOW UPDATE

Le destinataire indique ainsi qu'il est de nouveau prêt à recevoir une certaine quantité de données.

230 10.319141 192.168.168.200 94.23.2.73 TCP 54 [TCP ZeroWindow] 50941 > dpserve [ACK] Seq=	231 12.238701 192.168.168.200 94.23.2.73 TCP 5 (TCP Window Update)50941 > dpserve [ACK] 😑 📼 💌						
<pre>[n Frame 230: 54 bytes on wire (432 bits). 54 bytes captured (432 bits) B Ethernet II, Src: Elitegro_5e:9a:80 (00:25:11:5e:9a:80), DSt: Sonitwal_5e:72:f2 Internet Protocol Version 4, Src: 192.168.168.200 (192.168.168.200), DSt: 94.23 Transmission Control Protocol, Src Port: 50941 (50941), DSt Port: dpserve (7020 Source port: 50941 (50941) Destination port: dpserve (7020) Former index:</pre>	In Frame 231: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) B Ethernet II, Src: Elitegro_5e:9a:80 (00:25:11:5e:9a:80), Dst: Sonicwal_5e:72:f Internet Protocol Version 4, Src: 192.166.168.200 (192.166.168.200), Dst: 94.2 Transmission Control Protocol, Src Port: 50941 (50941), Dst Port: dpserve (702 Source port: 50941 (50941) Destination port: dpserve (7020) [Strram index: 0]						
Sequence number: 1 (relative sequence number) Acknowledgement number: 197101 (relative ack number) Header length: 20 bytes B Flags: 0x10 (AcK) Window size value: 0	Sequence number: 1 (relative sequence number) Acknowledgement number: 197101 (relative ack number) Header length: 20 bytes B Flags: 0x10 (Ack) Window size value: 16425						
[Calculated window size: 0] [window size scaling factor: −1 (unknown)] @ Checksum: 0xc9eb [validation disabled]	[calculated window size: 16425] [window size scaling factor: -1 (unknown)] ⊕ Checksum: 0xc9eb [validation disabled]						
۲	< <u> </u>						
0000 00 17 c5 5e 72 f2 00 25 11 5e 9a 80 08 00 45 00 4r%	0000 00 17 c5 sc7 f2 000 00 17 c5 sc7 f2 f2 f3 f3 f4 00 f3 f3 f4 f2 f3 f5 f4 f0 f3 f3 <t< td=""></t<>						

6.4.3 TCP ZEROWINDOWVIOLATION

Cette erreur survient lorsque l'émetteur ignore l'information "Zero Window" du destinataire et continue à envoyer des trames de données.

6.4.4 TCP ZEROWINDOWPROBE

L'émetteur teste si la condition « Zero Window » est toujours active, en envoyant le prochain octet au destinaire. Il recevra soit une trame d'acquittement, soit une nouvelle trame « Zero Window » avec un délai deux fois plus grand.

6.4.5 WINDOWS IS FULL

Ce message est en relation avec l'erreur « Zero Window » mais dans ce cas, c'est l'émetteur qui – connaissant la capacité du buffer de la destination (grâce à l'erreur zero window) – prévient la destination qu'il n'enverra aucune donnée jusqu'à réception d'un acquittement (ACK) car cette trame remplira complètement le tampon mémoire du destinaire.

6.4.6 BAD CHECKSUM IPv4

Wireshark calcule le checksum d'une trame et vérifie si ce calcul correspond à la valeur indiquée à la fin de la trame. En cas de différence, cela signifie que la trame a subit une modification (d'origine inconnue).

234 12.278687 192.168.168.200 94.23.2.73 TCP 54 50941 > dpserve [ACK] Seq=1 Ack=200021 Win=15695 [TCP CHECKS 💷 💷	3								
<pre>b Frame 234: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) Etherne TI, Src: Elitegro_Se9a:80 (00:251:15:e9a:80), DSt: Sonicwal_5e:72:f2 (00:17:65:5 Internet Protocol Version 4, Src: 192.168.168.200 (192.168.168.200), Dst: 94.23.2.73 (94.23) Transmission control Protocol, Src Port: 50941 (50941), Dst Port: dpserve (7020), Seq: 1, A Source port: 50941 (50941) Destination port: dpserve (7020) [Stream index: 0] Sequence number: 1 (relative sequence number) Acknowledgement number: 200021 (relative ack number) Header length: 20 bytes Flags: 0x10 (AcK) window size value: 15695 [Calculated window size: 15695] </pre>									
[Window size scaling factor: -1 (Unknown)] Checksum: OxC9eb [incorrect_should be Ox4dd6 (maybe caused by "TCP checksum offload"?)]									
	-								
0000 00 17 C5 Se 72 F2 00 25 11 Se 9a 80 08 00 45 00 Ar% .AE. 0010 00 28 39 Se 40 00 80 06 F7 a0 C0 a8 a8 C5 Se 17 Ar% .AE. 0020 02 49 C6 Fd 1b 6c 67 53 3F 01 35 ad 9c 72 50 10 Ar% .A6. 0030 3d 4F c9 eb 00 00									

Si cette erreur arrive fréquemment en émission, il y a cependant une explication possible : les cartes réseaux récentes disposent d'une option « *Checksum offloading* » : cette option évite le calcul au niveau du driver réseau de la machine et c'est la carte qui effectue ce calcul. Le driver laisse donc le champ checksum vide (remplit de zéro), ce qui trompe l'analyseur.

Si Wireshark affiche systématiquement ce type d'erreur, il peut être utile de dé-valider cette fonction sur la carte réseau (propriétés carte réseau sous Windows).



Une autre possibilité consiste à dévalider le contrôle de checksum dans wireshark : menu [Edit] [Preferences...] [Protocols], choisir TCP ou UDP et décocher "Validate XXX checksum..."

Vireshark: Preferences - Profile: Default	0x00-1+++71-002-1	990.00	
T.38	Protocol Show TCP summary in protocol trees		
TACACS+	show fer summing in protocol ace.		
TALI	Validate the TCP checksum if possible:		
тсар	Allow subdissector to reassemble TCP streams:		
ТСР	Analyze TCP sequence numbers:		
TCPENCAP	,		
TDS	Relative sequence numbers:		
Teredo	Track number of bytes in flight:		
tetra			
TFTP	Calculate conversation timestamps:		
TIPC	Try heuristic sub-dissectors first:		
TNS			
Token-Ring			
ТРКТ			
TPNCP			
TTE			
UCP			
UDP			
UDPlite			
ULP			
UMA			
Help		OK Apply	Cancel

6.4.7 DUPLICATE ACK

Dans le cas où les trames arrivent dans le désordre, la destination prévient l'émetteur de ce fait en émettant une trame « Duplicate ACK ».

No.	Time	Source	Destination	Protocol	Length Info	VI 🔼
	90 7.517669	10.202.103.72	10.17.7.76	TCP	1514 [TCP segment of a reassembled PDU]	
	91 .517763	10.17.7.76	10.202.103.72	TCP	54 empire-empuma > blackjack [ACK] Seq=2191 Ack=3275 Wir	n
	92 7.518210	10.202.103.72	10.17.7.76	TCP	1506 [TCP Previous segment lost] [TCP segment of a reasser	n
	93 7.518291	10.17.7.76	10.202.103.72	TCP	66(TCP Dup ACK 91#1) empire-empuma > blackjack [ACK] Se	e
	94 8.000711	Alcatelfb:1c:72	Spanning-tree-(for-brid	dg∈STP	60 Conf. Root = 61440/4095/ff:ff:ff:ff:ff:ff	
	95 9.000685	Alcatelfb:1c:72	Spanning-tree-(for-brid	dg∈STP	60 Conf. Root = 61440/4095/ff:ff:ff:ff:ff:ff Cost = 0	
	96 9.082038	Cisco_22:78:9a	PVST+	STP	64 Conf. Root = 49152/10/00:12:d9:22:78:80 Cost = 0 P(0
	97 9.092024	10.202.103.72	10.17.7.76	TCP	1514 [TCP Retransmission] blackjack > empire-empuma [ACK]	
	98 9.092142	10.17.7.76	10.202.103.72	TCP	60[TCP Dup ACK 91#2] empire-empuma > blackjack [ACK] S0	
	99 9.142206	10.202.103.72	10.17.7.76	DCERPC	1514 [TCP Retransmission] Response: call_id: 2 Fragment: :	
	100 9.142326	10.17.7.76	10.202.103.72	TCP	54 empire-empuma > blackjack [ACK] Seq=2191 Ack=6187 Wi	n
	101 9.142717	10.202.103.72	10.17.7.76	TCP	1514 [TCP Retransmission] [TCP segment of a reassembled PD	0
	102 9.192793	10.202.103.72	10.17.7.76	TCP	1514 blackjack > empire-empuma [ACK] Seq=6195 Ack=2191 Wi	л

Cependant, le protocole TCP ne peut déterminer s'il s'agit d'une perte de trame ou d'un problème d'ordonnancement. Un délai est donc appliqué pour permettre la réception d'un autre message « Duplicate ACK » qui permettra de vérifier s'il s'agit uniquement de 2 trames mal ordonnées ou bien si le désordre et les pertes sont plus graves.

Wireshark indique donc par un comptage s'il s'agit du premier message ou plus : « TCP Dup ACK *trame#compteur* »

6.4.8 FAST RETRANSMIT

Dans le cas ou l'émetteur reçoit des trames dont le numéro de séquence est supérieur au numéro de la trame d'acquittement, il peut retransmettre les trames manquantes avant la fin du timer d'acquittement.

Dans ce cas, les trames sont appelés "Fast Retransmission"

Dans tous les cas, les trames doivent être réémises dans un intervalle maximum de 3 fois "Duplicate ACK".

6.4.9 TCP RETRANSMISSION

Ce message intervient lorsque l'émetteur retransmet une trame après l'expiration du délai d'acquittement.

6.4.10 TCP OUT-OF-ORDER

Ce message survient lorsque une trame contient un numéro de séquence inférieur à la trame précédente reçue. Ce message n'est pas trop grave s'il survient de temps en temps : le protocole TCP ayant la capacité à réordonner les trames. Il s'agit donc seulement d'une information.

6.4.11 TCP PREVIOUS SEGMENT LOST

A l'inverse du message « TCP out-of-order », ce message survient lorsque une trame contient un numéro de séquence supérieur à la trame attendue (numéro de séquence prévu). Ce message est un bon indicateur des trames perdues et est souvent accompagné de l'évènement « TCP retransmission ».

6.4.12 BER ERROR

BER signifie **B**it **E**rror **R**ate. Une erreur BER correspond à un taux de bit en erreur sur un nombre bit total. Cette erreur étant très proche de la partie matérielle, sous Wireshark elle est souvent liée à une mauvaise analyse d'un protocole...

TCP_ACKed_lost_segment -

TCP Keep-Alive - Occurs when the sequence number is equal to the last byte of data in the previous packet. Used to elicit an ACK from the receiver.

TCP Keep-Alive ACK - Self-explanatory. ACK packet sent in response to a "keep-alive" packet.

TCP DupACK - Occurs when the same ACK number is seen AND it is lower than the last byte of data sent by the sender. If the receiver detects a gap in the sequence numbers, it will generate a duplicate ACK for each subsequent packet it receives on that connection, until the missing packet is successfully received (retransmitted). A clear indication of dropped/missing packets.

6.5 Flux particuliers

6.5.1 STREAMING

Il se caractérise par un accès régulier et (normalement) constant. L'outil « Time-sequence (tcptrace) est idéal pour établir le diagnostic :



Dans ce graphe, il est possible de zoomer pour trouver les erreurs de retransmissions et vérifier l'ordre des séquences :



Ici, il est visible que la première trame a été ré-émise puisque son numéro de séquence est plus petit tandis que dans le temps, elle est plus à droite que les autres.

Un autre graphe permet de constater qu'il n'y a pas eu de congestion : [Statistics] [TCP Stream Graph] [Windows Scaling Graph] :



Le mécanisme de fenêtrage TCP a conservé une valeur constante de 8192 octets tout au long de la diffusion du flux.

Les images ci-après montrent un fonctionnement moins régulier du flux mais sans erreurs :



Enfin, un graphe contenant de nombreuses retransmissions :



Dans ce dernier cas, il est possible de vérifier les variations de débits : outil [Statistics] [IO Graph]



6.5.2 SPANNING-TREE

Les flux spanning-tree de type DSAP sont très constants : une trame est émise toute les secondes. Il est facile de le vérifier dans l'outil graphique « IO Graphs », en plaçant un filtre de type 'llc.dsap' et en choisissant un style 'impulse' (en rose sur le graphe).



Les trames font ici 480 octets, soit une charge globale de 3840 bits/s ce qui est relativement négligeable par rapport aux autres protocoles présents sur le graphe ci-dessus.